Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2015-12-04 (ITC-5576)
Certification No.	C0536
Sponsor	Hitachi, Ltd.
TOE Name	Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software
TOE Version	8.0.1-02
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.
2017-02-13

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 Device Manager Software, Hitachi Tiered Storage Manager Software" 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 Device Manager Software, Hitachi Tiered Storage Manager Software Version 8.0.1-02" (hereinafter referred to as the "TOE") developed by Hitachi, Ltd., and the evaluation of the TOE was finished on 2017-01 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 "TOE users (Storage administrators, Account administrators and System integrators)" 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

The TOE consists of Hitachi Device Manager Software and Hitachi Tiered Storage Manager Software.

The TOE has a management function to input or modify the information that represents the configuration of the storage system resources (hereinafter referred to as the "storage resource information").

The TOE provides the following as security functions: display of warning banner against illegal use; identification and authentication for users; access control function for the storage resource information and the warning banner message information (hereinafter referred to as the "banner information").

For these security functions, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance package. The following section describes the threats and assumptions that the TOE assumes.

1.1.2.1 Threats and Security Objectives

This TOE counters the various threats by using the security functions as follows.

It is assumed to be a threat that an illegal user or an authorized storage administrator or account administrator might delete, modify, or disclose the storage resource information, which are assets to be protected, or might delete, modify the banner information, by performing unauthorized operation from a storage management client.

To counter the threat, the TOE identifies and authenticates users when the users access the TOE from storage management clients. The TOE controls access to the storage resource information or banner information so that only authorized users who have the appropriate permissions can use the permitted operations.

1.1.2.2 Configuration and Assumptions

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

The TOE is installed on the management server, and it must be located with peripheral devices in a physically isolated business server area. Only the trusted administrators of the hardware and software, who will not perform malicious acts, are permitted to enter this area.

The TOE is used from the storage management client, which is located outside the business server area. The communication to the internal network from the external networks outside the business server area connected to the TOE is assumed to be the managed network environment, which is restricted only to the TOE communications from the storage management client.

If the external authentication server and authorization server are used in place of the TOE identification and authentication function, the servers shall be installed in the same business server area as the storage management software server. If the servers are installed in a different business server area, it is assumed that confidentiality and integrity are maintained between the servers. Note that if confidentiality and integrity cannot be maintained in the communication paths between the servers.

1.1.3 Disclaimers

- This evaluation does not assure the TOE behavior outside the specified operational environment. For details on the operational environment, see “4.2 Environmental Assumptions.”

- In the information publicly disclosed by the developer, the TOE is presented as a product for managing resources of an actual storage system. However, this evaluation does not assure the configuration in which the resources of the actual storage system are managed.

  In this evaluation, the configuration in which the TOE manages the “storage resource information” (which is data in the management server, and is not data in the actual storage system) is assured.

- This TOE assumes to counter attacks only from a storage management client to the TOE. It is not assured for the TOE to counter other attack measures in this evaluation, and the assumption is that the operational environment will prevent other attacks.

- This evaluation is not intended to evaluate the identification and authentication function of an external authentication server or external authorization server, if the external authentication function or external authentication group linkage function is used. It is assumed that the operational environment will prevent spoofing attacks on the external authentication and authorization server.

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 2017-01, based on functional requirements and assurance requirements of the TOE according to the publicised 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] and the Observation Reports prepared by the Evaluation Facility as well as 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 Device Manager Software, Hitachi Tiered Storage Manager Software
TOE Version:	8.0.1-02
Developer:	Hitachi, Ltd.

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

By performing the version confirmation procedure described in the guidance documentation, users can confirm the right version of each product, Hitachi Device Manager Software and Hitachi Tiered Storage Manager Software.

3. Security Policy

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

The purpose of using the TOE is to manage the input or modification of the storage resource information.

To handle market requests, the TOE has a function to display a warning banner regarding illegal use.

To prevent illegal operations to the storage resource information or banner information, the TOE has the identification and authentication function and access control function.

By controlling access to the storage resource information, the TOE can control the scope of the storage resource information (components of the storage resource information, such as host groups and logical storage) that each user can access, and can control the type of operation (viewing, modifying, creating, etc.) that a user is permitted to perform on that information.

The TOE assumes that TOE users have the following roles.

System integrator

- A system integrator determines and sets parameters required for building and operating the system for the TOE to run. It is assumed that this work includes not only operations from a storage management client but also works in the business server area.

Account administrator

- An account administrator manages TOE accounts (registers or deletes accounts, and edits permissions). It is assumed that the account administrator performs operations from a storage management client.

Storage administrator

- A storage administrator inputs and modifies the storage resource information. It is assumed that the storage administrator performs operations from a storage management client.

The following role is assumed as a role related to the operational environment, while the use of the TOE is not assumed.

External authentication server administrator

- An external authentication server administrator operates and manages the external authentication server and authorization server, and sets up the authorization and authentication information. It is assumed that this work is performed in the business server area.

3.1 Security Function Policies

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

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the security functions to counter them.

Table 3-1 Assumed Threats

Identifier	Threat
T.ILLEGAL_ACCESS (illegal connection)	If an illegal user who does not have an account in the TOE accesses the TOE from a storage management client, this user might delete, modify, or reveal storage resource information, or delete or modify banner information. In addition, a user who has an account in the TOE might be misrecognized as having permissions that the user does not really have, and might delete or modify the storage resource information or banner information, which the TOE manages, from a storage management client. (Supplementary information) This threat indicates non-permitted operations carried out by spoofing attacks.
T.UNAUTHORISED_ACCESS (unauthorized access)	An authenticated storage administrator or account administrator might delete or modify the storage resource information or banner information, which the TOE manages, by performing an unauthorized operation from a storage management client.

3.1.1.2 Security Function Policies against Threats

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

(1) Countermeasure against threat “T.ILLEGAL_ACCESS”

When the user of a storage management client terminal accesses the TOE and storage management software, the TOE identifies and authenticates those users for whom internal authentication is specified, and the external authentication server identifies and authenticates those users for whom external authentication is specified, in order to confirm whether the users are authorized users.

The TOE and the external authentication server limit the patterns of passwords that can be registered so that difficult-to-guess passwords must be set. The users set

passwords that are difficult to guess from the combination of the password length and types of characters used, and change these passwords at appropriate intervals, so that they do not reveal their passwords. This process ensures secure password management. In addition, the TOE automatically locks the account of a user for whom an authentication attempt fails the defined number of times, to counter brute-force password attacks.

(2) Countermeasure against threat "T.UNAUTHORISED_ACCESS"

The TOE controls access to the storage resource information and banner information in accordance with the permissions granted to each TOE user.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE are shown in Table 3-2.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.BANNER (warning banners)	The TOE must have a function that displays advisory warning messages related to illegal use of the TOE.

3.1.2.2 Security Function Policies to Organisational Security Policies

The TOE provides the security functions to satisfy the organisational security policies shown in Table 3-2.

(1) Countermeasure against Organizational Security Policy "P.BANNER"

The TOE has a function to display advisory warning messages related to illegal use of the software.

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.PHYSICAL (hardware management)	The management server on which the TOE runs, peripheral devices, the external authentication server and external authorization server that the TOE uses, the internal network, and the firewall at the boundary of the internal network, must be installed in a physically isolated business server area. Only the administrators of the hardware and software in that area are permitted to enter this area. The administrators must be trusted persons who will not perform malicious acts in that area.
A.NETWORKS (networks)	The internal network, located in the business server area that houses the management network connected to the management server, must be restricted only to communication from storage management client terminals by means of a firewall. (Supplementary information) To ensure this assumption is satisfied, it is necessary to prevent fake storage management client terminals.
A.ADMINISTRATORS (administrators)	The system integrator must be a trusted person. Account administrators, storage administrators, and external authentication server administrators must not, in the course of the work associated with their own permissions, perform malicious acts related to the management of accounts and permissions of TOE users, and the management of storage systems. Other server administrators must not perform malicious acts with regard to their own work. (Supplementary information) The above-mentioned “management of storage systems” means operations of the storage resource information in the management server, and does not mean the management of the actual storage system.

Identifier	Assumptions
A.SECURE_CHANNEL (communication security)	The network between the management server, on which the TOE runs, and storage management clients, must be secured with regard to the confidentiality and integrity of communications. When the TOE and the external authentication server and external authorization server that the TOE uses are located in different business server areas, the network between them must be secured with regard to the confidentiality and integrity of communications.
A.PASSWORD (setting and updating passwords)	Account administrators, system integrators, and external authentication server administrators must determine an appropriate level of password complexity, as well as the number of login attempts to be permitted before an account is to be locked, and they must specify password settings accordingly. Each storage administrator, account administrators, system integrators, and external authentication server administrators must update their passwords appropriately so that passwords are not stolen or revealed via physical actions (for example, writing a password on a sticky note and sticking it on a PC monitor, or allowing over-the-shoulder snooping), or via human causes (for example, failing to update passwords, updating a password by using the same password again, using a password consisting of personal information, using a password that is used in other applications, or leaving password information in the cache).
A.CLIENTS (management of storage management client terminals)	Malicious software must not exist on the storage management client terminals.
A.SRV_MGMT (server management)	For the management servers, the settings for services that run on the server, server settings, and accounts registered on the server must be managed to prevent the storage management clients from bypassing the TOE and directly accessing the internal network. (Supplementary information) It is assumed that remote access by SSH or telnet is prohibited because such access is considered to be an access to the internal network.

4.2 Environmental Assumptions

According to the assumption A.PHYSICAL, the following must be installed in a physically secure business server area: the management server on which the TOE runs, peripheral devices, the external authentication server and external authorization server that the TOE uses, the internal network, and the firewall located at the boundary of the internal network. Figure 4-1 shows the operational environment of the TOE to be assured.

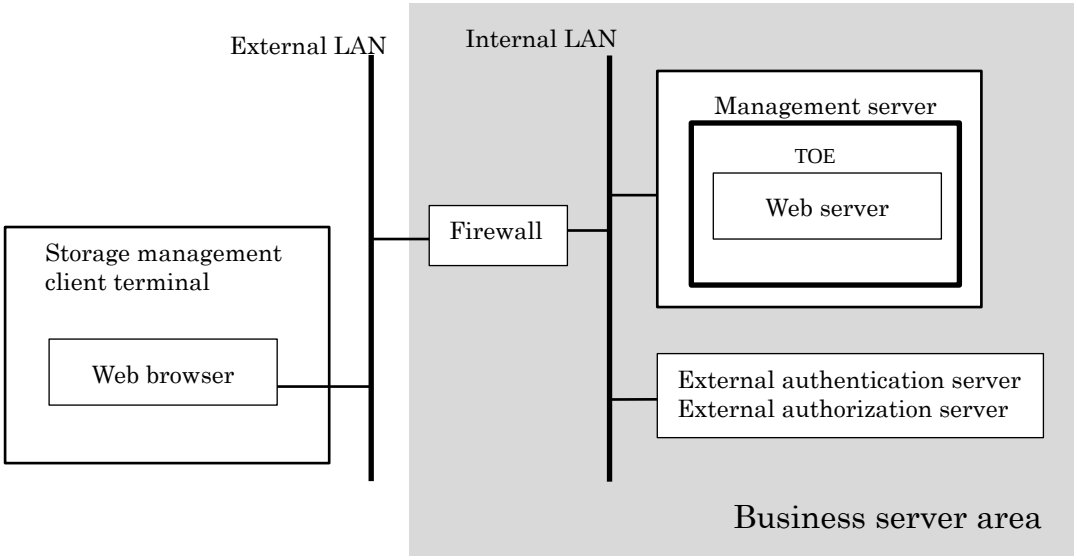

Figure 4-1 Operational Environment of the TOE to be Assured

The operational environment of the TOE to be assured is as follows:

Management server

Server machine with the following software:

- Windows Server 2012 R2 (64bit)
- Java™ SE Development Kit 8, Update 92

Storage management client terminal

PC with the following software:

- Windows 7 SP1
- Internet Explorer 9 (32bit)
- Flash Player 14.0

External authentication server and external authorization server

Server machine with the following software:

(It is necessary when the external authentication server and authorization server is used in place of the TOE identification and authentication function.)

- Windows Server 2012 R2 (64bit)

Firewall

A firewall must be installed so that communications to the internal network from external networks are restricted to communications from storage management client terminals.

However, if another method accomplishes this purpose, that method can also be used (for example, if the storage management client terminal is also connected to the internal network).

It should be noted that the reliability of the hardware and the cooperating software shown in this configuration is out of the scope in the evaluation. Those are assumed to be trustworthy.

4.3 Clarification of Scope

The external authentication server and authorization server is installed in the business server area, and the “external authentication function” and “external authentication group linkage function” can also be used in place of the TOE identification and authentication function. However, the scope of the TOE does not include the identification and authentication function of the external authentication server and authorization server, so it is the responsibility of the operator to operate the system securely in accordance with the security objectives.

The TOE is a server program that runs on a general OS, and therefore depends on OS functions (for example, for managing processes and for separating processes). With this assumption, accesses to the TOE are restricted only to communications from storage management clients. Furthermore, it is assumed that no malicious software is installed on the storage management clients, and that the OS commands are not used for malicious purposes.

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 software that runs on the management server and does not include the OS.

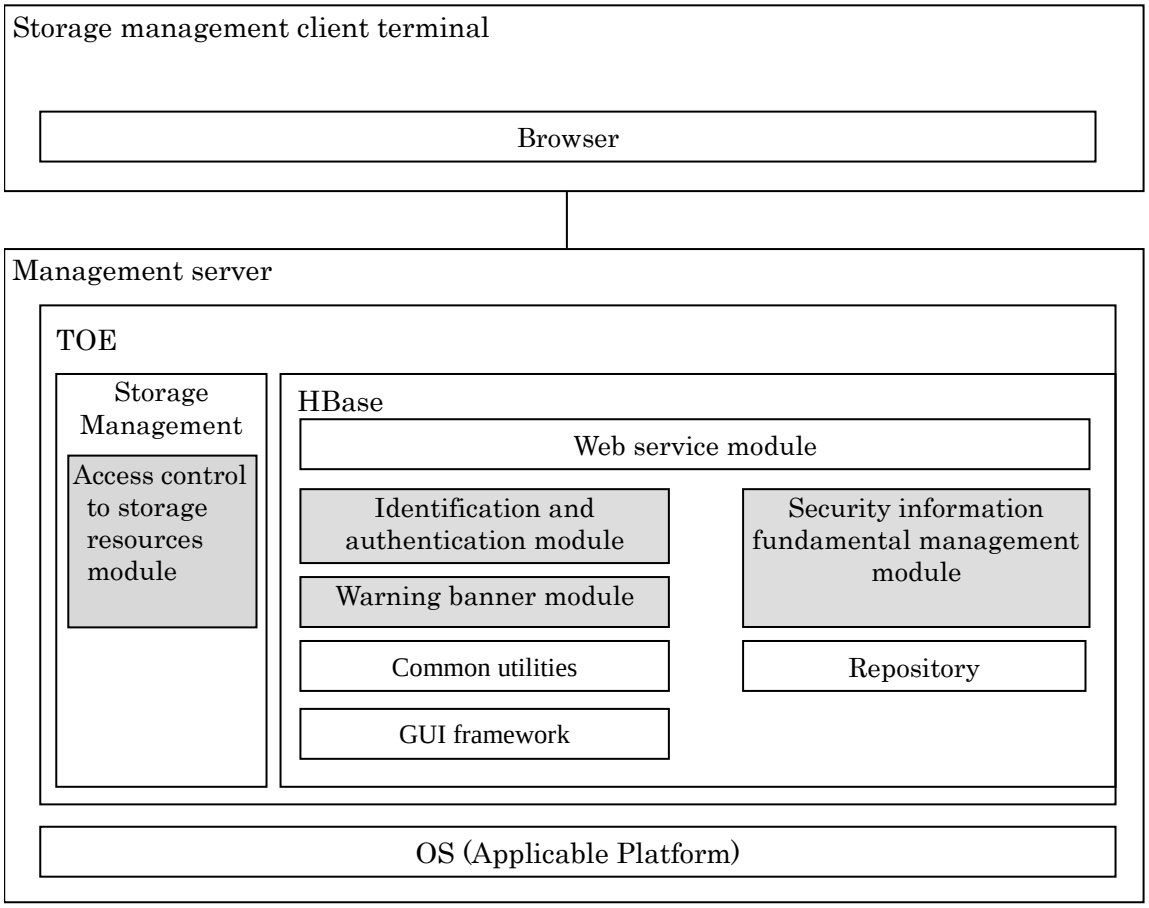

Figure 5.1 TOE boundary

- The identification and authentication module is a module that implements the identification and authentication function of the TOE.
- The security information fundamental management module is a module that implements the security information fundamental management function of the TOE.
- The warning banner module is a module that implements the warning banner function of the TOE.
- The common utilities are a module that implements the common utilities of the TOE.
- The web service module is a module that implements the TOE web services.
- The GUI framework is a module that implements the TOE's graphical user interface (GUI).

- The repository is the database that stores data for the TOE.
- The access control to storage resources module controls access to resources by associating information on the storage resource information with the security information fundamental management module.

5.2 IT Environment

The TOE is installed on a management server whose operating platform is Windows Server 2012 R2 (64bit) (with Java™ SE Development Kit 8, Update 92).

The TOE user operates the TOE via Internet Explorer 9 (32bit) from a storage management client terminal.

Microsoft Active Directory (Windows Server 2012 R2 (64bit) attached) is used on an external authentication server.

For external authentication, the authentication function of an LDAP directory server, a RADIUS server, or a Kerberos server is used.

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.

- Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software Security Guide P-2Z13-3084
- Hitachi Command Suite Installation and Configuration Guide 3021-9-006-10
- Hitachi Command Suite User Guide 3021-9-003-10
- Hitachi Command Suite Administrator Guide 3021-9-008-10
- Hitachi Command Suite Messages Guide 3021-9-011-10

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 joins Mutual Recognition Arrangement of 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 2015-12 and concluded upon completion of the Evaluation Technical Report dated 2017-01. 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. In addition, the evaluator examined the procedural status conducted in relation to the work unit for delivery by observing other products that were actually delivered by following the same procedure as the TOE on 2016-07. 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 2016-07.

Concerns found in evaluation activities for each work unit were all issued as the Observation Reports, and those were reported to the developer. Those concerns were reviewed by the developer, and all the concerns were solved eventually.

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 the evidence shown in the process of the evaluation and those confirmed validity, the evaluator performed the reproducibility testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

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

Figure 7-1 shows the testing configuration performed by the developer.

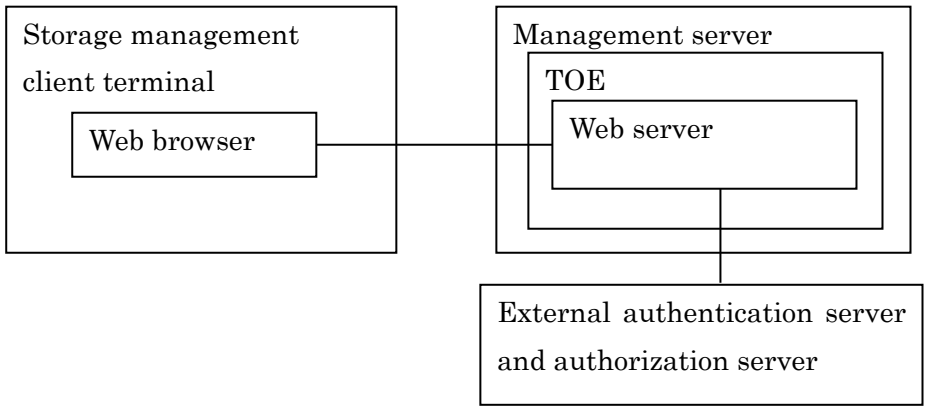

Figure 7-1 Configuration of the Developer Testing

The TOE to be tested by the developer is described as follows, and it is the same as what is written in the ST.

- Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software
  Version: 8.0.1-02

The components in the environment for testing performed by the developer are described as follows. This configuration is the same as what is identified in the ST. The evaluators checked that there was no problem with the confirmation of the TOE functions.

Management server
Server machine with the following software:
- Windows Server 2012 R2 Datacenter x64 (64bit)
- Java™ SE Development Kit 8, Update 92

External authentication server and external authorization server
Server machine with the following software:
- Windows Server 2012 R2 Datacenter x64 (64bit)

Storage management client terminal
PC with the following software:
- Windows 7 Professional SP1 (64bit)
- Internet Explorer 9 (32bit)
- Flash Player 14.0

2) Summary of the Developer Testing

A summary of the developer testing is as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>

The TOE's external interface were stimulated by normal usage of the TOE (by operation from the web browser of a storage management client terminal, by operation from the console of the management server, and by changing the configuration file of the TOE in the management server), and the TOE responses were confirmed. To efficiently input the storage resource information, a storage simulator was used for some tests.

For those TOE behavior which was difficult to confirm by normal usage of the TOE, Fiddler was used to change input to the web server and to confirm the TOE responses.

The TOE responses were observed from the management server console and from the web browser of the storage management client terminal.

<Developer Testing Tools>

Table 7-1 shows tools used in the developer testing.

Table 7-1 Developer Testing Tools

Tool Name	Outline and Purpose of Use
Fiddler	Fiddler version 2.4.2.6 It mediates communications between a web browser and web server, and changes or refers to the communication data between them.
Storage simulator	It provides the storage resource information.

<Content of the Performed Developer Testing>

By normal usage of the TOE, the developer tested the following cases: cases permitted by and prohibited by the security functional requirements, cases for which inappropriate input is given, and cases for which there was a concern that inconsistencies might occur if multiple operations were performed on the same data.

The developer used Fiddler to test the input of parameter values that could not be input by normal usage of a web browser.

b. Scope of the Performed Developer Testing

The developer testing was performed on 65 items by the developer. By the coverage analysis, the coverage of the testing for the external interfaces and security functions described in the functional specifications was confirmed. The coverage of some external interfaces was determined to be insufficient, so the evaluators performed the independent testing 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 environment for the independent testing performed by the evaluators was the same as the environment for the developer testing.

Although the evaluators prepared the components and testing programs used for the developer testing, the evaluators confirmed their specifications and performed their behavior testing as well as calibration.

2) Summary of the Independent Testing

A summary of the independent testing is 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.

Focusing on the following points of view, the evaluators extracted test items from the developer testing specifications.

I. Points of view of the security functions
To test security functions in an unbiased way, samples for each security function (identification and authentication, access control, and warning banner function) were taken.

II. Points of view of the interfaces
Samples were taken from each type of interfaces in order to confirm the behavior

caused by operations from a web browser, by operations from the console of the management server, and by changes to the TOE configuration files on the management server. At the same time, sampling tests were performed so that all the SFRs were covered.

III. Points of view of other testing characteristics
Samples were taken from those tests which have characteristics in test scenarios and methods, such as tests in which multiple operations were performed on the same data, or tests in which the input to a web server is changed using Fiddler.

Based on the following points of view, evaluators devised additional independent testing:

i. Variation of the developer testing: Roles
For a function which can be operated by multiple roles, the evaluators performed tests with different roles (system integrator, account administrator, and storage administrator) from those used in the developer testing.

ii. Variation of the developer testing: Input parameters
For a function which receives inputs from a parameter, the evaluators performed tests with different parameter values from those used in the developer testing.

iii. Variation of the developer testing: Enhanced coverage
For some TOE behavior which the evaluators determined was not confirmed by the developer testing, the evaluators performed additional tests to supplement insufficiency.

The evaluators examined each interface type (operations from a web browser, operations from the console of the management server, and changes to the TOE configuration files on the management server) to decide whether additional testing was necessary.

b. Independent Testing Outline

The evaluators performed sampling tests of the developer testing on 58 items. The samples were selected, in consideration of the above-mentioned points of view in I, II, III of “a) Viewpoints of the Independent Testing.”

The evaluators performed additional independent testing on 11 items. The tests were devised to supplement the developer testing, in consideration of the above-mentioned points of view in i, ii, iii of “a) Viewpoints of the Independent Testing.”

An outline of the independent testing that the evaluator performed is as follows.

<Content of the Performed Independent Testing>

Table 7-2 shows the points of view in the independent testing and the contents of the corresponding testing.

Table 7-2 Content of the Performed Independent Testing

Points of View for the Independent Testing	Testing Outline
(1) Testing the function for adding users Points of view to be considered: i and iii	The evaluators confirm the behavior when an account administrator registers a user. The developer tested the case in which a system integrator registers a user, but did not test the cases when other administrators register users. Therefore, the evaluators confirm the behavior when other administrators with different roles register users.
(2) Testing the function for changing user passwords Points of view to be considered: i and iii	The evaluators confirm the behavior when an account administrator changes his or her own password. The developer tested the case in which a system integrator changes his or her own password, but did not test the cases when other administrators change their own passwords. Therefore, the evaluators confirm the behavior when other administrators with different roles register their own passwords.
(3) Testing the function for changing password complexity setting Point of view to be considered: ii	The evaluators confirm the behavior of the password complexity setting. The developer did not confirm the case in which "0" and negative numbers are included in the password complexity setting. Therefore, the evaluators confirm the behavior related to the rule that includes "0" and negative numbers in the password complexity setting.
(4) Testing the function for changing the warning banner in the web interface Point of view to be considered: ii	The evaluators confirm the behavior of the warning banner setting. The developer tested the behavior in the case when an independent HTML tag was used, but did not confirm the cases when setting tags that consist of letters or character strings that include attributes. Therefore, the evaluators confirm the behavior in the cases when setting tags that consist of letters or character strings that include attributes.

Points of View for the Independent Testing	Testing Outline
(5) Testing the function for changing the warning banner in the command interface Point of view to be considered: iii	The evaluators confirm the behavior of setting the warning banner in the command interface. The developer tested the case in which a new warning banner is set, but did not confirm the behavior after setting it in the web interface. Therefore, the evaluators confirm the behavior of the warning banner when executing a command after setting it in the web interface.
(6) Testing the function for unlocking accounts Point of view to be considered: ii	The evaluators confirm the behavior of unlocking accounts. The developer did not confirm the behavior when passwords longer than the predetermined length are entered. Therefore, the evaluators confirm the behavior when passwords longer than the predetermined length are entered.
(7) Testing the external authentication function (LDAP) Points of view to be considered: i and iii	The evaluators confirm the behavior of the external authentication function when LDAP is specified as the external authentication protocol. The developer tested the external authentication function with a storage administrator, but did not confirm the behavior with other administrators. Therefore, the evaluators confirm the behavior with other administrators with different roles.
(8) Testing the external authentication function (RADIUS) Points of view to be considered: i and iii	The evaluators confirm the behavior of the external authentication function when RADIUS is specified as the external authentication protocol. The developer tested the external authentication function with a storage administrator, but did not confirm the behavior with other administrators. Therefore, the evaluators confirm the behavior with other administrators with different roles.
(9) Testing the external authentication function (Kerberos) Points of view to be considered: i and iii	The evaluators confirm the behavior of the external authentication function when Kerberos is specified as the external authentication protocol. The developer tested the external authentication function with a storage administrator, but did not confirm the behavior with other administrators. Therefore, the evaluators confirm the behavior with other administrators with different roles)

Points of View for the Independent Testing	Testing Outline
(10) Testing invalid values in the configuration files Point of view to be considered: ii	The evaluators confirm the behavior when an invalid value is set in the TOE configuration files on the management server. The developer tested the case in which an expected invalid value was set in the TOE configuration files, but did not confirm the case in which nothing is specified or unexpected values are specified. Therefore, the evaluators confirm the behavior when such values are specified.
(11) Testing user IDs and user passwords Point of view to be considered: ii	The evaluators confirm the behavior of adding a user or user login, in the cases in which the character string used for a user ID or password exceeds the maximum number of characters or includes invalid (not permitted) characters. The developer did not test the behavior when a user ID or password exceeds the maximum number of characters or includes invalid (not permitted) characters. The evaluators test the behavior in such cases. In addition, the evaluators confirm the behavior when the values used for the developer testing were changed to invalid (not permitted) characters.

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 (security architecture specification, structural design, and functional specification) and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

i. In terms of direct attacks, it is possible that the randomness of a token might be insufficient, and that attacks based on invalid tokens might occur.

ii. In terms of monitoring, there are risks of snooping. For example, while the TOE receives the password entered from a storage management client, the TOE itself does not provide a login screen, so SFR of authentication feedback is not selected, and a password is displayed on a screen during entering a login password and might be snooped by someone.

iii. Other publicly-known vulnerabilities, including vulnerabilities related to web applications, databases, and the OS.

b. Penetration Testing Outline

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

<Penetration Testing Environment>

The evaluators performed the penetration testing in an environment in which an inspection PC was added to the independent testing environment.

Table 7-3 shows details of the software used in the inspection PC. The evaluators confirmed the specifications of the software and performed the behavior testing as well as calibration.

Except for the inspection PC, this environment is the same as the environment used for the independent testing.

Figure 7-3 Software used for the Penetration Testing

Software name	Outline
Operation System	Windows 7 SP1
Web browser	Internet Explorer 9 (32bit) on Windows 7 SP1 with Flash Player 14.0
Nessus	Nessus 6.7.0 - A security scanner - The vulnerability database used contains the latest data (as of 2016-07-07).
Nikto	Nikto 2.1.5 - A security scanner targeted web servers - The vulnerability database used contains the latest data (as of 2016-07-07).
OWASP ZAP	ZAP 2.5.0 - A vulnerability diagnosis tool for web applications
Tamper IE	Tamper IE 1.0.1.13 - Tamper IE captures data transmitted from Internet Explorer, and enables such data to be tampered with.

<Penetration Testing Approach>

For the management servers installed in the independent testing environment, evaluators stimulated TOE interfaces from a storage management client and from an inspection PC.

- Evaluators confirm the TOE behavior by stimulating from TSFI.
- Evaluators capture packets transmitted to the TOE from a storage management client by using tools, and confirm the contents.
- Evaluators execute scans with vulnerability inspection tools.

For the binary inspection, the evaluators confirmed parts that were recognizable as character strings by using binary analysis tools, created by the Evaluation Facility, in terms that secret parameters which can be extracted might exist in the binary files.

<Content of the Performed Penetration Testing>

Table 7-4 shows vulnerabilities of concern and the content of the penetration testing corresponding to them.

Table 7-4 Outline of the Penetration Testing

Vulnerability	Outline of Testing
1) Confirming the randomness of tokens and the possibility of using invalid tokens	The evaluators acquire tokens and confirm that there is no regularity. The evaluators confirm the TOE behavior by inputting invalid tokens into parameters. Tamper IE is used to acquire tokens and input invalid tokens.
2) Testing the protection of input values when a password is entered	The evaluators confirm there is no risk of a password being snooped by being displaying on a screen, etc., when a password is entered.
3) Inspecting with tools	The evaluators perform inspections with tools (Nessus, Nikto, and OWASP ZAP) to inspect for other publicly-known vulnerabilities, including vulnerabilities related to web applications, databases, and operating systems.

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

In this evaluation, the assumed operational environment is specified in the ST, and this evaluation was performed in an environment that is the same as the operational environment specified by the ST.

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 are no special evaluator recommendations addressed to possible 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. Contents pointed out in the Observation Reports shall be adequate.

2. Contents pointed out in the Observation Reports shall properly be solved.

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

4. Rationale of the 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 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, Observation Reports 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

- Possible procurement entities should decide whether the TOE is acceptable in their environments based on the TOE behavior in this evaluation for which operational environment or settings is assured. When making this decision, the possible procurement entities need to note the following:

  > The TOE behavior outside the specified operational environment is not assured in this evaluation. For details on the operational environment, see “4.2 Environmental Assumptions.”

  > This evaluation is not intended to assure the configuration, in which the resources of the actual storage system is managed by the TOE functions

  In this evaluation, the configuration, in which the “storage resource information” (which is data in the management server, and is not data in the actual storage system) is managed by the TOE, is assured.

  > To counter attacks on the TOE from sources other than storage management clients is not assured in this evaluation. Such attacks must be prevented by the operating environment.

- The online help of the product is not included in the guidance documentation to be assured. For details on the guidance documentation to be assured, see “6. Documentation.”

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 Device Manager Software, Hitachi Tiered Storage Manager Software Security Target Version 1.0.28 (January 10, 2017) Hitachi, Ltd.

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 definitions of terms used in this report are listed below.

Banner information	Message information displayed as the warning banner function.
External authentication	An authentication method that uses the authentication function of the external authentication server (LDAP directory server, RADIUS server, or Kerberos server) outside the TOE from internal TOE.
External authentication group linkage	A function of the TOE that acquires information about a group registered on an external authorization server and the accounts in that group, and then grants permissions information to the TOE. Because this function requires the authentication function external to the TOE, and because the accounts belong to a group, this function is called “external authentication group linkage.”
Internal authentication	An authentication method that uses only the TOE internal authentication function.
Security parameter	Parameter information related to TOE security functions. It includes such information as the number and type of characters permitted in passwords; the number of consecutive login failures and the corresponding threshold values; and whether the threshold values have been exceeded, in which case the account is locked.
Storage resource information	The information that represents the configuration of the storage system as follows, which is stored on the management server. It contains the following; which host group uses which logical storage; which physical disk group ensures any capacity to each logical storage; and each physical disk group consists of which physical disk.
Warning banner	Warning messages displayed before users start to use the TOE. Warning banners are mainly used to call attention to the possibility of illegal use.

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 Device Manager Software, Hitachi Tiered Storage Manager Software Security Target Version 1.0.28 (January 10, 2017) Hitachi, Ltd.

[13] Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software Evaluation Technical Report, Version 3 (143599-01-R003-03), January 16, 2017, Mizuho Information & Research Institute, Inc., Information Security Evaluation Office