Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) CC:2022 Release 1

Certificato n. *(Certificate No.)*	09/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/04/2025/RC, v1.0
Decorrenza *(Date of 1st Issue)*	11 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	Huawei OceanProtect Software 1.6.0, X Series, E Series
Sviluppatore *(Developer)*	Huawei Technologies Co., Ltd.
Tipo di Prodotto *(Type of Product)*	Protezione dei dati (Data protection)
Livello di Garanzia *(Assurance Level)*	EAL2 con l'aggiunta di ALC_FLR.2, Conforme a CC Parte Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto, Conforme a CC Parte 2

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 11 febbraio 2026

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione CEM:2022 revisione 1 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione CC:2022 revisione 1. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation CEM:2022 release 1 for conformance to *Common Criteria for Information Technology Security Evaluation CC:2022 release 1. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Huawei OceanProtect Software 1.6.0, X Series, E Series

OCSI/CERT/CCL/04/2025/RC

Version 1.0

11 February 2026

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	11/02/2026

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AD	Active Directory
ADFS	Active Directory Federation Services
CIFS	Common Internet File System
CPU	Central Processing Unit
DNS	Domain Name System
HTTPS	Hyper Text Transfer Protocol Secure
iBMC	Intelligent Baseboard Management Controller
IDOR	Insecure Direct Object Reference

IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
NFS	Network File System
NTP	Network Time Protocol
OS	Operating System
PAM	Privileged Access Management
PDM	Product Data Management
PGP	Pretty Good Privacy
REST	Representational State Transfer
RSA	Rivest-Shamir-Adleman
SAML	Security Assertion Markup Language
SFTP	Secure File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TAC	Technical Assistance Center
UI	User Interface
VLAN	Virtual Local Area Network
XML	eXtensible Markup Language
XSS	Cross Site Scripting
XXE	External XML entity

4 References

4.1 Normative references and national Scheme documents

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, November 2022, CC:2022 Revision 1 CCMB-2022-11-001

[CC2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, November 2022, CC:2022 Revision 1 CCMB-2022-11-002

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, November 2022, CC:2022 Revision 1 CCMB-2022-11-003

[CC4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, November 2022, CC:2022 Revision 1 CCMB-2022-11-004

[CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022 Revision 1 CCMB-2022-11-005

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, November 2022, CC:2022 Revision 1 CCMB-2022-11-006

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[NIS4] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 4/23 – Gestione nel tempo delle garanzie di prodotti certificati, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[AGD_OPE] CC Huawei OceanProtect Software 1.6.0 AGD_OPE, Version: 1.1, 09 December 2025

[AGD_PRE] CC Huawei OceanProtect Software 1.6.0 AGD_PRE, Version: 1.1, 09 December 2025

[ETR] Evaluation of Huawei OceanProtect Software 1.6.0, HUAWEIEVOP-026_ETR_v2, CCLab – The Agile Cybersecurity Laboratory, Version: v2, 15 December 2025

[ST] Security Target CC Huawei OceanProtect Software 1.6.0 Security Target, Huawei Technologies Co., Ltd, Issue: 1.10, Date: 2025-12-09

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT -Products. A higher recognition level for evaluations beyond EAL4 is provided for IT -Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all claimed assurance components up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all claimed assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "**Huawei OceanProtect Software 1.6.0, X Series, E Series**" (also referred as Huawei OceanProtect Software 1.6.0 or Huawei OceanProtect), developed by Huawei Technologies Co., Ltd.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the and Scheme Information Notes [NIS1, NIS2, NIS3, NIS4]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC:2022 Release 1 for the assurance level EAL2, augmented with ALC_FLR.2 according to the information provided in the Security Target [ST] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3] and [CC5]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product named "Huawei OceanProtect Software 1.6.0" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Huawei OceanProtect Software 1.6.0, X Series, E Series
Security Target	CC Huawei OceanProtect Software 1.6.0 Security Target, Huawei Technologies Co., Ltd, Issue: 1.10, Date: 2025-12-09 [ST]
Evaluation Assurance Level	EAL2, augmented with ALC_FLR.2
Developer	Huawei Technologies Co., Ltd.
Sponsor	Huawei Technologies Co., Ltd.
LVS	CCLab – The Agile Cybersecurity Laboratory (Debrecen site)
CC version	CC:2022 Release 1
PP conformance claim	No conformance claimed
Evaluation starting date	24 February 2025
Evaluation ending date	15 December 2025

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description it is possible to refer to the Security Target [ST].

The TOE is a data protection software designed to back-up data of mission-critical services.

Huawei OceanProtect provides backup, recovery and high reliability with concurrent data flows and high backup bandwidth.

Major security features of the TOE include:

- backup and recovery of user data;
- audit generation and reviewing functions;
- secure, role-based administration with access control;
- identification and authentication.

The TOE runs on specific hardware devices, i.e. series X and series E versions. All products of the series run the same software and differ only in storage and computing resources. The evaluated models of Huawei OceanProtect are:

- X Series: X3000, X6000, X8000, X9000;
- E Series: E1000, E6000, E8000;

For a detailed description of the TOE, refer to section 1.4 of the Security Target [ST].

The TOE is made up of the **OceanProtect DataBackup** (hereinafter DataBackup), **OceanProtect Storage** (hereinafter Storage) Systems and **PAM**, **OpenSSH**, **lftp** and **NTP** components and the **Euler OS V2.0 SP12** based on Kernel 5.10.The DataBackup software component is used to manage the backups, archives, and restores. The software contains the backup catalog, which contains the internal database with information about OceanProtect' s backed-up data and configuration.

The Storage software component is deployed on OceanProtect Backup Storage Hardware Platform, which is designed to manage the storage hardware.

7.3.1 TOE architecture

The TOE includes the following subsystems:

- OceanProtect DataBackup (hereinafter DataBackup),
- OceanProtect Storage System (hereinafter Storage),
- components of the Euler OS (OpenSSH, PAM, lftp, NTP).

The DataBackup implements user management, configuration, and maintenance operations, including configuration, monitoring, alarm, statistics, user management, and license management, while Storage is responsible for file system management, network configuration, and its own user management. Euler OS supports the overall underlying system operations.

Interfaces include:

- RESTful,
- SSH,
- LDAP
- SFTP (1 and 2),
- Syslog,
- NTP,
- SAML,
- SMTP
- NFS,

- CIFS.

Each interface serves specific functions, such as remote management, authentication, and file transfer. The interfaces are designed to enhance security through protocols like HTTPS and SSH.

7.3.2 TOE description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

7.3.2.1 Physical Scope

An example deployment of the TOE (boundary is framed in red) is shown in the below Figure.

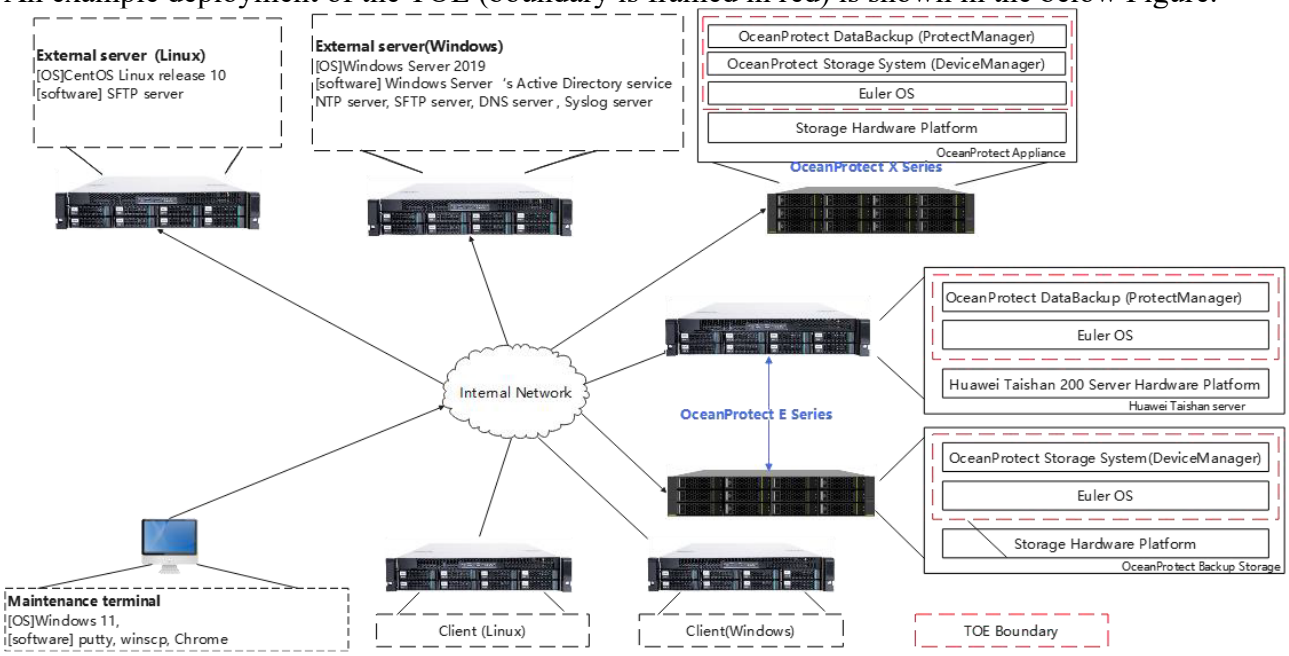

Figure 1 - TOE deployment and boundary.

The TOE boundary in the red frame includes the three distinct components (applications): OceanProtect DataBackup and Storage and Euler OS (components PAM, OpenSSH, lftp and NTP).

- **DataBackup**: In the X series, the OceanProtect Databackup software is deployed on the appliance. In the E series, the OceanProtect Databackup is deployed on the Huawei Taishan server.
- **Storage**: In the X series Storage is deployed on the appliance. In the E series, Storage is deployed on OceanProtect Backup Storage Hardware Platform, which is designed to manage the storage hardware.
- **Euler OS**: Running on the underlying hardware of all TOE appliances.

The Clients in Figure 1 (Windows and Linux) are used to communicate with the TOE and are out of the TOE scope.

The evaluated configuration assumes a network environment that provides internal connectivity between all components.

7.3.2.2 Logical Scope

The logical boundary of the TOE includes the interfaces and functions within the physical boundary. The TOE boundary from a logical point of view is represented by the elements that are displayed with a red dotted box within the rectangle in the Figure 2.

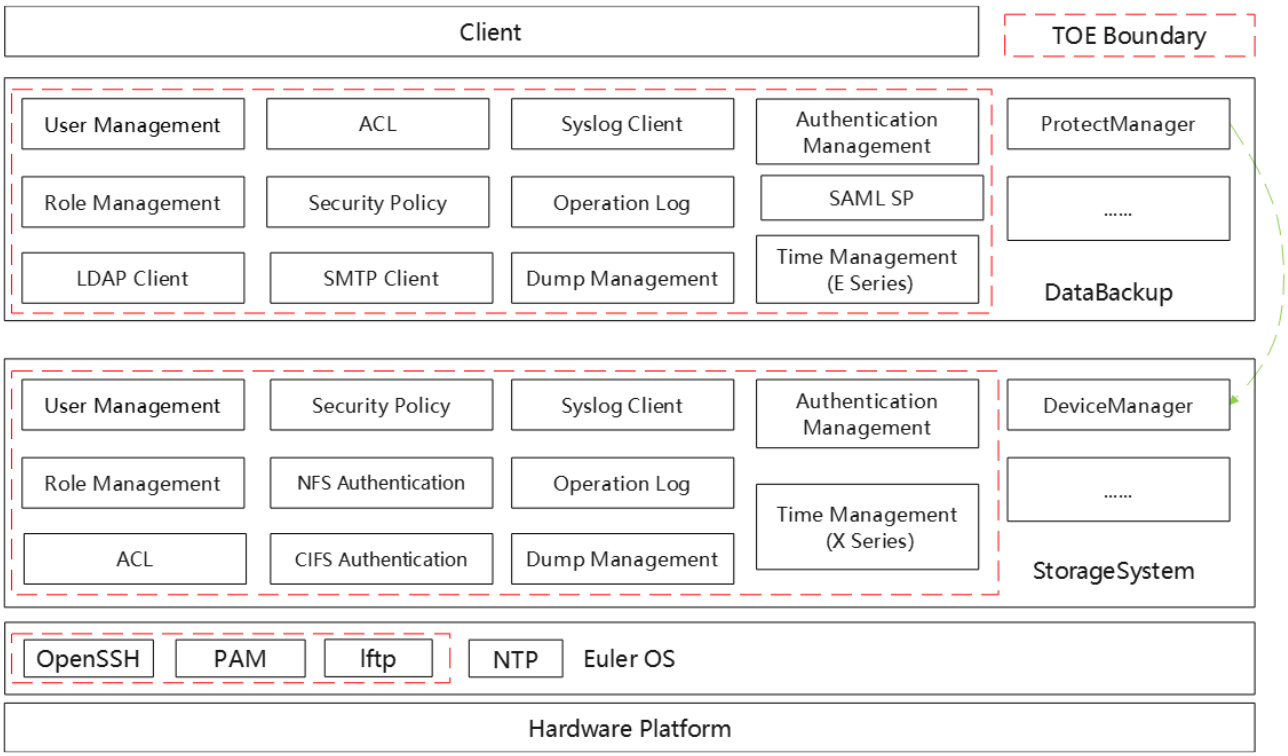

Figure 2 - Logical boundary of the TOE

The logical boundary of the TOE may be broken down by the security features, comprehensive described in section 5.2 of ST and grouped under the following Security Function Classes:

- Security Audit
- Access Control
- Identification and Authentication
- Authorization
- Security Management

7.3.3 TOE security features

The major security features of the TOE are summarised in the following:

1) Security Audit

Audit entries are generated by TOE for security-related backup events.

2) Access Control

The TOE provides a role-based access control capability both in DataBackup and Storage, to ensure that only authorized administrators are able to administer the TOE.

3) Identification and Authentication

The TOE ensures that users are identified and authenticated prior to being granted access to TOE functions.

4) Authorization

The TOE ensures that proper permissions is granted to identify sessions which are generated with subset of identified users' attributes.

5) Security Management

The TOE provides management capabilities via ProtectManager. Management functions allow the administrators to configure users and roles and manage backup and recovery functionality.

A detailed description of the TOE security functionality is provided in Chapter 6 of the Security Target [ST].

7.3.3.1 Product Physical/Logical Features and Functionality not included in the TOE

The TOE provides all the security features.

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The TOE does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] and are from EAL 2 assurance package, augmented with the CC part 3 components ALC_FLR.2.

All the SFRs have been selected from CC Part 2 [CC2].

It is possible to refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been

evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab – The Agile Cybersecurity Laboratory (Debrecen site).

The evaluation was completed on December 15, 2025, with the issuance by the LVS of the approved Evaluation Technical Report [ETR].

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in "Annex B – Evaluated configuration".

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; there is a probability, however small, that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS CCLab – The Agile Cybersecurity Laboratory (Debrecen site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "Huawei OceanProtect Software 1.6.0" meets the requirements of Part 2 and 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2 augmented with ALC_FLR.2, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2 augmented with ALC_FLR.2 (augmentation in *italics* in Table 1).

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	*Pass*
Test	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass

Assurance classes and components		Verdict
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product "Huawei OceanProtect Software 1.6.0" are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the "Security Objectives for the Operational Environment" specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.4 of the Security Target [ST] shall be satisfied.

The Certification Body recommends reviewing the assumptions in the [ST], section 3.4, which are necessary conditions to be implemented for the TOE security:

- *A.MANAGE - It is assumed that the administrators of the TOE are non-hostile, sufficiently trained, and follow all administrator guidance. They will not write down their passwords.*
- *A.PHYSICAL - It is assumed that the TOE and its operational environment are protected against unauthorized physical access.*
- *A.NETWORK - The TOE environment will provide a secure network communication to protect user data that is sent to and received from the TOE.*
- *A.TIMESTAMP - the TOE environment will provide reliable time to the TOE.*

This Certification Report is valid for the TOE in its evaluated configuration; in particular, "Annex A – Guidelines for the secure usage of the product" includes a number of recommendations relating to delivery, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([AGD_PRE] and [AGD_OPE]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The following procedural steps define how the TOE is delivered to the customer. The delivery procedures can be distinguished into two separate phases:

- verify and install the software package,
- deliver the TOE hardware appliance to the customer's end.

Software Delivery (internal process):

The download, verification, and installation of software packages are all completed on Huawei's production line. The hardware equipment the Developer delivers has the original TOE software installed.

This section summarizes describes the internal download and verification of the TOE software package before pre installation.

The software of the TOE is downloaded to the Huawei's production software server through Huawei's Product Data Management (PDM) system. The production software server is secured by IPsec which protect the TOE components' confidentiality, authenticity and integrity while in transport from the development area to the production area. The software is then written into the OceanProtect system, and the software's integrity is checked by comparing its signature and version number.

To verify the Software Package details the steps required to check the integrity of the received software package (e.g.: "OceanProtect_DataProtect_1.6.0_image_ARM_64.tgz") include utilizing the signature file of the received software package (file with the ".asc" extension), and Huawei's own public key, which was used for signing the signature file.

The verifier is required to download the public key file from Huawei's internal site and import it into their own list of PGP certificates to verify the key's validity.

The verification process for the TOE software package by the customer is the same, with the difference being that the customer needs to download the software package from the support website, but this does not necessarily happen, as the verification of the TOE software happens before delivery to the customer, as an internal process if the TOE software is delivered pre-installed.

To access the public key file at Huawei support site:

https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054/TV1000000016

The key is generated using RSA 2048.

To verify the signature file of the received software package (file with the ".asc" extension), and Huawei's own public key the "GnuPG" software is recommended by the Developer.

TOE preinstalled on hardware delivery:

The packaging operation of TOE is performed by Huawei production site staff. TOE parts and packaged TOEs are securely stored at the Dongguan production site. Before delivery of the TOE, the correctness and integrity of the anti-tamper tags that are applied to the TOE boxes are checked. If the verification is successful, the TOE delivery process to the customer will be initiated, and it is ensured that the TOE version is correct.

The Developer relies on third party shipping companies to deliver products from the facility to customers with contracts ensuring security during transport.

Huawei discloses information about the shipping company used for particular deliveries on a need-to-know basis. By this, it is difficult for an attacker to predict which shipping company will be used for a particular delivery and by this reduces the risk of fake deliveries by an attacker.

The recipient of a delivery is informed about the shipping company used and is advised to check that the delivery is carried out by the correct shipping company. the TOE finally leaves the Developer premises and is shipped to the customer.

Customers shall check the TOE as follows when receiving the products:

- check that the cargo boxes are not damaged,
- check that none of the anti-tamper tags are damaged or warped,
- check if there are traces of duplicate sealing;
- check that all parts of the TOE and guidance documentation are delivered.

The guidance documentation is published to the OceanProtect device's help information. Customers can access it through the OceanProtect system's Web portal under Help --> Online Help. The delivery parts can also be obtained via the Huawei TAC service https://e.huawei.com/en/about/service-hotline or through the sales team.

The list of deliverables as follows:

Type	**Delivery Item**	**Version**
Storage Subsystem Software	OceanProtect_BackupStorage_1.6.0_Software.tgz	1.6.0
DataBackup Subsystem Software	OceanProtect_DataProtect_1.6.0_image_ARM_64.tgz	1.6.0
	OceanProtect_DataProtect_1.6.0_chart_ARM_64.tgz	1.6.0
Product guidance	CC Huawei OceanProtect Software 1.6.0 AGD_PRE 1.0.pdf	1.0
	CC Huawei OceanProtect Software 1.6.0 AGD_OPE 1.0.pdf	1.0
	OceanProtect DataBackup 1.5.0-1.6.0 Error Code Reference.pdf	01
	OceanProtect Backup Storage 1.x Error Code Reference.pdf	01
	OceanProtect Appliance 1.6.0 REST Interface Reference.pdf	05
	OceanProtect Backup Storage 1.6.0 REST Interface Reference.pdf	02
	OceanProtect DataBackup 1.5.0-1.6.0 Administrator Guide.pdf	09
	OceanProtect DataBackup 1.5.0-1.6.0 Command Reference.pdf	01

Table 2 - TOE deliverables

Documents of the product have unique version numbers. The version information of documents of the product is specified in the [ST] section 1.4.1 Table 1-3 for the product. The ST shall be obtained from the website of the certification body. The version shall be verified by comparing the document

version information of the product with the version numbers in the ST. The links for the exact documents are also found in the ST as well.

9.2 Installation, configuration and secure usage of the TOE

TOE installation, configuration and secure usage should be done by following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the documents [AGD_PRE] and [AGD_OPE] contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure usage of the TOE in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

The Evaluators followed the preparation steps defined in the [AGD_PRE] and [AGD_OPE] documents for the TOE being in the evaluated configuration.

The TOE is identified in the Security Target [ST] with the version number 1.6.0. The evaluation of the TOE was conducted on configuration 1.6.0. The name, version and configuration number uniquely identify the TOE and the set of its subsystems, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

The OceanProtect software is available in two series: X Series and E Series, each with distinct models.

- X Series includes models X3000, X6000, X8000, and X9000, differing in CPU, cache, and I/O modules.
- E Series includes models E1000, E6000, and E8000, also varying in CPU, cache, and I/O modules.

All models fulfil the minimum hardware requirements for the software.

The X Series models have specific configurations for CPU, cache, I/O modules, and power supply. CPU configurations range from 2 x Kunpeng 920 24-core to 2 x Kunpeng 920 64-core and 8 x Kunpeng 920 48-core 2.6 GHz. Cache sizes vary from 256 GB to 1024 GB. I/O module support ranges from 4 to 28 modules depending on the model.

All models share identical power supply specifications of 2,000 W.

The E Series models also have distinct configurations for CPU, cache, I/O modules, and power supply. CPU configurations range from 2 x Kunpeng 920 32-core to 2 x Kunpeng 920 128-core. Cache sizes vary from 128 GB to 2048 GB. I/O module configurations differ, with a maximum of 10 modules for E8000.

The E1000 has a power supply of 900 W, while E6000 and E8000 share a 2,000 W power supply.

All models are compatible and identical from an evaluation perspective. Variations in hardware specifications do not impact the software's security functionalities.

The test environment contains **X8000** and **E1000** appliances of the TOE.

The most essential steps for the installation of each device are as follows:

As a **preparative step** the customer has to conclude obtaining the public key file, importing it and verifying the public key and signature. However, in this evaluation case this section is not applicable as the TOE arrived pre-installed.

OceanProtect X8000:

- installing and mounting the hardware chassis into a 2U enclosure, connecting the cables,
- powering-on,
- changing IP Addresses, configuring the network,
- initializing the system,
- setting device time,
- logging in to the Web UI,
- modifying the backup network.

OceanProtect E1000:

- installing and mounting the hardware chassis into a 2U enclosure, connecting the cables,
- powering-on,
- changing IP Addresses of the iBMC, configuring the network,
- configuring users,
- configuring port bonding,
- initializing the system,
- logging in to the Web UI,
- modifying the service network,
- creating Backup Storage Device and Backup Storage Unit.

10.1 TOE operational environment

The assumptions about the technical environment in which the TOE is intended to be used are reported in section 3.4 of [ST].

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

The Evaluators conducted the tests in the LVS premise. The test configuration was installed by the Evaluators who followed the steps described in [AGD_PRE] and the [AGD_OPE] document.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer performed extensive tests to verify the functionality of the TOE. The tests cover all Subsystems, Modules and TSFIs of the TOE.

11.2.2 Test coverage

Developer's tests were grouped in the following categories:

- Auditing;
- User Data Protection;
- Identification and Authentication;
- Security Management;
- Network Services.

11.2.3 Test results

All Developer's tests were run successfully, and the Evaluators verified the correct behaviour of the TSFIs and TSFs and the correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

In addition to the Developer's tests, the Evaluators created and performed three more independent test cases to test the TSF more in depth.

The independent tests were related to

1. login event audit data;
2. user identification and authentication mechanisms for newly created users;
3. rejection of invalid configuration changes of SFTP, SMTP and DNS services.

11.3.2 Test results

All test cases devised by the Evaluators were passed successfully and all the test results were consistent with the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked with the TOE already used for the functional test activities and verified that the TOE and the test environment were properly configured.

The Evaluators designed the following attack scenarios:

- authentication bypass;
- user enumeration;
- privilege escalation and authorization bypass;
- cross-site scripting (XSS);
- insecure direct object reference (IDOR);
- external XML entity (XXE) injection;
- SSH service attack;
- password recovery service attack.

The Evaluators has concluded that the TOE is resistant to **BASIC** attack potential in its intended operational environment.