MINISTERIO DE LA PRESIDENCIA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2013-20-INF-1591 v1	Created by: CERT11
Target: Público	Revised by: CALIDAD
Date: 13.04.2016	Approved by: TECNICO

CERTIFICATION REPORT

File: 2013-20 Huawei OceanStor Software

Applicant: 440301192W HUAWEI Technologies Co., Ltd.

References:

[EXT 2271] Certification request of Huawei OceanStor Software

[EXT 2956] Evaluation Technical Report of Huawei OceanStor Software.

The product documentation referenced in the above documents.

Certification report of the product Huawei OceanStor T&SX900 Series Storage System Software, version V100R005C30SPC300, as requested in [EXT 2271] dated on 28/08/2013, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT 2956] received on 20/11/2015.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei OceanStor T&SX900 Series Storage System Software, version V100R005C30SPC300.

The TOE is a software-only TOE in charge of managing a Storage system.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd.

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

ITSEF: Epoche & Espri S.L.U.

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R4 – EAL3+ALC_CMC.4 + ALC_CMS.4

Evaluation end date: 20/11/2015.

All the assurance components required by the evaluation level EAL3+ (augmented with ALC_CMC.4 Production support, acceptance procedures and automation + ALC_CMS.4 Problem tracking CM coverage) have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3 + ALC_CMC.4 + ALC_CMS.4, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4. Considering the obtained evidences during the instruction of the certification request of the product Huawei OceanStor T&SX900 Series Storage System Software, version V100R005C30SPC300, a positive resolution is proposed.

TOE summary

The TOE is a software-only TOE in charge of managing a Storage system.

The storage system combines files and blocks, various protocols, and diversified management interfaces. It is based on the industry-leading hardware specifications and integrates such high-end technologies as high density disk design, TurboModule flexible interface module and hot swap design, TurboBoost three-level performance boost technology, and multi-layer data protection technology. The storage system satisfies the increasingly complicated storage requirements of various service applications at a low cost, such as database online transaction processing, digital media, Internet operation, centralized storage, backup, disaster recovery, and data migration, effectively ensuring the security and continuity of user services.

CHAP authentication is supported when connecting to the TOE withaiSCSI network. The target LUN on the TOE can be accessed only when the CHAP authentication is passed.

All these security features belongs to the product surrounding the TOE and not to the TOE itself, and therefore no assurance is claimed over them.

TOE major security features

The major security features implemented by the TOE and subject to evaluation (no assurance can be supposed to any other functionality) to can be summarised as follows:

- Authentication and Identification
  - The TOE can authenticate administrative users by user name and password. The authentication is always enforced for virtual terminal sessions via SSH sessions. The authentication for access via the console is always enabled. It supports login of two type of users, local users and domain users via remote LDAP (always using LDAPS)/AD server.
  - The LUN access is limited by the LUN ID and WWN of the initiator for FC or by the custom name for iSCSI. Such WWN(FC)/custom name(iSCSI) are the unique identification methods for hosts.

- Access Control: the TOE controls access to the storage system for management and configuration by user roles. Three hierarchical access control levels are offered that can be assigned to individual user accounts.

- 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 including authentication, authorization, user management, defining IP addresses and address ranges for clients.

- NTP (Network Time Protocol) is an application layer protocol used on the internet to synchronize clock among a set of distributed time servers and clients. In this manner, the clock of the host is synchronized with certain time standards. NTP synchronizes all the clocks of devices (switches, PCs, and routers) on the network so that these devices can provide multiple applications based on the uniform time. The TOE supports this protocol in order to maintain timestamps in the audit records.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidences required to fulfil the evaluation level EAL3+ and the evidences required by the additional components ALC_CMC.4

Production support, acceptance procedures and automation and ALC_CMS.4 Problem tracking CM coverage, according to Common Criteria v3.1 R4.

Class	Family/Component
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.3 Functional specification with complete summary ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle model
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

Class	**Family/Component**
FAU	GEN.1 GEN.2 SAR.1 STG.1 STG.4
FDP	ACC.1/a ACC.1/b

	ACF.1/a ACF.1/b
FIA	ATD.1/a ATD.1/b UAU.2 UID.2
FMT	MSA.1/a MSA.1/b MSA.1/b2 MSA.1/b3 MSA.3/a MSA.3/b MTD.1/a MTD.1/a2 MTD.1/b MTD.1/b2 SMF.1/a SMF.1/b SMR.1
FPT	STM.1
FTA	SSL.3 TSE.1

IDENTIFICATION

Product: Huawei OceanStor T&SX900 Series Storage System Software, version V100R005C30SPC300

Security Target: Huawei OceanStor T&SX900 Series Storage System Security Target, v3.5

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R4 – EAL3 + ALC_CMC.4 + ALC_CMS.4

SECURITY POLICIES

There are no Organizational Security Policies defined for this evaluation.

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 [ST]. 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.

- A.Manage. Users with Super administrator or Administrator role are non-hostile, appropriately trained, and follow all administrator guidance.
- A.Physical. It is assumed that the TOE is protected against unauthorized physical access.
- A.I&A. The TOE environment will provide identification and authentication of users before allowing any actions.
- A.DataProtection. The TOE environment will provide a secure place to store user data.
- A.TrustedServers. The SFTP an LDAPS server are always trusted servers whose certificates are confidents too.
- A.NetworkSegregation. It is assumed that the ETH management interface in the TOE will be accessed only through an independent local network. This network is separated from the networks that use the other ETH interfaces of the TOE (and is not source of attacks).

THREATS

The threats to the IT assets against which protection is required by the TOE or by the security environment are listed below. The threat agents are divided into two categories:

- Non-TOE user or application without rights for accessing the TOE.
- TOE user (a human user, SERVER or application using the functionality of the TOE).

The threats defined are:

- T.UnauthenticatedAccess:
  - Threat agent: Non-TOE user or application without rights for accessing the TOE.
  - Asset: all assets
  - Adverse action: The threat agent gains access to the TOE through the LAN interface.
- T.UnauthorizedAccess:
  - Threat agent: TOE user (a user or application using the functionality of the TOE).
  - Asset: all assets
  - Adverse action: The threat agent gains access to commands or information he is not authorized for through the LAN interface.
- T.DataCorruption
  - Threat agent: all threat agents
  - Asset:all assets
  - Adverse action: Data corruption due to hardware failure caused by incorrect system access by threat agents performing unauthorized data modification and/or inadequate configuration actions through the LAN interface.
- T.UnauthorizedServer
  - Threat agent: Non-TOE user or application without rights for accessing the TOE.
  - Asset: User data in disks.
  - Adverse action: A system connected to the TOE could access data that was not intended to be accessed by unauthorized read and write through the SAN interface.

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 categorized below.

Security Objectives that are to be satisfied by the environment:

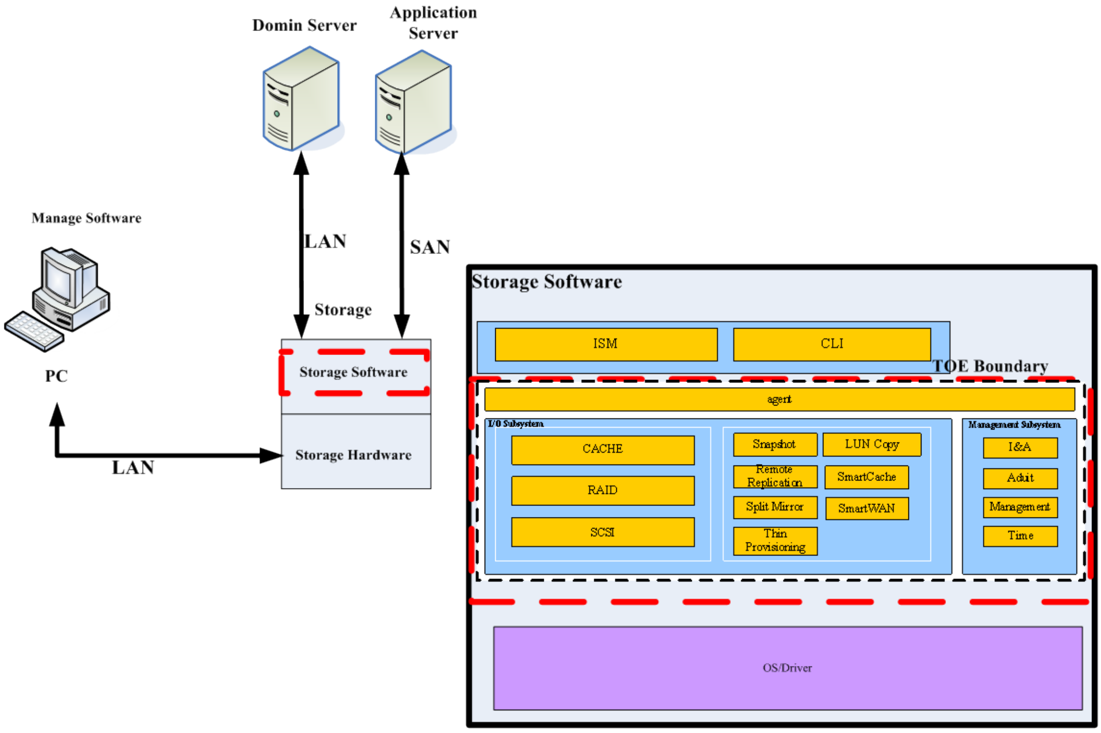
- OE.Manage. The TOE Environment must ensure that thesuper administrator and administrators are non-hostile, appropriately trained, and follow all administrator guidance.
- OE.Physical. The TOE shall be protected against unauthorized physical access.
- OE.I&A. The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.

- OE.DataProtection. The TOE Environment must protects the data of TOE stored in secure place.
- OE.TrustedServers. The SFTP an LDAPS server are always trusted servers whose certificates are confidents too.
- OE.NetworkSegregation. The ETH management interface in the TOE will be accessed only through an independent local network. This network will be separated from the networks that use the other ETH interfaces of the TOE.

ARCHITECTURE

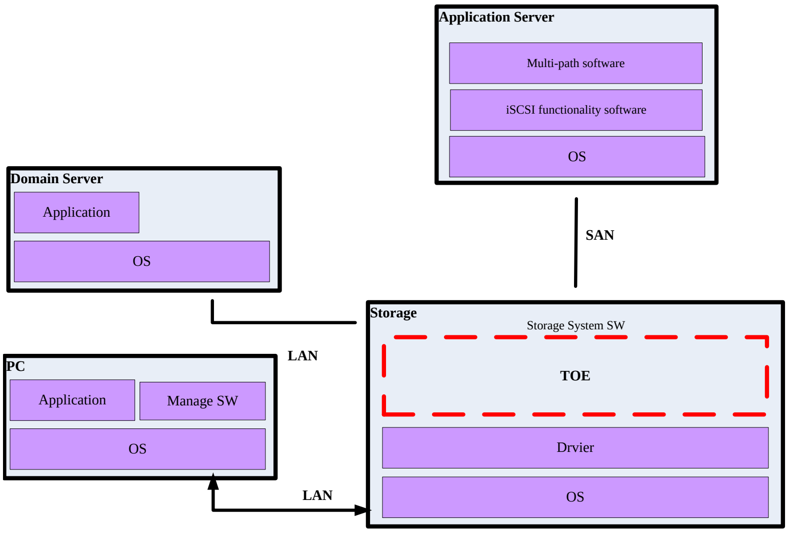
LOGICAL ARCHITECTURE

The TOE is a software-only TOE in charge of managing a Storage system. The following figure depicts the logical architecture on deployment showing the TOE boundary.



PHYSICAL ARCHITECTURE

The next figure illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.



The physical component of the TOE is the Storage System software:

- The TOE is installed in the Storage Server product and delivered to the customer site.
- The format of the software parts of TOE is a binary software package which contains the storage system software.

DOCUMENTS

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

- OceanStor S2200T & S2600T & S5500T & S5600T & S5800T & S6800T_V100R005_07_en_3118G2D8.hdx
- Huawei OceanStor T Serials Test Environment Buliding.doc (last version).
- Storage Controller Software Upgrade Guide 01.chm

PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification, the SFRs description included in [ST], and the subsystems defined in the TOE design documentation.

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 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 security target [ST].

PENETRATION TESTING

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 does NOT present exploitable vulnerabilities under the environment defined in the security target [ST]. All identified vulnerabilities can be considered closed if the TOE is installed and operated according to the security target [ST] and related documentation. The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. No attack scenario with the attack potential “Basic” has been successful in the TOE’s operational environment as defined in the security target [ST] when all measures required by the developer are applied.

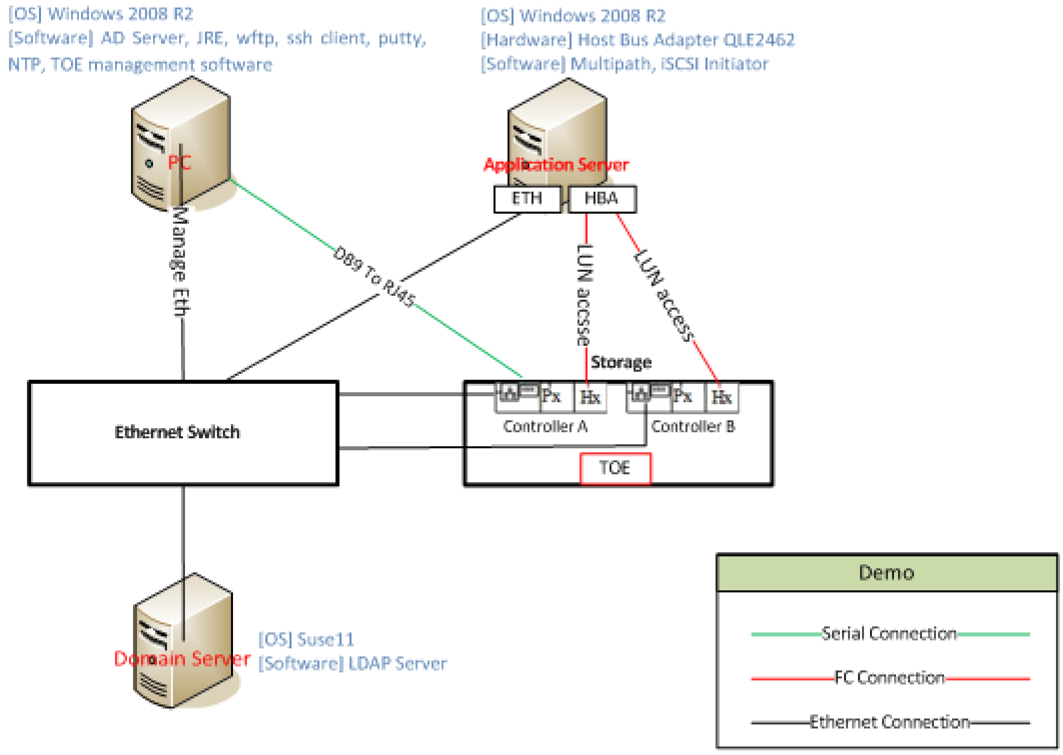
EVALUATED CONFIGURATION

The TOE is defined by its name and version number:

- Huawei OceanStor T&SX900 Series Storage System Software, version V100R005C30SPC300

To set up the TOE in a way consistent to the evaluated configuration and the operational environment defined in the security target [ST], users must follow the steps included in the installation and operation manuals (see section DOCUMENTS).

The deployed configuration for the evaluation is presented in the following figure:



EVALUATION RESULTS

The product “Huawei OceanStor T&SX900 Series Storage System Software, version V100R005C30SPC300“ has been evaluated against the “Huawei OceanStor T&SX900 Series Storage System Security Target, v3.5,13/08/2015”.

All the assurance components required by the evaluation level EAL3 + ALC_CMC.4 + ALC_CMS.4 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL3 + ALC_CMC.4 + ALC_CMS.4, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. Nonetheless, the following usage recommendations are given:

- The management network shall be a secure network, free of attackers.

- The fulfilment of the assumptions within indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.
- It is very important the adequate fulfilling of the installation procedures; the installation procedure may be vulnerable if those procedures are not followed.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product “Huawei OceanStor T&SX900 Series Storage System Software, version V100R005C30SPC300”, 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
SFR	Security Functional Requirement
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

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, R4 Final, Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, Sept. 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, Sept. 2012.

[ST] Huawei OceanStor T&SX900 Series Storage System Security Target, v3.5

SECURITY TARGET

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

- Huawei OceanStor T&SX900 Series Storage System Security Target, v3.5. 13/08/2015.