LGAI Technological Center S.A.
Campus UAB – Ronda de la Font del Carme, s/n
08193, Bellaterra, Barcelona (Spain)
CIF: A63207492
Tel: +34 93 567 20 00
www.applus.com

Certification Report

Huawei OceanStor Pacific V800R001C10SPC100

Product name & version:	**Huawei OceanStor Pacific Storage System V800R001C10SPC100**
Developer:	Huawei Technologies Co., Ltd.
Certificate ID:	EUCC-3096-2026-002
Internal File ID:	EUCC-2025-004
Project code:	EUCHUA002
Release Date:	16/10/2026
Author:	José Carlos Andreu Galán
Approver:	Núria Carrió Misas

Version Control

Version	Date	Description
1.0	16/10/2026	First release of the Certification Report.

Report created with template TEMCER023_Certification Report Template, version 2.0.

Contents

1 Introduction 4
2 Evaluated Product Information 5
3 Executive Summary 6
4 TOE description 8
4.1 Scope and Boundaries 8
4.2 Summary of the Security Target 9
4.3 Security Policies 9
4.4 Architectural information 10
4.5 TOE components 12
4.6 Assumptions and Operational Environment 14
4.7 Lifecycle management processes and production facilities 14
4.8 Supplementary Cybersecurity information and Vulnerability management processes 14
5 Evaluation Summary 15
5.1 Assessment against each assurance requirement 15
5.2 Documentation 16
5.3 Evaluated configuration 16
5.4 Testing approach and depth 17
5.5 State of the art documents and evaluation criteria used 17
5.6 Vulnerability Analysis and Penetration Testing 17
6 Evaluation and Certification Results 18
7 Mark and Label 18
8 Comments and Recommendations from Certification Body 19
9 Annex 20
10 Bibliography 20

1 Introduction

This report documents the evaluation and certification process of Huawei OceanStor Pacific Storage System V800R001C10SPC100 against the *Common Criteria for Information Technology Security Evaluation Version 2022, applying CC:2022 and CEM:2022 Errata v1.2.* The evaluation was conducted by Applus+ Laboratories (LGAI Technological Center S.A.) in accordance with the requirements of EUCC scheme using Common Criteria Evaluation methodology.

This document constitutes the Certification Report for the certification of the product Huawei OceanStor Pacific Storage System V800R001C10SPC100, requested on 22/12/2025, and evaluated by Applus+ Laboratories (LGAI Technological Center S.A.), as detailed in the Evaluation Technical Report *CCBHUA002-ETR-M0* [ETR].

Developer/manufacturer:	Huawei Technologies Co., Ltd.
Name and Contact:	Fuchu Ma (support@huawei.com)
Certification Body	LGAI Technological Center, S.A. (Applus+ Laboratories)
NCCA	Autoridad Nacional de Certificación de la Ciberseguridad en España
Evaluation Laboratory	LGAI Technological Center, S.A. (Applus+ Laboratories)
Protection Profile	N/A
Common Criteria Version	Common Criteria 2022 (Errata v1.2)
Evaluation end date	September 30, 2026

2 Evaluated Product Information

The next table provides information about the identification of the TOE and the certification scope:

TOE Name and Version	Huawei OceanStor Pacific Storage System V800R001C10SPC100
TOE Product's components	**Software:** Basic storage software package: *OceanStor Pacific_V800R001C10SPC100.tar.gz* Digital signature file: *OceanStor Pacific_V800R001C10SPC100.tar.gz.asc*
Security Target	Huawei OceanStor Pacific Storage System V800R001C10SPC100 Security Target version 0.19
Sanitized Security Target	**Not Applicable**
Protection profile	**Not Applicable**
Patch Management	**Not Applicable**
Supplementary Cybersecurity information	***https://e.huawei.com/en/documents/products/storage/971d03e61868431594fb031c33ca8932***
Life-cycle	**Applicable SARs:** ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1 and ALC_FLR.2.
Evaluation Level	EAL3 augmented with ALC_FLR.2

3 Executive Summary

This Certification Report states the outcome of the EUCC security evaluation of the Huawei OceanStor Pacific V800R001C10SPC100 software. The developer of the TOE is Huawei Technologies Co., Ltd. Located in P.R. of China and they also act as the sponsor of the evaluation and certification.

The TOE is a software that supports an intelligent distributed storage product that can be scaled horizontally or elastically.

OceanStor Pacific uses the storage system software to integrate local storage resources from common hardware into a distributed storage pool. OceanStor Pacific provides distributed Block Service, distributed Object Service, and distributed File Service for upper-layer applications. Each storage service provides various functions and value-added features. In addition, OceanStor Pacific supports flexible purchase and deployment of multiple storage services based on service requirements, helping enterprises cope with flexible and efficient data access requirements when services change rapidly. OceanStor Pacific provides highly efficient, highly available, and scalable intelligent distributed storage to meet higher performance, capacity, and scalability requirements of complex service loads in the cloud and AI era. It is widely applicable to cloud resource pools, mission-critical databases, big data analysis, content storage, and backup archiving in industries such as finance, carriers, and government public utilities.

The major security functions addressed by the TOE are:

- Identification and Authentication
- Authorization and Access Control
- Auditing
- Security Management
- User Data Protection
- Protection of The TSF
- Resource Utilisation
- TOE Access

The TOE (software based) runs on top of an OS (Euler OS) (non-TOE software) and hardware (non-TOE hardware) that are developed and maintained by the developer themselves.

The TOE has been evaluated by Applus+ Laboratories (LGAI Technological Center, S.A.) at the facilities located in Madrid, Spain. The evaluation was completed on September 30, 2026 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the EUCC as described in Commission Implementing regulation (EU) 2024/482.

The scope of the evaluation is defined by the Security Target [ST], which identifies assumptions made during the evaluation, the intended environment in which the TOE shall be running in, the security

requirements, and the level of confidence (EAL - Evaluation Assurance Level) at which the product is intended to satisfy the security requirements.

Consumers of the Huawei OceanStor Pacific V800R001C10SPC100 software are advised to verify that their own environment is consistent with the security target, and to give consideration to the comments outlined in this certification report.

There are no special configuration requirements except for those defined in the user guidance. All users shall read, apply and install the TOE in the operational environment accordingly.

The summary of the threats and security policies which the Security Target [ST] defines:

- The threats defined in section 3.2 of the Security Target [ST] are the ones addressed by the TOE in its operational environment. The assumed level of expertise of an attacker for all identified threats is Basic.

The Security Target [ST] does not define any Organizational Security Policy defined (OSP).

The results documented in the Evaluation Technical Report [ETR] for this TOE provide sufficient evidence that the TOE meets the requirements for the specified set of SARs and SFRs described in the Security Target [ST].

The claimed SARs for the evaluation (given by reference to an EAL3 augmented with ALC_FLR.2) are: ADV_ARC.1, ADV_FSP.3, ADV_TDS.2, AGD_OPE.1, AGD_PRE.1, ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ASE_CCL.1, ALC_FLR.2, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, and, AVA_VAN.2.

The assurance level is recognized by article 52 of [CSA] as “Substantial”.

The evaluation was conducted using the CC:2022 and CEM:2022 Release 1, applying the corrections introduced by CC:2022 and CEM:2022 Errata version 1.2.

The TOE does not claim conformance to any Protection Profile.

Applus+ CyberCB (LGAI Technological Center, S.A.) as a Certification Body for EUCC certification activities notified by the *Autoridad Nacional de Certificación de la Ciberseguridad en España,* declares that the evaluation activities meet all conditions for the issuing an EUCC certificate which will be published in the EUCC Certified Products list from ENISA. Note that the certification results apply only to the specific version of the product(s) as evaluated.

The initial date of issuance of the certificate was October 16th 2026, with a validity period of 5 years. The certificate unique identifier is EUCC-3096-2026-002.

4 TOE description

4.1 Scope and Boundaries

The scope of the TOE is defined in section 1.4 of the Security Target [ST], where the physical scope defines the TOE as part of the software of OceanStor Pacific V800R001C10SPC100 and its related product guidance.

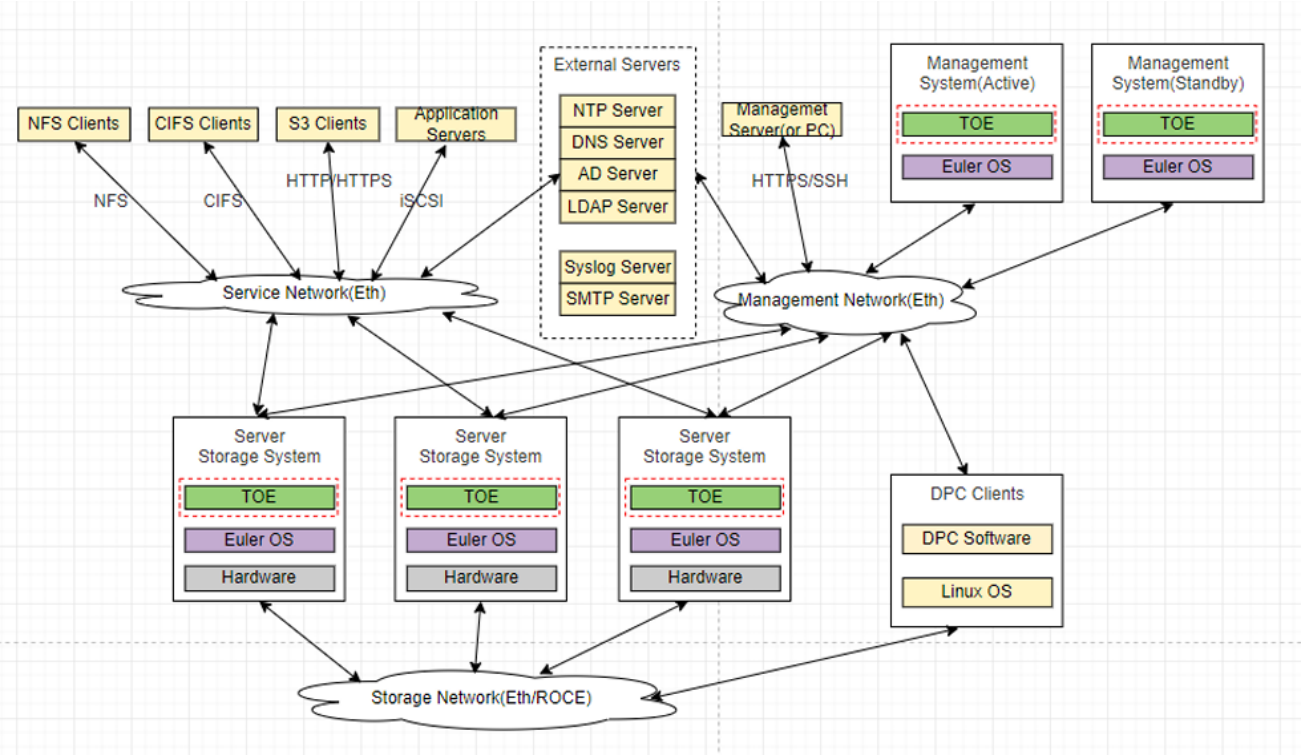


FIGURE 1 TOE BOUNDARIES

From a logical perspective, as described in section 1.4.2 of [ST], the scope boundaries of the software are defined by the security functions that it implements. The functions can be grouped as the major security features of the TOE:

- Identification and Authentication: The TOE works with multiple identity management systems to authenticate users and control access to storage data.
- Authorization and Access Control: Authorization indicates that devices assign operation authorities to accounts according to their validity.

  Access Control indicates that rules can be formulated by proper Administrative Users to globally control the access of a specific user to the TOE.
- Auditing: The TOE generates audit records for security-relevant management actions and stores the audit records in memory vault or manage board in the TOE.

• Security Management: Security functionality management includes not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters. According to security functionality management, customized security is provided.

• User Data Protection: The TOE uses account or user authentication, access control list (ACL) and bucket policy control object storage data access. Users must be authenticated before the ACL will be evaluated. Authentication occurs locally.

• Protection of The TSF: The TOE protects user data against disk and node failure.

The TOE also includes a sys clock, which provides the TOE with a reliable timestamp.

• Resource Utilization: The storage system protects data against failures using the multi-copy mechanism or erasure coding (EC). Data can be properly accessed even if a limited number of physical devices in the storage system become faulty, and data on the faulty devices will be automatically restored.

• TOE Access: Multiple parameters can be used to perform operations on limits to TOE Access.

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

The Security Target states that:

- The TOE must be installed and operated in a physically secure location.
- The TOE users are non-hostile, are properly trained in the TOE usage and follow guidance.
- The TOE's operational environment provides a secure network to protect the data exchanged to and from the TOE.
- Assumes the hardware and the operating system function properly and that there are no vulnerabilities in the hardware platform.

4.2 Summary of the Security Target

The evaluated Security Target is titled Huawei OceanStor Pacific Storage System V800R001C10SPC100 Security Target version 0.19. This document will be publicly available at the EUCC Certification page. No sanitization of the ST has been performed.

The security target [ST] does not claim conformance to any Protection Profile. The claimed assurance level is EAL3 augmented with ALC_FLR.2.

4.3 Security Policies

The Security Target does not define any Organizational Security Policies (OSP).

4.4 Architectural information

4.4.1 Logical architecture

Security audit

The TOE generates audit records for security-relevant management actions and stores the audit records in memory vault or manage board in the TOE. By default all configured commands along with a timestamp when they are executed are logged.

Attempts to login regardless success or failure are logged, along with user id, source IP address, timestamp, operation description, result(ok or error), and ID of the log.

The TOE allows the review of logs.

The TOE has means to export to external entities (FTP/SFTP) the logs and in real-time as well by using Syslog.

Identification and Authentication

The TOE works with multiple identity management systems to authenticate users and control access to storage data.

In management user access, the TOE provides local and remote authentication modes: In local authentication mode, the identities are stored in the TOE, whereas in remote authentication mode, the identities are stored in a remote LDAP server.

For Block Service data access, the available Volume is limited by the initiator. CHAP authentication is supported for connecting to the TOE over an iSCSI network.

For Object Service data access via S3 interface, the TOE provides local authentication mode.

For File Service data access via NFS interface, the TOE provides local and remote authentication modes LDAP or NIS.

For File Service data access via CIFS interface, the TOE provides local and remote authentication modes AD.

For File Service data access via POSIX interface of DPC, the TOE provides local authentication mode.

Authorization

The TOE controls access by the RBAC (Role Based Access Control) model. In RBAC, a permission is an approval to perform an operation on one or more RBAC protected objects (i.e. the commands in TOE), a role is a set of permissions and an account can be assigned with only one role. The TOE supports only 7 built-in roles which cannot be modify or deleted: Super administrator, administrator, Security Administrator, SAN resource administrator, system viewer, machine-machine account and account administrator.

Access Control

The TOE supports two Access Control mechanisms for Administrative Users:

- The IP Whitelist is configured globally to limit access from IP addresses out of the list.
- Login Method is a list including CLI, DeviceManager, and RESTful. A user can access the TOE only using the method/protocol included in this list configured for the user by other proper Administrative Users.

Security management

The following management can be performed on the TOE:

- Management of users and roles
- Management of security policies and access control
- Management of users sessions
- Management of domain authentication
- Management of the TOE's time setting
- Management of certificates
- Management of audit and alarm notification
- Block Service Management
- Object Service Management
- File Service Management

User Data protection

The TOE uses account or user authentication, access control list (ACL) and bucket policy control object storage data access. Users must be authenticated before the ACL will be evaluated. Authentication occurs locally. The TOE uses authentication and ACLs to control file data access. The file data access SFP relies on ACL and UNIX permissions, collectively called authorization data, to protect data at the file level.

Protection of the TSF

The TOE protects user data against disk and node failure. For the main storage disk/cache disk, the system performs periodic detection on the disk, based on the detection results of key indicators, the slow disk/failed disk is identified, the system actively sends an alarm, and automatically isolates the disk in the background and triggers data reconstruction.

The TOE detects node failures through a heartbeat mechanism. When a node failure is detected (such as operating system reset, CPU failure), it will trigger node failover and switch the services carried on it to other normal nodes.

The TOE also includes a sys clock, which provides the TOE with a reliable timestamp.

Resource Utilization

The storage system protects data against failures using the multi-copy mechanism or erasure coding (EC). Data can be properly accessed even if a limited number of physical devices in the storage system become faulty, and data on the faulty devices will be automatically restored.

Multi-copy Mechanism: The storage system supports two or three copies. When a piece of data is written, the storage system generates two copies for the data. The storage system writes the data and its copies into three storage nodes separately.

Erasure coding: The storage system supports this data protection technique that splits data into fragments and generates parity blocks to allow reconstruction even if some data is lost. Redundant data is stored across multiple nodes that conform the TOE.

4.4.2 Physical architecture

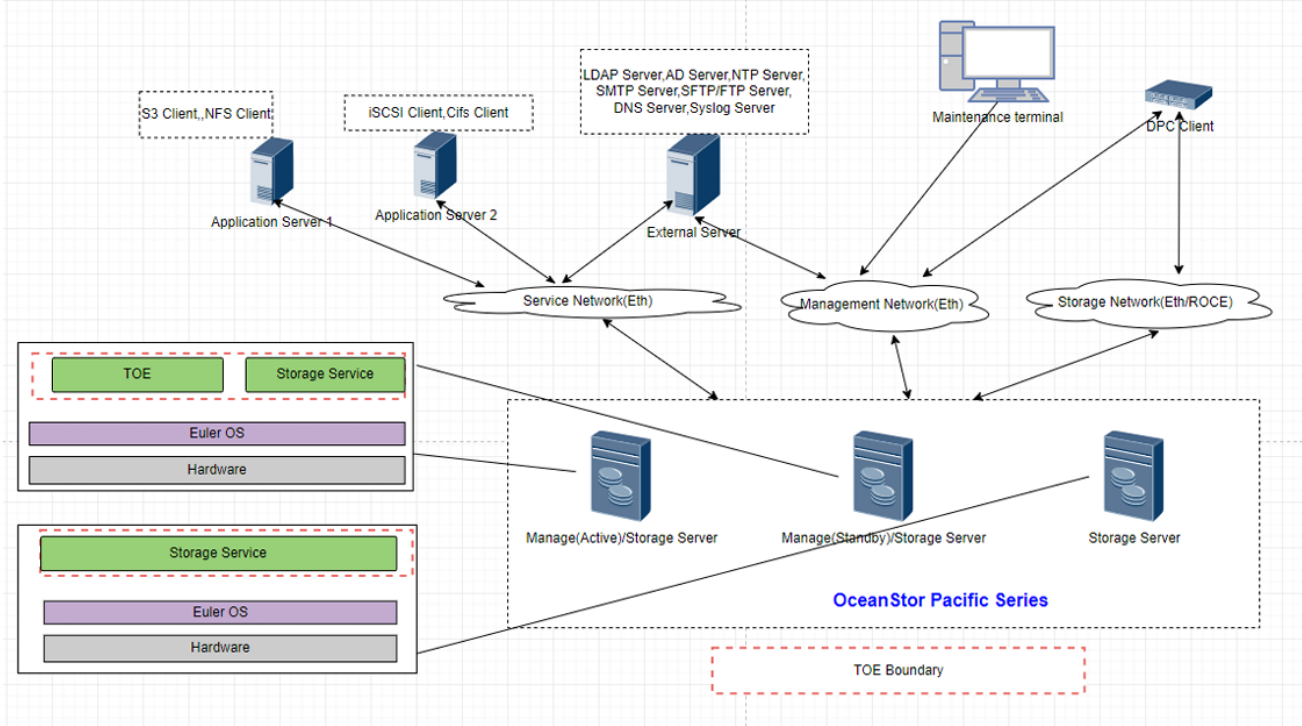


FIGURE 2 PHYSICAL ARCHITECTURE OF THE TOE

The TOE (software) is expected to be installed in (at least) 3 nodes (3 different hardware appliances) to be able to provide the minimum necessary redundancy to recover from faulty disks or nodes.

4.5 TOE components

The TOE components as defined in section 1.4.1 of the Security Target:

Type	Item	Version
Software	OceanStor Pacific_V800R001C10SPC100.tar.gz	V800R001C10SPC100

Digital Signature	OceanStor Pacific_V800R001C10SPC100.tar.gz.asc	V800R001C10SPC100
Product guidance	OceanStor Pacific Series V800R001C10 Event Reference	02
	OceanStor Pacific Series V800R001C10 Command Reference	02
	OceanStor Pacific Series V800R001C10 Error Code Reference	02
	OceanStor Pacific Series V800R001C10 REST Interface Reference	02
	OceanStor Pacific Series V800R001C10 Software Installation Guide	01
	OceanStor Pacific Series V800R001C10 Basic Service Configuration Guide for Object	03
	OceanStor Pacific Series V800R001C10 Basic Service Configuration Guide for File	02
	OceanStor Pacific Series V800R001C10 Basic Service Configuration Guide for Block	01
	OceanStor Pacific Series V800R001C10 API Description for Object	02
	OceanStor Pacific Series V800R001C10 Command Interface Role List	01
	OceanStor Pacific Series V800R001C10 RESTful Interface Role List	01
	Huawei OceanStor Pacific Storage System V800R001C10SPC100 AGD_OPE	0.7
	Huawei OceanStor Pacific Storage System V800R001C10SPC100 AGD_PRE	0.6

4.6 Assumptions and Operational Environment

The assumptions defined by the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives that are to be fulfilled by the TOE environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the Security Target [ST].

The user guidance, as referenced in section 4.5 contains necessary information about the usage of the TOE and the configuration of its environment to fulfill all the Assumptions as described in the Security Target [ST].

4.7 Lifecycle management processes and production facilities

See section ALC in section 5.1.

4.8 Supplementary Cybersecurity information and Vulnerability management processes

The contact information for the Huawei OceanStor Pacific was provided as: support@huawei.com.

The following link was provided to fulfill with the required supplementary cybersecurity information as referred to in Article 55 of Regulation (EU) 2019/881:

https://e.huawei.com/en/documents/products/storage/971d03e61868431594fb031c33ca8932

Subsequent links provide more information about compliance with:

- a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services.

  https://e.huawei.com/en/documents/products/storage/cc87306c45904bd69f362931e3e05562

- b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates:

  https://www.huawei.com/en/declarations/lifecycle-management-letter

- c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers:

  https://www.huawei.com/en/psirt/report-vulnerabilities

- d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories:

  https://securitybulletin.huawei.com/carrier/en/security-advisory

Note: From principal link it is possible to access the rest of supplementary information.

5 Evaluation Summary

LGAI Technological Center, S.A. is acting as both the ITSEF (Evaluation Laboratory) and CB (Certification Body) in the current certification process, under the notification of *Autoridad Nacional de Certificación de la Ciberseguridad en España*.

The CAB point of contact is: cybercert@applus.com

Evaluation Laboratory:	LGAI Technological Center, S.A. (Applus+ Laboratories)
Conformity Assessment Body	LGAI Technological Center, S.A. (Applus+ Laboratories)
National Cybersecurity Certification Authority	Autoridad Nacional de Certificación de la Ciberseguridad en España
Assurance components:	ADV_ARC.1, ADV_FSP.3, ADV_TDS.2, AGD_OPE.1, AGD_PRE.1, ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_FLR.2, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, and, AVA_VAN.2.
Protection Profile used	Not applicable
Common Criteria Version used	CC:2022 Release 1
Evaluation end date	September 30th, 2026

5.1 Assessment against each assurance requirement

ASE

The specific assurance requirements evaluated for the ASE class are: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1

The [ST] contains all relevant information to comply with all the families according to EAL3 augmented with ALC_FLR.2.

ADV

The specific assurance requirements evaluated for the ADV class are: ADV_ARC.1, ADV_FSP.3, ADV_TDS.2.

The developer demonstrated compliance by providing evidence regarding the Security Architecture of the TOE, its interfaces with complete summary through the functional specification and the TOE design decomposed in subsystems.

AGD

The specific assurance requirements evaluated for the ADV class are: AGD_OPE.1 and AGD_PRE.1

The evaluation of the user guidance (AGD) showed that the provided user guidance gives clear instructions on how to perform the acceptance procedures, installation and operation of the TOE such that its security claims are maintained. The evaluator concludes that the requirements of the assurance class AGD are met by the TOE.

ALC

The specific assurance requirements evaluated for the ALC class are**:** ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1 and ALC_FLR.2.

The evaluation of the lifecycle related aspects (ALC) successfully verified the TOE development and production lifecycle. The verification of proper application of the procedures regarding ALC_DVS involved an on-site visit to the development and production facility, and two data-centers related with the TOE's CM systems. The evaluator concluded that all the requirements for the ALC class are met.

ATE

The specific assurance requirements evaluated for the ATE class are**:** ATE_COV.2, ATE_DPT.1, ATE_FUN.1, and, ATE_IND.2.

The evaluation of the functional testing campaign consisted in the repetition of all the test plan provided by the developer and a set of independent tests to provide greater assurance of correct operation of the security functions. The repetition of developer's test plan and the execution of the independent tests was performed remotely by the evaluator.

The evaluator concludes that all requirements of the assurance ATE class are met.

AVA

The specific assurance requirements evaluated for the AVA class are**:** AVA_VAN.2.

The evaluator performed a public search of vulnerabilities for the TOE, its related third-party components and for vulnerabilities in components of its operational environment which could have an impact on the TOE's scope. The vulnerability analysis resulted in the developer devising a series of penetration tests. The tests were focused on exploiting logical flaws through the network interfaces of the TOE. The AVA related activities were conducted in full compliance with the assurance requirements set for AVA_VAN.2. As such, the evaluator demonstrates that the TOE is resistant to an attacker possessing basic attack potential.

5.2 Documentation

See section 4.5, product guidance row in the table.

5.3 Evaluated configuration

The evaluated configuration is based on the [AGD_PRE] guidance and all the accompanying product guidance in scope. The evaluator tested the TOE with 2 mutually exclusive configurations: with the block service enabled and with the file/object service enabled, in accordance to the descriptions provided in the Security Target [ST].

5.4 Testing approach and depth

The evaluator performed the installation and configuration in its operational environment according to the steps provided in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to the Security Target [ST].

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarized in the [ETR], with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its Security Target [ST] and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

5.5 State of the art documents and evaluation criteria used

No EUCC State of the art documents were used for this evaluation.

However, the following EUCC guideline documents were applied:

- ENISA, Agreed Cryptographic Mechanisms version 2 (May 2025) [ACM]

5.6 Vulnerability Analysis and Penetration Testing

The evaluator performed the Vulnerability Analysis and the Penetration Testing following AVA_VAN.2 SAR and its associated methodology defined in [CEM].

The evaluator did not find deviations from the expected results during the penetration testing campaign.

The evaluator conducted a public domain vulnerability search up until 15/09/2026 to check whether any new vulnerabilities may affect the TOE.

The total test effort expended by the evaluators was 1.5 weeks. During that test campaign, 100% of the time was spent on logical tests.

These activities were conducted successfully, demonstrating that the TOE is resistant to an attacker possessing Basic attack potential as defined for AVA_VAN.2.

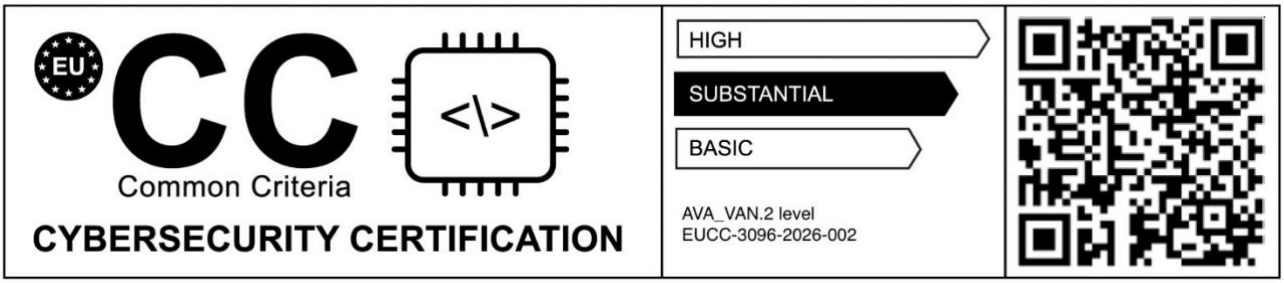
6 Evaluation and Certification Results

The ETR [ETR] did not reuse any previous results for the evaluation, as this was a first-time evaluation for this evaluation.

The Security Target does not claim conformance to a Protection Profile, referencing specific assurance requirements: ADV_ARC.1, ADV_FSP.3, ADV_TDS.2, AGD_OPE.1, AGD_PRE.1, ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_FLR.2, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, and, AVA_VAN.2.

Based on the above evaluation results presented in the ETR [ETR], the evaluation laboratory concluded that the Huawei OceanStor Pacific V800R001C10SPC100 to be CC Part 2 Conformant, CC Part 3 conformant. The obtained results imply that the product satisfies the security requirements set in the Security Target [ST]. The assurance level defined in [ST] is recognised by article 52 of [CSA] as “Substantial”.

7 Mark and Label



8 Comments and Recommendations from Certification Body

Considering the obtained evidence, the [ETR] from the laboratory and the own conclusions from the Certification Body, a positive resolution is proposed.

The certifier recommends TOE consumers to analyze the Security Target [ST] to verify that the security problem definition and the security functional requirements meet potential consumer security needs and recommends to strictly follow the guidance referenced in the Security Target [ST].

9 Annex

Not applicable.

10 Bibliography

[ACM] ENISA, «Agreed Cryptographic Mechanisms version 2,» May 2025.

[EUCC] European Parliament and of the Council, «Regulation (EU) 2024/482 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based sybersecurity scheme (EUCC),» 31 January 2024.

[CSA] European Parliament and of the council, «Regulation 2019/881 on ENISA and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act),» 17 April 2019.

[ETR] Applus+ Laboratories, «Evaluation Technical Report (Huawei OceanStor Pacific V800R001C10SPC100) version M0».

[ST] Huawei Technologies Co., Ltd., «Security Target Huawei Ocean Store Pacific V800R001C10SPC100 version 0.19».

[CEM] «Common Methodology for Information Technology Security Evaluation, version 2022 revision 1,» November 2022.

[AGD_PRE] Huawei Technologies Co., Ltd., «Huawei OceanStor Pacific Storage System V800R001C10SPC100 AGD_PRE version 0.6».