# Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

| | |
|---|---|
| Application date/ID | 2005-09-30 (ITC-5068) |
| Certification No. | C0102 |
| Sponsor | Hitachi Ltd. |
| Name of TOE | SANRISE Universal Storage Platform CHA/DKA Program (for Japan)<br>TagmaStore Universal Storage Platform CHA/DKA Program (International)<br>SANRISE Network Storage Controller CHA/DKA Program (for Japan)<br>TagmaStore Network Storage Controller CHA/DKA Program (International)<br>SANRISE H12000 CHA/DKA Program (for Japan)<br>SANRISE H10000 CHA/DKA Program (for Japan) |
| Version of TOE | 50-04-34-00/00 |
| PP Conformance | None |
| Conformed Claim | EAL2 |
| Developer | Hitachi Ltd. |
| Evaluation Facility | Electronic Commerce Security Technology Laboratory Inc. Evaluation Center |

This is to report that the evaluation result for the above TOE is certified as follows.
2007-06-27

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center

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

- Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408:1999)
- Common Methodology for Information Technology Security Evaluation Version 1.0
- CCIMB Interpretations (as of 01 December 2003)

Evaluation Result: Pass

"SANRISE Universal Storage Platform CHA/DKA Program (for Japan)", "TagmaStore Universal Storage Platform CHA/DKA Program (International)", "SANRISE Network Storage Controller CHA/DKA Program (for Japan)", "TagmaStore Network Storage Controller CHA/DKA Program (International)", "SANRISE H12000 CHA/DKA Program (for Japan)" and "SANRISE H10000 CHA/DKA Program (for Japan)" Version 50-04-34-00/00 has been evaluated in accordance with the provision of the "IT Security Certification Procedure" 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

## 1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "SANRISE Universal Storage Platform CHA/DKA Program (for Japan)", "TagmaStore Universal Storage Platform CHA/DKA Program (International)", "SANRISE Network Storage Controller CHA/DKA Program (for Japan)", "TagmaStore Network Storage Controller CHA/DKA Program (International)", "SANRISE H12000 CHA/DKA Program (for Japan)" and "SANRISE H10000 CHA/DKA Program (for Japan)" Version 50-04-34-00/00 (hereinafter referred to as "the TOE") conducted by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, Hitachi Ltd.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to "1.5.9 Documents Attached to Product" for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

## 1.2 Evaluated Product

### 1.2.1 Name of Product

The target product by this Certificate is as follows:

| | |
|---|---|
| Name of Product: | SANRISE Universal Storage Platform CHA/DKA Program (for Japan)<br>TagmaStore Universal Storage Platform CHA/DKA Program (International)<br>SANRISE Network Storage Controller CHA/DKA Program (for Japan)<br>TagmaStore Network Storage Controller CHA/DKA Program (International)<br>SANRISE H12000 CHA/DKA Program (for Japan)<br>SANRISE H10000 CHA/DKA Program (for Japan) |
| Version: | 50-04-34-00/00 |
| Developer: | Hitachi, Ltd. |

### 1.2.2 Product Overview

TOE is the software that controls the storage device.

TOE provides the security function of executing access control over the user data in the storage device for preventing unintended access (i.e. changes due to illegal access or erroneous operations to user data which must not be changed).

### 1.2.3 Scope of TOE and Overview of Operation

Figure 1-1 illustrates the configuration where the storage device including TOE is used.

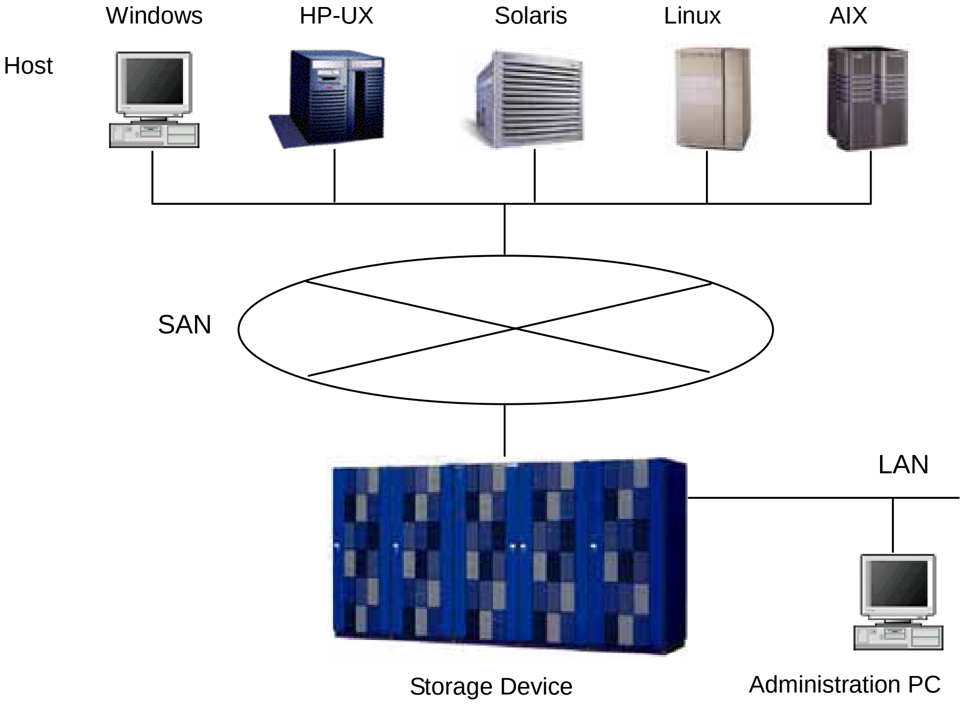

Figure 1-1 Configuration of the Storage Device

- Installation Site of the Storage Device

A storage device is usually installed in a secure area where entrance and exit is controlled.

- SAN and Hosts

Open-system servers such as Windows, HP-US or Solaris (those products are generically called “hosts” by this authentication report) and storage devices are usually connected via SAN (Storage Area Network). SAN is a dedicated network for the storage system that connects the hosts and the storage device via Fibre Channel.

- Administration PC

The administration PC is the PC for setting up device control information of the storage device from remote sites. Operates the program for the storage device administrator to set up the device control information on the administration PC.

The administration PC and the storage device are connected via LAN (Local Area Network).

The administration PC and other PCs are duly connected to LAN by the organization, assuming the environment where only proper people can operate it e.g. those authenticated by the function of the OS.

The internal configuration of the storage device is illustrated in Figure 1-2 below, where TOE consists of the "CHA program" and the "DKA program" in the storage device.

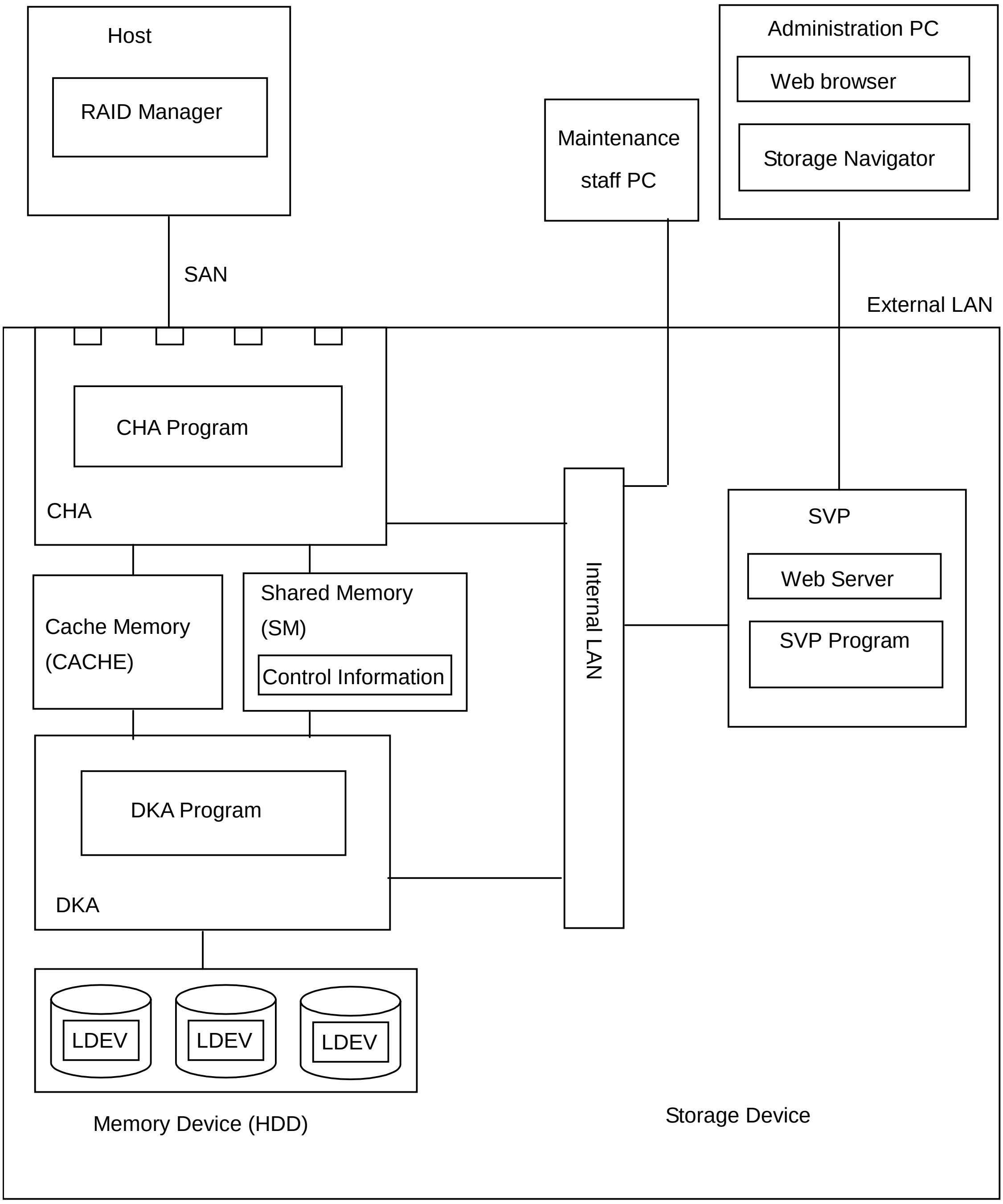

Figure 1-2 The Internal Configuration of the Storage Device

- Channel Adapter(CHA)

Channel Adapter processes a command by the host to the storage device, and controls data transmission. The host is connected to the fiber port on CHA via Fibre Channel. On CHA, the CHA program which is part of TOE operates.

- Disk Adapter (DKA)

Disk Adapter controls data transmission between CACHE and HDD.
On DKA, the DKA program which is part of TOE operates. The CHA program and the

DKA program work together to realize the “CHA/DKA program” function.

- Cache Memory(CACHE)

  Cache Memory is located between CHA and DKA, used for data Read/Write.

- Shared Memory (SM)

  Shared Memory is the memory that is accessible both from the CHA program and from the DKA program. Control information for accessing data from CHA and DKA is stored in it. This control information includes the setting information required for the security function to operate is included. Control information on Shared Memory is updated by TOE, according to the commands from SVP or Storage Navigator.

- Memory Device(HDD)

  Memory Device consists of multiple hard disks, in which user data is recorded. In HDD, an LDEV (Logical Device) which is the volume to store user data is created. Access to user data is controlled by the LDEV.

- SVP

  SVP is a service processor embedded in the storage device for administrating the whole storage device.

- Maintenance Staff PC

  The maintenance staff PC is used by maintenance staff in the maintenance process. They use it by connecting it to the SVP by the remote desktop function, via internal LAN which is the network in the storage device.

- Storage Navigator

  Storage Navigator is the software used by the storage administrator of the customer for administrating the device control information of the storage device.

### 1.2.4 TOE-Related People

TOE assumes the users with the following roles.

- Storage Administrator

  Administrates the storage device using Storage Navigator on the administration PC. Allowed to operate the setting of Data Retention Utility which is a TOE function.

- Maintenance Staff

  Staff of the special organization for maintenance, with whom the customer who uses the storage device has signed a contract concerning maintenance. Manages the initial startup process in installing the storage device, changing the settings required in maintenance operations such as replacement or addition of parts or disaster recovery. Maintenance staff access SVP from the maintenance staff PC, and executes maintenance operations. Only maintenance staff can directly contact the equipments inside the storage device and manipulate the equipments connected to internal LAN.

- Storage Users

  Storage device users who use the data saved in the storage device through the host connected to the storage device.

### 1.2.5 TOE Functionality

TOE has the following functions.

- Access mediation to an LDEV

  When an access request comes from the host to the port on CHA, TOE controls the data transmission between the port and the related LDEVs. As a result, access becomes possible from the host to the LDEV associated with the port on CHA.

- Associating the Port with LDEVs

  According to the requests from Storage Navigator/SVP, TOE associates the port with LDEVs.

- Managing LDEVs

  According to the requests from Storage Navigator/SVP, TOE creates and updates LDEVs (i.e. deleting, formatting and shredding).

- Copy Function

  According to the requests from Storage Navigator/SVP, TOE executes copying among LDEVs.

## 1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as “IT Security Evaluation and Certification Scheme”[2], “IT Security Certification Procedure”[3] and “Evaluation Facility Approval Procedure”[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined “SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 User Data Protection Function Security Target” as the basis design of security functions for the TOE (hereinafter referred to as “the ST”)[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex C of CC Part 1 (either of [5], [8], [11] or [14]) and Functional Requirements of CC Part 2 (either of [6], [9], [12] or [15]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10], [13] or [16]) as its rationale. Such evaluation procedure and its result are presented in "SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 CHA/DKA Program Version 50-04-34-00/00 (for Japan), TagmaStore Universal Storage Platform / TagmaStore Network Storage Controller CHA/DKA Program Version 50-04-34-00/00 (International) Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [22]. Further, evaluation methodology should comply with the CEM (either of [17], [18] or [19]). In addition, the each part of CC and CEM shall include contents of interpretations （either of [20] or [21]）.

### 1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated June 2007 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

### 1.5 Overview of Report

#### 1.5.1 PP Conformance

There is no PP to be conformed.

#### 1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL2 conformance.

#### 1.5.3 SOF

This ST claims "SOF-basic" as its minimum strength of function.
Being SOF-basic is sufficient as this TOE assumes the attack capability of the threatening agent to be "low."

#### 1.5.4 Security Functions

The security functions of this TOE are as follows:

- Data Retention Utility Function

The Data Retention Utility function controls the access from the host to the LDEV based on the access attribute "write allowed" or "write denied," set to the LDEV in the storage device, and prevents the LDEV with its attributes set to "write denied" from being altered due to the storage user's erroneous operation or unauthorized access.

As for Data Retention Utility, if the attribute of “write denied” is set to the LDEV, the validity period of that attribute is to be set at the same time. TOE prohibits changing the attribute from “write denied” to “write allowed” during the validity period, no matter what request is made by anything that is not TOE. Changing the access attribute to “write allowed” is accepted when the validity period of the access attribute has expired. In addition, for changing the validity period that has already been set, the period can be extended but cannot be shortened. This is out of consideration for the significance of the user data which is treated by the storage device.

Setting the access attribute and the validity period can be executed on Storage Navigator/SVP.

### 1.5.5 Threat

The property to be protected by this TOE is, out of the user data stored in the storage device, the user data that is defined not to be changed by the storage administrator (or by maintenance staff). The threats that could arise against such user data are described below. Note that “a third person” in the following description indicates the person that is not a storage administrator, a storage user or a maintenance staff, and is not authorized to use the storage device.
In addition, the attack capability of the attacker is assumed to be “low.”

This TOE assumes such threats presented in Table 1-1 and provides functions for countermeasure to them.

Table 1-1 Assumed Threats

| Identifier | Threat |
|---|---|
| T. Delete/Change_User_Data | A storage user or a third person might make a request for write from the host or the device connected to the SAN to the LDEV where the user data is stored which is prohibited to be changed, and the user data might be changed or deleted. |

### 1.5.6 Organisational Security Policy

The security policy of the organizations asks Data Retention Utility for the following functions. The requirements described below are the conditions which Data Retention Utility is asked to implement, and they are not prepared for any attacks of the property to be protected.

Table 1-2 Organisational Security Policy

| Identifier | Organisational Security Policy |
|---|---|
| P.Protect_DRU | TOE must prohibit the change of the attribute from “write denied” to “write allowed,” during the validity period which is set to the LDEV where the user data that must not be changed is stored. |

| Identifier | Organisational Security Policy |
|---|---|
| P.Retention_Period | TOE must prohibit the validity period which is set to the access attribute “write denied.” from being shortened. |

### 1.5.7 Configuration Requirements

TOE is included in any one of the following storage products.

- SANRISE Universal Storage Platform (for Japan)
- TagmaStore Universal Storage Platform (International)
- SANRISE Network Storage Controller (for Japan)
- TagmaStore Network Storage Controller (International)
- SANRISE H12000 (for Japan)
- SANRISE H10000 (for Japan)

### 1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-3.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-3 Assumptions in Use of the TOE

| Identifier | Assumptions |
|---|---|
| A.PhysicalProtection-Storage | A storage device is assumed to be set at a secure area where only storage administrators and maintenance staff are allowed to enter and exit, and the device is assumed to be completely protected from any unauthorized physical access. |
| A.Protection-Network | In the customer’s network environment including the storage device (external LAN), the storage device is assumed to be administrated so that it cannot be connected from any other product than the administration PC that is used by the storage administrator for administration and operation of the storage device. |
| A.Protection-PC | The administration PC is assumed to be managed so that the PC can only be used by the storage administrator. |
| A.Responsibility-Admin | The storage administrator must be the person who is trusted to have the sufficient ability to administrate and operate the storage device, to execute the operations exactly as specified by the manual, and never to commit any inappropriate behavior. |

| Identifier | Assumptions |
|---|---|
| A.Responsibility-Maintenance | A maintenance staff is assumed to be trusted to have the sufficient skills to safely execute the general maintenance operations of the storage device, including the connecting operations between the host and the port on CHA, to execute the proper operations as specified by the manual, and never to commit any inappropriate behavior. |
| A.Connect-Storage | When another storage device is connected to TOE for remote copy of user data, it is assumed that the storage device where copying operations are executed according to the access attribute of the LDEVs in TOE. |

### 1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISEH12000 / SANRISE H10000 ISO15408 Authentication Acquisition Function Manual

# 2. Conduct and Results of Evaluation by Evaluation Facility

## 2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

## 2.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on October 2005 and concluded by completion the Evaluation Technical Report dated June 2007. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on October 2006 and examined procedural status conducted in relation to each work unit for configuration management and delivery and operation by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on March 2007.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

## 2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

### 2.3.1 Developer Testing

1) Developer Test Environment

The configuration of the test executed by the developer is described below.

- TOE
  - CHA/DKA Program: Version 50-04-34-00/00
- Hardware

- Storage Device
  Device： SANRISE Universal Storage Platform(H-65A3-5/A-65A3-5)

- Host
  Server： HP-9000（PA-8000 875MHz)
  OS： HP-UX 11.23

- Administration PC
  PC： NEC Mate MJ28V/L-H(Pentium4 2.4GHz)
  OS： Windows XP Professional SP2

- Hub: Accton ES3016A

● Software

- Administration PC
  Storage Navigator(SVP Version 50-04-34-00/00)

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow.

a. Test configuration

The configuration of the test executed by the developer has been described above. The developer test was executed in the same TOE test environment as the TOE environment identified in ST.

b. Testing Approach

For the testing, following approach was used.

1. Choose from the menu which function to let the TOE execute, by using Storage Navigator installed in the administration PC, and check if the TOE for evaluation operates exactly as designed.
2. Use the test tool on the host to send the Read/Write command to the TOE, check if the TOE security functions work exactly as designed, according to the security attribute that has been set by Storage Navigator.
3. Execute the remote copy test in the configuration where a single storage device can act both as the copy source and as the copy target.
4. Compare the expected test results with the actual results by dumping the log of input/output information to/from TOE that is recorded on the administration PC or the host to examine the behavior.

c. Scope of Testing Performed

Testing is performed 48 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface.

d. Result

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

### 2.3.2 Evaluator Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

The configuration of the test executed by the evaluator is the same as that of the developer test. Evaluator testing was performed at the same TOE testing environment with the TOE configuration identified in ST.

b. Testing Approach

The same approach was used as that of the developer test.

c. Scope of Testing Performed

Total of 16 items of testing; namely 4 items from testing devised by the evaluator and 12 items from testing from sampling of developer testing was conducted. As for selection of the test subset, the following factors are considered.

1. Execute the test items from among the ones originally invented by the evaluator based on the description of the function specification, which are effective to enhance the developer test.
2. Execute the test that better covers the parameters of the test items executed in the developer test.
3. Execute the test that enhances the developer test, by using multiple interfaces in combination.
4. Execute the sampling so that each TSFI may be tested at least once.

d. Result

All evaluator testing conducted is completes correctly and could confirm the behaviour of the TOE. The evaluator also confirmed that all the test results are consistent with the behaviour.

### 2.4 Evaluation Result

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

## 3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator’s evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in certification process were prepared as certification review, which were sent to evaluation facility.

The Certification Body confirmed such concerns pointed out in Observation Report and certification review were solved in the ST and the Evaluation Technical Report.

# 4. Conclusion

## 4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL2 assurance requirements prescribed in CC Part 3.

## 4.2 Recommendations

None

## 5. Glossary

The abbreviations 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 |
| SOF: | Strength of Function |
| ST: | Security Target |
| TOE: | Target of Evaluation |
| TSF: | TOE Security Functions |
| LDEV: | Short for Logical Device. A unit of volumes created in the user area in the storage. Also called Logical Volume. |
| SAN: | Short for Storage Area Network. The network for the storage only, connecting the storage device to the host computer via Fibre Channel. Fibre Channel enables high-speed and highly reliable data communication. |

## 6. Bibliography

[1] SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 User Data Protection Function Security Target, Version 3.7 (June 14, 2007) Hitachi Ltd.

[2] IT Security Evaluation and Certification Scheme, July 2005, Information-technology Promotion Agency, Japan EC-01

[3] IT Security Certification Procedure, July 2005, Information-technology Promotion Agency, Japan EC-03

[4] Evaluation Facility Approval Procedure, July 2005, Information-technology Promotion Agency, Japan EC-05

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-00-031

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031 (Translation Version 1.2 January 2001)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032 (Translation Version 1.2 January 2001)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033 (Translation Version 1.2 January 2001)

[11] ISO/IEC15408-1: 1999 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model JIS

[12] ISO/IEC 15408-2: 1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:1999 - Information technology - Security techniques – Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] JIS X 5070-1: 2000 - Security techniques - Evaluation criteria for IT security - Part 1: General Rules and general model

[15] JIS X 5070-2: 2000 - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[16] JIS X 5070-3: 2000 - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999

[18] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999 (Translation Version 1.0 February 2001)

[19] JIS TR X 0049: 2001 – Common Methodology for Information Technology Security Evaluation

[20] CCIMB Interpretations (as of 01 December 2003)

[21] CCIMB Interpretations (as of 01 December 2003) (Translation Version 1.0 August 2004)

[22] SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 CHA/DKA Program Version 50-04-34-00/00 (for Japan), TagmaStore Universal Storage Platform / TagmaStore Network Storage Controller CHA/DKA Program Version 50-04-34-00/00 (International) Evaluation Technical Report Version 1.4, June 14, 2007, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center