REF: 2015-3-INF-1552 v2	Created by: CERT9
Target: Expediente	Revised by: CALIDAD
Date: 10.03.2016	Approved by: TECNICO

CERTIFICATION REPORT

File: 2015-3 SolidFire NetApp, Inc. Element OS 8

Applicant: 770307520 NetApp Inc

References:

[EXT 2683] Certification request of SolidFire NetApp, Inc. Element OS 8

[EXT 2884] Evaluation Technical Report of SolidFire NetApp, Inc. Element OS 8.

The product documentation referenced in the above documents.

Certification report of the product “NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Version 8.0.1.2”, as requested in [EXT-2683] dated 11/02/2015, and evaluated by the laboratory Epoche & Espri S.L.U, as detailed in the Evaluation Technical Report [EXT-2884] received on 02/02/2016.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TABLE OF 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**
THREATS 7
OPERATIONAL ENVIRONMENT FUNCTIONALITY 8
ARCHITECTURE **8**
LOGICAL ARCHITECTURE 8
PHYSICAL ARCHITECTURE 9
DOCUMENTS **9**
PRODUCT TESTING **9**
PENETRATION TESTING 10
EVALUATED CONFIGURATION **10**
EVALUATION RESULTS **12**
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM **12**
CERTIFIER RECOMMENDATIONS **13**
GLOSSARY **13**
BIBLIOGRAPHY **14**
SECURITY TARGET **14**

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product "NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Version 8.0.1.2".

The TOE is a software-only TOE (SolidFire Element OS 8) running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes. It is an OS running on SolidFire's storage and FC nodes that provides data protection, storage management, and block storage services for the SolidFire Storage System.

Developer/manufacturer: NetApp, Inc.

Documentary evidences developed by Corsec Security, Inc.

Sponsor: NetApp, Inc.

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 – EAL2+ (ALC_FLR.2).

Evaluation end date: 02/02/2016.

All the assurance components required by the evaluation level EAL2+ (augmented with ALC_FLR.2 Flaw reporting procedures) 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 EAL2 + ALC_FLR.2, 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 "NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Version 8.0.1.2", a positive resolution is proposed.

TOE summary

The software only TOE is Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes. It is an OS running on NetApp's SolidFire storage and FC nodes that provides data protection, storage management, and block storage services for the SolidFire Storage System.

TOE major security features

The TOE is designed for large scale IT infrastructures and multi-tenant environments and it implements several key security features:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- Account (tenant) isolation – Storage is provisioned by way of volumes accessed over a storage network via iSCSI. An account is assigned to every volume. This enables iSCSI clients, or initiators, with the proper CHAP account credentials to access associated volumes. Volumes may also be accessed by both iSCSI and FC clients alike with the use of volume access groups (VAGs). In this case, CHAP credentials are not required as specific mappings between IQNs25/WWPNs and volumes, made by authorized administrators, dictate access.
- Management via the Web UI and API with RBAC – Administrators are restricted to security functions and TSF data based on their role(s).
- Multiple authentication mechanisms – Both local and LDAP authentication can be configured to identify and authenticate administrators at the Web UI and API. Every API call whether direct, e.g., via scripting, or over the Web UI requires successful authentication.
- Storage access controls – Both CHAP authentication and VAGs can be configured for storage access control. Both unidirectional and bi-directional CHAP authentication is supported.
- Data protection and fault tolerance – SolidFire's Helix data protection technology protects against user data errors and hardware failures. In addition, a suite of self-tests provide added assurance that the TOE is operating correctly.
- Auditing – Event records are created for every successful API call (excluding read-only calls, i.e., Get and List methods) and all failed API calls. Every "APIEvent" record identifies the user making the call. Event records are also generated for system level events.
- Snapshots – Snapshots of volumes and volume groups can be created to preserve a point-in-time copy of one or more volume's metadata. These snapshots can be used to roll back a volume to restore it to a desired point-in-time.
- Security attribute and TSF data management – cluster-wide configuration details and other cluster-level metadata are stored in a distributed database. The distributed database is stored independently on all nodes in the cluster. A subset of three or five cluster nodes (dependent on cluster size) is elected as voting members of the distributed database. These voting member nodes are known as the database ensemble.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidences required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.2 Flaw reporting procedures, 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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

	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.2 Security-enforcing functional specification ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.2 Use of a CM system ALC_CMS.2 Parts of the TOE CM coverage ALC_DEL.1 Delivery procedures ALC_FLR.2 Flaw reporting procedures
ATE: Tests	ATE_COV.1 Evidence of coverage 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 ACF.1 ROL.1 SDI.2
FIA	ATD.1 UAU.2 UAU.5 UAU.7 UID.2 USB.1

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

FMT	MOF.1 MSA.1 MSA.3 MTD.1 SMF.1 SMR.1
FPT	FLS.1 STM.1
FRU	FLT.2
TOA	TST.1

IDENTIFICATION

Product: "NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Version 8.0.1.2"

Security Target: "NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Security Target, Version 1.7, March 2016"

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R4 – EAL2+ (ALC_FLR.2).

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.NETWORK The TOE environment provides the network infrastructure required for management and storage traffic.
- A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.
- A.LOCATE The TOE, the storage nodes, storage clients, switches, storage and management networks, firewall, and NTP and LDAP servers are located within a controlled access facility.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- A.PROTECT The TOE software will be protected from unauthorized modification.
- A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- A.NOEVIL The administrator users with Administrator privileges who manage the TOE are non-hostile, appropriately trained, and follow all guidance. Administrators will never accept unknown/untrusted certificates for the web communication with the TOE.
- A.ADMIN_PROTECT No malicious software is installed or running on the administrator workstation.

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:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE administrator users: Users in charge of administration of the TOE that have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- FC and iSCSI clients: Users of the TOE functionality that have access to the TOE and could attempt to bypass its protection mechanisms for access to another user's data.

All users are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Both the confidentiality and integrity of the data must be protected. The threats defined are:

- T.DATA_CORRUPTION. Data could become corrupted or security functionality compromised due to hardware failure or incorrect system access by FC and iSCSI clients or attackers.
- T.UNAUTH. An administrator with Reporting privileges may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.
- T.UNINTENDED_ACCESS. An attacker and user of the TOE functionality (FC and iSCSI client) could access SolidFire volumes they are not authorized to access.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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.

IT Security Objectives that are to be satisfied by the environment:

- OE.TIME. The TOE environment must provide reliable timestamps to the TOE.
- OE.PROTECT. The TOE environment must protect itself and the TOE from external interference or tampering.
- OE.NETWORK. The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
- OE.SSH_PROTECT. The SSH interface to the TOE is inaccessible as it is restricted by a firewall protecting the management and client networks.
- OE.ADMIN_PROTECT. The administrator workstation must be protected from any external interference or tampering.

Non-IT Security Objectives that are to be satisfied without imposing technical requirements on the TOE:

- OE.MANAGE: sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system and its environment are used securely.
- OE.PHYSICAL: the physical environment must be suitable for supporting a computing device in a secure setting.

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE is an OS running on SolidFire's storage and FC nodes that provides data protection, storage management, and block storage services for the SolidFire Storage System.

The TOE is preinstalled on the SolidFire storage and FC nodes and is intended to be deployed in a secure data center that protects physical access to the TOE.

The TOE is deployed as part of a distributed system made up of a cluster of nodes, each running Element OS 8.0.1.2 and communicating over the Cluster network. A cluster can be any combination of 4-100 storage nodes and, if needed, 2 FC nodes (six in the case of the evaluated configuration). The TOE is supported on the following SolidFire nodes:

- SF2405

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- SF4805
- SF9605
- FC0025

PHYSICAL ARCHITECTURE

The TOE is Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes.

Element OS 8 is a single binary that is pre-installed on each of the storage and FC nodes shipped to a customer. The same binary is pre-installed on each node supported by the TOE.

DOCUMENTS

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

- SolidFire Storage Node Getting Started Guide, P/N SOE-509-1150-02, REV A
- SolidFire Fibre Channel FC0025 Node - Getting Started Guide, P/N SOE-509-1150-03, REV B
- SolidFire Element 8.0 Release Notes, 06/18/2015
- SolidFire Element 8.0 User Guide, 06/10/2015
- SolidFire Element 8.0 API Reference Guide, 06/10/2015
- Configuring SolidFire on Windows for Element OS, Version:2.2, 8/10/2015
- Configuring SolidFire on Linux for Element OS, Version 2.2, 8/10/2015
- Configuring SolidFire Fibre Channel, Version: 2.0, 07/30/2015
- Best Practices for Networking with SolidFire Storage Systems, Version: 2.0.0.1, 6/11/2014
- Configuring VMware vSphere for Element OS, Version: 2.3, 5/18/2015
- SolidFire, Inc. Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes v8.0.1.2 Guidance Documentation Supplement v1.4

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].

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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:

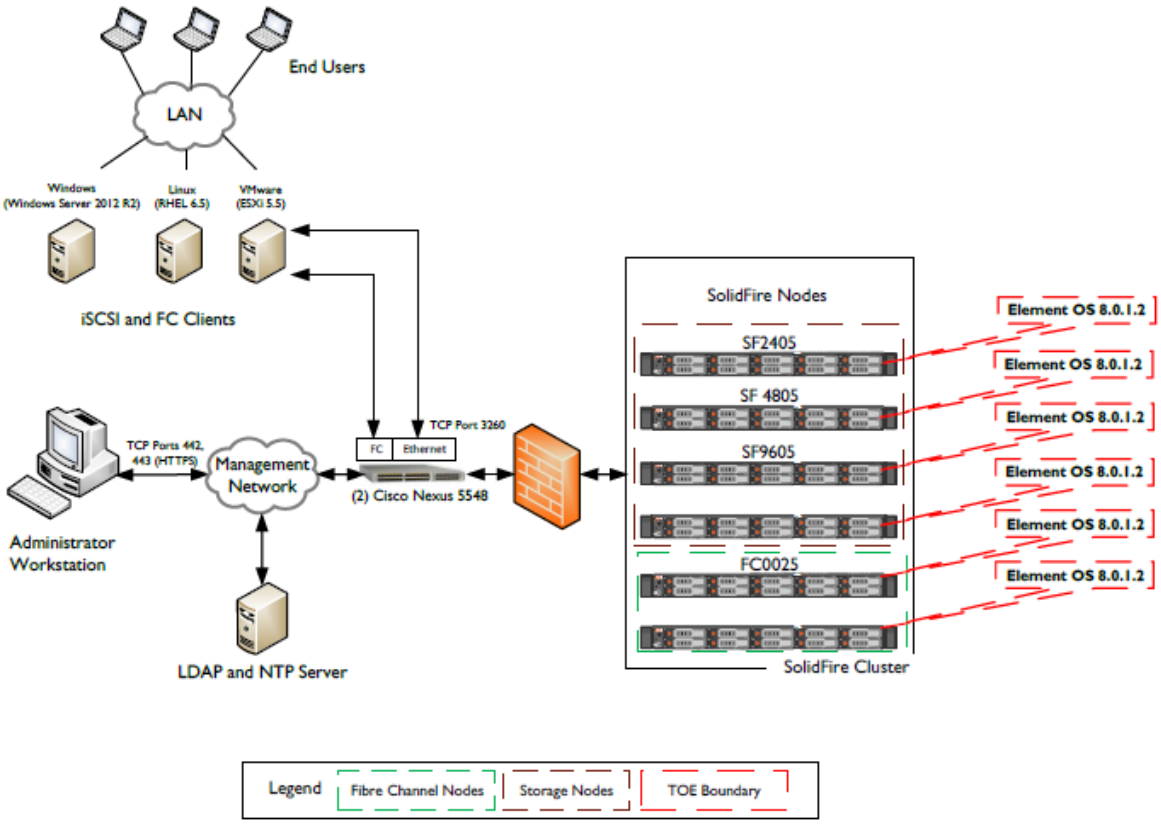
- “NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Version 8.0.1.2”

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:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es



There are four networks in the deployment configuration of the TOE: a 10 GbE network is used for iSCSI connections to clients (Storage network) and intracluster communication (Cluster network); a 1GbE management network (internal) is used for management of the TOE via the Web UI or API (Management network); and a FC storage network is used for FC connections (FC network). In the evaluated configuration, two Cisco Nexus 5548 switches are used to provide network connectivity; however other switches that meet the guidelines specified in SolidFire Best Practices for Networking with SolidFire Storage Systems are supported.

The cluster is presented to iSCSI and FC clients as virtual storage. A highly available storage VIP (SVIP) is the single point of access for all initial iSCSI connections. The SVIP is logically located on a node identified as a “cluster master”. The node holding the cluster master role can change as a cluster operates. Upon this initial iSCSI connection to the SVIP, the cluster master sends an iSCSI redirect back to the client indicating a specific node’s storage IP (SIP) that the client will use going forward for storage traffic to that specific volume.

The iSCSI and FC clients typically serve application-specific functions, e.g., hypervisor, web server, database server, mail server, file server, etc. End-user systems connect to the iSCSI and FC clients, which are located in a controlled access facility along with the TOE, through well-defined protocols. For example, an end-user accessing an iSCSI client serving as a web server may access the client

ENAC
CERTIFICACIÓN
Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

via a secure channel such as HTTPS. The end-users systems connect to the clients via an Ethernet LAN. Sites deploying the TOE must ensure that the client systems are secured according to industry best practices. Communications between end-users and iSCSI and FC clients must be authenticated and encrypted.

The cluster master is also assigned a management VIP (MVIP), which is used to access a cluster over the Web UI for cluster-level management. This is done by entering the MVIP in a web browser on an administrator workstation. Each node also has a limited UI (called the Node UI) and a node-level API that listens on a separate port (442) accessible by the individual node's management IP address (MIP). An attempt to access the cluster-level Web UI or API on an individual node's MIP will redirect the browser to the cluster's MVIP.

A Text User Interface (TUI) accessible only via a directly connected console is used to initially configure nodes and establish a cluster (i.e., initial system deployment) but is excluded from further use in the evaluated configuration.

An LDAP and NTP server provide LDAP authentication and cluster time synchronization, respectively.

EVALUATION RESULTS

The product "NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Version 8.0.1.2" has been evaluated against the "NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Security Target, Version 1.7, March 2016".

All the assurance components required by the evaluation level EAL2 + ALC_FLR.2 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 EAL2 + ALC_FLR.2, 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:

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- The fulfilment of the assumptions within indicated in the security target [ST] 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

The original applicant/developer in this certification process “SolidFire”, was acquired by the company “NetApp, Inc.” as of early this year. The vendor requested after the hearing prior to the resolution a change of the formal vendor name from “SolidFire, Inc”. to “NetApp, Inc.”, changing therefore the name of the TOE.

For this case, where we have the developer being acquired, and then the product name has changed at this late stage of the certification process, the vendor has declared that, no aspects of ALC compliance and procedures have been modified at all (i.e., the product is been developed as evaluated) and no product CM procedures have been altered, (i.e., the TOE versioning has been maintained, and only the product name has been updated).

The vendor has upgraded the security target to version 1.7. This has been reviewed to verify that only the TOE name and the vendor name have been modified.

Considering the obtained evidences during the instruction of the certification request of the product “NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Version 8.0.1.2”, 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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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] NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Security Target, Version 1.7, March 2016

SECURITY TARGET

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

NetApp, Inc. SolidFire Element OS 8 running on SF2405, SF4805, and SF9605 Storage Nodes and FC0025 Fibre Channel Nodes Security Target, Version 1.7, March 2016

C/ Argentona nº 20
Email: organismo.certificacion@cni.es