REF: 2010-35-INF-627 V1
Distribution: Public
Date: 18.04.2011

Created: CERT3
Reviewed: TECNICO
Approved: JEFEAREA

CERTIFICATION REPORT FOR EADS AIR SEGMENT SYSTEMS PROTECTION PROFILE (ASS-PP), Issue B

Dossier: 2010-35 EADS AIR SEGMENT SYSTEMS PP Issue B

References:

- [EXT1108] Certification Request of EADS AIR SEGMENT SYSTEMS PP Issue B
- [EXT-1201] Evaluation Technical Report of EADS AIR SEGMENT SYSTEMS PP Issue B, 01.03.2011, Ed. 1.0, CESTI-INTA

Certification report of EADS AIR SEGMENT SYSTEMS PROTECTION PROFILE ISSUE B, as requested by EADS-CASA in [EXT-1108] dated 13-12-2010, and evaluated by the laboratory CESTI-INTA, as detailed in the Evaluation Technical Report [EXT-1201] received on March 8th 2011, and in compliance with CCRA and SOGIS for components up to EAL4.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Table Of Contents

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

SUMMARY

This document constitutes the Certification Report for the protection profile “EADS AIR SEGMENT SYSTEMS”, Issue B, developed by EADS-CASA.

Developer/manufacturer: EADS-CASA

Sponsor: EADS-CASA

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

ITSEF: CESTI-INTA

Protection Profile: -

Evaluation Level: CC v3.1 r3 EAL3.

Evaluation end date: 01/03/2011.

All the assurance components required by the level EAL3 have been assigned a “PASS” verdict. Consequently, the laboratory (CESTI-INTA) assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

Considering the obtained evidences during the instruction of the certification request of the EADS AIR SEGMENT SYSTEMS PROTECTION PROFILE, Issue B, a positive resolution is proposed.

PP Summary

Air Segment Systems are these systems used by the aircraft crew or by the aircraft computers and sensors to store, record or manage information during mission.

This TOE reference to a military-purpose Air Segment Systems which allows to fly the aircraft, to manage the mission data and to use data links.

Security Assurance Components

The protection profile was evaluated with all the evidence required to fulfil EAL3, according to CC Part 3 [CC-P3].

Assurance Class: Protection Profile Evaluation (APE)

Assurance Components:

- APE_CCL.1
- APE_ECD.1
- APE_INT.1
- APE_OBJ.2
- APE_REQ.2
- APE_SPD.1

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Security Functional Components

The security functional components contained in this PP are based on the components in [CC-P2]. The functional components satisfied by the protection profile are:

- FAU_GEN.1 Audit Data Generation
- FAU_SAR.1 Audit review
- FAU_SAR.2 Restricted audit review
- FCS_CKM.4 Cryptographic key destruction
- FCS_COP.1 Cryptographic operation
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_IFC.1 Subset information flow control
- FDP_IFF.1 Simple security attributes
- FDP_ITC.1 Import of user data without security attributes
- FDP_RIP.1 Subset residual information protection
- FDP_UCT.1 Basic data exchange confidentiality
- FDP_UIT.1 Data exchange integrity
- FIA_UAU.1 Timing of authentication
- FIA_UAU.7 Protected authentication feedback
- FIA_UID.1 Timing of identification
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialisation
- FMT_SMF.1 Specification of management functions
- FMT_SMR.1 Security roles
- FPT_STM.1 Reliable time stamps

IDENTIFICATION

Protection Profile: EADS AIR SEGMENT SYSTEMS PROTECTION PROFILE, Issue B

Document no. : DT-T-MEP24-10002

Evaluation Level: CC v3.1 r3 EAL3

SECURITY POLICIES

The usage of the Protection Profile implies to implement some organizational policies that assure the commitment of different demands of security. The details

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

about them are included in the Protection Profile. In synthesis, the necessity settles down to implement the following organizational policies.

P.ACCOUNTABILITY

The users of the TOE shall be held accountable for their actions within the TOE.

P.AUTHORISED_USERS

Only those users who have been authorized access to information within the system may access the TOE.

P.NEED_TO_KNOW

The TOE must limit the access to, modification of, and deletion of the objects to those authorized users which have a “need to know” for that information. The access rights to specific data objects are determined by the owner of the object, the role of the subject attempting access, and the implicit and explicit access rights to the object granted to the role by the object owner.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

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

In order to assure the secure use of a product compliant with this protection profile, 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 product.

A.CLEARANCE

All persons requiring access to the Aircraft TOE which manage sensitive data shall have a clearance that dominates the protecting marking of that data, prior to any authorised access.

A.AUDIT_REVIEW

The ISM shall inspect the security audit and accounting log(s) on a regular and sufficiently frequent basis to detect any patterns of user behaviour that may be a threat to security.

A.CRYPTO_MANAGE

Information marked as ‘CRYPTO’ shall always be handled and stored in accordance with its Protective Marking and Caveat.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

A.INSTALL

All software or hardware installed in the Aircraft TOE equipment shall be subjected to rigorous configuration management procedures, stringent quality control and comprehensive testing.

A.PHYSICAL_ACCESS

In controlled areas and/or scenarios all personnel accessing the Aircraft where the TOE is located shall be reliably identified before access is granted.

A.TAMPER_SEALS

Tamper seals shall be fitted to Aircraft TOE equipment dependent on the design and as deemed necessary by the Security Accreditation Authority.

A.SYOPS

All users will be trained in accordance with their duties and will read, understand, and obey all the relevant Security Operating Procedures.

A.USER_CONFIDENCE

Privileged users shall be trusted not to abuse their privilege.

Threats

This section describes the security threats that are to be countered by the TOE, its operational environment, or a combination of the two.

T.CAPTURE

Hostile forces capture the equipment while combat, transport or accessing premises and steal information.

T.DATA_CORRUPTION

An attacker from inside or outside the organisation gains access to the equipment of the information system and corrupts or delete the sensitive information in an unauthorised manner.

T.EAVESDROPPING

Someone inside or outside the organisation connects a sniffer device to the network to store and analyse transmitted information.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

T.INFORMATION_THEFT

Someone inside or outside the organisation accessing digital media with the intention of stealing and using the information on them.

T.REMANANCE

An attacker recovers information from removed electronic media.

T.TELECOM_FAILURE

An attacker, through sabotage or disturbance of the telecom installation, gains access to the telecommunications equipment.

T.UNAUTHORIZED_USE

An attacker from inside or outside the organisation accesses the information system and uses one of its services to penetrate it, runs unauthorised operations or steal information.

T.UNTRUSTWORTHY_DATA

Outside sources send false data being used inside the organisation compromising the system.

Operational environment objectives

The TOE requires the cooperation from its operational environment to fulfil the requirements listed in the Protection Profile. This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. These security objectives are assumed by the Protection Profile to be permanently in place in the TOE environment. With this purpose, the security objectives declared for the TOE environment are the following.

O.E_ADMIN

Those responsible for the administration of the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.

O.E_AUDITDATA

Those responsible for the TOE must ensure that the audit functionality is used and managed effectively. In particular:

a) Procedures must exist to ensure that the audit trail for the product (i.e., all networked components containing an audit trail) is regularly analysed and archived, to allow retrospective inspection.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

b) The auditing system must be configured such that the loss of audit data is minimised upon planned or unplanned shutdown or lack of available audit storage.

c)The media on which audit data is stored must not be physically removable from the platform by unauthorised users.

O.E_AWARE

The personnel must be made accountable and informed of possible sanctions. The personnel must be made aware of the obligation of professional secrecy and discretion. The system user shall be informed about the accounting of their activities in the system.

O.E_INSTALL

Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are installed and configured in a secure manner.

O.E_LOCATE

While not flying or being transported, the operational environment must ensure that the TOE shall be located within controlled access facilities of the MOB which will prevent unauthorised physical access. The physical controls at the MOB will alert the system authorities to the physical presence of attackers within the controlled space where the TOE is located.

O.E_NO_KEYS_LEAK

To avoid sensitive data compromise the crypto keys must be correctly managed.

O.E_PROTECT

The operational environment must ensure that the TOE hardware and software critical to security policy enforcement shall be protected from unauthorised physical modification including unauthorised modifications by potentially hostile outsiders.

O.E_SECOP

Those responsible for the TOE must establish and implement procedures to ensure that the users will be trained in accordance with their duties and will read, understand, and obey all relevant Security Operating Procedures (SecOPs).

TOE ARCHITECTURE

The typical Air Mission Systems functionality is functionality related to:

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

- general purpose, which includes such hydraulic system; fuel system; etc. (excluded of the security problem)

- management, which includes flight control and management functions; navigation systems; etc.

- mission, which includes mission monitoring and control; payload management; data recorders; etc.

- communication, which includes dialog with traffic air control; interconnection with other allied aircrafts; etc.

Depending on the type of aircraft the TOE will need other software, in example, if the aircraft is a manned aircraft, the TOE could require operating systems as Microsoft Windows or Linux; or RDBMS as Microsoft SQL Server or Oracle. However if the aircraft is an unmanned aircraft it will require a RTOS.

DOCUMENTS

The protection profile is just one document identified as: “EADS AIR SEGMENT SYSTEMS PROTECTION PROFILE, Issue B”.

TOE TESTING

Not applicable.

TOE CONFIGURATION

Air Segment Systems are systems located in the aircraft and are used on-flight and on-ground.

These systems shall implement security functions to protect the sensitive information from unauthorized disclosure based on cryptography, identification and authentication, access control or secure erase, as well as an integrity control of the information.

EVALUATION RESULTS

The protection profile “EADS AIR SEGMENT SYSTEMS PROTECTION PROFILE, Issue B” has been evaluated using the Common Evaluation Methodology, v3.1 r3 [CEM], for conformance to the Common Criteria, v3.1, r3 [CC-P3].

All the assurance components required by the level EAL3 have been assigned a “PASS” verdict. Consequently, the laboratory (CESTI-INTA) assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3 level.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

The following recommendations to the users of Protection Profile are highlighted as the result of the evaluation process.

The reader of this protection profile should be noted that the Protection profile "EADS Air Segment Systems Protection Profile. Issue B":

- claims conformance to "Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3 July 2009".
- is CC Part2 Conformant
- is CC Part3 Conformant
- claims conformance to package EAL3
- does not claim conformance to another PP
- the conformance required for this Protection Profile is demonstrable

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the protection profile "EADS AIR SEGMENT SYSTEMS PROTECTION PROFILE, Issue B", a positive resolution is proposed.

This certification is recognised under the terms of the Recognition Agreements [CCRA] and [SOGIS] for components up to EAL4 according to the mutual recognition levels of them and the accreditation status of the Spanish Scheme.

GLOSSARY

CC Common Criteria

CCN Centro Criptológico Nacional

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

CESTI Centro de Evaluación de la Seguridad de las Tecnologías de la Información

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

INTA Instituto Nacional de Técnica Aeroespacial

ISM Information Security Manager

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

MOB Main Operating Base

PP Protection Profile

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

RDBMS Relational Database Management System

RTOS Real Time Operating System

SecOps Security Operating Procedures

SOGIS Senior Officers Group for Information Security

TOE Target of Evaluation (the product that will be compliant with this PP)

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, r3, July 2009.

[CC-P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, r3, July 2009.

[CC-P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, r3, July 2009.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r3, July 2009.

SECURITY TARGET

Not applicable

ENAC CERTIFICACIÓN Nº 45/C-PR110

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es