REF: 2013-29-INF-1492 v1	Created by: CERT10
Target: Expediente	Revised by: CALIDAD
Date: 16.07.2015	Approved by: TECNICO

CERTIFICATION REPORT

File: 2013-29 Aunav NEXT Explosives Disposal Robot

Applicant: B651137267 Proytecsa Security S.L.

References:

[EXT-2328] Certification request of Aunav NEXT Explosives Disposal Robot

[EXT-2775] Evaluation Technical Report of Aunav NEXT Explosives Disposal Robot.

The product documentation referenced in the above documents.

Certification report of the product aunav.NEXT, version 1.0, as requested in [EXT-2328] dated 27/09/2013, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-2775] received on 29/05/2015.

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

TABLE OF CONTENTS

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product aunav.NEXT.

The TOE is an articulated and extensible robot fitted with controls and intelligent handling that allows performing functions of reconnaissance, identification, and removal of any type of device or threat detected, especially the ones that are explosives. Its control system is remote so system operators are kept at a totally safe work distance.

Developer/manufacturer: PROYTECSA SECURITY S.L.

Sponsor: PROYTECSA SECURITY S.L.

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. EAL2 + ALC_FLR.1.

Evaluation end date: 29/05/2015.

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.1) 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.1, as defined by the [CC_P3] and the [CEM].

Considering the obtained evidences during the instruction of the certification request of the product aunav.NEXT v1.0, a positive resolution is proposed.

TOE SUMMARY

The TOE is an articulated and extensible robot fitted with controls and intelligent handling that allows performing functions of reconnaissance, identification, and removal of any type of device or threat detected, especially the ones that are explosives. Its control system is remote so system operators are kept at a totally safe work distance.

The TOE provides Security mechanisms to guarantee that only personnel duly authorized can use the TOE. The security characteristics are:

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

- Authentication: It is not possible to take any action with the TOE thru the communication RF and BT channels without previous authentication.
- Encrypted RF communication channel with secure protocols: The Security of the communications of the management console of the TOE (Remote Case Controller), is ensured with the implementation of the encrypted secure protocol AES-128 ECB.
- Service priority in the access with RF: data and orders sent thru the remote case controller have preference in the communication with the TOE.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.1, according to Common Criteria v3.1 R4.

Classes	Components
ADV Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 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
ASE Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definitions
	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
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

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

SECURITY FUNCTIONAL REQUIREMENTS

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

TOE Security Functional Requirements	Description
FIA_UAU.2/BT	User authentication before any action
FIA_UAU.2/RF	User authentication before any action
FCS_COP.1/RF	Cryptographic operation
FRU_PRS.1	Limited priority of service

IDENTIFICATION

Product: aunav.NEXT v1.0

Security Target: aunav.NEXT Security Target v1.0. 16/04/2015.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R4. EAL2 + ALC_FLR.1.

SECURITY POLICIES

The use of the product Aunav NEXT Explosives Disposal Robot v1.0 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. In short, it establishes the need of implementing organisational policies related to the following aspects.

Policy 01: P.PRIORITY

The data and commands sent thru the remote case controller have preference in communications with the TOE, over the ones sent thru the Bluetooth control.

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

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.

Assumption 01: AS.PERSONNEL

It is supposed that the users of the TOE behave according to expectations and do no act maliciously.

Assumption 02: AS.PHYSICAL

it is presumed that there is no physical access to the TOE, that it is protected by appropriate security measures to guarantee the access only to authorized personnel. The same way, the gamepad and the ROBOT remote case controller are presumed protected. This makes the attacks through them not possible as not being accessible by attackers.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Aunav NEXT Explosives Disposal Robot v1.0, although the agents implementing attacks have a basic attack potential according to the assurance level EAL2 + ALC_FLR.1 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.COMM_RF

One attacker impersonates the control suitcase and takes over the control of the TOE or eavesdrops upon its communications.

Threat 02: T.COMM_BT

One attacker impersonates the Bluetooth control and takes over the TOE control.

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.

Environment objective 01: OE.PERSONNEL

The environment of operation of the TOE has to guarantee that the TOE operators behave as expected and not maliciously.

Environment objective 02: OE.PHYSICAL

The operation environment of the TOE has to warranty the impossibility of physical access to the TOE, the Bluetooth control and the robot remote case controller.

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 TOE logical scope is defined grouping functionalities in the following functional classes:

- **Authentication of the communication channels**

  The authentication of the Bluetooth channel is given by the knowledge of the authentication key established in the pairing between PS3 Gamepad and the TOE according to the Bluetooth protocol, being impossible to perform any action on the TOE without knowing that key.

  The authentication in the RF channel is given by the knowledge of the encryption key used to communicate, being impossible to perform any action on the TOE without knowing that key.

- **Protection of communication channels**

  The ROBOT encrypts the RF communication channel. The security of the communications with the TOE from the control case, are ensured with the implementation of the encrypted secure protocol AES-128 ECB. The encryption password is configured during the manufacture process and is not changed nor destructed during the operation.

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

PHYSICAL ARCHITECTURE

The Physical scope of the TOE is summarized in the following table:

Name	Type	Description
aunav.NEXT Hardware The robot is distributed with the software pre-installed.	Hardware	Robot hardware
aunav.NEXT Software Pre-installed in hardware.	Software	Software that is executed on robot hardware
Preparation manual. Distributed on CD.	Document	Manual used to install TOE and prepare the operational environment in a secure way
Operation Manual Distributed on CD.	Document	Manual used to operate TOE in a secure way

DOCUMENTS

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

- aunav.NEXT Security Target v1.0. 16/04/2015.
- Preparation manual (distributed on CD).
- Operation manual (distributed on CD).

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.
During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

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

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The TOE is distributed in one unique version submitted to evaluation. For the operation of the product Aunav NEXT Explosives Disposal Robot v1.0 it is necessary the disposition of the corresponding robot hardware and the pre-installed software that is executed in that hardware.

EVALUATION RESULTS

The product Aunav NEXT Explosives Disposal Robot v1.0 has been evaluated against the Security Target: aunav.NEXT Security Target v1.2, 16/04/2015.

All the assurance components required by the evaluation level EAL2 + ALC_FLR.1 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.1, as defined by the [CC_P3] 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

- A verification of a correct communication must be performed before using the TOE between the control suitcase and the TOE in order to mitigate possible disconnection during the operation.
- It is essential to use the TOE strictly under the assumptions for the environment appearing in the security target.
- The necessary setup configuration for the establishment of the RF and BT channels (which includes the cipher key among others parameters) must be performed in a trusted environment to avoid the attackers to access to that setup configuration.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Aunav NEXT Explosives Disposal Robot v1.0, 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, R4, September 2012.

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

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

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

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

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: aunav.NEXT Security Target v1.2, 16/04/2015.

ENAC CERTIFICACIÓN Nº 45/C-PR110

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