Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2014-04-08 (ITC-4504)
Certification No.	C0514
Sponsor	Hitachi, Ltd.
TOE Name	Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform VX7 Control Program
TOE Version	80-01-25-00/00 (R8-01A-06_Z)
PP Conformance	None
Assurance Package	EAL2 augmented with ALC_FLR.1
Developer	Hitachi, Ltd.
Evaluation Facility	Mizuho Information& Research Institute, Inc. Information Security Evaluation Office

This is to report that the evaluation result for the above TOE is certified as follows.
2016-06-06

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center, Technology Headquarters

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

Evaluation Result: Pass
"Hitachi Virtual Storage Platform G1000, Hitachi Unified Storage VM7 Control Program" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "Hitachi Virtual Storage Platform G1000, Hitachi Unified Storage VM7 Control Program, Version 80-01-25-00/00 (R8-01A-06_Z)" (hereinafter referred to as the "TOE") developed by Hitachi, Ltd., and the evaluation of the TOE was finished on 2016-04 by Mizuho Information& Research Institute, Inc., Information Security Evaluation Office (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Hitachi, Ltd., and provide security information to procurement entities and consumers who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") that is provided along with this report. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes "procurement entities who purchase this TOE that is commercially available, general consumers, and Hitachi Data Systems Corporation" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL2 augmented with ALC_FLR.1.

1.1.2 TOE and Security Functionality

This TOE is a program dedicated to run Hitachi Virtual Storage Platform G1000 (also known as Hitachi Virtual Storage Platform VX7) (hereinafter referred to as the "storage system").

The TOE receives a request for access to a memory device in the storage system from a host computer (hereinafter referred to as the "host") and controls data exchange between the host and the memory device. The TOE provides the functions that identify hosts, control access, and protect the related settings, so that the host can access only the designated storage area for the host.

The TOE provides the function that erases data by overwriting dummy data to the memory device and the function that supports encryption of data to be written to the memory device, in order to prevent data leakage from the memory device (The encryption function is provided by the hardware of the storage system).

The TOE provides the function that identifies and authenticates a fibre channel switch to meet the requirements of the procurement entities.

Regarding these security functions, the validity of the design policy and the accuracy of the implementation were evaluated within the assurance package. Assumed threats and

assumptions are as described in the following section.

1.1.2.1 Threats and Security Objectives

This TOE counters each threat by using the security functions as follows.

The TOE identifies the host and controls access to prevent the storage area in the storage system that is assigned to the host from being accessed and falsified by other host. This allows only the host that is assigned the storage area to access the area.

To prevent the settings of the TOE security functions from being changed by attackers who connect the TOE management interface, and to prevent user data of the storage users stored in the memory device of the storage system from being illegally accessed and falsified, the TOE performs identification and authentication of TOE users (security administrator, storage resource administrator, and audit log administrator), controls user access, performs TLS communications between the Storage Navigator program and the SVP program, and manage security functions. Thus, it prevents the settings of the TOE security functions from being illegally changed.

In addition, to prevent the remaining data in the memory device of the storage system from being leaked, it performs the encryption key management function that supports encryption of user data to be stored in the memory device and the shredding function that erases the remaining data by overwriting the used area of the memory device with dummy data. The TOE records the events related to security functions to logs in order to prevent and reduce unauthorized operations.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

- The storage system that contains the TOE and the host are connected through a fibre channel switch.

- The storage system that contains the TOE, the host (including the fibre channel connection adapter), the devices that constitute a SAN environment (fibre channel switch, cable), other storage systems (when storage systems are connected), and the external authentication server should be installed in a secure area where only the authorized persons can enter and exit. The security administrator should properly perform operations and manage users, so that the connection status of a SAN environment and the settings of host identification can be maintained.

- The management PC should be installed in an environment where unauthorized use is prevented.

- For communications between the TOE and external authentication servers, one of the following protocols should be used; LDAPS, LDAP+starttls, or RADIUS (CHAP authentication).

- Security administrators, audit log administrators, and maintenance personnel must not engage in unauthorized actions.

1.1.3 Disclaimers

- TOE behavior in an environment other than the specific operational environment is not assured in this evaluation. For details of the operational environment, see "4.2 Environmental Assumptions." In the following cases, it is noted that TOE behavior is not assured in the evaluation.

  > The SAN environment has multiple fibre channel switches.

  > The SAN environment has multiple hosts.

  > The port in the storage system is connected with another disk storage system.

- Kerberos (v5) can also be used as a protocol between the TOE and the external authentication server. In this case, the security of authentication is not assured.

- The storage system has a function that encrypts and stores user data in the memory device, but the encryption function is not assured in this evaluation. Encryption is performed by the LSI that is installed in the storage system, and the LSI is out of the TOE scope.

- When the TOE is distributed overseas, the security of the TOE is assured in this evaluation until it is delivered to Hitachi Data Systems Corporation, which is a company to sell the TOE overseas.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2016-04, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme Document" [1], "Requirements for IT Security Certification" [2], and "Requirements for Approval of IT Security Evaluation Facility" [3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] prepared by the Evaluation Facility and related evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight reviews were also prepared for those concerns found in the certification process.

Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name:	Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform VX7 Control Program
TOE Version:	80-01-25-00/00 (R8-01A-06_Z)
Developer:	Hitachi, Ltd.

Users can verify that a product is the evaluated and certified TOE by the following means.

- Domestic distribution

  Identification information is described in the label of four CD-Rs that store the product. End users (procurement entities and general customers who actually use the TOE) can confirm the identification information according to the description in the guidance to confirm that the product is the evaluated TOE.

- Overseas distribution

  Hitachi Data Systems Corporation can confirm that the group of files that was obtained separately is this TOE, based on the information (file name and hash value) described in emails from the developer.

  Hitachi Data Systems Corporation is responsible for notifying end users (procurement entities and general customers who actually use the TOE) that the product is the evaluated TOE.

3. Security Policy

This chapter describes security function policies that the TOE adopts to counter threats, and organizational security policies.

The TOE is a program that controls access from the host connected with the storage system to the protected user data stored in the storage system and provides a function to manage the settings.

The security functions and purposes of the TOE are as follows.

- The TOE prevents falsification and leakage of user data through the host by identifying hosts and controlling access.

- The TOE prevents leakage of user data from the removed memory device by the secure management of encryption keys that are used by the storage system for the encryption processing of user data and by erasing user data completely.

- The TOE satisfies requests from procurement entities by identifying and authenticating a fibre channel switch.

- The TOE identifies and authenticates TOE users and permits the use of the functions to operate the storage system and to manage the TOE within the scope of user authority to avoid unauthorized use of the functions.

- For the communication between the TOE and the external authentication server or the Storage Navigator program via the external LAN, mutual identification/ authentication and encrypted communication are used to prevent the impersonation of TOE users.

- The TOE records the events related to security functions, and prevents and reduces unauthorized operations.

The TOE has the mechanism to protect implementation of these functionalities.

3.1 Security Function Policies

The TOE possesses the security functions to counter threats shown in Section 3.1.1 and to satisfy the organizational security policies shown in Section 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

This TOE assumes the threats shown in Table 3-1 and provides the functions for countermeasure against them.

Table 3-1 Assumed Threats

Identifier	Threat
T.TSF_COMP	A third party may impersonate the storage administrator by illegally obtaining the communication data, including ID and password of the storage administrator, from the external LAN to change disk storage system settings and may access the LDEV (logical volume) where user data are stored.
T.LP_LEAK	In a SAN environment where multiple hosts connect to the same port, a third party might be able to leak, falsify, and delete user data by accessing LDEV (logical volume) of the specific host from another host. In an operational environment assumed in this evaluation, when the connected host is changed to another host with a different WWN, or when the WWN of the host is changed, it is assumed that the other host is connected.
T.CHG_CONFIG	A third party may be able to leak, falsify, and delete user data by illegally changing the access setting to 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.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 based on the following security function policies.

(1) Countermeasure to the threat "T.TSF_COMP"

A third party who can connect to the external LAN may illegally connect a device in the communication path between the Storage Navigator program and the SVP PC, or between the SVP PC and the external authentication server, to obtain communication data including the user ID and the password of Storage Navigator user, and may access LDEV that stores the user data by changing the storage system settings as a Storage Navigator user.

The TOE counters the threat of wiretapping on the external LAN by using encrypted communication for communications between the Storage Navigator program and the SVP PC, or between the SVP PC and the external authentication server. Therefore, a third party who can connect to the external LAN is unable to obtain the user ID and the password of the Storage Navigator user to impersonate the Storage Navigator user. In addition, the user ID, the password, and the group information of the Storage Navigator users registered in the external authentication server are managed properly, so it is impossible to register a user ID and a password of an unauthorized Storage Navigator user to the external authentication server to impersonate a normal Storage Navigator user and log in.

(2) Countermeasure to the threat "T.LP_LEAK"

A third party may access LDEV other than LDEVs assigned to the host might leak or falsify user data.

The TOE identifies and authenticates the host and permits only access to the permitted LDEV from the host, based on the security attribute of the identified host. The storage system, host, and fibre channel switch are installed in a physically protected secure area where entrance and exit are managed properly. Therefore, the physical connection between the host fibre channel adapter and the fibre channel switch port and that between the channel adapter port of the TOE and the fibre channel switch port are protected. In addition, as for fibre channel switches, the communication path between the host and the fibre channel switch, between the fibre channel switch and the TOE, and the communication path from the host to the TOE on the fibre channel switch are properly set and maintained. Thus, it is considered that it counters the threat except for the case where an attacker gains control of the host.

(3) Countermeasure to the threat "T.CHG_CONFIG"

A third party who can connect to the external LAN may change the settings of the storage system by exploiting the Storage Navigator program to access LDEV and leak, falsify, or delete user data.

The TOE identifies and authenticates Storage Navigator users and maintenance personnel and rejects login for one minute if login fails three times in a row. Therefore, unauthorized login to the Storage Navigator program by a third party who can connect to the external LAN is reduced. In addition, the TOE records the events related to security to logs, so it can discover attempt to login to the Storage Navigator program by a third party and suspicious TOE setting changes and reduce the threat by taking appropriate actions.

(4) Countermeasure to the threat "T.HDD_THEFT"

User data may be leaked from the memory device removed from the storage system by maintenance personnel.

The storage system encrypts user data by using the installed encryption device (LSI for encryption processing) and stores them in a memory device, or decrypts them to send to the host. The TOE securely generates or discards the encryption key to be used at the time. User data on the memory device are always encrypted, and the TOE manages the encryption key securely so that the encrypted user data would not be decrypted even if the memory device is removed. Thus, it counters the above threat.

(5) Countermeasure to the threat "T.HDD_REUSE"

When a storage administrator reuses the storage system or memory device, the user data remaining in the memory device may be leaked to the storage users.

When the use of the storage area on the memory device assigned to the host is stopped, or when the memory device in the storage system is replaced, the TOE overwrites the user data in the storage area to counter the threat of leakage of user data from the removed memory device.

3.1.2 Organizational Security Policy and Security Function Policy

3.1.2.1 Organizational Security Policy

An organizational security policy required in use of the TOE is shown in Table 3-2.

Table 3-2 Organizational Security Policy

Identifier	Organizational Security Policy
P.MASQ	If a customer requests identification and authentication of a fibre channel switch that is connected to the host, the fibre channel switch connected to the host shall be identified and authenticated.

This policy is based on the assumption that the procurement entities who use the storage system may request to limit the fibre channel switch that is connected with the storage system.

3.1.2.2 Security Function Policy to Organizational Security Policy

The TOE provides the security function to satisfy the organizational security policy shown in Table 3-2.

(1) Means to support organizational security policy, "P.MASQ "

The TOE uses the FC-SP (Fibre Channel Security Protocol) to authenticate the fibre channel switches. If the fibre channel switch authentication is required, the Storage Area Network (hereinafter referred to as the "SAN") consists of the fibre channel switches that comply with the FC-SP.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.NOEVIL	Out of storage administrators, the security administrator and audit log administrator are assumed to have sufficient competence to operate and manage the entire disk storage system, perform proper operations as specified by manuals, and to never commit any unauthorized behavior. The storage resource administrator is assumed to have sufficient competence to manage and operate the disk subsystem within the scope permitted by the security administrator and to perform proper operations as specified by manuals, and to never commit any unauthorized behavior.
A.PHYSICAL_SEC	The security administrator is assumed to install the disk storage system, the host (including the fibre channel connection adapter), devices that constitute the SAN environment (fibre channel switch, cable), other disk storage systems, and the external authentication server in a secure area where entry and exit are managed and to perform operations appropriately so that the setting values (such as WWN) that are set in each device and the connection status (connection status to the SAN) are maintained.
A.MANAGE_SECRET	The secret for fibre channel switch authentication that is set in the fibre channel switch connected to the host is assumed to be managed under the security administrator's responsibility to protect it from the use by unauthorized person.
A.MANAGEMENT_PC	The storage administrator is assumed to properly install and manage the management PC to protect it from unauthorized use.

Identifier	Assumptions
A.MAINTENCE_PC	When a responsible person in an organization signs a maintenance contract, the acceptance of maintenance personnel and the maintenance PC is permitted, and maintenance personnel are permitted to enter a secure area and to install the maintenance PC. It is assumed that people other than maintenance personnel do not use the maintenance PC without authorization.
A.CONNECT_STORAGE	Other disk storage systems that are connected to the TOE are assumed to be limited to the disk storage system with the TOE installed.
A.EXTERNAL_SERVER	It is assumed that the external authentication server can use authentication protocols (LDAPS, LDAP+starttls, and RADIUS (authentication protocol is CHAP)) which can protect communication with SVP PC (management maintenance IF PC) supported by the TOE, and user identification information and user group information can be appropriately registered and managed while keeping consistency with the TOE.

4.2 Environmental Assumptions

The storage system with the TOE installed (including the internal LAN and maintenance PC), SAN (including the fibre channel switch), host (including the fibre channel connection adapter), other storage systems, and external authentication servers are installed in a physically protected secure area where entrance and exit are controlled and properly managed. The management PC is set in an area where the security administrator can directly manage, so that it is not illegally used. The storage system with the TOE installed, the external authentication server, and the management PC are connected to the external LAN.

Figure 4-1 shows the operational environment to be assured by the TOE. Table 4-2 describes the details of the operational environment.

The following describes the notes on the operational environment.

- The environment has a fibre channel switch and a host.
- The storage system and the host are connected through a fibre channel switch.
- For the function that copies data between storage systems by connecting the port in the storage system with “another disk storage system,” a different port in the same storage system is connected without using “another disk storage system.”

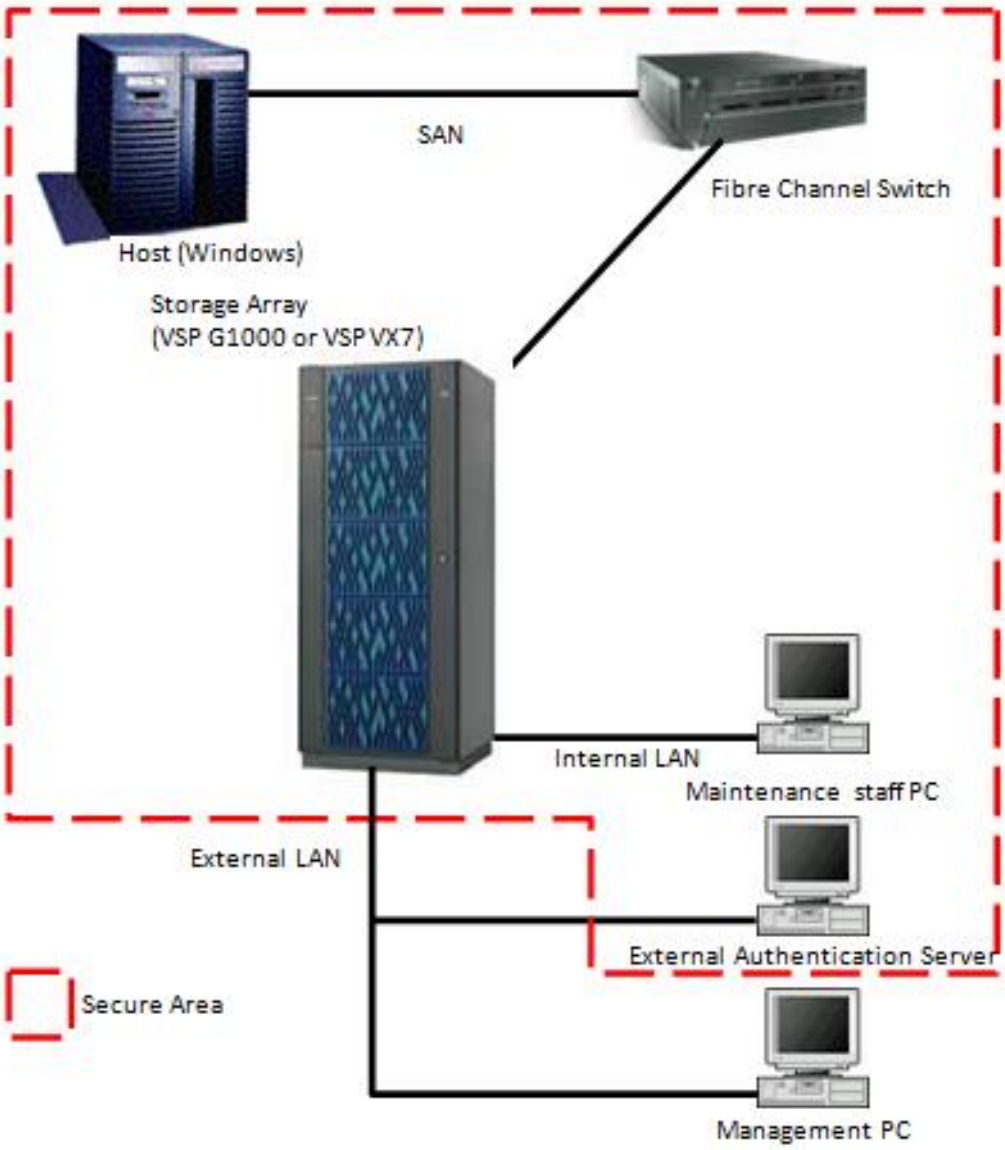


Figure 4-1 Operational Environment of the TOE to be Assured

Table 4-2 Details of the Operational Environment of the TOE to be Assured

Terminal/Device name	Product
Storage system	Hardware of Hitachi Virtual Storage Platform G1000 or Hitachi Virtual Storage Platform VX7 (details are following components) - MP packages: 2 - CHA: 2 - DKA: 2 - Cache 16G x 4 - Twelve 2.5-inch Disk Drives with three RAID1 (2D+2D) parity groups Windows 7 with Service Pack 1(x64) (OS for the SVP PC)
Host	Server machine with the following software and hardware • Windows Server 2008 • One of the following combination - Fibre Channel Connection Adapter: Qlogic Fibre Channel Adapter, Model: QLE2564-CK (corresponding driver: Fibre Channel Adapter STOR miniport driver 9.1.4.6) - Fibre Channel Connection Adapter: Brocade 16G FC HBA, Model: BR-1860-2P00 (corresponding driver: bfa 3.2.1.0) - Fibre Channel Connection Adapter: Emulex LightPulse, Model: Lpe12002-M-HI (corresponding driver: Storport Miniport Driver 7.2.20.6)
Fibre channel switch	One of the followings - Brocade300, Model: BR-360-0008 (firmware: Fabric OS v6.4.1b) - Brocade6505, Model: ER-7000-0340 (firmware: Fabric OS v7.2.0c)
Management PC	PC with the following software - Windows 7 SP1 - Internet Explorer 10 - Flash Player 11.6 - JRE 1.7.0_21
Maintenance PC	PC with the following software - Windows 7 SP1 - Internet Explorer 10 - Flash Player 11.6 - JRE 1.7.0_21
External authentication server	Server machine with the following software - Windows Server 2008

The storage system installed with the TOE and the host (including the fibre channel connection adapter) are connected to the SAN (including the fibre channel switch) to communicate with each other. The SAN should not be connected to other networks. The external LAN should not be connected directly to external network, such as the Internet, and the management PC cannot be accessed directly from outside.

In the storage system installed with the TOE, the encryption device (LSI for encryption processing) to encrypt/decrypt user data is installed. The storage system, fibre channel switch, and the fibre channel connection adapter shown in this configuration are not covered in this evaluation, but they should be sufficiently reliable.

4.3 Clarification of Scope

The following function of the TOE is not covered in this evaluation.

- The function that performs external authentication by using the Kerberos (v5) method

5. Architectural Information

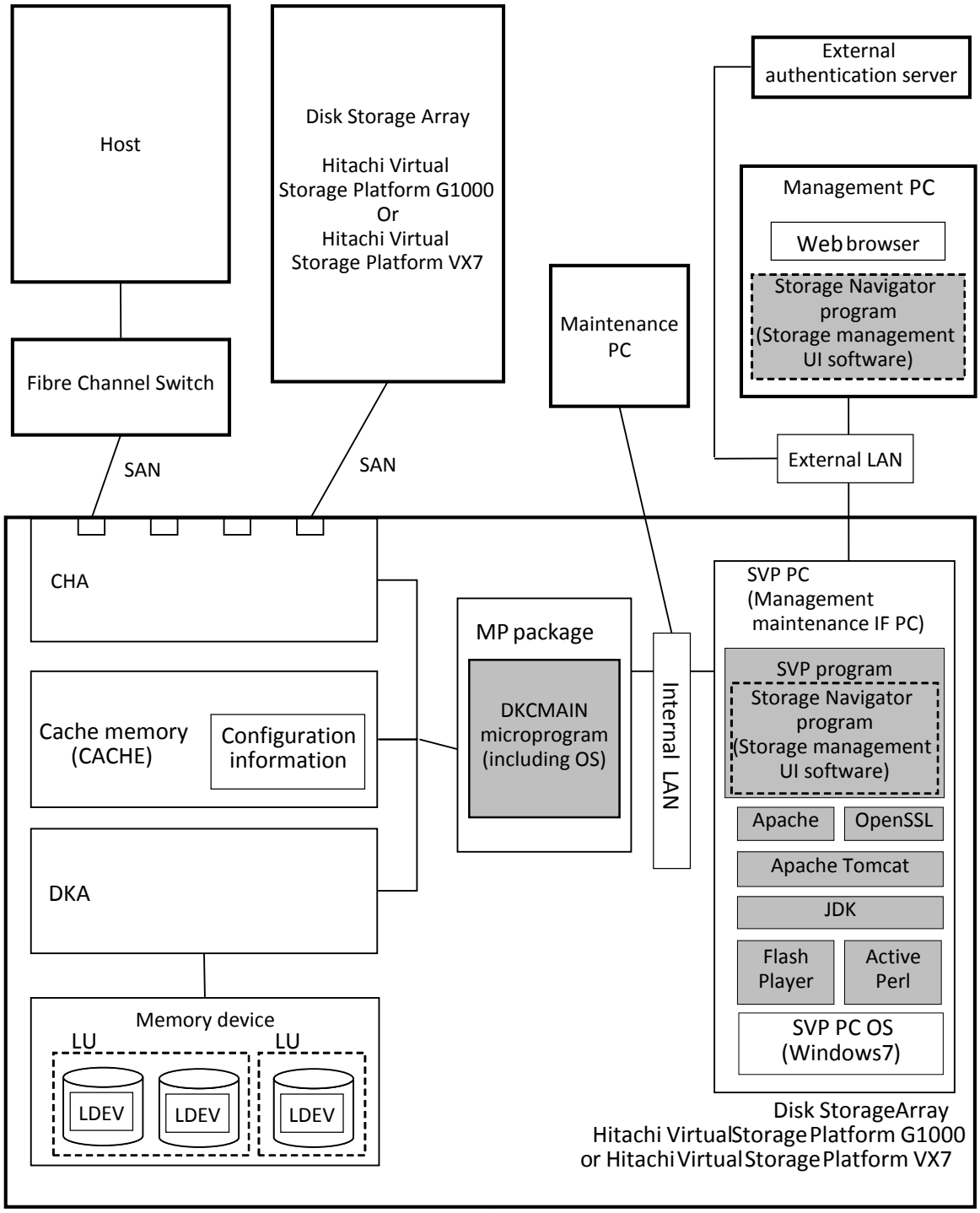
This chapter explains the scope and the main components (subsystems) of the TOE.

5.1 TOE Boundary and Components

Figure 5-1 shows the configuration of the TOE. The TOE is classified into the following programs.

- The DKCMAIN micro-program (including OS) that runs on the MP package
- The SVP program that runs on the SVP PC and a group of programs (JDK, Apache, Apache Tomcat, OpenSSL, Flashplayer, ActivePerl) that provide the functions required for running the SVP program
- The Storage Navigator program that runs on the management PC (It is included in the SVP program as data and is transferred to the management PC to operate.)

The hardware of the storage system on which the TOE runs and the OS of the SVP PC that runs the SVP program are not covered in the TOE scope.



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 5-1 TOE Boundary

The following descriptions explain the DKCMAIN micro-program (including OS) and the SVP program including the Storage Navigator program that constitute the TOE.

(1) DKCMAIN micro-program

The DKCMAIN micro-program is a control program of the storage system that controls host connections, data transfer between the host and the storage system, and data input/output to the memory device; manages encryption keys and security function data; and provides the shredding function. It is installed and runs on the MP package in the storage system. The following shows the major security functions of the DKCMAIN micro-program.

- Connection control of host/fibre channel switch (FC-SP/FCP connection)
  - > Identification and authentication of host/fibre channel switch (DH-CHAP authentication (Response verification including secret))
  - > Access control to logical units (LU) of the host
- Role-based access control to security function data
- Encryption key management (to generate and delete)
- Shredding function
- Settings to run/stop security functions
  - > Setting of the FC-SP authentication function
  - > Setting of the stored data encryption function
- Management of security function data (to create, modify, and delete)
  - > WWN, management of secret
  - > Management of resource group information, LU path information, LDEV information
  - > Management of users' role information
  - > Backing up/restoring encryption keys (hash verification of encryption keys)

(2) SVP program

The SVP program is management software that performs operations and maintenance of the storage system and manages the configuration information by establishing remote desktop connection with the Storage Navigator program, performing identification and authentication of TOE users, providing the interface to set the TOE, and requesting settings to the DKCMAIN micro-program. The SVP program is installed and runs on the OS (Windows 7 with Service Pack 1 (x64)) on the SVP PC. The following shows the major security functions of the SVP program.

- Identification and authentication of SVP program users
  - > Identification and authentication of users (security administrators, storage administrators, audit log administrators, maintenance personnel)
  - > Rejecting access when authentication fails in a row
  - > Internal authentication function, external authentication function, communication with the external authentication server (authentication, encryption)
- Management of accounts and host information (to create, change, and delete)
  - > Management of user information (user ID/password) and user group information
  - > Quality verification of passwords and secret
- TLS connection of the Storage Navigator program, the remote desktop connection
- The window control function of the SVP program
- Role-based control of setting requests for the DKCMAIN micro-program

> Control of requests to set up security functions
> Control of requests to run/stop security functions
> Control of requests to manage security function data

- Settings of security functions
  > Setting of the internal authentication method/external authentication method
  > Setting of connecting the external authentication server

- Input/output of setting file
  > Reading/writing backup file of encryption keys

- Audit log function
  > Recording and storing audit logs (wrap-around method)
  > Outputting audit logs

(3) Storage Navigator program

The Storage Navigator program is a client program that connects to the SVP program and provides the graphical user interface to operate the SVP program. The Storage Navigator program runs on the Web browser of the management PC. TLS communication is used between the Storage Navigator program and the SVP program.

5.2 IT Environment

The DKCMAIN micro-program and the SVP program that constitute the TOE run on separate hardware, but they are connected via internal LAN that is protected by the assumptions, and communicate with each other. The maintenance PC is also connected to the internal LAN and establishes the remote desktop connection to the SVP PC to use the SVP program.

The SVP program, the Storage Navigator program, and the external authentication server are connected via the external LAN. The external LAN is not protected by the assumptions, etc., so the authenticated and encrypted communication is used between the SVP program and the Storage Navigator program as well as between the SVP program and the external authentication server.

The DKCMAIN micro-program and the host are connected via the SAN that consists of a fibre channel switch. The SAN and the fibre channel switch are physically protected based on the assumptions, so that no third party would change the physical configuration of the SAN. The fibre channel switch has secure settings to avoid unauthorized use.

This storage system uses the security functions of the TOE, such as TLS communication of the Storage Navigator program and the access control, and physically separates the DKCMAIN micro-program and the SVP program to protect user data to be protected on the CHA, CACHE, DKA, and memory device from unauthorized access by attackers who connect to the external LAN.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions. English versions of the documents are English translations of the Japanese versions of the documents. Contents of the English versions are the same as those of the Japanese versions except some parts. "Table 6-3 Disk subsystem maintenance manual (Japanese version)" and "Table 6-4 Disk subsystem maintenance manual (English version)" show guidance documents for maintenance personnel.

Table 6-1 Users Guide (Japanese version)

No	Name of document attached to the product (Users guide)	Version
1	Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 ISO15408 Function of Acquiring Authentication; Instruction Manual	2.9
2	Hitachi Virtual Storage Platform G1000 Mainframe System Administrator Guide	1
3	Hitachi Virtual Storage Platform G1000 Hitachi Storage Navigator Messages	1
4	Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems	1
5	Hitachi Virtual Storage Platform G1000 Encryption License Key User Guide	1
6	Hitachi Virtual Storage Platform G1000 Hitachi Volume Shredder User Guide	1
7	Hitachi Virtual Storage Platform G1000 Hitachi Audit Log User Guide	1
8	Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 User Guidance	1.7

Table 6-2 Users Guide (English version)

No	Name of document attached to the product (Users guide)	Version
1	Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 Manual for Obtaining ISO15408 Certification	2.2
2	Hitachi Virtual Storage Platform G1000 Mainframe System Administrator Guide	MK-92RD 8016-00
3	Hitachi Virtual Storage Platform G1000 Hitachi Storage Navigator Messages	MK-92RD 8017-00i
4	Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems	MK-92RD 8014-00
5	Hitachi Virtual Storage Platform G1000 Hitachi Encryption License Key User Guide	MK-92RD 8009-00
6	Hitachi Virtual Storage Platform G1000 Hitachi Volume Shredder User Guide	MK-92RD 8025-00
7	Hitachi Virtual Storage Platform G1000 Hitachi Audit Log User Guide	MK-92RD 8008-00i

No	Name of document attached to the product (Users guide)	Version
8	Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 User's Guidance	1.4

Table 6-3 Disk Subsystem Maintenance Manual (Japanese version)

No	Name of document attached to the product (Maintenance manual)	Version
1	Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 ISO15408 Function of Acquiring Authentication; Disk Array System Maintenance Manual	2.3
2	A/H-65AD A-65BD HT-40BD Maintenance Manual	REV.0.1

Table 6-4 Disk Subsystem Maintenance Manual (English version)

No	Name of document attached to the product (Maintenance manual)	Version
1	Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 Obtaining ISO15408 Certification Maintenance Manual	2.0
2	DKC810I Maintenance Manual	REV.0.1

- "A/H-65AD A-65BD HT-40BD" and "DKC810I" are aliases of "Hitachi Virtual Storage Platform G1000."
- There are some differences in delivery method and maintenance system between Japan and foreign countries. Therefore, the English version of No.2 of the maintenance manual slightly differs from its Japanese version. The description of "INSTALLATION SECTION" of the "DKC810I Maintenance Manual" is not written in the Japanese version of the manual. However, an equivalent description is not attached to the TOE but exists as a document for maintenance personnel.

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Mizuho Information& Research Institute, Inc., Information Security Evaluation Office that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which is agreed on mutual recognition with ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2014-04 and concluded upon completion of the Evaluation Technical Report dated 2016-04. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2014-08 and 2014-12, and examined the procedural status conducted in relation to each work unit for configuration management and delivery by investigating records and interviewing staff. Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2014-08, 2015-02, 2015-09, 2016-02, and 2016-04.

Concerns that the Certification Body found in the evaluation process were described as the certification oversight reviews, and those were sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, those concerns were reflected in the Evaluation Technical Report.

7.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed.
As a result of verifying the evidence shown in the process of the evaluation and the testing performed by the developer, the evaluator performed the reproducibility testing and additional testing judged to be necessary, based on the vulnerability assessments.

7.4.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the documentation of actual testing results. The content of the developer testing evaluated by the evaluator is explained as follows.

1) Developer Testing Environment

The configuration of the testing conducted by the developer is the same as the one in "4.2 Environment Assumptions." The configuration in "4.2 Environmental Assumptions" is the configuration to be assured in the ST.

- The storage system for the developer testing is "Hitachi Virtual Storage Platform G1000." The evaluator determines that "Virtual Storage Platform VX7" and "Hitachi Virtual Storage Platform G1000" are the same as the operational environment because these are different only in the name.
- In "4.2 Environmental Assumptions," OS selections are available. In the developer testing configuration, a specific OS is selected. (For example, Windows 7 Professional SP1 is selected as an OS of the management PC.) The evaluator determines that these selections do not affect the testing.

The TOE to be tested in the developer testing is "Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform VX7 Control Program, Version 80-01-25-00/00 (R8-01A-06_Z)." It is consistent with the TOE identification described in the ST.

Therefore, it can be concluded that the developer testing was performed in the TOE testing environment, which was identical to the TOE configurations specified in the ST.

2) Summary of the Developer Testing

A summary of the developer testing is described as follows.

a. Developer Testing Outline

An outline of the developer testing is described as follows.

<Developer Testing Approach>

From the Storage Navigator program and maintenance PC, combinations of values that can be entered in the screen were tested for the external interfaces of the TOE. From the screen display and messages of the Storage Navigator program, the behavior of the TOE for input and the behavior related to the TOE and the external authentication server were indirectly confirmed.

As an approach to observe TOE responses, the following approach was also used.

- By using the network protocol analyzer, communication packets were captured and observed.
- The content of the memory device was observed by each sector from the host.

For the behavior that is difficult to confirm by observing TOE responses, the following approach was used.

- The source code of the TOE was reviewed.

<Developer Testing Tool>

The following testing tool was used in the developer testing.

- Wireshark 1.10.3 (used for network protocol analyzer)

<Content of the Performed Developer Testing>

From the Storage Navigator program and the maintenance PC, the developer entered data by directly manipulating the available external interfaces (1) and (2) below and confirmed that:

- The screen outputs and the expected testing results were compared, and security functions, such as identification and authentication of the Storage Navigator users and maintenance personnel as well as access control to the setting data, were confirmed.
- The content of the memory device was observed by each sector from the host, and it was confirmed that the shredding function was running.

Regarding the interface with the host as shown in (3) below, the developer accessed the storage system by manipulating the host and compared the TOE logs with the expected testing results. Security functions, such as identification and authentication of the fibre channel switch as well as access control of storage area, were checked.

As for the TLS communication of the interface (1) below and the authentication of the interface (4) below, the developer observed the content of the communication by using Wireshark, and confirmed that the protocols used for the TLS communication and authentication were appropriately implemented.

(1) Interface between the TOE and the Storage Navigator users (Management PC)

(2) Interface between the TOE and the maintenance PC

(3) Interface between the TOE and the host

(4) Interface between the TOE and the external authentication server

It is difficult to confirm that encryption keys for encrypting data to be stored in the memory device are properly generated by using the above interfaces from (1) to (4), so the developer reviewed the source code and confirmed.

b. Scope of the Performed Developer Testing

The developer testing was conducted on 117 items by the developer. The coverage of the testing to the security functions and external interfaces described in the functional specification had been confirmed by the coverage analysis. It was determined that the

coverage of some external interfaces was not sufficient, so the independent testing was conducted by the evaluator to cover this insufficiency.

c. Result

The evaluator confirmed the approach of the performed developer testing and the legitimacy of tested items, and confirmed consistencies between the testing approach described in the testing plan and the actual testing approach. The evaluator confirmed consistencies between the testing results expected by the developer and the actual testing results performed by the developer.

7.4.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the execution of security functions by the test items extracted from the developer testing. In addition, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to gain further assurance that security functions are certainly implemented, based on the evidence shown in the process of the evaluation. The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The configuration of the independent testing is almost the same as the configuration of the developer testing except that some OS selections are different. The evaluator determined that the difference in OS selections does not affect the testing. The components and testing tools used for the independent testing were prepared by the developer, and their validity confirmation and operation check were performed by the evaluator.

The TOE to be evaluated is "Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform VX7 Control Program, Version 80-01-25-00/00 (R8-01A-06_Z)." It is consistent with the TOE identification described in the ST.

The independent testing was conducted in an environment with the same TOE configuration as the one identified in the ST.

2) Summary of the Independent Testing

A summary of the independent testing is described as follows.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluator designed from the developer testing and the provided evaluation documentation are shown below.

For the sampling of the developer testing, sufficient tests were selected so that all interface types and testing approaches would be covered.

From the developer testing and the provided evaluation documentation, the evaluator devised the independent testing from the following viewpoints.

(i) The TOE behavior that was not confirmed in the developer testing shall be covered by the independent testing.

(ii) For the developer testing, testing procedure and observation shall be added to check

the TOE behavior more strictly.

(iii) For the TOE behavior that was confirmed in the developer testing, the testing shall be made stricter by testing the behavior with combinations of different parameters and interfaces.

(iv) For TOE behavior that was confirmed in the developer testing, the testing shall be made stricter by testing the situations of the conflicts with other behaviors.

b. Independent Testing Outline

The evaluator conducted sampling tests for 65 items from the following viewpoints based on the developer testing and the provided documentation. The evaluator devised additional independent testing for 11 items from the above viewpoints based on the developer testing and the provided documentation. The outline of the independent testing performed by the evaluator is described as follows.

<Independent Testing Approach>

The same approach with the developer testing was used.

<Content of the Performed Independent Testing>

The evaluator conducted the independent testing for 11 items.

Table 7-1 shows viewpoints of the independent testing and the content of the testing corresponding to them.

Table 7-1 Content of the Performed Independent Testing

No.	Outline of the Independent Testing
1	From the viewpoint (i); Access control for role-based operation function (1): When the role of a user is changed from the storage administrator to the security administrator, it is confirmed that it is impossible to access the operation menu of the storage administrator.
2	From the viewpoint (i); Access control for role-based operation function (2): It is confirmed that even if the security administrator specifies URL to try to access it, the security administrator cannot access the operation menu of the storage administrator.
3	From the viewpoint (ii); After the developer testing, in which the behavior is confirmed by changing the setting of the secret of the fibre channel switch that the TOE has, it is confirmed that the fibre channel switch is authenticated by correcting the setting.
4	From the viewpoint (ii); Login by a deleted user: After the developer testing, in which a user (storage administrator) registered to the external authentication server is deleted, it is confirmed that the user cannot log in from the Storage Navigator program.

No.	Outline of the Independent Testing
5	From the viewpoint (i); Access from the remote desktop: It is confirmed that the security administrator, storage administrator, and audit log administrator cannot connect from the remote desktop.
6	From the viewpoint (iii); For the function that is locked out due to continuous authentication failures by maintenance personnel, a case where the interface of the remote desktop and the external authentication are used is confirmed.
7	From the viewpoint (ii) and (iii); In the developer testing, in which the strength check function when changing the password of maintenance personnel is checked, it is confirmed that the changed password can be used for login. In the same testing, some tests are conducted to check with patterns of the number of characters and character types of passwords that are different from the developer testing.
8	From the viewpoint (iii); Restoring encryption keys: When a backed-up encryption key is falsified, it is confirmed that it cannot be restored to the TOE.
9	From the viewpoint (i); Suspension of the shredding function: It is confirmed that a storage administrator can stop the shredding function, and that the warning indicating the data are not shredded is displayed.
10	From the viewpoint (iv); The following behavior is confirmed when the host is accessing the storage system: When the WWN registered to the TOE is changed, it is confirmed that the host who has the old WWN cannot access the storage system.
11	From the viewpoint (i); It is confirmed that after the LDEV is deleted, the host cannot access the LDEV.

c. Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation. The penetration testing performed by the evaluator is explained as follows.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing. The following shows the five viewpoints of the identified vulnerabilities.

(1) Behavior for unexpected input and operation
There is a concern of unexpected behavior in the event of unexpected input and operation.

(2) Falsification of session
There is a concern, for maintenance management of sessions between the SVP PC and the management PC, that the TOE function might be used by bypassing in ways of modifying communications and directly specifying URL.

(3) Publicly-known vulnerability related to open ports
There is a concern, for unauthorized use of network service, which is publicly-known vulnerability information, and various vulnerabilities on the Web, that they might be exploited by accessing from the external LAN to the SVP PC.

(4) Encryption algorithm in communication
There is a concern in the encryption communications between the SVP PC and the management PC, that weak encryption methods might be used.

(5) Other concerns
There is a concern in vulnerabilities related to exclusive control, conflicting operations, and unexpected suspension that were not confirmed in the developer testing and the evaluator independent testing.

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

Figure 7-1 shows the penetration testing environment. In this environment, the test PC and testing tools are added to “4.2 Environmental Assumptions.”

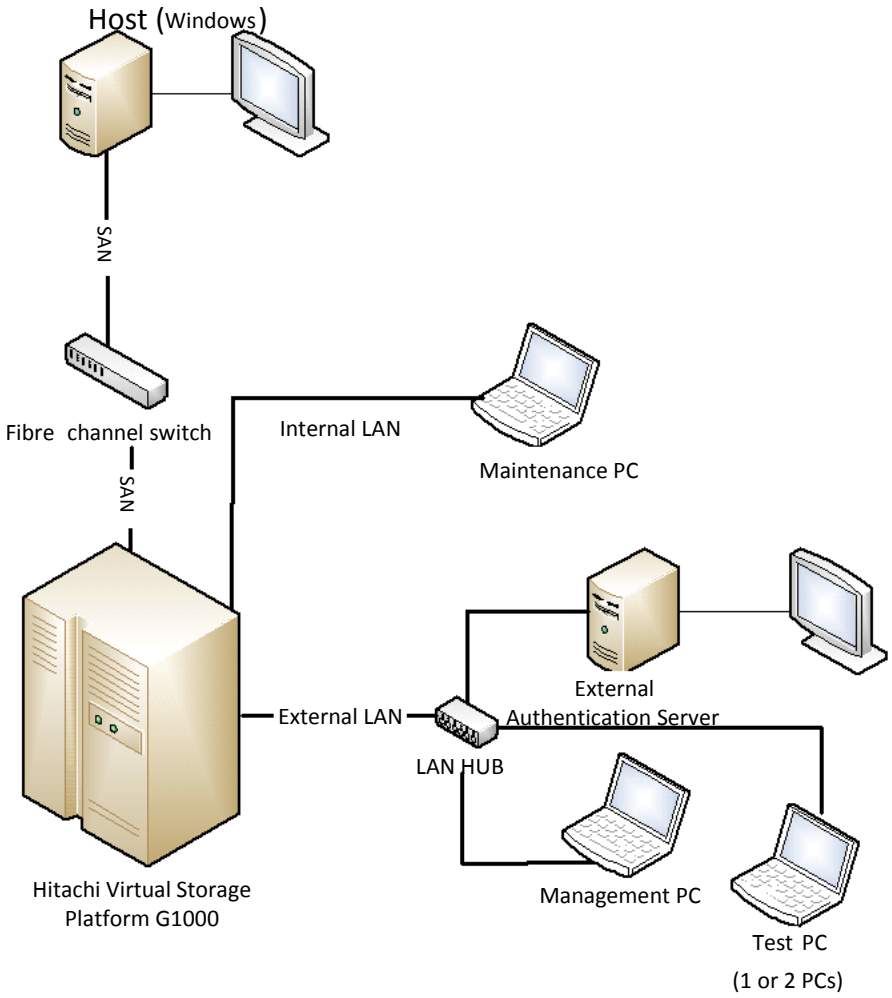


Figure 7-1 Penetration Testing Environment

Table 7-2 shows the details of the components of the penetration testing environment and testing tools used in the penetration testing.

Table 7-2 Tools used for the Penetration Testing

Tool name	Outline/Purpose of use
Nmap Ver 6.47	A tool that detects IP communication port that is opened by the device to be investigated. It investigates the ports open for the external LAN of the TOE.
Nessus Ver 6.5.4	A tool that checks publicly-known vulnerabilities, such as OS and application, based on the communication service and protocols to be used. The plug-in uses the data of February 10, 2016. It investigates the vulnerabilities of communication service open for the external LAN of the TOE.
Nikto Ver 2.1.5	A vulnerability diagnosis tool dedicated for the web server. It investigates publicly-known vulnerabilities, such as HTTP protocol and CGI. The plug-in uses the data of February 10, 2016. It investigates the web server of the TOE.

Tool name	Outline/Purpose of use
Fiddler Ver.4.4.9.0 or Ver.4.4.9.6	A tool that captures and displays HTTP packet and sends its contents by falsifying them. It investigates vulnerabilities by sending an unauthorized value to the web server of the TOE.
Wireshark Ver. 1.10.8 or Ver. 1.12.6	An analysis program of network packets. It collects packets on Ethernetwork and analyzes the protocols.
OWASP ZAP Ver. 2.3.3	An integrated penetration testing tool that tests vulnerabilities of the web applications.
openssl Ver. 1.0.2f	A tool that has the client function of SSL/TLS, hash functions, and the functions of encryption/decryption.

<Penetration Testing Approach>

By performing operations for the TOE from the Storage Navigator program and the maintenance PC, the evaluator confirms the screen transition, displayed messages, and logs of the TOE.

The use of the tools described in Table 7-2 is individually described in Table 7-3 Outline of the Penetration Testing.

<Content of the Performed Penetration Testing>

Table 7-3 shows the vulnerability of concern and the contents of the corresponding penetration testing.

Table 7-3 Outline of the Penetration Testing

No	Testing name	Outline of testing	Vulnerability of concern
1	Invalid parameter	For the parameter that has a restriction on the input values, an invalid value is set to confirm the behavior.	(1)
2	Replacing the fibre channel switch port cable	When the host accesses the storage system, the cable connected to the port of the fibre channel switch is replaced to confirm the behavior.	(1)
3	Port scan (SVP PC)	Nmap is used to check unnecessary ports open in the SVP PC.	(3)
4	General-purpose vulnerability scan (SVP PC)	The general-purpose vulnerability scan tool, Nessus, is used to check the publicly-known vulnerabilities in the SVP PC.	(3)
5	Web vulnerability scan (SVP PC)	The vulnerabilities of the web server of the SVP PC are checked by using vulnerability diagnosis tools of the web server, Nikto and OWASP ZAP. By specifying URL that shows the directory of the web server, it is checked if unauthorized access to the directory information is possible.	(3)

No	Testing name	Outline of testing	Vulnerability of concern
6	Session management	The cookie (session ID) used for session management is changed to confirm the behavior. By specifying URL from the web browser, it is checked if the session management can be prevented.	(2)
7	Exclusive control	It is confirmed that multiple storage administrators cannot edit LDEVs in the same resource group at the same time.	(5)
8	Conflicting operation	Immediately before the storage administrator edits LDEV, the behaviour is checked when the settings (storage administrator's permission, LDEV setting by maintenance personnel) that could conflict are changed.	(5)
9	Weak encryption method	By trying to connect to the TOE with a weak encryption method by using openssl and observing the communication content with Wireshark, it is confirmed that the weak encryption method is unacceptable.	(4)
10	Process suspension	The TOE behavior when the TOE process is suspended is checked by operating from the OS of the SVP PC.	(5)

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.5 Evaluated Configuration

This evaluation was performed by assuming the operational environment described in "4.2 Environmental Assumptions."

This configuration is the same as the operational environment that is assured by the ST. Note that it might be different from the operational environment that is assumed by procurement entities. (See "8.2 Recommendations.")

7.6 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM by submitting the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- Security functional requirements: Common Criteria Part 2 Conformant
- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL2 package
- Additional assurance component ALC_FLR.1

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to procurement entities.

8. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

2. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

3. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight reviews, and those were sent to the Evaluation Facility. The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report, and issued this Certification Report.

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL2 augmented with ALC_FLR.1 in the CC Part 3.

8.2 Recommendations

- The procurement entities determine whether this TOE is acceptable in the environment of the procurement entities based on the operational environment and the settings with TOE behavior to be assured. When making the determination, the procurement entities need to note the following:

  > The operational environments which assure the TOE behavior are limited. For the limited operational environments, see “4.2 Environmental Assumptions.”

  > Security is not assured when Kerberos (v5) is used as a protocol between the TOE and the external authentication server.

- The procurement entities who consider an introduction of this TOE to overseas need to note the following when judging whether this TOE is assured sufficiently:

  > When the TOE is distributed overseas, Hitachi Data Systems Corporation and TOE users maintain the security of the TOE on their own responsibilities according to the guidance after Hitachi Data Systems Corporation receives the TOE.

    For example, whether Hitachi Data Systems Corporation actually maintains the security of the TOE is not assured.

9. Annexes

There is no annex.

10. Security Target

The Security Target [12] of the TOE is provided as a separate document along with this Certification Report.

Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 Security Target, Version 3.4 (April 18, 2016) Hitachi, Ltd.

The name of this Security Target sounds like the Security Target of the storage system; however, the TOE is not the storage system but the control software of the storage system.

11. Glossary

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to the TOE used in this report are listed below.

CHA	Channel Adapter
CHAP	Challenge Handshake Authentication Protocol
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DKA	Disk Adapter
FCP	Fibre Channel Protocol
FC-SP	Fibre Channel Security Protocol
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
PC	Personal Computer
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SSL	Secure Sockets Layer
SVP	Service Processor
TLS	Transport Layer Security

WWN	World Wide Name

The definitions of terms used in this report are listed below.

Audit log administrator	Person who manages reference and download of audit logs and makes syslog related settings by using the Storage Navigator program.
CHAP authentication	Method to perform authentication by sending the encrypted password from the client to the server, based on the random character string sent from the server to the client.
Cookie	Mechanism that the web server temporarily writes and stores data in the web browser. It is used for user identification and authentication and session management.
Cross-site scripting	A web application problem that dynamically generates a web page: a vulnerability that allows injection of malicious script.
Disk subsystem	Storage system, Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform VX7
DKCMAIN micro-program	Control program of the storage system that is installed in the MP package in the storage system; it controls host connections, data transfer between the host and the storage system, and data input/output to the memory device; manages encryption keys and security function data; and provides the shredding function.
FC-SP	Protocol for secure communication using a fibre channel to authenticate each device when communicating between computers and the peripheral devices, such as storage system, and the fibre channel switch. The DH-CHAP with NULL DH Group authentication is used.
Fibre channel	Data transfer method between computers and the peripheral devices, such as the storage system. It is used when connecting the server that requires high performance with the memory device.
Fibre channel connection adapter	Network interface device for fibre channel that is installed in the computer
Fibre channel switch	Network device to mutually connect various devices that have the fibre channel interface. Using this fibre channel switch enables to build the SAN (Storage Area Network) by connecting multiple hosts and storage systems in high-speed.
LDEV	Abbreviation of “Logical Device.” It is a unit of the volume of storage area to be created in the user area in the storage system.
Logical unit (LU)	Logical unit. The minimum unit of storage area accessed by the host. It consists of one or multiple LDEVs (logical devices).

LU path information	Path information between the host and LU
Maintenance personnel	Person who belongs to a maintenance organization with which the customer who uses the storage system has a maintenance contract. The maintenance personnel is in charge of initial start-up processing performed when installing the storage system, maintenance operations, such as replacement and addition of parts, changing settings due to maintenance operations, and recovery processing in case of error.
Maintenance PC	Terminal that is used by maintenance personnel to connect to the SVP PC at maintenance.
Management PC	Terminal that is used by Storage Navigator users to operate the Storage Navigator program.
Resource group	Resource group information
Response verification	In the CHAP authentication, the server compares and verifies the encrypted password sent from the client with the encrypted password generated by the server itself.
Secret	Shared password that is used for mutual authentication using DH-CHAP with FC-SP.
Security administrator	Person who makes TOE settings by using the Storage Navigator program, such as managing accounts, resource groups, and user groups as well as authentication settings of hosts and fibre channel switches for the TOE.
Session hijacking	Attack technique that a third party takes over the communication session between the server and the client (a group of communications performed among specific users): e.g. web session hijacking in HTTP.
Shredding function	Function to overwrite memory devices, such as hard disks, with dummy data to erase the remaining data.
starttls	The extended version of the SMTP protocol. Communication is encrypted using SSL/TLS.
Storage administrator	Person who manages resources of the assigned storage system by using the Storage Navigator program.
Storage Area Network (SAN)	The network system that connects servers, etc., with memory devices, etc. It establishes communications using fibre channels and Ethernet.
Storage Navigator program	Program that provides GUI to make settings for the storage system. It consists of the Flex application and the Java applet, and runs on the SVP PC and the management PC. It is used by Storage Navigator users and maintenance personnel.

Storage Navigator users	Users of the Storage Navigator program, including security administrators, storage administrators, and audit log administrators.
Storage user	An entity which uses user data stored in the storage system. The entity is the host or manipulates the user data via the host.
SVP PC	PC in the storage system to install the SVP program
SVP program	Management software that is installed in the SVP PC in the storage system. It connects the Storage Navigator program with the remote desktop, performs identification/authentication of TOE users, displays the TOE setting interface, and communicates with the DKCMAIN micro-program to perform operations and maintenance of the storage system and manage the configuration information.
User group	User group information
Wrap-around method	When the log file size is limited, and the file becomes full, it is returned to the top of the file to overwrite the logs.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, June 2015, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2015, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001 (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002 (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003 (Japanese Version 1.0, November 2012)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004 (Japanese Version 1.0, November 2012)

[12] Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 Security Target, Version 3.4 (April 18, 2016) Hitachi, Ltd.

[13] Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 Control Program Evaluation Technical Report, Version 6 (128747-01-R003-06) April 26, 2016, Mizuho Information& Research Institute, Inc., Information Security Evaluation Office