Certification Report

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

İNVİCTA İNTERNET VERİ İLETIŞİMİ CHİP TEKNOLOJİLERİ AR-GE VE BİLGİ GÜVENLİĞİ SAN. VE TİC. LTD. ŞTİ.
Virtual Air Gap (VAG) v3.0.3

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-101

TABLE OF CONTENTS

Document Information

Date of Issue	**16.06.2026**
Approval Date	**19.06.2026**
Certification Report Number	**21.0.03/26-001**
Sponsor and Developer	**İNVİCTA İNTERNET VERİ İLETIŞİMİ CHİP TEKNOLOJİLERİ AR-GE VE BİLGİ GÜVENLİĞİ SAN. VE TİC. LTD. ŞTİ.**
Evaluation Facility	**BEAM TEKNOLOJİ A.Ş.**
TOE/ PP Name*	**Virtual Air Gap (VAG) v3.0.3**
Pages	**23**

Prepared by ***Common Criteria Candidate Inspection Expert***	**Ertan Osman ALABAY**
Prepared by ***Common Criteria Inspection Expert***	**Yavuz AVCI**
Reviewer (Approver)	**Mehmet Kürşad ÜNAL**

The experts whose names and signatures are shown as above prepared and reviewed this report.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	**16.06.2026**	**All**	**First Release**

DISCLAIMER

This certification report and the IT product/PP 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 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. 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 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 (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF 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 CCEF 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 BEAM TEKNOLOJİ A.Ş., 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) v3.0.3 whose evaluation was completed on May 22th, 2026 and whose evaluation technical report was drawn up by BEAM TEKNOLOJİ A.Ş. (as CCTL), and with the Security Target document with version no 1.0a of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at 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

Developer of the IT product: İNVİCTA İNTERNET VERİ İLETIŞİMİ CHİP TEKNOLOJİLERİ AR-GE VE BİLGİ GÜVENLİĞİ SAN. VE TİC. LTD. ŞTİ.

Evaluated IT product: Virtual Air Gap (VAG) v3.0.3

IT Product Version: 3.0.3

Name of IT Security Evaluation Facility: BEAM TEKNOLOJİ A.Ş.

Completion date of evaluation: 22.05.2026

Assurance Package: EAL 4+ (ALC_FLR.2, AVA_VAN.5)

1.1. Brief Description

The TOE, namely the Virtual Air Gap (VAG), is a software product that provides secure data flow (network traffic) between the two connected networks in order to realize mission-critical operations fundamentally by separating and preventing transit IP traffic, while providing near-real-time end-to-end traffic flow. 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 software components of TOE.

TOE system is deployed between external network (EXT-Net) and internal network (INT-Net) and does not use IP-based communication for internal communication between vag-int and vag-ext. Therefore, the TOE is actually forming a “virtual air gap” border providing a high-level of security.

1.2. Major Basic Security and Functional Attributes

The security functionalities of the TOE are:

- **Access control:** The TOE performs an access control for administrative users of the management interface, as well as for the Maintenance User.
- **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, generates an alarm and react as a consequence.

- **Cryptographic operations invocation**: The TOE invokes the operational environment to perform cryptographic operations to encrpt/decrypt and sign/verify the APDUs of dataflow between **vag-int** and **vag-ext**.
- **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 the TOE.
- **Dataflow Control**: A dataflow access control mechanism that is provided by the TOE to control information flow between the external and the internal network.
- **Identification & Authentication**: The TOE performs an Identification and Authentication mechanism for an administrative user that access through the management interface.
- **Security Management**: The TOE provides management functionality to users based on their user role.
- **Security Roles**: The TOE maintains security roles for users.

1.3. Threats

The security analysis identifies three threat agents, namely Agent External VAG User, Internal VAG User, and Mgmt-GUI User. Threat Agents External VAG User and Internal VAG User are characterized by a high attack potential, reflecting their ability to exploit vulnerabilities within the TOE. Threat Agent Mgmt-GUI User is regarded as a critical actor due to its privileged access to the Management Interface, which provides the capability to influence security-relevant functions and configurations of the TOE. Threats for the TOE are:

- **T.UNAUTH:** An internal VAG user may gain unauthorized access to the TOE through the management interface that causes a loss in the confidentiality and integrity of any of the assets.
- **T.EAVESDROP:** An internal VAG user may follow the traffic between management console and the TOE that cause a loss in the confidentiality of audit data, user credentials and configuration data.
- **T.OBTAIN:** An external VAG user may obtain the TOE's internal communication data being exchanged between external and internal hosts of the TOE, which will cause a loss in the confidentiality of the transmitted data.
- **T.CRYPTOKEYS:** An internal/external VAG user may compromise the cryptographic keys through an unauthorized access to the memory. This action, in turn, leads to compromise of signed and encrypted data (payload) which is a violation of confidentiality, integrity and availability principles.
- **T.MEDIATE:** An external/internal VAG user may bypass the filtering mechanism of the TOE by compromising the integrity of the configuration data.

- **T.PRIVILEGES:** Mgmt-GUI User of the system may have a potential of gaining unauthorized access to assets by capturing certain privileges.

1.4. Organizational Security Policies (OSPs)

OSPs for the TOE are:

- **OSP.LOCK:** Cryptographic Keys (on USB Flash Memory) 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.KACP:** A Keypair Access Control Policy is implemented for importing public and private keys of each side that are used for signing and verifying signature of messages (payload) exchanged. These keys are to be loaded from USB Flash Disk (Token) during boot time. Due to their content sensitivity, the two Tokens should be kept physically secure, accessable only by the Maintenance User. Generation, use and destruction of symmetric encryption and decryption keys are performed by the Message Layer. Each individual connection/session data exchange will be encrypted and decrypted by using dynamically generated IV pair (one for each direction); and those IV pairs are again dynamically destructed by TOE once the connection/session is terminated under the reponsibility of Message Layer.
- **OSP.MACP:** A Maintenance Access Control Policy is implemented allowing a specific user role (consolemaintenance, Administrator, Manager, Operator) to access to a particular set of maintenance functions. consolemaintenance user access is identified and authenticated by the Operating System (Linux tty terminal login) for both vag-int and vag-ext seperately. This requires physical access to location the two servers (vag-int and vag-ext) are deployed. The other users (Administrator, Manager, Operator) are able to access via a web browser connected to INT-Net. Each role has certain priviledges described in the ST.

1.5. Assumptions

Assumptions for the TOE are:

- **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 time-stamp.

- **A.NOEVIL:** The Maintenance User (consolemaintenance) is assumed to be assigned to non-hostile staff and these people are assumed to follow all administrative guidance. It is also assumed this entity (consolemaintenance) keeps its access credentials secure (undisclosed in any way)
- **A.SINGEN:** The TOE is the only communication channel between INT-Net and EXT-Net.
- **A.PLATFORM:** The underlying platform and operating system that hosts the TOE is assumed to be secure and properly configured. The platform provides a trusted execution environment for the TOE.
- **A.INITIALIZATION:** Cryptographic keys must be imported through a secure media during the initialization of the TOE according to a policy.

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-101
TOE Name and Version	Virtual Air Gap (VAG) v3.0.3
Security Target Title	Virtual Air Gap (VAG) v3.0.3 Security Target
Security Target Version	1.0a
Security Target Date	05.06.2026
Assurance Level	EAL 4+ (ALC_FLR.2, AVA_VAN.5)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 5, April 2017
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
Protection Profile Conformance	None

Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, conformant • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, conformant
Sponsor and Developer	İNVİCTA İNTERNET VERİ İLETIŞİMİ CHİP TEKNOLOJİLERİ AR-GE VE BİLGİ GÜVENLİĞİ SAN. VE TİC. LTD. ŞTİ.
Evaluation Facility	BEAM TEKNOLOJİ A.Ş.
Certification Scheme	TSE CCCS

2.2 Security Policy

Security policies for the TOE are:

- **OSP.LOCK:** Cryptographic Keys (on USB Flash Memory) 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.KACP:** A Keypair Access Control Policy is implemented for importing public and private keys of each side that are used for signing and verifying signature of messages (payload) exchanged. These keys are to be loaded from USB Flash Disk (Token) during boot time. Due to their content sensitivity, the two Tokens should be kept physically secure, accessable only by the Maintenance User. Generation, use and destruction of symmetric encryption and decryption keys are performed by the Message Layer. Each individual connection/session data exchange will be encrypted and decrypted by using dynamically generated IV pair (one for each direction); and those IV pairs are again dynamically destructed by TOE once the connection/session is terminated under the reponsibility of Message Layer.

- **OSP.MACP:** A Maintenance Access Control Policy is implemented allowing a specific user role (consolemaintenance, Administrator, Manager, Operator) to access to a particular set of maintenance functions. consolemaintenance user access is identified and authenticated by the Operating System (Linux tty terminal login) for both vag-int and vag-ext seperately. This requires physical access to location the two servers (vag-int and vag-ext) are deployed. The other users (Administrator, Manager, Operator) are able to access via a web browser connected to INT-Net. Each role has certain priviledges described in the ST.

2.3 Assumptions and Clarification of Scope

Assumptions for the TOE are:

- **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:** he environment provides reliable time-stamp.
- **A.NOEVIL:** The Maintenance User (consolemaintenance) is assumed to be assigned to non-hostile staff and these people are assumed to follow all administrative guidance. It is also assumed this entity (consolemaintenance) keeps its access credentials secure (undisclosed in any way)
- **A.SINGEN:** The TOE is the only communication channel between INT-Net and EXT-Net.
- **A.PLATFORM:** The underlying platform and operating system that hosts the TOE is assumed to be secure and properly configured. The platform provides a trusted execution environment for the TOE.
- **A.INITIALIZATION:** Cryptographic keys must be imported through a secure media during the initialization of the TOE according to a policy.

Software components and functional units of the TOE, TOE users, TOE boundary, as well as the environment that the TOE runs are identified and described in the following Figure-2. Physical deliverable software components including TOE are described in the Table-1. vag-ISO contains the TOE as well as other components.

Distribution Component	Description
vag-tokens	Two USB Flash Disks containing public/private key pairs for successful initialization of the system, and for internal cryptographic operations.
vag-ISO	A USB Flash Disk in an installable ISO image format, which contains TOE, other system components and Invictus (Invicta's specialized Linux) in binary form.
vag-user-guidance	VAG documentation (e.g., installation and user manuals) for guidance of administrative users and the Maintenance User. User Guidance documentation files are contained in vag-ISO in ".pdf" form.

Table 1: *TOE Deliverables*

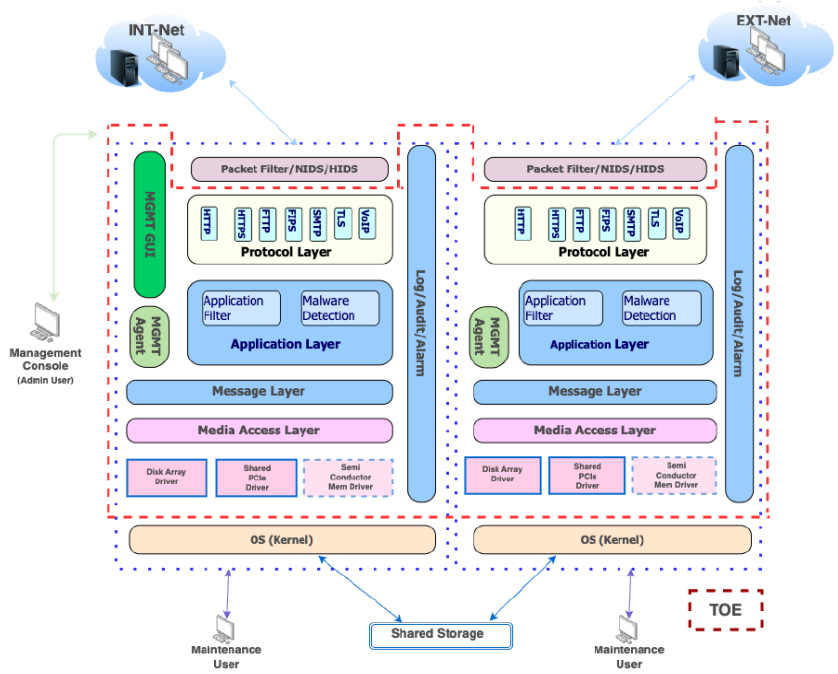

Figure 1: *Physical Scope of the TOE (indicated in red and/or brown dashed lines)*

The modules (TOE Components) surrounded by red dashed lines in Figure-1 are in the logical (functional) scope of TOE. Other components of the system (OS, OS security components) that are not part of TOE are also shown in this figure. It should be noted that SemiConductor Memory depicted in dashed lines is a near-future functionality of the TOE that is not available in the scope of TOE's evaluation, which is also stated in the ST.

For further clarification of scope and the details of layers in Figure-1, see related ST.

2.4 Architectural Information

TOE system is deployed between external network (EXT-Net) and internal network (INT-Net) and does not use IP-based communication for internal communication between **vag-int** and **vag-ext**. Therefore, the TOE is actually forming a "virtual air gap" border providing a high-level of security.

The complete system that runs the TOE is basically composed of internal and external hosts (servers) and a shared storage component as hardware infrastructure. General architecture of TOE and the operational environment is depicted in the Figure-2.

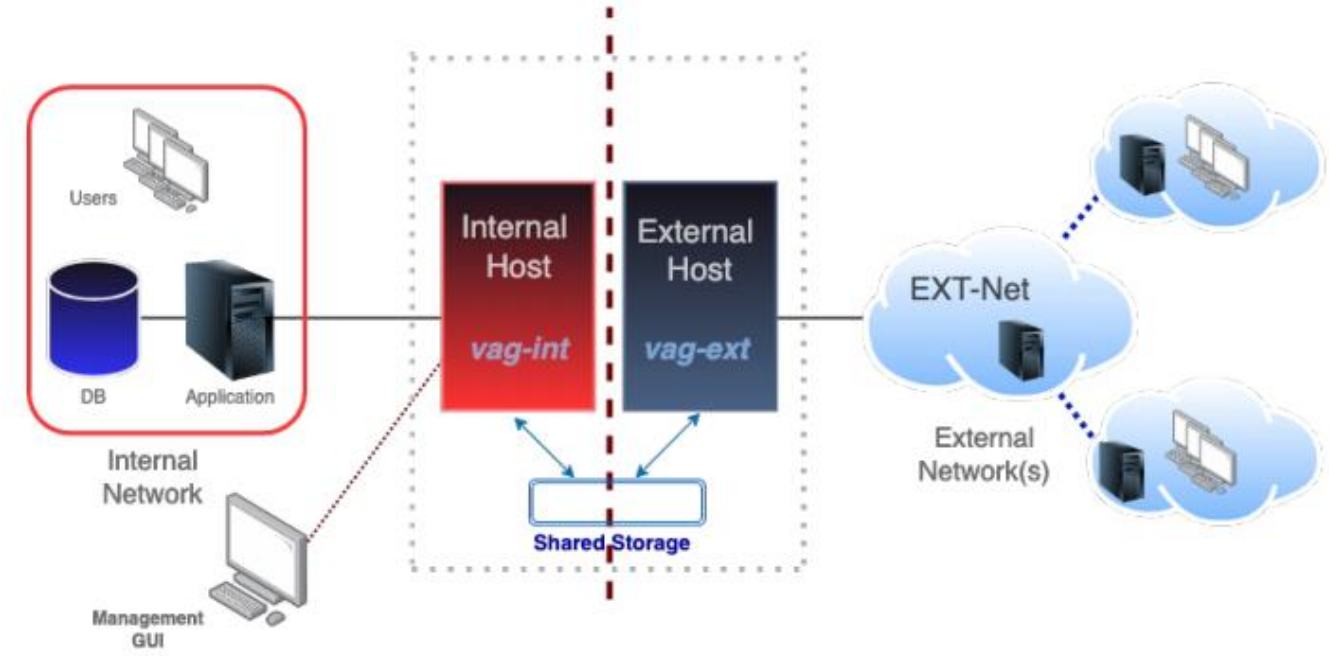

Figure 2: *General Architecture of TOE and the Operational Environment*

TOE is encapsulated and protected by a number of software components for additional product security. These components include packet filter [Firewall (FW)], network-based intrusion detection system (NIDS), a custom protocol filter, web application filter, malware detection and host based intrusion detection system (HIDS) running on both servers (vag-int and vag-ext).

TOE provides four different roles for administration. For the management interface, three roles are referred to as:

- Administrator
- Manager
- Operator

For accessing to systems' (vag-int and vag-ext) consoles, the fourth role is referred to as "Maintenance User" of the Linux Shell.

During system boot, two tokens (USB Flash Disks) must be presented to system (one token for vag-int and another one for vag-ext) via USB port for authentication. These token contain, for vag-int , its private key, the vag-ext public key, and for vag-ext , its private key, the vag-int public key. 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. Requests and responses of external network side are handled by the 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 storage after encryption and digital signing. Internal host (vag-int) takes the requests/responses from shared storage after signature verification and decryption. If no problem occurs, the requests/responses are recorded and transferred to the respective application on the internal network. Same information flow is also valid for the other direction, connections from internal network to external network.

Bidirectional communication between vag-int and vag-ext is encrypted and signed. Cryptographic operations are performed by the functions of crypto library of the operating system. Crypto/Sign functionality is contained in VAG architecture as a sub-layer of the Message Layer.

For further architectural information, see related ST.

2.5 Documentation

Developer provides TOE user guidance documentation for administrative users and maintenance user alongside the TOE, which are included in vag-ISO as stated in ST. TOE documentation provided by developer, including the ST, are mentioned below:

Document Name	Version	Release Date
Virtual Air Gap (VAG) v3.0.3 Security Target	1.0a	05.06.2026
Virtual Air Gap (VAG) v3.0.3 Installation Manual	1.0	14.05.2026
Virtual Air Gap (VAG) v3.0.3 User Manual	1.0	14.05.2026
Virtual Air Gap (VAG) v3.0.3 Media Access Subsystem Installation Manual	1.0	14.05.2026

Table 2: *Documentation provided by developer to users of TOE.*

At the time of this certification report's approval, all provided documentation in Table-2 are up-to-date and valid. For future documentational changes, users should consult the developer.

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 and the evaluation evidences has been established. The evaluation results are available at the final Evaluation Technical Report (ETR) of Virtual Air Gap (VAG) v3.0.3. It is concluded that the TOE supports EAL 4 augmented with ALC_FLR.2 and AVA_VAN.5. There exist 25 assurance families which are all evaluated with the methods detailed in the ETR.

- **Developer Testing:** Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE design documentation which includes TSF subsystems and their interactions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 261 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted 11 developer tests. Additionally, evaluator has prepared 13 independent tests. TOE has passed all functional tests to demonstrate that its security functions work as it is defined in the ST.
- **Penetration Tests:** TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 34 penetration tests have been conducted. TOE proved that it is resistant to “Attacker with High Attack Potential”. In addition, the developer carries out penetration tests regularly. These tests involve simulating real-world attacks to uncover security weaknesses and assess the application’s resilience against various attack vectors. No other external penetration test services are used.

2.7 Evaluated Configuration

Evaluated TOE configuration is composed of:

- Virtual Air Gap (VAG) v3.0.3 (TOE itself)
- Two identical rack servers which are composed of non-TOE and TOE elements, as specified in ST and Table-3 of this certification report.

Minimum non-TOE software and hardware requirements specified in the ST is included in the Table-3 below:

Requirements	Version & Specifications
Invictus Hardware (non-TOE)	• 2 x 1 TB SATA/SAS(Hardware Supported RAID 0/1) Disk, • 8 GB Main Memory, • 64-bit Intel/AMD 16 Core Processor, • 2 x Ethernet (100 Mbps OR 1 Gbps or 10 Gbps) Interface, • A graphical terminal with acceptable resolution (min. 1280 x 800 pixels)
Invictus Software (non-TOE)	• Debian GNU/Linux 13.4, • Linux Kernel 6.12.86, • iptables 1.8.11, • Suricata 7.0.10, • Samhain 4.1.4, • mod-security 2.9.11-1+vag01, • Amavisd-new 1:2.13.0-7, • Clamav 1.4.3, • Malware-Vault 1.9.90.260409-10310
Management Console Hardware	• A desktop OS (MS Windows, MacOS, Linux) providing compatibility with a COTS (Common off the Shelf) web browser (IE, Firefox, Opera, Chrome, Safari)
Management Console Software	• Microsoft Edge 100 and above, • Firefox 90 and above, • Chrome 100 and above, • Opera 90 and above, • Safari 14 and above
Disk Storage Hardware	• Dual port Fiber Channel Interface, • RAID 0/1/3/5 Support • 8 GB cache, • 12 x 80 GB SATA or SAS or SSD Disk Units
PCIe Shared Memory	• RDMA support (provided by Invicta)

Table 3: *Minimum Non-TOE Software and Hardware Requirements for TOE*

Further information regarding TOE and non-TOE requirements can be obtained in ST associated with this certification report.

2.8 Results of the Evaluation

The table below provides a complete list of the Security Assurance Requirements for the TOE. These requirements consist of the Evaluation Assurance Level 4 (EAL 4) components augmented with ALC_FLR.2 and AVA_VAN.5 as specified in Part 3 of the Common Criteria.

Class Heading	Class Family	Description	Result
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.4	Complete functional specification	PASS

Class Heading	Class Family	Description	Result
	ADV_IMP.1	Implementation representation	PASS
	ADV_TDS.3	Basic modular design	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC: Lifecycle Support	ALC_CMC.4	Production support, acceptance procedures and automation	PASS
	ALC_CMS.4	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
	ALC_DVS.1	Identification of security measures	PASS
	ALC_FLR.2	Flaw reporting procedures	PASS
	ALC_LCD.1	Developer-defined life-cycle model	PASS
	ALC_TAT.1	Well-defined development tools	PASS
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims	PASS
	ASE_ECD.1	Extended components definition	PASS
	ASE_INT.1	ST introduction	PASS
	ASE_OBJ.2	Security objectives	PASS
	ASE_REQ.2	Derived security requirements	PASS
	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS
ATE: Tests	ATE_COV.2	Analysis of coverage	PASS
	ATE_DPT.1	Testing: basic design	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability Analysis	AVA_VAN.5	Advanced methodical vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable with the stated security objectives for the operational environment and it can be suitably addressed.

In addition to general guidance mentioned in this certification report and ST, developer provided several hash values during evaluation and certification phases. At the time of this certification report's approval, SHA-256 hash values mentioned in this report's Annex are valid. Further discussion on this topic is included in Annex of this certification report.

3 SECURITY TARGET

The security target associated with this Certification Report is identified by the following terminology:

Title: Virtual Air Gap (VAG) v3.0.3 Security Target

Version: v1.0a

Date of Document: June 5, 2026

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale. Developer also provided SHA-256 hash value of associated ST to evaluators which can be found in section Annex of this certification report.

4 GLOSSARY

Administrative User: Those users that are granted authorization to configure and/or control and/or watch the running TOE via facilities provided by the management interface (MI).

Administrative User Security Attributes: TOE data associated with administrative users that is used for security policies of TOE.

Alarm: A system message that is displayed via management interface, indicating an unusual (and possibly harmful) activity. It is a trail that matches with predefined exception patterns in the log or audit file.

Approved Data Flow: Any proper traffic flowing over the TOE (a flow that is not rejected due to some reason).

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

CCRA: Common Criteria Recognition Arrangement

CKM: Cryptographic Key Management

COP: Cryptographic Operation

Critical Alarm: A special type of alarm that will trigger the system to go into non-operational (passive) mode.

Data Flow: Any allowed type of application layer protocol traffic flowing through the TOE.

Data input: A Data packet received from the INT-Net or EXT-Net by the connected respective host (i.e., vag-int or vag-ext).

Data output: A Data packet sent to the INT-Net or EXT-Net by the connected respective host (i.e., vag-int or vag-ext).

Disk Array: A particular form of the Shared Storage connected to vag-int and vag-ext via Fiber Channel Interface, providing disk sharing capability.

EAL: Evaluation Assurance Level

EXT-Net: The network which has lower security level.

External Host (vag-ext): The host that is connected to EXT network.

Host(s): The hardware platform on which the Invictus is deployed (i.e., the two hosts, vag-int and vag-ext).

Host Disk: Internal disk storage of the host for the installation of vag-ISO.

Host-based Intrusion Detection System (HIDS): A software component to detect intrusion to host operating system (file system entities) according to non-configurable pre-defined patterns.

IFC: Information Flow Control

INT-Net: The network which has higher security level.

Internal Host (vag-int): The host that is connected to INT network.

ITC: Inter TSF Confidentiality

Invictus: The whole system, which consists of the operating system (OS), OS components, the TOE and internal security components (Packet Filter, NIDS, HIDS, etc.). This collection of software is deployed on both vag-int and vag-ext.

Linux Shell: Command line terminal software provided by the customized Linux Operating System (Invictus) on both hosts (vag-int and vag-ext) where the TOE runs. This tty terminal is only accessible at the physical location(s) of vag-int and vag-ext, and thru VGA port of the concerned host.

Maintenance User: A special user having certain limited set of administrative capabilities for configuring and controlling the TOE through the Linux Shell, right after a successful login to the system through the text console via user name “consolemaintenance” and its associated password (Note: This user is not

allowed to login through the management interface). This is the only user allowed to access to the physical location(s) where vag-int and vag-ext are deployed.

Management Interface (MI): Web interface provided by the internal VAG Server (vag-int) for administrative users.

Management Console: A web browser that is connected to the INT-Net (or directly to vag-int) and used by administrative users to access to the Management Interface (MI).

MSA: Management of Security Attributes

Network Intrusion Detection System (NIDS): A software component to detect intrusion to the host according to semi-configurable pre-defined patterns.

OSP: Organizational Security Policy

Passive mode: A mode of operation where the information flow between vag- int and vag-ext is disabled for VAG Users. In this mode of operation, the information flow between vag-int and vag-ext is only available for for management purposes. The management interface and management console as well as Linux Shells on both sides remain enabled.

PCIe Shared Memory: A particular form of the Shared Storage connected to vag-int and vag-ext via PCIe bus, providing memory sharing capability.

Rejected Data Flow: Any illegitimate traffic that is filtered out as a result of its identification as malicious data or not allowed data.

SAR: Security Assurance Requirements

SFR: Security Functional Requirements

SHA: Secure Hash Algorithm

Shared Storage: Shared storage is the generic name of the device connected to both vag-int and vag-ext and forms the only and the unique path for the information flow between the two hosts.

SMF: Specification of Management Functions

ST: Security Target

System Logs: Files stored out of the TOE (in shared storage for vag-ext and in host disk for vag-int) to maintain the activities of the Linux OS that TOE runs in conjunction with.

TLS: Transport Layer Security

TOE: Target of Evaluation

TDC: TSF Data Consistency

TSF: TOE Security Functionality

TSFI: TSF Interface

TSP: TOE Security Policies

VAG: Virtual Air Gap

VAG User: An internal/external entity that sends requests to and gets responses from (i.e., interacts with) the TOE via supported application layer protocols.

vag-ISO: A USB Flash Disk in an installable ISO image format, which contains TOE, other system components and Invictus (Invicta's specialized Linux) in binary form.

vag-tokens: Two USB Flash Disks containing public/private key pairs for successful initialization of the system, and for internal cryptographic operations.

vag-user-guidance: VAG documentation (e.g., installation and user manuals) for guidance of administrative users and the Maintenance User. User Guidance documentation files are contained in vag-ISO in ".pdf" form.

VAG Logs: Files stored out of the TOE (in shared storage for vag-ext and in host disk for vag-int) where the activities performed by the TOE are recorded.

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] BTTM-CCE-071 DTR v.2.2 BTTM Evaluation Technical Report, Version 2.2, Rel. Date: June 5, 2026.

[4] Virtual Air Gap (VAG) v3.0.3 Security Target, Version 1.0a, Rel. Date: June 5, 2026.

6 ANNEXES

6.1 HASH VALUES OF TOE & TOE-DELIVERABLES

This section of certification report contains SHA-256 hash values provided by the developer, which are obtained during evaluation and certification processes. At the time of this certification report's approval, all hash values provided in this annex are valid. TSE CCCS is not responsible for changes of these values in the future and if need arises, potential purchasers should contact the developer for up-to-date information.

As stated in ST, deliverable version of TOE and delivered TOE documentation is included in a ".iso" file (known as "vag-ISO" and "vag-use-guidance" in ST, in respect), and has its own hash value. SHA-256 hash value of vag-ISO is used for checking the integrity of TOE delivered to customers and is also included in delivered guidance documents (which are denoted as "vag-user-guidance" in ST). However, TOE itself has the following SHA-256 hash value, which is provided by the developer:

TOE Name	**SHA-256 Hash Value**
Virtual Air Gap (VAG) v3.0.3	7F3795DBD421AF5DA82FBC5C41D1B20BBAF0A583F6BBBA5A84B4C83159A731DD

In addition to SHA-256 hash value of vag-ISO, developer also provided the hash value of ST in the table below, which is also mentioned in section 3 of this certification report:

TOE Deliverable / ST	**SHA-256 Hash Value**
Virtual Air Gap (VAG) v3.0.3 Security Target	480BF528A7E2DB3A2268B29FB7F545120368DF3E0C9DDA7436BEC8ACB5970633
vag-ISO	9CEA2980BE181C44A27FB9C1C7E6C49042CBD858C95BF23C39ADD5700CDFA8C9