HITACHI
Inspire the Next

Hitachi Unified Storage VM

Security Target

Issue date:	Apr. 18, 2016
Revision:	4.8
Prepared by:	Hitachi, Ltd.

This document is a translation of the evaluated and certified security target written in Japanese.

- Table of Contents -

List of tables

List of figures

1 ST overview

This chapter describes Security Target (hereinafter referred to as “ST”) reference, TOE reference, TOE overview and TOE description.

1.1 ST reference

This section describes ST identification information.

Title	: Hitachi Unified Storage VM Security Target
Version	: 4.8
Issue date	: Apr. 18, 2016
Created by	: Hitachi, Ltd.

1.2 TOE reference

This section describes TOE identification information.

TOE : Hitachi Unified Storage VM Control program

TOE version : 73-03-09-00/00(H7-03-10_Z)

It consists of the following programs

・ DKCMAIN micro-program	73-03-09-00/00
・ SVP micro-program (Including Storage Navigator program (Storage management user interface software))	73-03-06/00
・ JDK	1.6.0_45
・ Apache	2.2.24
・ Apache Tomcat	6.0.16
・ OpenSSL	1.0.1g
・ ActivePerl	5.10.0.1004
・ Flash Player	10.1.53.64

TOE consumer : Domestic TOE consumers are defined as people who purchase disk storage products including TOE. The distribution procedure until the products are provided to end-users is guaranteed. Overseas TOE consumer is the customer, Hitachi Data Systems. The distribution procedure until TOE is provided to the end-user is guaranteed.

Keyword : Disk storage, SAN, RAID, Virtualization, Role-base access control

Developed by : Hitachi, Ltd.

1.3 TOE overview

1.3.1 TOE type

TOE is the control program (software) that runs the disk storage system of Hitachi, Ltd., “Hitachi Unified Storage VM” (hereinafter called “HUS VM”).

1.3.2 Environment where TOE is used

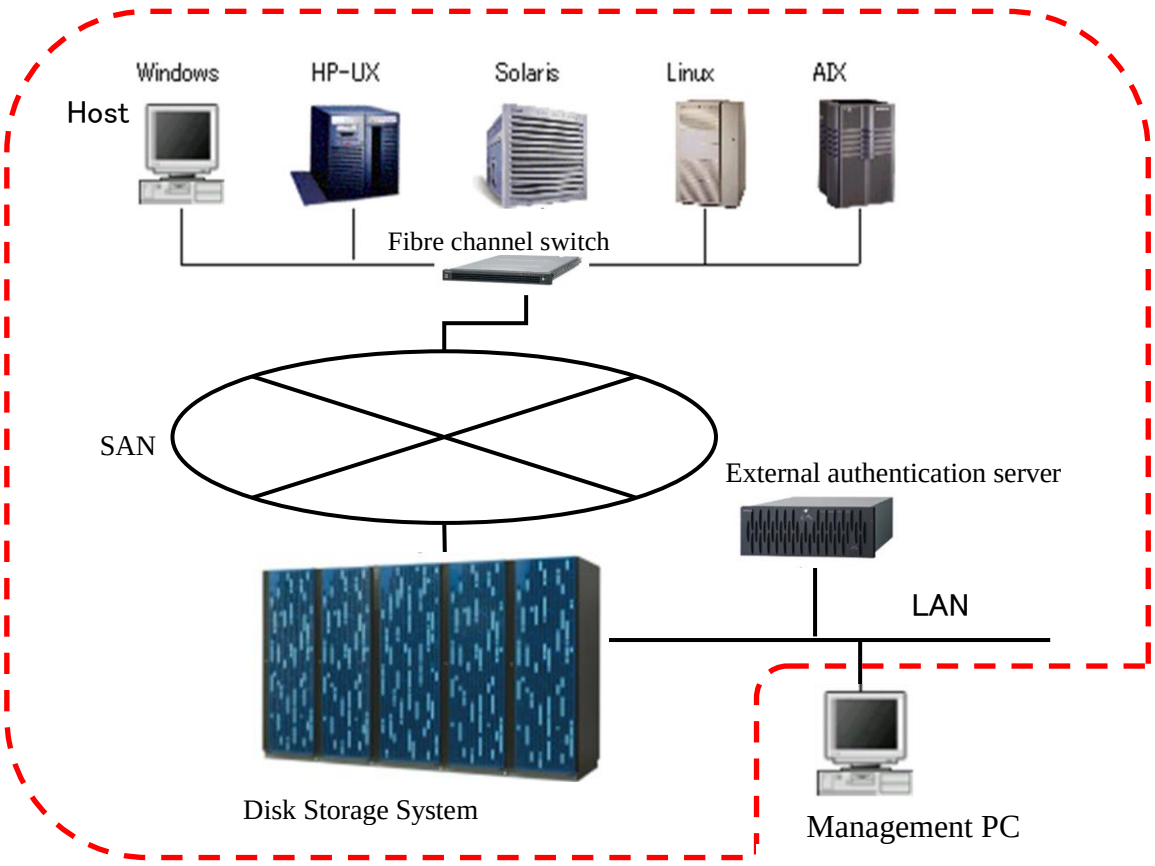


Figure 1-1 General system configuration that contains disk storage system

The following describes devices in the environment shown in Figure 1-1.

(1) Disk storage system

Normally the disk storage system in which TOE is installed is installed in a secure area where entry and exit are managed.

(2) SAN and host

Various open-system servers, such as Windows, HP-UX, and Solaris (These devices are referred to collectively as “hosts” in this ST) and disk storage systems are connected via SAN (Storage Area Network). SAN is a network dedicated to storage system that connects hosts and the disk storage system using a fibre channel.

To connect the host to SAN, it is necessary to install the fibre channel connection adapters (hardware, software) in the host. The disk storage system identifies the host by using the identification information in the fibre channel connection adapter. The identification information in the fibre channel connection adapter is set by the storage resource administrator (see 1.3.3) when connecting the host to the disk storage. Normally the host is installed in a secure area where entry and exit are managed.

Also, if required based on the security policy of the organization, TOE can identify/authenticate the fibre channel switch that is connected with the disk storage system. In this case, the fibre channel switch needs to identify/authenticate the connected host. The disk storage system identifies the fibre channel switch by using the identification information in the fibre channel switch. The identification information in the fibre channel switch is set by the security administrator (see 1.3.3) when connecting the fibre channel switch to the disk storage system. Normally the fibre channel switch is installed in a secure area where entry and exit are managed.

(3) Management PC

The management PC is used to set the configuration information of disk storage system remotely. It runs the program to enable the administrator of the disk storage system to set the configuration information in the management PC. The management PC and the disk storage system are connected via LAN (Local Area Network).

(4) External authentication server

The external authentication server is used to identify/authenticate the user when the administrator of the disk storage system accesses the disk storage system. Just like the disk storage system and hosts, it is installed in a secure area where entry and exit are managed.

1.3.3 Relevant personnel

The ST intends for the following users as relevant personnel to disk storage systems.

- Security administrator:

  The security administrator can register, modify and delete administrator accounts using the storage management user interface (UI) software called Storage Navigator program (see 1.4.2). Also, the administrator can assign the management authority of the group of storage resources, called “resource group” to a specific user. In addition to the above, the administrator can make an identification setting of the host, make identification and authentication settings of the fibre channel switch, and perform an encryption operation of stored data.

- Storage resource administrator:

  The administrator can manage resources assigned to the security administrator (such as port, cache memory, and disk) by using Storage Navigator program (Storage management UI software).

- Audit log administrator:

  The audit log administrator can manage audit logs obtained in disk storage systems. The administrator can refer and download the audit logs and make setting related to syslog using the Storage Navigator program (Storage management UI software).

- Maintenance personnel

  The maintenance personnel belong to an entity specialized in maintenance with whom customers who use the disk storage system sign contracts concerning maintenance. They are responsible for initial startup process in installing the disk storage system, changing settings required in maintenance activities such as parts replacement or addition, and disaster recovery.

Maintenance personnel access PC called SVP PC (Management maintenance IF PC) (see 1.4.2) that provides interface for maintenance/management of disk storage system from a PC for maintenance person (maintenance PC) to perform maintenance operations. Only maintenance personnel can directly contact parts inside the disk storage system and operate devices connected to the internal LAN. All resources of the disk storage system are assigned to the maintenance personnel and they can perform operations allowed by maintenance role (see Table 1-2). The TOE recognizes person who uses an interface to access SVP PC (Management maintenance IF PC) from the maintenance PC (see 1.4.2) as "the maintenance personnel" role.

- Storage user:

It is a user of disk storage system (represents a host) who uses data stored in the disk storage system through the host connected to the disk storage system.

The security administrator, storage resource administrator and the audit log administrator are hereinafter collectively called the storage administrator.

1.3.4 How to use TOE and major security feature

HUS VM is a disk storage system for companies that require multi-platform, high performance, high response and large capacity. It provides expandable connectivity, virtualization of external storages, logical resource partitioning, remote copy function and expandable disk capacity in environment of different system.

To a disk storage system, many hosts of variety type of platforms will be connected via the SAN environment or the IP network environment (In this ST, how to operate the disk storage system using the SAN environment is described). If an unauthorized operation is done in this disk storage system connection, it may result in unintended accesses to user data in the disk storage system. For this, the access control is required for the user data in disk storage system.

Under the condition that multiple storage resource administrators manage resources in a disk subsystem (such as port, cache memory and disk) a setting beyond the authority is made. The TOE therefore divides the port, disk (parity group (see 8.1.1)) and cache memory into multiple resource groups, and the multiple resource groups are assigned to each storage resource administrator. The assignment of authority for resource management allows each storage resource administrator to access the resource without affecting other resources. The control program for HUS VM, the TOE, consists of DKCMAIN micro-program, SVP program, Storage Navigator program (Storage management UI software), JDK, Apache, Apache Tomcat, OpenSSL, Flash player, and ActivePerl. The DKCMAIN micro-program controls resources in the disk storage system while the SVP program does authorities for administrators of disk storage system. The Storage Navigator program (Storage management UI software) is contained in the SVP program and can be used by downloading it from SVP PC (Management maintenance IF PC) to a management PC. Hereinafter the Storage Navigator program (Storage management UI software) is called Storage Navigator (Storage management UI software). JDK, Apache, Apache Tomcat, OpenSSL, Flash player, and ActivePerl are software (application/library) that are installed to realize the functions provided by SVP PC (Management maintenance IF PC).

This ST describes the security features to protect confidentiality and integrity of user data on HUS VM by providing functions to prevent unauthorized access to storage resources assigned to specific storage users from other storage users, and to encrypt and shred the user data in disk drive.

(a) to (h) show the security features provided by the TOE.

[Security features TOE provides]

(a) Access control of storage administrator and maintenance personnel:

Accounts of storage administrator and maintenance personnel who access the TOE belong to groups. More than one role (see 1.4.4.2.1) and more than one resource group are assigned to a group. The

resource group is of divided storage resource into multiple groups, and each account can execute control operations allowed by the role for resource in the assigned resource group.

(b) Host access control:

It performs access control to LDEV (logical volume) in the disk storage system from the host.

(c) Identification and authentication of fibre channel switch:

It identifies and authenticates fibre channel switches to prevent accesses from an unauthorized host to the disk storage system.

(d) Identification and authentication of storage administrator and maintenance personnel:

It controls, identifies, and authenticates storage administrator and maintenance personnel who access the TOE. It also can identify and authenticate storage administrator and maintenance personnel by using an externally connected authentication server (external authentication server).

(e) Encrypted communication between Storage Navigator (Storage management UI software) and SVP PC (Management maintenance IF PC), and between SVP PC (Management maintenance IF PC) and external authentication server:

It encrypts the communication between Storage Navigator (Storage management UI software) and SVP PC (Management maintenance IF PC), and between SVP PC (Management maintenance IF PC) and external authentication server.

(f) Encryption of stored data:

It encrypts user data to be stored in the disk storage system.

(g) Shredding:

It shreds user data in the disk storage system.

(h) Audit log:

It collects, refers and manages logs of configuration change and update for the disk storage system.

1.3.5 TOE and other configuration components

This section describes configuration components of hardware and software, and shows which one is included in the TOE or operating environment respectively. The hardware and software built in the disk storage system are installed at the factory shipment, and storage administrator and storage users (see 1.3.3) are not required to prepare or change them.

1.3.5.1 Hardware components

The table below shows necessary hardware components and whether each component is included in the TOE. The environment means that items are the component of other than TOE.

TOE/ environment	Configuration component	Description
Environment	Hitachi Unified Storage VM	It is the name of the disk storage system and consists of hardware and software, such as TOE, that constitutes the disk storage system. Parts excluding TOE are used in the environment.
Environment	Host	Computers that access the disk subsystem. Windows, HP-UX, Solaris, Linux and AIX are expected as host OS.
Environment	Fibre channel connection adapter	An adapter equipped in computer to connect to SAN.
Environment	Fibre channel switch	A switch to connect host with disk storage system, which constitutes the SAN. Connection between the hosts and the disk storage system equipped with TOE requires the fibre channel switch.
Environment	Management PC	Computers to administer the TOE. Requirements for the computer are; ・ CPU: Pentium 4 640 3.2GHz and higher Recommended: Core 2 Duo E6540 2.33GHz and higher ・ RAM: 2GB or larger Recommended: 3GB ・ Available HDD capacity: 500 MB and larger ・ Monitor: True Color 32 bit and higher; Resolution: 1280x1024 and higher ・ LAN card: 100Base-T
Environment	SAN	High speed network connecting disk storage system and computers by using fibre channel technology.
Environment	Other disk storage system	Other disk storage system connected with the disk storage system equipped with TOE. The other disk storage system is limited to the one equipped with TOE.
Environment	Maintenance PC	A computer used by maintenance personnel at maintenance, which is prepared by maintenance personnel.
Environment	External authentication server	A server that identifies and authenticates users by using LDAP server, and RADIUS server. - LDAP server is equipped with LDAPv3 - RADIUS server conforms to RFC2865
Environment	External LAN	LAN to connect disk storage system, management PC and external authentication server.
Environment	Internal LAN	LAN to connect package in the disk storage system and maintenance PC.

1.3.5.2 Software components

The table below shows necessary software components and whether each component is included in the TOE.

TOE/ environment	Configuration component	Description
TOE	DKCMAIN micro-program Version 73-03-09-00/00	The TOE is embedded in the disk storage system at factory shipment.
TOE	SVP program Version 73-03-06/00	It runs on SVP PC (Management maintenance IF PC) and Storage Navigator (storage management UI software) runs on management PC. The TOE is embedded in the disk storage system at factory shipment.
TOE	JDK Version 1.6.0_45	It runs on SVP PC (Management maintenance IF PC). The TOE is embedded in the disk storage system at factory shipment.
TOE	Apache Version 2.2.24	It runs on SVP PC (Management maintenance IF PC). The TOE is embedded in the disk storage system at factory shipment.
TOE	Apache Tomcat Version 6.0.16	It runs on SVP PC (Management maintenance IF PC). The TOE is embedded in the disk storage system at factory shipment.
TOE	OpenSSL Version 1.0.1g	It runs on SVP PC (Management maintenance IF PC). The TOE is embedded in the disk storage system at factory shipment.
TOE	ActivePerl Version 5.10.0.1004	It runs on SVP PC (Management maintenance IF PC). The TOE is embedded in the disk storage system at factory shipment.
TOE	Flash Player Version 10.1.53.64	It runs on SVP PC (Management maintenance IF PC). The TOE is embedded in the disk storage system at factory shipment.
Environment	SVP PC (Management maintenance IF PC) OS	SVP PC (Management maintenance IF PC) OS • Windows Vista Business US version (64bit version) SP2 It is embedded in the disk storage system at factory shipment.
Environment	Management PC OS	OS of management PC. • Windows 7 (SP1)
Environment	OS of maintenance PC	OS of maintenance PC. • Windows 7 (SP1)
Environment	Web browser	Web browser works on management PC. The following browser is supported. • Internet Explorer 8.0
Environment	Flash Player	It operates on management PC as a plug-in of web browser. The following version is used. • Flash Player witch can execute Action Script until Flash Player 10.1
Environment	Java runtime environment	Java runtime environment operates on management PC. • JRE 6.0 Update 20 (1.6.0_20)

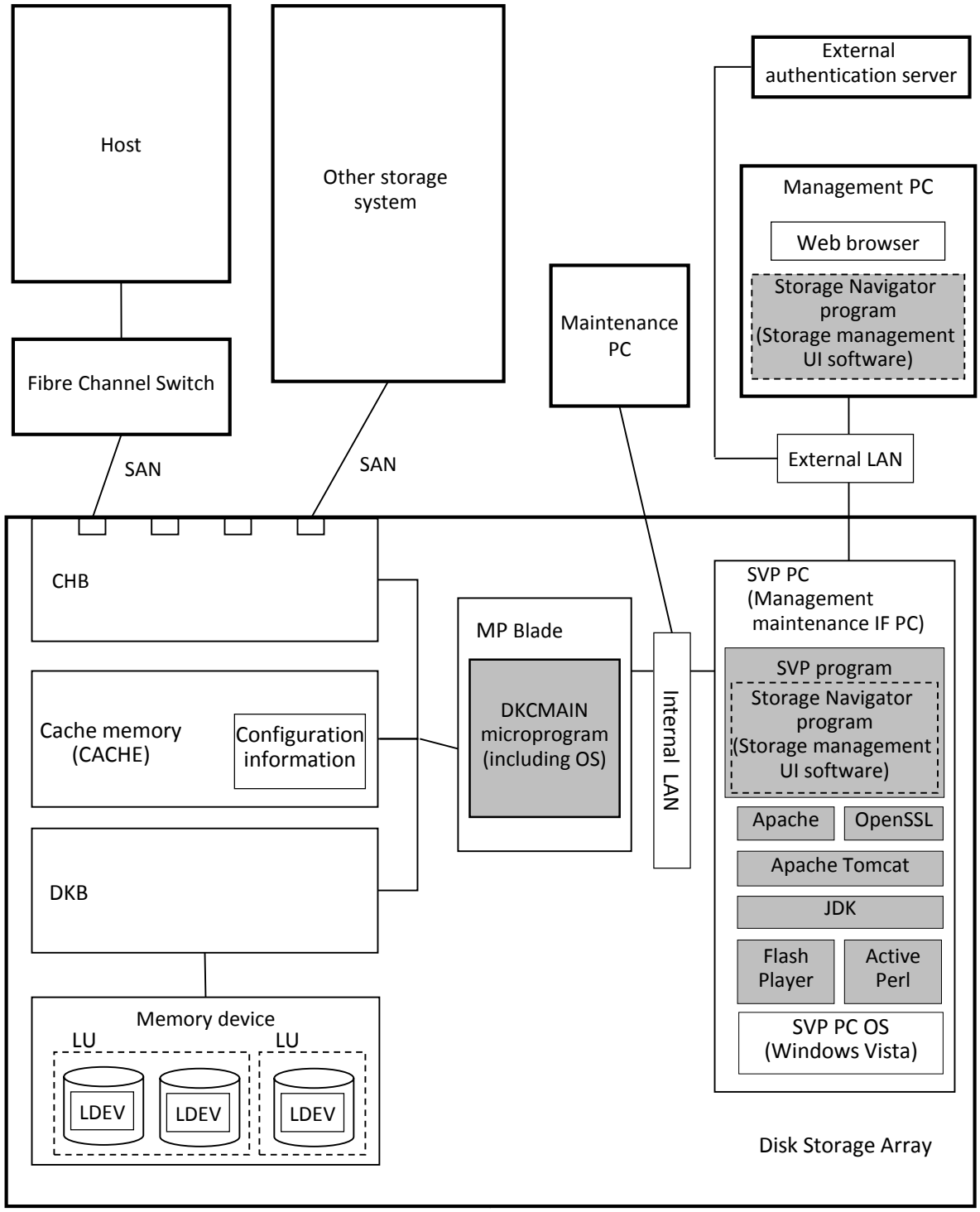
1.4 TOE description

The TOE consists of DKCMAIN micro-program, SVP program, Storage Navigator (storage management UI software), “JDK”, “Apache”, “Apache Tomcat”, “OpenSSL”, “Flash player”, and

“ActivePerl”.

The DKCMAIN micro-program is installed on multiple MP blades (see 1.4.1) in a disk storage system and has a role of controlling data transfer between the disk storage system and a host connected with the disk storage system. The SVP program is a program to execute operations and maintenances of the disk storage system. Storage Navigator (storage management UI software) provides the user interface function of SVP program.

Figure 1-2 illustrates hardware components constituting the disk storage system and shows that on which components the identified TOE sub set works.



Storage Navigator program (Storage Management UI software) consists of the Flex application and the Java applet and runs in the SVP PC and the management PC.

LU：Logical unit. The minimum unit of storage area accessed by the host. It consists of one or multiple LDEVs (logical devices).

Figure 1-2 Disk storage system configuration

The disk storage system can be divided into the control system that includes channel blade (CHB), cache memory (CACHE), disk blade (DKB), MP (microprocessor) blade, and memory device, and administration system that includes SVP (service processor). The control system controls data input and

output to and from memory device while the administration system does maintenance and management of the disk storage system. The configuration components are as follows.

The control network (CHB, CACHE, DKB, and MP blade together connected by high-speed crossbar switch) and administration network (internal LAN and external LAN) are completely independent each other. This configuration does not allow direct access from SVP PC (Management maintenance IF PC), management PC, and maintenance PC connected either to the internal LAN or external LAN, to the cache and memory device.

1.4.1 Control system

(1) Channel blade

Channel blade (CHB) processes a command from other disk storage system and hosts, which are connected through a fibre channel switch, to a local disk storage system and controls data transfer. Other disk storage system and a fibre channel switch are connected to a fibre port on the CHB.

(2) Disk adapter

Disk adapter (DKB) controls data transfer between the cache and memory device. The DKB is equipped with LSI to encrypt and decrypt the stored data as encryption function.

(3) Cache memory

Cache memory (CACHE) is located between CHB and DKB and is commonly accessible from DKCMAIN micro-program. The configuration information to access the data through CHB and DKB is stored in it to be used for data reading and writing. The configuration information on the memory can be accessed only through the DKCMAIN micro-program.

(4) MP blade

One quad core CPU is equipped in one blade for DKCMAIN micro-program to work.

(5) Memory device

Memory device consists of multiple disk drives and is used to store user data. In the memory device, an LDEV (logical volume) which is a volume to store user data is created. Access to the user data is controlled per LDEV (logical volume), and done via DKCMAIN micro-program. A part of or all data in the LDEV (logical volume) can be allocated to cache memory so as to enable high speed data access.

An LU (logical unit), which is an access unit from a host, is mapped to one or more LDEV (logical volume).

LDEVs (logical volumes) are created on a parity group in the memory device. The parity group is a series of disk drives handled as one data group, and composes RAID by storing the user data and parity information. This RAID configuration enables accesses to the user data even when one or more drive in the parity group is unavailable, which improves the reliability.

CHB, CACHE, DKB and MP blade are connected each other by the high-speed crossbar switch.

1.4.2 Administration system

(1) SVP PC (Management maintenance IF PC)

The SVP PC (Management maintenance IF PC) is PC that provides interface for maintenance/management for disk storage system. It operates as a service processor embedded in the disk storage system to manage the entire disk storage system, and SVP program, which is a part of TOE, runs on it. The SVP program is the software to manage configuration information and maintenance function of the disk storage system, and has a function to send DKCMAIN micro-program a command to set configuration information received from Storage Navigator (storage management UI software) that works on management PC. It also has a function related to operations of security function in the disk storage system. JDK, Apache, Apache Tomcat, OpenSSL, Flash player, and ActivePerl are software

(application/library) installed to realize functions provided by SVP PC (Management maintenance IF PC).

(2) Maintenance PC

The maintenance PC is the PC used by maintenance personnel at maintenance. It is connected to the SVP PC (Management maintenance IF PC) by remote desktop function via internal LAN which is the network in the disk storage system.

(3) Management PC

Management PC is a customer's PC used by the storage administrator (see 1.3.3) for disk storage system operations and maintenance. Storage Navigator (storage management UI software), which is a part of TOE, works on it. The management PC and the SVP PC (Management maintenance IF PC) are connected via the external LAN.

(4) External authentication server

The external authentication server identifies and authenticates users by a request from the SVP program when the storage administrator (see 1.3.3) accesses TOE using Storage Navigator (storage management UI software), and returns to the SVP program the authentication result and user group information (see 1.4.4.2.1) that is a basis of approval information when the authentication succeeds. The communication between the SVP PC (Management maintenance IF PC) and the external authentication server is encryption communication.

(5) Storage Navigator program (storage management UI software)

Storage Navigator (storage management UI software) is software used by the storage administrator (see 1.3.3) to manage configuration information of disk storage system.

Storage Navigator (storage management UI software) consists of Flex application and Java applet. The Flex application executes operations specified from Web browser on the management PC on the SVP PC (Management maintenance IF PC), and displays the result on the Web browser of the management PC Java applet on the other hand downloads programs from the SVP PC (Management maintenance IF PC) to the management PC. The programs run on the management PC. The communication between the SVP PC (Management maintenance IF PC) and Storage Navigator (storage management UI software) uses SSL. The storage administrator interacts with Storage Navigator (storage management UI software) using the web browser of the management PC to perform setting operations of the disk storage system.

In order to prevent unauthorized use of Storage Navigator (storage management UI software) by any malicious third party (see 3.1), Storage Navigator (storage management UI software) identifies and authenticates users in collaboration with the SVP program.

1.4.3 Other disk storage systems

To a port of channel adapter mounted on the disk storage system, an external disk storage system can be connected other than hosts. Sending and receiving commands to and from another disk storage system via the channel adapter enables data copy and backup between disk storage systems. When data copy is executed on the data sending side, backup is executed on the data receiving side. Copy operations executed from another disk storage system is executed by a reliable storage resource administrator. In addition, as the disk storage system and another one shares their own data each other, a reliable storage resource administrator is essential. Therefore, other disk storage system connected with the disk storage system is limited to the one with the TOE installed.

1.4.4 TOE functions

Basic function and security function the TOE provides are as follows.

1.4.4.1 Basic functions TOE provides

Table 1-1 shows a part of the basic functions provided by the TOE.

Table 1-1 Basic functions provided by TOE

Function	Description
Customized volume size function	The customized volume size function can regard multiple LDEVs (logical volumes) as free space and create multiple customized volumes in arbitrary size, which enables effective use of disk capacity.
Cache memory management function	Specific data in an LDEV (logical volume) is resident in cache memory. The resident data can always be accessed by memory access function.
Performance information management function	Monitoring Resource usage rate in disk subsystem, disk load and port load measurement are enabled.
External storage management function	The function realizes virtualization (virtualization technology) of disk storage. By using the external storage management function, multiple disk subsystems including HUS VM can be handled as one disk subsystem. It also allows the system administrator to easily manage multiple disk storage systems in different types.
Remote copy function	In HUS VM, replica volumes can be created at remote site without passing through a server. The replica can be used for backup as a measure for not only local/regional but also large-scale disasters. Without passing through a host, by updating the replica volume in synchronization with update at the main site, remote copy between disk subsystems is realized. For the connection between disk subsystems, fibre channel is used.
Asynchronous remote copy function	This is an asynchronous remote copy function with a new technology. Adapting the technology to accumulate update records (journal) in a disk drive with capacity larger than cache can realize stable copy which is less affected by fluctuations of bandwidth and operation traffic.
Local copy function	Volume replication to create a replica of logical volume in a disk subsystem without passing through a host is enabled. Using the replica allows obtaining backup in the same database and concurrent processing such as batch processing while continuing online operation for the data base and minimizing the impact on operating performance.
Virtual volume management function	With the virtual volume management function, the data of volume in a pool is accessed via a virtual volume. For the virtual volume and pool volume, thresholds are set to continuously monitor overflow of the area, which eventually brings the following effects. - Cost reduction at implementation by reducing operating rate of volumes. - Prevention of increases in management cost and time period of no operation due to the stop of operation while establishing the system.

1.4.4.2 Security functions TOE provides

1.4.4.2.1 Access control function of storage administrator and maintenance personnel

In an intensive environment with large-scale storage where data of multiple companies, departments, systems and applications exist in a disk subsystem, so-called Multi-tenancy function to manage storage operations individually by assigning storage resource administrators per company or department is required. The Multi-tenancy function promises cost reduction by effective use of resource and management simplification by dividing.

In Multi-tenancy environment, a security mechanism not to destroy the data of other organization by mistake, not to leak the data to other organization, and not to affect operations by other storage resource administrator is necessary.

Access control function of storage administrator and maintenance personnel is per user group. A role and a resource group, a group of resources which can be controlled by the role, are assigned to the user group. Figure 1-3 shows the relationship between user (administrator), user group, resource group and role.

This function enables each user to perform flexible resource allocation and realizes the above security.

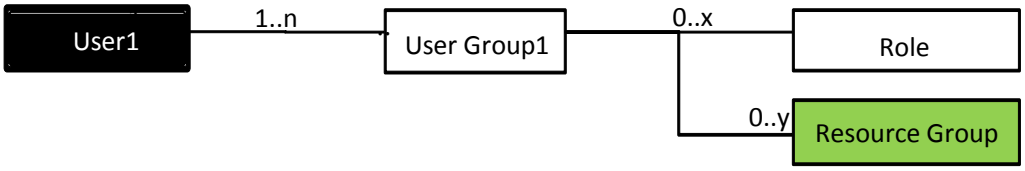


Figure 1-3 Relationship between user, user group, role and resource group

A user belongs to one or more user group. The user group is assigned roles and resource groups and uses them as approved information. The user group information is obtained from SVP PC (Management maintenance IF PC) or external authentication server to be used. Each account can execute management operation allowed by the assigned role for the assigned resource.

(1) Role

The security administrator creates a user account using Storage Navigator (storage management UI software) and registers it to a user group.

Permission of which operation is assigned to a user is determined based on the role assigned to the user group. The role has categories as follows.

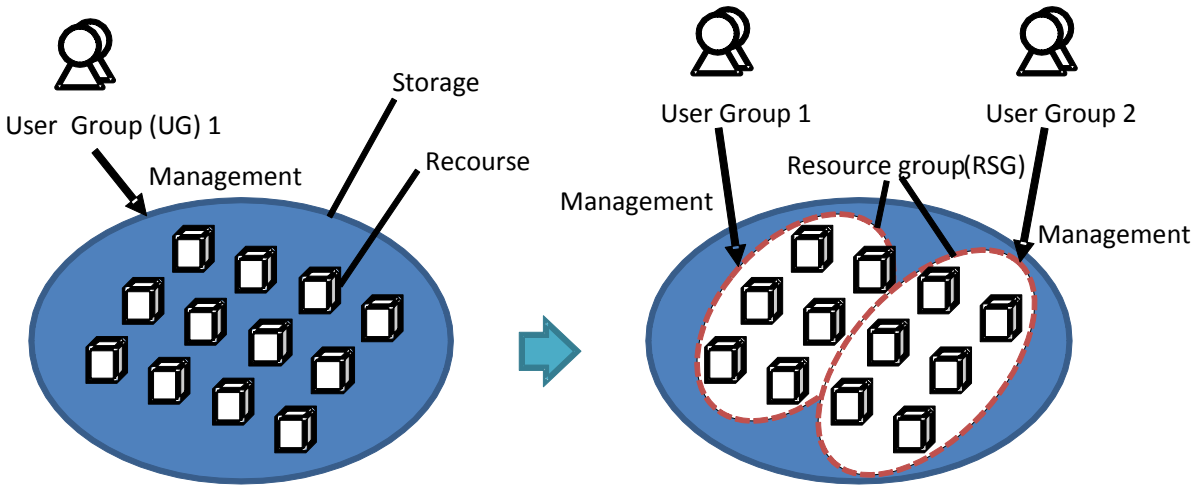
Table 1-2 Role category and operation

Role	Allowed operation
Security administrator role	A role that is assigned to security administrator and can perform user management operations, resource management operations, identification and authentication setting operations of host and fibre channel switch, encryption of stored data, and management of external authentication server.
Audit log administrator role	A role that is assigned to audit log administrator and can execute operations related to audit logs.
Storage administrator role	A role that is assigned to storage resource administrator and can perform storage management operations in the permitted resource group.
Maintenance role	A role that is assigned to maintenance personnel and can perform maintenance operations of the disk storage system.

(2) Resource group

Dividing storage resource into multiple groups is called resource group (RSG). Each resource group is assigned a number (RSG number) for identification. Also, each resource group is assigned to a user group and each storage resource administrator can perform management operation within the range of resource group assigned to the user group the administrator belongs to. As all resource groups are assigned to

maintenance personnel, they can perform maintenance for all storage resources.



1.4.4.2.2 Host access control

LDEV (logical volume) that stores user data is created by using Storage Navigator (storage management UI software). In order to access the LDEV (logical volume) from a host, the LDEV (logical volume) needs to be associated with a port on CHB connected to the host. In particular, LU number is assigned to associate the host and the LDEV (logical volume) to be accessed to set LU path. Data reading and writing for the corresponding LDEV (logical volume) is enabled only from the host with the LU path setting. In other words, data reading and writing from hosts without LU path setting are not allowed.

1.4.4.2.3 Identification and authentication of fibre channel switch connected with hosts

When connecting a host to SAN, the connection management is done in a customer operation to prevent unauthorized host connection. If the prevention of impersonation is required to further ensure safety based on the organization's security policy, identification and authentication by the FC-SP function (see 8.1.1) is available for the communication between the fibre channel switch and the port of the disk subsystem. The port of the disk subsystem can identify and authenticate the fibre channel switch, and the fibre channel switch can identify and authenticate the disk subsystem port as well. For the fibre channel switch identification and authentication setting, a security administrator uses the access control function of the fibre channel switch and sets each fibre channel whether to identify and authenticate the fibre channel switch. Also, the security administrator registers to the disk subsystem the authentication data (WWN, secret) of the fibre channel switch to identify and authenticate. The secret is a password for authentication and consists of 12 to 32 characters of alphanumeric and symbols.

1.4.4.2.4 Identification and authentication of storage administrator and maintenance personnel

Storage Navigator (storage management UI software) is used by customers to manage disk subsystem including security setting. The TOE executes user identification and authentication at disk subsystem management (configuration of each function and setting change) using Storage Navigator (storage management UI software) and remote desktop connection to SVP PC (Management maintenance IF PC) by maintenance personnel. If the identification and authentication fails three times in a row, the identification and authentication of the user is rejected for one minute.

As user authentication, the following 2 methods are supported.

(1) SVP PC (Management maintenance IF PC) internal authentication

ID and password of users are registered in the SVP PC (Management maintenance IF PC), and the TOE authenticate. The password used for user authentication is 6 to 256 letters with a combination of alphanumeric characters and symbols. (The password of maintenance personnel is 127 letters)

(2) External authentication server

The SVP PC (Management maintenance IF PC) does not manage ID and password but the ID and the password are sent to an external authentication server and the authentication result is sent back. After the success of authentication by the external authentication server, the user group information is obtained from the server and used as approved information. As protocols for user authentication, LDAP (Encryption supports LDAPS, starttls), and RADIUS (authentication protocol is CHAP) are supported.

1.4.4.2.5 Encrypted communication between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC), and between SVP PC (Management maintenance IF PC) and external authentication server

To prevent the falsification and leakage of communication data between disk storage system and the management PC, the communication between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC) is encrypted by SSL. In addition, one of LDAPS, starttls, and RADIUS (authentication protocol is CHAP) protocols is employed for the communication between the SVP PC (Management maintenance IF PC) and the external authentication server to protect passwords of the storage administrator and maintenance personnel.

1.4.4.2.6 Encryption of stored data

The TOE can encrypt the data stored in a volume in the storage system. For encryption and decryption, LSI mounted in DKB is used. Encrypting data can prevent the information from being leaked at replacement of disk drive in the storage system or when the data is stolen. In addition, the following key management functions are available.

- Encryption key creation
- Encryption key deletion
- Encryption key backup and restoring

Only security administrator with user account can operate the encryption of stored data function.

1.4.4.2.7 Shredding

This is a function to disable to restore data by writing dummy data over all the data in a volume, so as to avoid data leakage and unauthorized use at reuse of the volume.

When the Shredding is executed, dummy data is written in the volume containing user data and the user data cannot be restored. The function complies with DoD5220.22-M, recommends writing dummy data at least 3 times. The dummy data is overwritten 3 times in the volume as default setting.

Only storage administrator with user account can operate the Shredding function.

1.4.4.2.8 Audit log

The audit log function is provided by SVP program (including Storage Navigator (storage management UI software)) and DKCMAIN micro-program. Storage Navigator (storage management UI software) records events related to the security such as success/fail of login and configuration/setting change.

The maximum number of letters in a line of audit log is 1,024 (single byte), and up to 250,000 lines

information is stored on the HDD in SVP PC (Management maintenance IF PC). Storage Navigator (storage management UI software) provides the interface to refer audit logs.

1.4.5 Guidance documentation

Guidance documents for the TOE are as follows.

(1) Users guide for security function

- Hitachi Unified Storage VM ISO15408 Function of Acquiring Authentication; Instruction manual Ver. 2.9
- Hitachi Unified Storage VM Storage Navigator User Guide 8th edition
- Hitachi Unified Storage VM Storage Navigator Messages 8th edition
- Hitachi Unified Storage VM Provisioning Guide 10th edition
- Hitachi Unified Storage VM Encryption License Key User Guide Second edition
- Hitachi Unified Storage VM Volume Shredder User Guide 4th edition
- Hitachi Unified Storage VM Audit Log User Guide 6th edition
- Hitachi Unified Storage VM Operations Using Spreadsheets 3rd edition
- Hitachi Unified Storage VM User Guidance Ver.1.8
- Hitachi Unified Storage VM Manual for Obtaining ISO15408 Certification Ver. 1.9
- Hitachi Unified Storage VM Block Modular Hitachi Storage Navigator User Guide MK-92HM7016-06
- Hitachi Unified Storage VM Block Modular Hitachi Storage Navigator Messages MK-92HM7017-03f
- Hitachi Unified Storage VM Block Modular Provisioning Guide MK-92HM7012-07
- Hitachi Unified Storage VM Block Modular Hitachi Encryption License Key User Guide MK-92HM7051-00
- Hitachi Unified Storage VM Block Module Hitachi Volume Shredder User Guide MK-92HM7021-03
- Hitachi Unified Storage VM Block Modular Hitachi Audit Log User Guide MK-92HM7009-03d
- Hitachi Unified Storage VM Hitachi System Operations Using Spreadsheets MK-92HM7015-01
- Hitachi Unified Storage VM User's Guidance Ver.1.5

(2) Disk subsystem maintenance manual

- Hitachi Unified Storage VM ISO15408 Function of Acquiring Authentication; Maintenance manual Ver. 2.3
- HT-40SA Disk Array System Maintenance ManualREV.4.5
- Hitachi Unified Storage VM Obtaining ISO15408 Certification Maintenance Manual Ver. 1.6
- DW700 Maintenance Manual REV. 4.5

1.5 Evaluation Environment

The TOE evaluation environment is as follows. The following management PC, fibre channel switch, fibre channel connection adapters are used in the TOE evaluation.

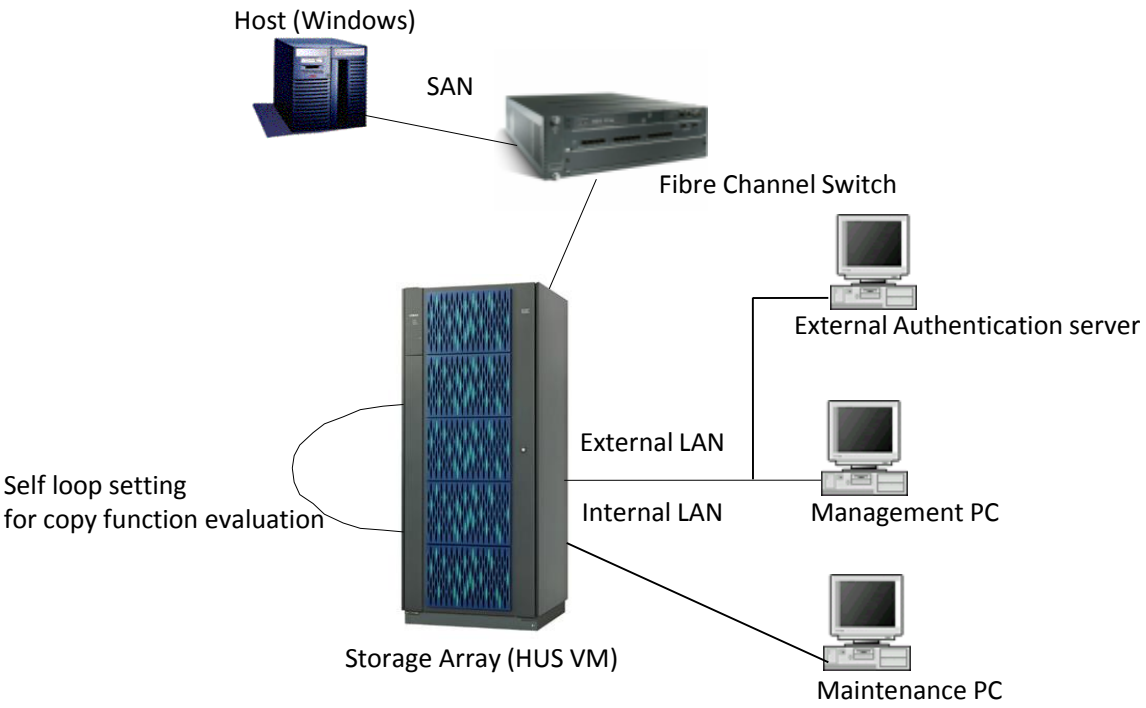


Table 1-3 TOE components used for evaluation

No.	Component	Software/OS
1	Hitachi Unified Storage VM	DKCMAIN micro-program: 73-03-09-00/00
2	SVP	SVP micro-program: 73-03-06/00 JDK: 1.6.0_45 Apache: 2.2.24 Apache Tomcat: 6.0.16 OpenSSL: 1.0.1g ActivePerl: 5.10.0.1004 Flash Player: 10.1.53.64

Table 1-4 Physical components of Hitachi Unified Storage VM used for evaluation

No.	Component	Number	Description
1	Hitachi Unified Storage VM	1	
1-1	MP blade	2	
1-2	CHB	4	
1-3	Encryption DKB	2	
1-4	Cache	4G×16	
1-5	2.5-inch Disk Drive	12	Three RAID1(2D+2D) parity groups

Table 1-5 Host for Evaluation

No.	Host OS
1	Windows 2008 Server

Table 1-6 Management PC for Evaluation

No.	Management PC OS	Java runtime environment	Web browser and Plug-in
1	Windows7 (SP1)	JRE 1.6.0_20	Internet Explorer 8.0 Flash Player 10.1
2	Windows7 (SP1)	JRE 1.6.0_20	Internet Explorer 8.0 Flash Player 16.0

Table 1-7 Maintenance PC for Evaluation

No.	Maintenance PC OS	Java runtime environment	Web browser and Plug-in
1	Windows7 (SP1)	JRE 1.6.0_20	Internet Explorer 8.0 Flash Player 10.1

Table 1-8 External Authentication Server for Evaluation

No.	External Authentication Server OS	Software
1	Windows 2008 Server	Active Directory LDAP v3 support RFC2865 compliant

Table 1-9 Fibre Channel Switch for Evaluation

No.	Switch	Model Name	FW version
1	Brocade300	BR-360-0008	Fabric OS v6.4.1b
2	Brocade6505	ER-7000-0340	Fabric OS v7.2.0c

Table 1-10 Fibre Channel Connection Adapter for Evaluation

No.	Fibre Channel Connection Adapter	Model	Driver	Version
1	Qlogic Fibre Channel Adapter	QLE2564-CK	Fibre Channel Adapter STOR miniport driver	3.14.0.0 or 9.1.4.6
2	Brocade 16G FC HBA	BR-1860-2P00	bfa	3.2.1.0

2 Conformance claim

2.1 CC conformance claim

This ST complies with the following standards.

Common Criteria for Information Technology Security Evaluation

Part1: Introduction and general model Version 3.1 Revision 4

Part2: Security functional components Version 3.1 Revision 4

Part3: Security assurance components Version 3.1 Revision 4

Security functional requirements: Part2

Security assurance requirements: Part3

2.2 PP conformance

This ST does not claim compliance with any PP.

2.3 Package name conformant

This ST complies with package: EAL2. Assurance component of ALC_FLR.1 is added.

3 Security Problem Definition

3.1 TOE assets

The most important asset for disk storage system is the user data of storage user stored in disk drives. In order to maintain integrity and confidentiality of the user data, the user data is protected from unauthorized access by a third party, and from setting change outside authority by the storage administrator. In addition, for sniffing of communication data between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC) and between SVP PC (Management maintenance IF PC) and external authentication server by a third party who can connect to external LAN, TSF data (user ID and password) contained in the communication data must be protected by utilizing high reliable channel.

In the ST, the user data of storage user exists in a resource group is the asset subject to protection in the environment of large-scale storage with data of multiple companies, departments, systems and applications in disk subsystem, and the asset is protected from unauthorized accesses by a third party.

3.2 Threats

The TOE counters threats shown below. A third party in the following description means a person who is none of storage administrator, storage user, and maintenance personnel, and is not authorized to use the disk storage system.

T.TSF_COMP	A third party may impersonate the storage administrator by obtaining the communication data including ID and password of the storage administrator wrongly from external LAN to change disk storage system setting and may access the LDEV (logical volume) where user data is stored.
T.LP_LEAK	In a SAN environment where multiple hosts are connected to the same port, a third party may be able to leak, falsify, and delete user data by accessing LDEV (logical volume) of a specific host from other host.
T.CHG_CONFIG	A third party may be able to leak, falsify, and delete user data by wrongly changing the access setting for LDEV (logical volume) in the disk storage system.
T.HDD_THEFT	When returning a disk drive to the vendor for preventive maintenance or failure, the disk drive may be stolen while it is delivered, and the user data could be leaked.
T.HDD_REUSE	The user data in the disk drive may be leaked to a third party due to reuse of the disk storage system or reuse of the disk drive.

3.3 Organizational security policies

P.MASQ	If a customer requests identity authentication of a fibre channel switch that is connected to hosts, the fibre channel switch that is connected to hosts is identified and authenticated.

3.4 Assumptions

A.NOEVIL	Within storage administrators, the security administrator and audit log administrator are assumed to be the qualified person who is capable of operating and managing the entire disk storage system, executes proper operations as specified by manuals, and never commit any wrongdoing. The storage resource administrator is assumed to be the qualified person who is capable of managing and operating a disk subsystem to the range permitted by the security administrator and executes proper operations as specified by manuals and never commits any wrongdoing.
A.PHYSICAL_SEC	The security administrator installs the disk storage system, host (including fibre channel connection adapter), devices that constitute the SAN environment (fibre channel switch, cable), other disk storage system, and external authentication server in a secure area where entry and exit are managed. Operation and management are performed, so that the setting values (such as WWN) that are set in each device and the connection status (connection status to SAN) would be maintained properly.
A.MANAGE_SECRET	The secret for fibre channel switch authentication that is set in the fibre channel switch connected to hosts is assumed to be controlled under the security administrator's responsibility to protect it from the use by unauthorized person.
A.MANAGEMENT_PC	The storage administrator is assumed to install and manage the management PC at a secure area to protect it from unauthorized use.
A.MAINTENANCE_PC	When the responsible official of the organization signs a maintenance contract, accept maintenance personnel and the maintenance PC. Allow maintenance personnel in a secure area and permit maintenance personnel to install the maintenance PC. Also people other than maintenance personnel do not use the maintenance PC wrongly.
A.CONNECT_STORAGE	Other disk storage systems connected to TOE are assumed to be limited to those TOE is embedded.
A.EXTERNAL_SERVER	An external authentication server is assumed to be capable of using authentication protocol (LDAPS, starttls and RADIUS (authentication protocol is CHAP)) which can protect communication with SVP PC (Management maintenance IF PC) supported by the TOE, and registering and managing user identification information and user group information while keeping consistency with the TOE.

4 Security objectives

This chapter describes TOE security objective, operational environment security objective, and security objective rationale.

4.1 TOE security objectives

The TOE security objectives are as follows.

O.ADM_AUTH	The TOE must succeed the identity authentication of storage administrator and maintenance personnel before the storage administrator and maintenance personnel execute the management operations of disk subsystem.
O.ADM_ROLE	The TOE must control the management operations done by the storage administrator and maintenance personnel as follows. − Security administrator can perform user management operation, resource management operation, host and fibre channel switch identification and authentication setting, encryption of stored data, and management operations of the external authentication server. − Audit log administrator can perform operations related to audit log. − Storage resource administrator can perform storage management operation within the permitted resource group. − Maintenance personnel can perform disk storage system maintenance operations.
O.SEC_COMM	The TOE must provide the communication function which is secured by the encrypted data on the channel between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC), and between SVP PC (Management maintenance IF PC) and external authentication server to protect from sniffing of the data from the communication path between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC) and between SVP PC (Management maintenance IF PC) and external authentication server.
O.SWITCH_AUTH	The TOE must perform identity authentication of the fibre channel switch that is connected with hosts by the FC-SP function when the fibre channel switch is connected.
O.HOST_ACCESS	The TOE must identify hosts to control that only the host which is allowed to connect to the disk storage system can access the permitted LDEV (logical volume).
O.HDD_ENC	The TOE must manage encryption key to encrypt the stored data to prevent the user data from being leaked from the disk drive taken out of the disk storage system.
O.HDD_SHRED	The TOE must shred the user data to make sure that the user data does not remain in the disk drive when the disk drive in the disk storage system is replaced or stops to be used.
O.AUD_GEN	The TOE must track events regarding the security such as identity authentication and setting change operation.

4.2 Operational environment security objectives

The operational environment security objectives are as follows.

OE.NOEVIL	The representative of organization must assign person who is capable of managing and operating the entire disk storage system, executes proper operations as specified by manuals, and never commits any wrongdoing to security administrator and audit log administrator within storage administrators. The storage resource administrator must be assigned to the qualified person who has been trained to execute proper operations as specified by manuals and never commits any wrongdoing to manage and operate disk subsystem to the range permitted by the security administrator.
OE.PHYSICAL_SEC	The security administrator installs a disk storage system, host (including fibre channel connection adapter), devices that constitute a SAN environment (fibre channel switch, cable), other storage system and external authentication server in a secure area where only storage administrator and maintenance personnel are allowed. They must be completely protected from unauthorized setting changes and switching the connection target.
OE.MANAGE_SECRET	The security administrator must control the secret for fibre channel switch authentication set in the fibre channel switch to protect it from the use by unauthorized person.
OE.MANAGEMENT_PC	The storage administrator must properly install and manage the management PC to protect it from unauthorized use.
OE.MAINTENANCE_PC	Maintenance personnel install the maintenance PC in a secure area appropriately according to instructions of the responsible official of the organization. The maintenance PC must be protected, so that other people than maintenance personnel cannot use it.
OE.CONNECT_STORAGE	Other disk storage systems connected to the TOE must be limited to those with TOE embedded
OE.EXTERNAL_SERVER	The security administrator must use protocol (LDAPS, starttls, and RADIUS (authentication protocol is CHAP)) which can protect the communication with SVP PC (Management maintenance IF PC) supported by the TOE for external authentication server, and properly register and control the user identification information and user group information while keeping the consistency with TOE.
OE.FC-SP_HBA	When identification and authentication of fibre channel switch connected hosts is required, a fibre channel connection adapter with the FC-SP function and a fibre channel switch with the FC-SP function must be used.
OE.HDD_ENC	In operational environment, a disk storage system which is capable of encrypting user data by using LSI equipped in DKB must be used to prevent the user data from being leaked from disk drive.

4.3 Security objective rationale

The security objective must be to address to assumptions stipulated in Security problem definition, to counter threats or to realize organizational security policy. Table 4-1 shows relationships between security objective and corresponding assumption, threats to counter, and organizational security policy.

Table 4-1 Relationship between TOE security problem and security objective

		Security objectives																
		O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.SWITCH_AUTH	O.HOST_ACCESS	O.AUD_GEN	O.HDD_ENC	O.HDD_SHRED	OE.NOEVIL	OE.PHYSICAL_SEC	OE.MANAGE_SECRET	OE.MANAGEMENT_PC	OE.MAINTENANCE_PC	OE.CONNECT_STORAGE	OE_EXTERNAL_SERVER	OE.FC-SP_HBA	OE.HDD_ENC
TOE security problem	A.NOEVIL									X								
	A.PHYSICAL_SEC										X							
	A.MANAGE_SECRET											X						
	A.MANAGEMENT_PC												X					
	A.MAINTENANCE_PC													X				
	A.CONNECT_STORAGE														X			
	A.EXTERNAL_SERVER															X		
	T.TSF_COMP			X												X		
	T.LP_LEAK					X					X							
	T.CHG_CONFIG	X	X				X											
	T.HDD_THEFT							X										X
	T.HDD_REUSE								X									
	P.MASQ				X												X	

4.3.1 Security objective rational for assumption

Table 4-2 shows that the assumptions are addressed by the security objectives

Table 4-2 Validity of the security objectives for the assumptions

Assumptions	Rationale that assumptions are addressed
A.NOEVIL	A.NOEVIL, as the description of OE. NOEVIL shows, assigns

	a reliable person to the security administrator and audit log administrator respectively for managing or operating the whole disk storage system. This can be realized by assigning a reliable person to the storage resource administrator for managing and operating the storage system in the ranged authorized by the administrator who has the authority.
A.PHYSICAL_SEC	A.PHYSICAL_SEC can be realized by ensuring that disk storage systems, host (including fibre channel connection adapter), devices that constitute a SAN environment (fibre channel switch, cable), other disk storage system and external authentication server are installed in a secure area where only security administrator, storage resource administrator, audit log administrator and maintenance personnel can access, and completely protected from unauthorized change of setting values and switching the connection target as the description of OE.PHYSICAL_SEC shows.
A.MANAGE_SECRET	A.MANAGE_SECRET can be realized by ensuring that the secret for authentication of the fibre channel switch connected with hosts is managed not to be used by a person who is not authorized by the security administrator as the description of OE.MANAGE_SECRET shows.
A.MANAGEMENT_PC	A.MANAGEMENT_PC can be realized by ensuring that the storage administrator correctly installs and manages the management PC to prevent unauthorized use as the description of OE.MANAGEMENT_PC shows.
A.MAINTENANCE_PC	A.MAINTENANCE_PC can be realized by managing the maintenance PC by maintenance personnel, so that people other than maintenance personnel cannot use it as the description of OE.MAINTENANCE_PC shows.
A.CONNECT_STORAGE	A.CONNECT_STORAGE can be realized by limiting that other disk storage system to be connected with the TOE must be the one consists of TOE as the description of OE.CONNECT_STORAGE shows.
A.EXTERNAL_SERVER	A.EXTERNAL_SERVER can be realized by ensuring that the external authentication server is capable of using authentication protocol that can protect the communication with SVP PC (Management maintenance IF PC) supported by the TOE and registering and managing user identification information and user group information correctly while keeping the consistency with the TOE as the description of OE.EXTERNAL_SERVER shows.

4.3.2 Security objective rationale for threat

Table 4-3 shows that the security objectives can help to cope with threats.

Table 4-3 Validity of the security objectives to cope with threats

Threats	Rationale that threats are being addressed
T.TSF_COMP	T.TSF_COMP is addressed by O.SEC_COMM and

Threats	Rationale that threats are being addressed
	OE.EXTERNAL_SERVER as follows. ・ The encrypted communication is employed for the communication between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC), which can reduce the threats, such as sniffing by connecting unauthorized devices. ・ The encrypted communication is employed for the communication between SVP PC (Management maintenance IF PC) and an external authentication server, which can reduce threats such as sniffing by connecting unauthorized devices. ・ One of LDAPS, starttls, and RADIUS (authentication protocol is CHAP) is used for the protocol of communication between SVP PC (Management maintenance IF PC) and an external authentication server to manage the user identity information and group information registered in the external authentication server while keeping consistency with the TOE, which can reduce the threats to leakage of storage administrator and maintenance personnel user ID and password, and of group information.
T.LP_LEAK	T.LP_LEAK is addressed by O.HOST_ACCESS and OE.PHYSICAL_SEC as follows. ・ The TOE identifies and controls host so to ensure that the authorized host only can access the authorized LDEV (logical volume), which can reduce threats. ・ Disk storage system, host (including fibre channel connection adapter), fibre channel switch, other disk storage system and external authentication server are installed in a secure area where only security administrator, storage resource administrator, audit log administrator and maintenance personnel are allowed to access and are completely protected from unauthorized physical access, which can reduce threats.
T.CHG_CONFIG	T.CHG_CONFIG is addressed by O.ADM_AUTH, O.ADM_ROLE, and O.AUD_GEN as follows. ・ The TOE authenticates Storage Navigator (storage management UI software) user before management operation of disk subsystem and reject them if the identity authentication fails, which reduces unauthorized accesses by the third party. ・ The TOE identifies and authenticates storage administrator and maintenance personnel and limits the management operations performed by storage administrator and maintenance personnel to reduce threats. ➢ Security administrator is able to perform user management operations, resource management operations, identification and authentication setting operations of fibre channel switch and host, encryption operations of stored data, and operations of external authentication server.

Threats	Rationale that threats are being addressed
	➢ Audit log administrator is able to perform operations related to audit logs. ➢ Storage resource administrator is able to perform storage management operations in the permitted resource group. ➢ Maintenance personnel can perform maintenance operations of disk storage system. ・ The TOE can trace security related issues when the identity authentication fails, which can reduce unauthorized accesses by the third party.
T.HDD_THEFT	T.HDD_THEFT is addressed by O.HDD_ENC and OE.HDD_ENC as follows. ・ The TOE manages encryption key used to encrypt user data in a disk drive, which can reduce threats such as leakage of user data from the disk drive. ・ The user data is encrypted by using LSI equipped in DKB of disk storage system, which can reduce threats to user data leakage from the disk drive that is taken out of the disk storage system.
T.HDD_REUSE	T.HDD_REUSE is addressed by O.HDD_SHRED as follows. ・ The TOE shreds the user data in disk drive of disk storage system when the use of disk drive stops, which can reduce the threat to the user data leakage from the disk drive.

4.3.3 Security objective rationale for organizational security policy

Table 4-4 shows that the organizational security policy is realized by the security objective.

Table 4-4 Validity of the security objectives for organizational security policy

Organizational security policy	Rationale for the fact that organizational security policy is realized
P.MASQ	P.MASQ is realized by O.SWITCH_AUTH and OE.FC-SP_HBA as follows. ・ For identification and authentication of the fibre channel switch that is connected with a host, the fibre channel connection adapter with the FC-SP function needs to be installed in the host, the fibre channel switch with the FC-SP function needs to be used. ・ The TOE performs identity authentication of the fibre channel switch by the FC-SP function before the port is accessed through the fibre channel switch.

5 Extended components definition

This ST complies with CC Part2 and CC Part3, and does not define any extended components.

6 Security requirement

This section describes security requirements.

6.1 Security functional requirements

Security requirements provided by the TOE are as follows.

All the following components are included in CC Part 2.

Notation system on the operation of functional requirements (selection, assignment and detailed) is described below.

When selecting: [selection: *Description of functional requirements*]: Chosen contents.

When assigning: [assignment: *Description of functional requirements*]: Assigned contents.

When refining: [refinement: *Description of functional requirements*]: Refined contents.

The letters at the end of duplicated defined functional requirements means as follows.

a: The functional requirement related to access restriction, and identification and authentication of storage administrator and maintenance personnel.

b: The functional requirements related to host access control and fibre channel switch identity authentication.

- Security audit (FAU)

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and

c) [assignment: *other specifically defined auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

[selection, choose one of: *minimum, basic, detailed, not specified*]: Not specified.

[assignment: *other specifically defined auditable events*]: Auditable event to be described in “Audit Items” on Table 6-1.

[assignment: *other audit relevant information*]: None

Table 6-1 Individually defined items to be audited

Required functions	Audit Items
FAU_GEN.1	None.

Required functions	Audit Items
FAU_GEN.2	None.
FAU_SAR.1	None.
FAU_STG.1	None.
FAU_STG.3	None.
FAU_STG.4	None.
FCS_CKM.1	・ Record success or failure of the creation of encryption key for data encryption, in the log file.
FCS_CKM.4	・ Record success or failure of the deletion of encryption key for data encryption, in the log file.
FDP_ACC.1	None.
FDP_ACF.1	None.
FDP_RIP.1	・ Record success or failure of start or stop of user data shredding, in the log file.
FIA_AFL.1	None. Reaching threshold of authentication try is not recorded in log file.
FIA_ATD.1a	None.
FIA_ATD.1b	None.
FIA_SOS.1a	None. Unmatched metric is not recorded.
FIA_SOS.1b	None. Unmatched metric is not recorded.
FIA_UAU.2	・ Record the success or failure of identity authentication of storage administrator and maintenance personnel in the log file. ・ Record the result of identity authentication of the fibre channel switch that is connected with hosts by FC-SP in the log file.
FIA_UID.2	・ Record the success or failure of identity authentication of storage administrator and maintenance personnel, in the log file. ・ Record the result of fibre channel switch identity authentication by FC-SP, in the log file.
FIA_USB.1a	None.
FIA_USB.1b	None.
FMT_MOF.1	・ Record the enabled or disabled setting of stored data encryption function, in the log file. ・ Record the setting change of fibre channel switch authentication by FC-SP, in the log file. ・ Record the start or stop of shredding function, in the log file.
FMT_MSA.1	・ Record LU path information creation and deletion, in the log file. ・ Record that user account is added to or deleted from user group, in the log file. ・ Record that role is added to or deleted from user group, in the log file. ・ Record that resource group is added to or deleted from user group, in the log file.
FMT_MSA.3	None.
FMT_MTD.1	・ Record creation or deletion of user ID for user account and change of password, in the log file. ・ Record fibre channel switch WWN, secret creation, change, or deletion, in the log file. ・ Record creation, deletion, backup or restore of encryption key for data encryption, in the log file. ・ Record the change of user authentication method, in the log file.
FMT_MTD.3	・ Record that encryption key for data encryption is restored, in the log file.
FMT_SMF.1	・ Record creation or deletion of user ID for user account, change of password, or change of belonged user group, in the log file. ・ Record creation, change, or deletion of fibre channel switch WWN or secret.
FMT_SMR.1	・ Record change of user group where the user account belongs to, in the log file. ・ Record that role is added to or deleted from user group, in the log file.
FPT_STM.1	None.
FTP_ITC.1	・ Record the success or failure of identity authentication of storage administrator

Required functions	Audit Items
	and maintenance personnel, in the log file.
FTP_TRP.1	・ Record the success or failure of identity authentication of storage administrator and maintenance personnel, in the log file.

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

[assignment: *authorised users*]: Audit log administrator

[assignment: *list of audit information*]: It describes in the Audit Information on Table 6-2.

Table 6-2 Audit Information

Audit event	Audit Information
Identity authentication of storage administrator	・ Success or failure of the identity authentication of storage administrator, executed date and time of the identity authentication, user ID of the Storage Navigator (storage management UI software), IP address of the management PC.
Identity authentication of the maintenance personnel	・ Success or failure of the identity authentication of maintenance personnel, executed data and time, user ID of the maintenance personnel, and IP address of maintenance PC.
Creation, modification and deletion of user account of storage administrator and maintenance personnel	・ User ID of security administrator who creates or deletes a user ID of user account, executed date and time, user ID of the operation target, authentication method, operation (creation, modification, deletion), operation result (success or failure)
Change of user account password of storage administrator and maintenance personnel	・ User ID of the storage administrator and maintenance personnel who change user account password, executed date and time, user ID of operation target and operation result (success or failure).
Change of user group where the user account of storage administrator and maintenance	・ User ID of the security administrator who changes user group, executed date and time, name of user group, name of role, name of resource group, operation (role addition, deletion, RSG # addition, and deletion), and operation results (success or failure).

Audit event	Audit Information
personnel belongs to	
Creation and deletion of LU path information	・ User ID of the storage resource administrator who creates or deletes the LU path information, executed date and time, operation (creation or deletion), port number, host WWN, LU number, LDEV (logical volume) number and operation result (success or failure).
Addition, modification and deletion of fibre channel switch WWN and secret	・ User ID of the storage resource administrator, security administrator, or maintenance personnel who create, modify or delete the fibre channel switch WWN and secret (in this case security administrator only), executed date and time, port number, fibre channel switch WWN, operation (creation, modification, deletion) and operation result (success or failure).
Setting change of existence or nonexistence of fibre channel switch identity authentication by FC-SP	・ User ID of the security administrator who changes existence or nonexistence of fibre channel switch identity authentication by FC-SP, executed date and time, fibre channel switch WWN, existence of authentication, operation (change), and operation result (success or failure).
Fibre channel switch identity authentication by FC-SP	・ WWN of fibre channel switch whose identity is authenticated, executed date and time and authentication result.
Setting for encryption of stored data	・ User ID of the administrator who per forms the setting to enable or disable encryption of stored data, executed date and time, parity group number, encryption setting status (enable/disable), the number of setting parity groups, and operation result (success or failure).
Generation, deletion, backup and restoring of encryption key for encryption of stored data	・ User ID of the security administrator who performs generation, deletion, backup and restoring of encryption key for data encryption, executed date and time, operation (generation, deletion, backup or restoring), encryption key number, the number of operated encryption keys, and operation result (success or failure).
Start or stop of shredding	・ User ID of the storage resource administrator who performs volume shredding, executed date and time, operation (start or stop), written data, the number of writing operations, target LDEV (logical volume) number, the number of target LDEVs (logical volumes), the execution order of shredding, and operation result (success or failure).

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

[Selection: choose one of: *prevent, detect*]: prevent

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*].

[assignment: *pre-defined limit*]: 175,000 lines

[assignment: *actions to be taken in case of possible audit storing failure*]: Give a warning on Storage Navigator (storage management UI software) screen.

FAU_STG.4 Prevention for audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

[selection: choose one of: *"ignore audit event", "prevent audit events, except those taken by authorized user with special rights", "overwrite the oldest stored audit records"*]: *overwrite the oldest stored audit records*

[assignment: actions to be taken when storing audit records fails]: None

- Cryptographic support (FCS)

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

[refinement: cryptographic key]: Encryption key for data encryption

[assignment: *list of standard*]: Shown in "Standard" on Table 6-3.

[assignment: *cryptographic key generation algorithm*]: Shown in "Algorithm on Table 6-3.

[assignment: *cryptographic key sizes*]: Shown in "Key size(bit) on Table 6-3.

Table 6-3 Generation of encryption key

Encryption key	Standard	Algorithm	Key size(bit)
Encryption key for data encryption	FIPS PUB 197	AES	256

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

[refinement: cryptographic key]: Encryption key for data encryption

[assignment: *list of standards*]: None

[assignment: *cryptographic key destruction method*]: shown in "Encryption destruction method on Table 6-4. Encryption key destruction method.

Table 6-4 Encryption key destruction method

Encryption key	Destruction method
Encryption key for data encryption	According to an instruction of security administrator, destroy the specified encryption key information and release the memory where the information is stored.

- User data protection (FDP)

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Subject: Shown in "Subject" on Table 6-5.

Object: Shown in "Object" on Table 6-5.

List of operations between subjects and objects handled by SFP: Shown in "Operations between subjects and objects on Table 6-5.

[assignment: *access control SFP*]: LM access control SFP

Table 6-5 Operations between subjects and objects

Subject	Object	Operation between subject and object
Processing acts for host	LDEV (logical volume)	➢ Access to LDEV (logical volume)
Processing acts for Storage Navigator (storage management UI software)	LDEV (logical volume)	➢ LDEV (logical volume) creation and deletion
	RSG	➢ RSG creation and deletion

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]:

Subjects: Processing acts for host, processing acts for Storage Navigator (storage management UI software)

Objects: LDEV (logical volume), RSG

The SFP-relevant security attribute or groups with name of SFP-relevant security attribute: Shown in "Security attribute of subject" and "Security attribute of object" on Table 6-6.

Table 6-6 SFP-relevant security attribute

Subject	Security attribute of subject	Security attribute of object
Processing acts for host	WWN, LU number	LU path information (host WWN, LU number, LDEV (logical volume) number)
Processing acts for Storage Navigator (storage management UI software)	User group information (role, RSG number)	Resource group information (RSG number) LU path information (host WWN, LU number, LDEV (logical volume) number)

[assignment: *access control SFP*]: LM access control SFP

[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]: Rules described in "Rule" on Table 6-7.

[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]: None

[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]: None

Table 6-7 Rules between subjects and objects

Subjects	Rules	Objects
Processing acts for host	Allow access to objects if the WWN and LU number given from a host to the processing acts for host, and the LU path information that is the security attribute of corresponding objects match each o. Refuse access if the above do not match each other.	LDEV (logical volume)
Processing acts for Storage Navigator (storage management UI software)	Rule to create or delete the objects by the processing acts for Storage Navigator (storage management UI software). 1) In case of security administrator role Creation allows if RSG number is not duplicated, while deletion is allowed if RSG number exists.	RSG
	Rule to create or delete objects by the processing acts for Storage Navigator (storage management UI software). 1) In case of storage administrator role Creation of the LDEV (logical volume) is allowed if a resource group of RSG number allocated to the storage resource administrator contains the LDEV (logical volume) number to be created. Deletion of the LDEV (logical volume) is allowed if a resource group or RSG number allocated to the storage resource administrator contains LDEV (logical volume) number to be deleted and the information of LU path associated with the LDEV (logical volume) does not exist.	LDEV (logical volume)

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].

[assignment: *list of objects*]: LDEV (logical volume)

[selection: *allocation of the resource to, deallocation of the resource from*]: resource allocation release from

- Identification and authentication (FIA)

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of*

authentication events].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

[assignment: *list of authentication events*]*:* Authentication by Storage Navigator (storage management UI software), or that when connecting to SVP PC (Management maintenance IF PC) via remote desktop.

[refinement: *administrator*]: Security administrator

[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]: 3

[selection: *met, surpassed*]: surpassed

[assignment: *list of actions*]: refuse the login of the user for a minute, and then the number of unsuccessful authentication attempts cleared to be 0.

FIA_ATD.1a User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1a The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

[assignment: *list of security attributes*]: Role, RSG number

FIA_ATD.1b User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1b The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

[assignment: *list of security attribute*]: WWN, LU number

FIA_SOS.1a Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1a The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]: at least 6 characters and no more than 256 characters (password for maintenance personnel is 127 characters) containing one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, and any of the following 32 symbols; !”#$%&’()*+,-./:;<=>?@[\]^_`{|}~.

FIA_SOS.1b Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1b The TSF shall provide a mechanism to verify that secrets meet [assignment: *a*

defined quality metric].

[assignment: *a defined quality metric*]: at least 12 characters and no more than 32 characters containing one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, one-byte space and any of the following 12 symbols;.-+@_=:/[],~.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1Timing of authentication

Dependencies: FIA_UID.1Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[refinement: user]: Storage administrator, maintenance personnel, or fibre channel switch

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[refinement: user]: Storage administrator, maintenance personnel, host, or fibre channel switch

FIA_USB.1a User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1a The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

FIA_USB.1.2a The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3a The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

[assignment: *list of user security attributes*]: Role, RSG number

[assignment: *rules for the initial association of attributes*]: None

[assignment: *rules for the changing of attributes*]: None

FIA_USB.1b User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1b The TSF shall associate the following user security attributes with subjects acting

on the behalf of that user: [assignment: *list of user security attributes*].

FIA_USB.1.2b The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3b The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

[assignment: *list of user security attributes*]: WWN, LU number

[assignment: *rules for the initial association of attributes*]: None

[assignment: *rules for the changing of attributes*]: None

- Security management (FMT)

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

[assignment: *list of functions*]: Shown in "Function" on Table 6-8.

[selection: *determine the behaviour of, disable, enable, modify the behaviour of*]: disable, enable

[assignment: *the authorised identified roles*]: Shown in "Role" on Table 6-8.

Table 6-8 List of functions restricting operations for roles

No	Roles	Functions
1	Security administrator	➢ Encryption of stored data function ➢ FC-SP authentication function ➢ External authentication server connection function
2	Storage resource administrator	➢ Shredding function
3	Maintenance personnel	---

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *list of security attributes*]: LU path information, user group information

[selection: *change_default, query, modify, delete,* [assignment: *other operations*]]: Operations described in "Operations for LU path information" on Table 6-9, and in "Operations for user group information" on Table 6-10.

[assignment: *the authorised identified roles*]: Described in "Roles" on Table 6-9.

[assignment: *access control SFP(s), information flow control SFP(s)*]: LM access control SFP

Table 6-9 Operations of storage administrator and maintenance personnel for security attributes of processing act for host

Roles	Operations for LU path information					
	RSG number = n			RSG number ≠ n		
	host WWN	LU number	LDEV (Logical volume) number	host WWN	LU number	LDEV (Logical volume) number
Storage resource administrator (RSG number = n)	Query, creation, deletion	Query, creation, deletion	Query, creation, deletion	-	-	-
Security administrator	-	-	-	-	-	-
Audit log administrator	-	-	-	-	-	-
Maintenance personnel (All resource groups are assigned to maintenance personnel)	Query, creation, deletion	Query, creation, deletion	Query, creation, deletion			

-: No operation

Host WWN of LU path information is used for host identification.

Table 6-10 Operations of storage administrator and maintenance personnel for security attribute (user group information) of processing act for Storage Navigator (storage management UI software)

Roles	Operations for user group information	
	Roles	RSG number

Roles	Operations for user group information	
	Roles	RSG number
Security administrator	➢ Addition ➢ Deletion ➢ Query	➢ Addition ➢ Deletion ➢ Query
Storage resource administrator	➢ (own) Query	➢ (own) Query
Audit log administrator	➢ (own) Query	➢ (own) Query
Maintenance personnel	➢ (own) Query	➢ (own) Query

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[selection, choose one of: *restrictive, permissive, [assignment: other property]*]: restrictive

[assignment: *access control SFP, information flow control SFP*]: LM access control SFP

[assignment: *the authorized identified role*]: None

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

[assignment: *list of TSF data*]:

User ID and password of storage administrator and maintenance personnel

Fibre channel switch WWN, secret

Encryption key for data encryption

User authentication method

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]: Operations for “User account” on Table 6-11, operations for “Fibre channel switch authentication data” on Table 6-12, operations for “Encryption key for data encryption” on Table 6-13, operations for “User authentication method” on Table 6-14.

[assignment: *the authorised identified roles*]: Roles described in “Roles” on Table 6-11, Table 6-12, Table 6-13 and Table 6-14.

Table 6-11 Operations of storage administrator and maintenance personnel for user account

Roles	User account of storage administrator and maintenance personnel	
	User ID	Password
Security administrator	Query, creation, deletion	Modification
Storage resource administrator	(own) Query	(own) Modification
Audit log administrator	(own) Query	(own) Modification
Maintenance personnel	(own) Query	(own) Modification

Table 6-12 Operations of storage administrator and maintenance personnel for fibre channel switch authentication data

Role	fibre channel switch authentication data	
	fibre channel switch WWN	fibre channel switch secret
Security administrator	Query, creation, modification, deletion	Creation, modification, deletion
Storage resource administrator	Query, creation, modification, deletion	-
Audit log administrator	-	-
Maintenance personnel	Query, creation, modification, deletion	-

-: No operation

Table 6-13 Operations of storage administrator and maintenance personnel for encryption key for data encryption

Roles	Encryption key for data encryption

Roles	Encryption key for data encryption
Security administrator	Creation, deletion, query, modification
Storage resource administrator	-
Audit log administrator	-
Maintenance personnel	-

-: No operation

Table 6-14 Operations of storage administrator and maintenance personnel for user authentication method

Roles	User authentication method
Security administrator	Query, modification
Storage resource administrator	-
Audit log administrator	-
Maintenance personnel	-

-: No operation

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for [assignment: *list of TSF data*].

[assignment: *list of TSF data*]: Encryption key for data encryption

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

[assignment: *list of management functions to be provided by the TSF*]: The following functions are provided.

- Function to manage user ID of user account and host identification
- Function to manage password for user ID of user account

- Function to manage fibre channel switch authentication data
- Function to manage role of user account
- Function to manage security attribute of processing acting for fiber channel switch
- Function to manage security attribute of processing acting for Storage Navigator (storage management UI software)
- Function to manage operations by storage administrator and maintenance personnel for user account
- Function to manage operations by storage administrator and maintenance personnel for authentication data of the fibre channel switch that is connected with the host
- Function to manage operations by storage administrator and maintenance personnel for encryption key for data encryption
- Function to stop and activate data encryption function
- Function to stop and activate FC-SP authentication function
- Function to stop and activate shredding function
- Function to stop and activate external authentication server connection function

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *the authorised identified roles*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

[assignment: *the authorised identified roles*]:

- Security administrator
- Storage resource administrator
- Audit log administrator
- Maintenance personnel
- Storage user

- Protection of the TSF (FPT)

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

- Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies..

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

[refinement: *another trusted IT product*]: External authentication server

[selection: *the TSF, another trusted IT product*]: TSF

[assignment: *list of functions for which a trusted channel is required*]: Sending password and user ID of user account used for identification and authentication (external authentication server method) of storage administrator and maintenance personnel.

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*].

FTP_TRP.1.2 The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication, [assignment: other services for which trusted path is required]*].

[selection: *remote, local*]: remote

[selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]: disclosure

[selection: *the TSF, local users, remote users*]: remote user

[selection: *initial user authentication, [assignment: other services for which trusted path is required]*]:

[*assignment: other services the reliable path is required*]: Communication using Storage Navigator (storage management UI software)

6.2 Security assurance requirements

The TOE security assurance requirements are as follows.

The evaluation assurance level of the TOE is EAL2, and the added assurance component is ALC_FLR.1. All security assurance requirements directly use security assurance components stipulated in CC Part3.

(1) Development (ADV)

ADV_ARC.1 : Security architecture description

ADV_FSP.2 : Security-enforcing functional specification

ADV_TDS.1 : Basic design

(2) Guidance document (AGD)

AGD_OPE.1 : Operational user guidance

AGD_PRE.1 : Preparative procedures

(3) Life cycle support (ALC)

ALC_CMC.2 : Use of a CM system

ALC_CMS.2 : Parts of the TOE CM coverage

ALC_DEL.1 : Delivery procedures

ALC_FLR.1 : Basic flaw remediation

(4) Security target evaluation (ASE)

ASE_CCL.1 : Conformance claims

ASE_ECD.1 : Extended components definition

ASE_INT.1 : ST introduction

ASE_OBJ.2 : Security objectives

ASE_REQ.2 : Derived security requirements

ASE_SPD.1 : Security problem definition

ASE_TSS.1 : TOE summary specification

(5) Test (ATE)

ATE_COV.1 : Evidence of coverage

ATE_FUN.1 : Functional testing

ATE_IND.2 : Independent testing - sample

(6) Vulnerability evaluation (AVA)

AVA_VAN.2 : Vulnerability analysis

6.3 Security requirement rationale

6.3.1 Security requirement rationale

Table 6-15 shows correspondence relation between security function requirements and TOE security objectives. Each security function requirement corresponds to at least one TOE security objective.

Table 6-15 Correspondence between security objectives and security function requirements

		TOE security objectives							
		O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.SWITCH_AUTH	O.HOST_ACCESS	O_HDD_ENC	O_HDD_SHRED	O.AUD_GEN
TOE security function requirements	FAU_GEN.1								X
	FAU_GEN.2								X
	FAU_SAR.1								X
	FAU_STG.1								X
	FAU_STG.3								X
	FAU_STG.4								X
	FCS_CKM.1						X		
	FCS_CKM.4						X		
	FDP_ACC.1		X			X			
	FDP_ACF.1		X			X			
	FDP_RIP.1							X	
	FIA_AFL.1	X							
	FIA_ATD.1a	X							
	FIA_ATD.1b					X			
	FIA_SOS.1a	X							
	FIA_SOS.1b				X				
	FIA_UAU.2	X			X				
	FIA_UID.2	X			X	X			
	FIA_USB.1a	X							
	FIA_USB.1b					X			
	FMT_MOF.1		X						

	TOE security objectives							
	O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.SWITCH_AUTH	O.HOST_ACCESS	O_HDD_ENC	O_HDD_SHRED	O.AUD_GEN
FMT_MSA.1		X						
FMT_MSA.3		X						
FMT_MTD.1		X				X		
FMT_MTD.3						X		
FMT_SMF.1		X						
FMT_SMR.1		X						
FPT_STM.1								X
FTP_ITC.1			X					
FTP_TRP.1			X					

Table 6-16 shows that the TOE security objectives are realized by the TOE security function requirements.

Table 6-16 Validity of security function requirements for TOE security objectives

TOE security objectives	Rationale that TOE security objectives are realized
O.ADM_AUTH	O.ADM_AUTH requires performing identification and authentication of Storage Navigator (storage management UI software) user before the Storage Navigator user performs management operation of disk subsystem. The details of necessary measures and required functions for the above request are as follows. a. Maintaining Storage Navigator (storage management UI software) user The TOE must define user accounts, associate users with the user accounts, and maintain them to identify Storage Navigator (storage management UI software) users. In other words, it enables identification of Storage Navigator (storage management UI software) users. The security requirements corresponding to the requirement are FIA_ATD.1a and FIA_USB.1a. b. Identity authentication of Storage Navigator (storage management UI software) user account before using the TOE Before the TOE is used, the TOE must identify user accounts. Therefore, performing identity authentication of user accounts before execution of any of all Storage Navigator (storage management UI software) functions is required. The security function requirements corresponding to the requirement are FIA_UID.2 and FIA_UAU.2.

TOE security objectives	Rationale that TOE security objectives are realized
	c. Managing password The password for the TOE to authenticate user accounts must be at least 6 characters and no more than 256 characters (the password for maintenance personnel is 127 characters) consist of combination of one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, and any of the following 32 symbols; !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~. If authentication fails 3 times in a row due to entering incorrect password, login of the user ID is refused for a minute, which can decrease the possibility of breaking password. The security function requirements corresponding to the function are FIA_AFL.1 and FIA_SOS.1a. O.ADM_AUTH can be satisfied by achieving all of a, b, and C. And that is, meeting FIA_ATD.1a, FIA_USB.1a, FIA_AFL.1, FIA_SOS.1a, FIA_UAU.2, and FIA_UID.2, which are necessary security requirements, can realize O.ADM_AUTH.
O.ADM_ROLE	O.ADM_ROLE requires be able to restrict management operations by storage administrator and maintenance personnel based on roles of identified and authenticated user ID. The details of necessary measurement and required functions for the above request are as follows. a. Restricting operations of role and RSG number The TOE must restrict addition and deletion of role of user account and RSG number, and creation and deletion of RSG according to the role of user account. The TOE therefore restricts the change for user account based on the rule defined as [LM access control SFP]. The security function requirement corresponding to the requirement is FMT_MSA.1. b. Managing identity authentication information The TOE must restrict change of password and user ID of user account, authentication method, fibre channel switch WWN, and secret according to the role of user account. This can prevent unauthorized change of password and user ID of user account, authentication method, fibre channel switch WWN, and secret. The security function requirement corresponding to the requirement is FMT_MTD.1. c. Holding management function The TOE must have a function to manage Storage Navigator (storage management UI software) user account, role of user account, fibre channel switch identification and authentication information, LU path information, and user group information. The TOE must have a function to manage operations by storage administrator and maintenance personnel. Also, it must have a function to stop and activate the data encryption function, the FC-SP authentication function, the shredding function, and the external authentication server connection function. The security function requirement corresponding to the above requirements is FMT_SMF.1. d. Maintaining role The TOE must maintain the roles of security administrator, storage resource administrator, audit log administrator, maintenance personnel and storage user, and associate them with users. The security function requirement corresponding to the above requirement is FMT_SMR.1. e. Managing behavior of security function The TOE must restrict activation and stop of stored data encryption/decryption, fibre channel switch authentication, connection with external authentication server, and

TOE security objectives	Rationale that TOE security objectives are realized
	shredding function according to roles of user account. It can prevent unauthorized change to use or stop each function. The security function requirement corresponding to the above function is FMT_MOF.1. f. Defining and executing access control The TOE must create and delete RSG and LDEV in accordance with the rule defined as [LM access control SFP] for storage administrator and maintenance personnel. It enables the storage resource administrator to create and delete LDEVs (logical volumes) in the allocated RSG. Also, restrictive default value can be assigned as access attribute at LDEV (logical volume) creation. It means that accesses are limited because LU path information does not exist at the LDEV (logical volume) creation. The security function requirements corresponding to the above requirement are FDP_ACC.1, FDP_ACF.1 and FMT_MSA.3. O.ADM_ROLE is satisfied by achieving the above a, b, c, d, e, and f. And that is, achieving FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FMT_MOF.1, FDP_ACC.1, and FDP_ACF.1, which are necessary security function requirements for each measurement, can realize O.ADM_ROLE.
O.SEC_COMM	O.SEC_COMM requires providing a secure communication function by encrypting communication data between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC), and between SVP PC (Management maintenance IF PC) and external authentication server to prevent sniffing. The detail of necessary measurement and required function for the above request are as follows. a. Protecting communication data between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC) Reliable path is used for the communication between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC) to protect the data from sniffing. The security function requirement corresponding to the function is FTP_TRP.1. b. Protecting communication data between SVP PC (Management maintenance IF PC) and external authentication server When an external authentication server is used for identity authentication (the external authentication server method), reliable channel is used for the communication between SVP PC (Management maintenance IF PC) and the external authentication server. It can protect the communication data from sniffing. The security function requirement corresponding to the function is FTP_ITC.1. O.SEC_COMM can be satisfied by achieving all of the above a and b. And that is, achieving FTP_TRP.1 and FTP_ITC.1, which are the necessary security function requirements for each measurement, cam realize O.SEC_COMM.
O.SWITCH_AUTH	After the setting of fibre channel switch identification and authentication, O.SWITCH_AUTH requires identification and authentication of a fibre channel switch when the cable connection of the appropriately set fibre channel switch and TOE is detected. The details of necessary measurement and required function for the above requirement are as follows. a. Executing the FC-SP function The TOE sends the command of security authentication to a fibre channel switch and identifies and authenticates the fibre channel switch by using the DH-CHAP

TOE security objectives	Rationale that TOE security objectives are realized
	authentication code. The security requirements corresponding to the function are FIA_UID.2 and FIA_UAU.2. b. Managing secret A secret for the TOE to authenticate a fibre channel switch is at least 12 characters and no more than 32 characters containing one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, one-byte space and any of the following 12 symbols; .-+@_=:/[],~. It can decrease the possibility of breaking password. The security function requirement corresponding to the function is FIA_SOS.1b. O.SWITCH_AUTH can be satisfied by achieving both of above a and b. And that is, achieving FIA_UID.2, FIA_UAU.2, and FIA_SOS.1b, which are the necessary security function requirements, can realize O.SWITCH_AUTH.
O.HOST_ACCESS	O.HOST_ACCESS requires performing identification of host and access control to allow the host to access only LDEVs (logical volumes) allocated to the host when the host accesses the user data of LU that is the protection target property of the TOE. The detail of necessary measurement and required functions for the above request are as follows. a. Maintaining host The TOE must define host attribute information (WWN, LU number), associate the attribute to the host, and maintain them. The security function requirements corresponding to the requirement are FIA_ATD.1b and FIA_USB.1b. b. Identifying host before using TOE Before the TOE is used, the TOE must identify host. The security function requirement corresponding to the request is FIA_UID2. c. Defining and executing access control For each host, the TOE determines access to LDEV (logical volume) according to the rule defined as [LM access control SFP] and must exactly perform the access control so that the host can access user data in allocated LDEVs (logical volumes). The security function requirements corresponding to the request are FDP_ACC.1 and FDP_ACF.1. O.HOST_ACCESS can be satisfied by achieving all of a, b, and c. And that is, achieving FIA_ATD.1b, FIA_USB.1b, FIA_UID2, FDP_ACC.1, and FDP_ACF.1 which are the necessary security function requirements can realize O.HOST_ACCESS.
O.HDD_ENC	O.HDD_ENC requires managing encryption key for data encryption to prevent user data in a disk drive taken out of disk storage system from being leaked. The detail of necessary measure and required function for the request are as follows. a. Generating and deleting encryption key for data encryption User data stored in a disk drive needs to be encrypted to prevent the user data from being leaked from the disk drive replaced as preventive maintenance. For encryption and decryption, LSI embedded in DKB is used. The TOE generates encryption keys to user for encryption and deletes them after user. The security function requirements corresponding to the above function are FCS_CKM.1, and FCS_CKM.4. b. Restricting operations for encryption key for data encryption The TOE needs to restrict operations for encryption keys according to user account

TOE security objectives	Rationale that TOE security objectives are realized
	roles. In addition, it manages encryption keys so that keys other than those with backup cannot be restored. This prevents unauthorized modification for encryption keys. The security function requirements corresponding to the request are FMT_MTD.1 and FMT_MTD.3. O.HDD_ENC can be satisfied by achieving all of the above a and b. And that is, achieving FCS_CKM.1, FCS_CKM.4, FMT_MTD.1, FMT_MTD.3 which are necessary security function requirements can realize O.HDD_ENC.
O.HDD_SHRED	O.HDD_ SHRED requires shredding old user data in a disk drive before re-using the disk drive of disk storage system to prevent the user data from being leaked. The detail of necessary measurement and required function for the request are as follows. a. Protecting user data in disk drive When a disk drive becomes disuse, the user data stored in the disk drive needs to be shred so as to protect the user data from being leaked from the disk drive. The security function requirement corresponding to the above function is FDP_RIP.1. O.HDD_ SHRED can be satisfied by achieving the measurement. And that is, achieving FDP_RIP.1 that is the necessary function requirement for the measurement can realize O.HDD_ SHRED.
O.AUD_GEN	O.AUD_GEN requires observing unauthorized creation, modification and deletion of security related information. The detail of necessary measurement and required function for the above request are as follows. a. Generating audit log of security function related issues If identity authentication by Storage Navigator (storage management UI software) or falsifications of user account, role, or RSG occurs, SVP PC (Management maintenance IF PC) must generate audit log of the issue for identification from the audit log if such information is incorrectly falsified. The security function requirement corresponding to the request is FAU_GEN.1. Because FAU_GEN.1 obtains audit logs of identity authentication issue, operating issues of setting change, encryption, and user data shredding, the security objective is satisfied. Items without audit item in Table 6-1 of FAU_GEN.1 have no problem if there are no items to be audited since no efficacy is expected from the trace, or they are included in other audit target and can be surely traced. In addition, in the state of no LU path information setting, because a host cannot recognize the corresponding LDEV (logical volume) as a logical device, therefore cannot access the LDEV (logical volume), not to obtain the audit issue related to the security function requirement of access from host to LDEV (logical volume) does not cause any problem. Because time stamps provided by FPT_STM.1 are those for SVP PC (Management maintenance IF PC) OS and cannot be modified by other than maintenance personnel, logs for issue such as time setting change do not need to be obtained. When generating audit log, the date and time the issue occurs and user ID of user who performs the operation need to be put in the audit log so that occurrence date and time and the user who operates can be identified. The security function requirements corresponding to the request are FAU_GEN.2 and FPT_STM.1.

TOE security objectives	Rationale that TOE security objectives are realized
	b. Restricting reference to audit log To refer audit records, the audit record in SVP PC (Management maintenance IF PC) needs to be downloaded from Storage Navigator (storage management UI software). Downloading the audit record is limited to a user account with audit log administrator role to protect the audit logs from unauthorized reference. The security function requirement corresponding to the request is FAU_SAR.1. c. Protecting the audit log from falsification The TOE must prevent deletion and falsification of audit logs by an unauthorized user. Downloading the audit logs is limited to a user account with audit log administrator role. The TOE itself does not have a function to modify the audit logs to protect the audit logs from unauthorized deletion or modification. The security function requirement corresponding to the request is FAU_STG.1. d. Warning risk of loss of audit log Up to 250,000 lines audit logs can be created but when the number of audit logs exceeds the maximum, the oldest audit log is erased. To avoid the loss of audit logs, when the number of audit logs goes over 175,000, a warning to indicate the exceedance is displayed on Storage Navigator (storage management UI software) window to persuade downloading the audit logs. The security function requirements corresponding to the request are FAU_STG.3 and FAU_STG.4. O.AUD_GEN can be satisfied by achieving all the above measurements a, b, c, and d. And that is, achieving FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_STG.1, FAU_STG.3, and FAU_STG.4 which are the security function requirements can realize O.AUD_GEN.

6.3.2 Security requirement internal consistency rationale

Table 6-17 shows dependencies of security requirement components.

Table 6-17 Dependencies of security function requirements

No	TOE/IT environment	Security function requirements	Dependencies defined in CC Part2	Function requirement addressed by this ST
1	TOE	FAU_GEN.1	FPT_STM.1	FPT_STM.1
2	TOE	FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
			FIA_UID.1	FIA_UID.2 *1
3	TOE	FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
4	TOE	FAU_STG.1	FAU_GEN.1	FAU_GEN.1
5	TOE	FAU_STG.3	FAU_STG.1	FAU_STG.1
6	TOE	FAU_STG.4	FAU_STG.1	FAU_STG.1
7	TOE	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	None *3
			FCS_CKM.4	FCS_CKM.4
8	TOE	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
9	TOE	FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
10	TOE	FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
			FMT_MSA.3	FMT_MSA.3
11	TOE	FDP_RIP.1	None	-
12	TOE	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 *2
13	TOE	FIA_ATD.1a	None	-
14	TOE	FIA_ATD.1b	None	-
15	TOE	FIA_SOS.1a	None	-
16	TOE	FIA_SOS.1b	None	-
17	TOE	FIA_UAU.2	FIA_UID.1	FIA_UID.2 *1
18	TOE	FIA_UID.2	None	-
19	TOE	FIA_USB.1a	FIA_ATD.1	FIA_ATD.1a
20	TOE	FIA_USB.1b	FIA_ATD.1	FIA_ATD.1b
21	TOE	FMT_MOF.1	FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
22	TOE	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1
			FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
23	TOE	FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
			FMT_SMR.1	FMT_SMR.1

No	TOE/IT environment	Security function requirements	Dependencies defined in CC Part2	Function requirement addressed by this ST
24	TOE	FMT_MTD.1	FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
25	TOE	FMT_MTD.3	FMT_MTD.1	FMT_MTD.1
26	TOE	FMT_SMF.1	None	-
27	TOE	FMT_SMR.1	FIA_UID.1	FIA_UID.2 *1
28	TOE	FPT_STM.1	None	-
29	TOE	FTP_ITC.1	None	-
30	TOE	FTP_TRP.1	None	-

*1: Dependency is satisfied by FIA_UID.2 which is the upper hierarchy to FIA_UID.1.

*2: Dependency is satisfied by FIA_UAU.2 which is the upper hierarchy to FIA_UAU.1.

*3: Because the TOE is software, and encryption and decryption are fulfilled by hardware, there is no corresponding function requirement.

Table 6-18 shows the rationale that the definition maintains consistency of function requirements in the same category for each TOE security function requirements.

Table 6-18 Consistency between security function requirements

No	Category	Security function requirements	Rationale of consistency
1	Access control	FDP_ACC.1 FDP_ACF.1 FDP_RIP.1	Access control is defined based on these function requirements. Because they require applying the same SFP to the same object and subject, there is no confliction or inconsistency, but the whole contents are consistent.
2	Management	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_MTD.3 FMT_SMF.1 FMT_SMR.1	Security management is defined based on these function requirements. There is no confliction or inconsistency for target security attribute or action and the whole contents are consistent.
3	Identification and authentication	FIA_AFL.1 FIA_ATD.1a FIA_ATD.1b FIA_SOS.1a FIA_SOS.1b FIA_UAU.2 FIA_UID.2 FIA_USB.1a	These function requirements realize the identification and authentication. As TSF, (1) Storage Navigator (storage management UI software) user ID and password, (2) fibre channel switch WWN and secret, and (3) host WWN are separately defined, and there is no confliction or inconsistency. The whole contents are consistent.

No	Category	Security function requirements	Rationale of consistency
		FIA_USB.1b	
4	Audit	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_STG.1 FAU_STG.3 FAU_STG.4	Audit log is defined based on the function requirements, and there is no confliction or inconsistency. The whole contents are consistent.
5	Encryption key management and operation	FCS_CKM.1 FCS_CKM.4	These function requirements define operations of encryption key used to encrypt stored data, and there is no confliction or inconsistency. The whole contents are consistent.
6	Reliable path/channel	FTP_ITC.1 FTP_TRP.1	There function requirements define communication paths and channels between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC), and between SVP PC (Management maintenance IF PC) and external authentication server, and there is no confliction or inconsistency. The whole contents are consistent.
7	Complementary	FPT_STM.1	This function requirement is to complement other function requirements. From the fact that FPT_STM.1 is requirement for time stamp of audit log, it is obvious that there is no confliction or inconsistency between function requirements in this category and the whole contents are consistent.
8	Between categories	#1 - #2	Because requirements for access control defines the control for user data in LU which is protection target property, and the requirement for management is to define the management TSF data, there is no confliction or inconsistency between them.
		#1- #3 #2- #3	There is no confliction or inconsistency between identification requirement and access control or management requirement.
		#1 - #4 #2 - #4 #3 - #4	They are to record audit for requirements of access control, management, identification and authentication, and there is no confliction or inconsistency.
		#1 - #5 #2 - #5 #3 - #5 #4 - #5	There is no confliction or inconsistency between requirements for access control, management, identification and authentication, and audit log.

No	Category	Security function requirements	Rationale of consistency
		#1 - #6 #2 - #6 #3 - #6 #4 - #6 #5 - #6	There is no confliction or inconsistency between requirements for access control, management, identification and authentication, audit log, and encryption key management and operation.
		#1 - #7 #2 - #7 #3 - #7 #4 - #7 #5 - #7 #6 - #7	FPT_STM.1is to provide FAU_GEN.1 with time information and there is no confliction or inconsistency with other requirements.

As stated below, mutual support is established by security function requirements which do not have interdependence.

- For FIA_UID.2 and FIA_UAU.2, FMT_MOF.1 limits operations to start or stop the security function according to roles, and operations can be allowed only from Storage Navigator (storage management UI software). The security function cannot be started or stopped by any other method to prevent deactivation.

As aforementioned, IT security requirements described in the ST establish the whole with internal consistency by mutual support in integrated manner.

6.3.3 Security requirement rationale

Disk storage system including the TOE is installed in a secure area and does not expect other than attack path using LAN. As shown in Section3.2, attacks from communication path between Storage Navigator (storage management UI software) or management PC and disk storage system, and between the disk storage system and external authentication server. The attacks do not require special knowledge, skill and tool.

Beside, as installation of unauthorized software on the management PC where Storage Navigator (storage management UI software) works is prohibited, potential threat based on the detailed interface to the disk storage system is excluded from supposition. Evaluating [certain vulnerability] can achieve the balance against the expected threat.

Even though the TOE has a function to encrypt user data stored in a disk drive using LSI embedded in DKB, implementation of encryption key is done by a reliable security administrator at the installation. For this, there is no security characteristic such that not to handle as confidential leads to vulnerability of TOE.

The TOE is software which can ensure to be able to counter expected threats by implementation of security functions based on design documents and evaluation by testing, accordingly classifying it in EAL2 of evaluation assurance level is reasonable. Note that by the distribution procedure of TOE, security is maintained in TOE distribution for consumers shown as TOE consumers in TOE reference.

In addition, it is important to address security vulnerability issues these days. This product takes charge of important part that manages disk storage system and is required to track security defects and take actions for vulnerability immediately. It is important to provide assurance for security defects to secure reassurance for users, and thus ALC_FLR.1 component is applied.

7 TOE summary specification

This chapter describes summary specification of security functions provided by the TOE.

7.1 TOE Security function

Table 7-1 shows correspondence relation between TOE security functions and security function requirements (SFR). As shown here, security functions explained in this section meet all SFRs described in section 6.1.

Table 7-1 Correspondence relation between TOE security functions and security function requirements

		TOE IT security function					
		SF.LM	**SF.FCSP**	**SF.SN**	**SF.ROLE**	**SF.HDD**	**SF.AUDIT**
TOE security function requirements	FAU_GEN.1						X
	FAU_GEN.2						X
	FAU_SAR.1						X
	FAU_STG.1						X
	FAU_STG.3						X
	FAU_STG.4						X
	FCS_CKM.1					X	
	FCS_CKM.4					X	
	FDP_ACC.1	X					
	FDP_ACF.1	X					
	FDP_RIP.1					X	
	FIA_AFL.1			X			
	FIA_ATD.1a	X					
	FIA_ATD.1b	X					
	FIA_SOS.1a			X			
	FIA_SOS.1b		X				
	FIA_UAU.2		X	X			
	FIA_UID.2	X	X	X			
	FIA_USB.1a	X					
	FIA_USB.1b	X					

	TOE IT security function					
	SF.LM	**SF.FCSP**	**SF.SN**	**SF.ROLE**	**SF.HDD**	**SF.AUDIT**
FMT_MOF.1				X		
FMT_MSA.1				X		
FMT_MSA.3	X					
FMT_MTD.1				X	X	
FMT_MTD.3					X	
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_STM.1						X
FTP_ITC.1			X			
FTP_TRP.1			X			

The following states each TOE security functions and the specific method to realize SFR corresponding to the security functions.

7.1.1 SF.LM

The TOE is connected with a host via SAN environment. SAN is the dedicated network for disk storage system that connects hosts and disk storage systems via the fibre channel. The TOE performs access control by SF.LM while the host accesses LDEVs (logical volumes) in the disk storage system.

[Satisfied Requirements] FIA_ATD.1a, IA_USB.1a, FIA_ATD.1b, FIA_USB.1b, FIA_UID.2, FDP_ACC.1, FDP_ACF.1, and FMT_MSA.3

The TOE maintains user group information (such as role and RSG number) and associates them with processing acting for Storage Navigator (storage management UI software) (FIA_ATD.1a and FIA_USB.1a).

The TOE maintains the attribute information of host (such as WWN and LU number) and associates them with processing acting for the host (FIA_ATD.1b and FIA_USB.1b).

The TOE identifies the host before an operation of security function related to access from host using host WWN of LU path information. this operates after identity authentication of fibre channel switch when fibre channel switch identity authentication is required. (FIA_UID.2).

The TOE performs [LM access control SFP] when the processing acting for a host accesses an LDEV (logical volume) or the processing acting for Storage Navigator (storage management UI software) creates or delete the LDEV (logical volume).

[LM access control SFP] consists of the following rules (FDP_ACC.1, FDP_ACF.1, and FMT_MSA.3)

- When WWN and LU number passed over to the processing acting for the host are consistent with LU path that is the security attribute of the corresponding object, the access to the LDEV (logical volume)

is allowed while it is rejected if the LU path information is not consistent.

- When the processing acting for Storage Navigator (storage management UI software) creates or deletes RSG, only the security administrator can create or delete the RSG according to [User group information of Storage Navigator (storage management UI software)] (such as role and RSG) passed over to the processing acting for Storage Navigator (storage management UI software).
- When the processing acting for Storage Navigator (storage management UI software) creates or deletes LDEV (logical volume), according to [User group information of Storage navigator (storage management UI software)] (such as role and RSG) passed over to the processing acting for Storage Navigator (storage management UI software), the storage administrator can create or delete LDEV (logical volume) in a resource group only when RSG number assigned to the user group where the storage resource administrator belongs matches with the RSG number of the LDEV (logical volume).
- Condition when deleting LDEV (logical volume): Delete an LDEV (logical volume) when there is no LU path associated with the LDEV (logical volume).
- When storage resource administrator creates LDEV (logical volume), a restrictive default value is given as the access attribute. It means that the access from the host is restricted because there is no LU path information at the LDEV (logical volume) creation. (FMT_MSA.3)

7.1.2 SF.FCSP

The TOE executes identity authentication of fibre channel switch if the organization’s security policy requires. DH-CHAP with NULL DH Group authentication is used for this authentication.

[Satisfied requirements] FIA_SOS.1b,FIA_UID.2, FIA_UAU.2

If fibre channel switch authentication is required, the TOE performs identity authentication when the cable connection of the fibre channel switch and TOE is detected. The TOE checks whether the fibre channel switch requires the authentication or not. When it requires the authentication, the TOE identifies and authenticates the fibre channel switch by using DH-CHAP with fibre channel switch port's WWN and secret (FIA_UID.2, FIA_UAU.2). The connection between the fibre channel switch and the disk storage system is allowed when a secret received from the host matches a secret that the TOE has (FIA_UAU.2).

The TOE restrict the entry of secret used for fibre channel switch identity authentication by FC-SP to be at least 12 characters and no more than 32 characters consists of one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, one-byte space and any of the following 12 symbols; .-+@_=:/[],~. (FIA_SOS.1b)

7.1.3 SF.SN

[Satisfied requirements] FIA_AFL.1, FIA_SOS.1a, FIA_UID.2, FIA_UAU.2, FTP_TRP.1, and FTP_ITC.1

The TOE executes identity authentication at remote desktop connection to Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC) using user ID and password before any operations of other security functions. If the identity authentication fails 3 times in a row, the identity authentication of the user is refused for one minute. (FIA_UID.2, FIA_UAU.2, and FIA_AFL.1)

The TOE restricts the entry for password used for storage administrator or maintenance personnel authentication to be at least 6 characters and no more than 256 characters (127 characters for maintenance personnel password) consists of one-byte upper-case alphabet, one-byte lower-case alphabet, one-byte number, any of the following 32 symbols; !”#$%&’()*+,-./:;<=>?@[\]^_`{|}~. (FIA_SOS.1a)

The TOE employs SVP PC (Management maintenance IF PC) internal authentication method for identity authentication of storage administrator and maintenance personnel. If the entered user ID does not exist in the TOE, external authentication server method is used.

When identity authentication of storage administrator and maintenance personnel is executed by the external authentication server method, TOE starts communication between SVP PC (Management

maintenance IF PC) and external authentication server using one of LDAPS, starttls, and RADIUS (authentication protocol is CHAP) and sends user ID and password of user account to be used for identification and authentication of storage administrator and maintenance personnel. Using LDAPS, starttls, and RADIUS (authentication protocol is CHAP) for the communication between the SVP PC (Management maintenance IF PC) and the external authentication server can prevent TSF data from being sniffed. (FTP_ITC.1)

The TOE allows starting communication when storage administrator activates Storage Navigator (storage management UI software) on management PC. For the communication between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC), SSL is used to prevent the TSF data from being sniffed. (FTP_TRP.1)

The SSL used for the communication between Storage Navigator (storage management UI software) and SVP PC (Management maintenance IF PC) supports [TLSv1.0]. Table 7-2 shows Encryption-relevant algorithm used by SSL.

Table 7-2 Encryption-relevant algorithm used by SSL

Standard	Algorithm	Key size (bit)	Encryption operation	How to use
ANSI X9.30 Part1-1997	DSA	1024	Authentication	To be used as certificate to prove SVP PC (Management maintenance IF PC) against management PC (server authentication)
RSA Security Inc. Public-Key Cryptography Standards(PKCS)#1 v2.1	RSA	512 or more	Authentication	
			Key exchange	To be used at session key exchange.
FIPS PUB 197	AES	256 128	Communication data encryption and decryption	To select algorithm used for session key by hand-shake protocol in version of [TLSv1.0]
FIPS PUB 46-3	3DES	168		
FIPS PUB 180-2	SHA-256	256	Hash	To be used at hash value calculation
IEEE P1363 G.7	SHA1PRNG	64	Random digit	To be used as key information at session key creation

7.1.4 SF.ROLE

[Satisfied requirements] FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, and FMT_MOF.1

The TOE executes [LM access control SFP] for the access from the processing acting for Storage Navigator (storage management UI software) to SVP PC (Management maintenance IF PC).

[LM access control SFP] consists of the following rules.

- [LM access control SFP] restricts operations to create, delete and refer LU path information (host WWN, LU number, LDEV (logical volume) number) based on roles and RSG numbers. (FMT_MSA.1). Table 6-9 shows operations each role can perform for the LU path information.
- [LM access control SFP] restrict operations to add, delete and refer user group information (role and RSG number) based on roles (FMT_MSA.1). Table 6-10 shows operations each role can perform for the user group information.

The TOE manages the following TSF data. (FMT_MTD.1)

- The account management function of Storage Navigator (storage management UI software) manages

user ID, password, role and RSG number of storage administrator and maintenance personnel. Table 6-10 and Table 6-11 show management operations each role can perform.

- The FC-SP function of Storage Navigator (storage management UI software) manages WWN and secret which are authentication data of fibre channel switch. Table 6-12 shows management operations each role can perform.
- The stored data encryption function of Storage Navigator (storage management UI software) manages encryption key used for user data encryption. Table 6-13 shows management operations each role can perform.
- The access control function of Storage Navigator (storage management UI software) manages user authentication method. Table 6-14 shows management operations each role can perform.

The TOE has the following management functions (FMT_SMF.1).

- The function to manage user account of Storage Navigator (storage management UI software), role of user account, fibre channel switch authentication information, WWN authentication information, LU path information, and user group information.
- The function to manage operations by storage administrator and maintenance personnel.
- The function to manage functions for stored data encryption, FC-SP authentication function, shredding function, management function for starting or stopping connection to external authentication server.

The TOE restricts an operation to set whether the fibre channel switch that is connected with the host is authenticated by FC-SP based on roles. Table 6-8 shows operations each role can perform (FMT_MOF.1).

The TOE restricts setting operation to use or not to use the stored data encryption function based on roles. Table 6-8 shows operations each role can perform (FMT_MOF.1).

The TOE restricts setting operation to user or not to use connecting function of external authentication server (including connection setting parameter) based on roles. Table 6-8 shows operations each role can perform (FMT_MOF.1).

The TOE restricts operations to start and stop shredding function based on roles. Table 6-8 shows operations each role can perform (FMT_MOF.1).

The TOE maintains and associate roles (security administrator, storage resource administrator, audit log administrator, maintenance personnel, and storage user). (FMT_SMR.1)

7.1.5 SF.HDD

[Satisfied requirements] FCS_CKM.1, FCS_CKM.4, FMT_MTD.1, FMT_MTD.3, and FDP_RIP.1

The TOE encrypts user data when storing it in a disk drive. For encryption and decryption, LSI embedded in DKB is used. The TOE creates encryption key for data encryption. Table 6-3 shows the algorithm for encryption key generation and Table 6-4 shows method to remove encryption key (FCS_CKM.1, FCS_CKM.4).

The TOE limits administrators who can perform operations for encryption key used for data encryption. Only security administrator can create, delete, backup (inquiry) and restore (inquiry and modification) the encryption keys (FMT_MTD.1).

The TOE can make backup of encryption key for data encryption in management PC. It also can restore the backup encryption key from the management PC to disk storage system. At the restoring, a hash value set in the backup data at the backup is verifies with a hash value of data to be restored. Only when the hash values are consistent, the encryption key can be restored. As the hash value contains serial number of the disk storage system, the encryption key can be restored only in the backed up disk storage system. (FMT_MTD.3)

The TOE shreds user data in LDEV (logical volume) which becomes disuse. (FDP_RIP.1)

7.1.6 SF.AUDIT

[Satisfied requirements] FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FAU_SAR.1, FAU_STG.1, FAU_STG.3 and FAU_STG.4

The TOE has the following audit functions.

- When an audit issue related to the security function in the TOE occurs, an audit log is generated. The user ID of user account that causes each audit issue is added to the audit log. In addition, for the date used when the audit log is generated, the time managed by OS on SVP PC (Management maintenance IF PC) is used. Table 6-2 describes the audit information.
- There is no role which can modify and delete audit logs.
- Up to 250,000 lines audit logs can be created. When the number of audit logs exceeds the maximum, the oldest audit log is erased by returning to the line where the storing starts (wraparound method). When the number of audit logs goes over 175,000, a warning to indicate the exceedance is displayed on Storage Navigator (storage management UI software) window to persuade audit administrator to download the audit logs. If the audit logs are downloaded, the number of lines is reset and audit log starts at the first line.
- Only audit log administrator can download audit logs.
- Starting and ending audit function works in conjunction with TOE activation and termination.

The audit logs the TOE obtains consists of basic information and detailed information. Table 7-3 and Table 7-4 show contents of output basic information and detailed information respectively.

Table 7-3 Output content of basic information

<table>
<tr><th>No</th><th>Item</th><th colspan="2">Description</th></tr>
<tr><td>1</td><td>Date</td><td colspan="2">Date when issue occurs</td></tr>
<tr><td>2</td><td>Time</td><td colspan="2">Time when issue occurs</td></tr>
<tr><td>3</td><td>Time zone</td><td colspan="2">Time difference with GMT (Greenwich Mean Time)</td></tr>
<tr><td>4</td><td>User ID</td><td colspan="2">Storage Navigator (storage management UI software) user ID</td></tr>
<tr><td rowspan="7">5</td><td rowspan="7">Function name</td><td colspan="2">Character string indicates function which executes setting operation</td></tr>
<tr><td>Function names</td></tr>
<tr><td>Name of function for identity authentication of storage administrator and maintenance personnel</td></tr>
<tr><td>Name of function to create, change and delete user account, to change password, and to change user group.</td></tr>
<tr><td>Name of function to create and delete LU path information, to create, change and delete WWN and secret of fibre channel switch, and to change setting for fibre channel switch authentication by FC-SP.</td></tr>
<tr><td>Name of function for fibre channel switch authentication by FC-SP.</td></tr>
<tr><td>Name of function to enable and disable data encryption, to create, delete, backup and restore encryption keys.</td></tr>
<tr><td>Name of function for shredding</td></tr>
<tr><td>6</td><td>Operation name or issue</td><td colspan="2">Abbreviation of operation name of each function</td></tr>
</table>

<table>
<tr><th>No</th><th>Item</th><th colspan="2">Description</th></tr>
<tr><td></td><td>name</td><td></td><td>Operation names</td></tr>
<tr><td></td><td></td><td></td><td>Identity authentication of storage administrator and maintenance personnel</td></tr>
<tr><td></td><td></td><td></td><td>User account creation</td></tr>
<tr><td></td><td></td><td></td><td>User account change</td></tr>
<tr><td></td><td></td><td></td><td>User account deletion</td></tr>
<tr><td></td><td></td><td></td><td>User account password change</td></tr>
<tr><td></td><td></td><td></td><td>Role addition to user group</td></tr>
<tr><td></td><td></td><td></td><td>Role deletion from user group</td></tr>
<tr><td></td><td></td><td></td><td>RSG number addition to user group</td></tr>
<tr><td></td><td></td><td></td><td>RSG number deletion from user group</td></tr>
<tr><td></td><td></td><td></td><td>Lu path information creation</td></tr>
<tr><td></td><td></td><td></td><td>LU path information deletion</td></tr>
<tr><td></td><td></td><td></td><td>Fibre channel switch WWN and secret creation</td></tr>
<tr><td></td><td></td><td></td><td>Fibre channel switch WWN and secrete change</td></tr>
<tr><td></td><td></td><td></td><td>Fibre channel switch WWN and secret deletion</td></tr>
<tr><td></td><td></td><td></td><td>Setting change for host authentication by FC-SP</td></tr>
<tr><td></td><td></td><td></td><td>Fibre channel switch authentication by FC-SP</td></tr>
<tr><td></td><td></td><td></td><td>Setting to enable/disable data encryption</td></tr>
<tr><td></td><td></td><td></td><td>Generation of encryption key for data encryption</td></tr>
<tr><td></td><td></td><td></td><td>Deletion of encryption key for data encryption</td></tr>
<tr><td></td><td></td><td></td><td>Backup of encryption key for data encryption</td></tr>
<tr><td></td><td></td><td></td><td>Restoring encryption key for data encryption</td></tr>
<tr><td></td><td></td><td></td><td>Starting shredding</td></tr>
<tr><td></td><td></td><td></td><td>Stopping shredding</td></tr>
<tr><td>7</td><td>Parameter</td><td colspan="2">Parameter for executed setting operation</td></tr>
<tr><td>8</td><td>Operation result</td><td colspan="2">Operation result</td></tr>
<tr><td>9</td><td>Identity information of source host</td><td colspan="2">IP address of management PC or maintenance PC
In case of fibre channel switch authentication by FC-SP, fibre channel switch WWN is output.</td></tr>
<tr><td>10</td><td>Serial number of log information</td><td colspan="2">Serial number of log information stored</td></tr>
</table>

Table 7-4 Output content of detailed information

No	Audit issue	Detailed information
1	Identity authentication of storage administrator	· None
2	Identity authentication of maintenance personnel	· None
3	Creation, modification, deletion of user account of storage administrator and maintenance personnel	· User ID of operation target, enable/disable setting information, authentication method, user group name, operation result (success or failure)
4	Password change of user account of storage administrator and maintenance personnel	· User ID of operation target, operation result (success or failure)
5	Change of user group where storage administrator and maintenance personnel belong to	· User ID of operation target, user group name, role, RSG number, operation result (success or failure)
6	Creation and deletion of LU path information	· Port number, host WWN, LU number, LDEV (logical volume) number
7	Creation, modification, deletion of fibre channel switch WWN and secret	· Port number, fibre channel switch WWN, the number of ports
8	Setting change of fibre channel switch authentication by FC-SP	· Port number, port WWN, whether to execute authentication, operation (change), the number of ports
9	Fibre channel switch authentication by FC-SP	· None
10	Setting to enable/disable data encryption	· Parity group number, setting to enable/disable encryption, operated encryption key number, the number of setting parity group
11	Generation, deletion, backup, and restoring of encryption key for data encryption	· Encryption key number, the number of operated encryption keys
12	Start or stop shredding	· Written data , the number of writing, target LDEV (logical volume) number, the number of target LDEVs (logical volumes), execution order or shredding processing

8 Reference

- Common Criteria for Information Technology Security Evaluation
  Part1: Introduction and general model Version 3.1 Revision 4
  CCMB-2012-09-001

- Common Criteria for Information Technology Security Evaluation
  Part2: Security functional components Version 3.1 Revision 4
  CCMB-2012-09-002

- Common Criteria for Information Technology Security Evaluation
  Part3: Security assurance components Version 3.1 Revision 4
  CCMB-2012-09-003

- Common Methodology for Information Technology Security Evaluation
  Evaluation methodology Version 3.1 Revision 4
  CCMB-2012-09-004

- Common Criteria for Information Technology Security Evaluation
  Part 1: Introduction and general model, September 2012, Version 3.1, Revision 4 Final
  CCMB-2012-09-001, September 2012, Japanese translated version 1.0, November 2012,
  Information-Technology Promotion Agency, Japan

- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements, September 2012, Version3.1, Revision 4 Final
  CCMB-2012-09-002, Japanese translated version 1.0, November 2012 Final
  Information-Technology Promotion Agency, Japan
  Information-Technology Promotion Agency, Japan

- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements, September 2012, Version 3.1, Revision 3 Final
  CCMB-2012-09-003 Japanese translated version 1.0 Final November 2012,
  Information-Technology Promotion Agency, Japan

- Common Methodology for Information Technology Security Evaluation
  Evaluation methodology September 2012, Version3.1 Revision 4, Final
  CCMB-2012-09-004
  Japanese translated version 1.0 Final November 2012
  Information-Technology Promotion Agency, Japan

8.1.1 Terms and definitions

For CC terms used commonly, see CC Par1 Section 4.

8.1.1.1 Glossary for ST

Terms	Definition
Disk subsystem	Disk storage system, Hitachi Unified Storage VM
Redundant Array of Independent Disks (RAID)	A technology which can recover damaged data by spreading or duplicating to multiple disk drives, improve the performance, and keep redundancy of data. There are RAID0 (data striping), RAID 1 (disk mirroring) and RAID5 (data striping with distributed parity added) as commonly used raid types.
Storage Navigator	The program which provides GUI for disk storage system setting. It consists of Flex application and Java applet, works on SVP PC (Management maintenance IF PC) and management PC. It is used by storage administrator and maintenance personnel.
Parity group	A group of disk drives to realize RAID system (see above). A parity group consists of multiple disk drives where user data and parity information are stored. The user data can be accessed even if one or more drive in the group becomes unavailable.
SAN	Abbreviation for Storage Area Network. It is a network dedicated to storage that connects a disk storage system and a host computer by using a fibre channel. High-speed/Highly-reliable data communications are available by fibre channels.
Fibre channel	High speed network technology to build Storage Area Network (SAN).
Fibre channel switch	A switch to connect each device of fibre channel interface. Using the fibre channel switch enables to build SAN (Storage Area Network) by connecting multiple hosts and disk storage systems in high speed.
LDEV (Logical volume)	Abbreviation of logical device and a unit of volume created in a user area in disk storage system. It is also called as logical volume.
LDEV (Logical volume) number	Unique number assigned to logical device at creation.
Logical unit (LU)	The LDEV (logical device) used from a host of Open system is called LU. On the Open system fibre channel interface, access to LU mapped with one or more LDEV (logical device) is enabled.
LU path	Data input/output channel connecting Open system host and LU.
LU number (LUN)	LDEV (logical device) which is associated with fibre channel port and accessible from host. Or it is an address allocated to volume for Open system.
Port	The end of fibre channel. Each port is identified by port number.
Fibre Channel Security Protocol (FC-SP)	A protocol to execute authentication each other at communication between host and fibre channel switch and fibre channel switch and disk storage system. DH-CHAP with NULL DH Group authentication is used.

Terms	Definition
Connection setting parameter for external authentication server	A parameter to be set in SVP PC (Management maintenance IF PC) for identification and authentication by using external authentication server. It contains the following information. Type of external authentication server (LDAP, RADIUS), address of external authentication server, certificate of external authentication server, protocol (LDAPS, starttls, CHAP), and port number and so on.
starttls	A protocol to encrypt TCP session connecting with LDAP.
RADIUS	A protocol to realize authentication and accounting.
CHAP	A protocol to encrypt password to be sent from client to server at authentication.
DH-CHAP	A protocol used for FC-SP. It uses CHAP protocol for key exchange.
HT-40SA	Model name of Hitachi Unified Storage VM for Japan.
DW700	Model name of Hitachi Unified Storage VM for overseas.

8.1.1.2 Abbreviation

In this document, the following abbreviations are used.

CACHE	CACHE memory
CC	Common Criteria
CHB	Channel Blade
CHAP	Challenge Handshake Authentication Protocol
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DKB	Disk Blade
DKC	Disk Controller
EAL	Evaluation Assurance Level
FC-SP	Fibre Channel Security Protocol
HDD	Hard disk drive
JRE	Java Runtime Environment
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over TLS
LDEV	Logical Device
LSI	Large Scale Integration
LU	Logical unit

LUN	Logical Unit Number
PC	Personal Computer
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SF	Security Function
SFP	Security Function Policy
SSL	Secure Sockets Layer
ST	Security Target
SVP	Service Processor
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
HUS VM	Hitachi Unified Storage VM
WWN	World Wide Name