

Reference: 2020-53-INF-3711- v2  
Target: Pública  
Date: 03.02.2022

Created by: CERT9  
Revised by: CALIDAD  
Approved by: TECNICO

## CERTIFICATION REPORT

---

Dossier # **2020-53**

TOE **Huawei OceanStor 100D Storage System Software v8.0.3**

Applicant **440301192203821 - Huawei Technologies Co., Ltd.**

References

[Tipo-Código] Ref - Description

---

Certification report of the product Huawei OceanStor 100D Storage System Software v8.0.3, as requested in [EXT-6210] dated 25/05/2020, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-7413] received on 12/11/2021.

## CONTENTS

EXECUTIVE SUMMARY .....	3
TOE SUMMARY .....	3
SECURITY ASSURANCE REQUIREMENTS .....	4
SECURITY FUNCTIONAL REQUIREMENTS .....	5
IDENTIFICATION .....	6
SECURITY POLICIES .....	6
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT .....	6
CLARIFICATIONS ON NON-COVERED THREATS .....	6
OPERATIONAL ENVIRONMENT FUNCTIONALITY .....	7
ARCHITECTURE .....	7
LOGICAL ARCHITECTURE .....	7
PHYSICAL ARCHITECTURE .....	7
DOCUMENTS .....	8
PRODUCT TESTING .....	8
EVALUATED CONFIGURATION .....	9
EVALUATION RESULTS .....	9
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM .....	9
CERTIFIER RECOMMENDATIONS .....	9
GLOSSARY .....	10
BIBLIOGRAPHY .....	10
SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE) .....	10
RECOGNITION AGREEMENTS .....	11
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) .....	11
International Recognition of CC – Certificates (CCRA) .....	11

## EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei OceanStor 100D Storage System Software v8.0.3.

OceanStor 100D is an intelligent distributed storage product that can be scaled horizontally or elastically. Based on the unique elastic erasure coding (EC) technology, as well as the dynamic deduplication and compression technology based on automatic load control, OceanStor 100D provides more available space for customers while ensuring service performance. In addition, it provides the ever new capability to support smooth software upgrade. Hardware can coexist for multiple generations without service interrupting caused by software and hardware updates.

**Developer/manufacturer:** Huawei Technologies Co., Ltd.

**Sponsor:** Huawei Technologies Co., Ltd..

**Certification Body:** Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

**ITSEF:** Applus Laboratories.

**Evaluation Level:** Common Criteria v3.1 R5 -EAL3+ (ALC\_FLR.2).

**Evaluation end date:** 03/02/2022

**Expiration Date<sup>1</sup>:** 05/03/2027

All the assurance components required by the evaluation level EAL3 (augmented with ALC\_FLR.2) have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3+ (ALC\_FLR.2), as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Huawei OceanStor 100D Storage System Software v8.0.3, a positive resolution is proposed.

## TOE SUMMARY

OceanStor 100D is an intelligent distributed storage product that can be scaled horizontally or elastically. Based on the unique elastic erasure coding (EC) technology, as well as the dynamic deduplication and compression technology based on automatic load control, OceanStor 100D provides more available space for customers while ensuring service performance. In addition, it

---

<sup>1</sup> This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

provides the ever new capability to support smooth software upgrade. Hardware can coexist for multiple generations without service interrupting caused by software and hardware updates.

OceanStor 100D uses storage system software to integrate local storage resources from common hardware into a distributed storage pool. OceanStor 100D 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 100D 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 100D 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 features implemented by the TOE subject to evaluation are:

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

## **SECURITY ASSURANCE REQUIREMENTS**

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3 and the evidences required by the additional component ALC\_FLR.2 to the table, according to Common Criteria v3.1 R5.

Assurance class	Assurance components
ASE	ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.2 ASE_REQ.2 ASE_SPD.1 ASE_TSS.1

ADV	ADV_ARC.1 ADV_FSP.3 ADV_TDS.2
AGD	AGD_OPE.1 AGD_PRE.1
ALC	ALC_CMC.3 ALC_CMS.3 ALC_DEL.1 ALC_DVS.1 ALC_LCD.1 ALC_FLR.2
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_VAN.2

## SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

SECURITY FUNCTIONAL REQUIREMENTS
FAU_GEN.1
FAU_GEN.2
FAU_SAR.1
FAU_SAR.2
FAU_SAR.3
FAU_STG.1
FAU_STG.3
FAU_STG.4
FDP_ACC.1
FDP_ACF.1
FIA_ATD.1
FIA_UAU.2
FIA_UAU.5
FIA_UAU.6
FIA_UAU.7
FIA_UID.2
FIA_AFL.1
FIA_USB.1
FIA_SOS.2
FMT_MSA.1
FMT_MSA.3

FMT_SMF.1
FMT_SMR.1
FPT_STM.1
FPT_FLS.1
FRU_FLT.1
FTA_MCS.2
FTA_SSL.3
FTA_TAH.1
FTA_TSE.1
FCS_COP.1

## IDENTIFICATION

**Product:** Huawei OceanStor 100D Storage System Software v8.0.3

**Security Target:** CC Huawei OceanStor 100D Storage System Software 8.0.3 ST, v2.3, 29/10/2021

**Evaluation Level:** EAL3+ (ALC\_FLR.2).

## SECURITY POLICIES

The use of the product Huawei OceanStor 100D Storage System Software v8.0.3 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.3 (“Organizational Security Policies”).

## ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3.4 (“Assumptions”).

## CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei OceanStor 100D Storage System Software v8.0.3, although the agents implementing attacks have the attack potential according to the EAL3 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.2 (“Threats”).

## **OPERATIONAL ENVIRONMENT FUNCTIONALITY**

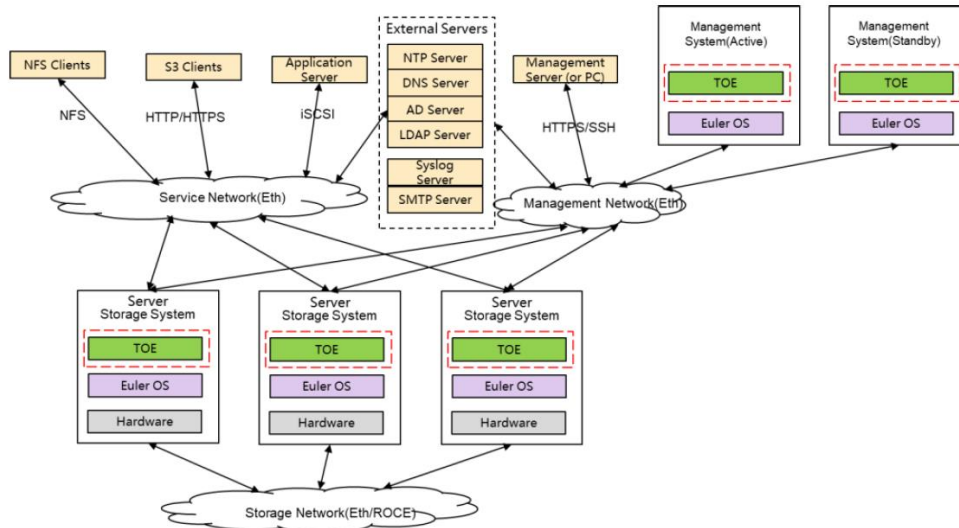
The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 (“Security Objectives for the operational Environment”).

## **ARCHITECTURE**

### **LOGICAL ARCHITECTURE**

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.



**Figure 1-1** Shows the physical scope and physical boundary of the TOE environment

### **PHYSICAL ARCHITECTURE**

The TOE is a ‘software only’, does not contain hardware. The software package, signature file, and the guidance documentation are delivered to the customer site by downloading from support website.

## DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- CC Huawei OceanStor 100D Storage System Software 8.0.3 AGD\_OPE
- CC Huawei OceanStor 100D Storage System Software 8.0.3 AGD\_PRE
- OceanStor 100D 8.0.3 Administrator Guide 05
- OceanStor 100D 8.0.3 Basic Object Service Configuration Guide 05
- OceanStor 100D 8.0.3 CLI Command Reference
- OceanStor 100D 8.0.3 Error Code Reference
- OceanStor 100D 8.0.3 Event Reference
- OceanStor 100D 8.0.3 Object Service Account Management API Description
- OceanStor 100D 8.0.3 Object Service API Reference
- OceanStor 100D 8.0.3 REST Interface Reference
- OceanStor 100D 8.0.3 Security Configuration Guide 05
- OceanStor 100D 8.0.3 Software Installation Guide
- CC Huawei OceanStor 100D Storage System Software 8.0.3 ST, v2.3, 29/10/2021

## PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification and the SFRs description included in the Security Target [ST].

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included 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 evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same



results as the expected ones. The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a non-expected manner. There has not been any deviation from the expected results under the environment defined in the Security Target [ST].

## EVALUATED CONFIGURATION

The TOE is defined by its commercial name and version number: Huawei OceanStor 100D Storage System Software v8.0.3.

The acceptance and installation procedures are given in section 2 (Secure Acceptance by Users) of the preparative user guidance CC Huawei OceanStor 100D Storage System Software 8.0.3 AGD\_PRE.

To obtain the proper operation of the product according to the evaluated configuration the components indicated in section 1.3.3 (Non-TOE hardware, Software, and Firmware Required by the TOE) of the Security Target [ST] are required.

## EVALUATION RESULTS

The product Huawei OceanStor 100D Storage System Software v8.0.3 has been evaluated against the Security Target “CC Huawei OceanStor 100D Storage System Software 8.0.3 ST, v2.3, 29/10/2021”.

All the assurance components required by the evaluation level EAL3+ (ALC\_FLR.2) have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL3+ (ALC\_FLR.2), as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

## COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

There is no additional recommendation from the Laboratory in order to use the TOE since guidance documentation is enough to make a secure usage of the TOE.

## CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei OceanStor 100D Storage System Software v8.0.3, a positive resolution is proposed.

## GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

## BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC\_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC\_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC\_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

## SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- CC Huawei OceanStor 100D Storage System Software 8.0.3 ST, v2.3, 29/10/2021

## RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

### ***European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)***

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at <https://www.sogis.eu>.

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

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

### ***International Recognition of CC – Certificates (CCRA)***

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC\_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC\_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: <http://www.commoncriteriaportal.org>.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC\_FLR.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.