Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2008-03-28 (ITC-8223)
Certification No.	C0199
Sponsor	Hitachi, Ltd.
Name of TOE	Hitachi Storage Command Suite Common Component
Version of TOE	6.0.0-01
PP Conformance	None
Conformed Claim	EAL2 Augmented with ALC_FLR.1
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.
2008-12-24

Hideji Suzuki, 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 2.3 (ISO/IEC 15408:2005)
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

Evaluation Result: Pass

"Hitachi Storage Command Suite Common Component Version 6.0.0-01" 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 "Hitachi Storage Command Suite Common Component Version 6.0.0-01" (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:	Hitachi Storage Command Suite Common Component
Version:	6.0.0-01
Developer:	Hitachi, Ltd.

1.2.2 Product Overview

The target of evaluation, Hitachi Storage Command Suite Common Component (abbreviated hereafter to HSCC), runs as the base module that provides the common functions for storage management software that centrally manages multiple storage devices connected in a SAN environment.
The storage management software includes Hitachi Device Manager Software, Hitachi Replication Manager Software, and Hitachi Tiered Storage Manager Software, etc. These products and HSCC are generically referred to as Hitachi Storage Command Suite.
HSCC is bundled with each product package as the base module of Hitachi Storage Command Suite.

The HSCC security functions are as follows:

- Identification and authentication functions (an external authentication function of an external authentication server may also be used.)
- Security information (set for each user and used by the storage management software to determine the behavior of its security function) management function
- Warning banner functions

1.2.3 Scope of TOE and Overview of Operation

1.2.3.1 TOE Physical boundary and configuration

The TOE is the entire software identified by Hitachi Storage Command Suite Common Component version 6.0.0-01.
The TOE is used in an environment as shown in Figure 1-1.

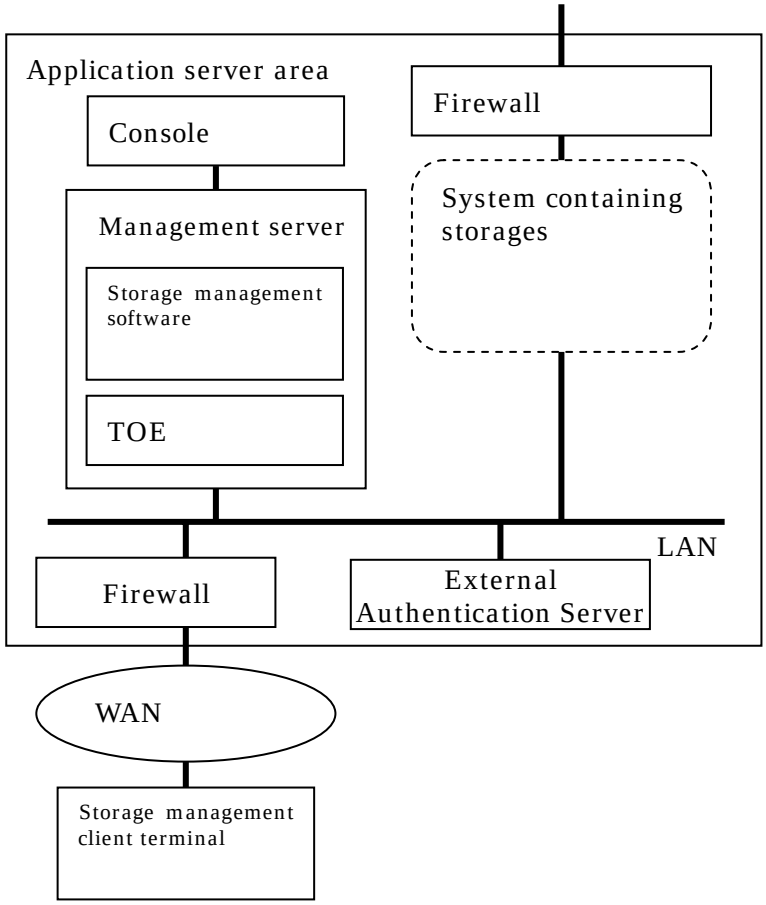

Figure 1-1 Operational environments of the TOE

The management server is one of the following platforms:
- Platform running Java™VM (Version 1.5.0_11) that has been installed by Hitachi Storage Command Suite Common Component for Windows
- Platform running Java™VM (Version 1.5.0_11) that has been installed by Hitachi Storage Command Suite Common Component for Solaris
- Platform running Java™VM (Version1.5.0_05) that has been installed by Hitachi Storage Command Suite Common Component for Linux

An external authentication server is a server with the authentication function based on LDAPv3 or RADIUS. The external authentication server is not indispensable, and when using the authentication function outside TOE instead of the authentication function of TOE, it is needed.

Entry to and exit from the application server area are restricted. In the application server area, management servers, firewalls, and, if required, an external authentication server are installed. In addition, a system that contains storages to be

managed by the storage management software may also be installed.

An application server area may divided into two or more places, and may be set up in a place where external authentication server is different from management server. In this case, confidentiality and integrity have to be preserved in the channel between both servers.

All networks within the application server area are protected from the outside by firewalls that are provided at every point of contact with the outside of the application server area. In this document, those networks that exist within the firewalls are referred to as internal networks and those networks that exist outside the firewalls are referred to as external networks.

The storage administrator and the account administrator use the client terminal for storage management to access the TOE from an external network to issue requests to the storage management software for the performance of operations. When the administrators log on, warning banners are displayed to draw attention to any illegal use. In addition, users are instructed to use passwords that are difficult to guess.

1.2.3.2 Summary of the TOE operation

The TOE is used by the storage management software as described below. If the storage management software is designed to use the TOE in the following way, it can leave functions for identification and authentication, permission information management, and warning banner display to the TOE without having to provide these functions by itself.

- When the storage management software requests the TOE for warning banner information, the TOE returns warning banner information. The storage management software displays the warning banner information when asking a user for identification and authentication information.

- Upon reception of the user's identification and authentication information, the storage management software supplies the information to the TOE. The TOE verifies the identification and authentication information, or requests verification of the information to an external authentication server and, if it is appropriate, a session is established between the user and TOE. When a session is established, the TOE returns the user's permission information and the storage management software receives the information.

- When a user attempts to perform any operation on the storage, the storage management software queries the TOE about whether the session between the user and the TOE is still established. When the storage management software judges based on the answer from the TOE that the session is still established, it then judges whether to allow the user to access the storage based on the user's permission information.

1.2.3.3 TOE-related personnel

The TOE assumes the following types of users. Users perform operations within a predefined scope of permissions.

- System builder (server / network administrator)
  Role: Maintains and manages the system by, for example, backing up server data.
  Permissions: Allowed to determine and set parameters required for building and

running the system. Accordingly, the system builder can update (change and delete) the permissions of users, which are user data. The system builder's permissions are not changed by any other person.
Level of trust: Has responsibility for the system and is trusted.

- Account administrator
  Role: Manages the accounts of users who use the system and specify settings for the system.
  Permissions: Allowed to manage accounts based on the source information for an account. The source information for an account includes determining whether an account should be created and which permissions should be granted to the account, and is derived from organizational information such as the organizational hierarchy. Accordingly, the account administrator can update (change and delete) the permissions of users, which are user data.
  Level of trust: Has responsibility for own work and is trusted within the scope of that work.

- Storage administrator
  Role: Manages storages by, for example, managing the resources in the storages.
  Permissions: Allowed to allocate resources in the storages installed by the system builder. Accordingly, the storage administrator can access the permissions of users, which are user data, to determine the permissions granted to the storage administrator
  Level of trust: Has responsibility for own work and is trusted within the scope of that work.

1.2.4 TOE Functionality

The TOE provides the following security functions in order to furnish the storage management software with identification and authentication, permission information management, and warning banner functions.

- Warning banner function
  When the TOE receives a request for warning banner information from the storage management software running on the management server, it returns warning banner information.

- Identification and authentication
  When the TOE receives user identification and authentication information from the storage management software running on the management server, it verifies the information, or requests verification of the information to an external authentication server (it can be specified for every account whether TOE verifies the information or an external authentication server verifies the information). If the information is correct, the TOE enters a session management phase appropriate to the request (determined depending on whether it was issued for user login or for security information management function execution).
  If the TOE fails to authenticate a storage administrator or account administrator after a certain number of successive retries, it automatically locks the account of the storage or account administrator indefinitely.

- Session management (for user login)
  If identification and authentication are successful, the TOE establishes a session

between the user and the TOE and returns a session-specific token and the user's permission information.
The TOE maintains the session as established until it receives a session disconnection request from the user.
When the TOE receives a token and a query about whether the session for the token is still established from the storage management software running on the management server, it answers whether the session is established at present. If the session is established, the TOE can return the identification and permission information of the storage administrator for the session when so requested from the storage management software.

- Session management (for execution of the security information management function)
  If identification and authentication are successful, the TOE establishes a session between the user and the TOE and maintains this status while the security information management function is being executed.

- Security information management functions
  The TOE provides the following functions as its security information management functions:

  > Account management
  Upon a request from the user, the TOE provides the user with a means that can be used:
  - to register or delete a user ID (account);
  - to register, modify, or delete a password (if a password is deleted, the corresponding account is also deleted as a whole);
  - to query or change the lock status, and ;
  - to select an internal server (TOE verifies authentication information) or an external server (verification of authentication information is requested to an external authentication server.).

  The TOE grants account administrators and system builders the authority to perform all of the above tasks, whereas it grants the storage administrators only the authority to change their own password.

  However, the following restriction exists for the account that is assigned the role of system builder:
  - to newly register or delete an account are not permitted, and ;
  - to select the external authentication server (i.e. the TOE verifies the authentication information.).

  The TOE will not accept any password if it does not satisfy the quality requirement determined by the security parameters described later.

  > Role and permission information management
  The TOE maintains role and permission information for each user ID. When a user ID is created, its role and permission information is not set yet. The TOE only allows account administrators and system builders to generate, delete, or modify the role and permission information of users other than system builders. The TOE does not allow account administrators to delete or modify their own role and permission information.

  > Warning banner information management
  The TOE only allows account administrators and system builders to generate, delete, or modify warning banner information.

> Security parameter management
The TOE maintains the security parameters indicated below and only allows account administrators and system builders to query, modify, or delete these parameter values:

#	Parameter	Description
1	Threshold value for the number of consecutive authentication attempt failures	Threshold value used by the automatic account lock function as the trigger for automatically locking accounts when repeated authentication attempts fail
2	Minimum number of characters in a password	Minimum number of characters in a password
3	Password complexity condition	Condition specifying that the specified number of the specified types of characters must be included in a password

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 "Hitachi Storage Command Suite Common Component Security Target Version 2.03" (hereinafter referred to as "the ST")[1] as the basis design of security functions for the TOE, 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 B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) 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] or [13]) as its rationale. Such evaluation procedure and its result are presented in "Hitachi Storage Command Suite Common Component Version 6.0.0-01 Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

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 2008-12 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 Augmented.
The augmented assurance component is ALC_FLR.1.

1.5.3 SOF

The ST asserts that the minimum strength of function is "SOF-basic."

The threats assumed by this TOE are low-level agents without advanced expertise that use the interface of the clients that are operated by administrators. Therefore, SOF-basic is appropriate as the minimum strength of the function level.

1.5.4 Security Functions

Security functions of the TOE are shown in "1.2.4 TOE Functionality".

1.5.5 Threat

This TOE assumes the following as threat agents:

- Illegal user (user who is not authorized to use the TOE and all of the storage management software)
- Storage administrator (person who is authorized to use the TOE and one of the storage management software programs)

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.ILLEGAL_ACCESS (illegal connection)	From a management client, an illegal user might delete, change, or expose the permissions managed by the TOE for the storage management software functions, or delete or change banner information.
T.UNAUTHORISED_ ACCESS (unauthorized access)	From a management client, an authenticated storage administrator or account administrator might perform an unauthorized operation that deletes, changes, or exposes the permissions managed by the TOE, or might delete or change banner information.

1.5.6 Organisational Security Policy

Table 1-2 indicates the organisational security policies required to use the TOE.

Table 1-2 Organisational Security Policy

Identifier	Organisational Security Policy
P.BANNER (warning banners)	Storage management software must have functions that display advisory warning messages related to its illegal use of the software.

1.5.7 Configuration Requirements

The TOE runs on one of the following platforms:

- Platform running Java™VM (Version 1.5.0_11) that has been installed by Hitachi Storage Command Suite Common Component for Windows
- Platform running Java™VM (Version 1.5.0_11) that has been installed by Hitachi Storage Command Suite Common Component for Solaris
- Platform running Java™VM (Version 1.5.0_05) that has been installed by Hitachi Storage Command Suite Common Component for Linux

When external authentication server is used, it is required that the server should have an authentication function based on LDAPv3 or RADIUS.

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.PHYSICAL (management of hardware)	The management server on which the TOE and storage management software run, peripheral devices, storage devices, the internal network, and firewall at the boundary of the internal network are installed in the physically isolated business server area. Only authorized administrators are permitted to enter this area.
A.NETWORKS (networks)	The internal network containing the management network connected to the management server is installed in the business server area and performs only the communication that is necessary. A firewall that monitors traffic logically separates the internal network from external networks and detects traffic that is inappropriate.
A.ADMINISTRATORS (administrators)	The system builder is trusted. Account administrators, storage administrators, and administrators of other servers, including application servers, do not perform malicious acts with regard to one another's work. Work includes the management of accounts and permissions of storage management software users, the management of storages, and the management of other servers.
A.SECURE_CHANNEL (communication secrecy)	The network between the management server on which the TOE and storage management software run, and the management clients is secure with regard to secrecy and completeness of communication.
A.TOKEN (available tokens)	The TOE does not create an environment containing products with either tokens that are generated outside the TOE or tokens of insufficient strength.
A.PASSWORD (complex passwords)	Authentication methods have sufficient strength so that illegal users cannot log on to the system by guessing passwords.
A.CLIENTS (Management of storage management client)	Malicious software does not exist in the storage management client. (Supplementary explanation) "Malicious software" means software that may attack the assets or may allow thread agent to attack the assets.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- Hitachi Storage Command Suite Common Component Security Guide
  - Description and Operation Edition 1
- Hitachi Device Manager Software Web Client User's Guide
  - Description and Operation - 3020-3-P11 Edition 1
- Hitachi Device Manager and Provisioning Manager Software System Configuration Guide 3020-3-P13 Edition 1

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 2008-04 and concluded by completion the Evaluation Technical Report dated 2008-12. 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. During an evaluation of another TOE, assurance level of which is same as the TOE, the evaluation facility directly visited the development and manufacturing sites on 2007-02 and examined procedural status conducted in relation to each work unit for delivery and operation by investigating records and staff hearing. The evaluation facility determined that the result of the examination on 2007-02 is also applicable to evaluation of the TOE, by examining difference of procedure from the other TOE to the TOE, and by interview to the developer about procedural status. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2008-08.

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

Developer tests were conducted in the environments each of which ran one of the OSs listed in Table 2-1.

Table 2-1 Configuration of Developer Testing

TOE	Version and others
Hitachi Storage Command Suite Common Component	6.0.0-01
Hitachi Storage Command Suite products (storage management software product)	Version and others
Hitachi Storage Command Suite Device Manager (for Windows)	6.0.0-02
Hitachi Storage Command Suite Replication Manager (for Windows)	6.0.0-00
Hitachi Storage Command Suite Device Manager (for Linux)	6.0.0-02
Hitachi Storage Command Suite Device Manager (for Solaris)	6.0.0-02
Java(TM) VM installed with the Hitachi Storage Command Suite product	Version and others
For Windows: Java(TM) 2	1.5.0_11
For Solaris: Java(TM) 2	1.5.0_11
For Linux: Java(TM) 2	1.5.0_05
OS	Remarks
Windows Server 2003 Enterprise Edition SP2	Management server
Solaris 10	Management server
Red Hat Enterprise Linux Advanced Edition 4 update 5	Management server
Windows XP SP2	Client terminal
Windows Server 2003 Enterprise Edition SP2	External authentication server
Software for external authentication	Remarks
Active Directory (Program on Windows Server 2003)	LDAP Version 3, PAP and CHAP

2) Outlining of Developer Testing

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

a. Test configuration

The developer tests were conducted in a TOE test environment that included the same TOE components as identified in the ST.

b. Test methods

The tests were conducted using the following methods:
1. Operation from the browser window and verification of the screen display
2. Operation from the console window and verification of the screen display

c. Coverage of the tests conducted

The developer tested 193 test items in each OS environment. A coverage analysis was conducted and revealed that all the security functions and external interfaces stated in the function specification were sufficiently tested.

d. Result

It was verified that the actual results of the developer-conducted tests matched the expected results. The evaluator validated the methods and items of the developer tests and verified that the test methods and results matched those indicated in the test plan.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

Evaluator tests were conducted in the environments each of which ran one of the OSs listed in Table 2-2.

Table 2-2 Evaluator-conducted test configuration

TOE	Version and others
Hitachi Storage Command Suite Common Component	6.0.0-01
Hitachi Storage Command Suite product (storage management software product)	Version and others
Hitachi Storage Command Suite Device Manager (for Windows)	6.0.0-02
Hitachi Storage Command Suite Provisioning Manager (for Windows)	6.0.0-00
Hitachi Storage Command Suite Device Manager (for Linux)	6.0.0-01
Hitachi Storage Command Suite Device Manager (for Solaris)	6.0.0-01
Java(TM) VM installed with the Hitachi Storage Command Suite product	Version and others
For Windows: Java(TM) 2	1.5.0_11
For Solaris: Java(TM) 2	1.5.0_11
For Linux: Java(TM) 2	1.5.0_05
OS	Remarks
Windows Server 2003 Enterprise Edition x64 Edition SP2	Management server
Solaris 10	Management server
Red Hat Enterprise Linux Advanced Edition 4.5 x86	Management server
Windows XP Professional SP2	Client terminal
Windows Server 2003 Enterprise Edition x64 Edition SP2	External authentication server
Software for external authentication	Remarks
Active Directory (Program on Windows Server 2003)	LDAP Version 3, PAP and CHAP
Browser	Remarks
Microsoft Internet Explorer 6 SP2	Client terminal

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

The evaluator tests were conducted in a TOE test environment that included the same TOE components as identified in the ST.

b. Test methods

The tests were conducted using the following methods:
1. Operation from the browser window and verification of the screen display
2. Operation from the console window and verification of the screen display

c. Coverage of the tests conducted

The evaluator tested 21 test items designed by the evaluator itself and 30 test items sampled from the developer-conducted tests (51 test items in total) in each OS environment. The test items were chosen considering the following:

1. All the security functions should be covered.
2. Whether any parameter range (limit value) is left untested in any interface to each security function.
3. Whether a change to a security parameter used by the security information management function will take effect immediately.

d. Result

All the evaluator-conducted tests were completed properly and the TOE behaviors were verified. The evaluator verified that all the test results matched the expected behaviors.

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 and ALC_FLR.1 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
SAN:	Storage Area Network
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

The glossaries used in this report are listed below.

Token:	Identifier used by HSCC for managing sessions.
Warning banner:	Warning text to be displayed before users use the storage management software. A warning banner is mainly used to call attention to illegal use.

6. Bibliography

[1] Hitachi Storage Command Suite Common Component Security Target Version 2.03 (December 4, 2008) Hitachi, Ltd.

[2] IT Security Evaluation and Certification Scheme, September 2006, Information-technology Promotion Agency, Japan EC-01

[3] IT Security Certification Procedure, September 2006, Information-technology Promotion Agency, Japan EC-03

[4] Evaluation Facility Approval Procedure, September 2006, Information-technology Promotion Agency, Japan EC-05

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)

[11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] Hitachi Storage Command Suite Common Component Version 6.0.0-01 Evaluation Technical Report Version 3.0, December 11, 2008, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center