REF: 2011-6-INF-1085 v1	Created by: CERT8
Target: Expediente	Revised by: CALIDAD
Date: 07.12.2012	Approved by: TECNICO

CERTIFICATION REPORT

File: 2011-6 VAG
Applicant: 0860042250 ASELSAN INC.

References:

[EXT 1184] SOLICITUD DE CERTIFICACIÓN CORREGIDA VAG
[EXT-1906] Evaluation Technical Report of VAG.

The product documentation referenced in the above documents.

Certification report of the product VIRTUAL AIR GAP, as requested in [EXT-1184] dated 25-02-11, and evaluated by the laboratory EPOCHE AND ESPRI, as detailed in the Evaluation Technical Report [EXT-1906] received on 09/10/2012.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product VIRTUAL AIR GAP.

The TOE, namely the Virtual Air Gap (VAG), is a software package which provides a secure network traffic flow for private and public institutions in order to realize mission-critical operations fundamentally by preventing transit IP traffic. The TOE is running on internal and external host machines (vag-int and vag-ext) on top of Linux operating systems and mediates the information flow with the support of external software installed in its environment.
TOE is designed for institutions (public and private) that are connected to Internet and offering/getting real-time web and mail service and data interaction over Internet to prevent and remove security threats towards mission-critical operations.

Developer/manufacturer: ASELSAN Inc.
Sponsor: ASELSAN Inc.
Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).
ITSEF:EPOCHE AND ESPRI.
Protection Profile: -
Evaluation Level: Common Criteria. EAL4+ ALC_FLR.2 y AVA_VAN.5.
Evaluation end date: 08/10/2012

All the assurance components required by the evaluation level EAL4+ ALC_FLR.2 y AVA_VAN.5 have been assigned a “PASS” verdict. Consequently, the laboratory EPOCHE AND ESPRI assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4+ ALC_FLR.2 y AVA_VAN.5, as defined by the Common Criteria v 3.1 (CC_P1, CC_P2, CC_p3) and the CEM.

Considering the obtained evidences during the instruction of the certification request of the product VIRTUAL AIR GAP v1.0.6, a positive resolution is proposed.

TOE SUMMARY

The TOE, namely the Virtual Air Gap (VAG), is a software package which provides a secure network traffic flow for private and public institutions in order to realize mission-critical operations fundamentally by preventing transit IP traffic. The TOE is running on internal and external host machines (vag-int and vag-ext) on top of Linux operating systems and mediates the information flow with the support of external software installed in its environment.
TOE is designed for institutions (public and private) that are connected to Internet and offering/getting real-time web and mail service and data interaction over Internet to prevent and remove security threats towards mission-critical operations.

TOE system is deployed between external network and institution's internal network and does not use IP-based communication for internal connection. Therefore, the TOE is actually forming a "virtual air gap" border providing high-level security.
The system which runs the TOE is basically composed of internal and external security components (servers) and a shared memory (shared disk) component. Figure-1 shows the general architectural view of the TOE and its environment.

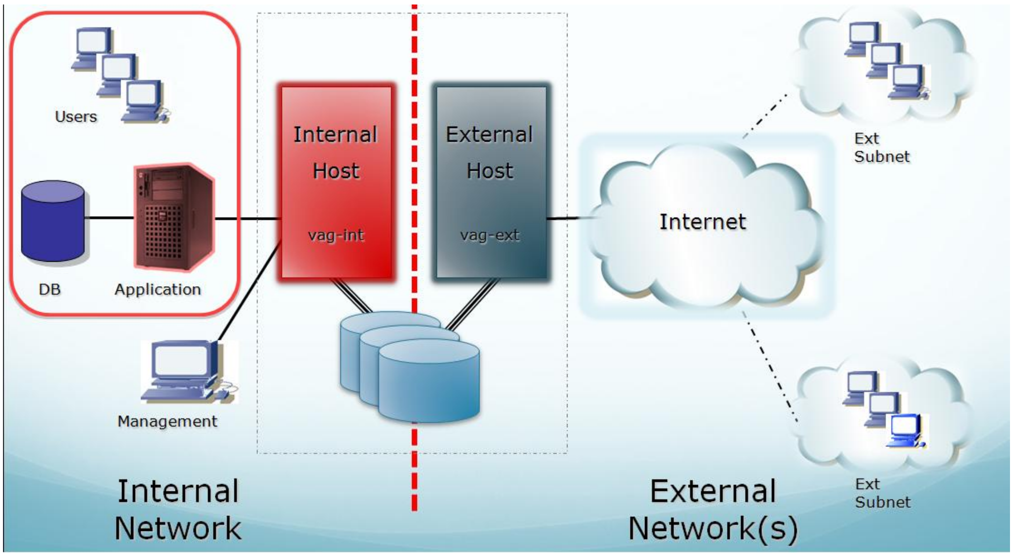

Figure 1. General Architecture of Virtual Air Gap and the Operational Environment

TOE is protected by a number of environmental components in order to function appropriately. These components include firewall (FW), intrusion detection system (IDS), protocol filter and host based intrusion detection system (HIDS) working on both servers (vag-int and vag-ext). vag-int has a management interface that enables administrative users (with sufficient access rights) to manage and monitor both internal and external hosts' system information, configuration data, partial backups, administrative users, audit logs and user passwords. The TOE performs user identification and authentication and an access control policy for the administrative users. The identification and authentication of administrative users makes use of the user name and password. This password must follow a certain policy. The TOE protects itself from brute force attacks by locking a user when three unsuccessful authentication attempts are reached. Additionally, an access control policy is performed for the Maintenance User, which is the user able to access the system through the Linux terminal to perform some certain management functionality. In this case, the identification and authentication of this user is performed by the TOE environment. This user is able to import and export full backups, read the software license, change its password, install patchs and moun/umount USB devices. The TOE maintains four roles: administrator, manager, operator for the management interface and maintenance for the Linux Shell.
During system boot, two tokens must be presented to system (one token for vag-int and another one for vag-ext) via USB port for authentication. These token contains,

for vag-int, its private key, the vag-ext public key, and the key used for the data flow encryption, and for vag-ext, its private key, the vag-int public key, and the key used for the data flow encryption. Data flow encryption key is stored in memory (in both parts, vag-int and vag-ext) during startup with certain obfuscation. VAG does not initialize unless these dedicated tokens are presented, so they must be kept in a safe place, and used only for system startup.

Information flow over TOE is bi-directional; through external to internal network and vice versa. External network requests/responses are taken by external host (vag-ext). The requests/responses are passed through application level controls by a process running on external host. Filtered and controlled requests/responses are transferred to shared disk after encryption and digital signing. Internal host (vag-int) takes the requests/responses from shared disk after decryption, and signature verification procedures. If no problem occurs, the requests/responses are recorded and transferred to the respective application on the internal network. Same information flow is valid for connections from internal network to external network.

The communication between vag-int and vag-ext is encrypted and signed. Cryptographic operations are made by the crypto library of the operating system. Crypto/Sign layer of the VAG architecture that is shown in Figure 2 invokes two cryptographic actions on the data packets flowing from message layer to disk access layer. Operational Environment first encrypts the payload of the data packet, and then signs the whole packet through crypto/sign module of the TOE. This way, disk has signed and encrypted data packets, which can only be resolved by peer host.

The shared disk array hosts a file system which is used as a database for log files. The shared disk array and the file system are not in the scope of the TOE and are considered as environmental components.

All the problems that may arise in any of these stages are recorded in the audit log; these records can be used to analyze the security or operation of the system. All the history of interactions is accessible through management interface. An automatic procedure searches the audit logs for predefined attack patterns and generates alarms in case of detecting a potential attack. The TOE is able to take certain actions in case of reaching this circumstance.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4+ ALC_FLR.2 y AVA_VAN.5, according to [CC_P3].

Clase	Familia/Componente
ADV	ADV_ARC.1 ADV_FSP.4 ADV_IMP.1 ADV_TDS.3
AGD	AGD_OPE.1 AGD_PRE.1

ALC	ALC_CMC.4 ALC_CMS.4 ALC_DEL.1 ALC_DVS.1 ALC_FLR.2 ALC_LCD.1 ALC_TAT.1
ASE	ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.2 ASE_REQ.2 ASE_SPD.1 ASE_TSS.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_VAN.5

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the [CC_P2]:

Clase	Familia/Componente
FAU	ARP.1 GEN.1 GEN.2 SAA.1 SAR.1 SAR.2
FCS	COP_EXT.1
FDP	ACC.1/MANAGEMENT ACF.1/MANAGEMENT ACC.1/MAINTENANCE ACF.1/MAINTENANCE ETC.1 IFC.1 IFF.1 ITC.1
FIA	AFL.1 ATD.1 SOS.1

	UAU.2 UID.2
FMT	MSA.1 MSA.3 SMF.1 SMR.1

IDENTIFICATION

Product: VIRTUAL AIR GAP v1.0.6
Security Target: Declaración de Seguridad "Virtual Air Gap (VAG) v1.0.6 Security Target Version 1.10".
Protection Profile: -
Evaluation Level: EAL4+ ALC_FLR.2 y AVA_VAN.5.

SECURITY POLICIES

The use of the product VIRTUAL AIR GAP v1.0.6 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.

OSP	Descripción
OSP.LOCK	Cryptographic Keys (on USB Flash Disk) must be under the sole control of the Maintenance User.
OSP.AUDIT	The TOE must generate reviewable audit data and all users must be accountable for their actions.
OSP.MACP	A **Maintenance Access Control Policy** shall be implemented allowing a specific maintenance role the access to a particular set of maintenance functions. The user holding this maintenance role is identified and authenticated by the Operating System login terminal (for both **`vag-int`** and **`vag-ext`**). The UserID is to be provided to the TOE to exercise the access control policy. Only the following maintenance functions will be accessible for this role: Mount/umount USB Device Read license Install Patch file Modify Password Export audit logs Export/Restore full backup These maintenance functions will only be accessible for the user holding this role.

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.

Hipótesis	Descripción
A.PHYSICAL	The TOE is installed in a physically secure location and the only user who can access to the physical location where the TOE is located is the Maintenance User.
A.TIME	The environment provides reliable timestamp.
A.NOEVIL	The administrator of the management interface and the Maintenance User are non-hostile and follow all administrative guidance.
A.SINGEN	The TOE is the only communication channel between internal and external network.
A.PLATFORM	No claims are made on the security of the platform that contains the OS. Compromise of the platform can lead to compromise of TOE.
A.INITIALIZATION	Cryptographic keys must be imported through a secure media during the initialization of the TOE according to a 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.

Objetivo	Descripción
OE.PHYSECURE	The TOE must be kept in a physically secured location to prevent attacker from physically accessing the TOE.
OE.NOEVIL	The administrator of the management interface and the Maintenance User are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance.
OE.TIME	The operational environment shall provide a reliable date and timestamp from trusted source.

OE.SINGEN	Owners of the TOE must ensure that TOE is the only connection between the internal and external network.
OE.PLATFORM	The platform that runs TOE shall be protected against compromise.
OE. INITIALIZATION	Maintenance User of the TOE must ensure that importing the cryptographic keys via a secure media will initialize TOE, and this secure media will be under the sole control of this user.
OE.SECURECOMMUNICATION	The Operational Environment shall provide a secure communication line between the TOE and the Management Console.
OE.CRYPTOOP	The Operational Environment shall provide encryption and signature services to the TOE.
OE.USERID_PROVIDER	The operating system login mechanism in both **`vag-int`** and **`vag-ext`** shall identify and authenticate the user and provide the UserID to the TOE for the purpose of exercising the **Maintenance Access Control Policy** referred in the OSP.MACP organisational policy.

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

Management and Maintenance (MM)

Management interface of the TOE is the WEB interface where the administrative users can monitor and/or configure some components of the system.

Management interface is provided by internal host (vag-int) and accessed via management console that communicates over HTTPS protocol on vag-int's network interface. Management console client, which is not in the scope of TOE, is a simple web browser that can run JavaScript code.

The TOE performs an authentication and identification of administrative users by using the username and password. After that, an access control policy is exercised in order to provide access rights to the certain administrative user.

In addition to the Administrative Users who access the system through a web interface, there is also a Maintenance User whose username is “consolemaintenance” who is able to connect to vag-int and vag-ext through Linux Shell.

In this case, the TOE does not perform the authentication and identification of the Maintenance User. This task is responsibility of the operational environment. After that, an access control policy is exercised in order to provide access rights to the Maintenance User.

Application Layer

Application layer of the system is basically responsible for forwarding packets from protocol layer to message layer. For HTTP packets, it consists of built-in malicious data pattern rules that it searches and filters out from the incoming data packets. Clean data packets are registered to system and forwarded to message layer. For SMTP packets, it simply does the registration and forwarding operation.

Message Layer

Message layer of the system is responsible for reorganizing the incoming and outgoing data packets for supported APs. Incoming packets are broken down into portions like header, payload, etc.; and outgoing packets are re-built into their supported AP packets. System uses proprietary data structure to transfer APDU packets between message layers of internal and external host.

Crypto/Sign Layer

Crypto sign layer of the system is responsible for the invocation of cryptographic operations functionality in the operating system. With this layer the incoming and outgoing messages are signed/encrypted and verified/decrypted respectively during a regular data flow between internal and external hosts.

Audit

All the activity that takes place in the TOE is audited on disk storage in exclusive locations (on internal disk for vag-int and on shared disk for vag-ext) and these audit data is available to be read by administrative via management interface and to be exported by the Maintenance User through the Linux Shell.

Alarm

All the activity that takes place in the OS is recorded by logging components in shared disk in exclusive locations for the internal and external host (out of the scope of TOE). These are collectively referred to as “Logs” of the system.
Alarm module is responsible for checking pre-defined rules over the “Log” and “Audit” data and warns administrative users through management interface in case of a matching condition.
Upon receiving a critical alarm through the system, the TOE will set the system in passive mode.

Disk Access Layer

Main feature of this layer is to read and write to a disk prior to a cryptographic operation.
The modules written in RED font and bold in the following figure are in the logical scope of TOE. Modules of the system are detailed as follows:

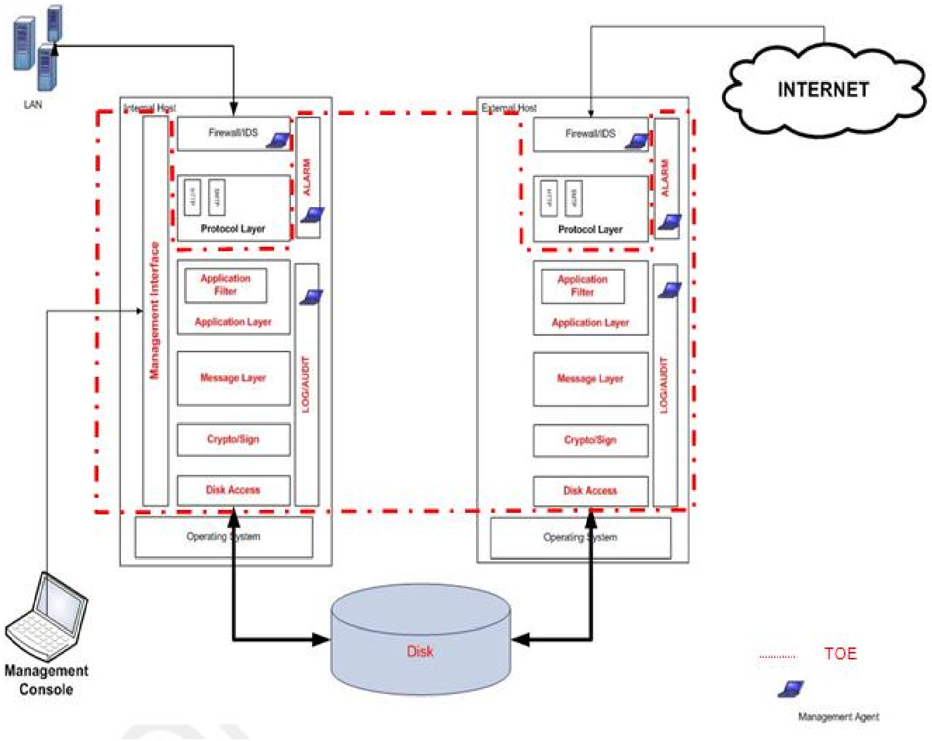

Figure 2: *Logical Scope of TOE*

PHYSICAL ARCHITECTURE

1	vag-mgmt-interface	VAG components running on internal host and client browser, and collectively providing services of management interface to the administrative users.
2	vag-int, vag-ext	VAG software including application, message, Crypto/Sign and Disk Access layers (Identical –symmetrical- software having different binary names on internal and external hosts). It also include the management interface for **`vag-int`**, and Alarm Log/Audit for both.
3	vag-user-guidance	VAG documentation (e.g., installation and user manuals) for guidance of administrative users and Maintenance User.

DOCUMENTS

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

- VAG-UM-v1.4 (User manual)
- VAG-SM-v0,7 (Storage Installation Manual)
- VAG-IM-v1.4 (Installation Manual)

PRODUCT TESTING

The evaluator, as part as the independent tests, has:

- repeated a sample of the developer tests, following his procedures in order to gain confidence in the results obtained.
- executed their own test scenarios to operate the TOE.

The main objective when repeating the developer tests is to execute enough tests to confirm the validity of their results.

The evaluator has repeated the whole set of the test cases specified in the developer testing documentation and has compared the obtained results with those obtained by the developer and documented in each associated report.

For all the test cases, the obtained results were consistent with those obtained by the developer, obtaining in all of them a positive result.

The evaluator considers that both the TSFIs and subsystem tests defined by the developer are correct having checked that the results obtained when repeating the tests are the same than the results obtained by the developer.

Regarding the independent tests, the evaluator has designed a set of tests following a suitable strategy for the TOE type taking into account:

- 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;
- complete coverage of all the SFRs defined in the security target.

The evaluator has designed his TSFIs and subsystems independent test cases including all the external interfaces. 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 the security target.

The process has 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.

The TOE configuration or setup is described in each test. Evaluator devised test results are consistent with the expected results.

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.

The evaluator examined the design specification and test documentation, concluding that all the modules functionality are tested. Therefore, all TSFIs are fully tested. The evaluator verified that TSFI were tested in test plan. The test procedures mapped all TSFI to SFR-enforcing modules.

The result of independent tests was successfully performed and there were neither inconsistencies nor deviations between the actual and the expected results.

EVALUATED CONFIGURATION

The evaluated configuration of the TOE is VIRTUAL AIR GAP v1.0.6.

EVALUATION RESULTS

The product VIRTUAL AIR GAP v1.0.6 has been evaluated against the Security Target "Virtual Air Gap (VAG) v1.0.6 Security Target Version 1.10".

All the assurance components required by the evaluation level EAL4+ ALC_FLR.2 y AVA_VAN.5 have been assigned a "PASS" verdict. Consequently, the laboratory EPOCHE AND ESPRI assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4+ ALC_FLR.2 y AVA_VAN.5, as defined by the Common Criteria [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.

The following usage recommendations are given:

- The physical access to the location where the TOE is deployed must be deeply controlled to ensure that only authorized personnel have access rights.

- Maintenance user and Administrative users of the TOE must have profound knowledge of the system, and they must be trained before operating with it.
- The time source of the TOE is the time of the Linux operating systems of both vag-int and vag-ext. It is necessary to ensure that both computers are synchronized and set to the local time where the TOE is installed.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product VIRTUAL AIR GAP v1.0.6, 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
CB	Certification Body
HW	Hardware
OR	Observation Report
PP	Protection Profile
SW	Software
ST	Security Target

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 Final, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R3 Final, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R3 Final, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R3 Final, July 2009.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:
Declaración de Seguridad "Virtual Air Gap (VAG) v1.0.6 Security Target Version 1.10".