Certification Report

EAL 4+ (ALC_FLR.1) Evaluation of

HAVELSAN HAVA ELEKTRONİK SAN. VE TİC. A. Ş.

HVL Bariyer V1.0.1

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-63

TABLE OF CONTENTS

Document Information

Date of Issue	*27.11.2019*
Approval Date	*28.11.2019*
Certification Report Number	*21.0.03/19-009*
Sponsor and Developer	*Havelsan Hava Elektronik San. Ve Tic. A.Ş.*
Evaluation Facility	*TÜBİTAK BİLGEM TDBY OKTEM*
TOE	*HVL Bariyer v1.0.1*
Pages	*16*

Prepared by	*İbrahim Halil KIRMIZI*
Reviewed by	*Halime Eda BİTLİSLİ ERDİVAN*

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	*27.11.2019*	*All*	*First Release*

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 conformant to Common Criteria for IT Security Evaluation, *version 3.1*, *revision 5*, using Common Methodology for IT Products Evaluation, *version 3.1*, *revision 5*. 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.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission 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 ITCD 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 products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) 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 TÜBİTAK BİLGEM TDBY OKTEM, which is a public/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 *HVL Bariyer v1.0.1* whose evaluation was completed on *04.11.2019* and whose evaluation technical report was drawn up by *04.11.2019* (as CCTL), and with the Security Target document with version no *2.5* of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at 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 EAL2. 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: *HVL Bariyer*

IT Product version: *v1.0.1*

Developer's Name: *HAVELSAN HAVA ELEKTRONİK SAN. VE TİC. A.Ş.*

Name of CCTL: *TÜBİTAK BİLGEM TDBY OKTEM*

Assurance Package: *EAL 4+ (ALC_FLR.1)*

Completion date of evaluation: *04.11.2019*

1.1. Brief Description

The TOE is Management Web Application of a Data Leakage Prevention System. It manages the system that prevents authorization disclosure or leakage of corporate information and data using agents installed in the targeted machines.

1.2. Major Security Features

The TOE provides the following security services;

- Security Audit,
- Identification, Authentication and Authorization
- Data Protection,
- Security Management,
- Cryptographic Support

1.3. *Threats*

The threats are;

- T.Unauthorized_Access: A malicious user may gain unauthorized access to the TOE and change the TOE configuration.
- T.Eavesdropping: A malicious user could gain the valuable information (credentials and enterprise data) of authorized administrator by sniffing the traffic between agent and management server.
- T.No_Act_Rec: Authorized users may change settings of the TOE to not be held accountable for their actions related to the entities checked by the DLP that is controlled by the TOE.

2. CERTIFICATION RESULTS

2.1. *Identification of Target of Evaluation*

Certificate Number	*21.0.03/TSE-CCCS-63*
TOE Name and Version	*HVL Bariyer v1.0.1*
Security Target Title	*HVL Bariyer v1.0.1 Security Target*
Security Target Version	*2.5*
Security Target Date	*24.07.2019*
Assurance Level	*EAL 4+(ALC_FLR.1)*
Criteria	• *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017*

Criteria	- *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017* - *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017*
Methodology	*Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017*
Protection Profile Conformance	*None*
Sponsor and Developer	*HAVELSAN HAVA ELEKTRONİK SAN. VE TİC. A.Ş.*
Evaluation Facility	*TÜBİTAK BİLGEM TDBY OKTEM*
Certification Scheme	*TSE CCCS*

2.2. *Security Policy*

There is no Organisational Security Policy presented at the Security Target.

2.3. *Assumptions and Clarification of Scope*

Assumptions for the operational environment of the TOE are;

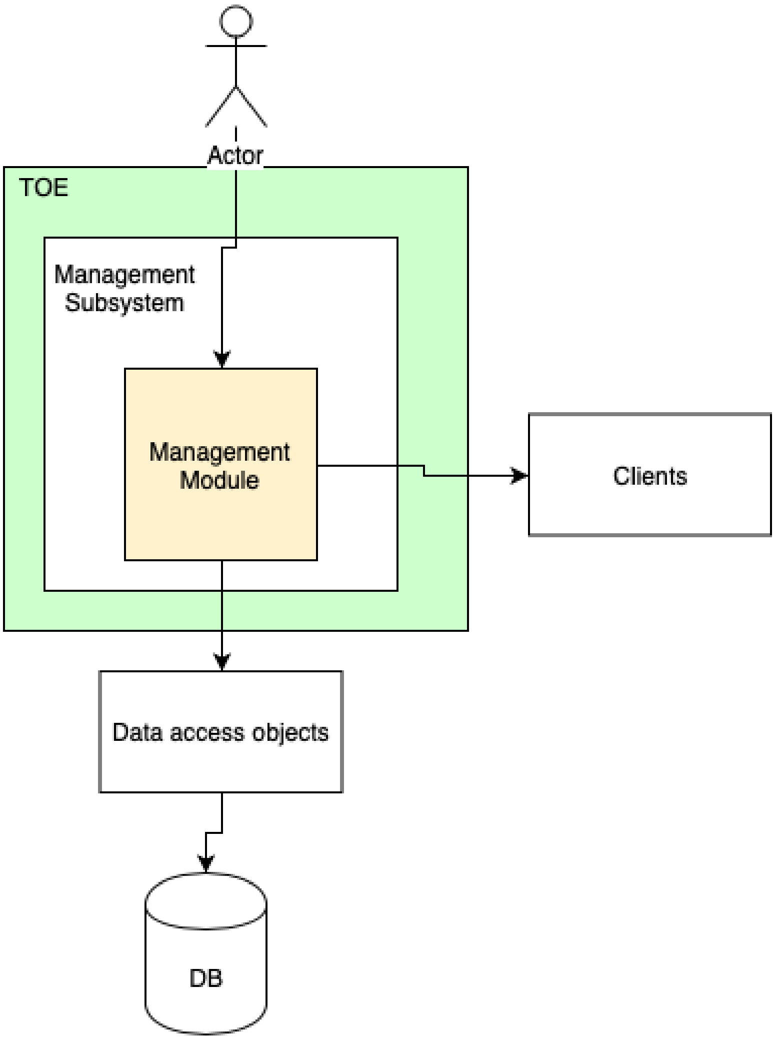
- A.Admin: It is assumed that authorized administrator who is responsible to install, configure and operate the TOE and the IT entities in the operational environment of the TOE are experienced, trained and meet the security conditions.

- A.Sec_Trans: It is assumed that all hardware within the environment, including network and peripheral devices, has been approved for the transmitting of secure data. Each of these appliance configurations is securely managed by administrators to provide protection of secured data in terms of its confidentiality and integrity.

- A.Physical: Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- A.Time_Server: It is assumed that trusted time server provides reliable time information.

2.4. Architectural Information

TOE is composed of one subsystem. The Management Subsystem is the main component of the TOE and connects user to the system. The underlying OS and the hardware aren't part of the TOE.



2.5. Documentation

Documents below are provided to the customer by the developer alongside the TOE;

Name of Document	Version Number	Date
HVL Bariyer v1.0.1 Security Target	*V2.5*	*24.07.2019*
HVL-BARİYER-AGD-UM	*V1.6*	*July 2019*
HVL BARİYER v1.0.1 KURULUM PROSEDÜRLERİ	*V1.5*	*24.07.2019*

2.6. IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developer. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report (ETR) of HVL Bariyer v1.0.1.

It is concluded that the TOE supports EAL 4+ (ALC_FLR.1). There are 25 assurance families which are all evaluated with the methods detailed in the ETR.

2.6.1. Developer Testing

Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE Design documentation which includes TSF subsystems and its interactions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 41 functional tests in total.

2.6.2. Evaluator Testing

- Independent Testing: Evaluator has chosen 5 developer tests to conduct by itself. Additionally, evaluator has prepared 12 independent tests. TOE has passed all 17 functional tests to demonstrate that its security functions work as it is defined in the ST.

- Penetration Testing: TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 10 penetration tests have been conducted.

2.7. Evaluated Configuration

The evaluated TOE configuration is composed of;

- HVL Bariyer v1.0.1,
- Guidance Documents

Also minimum Hardware/Software/OS requirements for the TOE are;

- 8 Core Processor,
- 8 GB RAM,
- 500 GB Hard Drive space,
- Docker,
- Docker Compose,
- Ubuntu 16.04.3,
- MariaDB

2.8. Results of the Evaluation

The table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_FLR.1

Assurance Class	**Component**	**Component Title**
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-Defined Development Tools
	ALC_FLR.1	Basic Flaw Remediation

Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	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
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
Vulnerability Analysis	AVA_VAN.3	Focused Vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4+ (ALC_FLR.1) assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE “HVL Bariyer v1.0.1”, the results of the assessment of all evaluation tasks are “Pass”.

2.9. Evaluator Comments / Recommendations

It is recommended that all guidance outlined in the Guidance Documents be followed and all assumptions are fulfilled in order to the secure usage of the TOE.

3. SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:

Title: *HVL Bariyer v1.0.1 Security Target*

Version: *2.5*

Date of Document: *24.07.2019*

A public version has been created and verified according to ST-Santizing:

Title: *HVL Bariyer v1.0.1 Security Target*

Version: 2.5

4. GLOSSARY

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

DLP: Data Leakage Prevention

ITCD: Information Technologies Test and Certification Department

EAL : Evaluation Assurance Level

OSP : Organisational Security Policy

PP : Protection Profile

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

5. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017,

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017,

[3] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel.Date: February 8th 2016,

[4] DTR 67 TR 01 HVL Bariyer v1.0.1 EAL4+ (ALC_FLR.1) CC Değerlendirmesi DTR, November 4th 2019

6. ANNEXES

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