Certification Report

SAITO Yutaka, Commissioner
Innovation Platform Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

IT Product (TOE)

Reception Date of Application (Reception Number)	2025-12-15 (ITC-5939)
Certification Identification	JISEC-C0870
Product Name	Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box
Version and Release Numbers	HA-DKC-04A-03X
Product Manufacturer	Hitachi Vantara, Ltd.
Collaborative Protection Profile Conformance	collaborative Protection Profile for Network Devices Version 3.0e (Certification Identification: CCEVS-VR-PP-0099)
Name of IT Security Evaluation Facility	ECSEC Laboratory Inc., Evaluation Center

This is to report that the evaluation result for the above TOE has been certified as follows.
2026-06-19

YANO Tatsuro, Technical Manager
IT Security Technology Evaluation Department
IT Security Center

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 5
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5
- Evaluation Activities for Network Device cPP Version 3.0e

Evaluation Result: Pass

"Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box, Version HA-DKC-04A-03X" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Innovation Platform 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 certification result in relation to IT Security Evaluation of "Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box, Version HA-DKC-04A-03X" (hereinafter referred to as the "TOE") developed by Hitachi Vantara, Ltd., and the evaluation of the TOE was completed on 2026-06-11 by ECSEC Laboratory Inc., Evaluation Center (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Hitachi Vantara, Ltd., and provide security information to procurement entities who are interested in the TOE.

This Certification Report assumes procurement entities who purchase the TOE to be readers. Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") described in Chapter 10. Especially, security functional requirements to be satisfied by the TOE and summary specifications of the security functionality to implement the requirements are detailed in the ST.

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 Protection Profile or Assurance Package

The TOE conforms to the following collaborative Protection Profile [10] (hereinafter referred to as the "Conformance cPP").

collaborative Protection Profile for Network Devices Version 3.0e
(Certification Identification: CCEVS-VR-PP-0099)

1.1.2 TOE and Security Functionality

The TOE is a disk storage device with remote management. The TOE provides disk storage functions to host computers via a dedicated storage network. Additionally, the TOE provides remote management functions via a network for operational management.

The TOE provides the security functions required by the Conformance cPP to protect the data handled by the TOE against attacks targeting its remote management functions and to prevent unauthorized access to the TOE.

For these security functions, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance requirements of the Conformance cPP.

Threats and assumptions assumed for the TOE are described in the following sections.

1.1.2.1 Threats and Security Objectives

The TOE provides remote management functions, and there are threats that the data

handled by the TOE could be exposed or altered, or that the TOE security functions could be compromised, due to unauthorized access to the communication data for remote management or unauthorized access to the TOE itself.

To counter these threats, the TOE provides security functions required by the Conformance cPP, such as identification and authentication, encryption, and digital signatures.

1.1.2.2 Configuration and Assumptions

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

The TOE is assumed to be operated in an environment where unauthorized physical access is restricted.

The operational management of the TOE assumes that a trusted administrator will adhere to the guidance documents and act in the best.

1.1.3 Disclaimers

Disk storage functions and their security measures of the TOE are outside the scope of this evaluation.

Furthermore, the following operations are not guaranteed in this evaluation.

- An operational environment or configuration different from the description in "4.2 Environmental Assumptions"

- A TOE with settings different from the description in "7.5 Evaluated Configuration"

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 in 2026-06, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [9] 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. The Certification Body confirmed that all the concerns were fully resolved, and that the TOE evaluation had been appropriately conducted in accordance with the CC [4][5][6], the CEM [7] and the support document for the Conformance cPP [11]. The Certification Body prepared this Certification Report based on the Evaluation Technical Report and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name:	Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box
TOE Version:	HA-DKC-04A-03X

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

Confirm the following information displayed on the TOE management screen in accordance with the guidance documents of the product:

- Brand Name: "HITACHI"

- Model name: One of the following:

  (For Japan)
  VSP One B 23, VSP One B 26, VSP One B 28

  (For other countries)
  VSP One B 24, VSP One B 26, VSP One B 28

- Version: "HA-DKC-04A-03X"

- Drive box type: "DBN2"

3. Security Policy

The TOE provides the security functions required by the Conformance cPP to protect the data handled by the TOE from attacks targeting its remote management functions and to prevent unauthorized access to the TOE.

As the background of the security functions provided by the TOE, user roles, threats, and organizational security policy specified by the Conformance cPP are described in Sections 3.1 through 3.3 below. Details of the security functions of the TOE are described in Chapter 5.

3.1 User Roles

The user roles of the TOE are described in Table 3-1.

Table 3-1 User Roles

Name	Description
Security Administrator (or simply referred to as "Administrator")	A user with the authority to manage the configuration of the TOE security functions. In the TOE, the following four roles fall under this category: Security Administrator (View & Modify), Storage Administrator (Initial Configuration), Audit Log Administrator (View & Modify), and User Maintenance. - Security Administrator (View & Modify) manages administrator accounts, X.509v3 certificates and cryptographic keys. - Storage Administrator (Initial Configuration) configures initial settings such as the time and banner messages. - Audit Log Administrator (View & Modify) configure audit log settings and view audit logs. - User Maintenance performs maintenance tasks such as software updates.

3.2 Threats

The threats to be countered by the TOE are described in Table 3-2.

Table 3-2 Threats

Name	Description
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.3 Organizational Security Policy

The organizational security policy required for the TOE is described in Table 3-3.

Table 3-3 Organizational Security Policy

Name	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which Administrators consent by accessing the TOE.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment for operating the TOE.

4.1 Usage Assumptions

Assumptions for operating the TOE are described in Table 4-1. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Note that the Conformance cPP includes the conditional assumption A.COMPONENTS_RUNNING for "distributed TOEs"; however, the assumption is not listed in Table 4-1 because the TOE is not a distributed TOE.

Table 4-1 Assumptions

Name	Description
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. Note: The Conformance cPP includes the conditional assumption statement for "virtual Network Device (vND)"; however, the statement is removed because the TOE is not a vND.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). Note: The Conformance cPP includes the conditional assumption statement for "virtual Network Device (vND)"; however, the statement is removed because the TOE is not a vND.

A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

4.2 Environmental Assumptions

Figure 4-1 shows the operational environment assumed for the TOE. The TOE connects to hosts via a dedicated storage network (Storage Area Network or IP Network) and provides disk storage functionality to the hosts. Additionally, the TOE is connected to servers and management PCs via a Local Area Network (hereinafter referred to as "LAN") for operational management. Administrators manage the TOE using a management PC

connected via a LAN. Some management functions are performed using a management PC connected locally to the TOE.

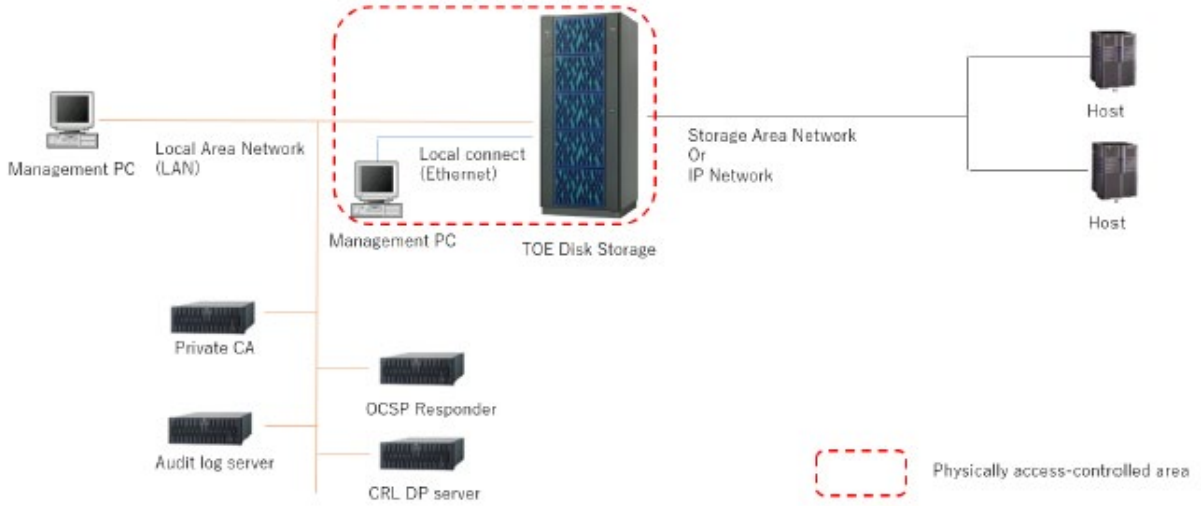

Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following components.

1) Host (Not evaluated)

A host computer that accesses the disk storage device, which is the TOE. It is outside the scope of this evaluation based on the Conformance cPP.

2) Management PC (LAN connection)

A general-purpose PC used to manage the TOE. A web browser supporting the HTTPS protocol (TLS 1.2, 1.3) and a REST API client are required. The following software was used in this evaluation:

- OS: Windows 11 Pro
- Web browser: Google Chrome 141.0.7390.108, Mozilla Firefox 144.0
- REST API client: script using Python 3.13.5

3) Management PC (local connection)

A general-purpose PC directly connected to the TOE via Ethernet. In accordance with the requirements of the Conformance cPP, it is used by administrators to perform administration when they are locked out and unable to login due to consecutive unsuccessful login attempts from the management PC connected via LAN. A web browser supporting the HTTPS protocol (TLS 1.2, 1.3) is required. The following software was used in this evaluation:

- OS: Windows 11 Pro
- Web browser: Google Chrome 141.0.7390.108

4) Audit Log Server

A server that stores audit logs generated by the TOE. Software supporting the Syslog over TLS (TLS 1.2, 1.3) is required. The following software was used in this evaluation:

- OS: Ubuntu 21.10
- Server software: rsyslogd 8.2302.0

5) Private CA

A server that issues the X.509v3 certificates used by the TOE. The following software was used in this evaluation:

- OS: Kali Linux 2023.4
- Server software: OpenSSL 3.0.8

6) OCSP Responder and CRL DP Server

A server that the TOE uses to verify the revocation status of X.509v3 certificates. Either an OCSP responder or a CRL DP server is required. An OCSP responder returns the revocation status of a certificate queried via the OCSP protocol. A CRL DP server distributes a list of revoked certificates via the HTTP protocol. The following software was used in this evaluation:

[OCSP Responder]

- OS: Kali Linux 2023.4
- Server software: OpenSSL 3.0.8

[CRL DP Server]

- OS: Kali Linux 2023.4
- Server Software: Python 3.13.5

It should be noted that the reliability of the hardware and the software other than the TOE shown in this configuration is outside the scope in the evaluation. They are assumed to be trustworthy.

4.3 Clarification of Scope

The functions provided by the TOE or those guaranteed by this evaluation have the following limitations.

1) Servers and Management PC

Administrators are responsible for secure operation of servers and management PCs working with the TOE.

2) Non-evaluated functions

The following functions are disabled in the evaluated configuration and are outside the scope of the assurance provided by this evaluation.

- SSH (Secure Shell) functionality for remote operation

- Time synchronization from an external NTP (Network Time Protocol) server to the TOE

3) Protection of network communications

The "Trusted Path/Channels" function provided by the TOE protects network communications between the management PC (LAN connection) and the TOE, and between the TOE and the audit server. It does not apply to communications between the TOE and other IT devices.

4) Web Browser and REST API client on the management PC

Most of the administration of the TOE can be performed on the management PC using either a web browser or a REST API client. However, some procedures during the installation of the TOE are not supported via a web browser and require the use of a REST API client.

5. Architectural Information

This chapter describes the scope and the main components of the TOE.

5.1 TOE Boundary and Components

The TOE is the entire product described in the TOE identification in Chapter 2.

The security functions of the TOE are described below.

1) Security Audit

This function generates audit logs of audit events relevant to security functions, stores them within the TOE, and transmits them to the audit log server.

If the storage capacity is exceeded when storing audit logs within the TOE, the oldest audit logs are overwritten by new ones. Audit logs stored in the TOE can be downloaded to a management PC only by authorized administrators. Audit logs stored in the TOE cannot be modified or deleted.

2) Cryptographic Support

This function consists of the cryptographic functions used in "Trusted Path/Channels" and "Protection of the TSF." It provides the following cryptographic functions:

- Encrypted communication protocols (HTTPS, TLS 1.2, TLS 1.3)
- Cryptographic key generation, key establishment, and key destruction
- Data encryption and decryption
- Generation and verification of digital signatures
- Hash
- Keyed-hash message authentication
- Deterministic random bit generation

The cryptographic communication protocols, cryptographic algorithms, and key lengths used in the functions listed above are those specified by the Conformance cPP.

The seed input for deterministic random bit generation has sufficient unpredictable entropy using random numbers output by a third-party CPU implemented in the TOE.

3) Identification and Authentication

This function consists of the function that identifies and authenticates administrators using a user ID and password, and the function that verifies X.509v3 certificates to authenticate communication peer in encrypted communication protocols.

The function that identifies and authenticates administrators using a user ID and password includes the following functionality to strengthen identification and authentication:

- Minimum password length requirement.
- Lock out the account for a set period after consecutive unsuccessful login attempts.

However, account lockout applies only when logging in from a management PC with LAN

connection, i.e. it does not apply when logging in from a management PC with local connection.

Verification of X.509v3 certificates includes revocation verification using an OCSP responder or a CRL DP server. If communication with both the OCSP responder and the CRL DP server is not possible when establishing a connection using the encrypted communication protocol, the connection with the communication peer will not be permitted.

4) TOE Access

This function allows administrators to control sessions that access TOE. It includes the following functionality:

- Session termination due to a set period of inactivity after administrator login
- Session termination by administrator logout
- Display of a warning banner regarding unauthorized use before login
(However, it is not displayed when logging in via a REST API client on the management PC)

5) Security Management

This function restricts settings of security functions to administrators. Administrative privileges are subdivided into four roles based on scope of operations, and only administrators with the appropriate role are permitted to perform the operation.

6) Protection of the TSF

This function protects the security functions of the TOE. It includes the following functionality:

- Verification of digital signatures of the firmware during TOE start-up
- Known answer tests of cryptographic algorithms during TOE start-up
- Verification of digital signatures of the update firmware during firmware updates
- Hashing of administrator passwords when storing (plaintext passwords are not stored)
- Providing reliable date and time information (the TOE maintains the date and time set by the administrator)

The cryptographic algorithms for verifying digital signatures and hashing use the "Cryptographic Support" function.

7) Trusted Path/Channels

This function protects communications from a remote management PC (LAN connection) to the TOE using the encrypted communication protocol HTTPS, and communications from the TOE to the audit server using the encrypted communication protocol TLS. HTTPS, TLS, and related cryptographic functions use the "Cryptographic Support" function.

5.2 IT Environment

The TOE security function "Trusted Path/Channels" works with IT devices external to the TOE and uses the following protocols. The TLS version is 1.2 or 1.3.

- Management PC (LAN connection): HTTPS (HTTP over TLS)
- Audit server: Syslog over TLS

The verification of X.509v3 certificates in the TOE security function "Identification and Authentication" uses an OCSP responder and a CRL DP server external to the TOE.

6. Documentation

The guidance documents of the TOE are identified in Table 6-1 and Table 6-2. TOE users are required to fully understand and comply with the following documents to satisfy the assumptions.

Table 6-1 Guidance (Japanese)

Name[1]	Version
Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 System Administrator Guide	4050-1J-U50-41
Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 ESM Message Guide	4050-1J-U07-41
Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 Audit Log Reference Guide	4050-1J-U00-41
Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 System Provisioning Guide	4050-1J-U09-41
Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 VSP One Block Administrator REST API Reference Guide	4050-1J-U41-40
Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 VSP One Block Administrator Users Guide	4050-1J-U40-40

[1] The guidance name listed in Table 6-1 is the translation of Japanese name.

Hitachi Virtual Storage Platform One Block 23, Block 26, Block 28 Hitachi Virtual Storage Platform 5100, 5200, 5500, 5600, 5100H, 5200H, 5500H, 5600H Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H Hitachi Virtual Storage Platform F350, F370, F700, F900 Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900 REST API Reference Guide	4060-1J-U71-60
Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 SIM Reference	4050-1J-U21-41
Hitachi Virtual Storage Platform One Block 23/26/28 with Drive Box HA-DKC-04A-03X Users guidance	1.14

Table 6-2 Guidance (English)

Name	Version
Hitachi Virtual Storage Platform One Block A3-04-0x System Administrator Guide	MK-23VSP1B009-03
Hitachi Virtual Storage Platform One Block 20[2] A3-03-2x Installation Guide	MK-23VSP1B008-03
Hitachi Virtual Storage Platform One Block SVOS 10.4 Maintenance Utility Messages	MK-23VSP1B005-03
Hitachi Virtual Storage Platform One Block SVOS 10.4 Provisioning Guide	MK-23VSP1B012-03
Hitachi Virtual Storage Platform One Block SVOS 10.4 VSP One Block Administrator REST API Reference Guide	MK-23VSP1B002-02
Hitachi Virtual Storage Platform One Block SVOS 10.4 VSP One Block Administrator Users Guide	MK-23VSP1B001-02

[2] The term "Hitachi Virtual Storage Platform One Block 20" in this guidance is a collective term for the following three models for countries other than Japan.
- Hitachi Virtual Storage Platform One Block 24
- Hitachi Virtual Storage Platform One Block 26
- Hitachi Virtual Storage Platform One Block 28

Hitachi Virtual Storage Platform One Block Hitachi Virtual Storage Platform 5000 Series Hitachi Virtual Storage Platform E Series Hitachi Virtual Storage Platform G130, G/ F350, G/F370, G/F700, G/F900 SVOS 10, SVOS RF 9 REST API Reference Guide	MK-23VSP1B003-05
Hitachi Virtual Storage Platform One Block 24/26/28 with Drive Box HA-DKC-04A-03X Users guidance	1.13

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

ECSEC Laboratory Inc., Evaluation Center 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, in accordance with the requirements of ISO/IEC 17025. It is periodically confirmed that the Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Method

The evaluation was conducted in accordance with the assurance requirements in the CC Part 3 required by the Conformance cPP using the evaluation methods prescribed in the CEM and the assurance activities of the Conformance cPP.

Details of the evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report describes the content of the evaluation and the verdict for each work unit in the CEM and assurance activity of the Conformance cPP.

7.3 Overview of Evaluation Activity

The evaluation started in 2025-12 and concluded upon completion of the Evaluation Technical Report dated 2026-06. This evaluation is a continuation of the previous evaluation conducted from 2024-12 to 2025-12.

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. Furthermore, the evaluator conducted the evaluator testing at the developer site in 2025-10, 2025-11, 2026-03 and 2026-04.

Concerns found by the Evaluation Facility during the evaluation were issued as the Observation Reports and reported to the developer. The concerns were reviewed by the developer, and all of them were resolved eventually.

Concerns found by the Certification Body during the evaluation certification were issued as the certification oversight reviews and reported to the Evaluation Facility. The concerns were examined by the Evaluation Facility and the developer, and reflected in the Evaluation Technical Report.

7.4 IT Product Testing

Based on the evaluation documentation, the evaluator conducted evaluator independent testing to ensure that the security functions of the product are accurately implemented, and evaluator penetration testing based on vulnerability analysis.

7.4.1 Developer Testing

Developer testing is not included in the assurance requirements for this evaluation.

7.4.2 Evaluator Independent Testing

The evaluator conducted evaluator independent testing (hereinafter referred to as the "independent testing") based on the evaluation documentation to ensure that the security functions of the product are accurately implemented. The independent testing performed by the evaluator is described below.

1) Independent Testing Environment

The environment for the independent testing is based on the operational environment of the TOE shown in Figure 4-1. The components used in the independent testing environment are listed in Table 7-1.

Table 7-1 Components of the Independent Testing Environment

Components	Description
TOE	(For Japan) - Hitachi Virtual Storage Platform One Block 28 with Drive Box, HA-DKC-04A-03X (For other countries) - Hitachi Virtual Storage Platform One Block 26 with Drive Box, HA-DKC-04A-03X
Management PC (LAN connection)	- OS: Microsoft Windows 11 Pro - Web browser: Google Chrome 141.0.7390.108, Mozilla Firefox 144.0 - REST API client: Python 3.13.5
Management PC (local connection)	- OS: Microsoft Windows 11 Pro - Web browser: Google Chrome 141.0.7390.108
Audit Log Server	- OS: Ubuntu 21.10 - Server software: rsyslogd 8.2302.0
Private CA	- OS: Kali Linux 2023.4 - Server software: OpenSSL 3.0.8
OCSP Responder	- OS: Kali Linux 2023.4 - Server software: OpenSSL 3.0.8
CRL DP Server	- OS: Kali Linux 2023.4 - Server software: Python 3.13.5

The following differences exist between the configuration of the independent testing and the TOE configuration identified in the ST. The evaluator determined that there are no problems with those differences and that the security functions of the TOE configuration identified in the ST can be considered properly tested.

(1) Tested models

In the models of the TOE described in Chapter 2 "TOE identification," there are multiple models due to the following differences:

- Differences in languages for Japan and for other countries
- Differences in storage capacity

The evaluator determined that the security functions of all the models of the TOE can be considered to have been tested by testing two representative models considering the above differences, because the software for each model is identical.

(2) Use of the developer interface (SSH)

In the independent test, the developer interface (SSH) was used to modify and verify data within the TOE. The evaluator determined that the testing using the developer interface was valid, because SSH, which is disabled in the TOE evaluated configuration, was only temporarily enabled.

(3) Use of additional test tools

In the independent testing, some test tools were used to verify and modify communication data. The validity of those test tools was confirmed by the evaluator.

2) Summary of the Independent Testing

The independent testing conducted by the evaluator is as follows.

a. Independent Testing Viewpoints

Viewpoints of the independent testing devised by the evaluator based on the requirements of the Conformance cPP and the evaluation documentation are as follows.

<Viewpoints of the Independent Testing>
(1) Verify security functions for each Security Functional Requirement (SFR).
(2) Verify that the implementation of the cryptographic algorithms is correct.

b. Independent Testing Outline

An outline of the independent testing conducted by the evaluator is as follows.

<Independent Testing Approach>
Inputs are provided to the TOE using a management PC, test tools, and a developer interface, and its behavior is verified using input responses, communication data, audit logs, and log information within the TOE.

< Independent Testing Contents>
Table 7-2 shows the independent testing content for each perspective.

Table 7-1 Performed Independent Tests

Viewpoint	Test Overview
(1)	<Verification of security functions> Verify that all security functions work as the specification with the test items devised based on the assurance activities of the Conformance cPP for each SFR or the requirements of the SFR.

(2)	<Verification of implementation of cryptographic algorithms> Verify that the following cryptographic algorithms are implemented as the specification. - RSA-2048, RSA-3072, RSA-4096 - ECDSA P-256, ECDSA P-384, ECDSA P-521 - KAS-ECC, KAS-FFC - AES-CTR-256, AES-GCM-128, AES-GCM-256 - SHA-256, SHA-384, SHA-512 - HMAC-SHA-256, HMAC-SHA-384 - CTR_DRBG (AES-256)

c. Results

All independent tests performed by the evaluator were correctly completed, and the evaluator verified the behavior of the TOE. The evaluator confirmed that all test results were consistent with the expected behavior.

7.4.3 Evaluator Penetration Testing

The evaluator devised and conducted evaluator penetration testing (hereinafter referred to as the "penetration testing") on potentially exploitable vulnerabilities of concern under the assumed operational environment and attack level. The penetration testing conducted by the evaluator is described below.

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 for potential vulnerabilities based on the evaluation documentation and publicly available information, and identified the following vulnerabilities that require penetration testing.

(1) There is a concern that unintended network ports may be open on the TOE.

(2) There is a concern that known vulnerabilities may exist in the web interface of the TOE.

(3) There is a concern that buffer overflow vulnerability may exist in the input processing of the TOE.

Note that the evaluation documentation includes a list of hardware and software components used within the TOE, as required by the Conformance cPP. The evaluator confirmed that these components did not contain any known vulnerabilities.

b. Penetration Testing Outline

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

<Penetration Testing Environment>
The penetration testing environment was identical to the independent testing

environment, except for the addition of penetration testing tools. The tools used in the penetration testing are listed in Table 7-3.

Table 7-3 Penetration Testing Tools

Name	Overview and Purpose of Use
Nmap Version 7.97	A tool for detecting available network ports.
OWASP ZAP Version 2.16.1	A tool for assessing vulnerabilities in web applications.
Burp Suite Professional Version 2025.5.4	A tool used to view and modify communication data between the web browser and the web server (TOE).

<Penetration Testing Contents>

Table 7-4 shows the penetration testing content for each vulnerability of concern.

Table 7-4 Performed Penetration Tests

Vulnerability	Test Overview
(1)	- Verify that no unexpected network ports are open on the TOE using Nmap.
(2)	- Verify that there are no known vulnerabilities in the web interface of the TOE using OWASP ZAP. - Verify that there are no known vulnerabilities in the web interface of the TOE by modifying data sent from a web browser to the TOE using Burp Suite Professional.
(3)	- Verify that countermeasures to prevent buffer overflow attacks are enabled for the process that handles external inputs within the TOE.

c. Results

In the penetration testing performed by the evaluator, no vulnerabilities were identified that could be exploited by an attacker with the assumed attack potential.

7.5 Evaluated Configuration

The conditions of the TOE configuration that are prerequisites for this evaluation are as described in the guidance documents listed in Chapter 6. In order to use the TOE securely, as ensured by the evaluation, the TOE must be configured as described in the guidance documents. Configurations that differ from the guidance documents are outside the scope of the assurance provided by this evaluation.

7.6 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM and all assurance activities in the Conformance cPP as per the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance:
  collaborative Protection Profile for Network Devices Version 3.0e

- Security functional requirements: Common Criteria Part 2 Extended

- Security assurance requirements: Common Criteria Part 3 Conformant

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

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1,
ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1,
ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

The evaluation results apply only to the configurations described in "4.2 Environmental Assumptions" and "7.5 Evaluated Configuration" for the TOE identified in Chapter 2.

7.7 Evaluator Comments/Recommendations

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

8. Certification

The Certification Body certified the evaluation from the following viewpoints based on the materials submitted by the Evaluation Facility.

1. Contents pointed out in the Observation Reports shall be adequate.

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

3. The submitted documentation was sampled, the content was examined, and the related work units in the CEM and assurance activities of the Conformance cPP 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 and the assurance activities of the Conformance cPP.

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

8.1 Certification Result

As a result of verification of the Evaluation Technical Report, Observation Reports and related evaluation documentation submitted by the Evaluation Facility, the Certification Body determined that the TOE evaluation satisfies the assurance requirements required by the Conformance cPP.

8.2 Recommendations

Procurement entities who are interested in the TOE are advised to refer "4.2 Environmental Assumptions" and "7.5 Evaluated Configuration" to make sure the scope of the evaluation and the operational requirements of the TOE meet the operational conditions assumed by each user.

9. Annexes

There is no annex.

10. Security Target

The Security Target [8] of the TOE is provided as a separate document from this Certification Report and identified as follows:

Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box Security Target, Version 1.15, June 10, 2026, Hitachi Vantara, Ltd.

11. Glossary

The abbreviations related 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
cPP	collaborative Protection Profile
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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

CRL DP	Certificate Revocation List Distribution Point
OCSP	Online Certificate Status Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
REST API	Representational State Transfer Application Programming Interface
SSH	Secure Shell
TLS	Transport Layer Security

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

Evaluation Activities	Evaluation work to be performed by an evaluator for PP conformance. It is a supplement of the CEM. In the case of the Conformance cPP [10], it is described in the supporting document [11] for the cPP.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, August 2025, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, December 2023, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2021, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[8] Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box Security Target, Version 1.15, June 10, 2026, Hitachi Vantara, Ltd.

[9] Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box HA-DKC-04A-03X Evaluation Technical Report, Version 1.7, June 11, 2026, ECSEC Laboratory Inc., Evaluation Center

[10] collaborative Protection Profile for Network Devices, Version 3.0e, December 6, 2023 (Certification Identification: CCEVS-VR-PP-0099)

[11] Evaluation Activities for Network Device cPP, Version 3.0e, December 6, 2023