COMMON CRITERIA RECOGNITION ARRANGEMENT
FOR COMPONENTS UP TO EAL 4

Certification Report

EAL 4+ (ALC_FLR.2 and AVA_VAN.5)
Evaluation of

ASELSAN
ELEKTRONIK SAN.ve TİC.A.Ş.

VIRTUAL AIR GAP (VAG) v1.0.6

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	*10.09.2012*
Version of Report	*1.01*
Author	*Murat ADSIZ*
Technical Responsible	*Mariye Umay AKKAYA*
Approved	*Fatih ÇETİN*
Date Approved	*10.09.2012*
Certification Report Number	*14.10.01/12-316*
Sponsor and Developer	*ASELSAN A.Ş.*
Evaluation Lab	*EPOCHE & ESPRI*
TOE Name	*Virtual Air Gap (VAG) v1.0.6*
Pages	*13*

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
v1	*10.09.2012*	*All*	*First released*
v1.01	*12.09.2012*	*2 pages*	*Final released*

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 3, using Common Methodology for IT Products Evaluation, version 3.1, revision 3. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Committee the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the PCC Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCCS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Testing Laboratory (CCTL) under CCCS' supervision.

CCTL is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCTL has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by EPOCHE & ESPRI, which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Virtual Air Gap (VAG) v1.0.6 whose evaluation was completed on 10.09.2012 and whose evaluation technical report was drawn up by EPOCHE & ESPRI (as CCTL), and with the Security Target document with version no v1.0.6. of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the PCC Certified Products List at http://bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: Virtual Air Gap (VAG)
IT Product version: v1.0.6
Developer`s Name: ASELSAN A.Ş. Communications and InformationTechnologies Division
Name of CCTL : EPOCHE&ESPRI
Assurance Package : EAL 4+ (ALC_FLR.2, AVA_VAN.5)
Completion date of evaluation : 10.09.2012

Virtual Air Gap (VAG) is a software package which is jointly developed by Aselsan Inc. and Invicta R&D Ltd. VAG 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.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for VAG v1.0.6, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

TOE major security features for operational use:

Audit: The TOE generates audit logs, and provides the capability of reviewing these audit logs.
Alarm: The TOE includes an automatic procedure to search for predefined attack patterns into the audit logs, and, in case of detecting a potential attack, notify an alarm and act in consequence.

Cryptographic operations invocation: The TOE invokes the operational environment to perform cryptographic operations to cipher and sign the dataflow between vag-int and vag-ext.

Access control: The TOE performs an access control for administrative users of the management interface, and an access control for the Maintenance User.

Data Importation: The Maintenance User of the TOE is able to import data into the TOE.

Data Exportation: The Maintenance User of the TOE is able to export data from theTOE.

Dataflow Control: A dataflow access control is performed by the TOE to control the information flow between the external and the internal network.

Identification & Authentication: The TOE performs an Identification and Authentication mechanism for administrative user that access through the management interface.

Security Management: The TOE provides management functionality to users depending on the user role.

Security Roles: The TOE maintains security roles for users.

There are 6 assumptions made in the ST regarding the development environment, production environment, initialization and maintenance environment, use environment. The ST defines 3 Organizational Security Policy. There is 6 threat covered by TOE and the operational environment. The assumptions, the threats and the organizational security policies are described in chapter 3 of ST in detail.

The results documented in the Evaluation Technical Report (ETR) for this product provide sufficient evidence that it meets the EAL 4 augmented with ALC_FLR.2, AVA_VAN.5 assurance requirements for the evaluated security functionality. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. CCS Certification Body declares that the VAG v1.0.6 evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Project Identifier	*TSE-CCCS-0012*
TOE Name and Version	*Virtual Air Gap (VAG) v1.0.6*
Security Target Document Title	Virtual Air Gap(VAG) v1.0.6 Security Target
Security Target Document Version	*1.10*
Security Target Document Date	*August 2012*
Assurance Level	EAL 4+ (ALC_FLR.2, AVA_VAN.5)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3, July 2009 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009
Methodology	• Common Methodology for Information Technology Security Evaluation v3.1 rev3, July 2009
Protection Profile Conformance	***No***
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009, extended. • Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1, Revision 3, July 2009, conformant.
Sponsor and Developer	*ASELSAN A.Ş.*
Evaluation Facility	EPOCHE&ESPRI
Certification Scheme	Turkish Standards Institution Common Criteria Certification Scheme

2.2 Security Policy

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.

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.

VAG is designed for institutions (public and private) that are connected to Internet and offering/getting real-time web and mail service over Internet to prevent and remove security threats towards mission-critical operations.

2.3 Assumptions and Clarification of Scope

The following topics are TOE assumptions;

- 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.
- The environment provides reliable timestamp.
- The administrator of the management interface and theMaintenance User are non-hostile and follow all administrative guidance.
- The TOE is the only communication channel between internal and external network.
- No claims are made on the security of the platform that contains the OS. Compromise of the platform can lead to compromise of TOE.
- Cryptographic keys must be imported through a secure media during the initialization of the TOE according to a policy.

VAG is designed for institutions (public and private) that are connected to Internet and offering/getting real time web and mail service over Internet to prevent and remove security threats towards mission critical operations.

Logical scope of TOE explained in detail in section 1.4.1 of ST. And, physical scope of the TOE identified and described in section 1.4.2 of ST.

2.4 Architectural Information

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.

2.5 Documentation

Virtual Air Gap (VAG) v1.0.6 Security Target, v 1.10
Virtual Air Gap (VAG) v1.0.6 User Manual v 1.4
Virtual Air Gap (VAG) v1.0.6 Installation Manual v 1.4
Virtual Air Gap (VAG) v1.0.6 Storage Installation Manual v 0.7
Virtual Air Gap (VAG) v1.0.6 Delivery Procedures v0.6

2.6 IT Product Testing

Developer tests effort: Description and tests results, the developer scheduling, description and test results are documented in Virtual Air Gap (VAG) v1.0.6 Test description report v0.6. The approach defined in these documents for TSFIs and depth testing is adequate to check whether the TOE behaves as described in the design documentation. The approach is oriented to test the interfaces and subsystems as they are detailed in Software Functional Specification v1.3, System Design v0.5 and ancillary documentation. The setup and procedures for the test cases allows demonstrating that the behavior of each subsystem is checked.

Evaluator tests effort:

Repeating Developer Tests:

- The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report.
- The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included.

Independent Test Strategy:

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

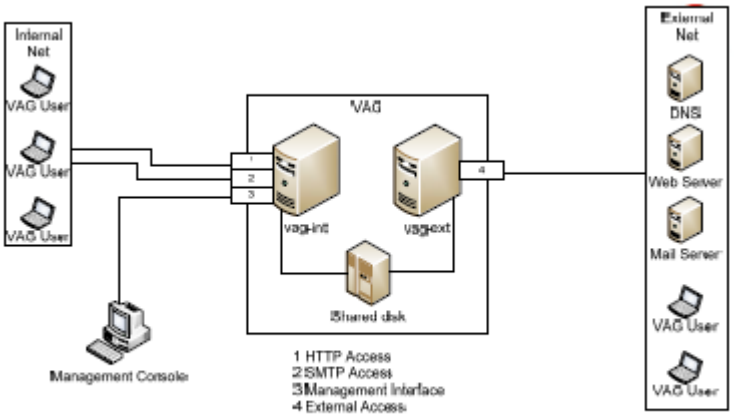
- The evaluator has chosen a subset of tests and an appropriate strategy for the TOE delivered by the developer. The evaluator has also considered the information coming from the security functional requirements in the security target.
- The evaluator has designed a set of tests following a suitable strategy for the TOE type.
- 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.
- All the test cases have been performed using the external interfaces that allow testing appropriately both the SFRs defined in ST and the subsystems.
- The evaluator has executed for TOE, all the tests cases defined in the independent test plan and the results obtained have been documented and referenced in this ETR.

2.7 Evaluated Configuration

The TOE configuration used in the penetration testing is consistent with the evaluated configuration according to security target

The evaluator has defined the test cases taking into account the security requirements defined in ST and the external interfaces defined in Software Functional Specifications.

The following picture describes the operational environment used during the evaluation.



The evaluator has used a virtual machine connected to the internal network in order to manage the internal host of the TOE (vag-int) using the management interface, and two more virtual machines placed outside the external network (connected to vag-ext) using a router. These virtual machines provide the following services: Domain Name Server, Web Server and Mail server.

The evaluator has configured the TOE using the management interface in order to access the external services from the internal network.

The connection between the internal host and the external host of the TOE is performed using a Disk Array. This Disk Array is connected to both parts of the TOE (internal and external host) using Fiber Channel technology.

2.8 Results of the Evaluation

All evaluator actions are satisfied for the evaluation level of EAL 4+ (ALC_FLR.2, AVA_VAN.5) as defined by the Common Criteria and the Common Methodology. The overall verdict for the evaluation is **PASS**. The results are supported by evidence in the ETR.

2.9 Evaluator Comments / Recommendations

Several important aspects that could influence the use of the product, taking into account the scope of the findings of the evaluation and its security target are listed;

- The TOE usage is NOT recommended given that there are exploitable vulnerabilities in the operational environment.
- 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.

3 SECURITY TARGET

The ST associated with this Certification Report is identified by the fallowing nomenclature:

Title : Virtual Air Gap(VAG) v1.0.6 Security Target

Version : 1.10

Date : August 2012

4 GLOSSARY

CB: Certification Body (TSE)

CC: Common Criteria

CCTL: Common Criteria Test Laboratory (Epoche&Espri)

CCCS: Common Criteria Certification Scheme (Turkish CC Scheme)

CCMB: Common Criteria Management Board

CCRA: Common Criteria Recognition Arrangement

EAL: Evaluation Assurance Level

ETR: CCTL VAG ETR v2.0 (04.09.2012)

IT: Information Technology

PCC: Product Certification Center (of TSE)

ST: Security Target (VAG v1.0.6 Security Target v1.10)

TOE: Target of Evaluation (VAG v1.0.6)

TSE: Turkish Standards Institution

TSFI: TOE Security Functionality Interface

VAG: Virtual Air Gap

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

[5] PCC-03-WI-04 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 2.0

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections.