REF: 2016-18-INF-1809 v1	Created by: CERT10
Target: Expediente	Revised by: CALIDAD
Date: 08.06.2017	Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-18 HPE Network Node Manager i Premium Edition 10.21.402

Applicant: Hewlett Packard Enterprise Development LP

References:

[EXT-2871] Certification request.

[EXT-3373] Evaluation Technical Report v2.1.

The product documentation referenced in the above documents.

Certification report of the product HPE Network Node Manager i Premium Edition 10.21.402, as requested in [EXT-2871] dated 23/02/2016, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-3373] received on 04/04/2017.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product HPE Network Node Manager i Premium Edition 10.21.402.

The TOE is a network management solution that provides unified fault, availability, and performance monitoring for physical, virtual, hybrid, and cloud network environments.

Developer/manufacturer: Hewlett Packard Enterprise Development LP.

Sponsor: Hewlett Packard Enterprise Development LP.

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

ITSEF: Epoche & Espri S.L.U..

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 r4 - EAL 2 + ALC_FLR.2.

Evaluation end date: 04/04/2017.

All the assurance components required by the evaluation level EAL 2 (augmented with 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 EAL 2 + 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 HPE Network Node Manager i Premium Edition v10.21.402, a positive resolution is proposed.

TOE SUMMARY

HPE Network Node Manager i (NNMi) Premium Edition software is a highly-scalable, customizable network management solution that provides unified fault, availability, and performance monitoring for physical, virtual, hybrid, and cloud network environments. HPE NNMi Premium Edition consists of HPE NNMi and several HPE NNMi Smart Plug-in (SPI) add-on modules (also referred to as NNM4 iSPIs).

HPE NNMi is the core component of the network management solution. Its continuous spiral discovery automatically keeps network topology data accurate and up-to-date. Network events are automatically correlated and analysed for root cause to aid in identifying service impacting events. These features help to reduce downtime and increase network service levels for a managed network. A single HPE NNMi server scales up to 30,000 network devices (nodes). Network and device load are minimized with unified polling of fault, availability, and performance data using SNMP[6], ICMP[7], HTTPS[8], and Network Configuration Protocol (NETCONF)/SSH[9] communication protocols.

HPE NNMi's web-based graphical user interface (GUI), called the NNMi Console, provides a centralized operations and management console with workflow-based navigation and filtering (e.g., by incidents, nodes, paths, and metrics) for fast access to information. User roles and administrator configured user and security groups control access to node data and logically partition the network for security and multi tenancy capability.

There is also an SOA[10]-based web services API (referred to hereafter as the NNMi API) that allows for integrations with third-party software products as well as other HPE software products, like HPE Network Automation Software and HPE Operations Orchestration. An NNMi command-line interface (CLI) allows for automating administration activities.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL 2 and the evidences required by the additional component ALC_FLR.2, according to Common Criteria v3.1 r4.

ASE: Security Target Evaluation	ASE_INT.1. ST Introduction
	ASE.CCL.1. Conformance claims
	ASE_SPD.1. Security problem definition
	ASE_OBJ.2. Security objectives
	ASE_ECD.1. Extended component definition
	ASE_REQ.2. Derived security requirements
	ASE_TSS.1. TOE summary specification
ADV: Development	ADV_ARC.1. Security architecture
	ADV_FSP.2. Functional specification
	ADV_TDS.1. TOE design
AGD: Guidance documents	AGD_OPE.1. Operational user guidance
	AGD_PRE.1. Preparative procedures
ALC: Life cycle support	ALC_CMC.2. CM capabilities

	ALC_CMS.2. CM Scope
	ALC_DEL.1. Delivery
	ALC_FLR.2. Flaw remediation
ATE: Tests	ATE_COV.1. Coverage
	ATE_FUN.1. Functional tests
	ATE_IND.2. Independent testing
AVA: Vulnerability assessment	AVA_VAN.2. Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to Common Criteria v3.1 r4:

FAU: Security audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
FCS: Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
FDP: User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
FMT: Security management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
FPT: Protection of the	FPT_ITT.1	Basic internal TSF data transfer protection

TSF		
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

IDENTIFICATION

Product: HPE Network Node Manager i Premium Edition 10.21.402

Security Target: Hewlett Packard Enterprise Development LP HPE Network Node Manager i Premium Edition 10.21.402 Security Target, version 1.3. 28/03/2017.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 r4 - EAL 2 + ALC_FLR.2.

SECURITY POLICIES

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the [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.

Assumption 01: A.INSTALL

The TOE is installed on the appropriate dedicated hardware and operating system.

Assumption 02: A.NETCON

The TOE environment provides the network connectivity required to allow the TOE to perform its functions.

Assumption 03: A.TIMESTAMP

The IT environment provides the TOE with the necessary reliable timestamps.

Assumption 04: A.LOCATE

The TOE is located within a controlled access facility.

Assumption 05: A.PROTECT

The TOE software will be protected from unauthorized modification.

Assumption 06: A.MANAGE

There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.

Assumption 07: A.NOEVIL

TOE and OS administrators are non-hostile, appropriately trained, and follow all guidance.

Assumption 08: A.NPS_CONSOLE_PROTECT

TOE users and administrators will only access the NPS Console by starting it at the NNMi Management Server (TOE administrators only) or through SSO access to it via the NNMi Console.

Assumption 09: A.AGENT_PROTECT

Machines with SNMPv3/hypervisor agents located outside the controlled access facility are protected and no malicious software is running on them.

Assumption 10: A.USER_PROTECT

No malicious software is installed or running on the Administrator and TOE user workstations.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product HPE Network Node Manager i Premium Edition v10.21.402, although the agents implementing attacks have the attack potential according to the basic attack potential of EAL 2 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 categorized below.

Threat 01: T.DATA_COMPROMISE

An attacker may read, modify, delay, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.

Threat 02: T.INTERCEPT

The TOE may communicate with remote IT entities and TOE user, TOE administrator, and Web Services Client workstations that lie outside of the organization's trusted network. An attacker may attempt to intercept these communications in order to read or modify critical TSF data.

Threat 03: T.MASQUERADE

An attacker or process may masquerade as another entity to gain unauthorized access to data or TOE resources.

Threat 04: T.TAMPERING

An attacker or process may be able to bypass the TOE’s security mechanisms by tampering with the TOE or TOE environment.

Threat 05: T.UNAUTH

Attackers, TOE users, or Web Services Clients may gain access to user or TSF data on the TOE, even though they are not authorized in accordance with the TOE security policy.

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.

Environment objective 01: OE.NETWORK

The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.

Environment objective 02: OE.PLATFORM

The TOE hardware and OS must support all required TOE functions.

Environment objective NN: OE.PROTECT

The TOE environment must protect itself and the TOE from external interference or tampering.

Environment objective NN: OE.TIME

The TOE environment must provide reliable timestamps to the TOE.

Environment objective NN: OE.AGENT_PROTECT

Sites deploying the machines running the SNMPv3 and hypervisor agents will protect them from external interference or tampering. Administrators will ensure there is no malicious software running on them.

Environment objective NN: OE.USER_PROTECT

The Administrator and TOE user workstations must be protected from any external interference or tampering.

Environment objective NN: OE.MANAGE

Sites deploying the TOE will provide competent, non-hostile TOE and OS administrators who are appropriately trained and follow all administrator guidance. TOE and OS administrators will ensure the system is used securely.

Environment objective NN: OE.PHYSICAL

The physical environment must be suitable for supporting a computing device in a secure setting.

Environment objective NN: OE.AUTHORIZED_ACCESS

Only TOE and OS administrators are granted access to the controlled access facility in which the TOE is located

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- Trusted Path/Channels

PHYSICAL ARCHITECTURE

The TOE is HPE Network Node Manager i Premium Edition 10.21.402 that consists of three software components:

- HPE NNMi 10.21.402
- HPE NNM iSPI Performance for Quality Assurance 10.21.402

- HPE NNM iSPI Performance for Metrics 10.21.402

The TOE software runs on Windows or Linux physical or virtual platforms compliant with the minimum software and hardware requirements listed in the [ST].

DOCUMENTS

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

The Security Target: Hewlett Packard Enterprise Development LP HPE Network Node Manager i Premium Edition 10.21.402 Security Target, version 1.3. 28/03/2017.

The following guides are provided in PDF format, are downloaded from HP's support website at https://softwaresupport.hp.com/, and are required reading and part of the TOE. Although the titles of the guidance documentation make reference to 10.20, they are also applicable to the TOE version 10.21.402.

- HPE Network Node Manager i Software, Software Version: 10.20, for the Windows and Linux operating systems, Deployment Reference, June 2016
- HPE Network Node Manager i Software, Software Version: 10.20, Windows and Linux operating systems, Online Help: Help for Administrators, June 2016
- HPE Network Node Manager i Software, Software Version: 10.20, Windows and Linux operating systems, Online Help: Help for Operators, June 2016
- HPE Network Node Manager i Software, Software Version: 10.20, Windows and Linux operating systems, Online Help: Using the Console, June 2016
- HPE Network Node Manager i Software, For the Windows and Linux operating systems, Software Version: 10.20, Reference Pages, July 2016
- HPE Network Node Manager i Software Premium Edition, Software Version: 10.20 , for the Windows and Linux operating systems, Release Notes, July 2016
- HPE Network Node Manager i Software Premium Edition, Software Version: 10.20, for the Windows and Linux operating systems, Support Matrix, July 2016
- HPE Network Node Manager i Software Read me first, July 2016
- HPE Network Node Manager iSPI Performance for Quality Assurance Software For the Windows and Linux operating systems, Software Version: 10.20, Online Help, June 2016
- HPE Network Node Manager iSPI Performance for Quality Assurance For the Windows and Linux operating systems, Software Version: 10.20, Deployment Reference, June 2016

- HP Network Node Manager iSPI Performance for Quality Assurance Software Version: 10.20, for the Windows and Linux operating systems, Reference Pages, November 2015
- HPE Network Node Manager iSPI Performance for Metrics Software For the Windows and Linux operating systems, Software Version: 10.20, Online Help, July 2016
- HPE Network Node Manager iSPI Performance for Metrics For the Windows and Linux operating systems, Software Version: 10.20, Deployment Reference, July 2016
- HPE Network Node Manager iSPI Performance for Metrics Read me first, July 2016
- HPE Network Node Manager I Software, Software Version: 10.20 for the Windows and Linux operating systems, Hardening Guide, August 2016.

The following guides are provided in HTML format and are required reading and part of the TOE:

- HPE Network Node Manager i Software (NNMi) Device Support Matrix, Software Version: 10.20, Last Updated: 07/26/2016
- HPE Network Node Manager i Software Interactive Installation and Upgrade Guide, July 2016.
- HPE Network Node Manager iSPI Performance for Quality Assurance Interactive Installation and Upgrade Guide, July 2016
- HPE Network Node Manager iSPI Performance for Metrics Interactive Installation and Upgrade Guide, July 2016

PRODUCT TESTING

The main objective of the tests performed by the evaluator is to check that the security functional requirements in [ST13] are implemented as expected, that the subsystems defined behave as expected, and that the TSFIs definitions are consistent with the TOE.

The evaluator has chosen a subset of tests and an appropriate strategy for the TOE delivered by the developer. The documentation of the vendor describes the complete behaviour of the TSFIs and subsystems. The evaluator has built a set of test cases, considering documentation and knowledge acquired during the evaluation.

The evaluator has designed a set of tests following a suitable strategy for the

TOE type taking into account:

1. All SFRs have been tested whether through TSFIs excitation or subsystem interactions checking.

2. Increasing test coverage of each interface varying the input parameters: search for critical parameters in the TSFIs interactions, incorrect behaviour suspicion with specific input values;
3. Selecting TSFIs to be tested based on:
   - Developer tests rigor;
   - Developer test results including those TSFIs and subsystems which tests results are not reliable;
   - Importance of the TSFIs and subsystems
   - Types of TSFIs and subsystems
   - Number of TSFIs and subsystems.

To choose the tests, the evaluator has used as criteria: search for critical parameters in the TSFIs and subsystems interactions, requirements used by the interfaces, exhaustive tests over the most important TSFIs and subsystems, incorrect behaviour suspicion with specific input values and the performance of testing in the most important TSFIs and subsystems, interactions between the subsystems, and the interactions between interfaces and subsystems.

Moreover, the evaluator has carried out tests with parameters of the TSFIs and subsystems that could have special importance in the maintenance of the TOE security. The evaluator has designed his TSFIs and subsystems independent test cases including all the security requirements defined in [ST].

The evaluator testing plan is SFR oriented, and the functionality of each SFR included at the security target has been considered.

During the testing plan execution, the evaluator has checked that some SFRs on previous ST versions did not define TOE's real operation and have been updated.

All the test cases have been performed using the external interfaces that allow testing appropriately both the SFRs and the subsystems (including TSFIs).

EVALUATED CONFIGURATION

Figure 1 shows the evaluated configuration of the TOE that consists of a Global Network Management deployment.

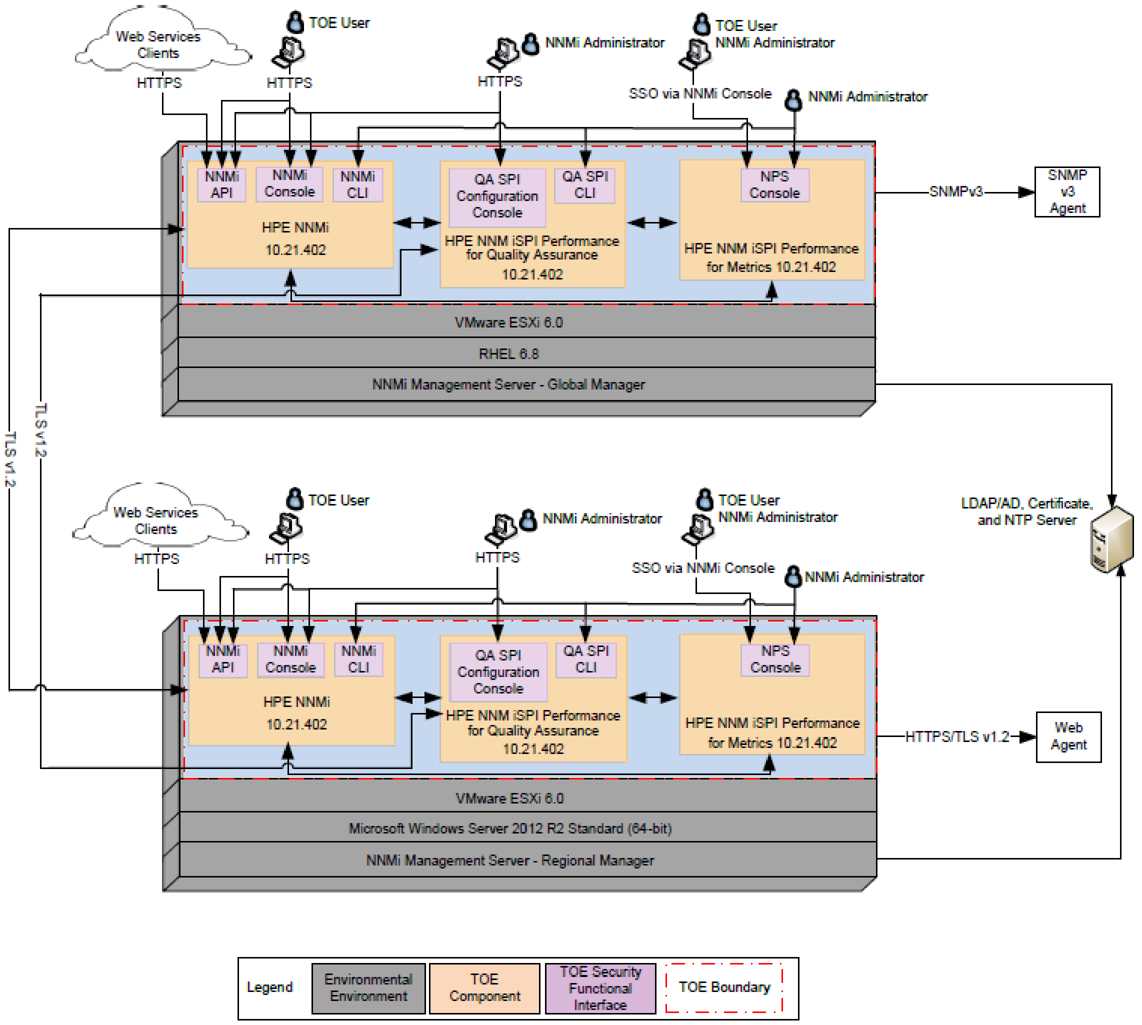

Figure 1 Evaluated Configuration of the TOE

In the evaluated configuration shown in Figure 1, the TOE is configured as both a Global and Regional Manager. Both the Global and Regional Manager are running all of the TOE components on a single virtual machine (VM) provided by VMware ESXi 6.0 with the minimum hardware requirements listed in the [ST]; however they are configured for Linux and Windows, respectively. More specifically, the Global Manager OS is RHEL 6.8 whereas the Regional Manager OS is Microsoft Windows Server 2012 R2 Standard (64-bit). The TOE binaries, which are specific to each OS, are downloaded from HP’s support website at https://softwaresupport.hp.com/ as both zip and tar files.

The TOE includes patches that update the version 10.20 of each component to 10.21.402. The TOE binaries for RHEL 6.8 are listed below:

- HPE NNMi 10.20 – TB768-15009.tar.gz

- HPE NNM iSPI Performance for Quality Assurance 10.20 – TB759-15035.tar.gz
- HPE NNM iSPI Performance for Metrics 10.20 – TB771-15021.tar.gz
- V10.21.402 software patches for each component:
    - HPE NNMi 10.21.402 – NNM1020L_00001.rpm
    - HPE NNM iSPI Performance for Quality Assurance 10.21.402 – QA1020L_00001.rpm
    - HPE NNM iSPI Performance for Metrics 10.21.402 – NPS1020L_00001.rpm

The TOE binaries for Microsoft Windows Server 2012 R2 Standard (64-bit) are listed below:

- HPE NNMi 10.20 – TB765-15017.zip
- HPE NNM iSPI Performance for Quality Assurance 10.20 – TB759-15034.zip
- HPE NNM iSPI Performance for Metrics 10.20 – TB771-15020.zip
- V10.21.402 software patches for each component
    - HPE NNMi 10.21.402 – NNM1020W_00001.msi
    - HPE NNM iSPI Performance for Quality Assurance 10.21.402 – QA1020W_00001.msi
    - HPE NNM iSPI Performance for Metrics 10.21.402 – NPS1020W_00001.msi

The Global Manager receives and displays node data from the Regional Manager. The Regional Manager collects data from managed network devices (i.e., devices with agents26 on them) and forwards it to the Global Manager based on administrator-configured forwarding filters. The Global Manager also independently collects data from managed network devices. All communication to the managed network devices is secured using SNMPv3 and TLS sockets. The following managed network devices are included in the TOE environment of the evaluated configuration:

- Net-SNMP for Linux, which provides a SNMPv3 agent that responds to SNMPv3 protocol requests from the TOE. The Global Manager is connected to one of these SNMPv3 agents as shown in Figure 1.
- ESXi hypervisor, which includes a web agent that responds to HTTPS protocol requests from the TOE. The Regional Manager is connected to one of these web agents as shown in Figure 1.

Access to the TOE's NNMi and QA SPI Configuration consoles and NNMi API is provided through encrypted HTTPS connections. The NNMi and QA SPI CLIs and the NPS Console may be accessed locally by NNMi Administrators. In the evaluated configuration, TOE users have no access to the CLIs and only access the NPS Console via SSO from the NNMi Console.

Both Global and Regional Managers are on the same domain and share an LDAP/AD server in the TOE environment to provide LDAP authentication and store user security attributes. Communication to the LDAP/AD server is secured through TLS v1.2. The LDAP/AD server is configured to provide NTP for reliable system time for the TOE.

EVALUATION RESULTS

The product HPE Network Node Manager i Premium Edition10.21.402 has been evaluated against the Security Target: Hewlett Packard Enterprise Development LP HPE Network Node Manager i Premium Edition 10.21.402 Security Target, version 1.3. 28/03/2017.

All the assurance components required by the evaluation level EAL 2 + 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 EAL 2 + ALC_FLR.2, as defined by the Common Criteria Version 3.1, R4 and the [CEM].

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.

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

- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product HPE Network Node Manager i Premium Edition v10.21.402, 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
TSFi	TOE Security functional 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] Hewlett Packard Enterprise Development LP HPE Network Node Manager i Premium Edition 10.21.402 Security Target, version 1.3. 28/03/2017.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: Hewlett Packard Enterprise Development LP HPE Network Node Manager i Premium Edition 10.21.402 Security Target, version 1.3. 28/03/2017.

There isn't a Security Target lite-version available for this certification.