REF:	2010-12-INF-626 V1	Created:	CERT3
Distribution:	Public	Reviewed:	TECNICO
Date:	29.04.2011	Approved:	JEFEAREA

CERTIFICATION REPORT FOR EADS GROUND SEGMENT SYSTEMS PROTECTION PROFILE (GSS-PP) ISSUE B

Dossier: 2010-12 EADS GSS-PP Issue B

References:

- [EXT-1018] Certification Request of EADS GSS-PP Issue B.
- [EXT-1239] Evaluation Technical Report of EADS GSS-PP Issue B, 14-04-2011, Ed. 1.1, CESTI-INTA.
- CCRA. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.
- SOGIS. European Mutual Recognition Agreement of IT Security Evaluation Certificates v3.0, January 2010.

Certification report of EADS GROUND SEGMENT SYSTEMS PROTECTION PROFILE ISSUE B, as requested by EADS-CASA in [EXT-1018] dated 12-7-2010, and evaluated by the laboratory CESTI-INTA, as detailed in the Evaluation Technical Report [EXT-1239] received on November 26th 2011, and in compliance with CCRA and SOGIS for components up to EAL4.

ENAC CERTIFICACIÓN Nº 45/C-PR110

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 GROUND 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 EAL4.

Evaluation end date: 14/04/2011.

All the assurance components required by the level EAL4 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 EAL4 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 GROUND SEGMENT SYSTEMS PROTECTION PROFILE, Issue B, a positive resolution is proposed.

PP Summary

Ground Segment Systems are these systems used by the aircraft crew to manage all the classified or unclassified data related to the aircraft (mission data, health data, etc.). Ground Segment Systems are located in a Main Operating Base (MOB) or in a Deployed Operating Base (DOB) and should include among others the following functionality:

- Mission Management: mission plan data preparation and re-planning
- Mission Briefing/Debriefing
- Payloads data exploitation
- Data Recording

Security Assurance Components

The protection profile was evaluated with all the evidence required to fulfil EAL4, according to CC Part 3 [CC-P3].

Assurance Class: Protection Profile Evaluation (APE)

Assurance Components:

- APE_CCL.1
- APE_ECD.1
- APE_INT.1

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

- APE_OBJ.2
- APE_REQ.2
- APE_SPD.1

Security Functional Components

Majority of the security functional components contained in this PP are based on the components in [CC-P2]. However, there are some security functional components which are applicable to the PP (e.g. virus scanning, integrity checks based in the bespoke application) that are not defined in CC. In this case extended components have been defined. The functional components satisfied by the protection profile are:

- FAU_GEN.1 Audit Data Generation
- FAU_GEN.2 User identity association
- FAU_SAR.1 Audit review
- FAU_SAR.2 Restricted audit review
- FAU_SAR.3 Selectable audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.4 Prevention of audit data loss
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_RIP.2 Full residual information protection
- FIA_AFL.1 Authentication failure handling
- FIA_ATD.1 User attribute definition
- FIA_SOS.1 Verification of secrets
- FIA_UAU.1 Timing of authentication
- FIA_UAU.7 Protected authentication feedback
- FIA_UID.1 Timing of identification
- FIA_USB.1 User-subject binding
- FMT_MOF.1 Management of security functions behaviour
- FMT_MSA.1 Management of security attributes
- FMT_MSA.2 Secure security attributes
- FMT_MSA.3 Static attribute initialisation
- FMT_MTD.1 Management of TSF data
- FMT_MTD.2 Management of limits on TSF data
- FMT_SAE.1 Time-limited authorisation
- FMT_SMF.1 Specification of management functions
- FMT_SMR.1 Security roles
- FMT_SMR.3 Assuming roles

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

- FPT_STM.1 Reliable time stamps
- FAV_ACT_EXP.1 Anti-virus actions (extended component)
- FAV_ALR_EXP.1 Anti-virus alerts (extended component)

IDENTIFICATION

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

Document no. : DT-T-MEE44-10001

Evaluation Level: CC v3.1 r3 EAL4

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 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.AUTOMATIC_SCAN

The TOE must be able to initiate automatic virus scans of removable media (e.g. USB pen drives, CD/DVD) when introduced into the workstation before accessing any data on the removable media.

P.EXTERNAL

The TOE must be able to prevent attacks from external systems.

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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

The rights for users to gain access and perform operations on information are based on their user profile. The user profile is created by the TOE administrator according to the users allowed access and operations.

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 behavior that may be a threat to security.

A.DEVELOPEMENT

All in-service software development, modification, maintenance and testing shall be carried out on a physically separate system which shall be electronically isolated from the TOE.

A.INSTALL

Procedures shall exist to ensure that the system is installed in a secure manner.

A.LOCATE

The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.

A.MANAGE

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

A.NO_EVIL_ADMIN

The system administrative personnel are not careless, will fully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

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

A.PROTECT

TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification including unauthorized modifications by potentially hostile outsiders. It is assumed that all software and hardware, including network and peripheral cabling is approved for the transmittal of the protectively marked data held by the system. Such items are assumed to be physically protected against threats to the confidentiality and integrity of the data transmitted.

A.SEC_OPERATION

Security Operating Procedures (SecOPs) shall exist to ensure that the system is operated in a secure manner.

A.SYOPS

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

A.USER_ID

Each individual user shall be identified unequivocally by IT functions or by organizational procedures.

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.ABUSE

An attacker from inside or outside the organization with special rights (network administration) modifies the operating characteristics of the resources without informing the users.

T.DATA_CORRUPTION

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

T.DOS

Users due to a misuse can cause an IT assets (hardware, software, network, etc.) overload.

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

T.EQUIPMENT_THEFT

Someone inside or outside the organization accessing equipment located on the premises or transported outside steals the equipment.

T.IMPERSONATION

A person assumes the identity of a different person in order to use his/her access rights to the information system, commit a fraud, etc.

T.INFORMATION_DISCLOSURE

Someone inside the organization who, through negligence, passes information to others in the organization who have no need to know or to the outside.

T.INFORMATION_THEFT

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

T.UNAUTHORIZED_USE

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

T.UNTRUSTWORTHY_DATA

Outside sources send false data or unsuitable equipment being used inside the organization 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_ACCESS

Those responsible for the administration must ensure that the rights for users to gain access and perform operations on information are based on their user profile. The user profile is created by the TOE administrator and it accurately reflects the user's job function.

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

O.E_ACCOUNTABLE

Those responsible for the TOE must ensure that:

a) the TOE is configured such that only the approved users may access the system.

b) each individual user is assigned a unique user ID or identified unequivocally.

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 analyzed and archived, to allow retrospective inspection.

b) The auditing system must be configured such that the loss of audit data is minimized 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 unauthorized users.

O.E_CREDEN

Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner which maintains IT security objectives. Those responsible for the TOE must ensure that user authentication data is stored securely and not disclosed to unauthorized individuals. In particular:

a) Procedures must be established to ensure that user passwords generated by an administrator during user account creation or modification are distributed in a secure manner, as appropriate for the clearance of the system.

b) The media on which authentication data is stored must not be physically removable from the system by unauthorized users.

c) Users must not disclose their passwords to other individuals.

O.E_EXTERNAL_SYS

Those responsible for the TOE must establish and implement procedures to ensure that the users:

a) Review the classification of the information prior to dissemination assuring that users know the security mark.

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

b) Ensuring that the protective marking of the TOE information is consistent with the external system to which the information is being sent.

O.E.HW-SW_INSTALL

The installation of those parts of the TOE critical to security policy (e.g. servers, firewall, DMZ) is protected from physical attack which might compromise IT security objectives.

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

The operational environment must ensure that the TOE shall be located within controlled access facilities of the MOB which will prevent unauthorized 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_PROTECT

The operational environment must ensure that the TOE hardware and software critical to security policy enforcement shall be protected from unauthorized physical modification including unauthorised modifications by potentially hostile outsiders. This includes all software and hardware, including network and peripheral cabling is approved for the transmittal of the protectively marked data held by the system.

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).

O.E_SW_LIFECYCLE

The software development, modification, maintenance and testing shall be carried out on a physically separate system which shall be electronically isolated from the TOE.

TOE ARCHITECTURE

The TOE compliant with this protection profile is a software solution, usually composed by two domains, with the possibility to include hardware, but there are some hardware components out of the TOE where the TOE relies to run on (this

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

hardware could be laptops, workstations, servers or even real time platforms if the aircraft is an UAV).

DOCUMENTS

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

TOE TESTING

Not applicable.

TOE CONFIGURATION

Ground Segment Systems are these systems used by the aircraft crew to manage all the classified or unclassified data related to the aircraft (mission data, health data, etc.).

Ground Segment Systems are located in a Main Operating Base (MOB) or in a Deployed Operating Base (DOB) and should include among others the following functionality:

- Mission Management: mission plan data preparation and re-planning
- Mission Briefing/Debriefing
- Payloads data exploitation
- Data Recording

EVALUATION RESULTS

The protection profile “EADS GROUND 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 EAL4 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 EAL4 level.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

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

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

The reader of this protection profile should be noted that the Protection profile "EADS Ground 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 Extended (components FAV_ACT_EXP.1 and FAV_ALR_EXP.1)
- is CC Part3 Conformant
- claims conformance to package EAL4
- 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 GROUND 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

DOP Deployable Operating Base

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

SecOps Security Operating Procedures

SOGIS Senior Officers Group for Information Security

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

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

UAV Unmanned Aerial Vehicle

USB Universal Serial Bus

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.

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