VIRTUAL AIR GAP

(VAG)

v3.0.3

Security Target

Version 1.0a

June 2026

https://www.invicta.com.tr/

info@invicta.com.tr

© All rights reserved.

Contents

© All rights reserved.

© All rights reserved.

1 INTRODUCTION

This section provides an introduction to the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, and the ST organization.

The TOE, namely Virtual Air Gap (VAG) v3.0.3 is designed and developed as an enhanced product, based on its earlier version *v2.0* and the patents;

- ***TR 2007 08644 B***
- ***US 8,984,275 B2***

This section of the document;

- identifies the Security Target (ST) and Target of Evaluation (TOE),
- specifies the ST conventions,
- provides an overview and the description of TOE,
- describes the ST organization.

1.1 ST Reference and TOE Reference

ST Title	Virtual Air Gap (VAG) v3.0.3 Security Target
ST Version	v1.0a
ST Release Date	5 June 2026
TOE Identification	Virtual Air Gap (VAG) v3.0.3
CC Identification	Common Criteria for Information Technology Security Evaluations, Version 3.1R5
Keywords	Virtual Air Gap, VAG, Border Security, Network Isolation and Separation, Information Exchange Gateway (IEG), Cross Domain/Border Solution

1.2 Conventions, Terminology & Acronyms

This section of the document specifies the conventions and formatting information used throughout the whole ST Document.

1.2.1 Acronyms

Acronym	Expansion
TOE	Target of Evaluation
ST	Security Target
TSP	TOE Security Policies
VAG	Virtual Air Gap
FW	Firewall (Packet Filter)
NIDS	Network Intrusion Detection System
HIDS	Host-based Intrusion Detection System

1.2.2 Conventions

In this Security Target (ST) document some notations and conventions, which are taken from the Common Criteria v3.1R5 have been used in order to guide the reader.

In specifications of the functional requirements under Section 6, the functional components are interpreted according to the “assignment”, “refinement” and “selection” operations.

- The outcome of the assignment operations is shown with **bold** and identified between “[**brackets**]”.
- The outcome of the selection operations is shown with **bold** and ***underlined*** and identified between “[**brackets**]”.
- The outcome of the refinement operation is shown with **bold** items separated with commas **(“,”)** and identified between “[**brackets**]”.
- The iterated components are shown as **ComponentID/”IterationLabel”.**

1.2.3 Terminology

The following terminology is used throughout this ***Security Target (ST)*** document.

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

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

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

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

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**.

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**.

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. Two different technologies could be used for this purpose:

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

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

Access Control: Security service that controls the usage of assets defined in the TOE.

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).

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.

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 ot 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.

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.

System Information: vag-int status, vag-ext status, bandwidth information, liveliness between vag-int and vag-ext, active user session(s) kept in the management interface, firewall status, IDS status and network status.

Configuration Data: Network (Ethernet) interface definition, IDS status, packet filter rules, web rules and mail rules seperately set for **vag-int** and **vag-ext**.

Backup: A system backup of either **vag-int** or **vag-ext** containing shared storage configuration information, network configuration information, all application level protocols' configuration information, users information, audit information and alert information.

Snapshot: A system snapshot of either **vag-int** or **vag-ext** containing system state for a particular time-stamp.

Encryption/Decryption Key (ED-Key) Set: Keys dynamically created by the TOE and used in symmetric encryption and decryption of messages *(sk, IVin, IVout)*.

Message Signing/Verification Key (MSV-Key): Key-pair used in signing and verification of messages.

Cryptographic keys: The ED-Key and the MSV-Key are collectively known as *'cryptographic keys'*. These are secret data used for cryptographic operations.

Cryptographic operation: A cryptographic algorithm's action that perform one of the following operations;

- transforming plain text into cipher text.
- transforming cipher text into plain text.
- computing a digital signature from data.
- verifying of a digital signature

Packet Filter (Firewall): A rule-based software that is configured via management interface to mediate (impose rules for) the information flow.

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.

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

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.

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

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.

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

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.

AP: Application Protocol.

APDU: Application Protocol Data Unit.

Supported APs: Those APs that are supported by the TOE. These APs are Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), File Transfer Protocol Secure (FTPS), Transport Layer Security (TLS), Session Initiation Protocol (SIP), and Real-time Transport Protocol (RTP), Websocket (WS), Network Time Protocol (NTP).

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**).

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

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

1.3 TOE Overview

1.3.1 TOE Usage

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 seperating 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.

VAG is designed for environments for which there is a need for secure data exchange between two networks (*INT-Net* and *EXT-Net*) of different security levels. It provides web, mail, file transfer, VoIP services and some other APs for data interaction while preventing security threats towards organization's critical operations.

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

© All rights reserved.

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 harware infrastructure. Figure-1 depicts the general architectural view of the whole system and the environment.

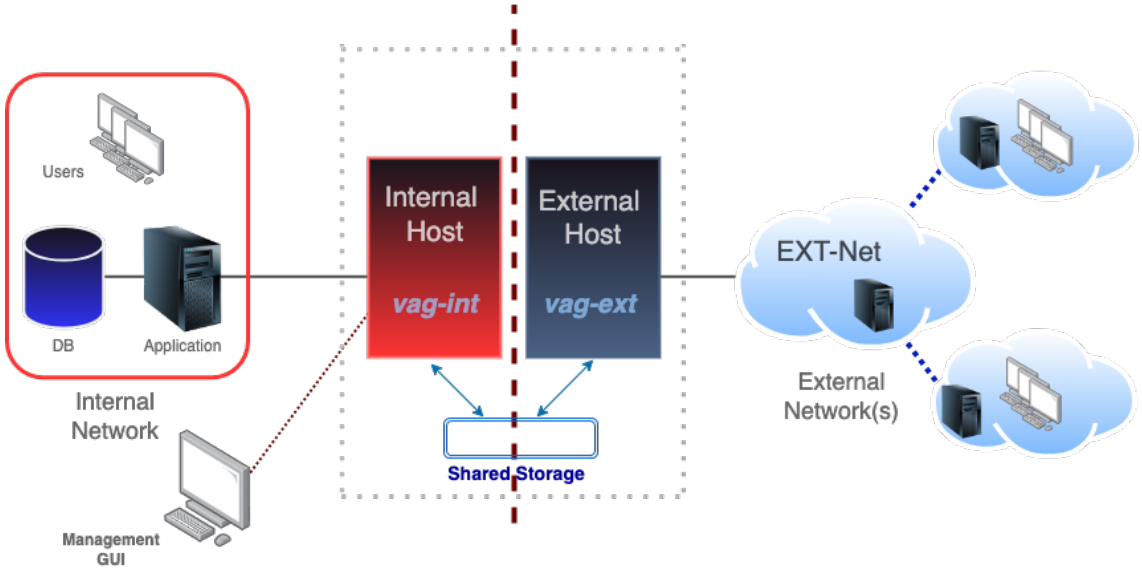


Figure 1. *General Architecture of Virtual Air Gap and the Operational Environment*

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**).

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, snapshots, administrative users, audit logs and user passwords.

The TOE performs user identification and authentication and appliess 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 *(consolemaintenance)* that is able to access the system through the Linux tty terminal to perform administrative functions. The TOE environment (Linux) performs the identification and authentication of this user.

This user *(consolemaintenance)* is able to perform administration functions that are listed in the Logical Scope section.

© All rights reserved.

The 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.

Data flow encryption key for each and every connection is dynamically created, negotiated and shared by both parts (**vag-int** and **vag- ext**) during session establishment.

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.

As indicated in the previous paragraph, 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. It invokes four cryptographic operations on the data packets (payload) flowing between message layer and media access layer. These are: (i) crypt, (ii) sign, (iii) verify signature (iv) decrypt. Under the operational environment, sending side first encrypts the payload and then signs it. Receiving side first verifies the signature and then decrypt the payload. This way, shared storage contains signed and encrypted data packets, which can only be properly accessed by the peer host.

All possible abnormal conditions 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 automated procedure searches the audit logs for predefined attack patterns and generates alarms in case of detecting such an event occurrence. The TOE is able to take certain actions under such circumstances.

© All rights reserved.

1.3.2 TOE Type

TOE Type is classified under *Boundary Protection Devices and Systems*. TOE is compliant with **CC/EAL4+** (with the augmentation of **ALC_FLR.2** and **AVA_VAN.5**).

Virtual Air Gap (VAG) is a software product that runs on two separate hosts (VAG-Int and VAG-ext), controlling bi-directional data flow between the two networks, INT-Net and EXT-Net. These hosts utilize a storage placed in between to provide isolation (air gap) by exchanging only the pure payload of each and every connection.

Configuration management, and survelliance functionality is accessible through VAG Management Interface via a Web Browser on INT-Net side. The user can view *System Status* info as well as view and/or update the *System Configuration*.

VAG provides secure and controlled data exchange between connected two networks (INT-Net and EXT-Net) having different security levels.

1.3.3 Required non-TOE Hardware/Software/Firmware

Following table depicts environmental (nonTOE) components of the system.[1]

Requirements	Descriptions	Version & Specifications
Deployment Network Infrastructure	- Internal and external network interfaces	INT and EXT hosts ethernet interfaces to be connected to corresponding switches' ports.
Invictus Hardware	- Internal and external hosts, - Local Disk Storage, - RAM, - Processor, - Monitor	-There are two identical servers. Each will have (as a minimum); - 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).

[1] VAG v3.0.3

Requirements	Descriptions	Version & Specifications
Invictus Software (non-TOE)	- OS, - Packet Filter, - IDS, - HIDS	- 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	- Management GUI Host	- Any desktop computer capable of running; - a desktop OS (MS Windows, MacOS, Linux) providing compatibility with a COTS (Common of the Shelf) web browser (IE, Firefox, Opera, Chrome, Safari)
Management Console Software	- Operating System and Web Browser	- Any OS supporting any of the following Web Browsers: - Microsoft Edge 100 and above, - Firefox 90 and above, - Chrome 100 and above, - Opera 90 and above, - Safari 14 and above
Disk Storage Hardware	- Disk Array	- 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	- PCI-e Shared Memory Card	- RDMA support (provided by Invicta)

1.3.4 TOE Security Features (TSF)

The security functionalities of the TOE are the followings:

- **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** .
- **Access control**: The TOE performs an access control for administrative users of the management interface, as well as 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 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.

1.4 TOE Description

VAG is designed for provisioning fundemental features of a secure Information Exchange Gateway (IEG). It is classified as a Cross Border/Domain Solution. With its unique design for isolation (air gapping) it sits in between two networks having different security levels and allowing bi-directional communication via supported APs' services, while preventing and defeating of security threats.

1.4.1 Physical Scope

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.

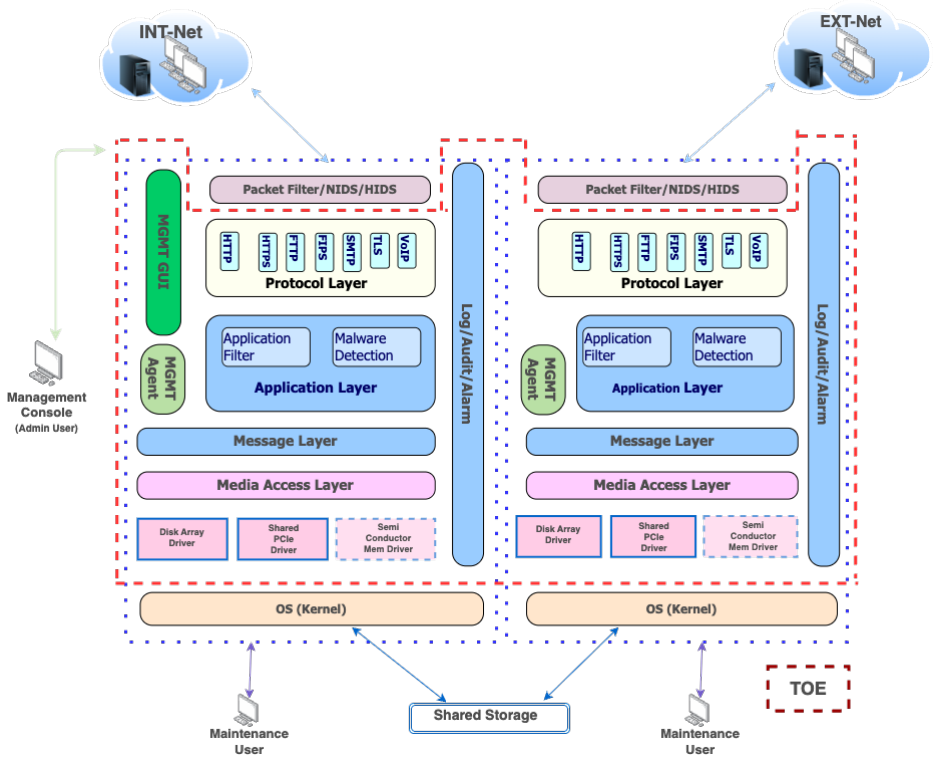


Figure-2 *Physical Scope of TOE*

© All rights reserved.

Note: *SemiConductor Memory depicted in dashed lines is a near-future functionality of the TOE that is not available in the scope of this ST.*

Physical deliverable software components including TOE are described in the following (first) table. **vag-ISO** contains the TOE as well as other components.

Distribution Component	Description
vag-tokens	Two USB Flash Disks containing pub/pri key pairs for successful initalization of the system, and for internal cyryptographic operations.
vag-ISO	A USB Flash Disk in an installable ISO image format, which contains TOE, other sytem 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.

vag-ISO (including TOE), **vag-tokens**, and **vag-user-guidance** is delivered to the customer by an Invicta's authorized service personnel.

The TOE is contained in **vag-ISO**. Components of the TOE are explained in the following table.

TOE Component	Description
vag-int, vag-ext	VAG software including Management Components, Alarm, Log, Audit, Application Layer, Message Layer, and Media Access Layers is identical –symmetrical- software having different binary names on internal and external hosts. **Mgmt-GUI** is included in **vag-int**.
vag-mgmt	VAG software components that run on (i) a client web browser, (ii) internal host, (iii) external host and collectively provide services of management interface to the administrative users.
Mgmt-GUI	VAG software sub-component of **vag-mgmt** to interact with *Admin Users*. This sub-component has a client part which runs on the client's web browser as well as a server side part which runs on **vag-int**.
Mgmt-Agent	VAG software sub-component of **vag-mgmt** to perform management actions on both hosts.
Logging	VAG software feature to record events of VAG software components.
Audit	VAG software feature to record important events of VAG software components.
Alarm	VAG software feature to notify events of different security levels.
Protocol-Layer	VAG software component that provides protocol-specific proxy services for secure data transmission between two hosts vag-int and vag-ext.
Application-Layer	VAG software component for implementing additional customer requirements (delivered as non-functional).

TOE Component	Description
Message-Layer	VAG software component to establish and sustain connections between two hosts **vag-int** and **vag-ext**.
Media-Access-Layer	VAG software component to access media for passing the data (payload).
Disk-Array-Driver	VAG software sub-component to access Disk-Array for retreiving/submitting (reading/writing) the data (payload).
Shared-PCI-Driver	VAG software sub-component to access PCIe Shared Memory for retreiving/submitting (reading/writing) the data (payload).

1.4.2 Logical Scope

TOE System Components and Their Functions

The modules (TOE Components) surrounded by red dashed lines in Figure-2 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.

Security Functions of the TOE components are introduced in the following sub-sections.

1.4.2.1 Management and Maintenance (MM) Functionality

Management interface of the TOE is the web interface, from where the administrative users based on their associated security level can monitor and/or configure some or all components of the system.

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

The TOE performs authentication and identification of administrative users by using a username/password pair. After succesfull login, an access control policy is exercised in order to determine access rights for this administrative user.

The TOE enforces a strict access control policy for managing security attributes, ensuring that only authorized administrators can modify critical settings, such as the administrative user role. It maintains a list of security attributes, including user roles and credentials, to support secure user authentication and role-based access control. The system requires administrative users to follow a password policy with a minimum of 8 characters and limits login attempts to 3 retries for accuracy.

Additionally, the TOE provides permissive default values for security attributes essential to enforcing the Security Function Policy (SFP). These default values can be adjusted by administrators when creating or modifying objects, ensuring flexibility while maintaining the security and integrity of the system's access control.

Administrative Users of the system are categorized into 3 groups, in increasing priviledge order.

- **Operator:** This kind of users have the least privileges. They can open multiple sessions from different client

hosts. They are able to perform the following actions:

- Read system information.
- Partially read configuration data.
- Change own password.
- Read audit logs.

• **Manager:** Managers can perform all the operations that an operator can, plus the following actions:

- Read complete configuration data and modify partial configuration data.
- Read administrative users list.
- Create backups and snapshots.
- Get list of available backups and snapshots.

• **Administrator:** Administrator of the system is a single entity having full control over all available functionalities of the management interface. Administrator can perform all the operations that a manager can, and additionally can perform the following actions:

- Modify Configuration Data.
- Create/Modify/Delete all administrative users other than itself.
- Change the password of any administrative user.
- Restore backups and snapshots.

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** system terminals through Linux Shell.

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*.

Maintenance User (consolemaintenance) can conduct a limited set of activities after a successful authentication. This set of limited actions is given below.

Administrative Functions Performed by the Maintenance User *(consolemaintenance)*

- Install patches (deb packages)
- Export logs
- Export full backups
- Restore full backups
- Change *(consolemaintenance)* password
- Admin Password Reset
- Stop and start application services
- Change network configuration
- Management Interface (Ethernet) Configuration
- Certificate Management
- Firewall Configuration
- Disk Array Configuration
- Liveness and Delay Measurement
- Debugging Mode Enable/Disable
- Syslog Server Configuration
- Remote Server Access (TCP/UDP)
- HTTP (L7) and Malware Protection Configuration

The TOE enforces the maintenance access control policy to ensure that only authorized Maintenance Users can export or import user data. When exporting logs and backups, the TOE ensures that no user-related security attributes (e.g., user roles, authentication credentials) are included, minimizing the risk of exposing sensitive information or security policies. Similarly, when importing user data from external sources, such as patches or backups, the TOE treats the data as neutral information, ignoring any associated security attributes. This ensures that only the necessary data is processed, maintaining the integrity of the system's security policies and protecting sensitive metadata throughout both the export and import operations.

1.4.2.2 Other System Functions

In this section, other system components are described along with their Security Functions. Security Objectives and Security Functions are described in *Section 4* and *Section 6* respectively.

Application Layer

Application layer of the system is basically responsible for passing AP payloads from protocol layer to message layer and vice versa. Based on the particular type of supported APs (e.g., HTTP, HTTPS, SMTP, FTP, FTPS, TLS, SIP or RTP, WS, NTP) this layer uses certain set of built-in malicious data pattern/signature rules to identify and filter out (block) malicious content. Clean data packets are forwarded to their intended destinations.

Message Layer

Message layer of the system is responsible for organizing the incoming and outgoing connections and data packets for supported APs. System uses proprietary data structures to transfer APDU packets between message layers of internal and external host.

Crypto Sub-Layer

Crypto sub-layer of the system is responsible for the invocation of cryptographic operations functionality thru a library (OpenSSL) provided by the operating system distribution. Functionality of this layer ensures that the incoming and outgoing messages are signed/encrypted and verified/decrypted respectively during a regular data flow between internal and external hosts (**vag-int** and **vag-ext**).

APDU packets are crypted and decrypted by using a symmetric key algorithm (AES-256-CBC), for which specific keys are generated and exchanged for a single connection/session and are never used again for any other connection/session. Those generated keys are destructed, once the connection/session is terminated.

APDU packets are signed and their signatures are verified by using an asymmetric algorithm (DSA/RSA). The private key and other side's public key are stored in the USB. Users can create and write their own keys on USBs at any time they wish.

Audit Facility

All the activity that takes place within the TOE is audited on hosts log files in respective locations .Audit data is available to be read by administrative users via management interface. Audit data can be exported by the Administrator and/or Maintenance User through the Linux Logging facilities.

Audit functionality of the system is always enabled (i.e., set ON)

Logging

The activity that takes place in the TOE's components, as well as in non-TOE components are sent to the logging system of the Invictus. These activity logs are stored on the local system. They can also be exported to a logging server via *rsyslogd* protocol upon proper configuration on the management interface by the the authorized user.

Alarm

All the activity that takes place in the OS is recorded by the logging components on 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.

© All rights reserved.

Media Access Layer

Main feature of this layer is to send/receive messages to/from the peer side by reading and writing crypted and signed messages from/to the shared storage (Disk Storage, Shared PCI Storage, or SemiConductor Memory). Sub-modules for accessing these media are also shon under the Media Access Layer.

> **Note:** *SemiConductor Memory depicted in dashed lines is a future functionality of the TOE that is not available in the scope of this ST.*

© All rights reserved.

2 CONFORMANCE CLAIM

This TOE's and ST's conformance claim is stated in the following sub-sections.

2.1 CC Conformance Claim

This TOE and ST are consistent with the following specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: SecurityFunctional Requirements, Version 3.1, Revision 5, April 2017, conformant.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements Version 3.1, Revision 5, April 2017, conformant.

2.2 PP and Package Claim

2.2.1 Protection Profile (PP) Claim

This ST makes no conformance claims of any certified Protection Profile (PP).

2.2.2 Package Claim

This ST makes conformance claims of **EAL4+** (EAL4 augmented with **ALC_FLR.2** and **AVA_VAN.5**").

This Security Target elaborated in conformance with "Common Criteria for Information Technology Security Evaluation, Version 3.1 Rev 5" contains the IT security requirements of the TOE and specifies the functional and assurance security measures to meet the stated requirements.

2.3 Conformance Rationale

The assurance level of EAL 4+ (ALC_FLR.2, AVA_VAN.5) is considered to be most appropriate for this type of TOE due to its critical positioning as a Information Exchange Gateway in security sensitive environments. Potential attacks are highligted in the assumptions, organizational security policies and the threats sections of Chapter 3.

© All rights reserved.

3 SECURITY PROBLEM DEFINITION

3.1 Threat Agents

Threats agents of the TOE are described in the table below.

Threat Agent	Description
External VAG User	Any person or software agent sending/receiving IP packets to/from TOE from external network. Attack potential of external VAG user is accepted as high.
Internal VAG User	Any person or software agent sending/receiving IP packets to/from TOE from internal network. Attack potential of internal VAG user is accepted as high.
Mgmt-GUI User	Any person having access to Management Interface with *(Administrator, Manager, Operator)* login credentials. Attack potential of this user is accepted as critical.

3.2 Assets

Assets of the TOE are described in the table below. Confidentiality, integrity and availability of these assets are fundamental for the proper operation of the TOE.

Asset	Description
Administrative User Credentials	Credentials of administrative users for TOE management interface.
Maintenance User Credentials	Credentials of the Maintenance User of the TOE.
Cryptographic Keys	The cryptographic keys that are used for encryption / decryption (ED-Key) and digital signature creation and verification (MSV-Key).
Audit Data	Audit data stored in the operational environment.
TOE Internal Communication	The communication channel between internal and external hosts of the TOE.
Configuration Data	The configuration data of the TOE and its operational environment.

3.3 Threats

Threats for the TOE are described in the table below.

Threat	Description
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.

Threat	Description
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.

3.4 Organizational Security Policies

OSPs	Description
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 this document.

3.5 Assumptions

Assumptions	Description
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.

© All rights reserved.

Assumptions	Description
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.

© All rights reserved.

4 SECURITY OBJECTIVES

4.1 Security Objectives for the TOE

Security Objective	Description
O.AUDIT	The TOE shall generate audit data that can be reviewed by authorized administrative users. All actions performed by a user shall be registered in the audit data.
O.AUTH	The TOE shall authenticate the administrative users before conducting operations through management interface.
O.ALARM	The TOE shall inspect audit / log data in order to generate alarms, and act in consequence.
O.ACCESSCONTROL	The TOE shall implement a **Management interface access control policy** to provide authorization to the administrative users according to their role.
O.FLOW	The TOE controls information flow between internal and external network. Messages (Payload) are exchanged between **vag-int** and **vag-ext** in encryped form by use of secure pub/pri keys and dynamically generated symmetric keys. This ensures seperation of wills of **vag-int** and **vag-ext**.
O.CRYPTOOP	The TOE uses (invokes) *OpenSSL* cytptographic library, which resides in operational environment (Debian Linux) for encrypt/decrypt and sign/verify messages of the communication between its internal and external hosts. In this respect, crptographic operations are initiated by the TOE and performed by the OpenSSL library. The TOE maintains the cryptographic keys in memory.
O.KACP	The TOE shall implement a **Keypair Access Control Policy** for importing keys and generation of IV pair for connection/session encryption.
O.MACP	The TOE shall implement a Maintenance Access Control Policy to restrict a specific maintenance role, for accessing the maintenance functions specified in OSP. Implementation of the access control policy will be based on the UserID attribute provided by the operating system login mechanism.

4.2 Security Objectives for the Operational Environment

Security Objective	Description
OE.PHYSECURE	The TOE must be kept in a physically secured location to prevent attacker from physically accessing the TOE.
OE.NOEVIL	The Maintenance User is 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.

© All rights reserved.

Security Objective	Description
OE.SECURECOMMUNICATION	The Operational Environment shall provide a secure communication channel between the TOE and the Management Console.
OE.CRYPTOOP	The Operational Environment shall provide encryption/decryption and sign/verify services to the TOE. Some of the cryptographic keys used for these operations are generated within the TOE, and some others are imported by 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.

4.3 Security Objectives Rationale

The following table shows the mappings between security objectives and threats/assumptions and security policies. The table is also stating the rationales for the mappings.

Threat / Policy / Assumption	Security Objective	Rationale
T.UNAUTH	O.AUTH	The objective of O.AUTH guarantees that only authenticated administrative user can access to the management interface via management console.
T.EAVESDROP	OE.SECURECOMMUNICATION	The objective of OE.SECURECOMMUNICATION is to prevent eavesdropping and similar type of internal attacks during the communication between management console and the management interface of the TOE.
T.OBTAIN	O.CRYPTOOP OE.CRYPTOOP	The objective of O.CRYPTOOP is to invoke the cryptographic operation functions provided by the operating environment. The objective of OE.CRYPTOOP is to ensure confidentiality and integrity of user data during the transfer between internal and the external host of the TOE by encryption, decryption, signing and signature verification.
T.CRYPTOKEYS	O.ACCESSCONTROL OE.PHYSECURE OE.NOEVIL	The objective of O.ACCESSCONTROL is to ensure that the access control policy for administrative users through the management interface will be exercised to avoid access to the cryptographic keys. OE.PHYSECURE guarantees that unauthorised physical access is not possible to the location where VAG is deployed, and OE.NOEVIL indicates that the unique users who can access to the physical location where VAG is deployed are trusted.

© All rights reserved.

Threat / Policy / Assumption	Security Objective	Rationale
T.MEDIATE	O.FLOW O.ALARM O.AUDIT O.ACCESSCONTROL O.AUTH	The objective of O.FLOW is to control the information flow between internal and external network and allow only encrypted data flow is passed to the other side and properly decrypted there. Both sides have their own credentials (not known by the other side). The Data Flow mechanism processes the APDU (Payload) as a transit item as not to interfere with any other TOE component having the potential of changing configuration data. All APDUs are controlled for any potential security breaches, including L7 attacks, malware, etc. The objective of O.ALARM is to assure a mechanism for automatic audit review in order to prevent predefined attack patterns, and act in case of attack detection. The objective of O.AUDIT is to assure that necessary audit logs will be generated and recorded for satisfaction of O.ALARM. The objective of O.ACCESSCONTROL is to ensure that the access control policy for administrative users through the management interface will be exercised to avoid access to the configuration data. The objective of O.AUTH guarantees that only authenticated administrative user can access the management interface to change the configuration data.
T.PRIVILEGES	O.ACCESSCONTROL	The objective of O.ACCESSCONTROL guarantees that authorized administrative users can read/modify data through management interface according to their access rights.
OSP.AUDIT	O.AUDIT	The objective of O.AUDIT is to associate each event with a user where applicable.
OSP.KACP	O.KACP	The OSP.KACP requires the implementation of a keypair access control policy to restrict the accessibility to cryptographic keys. The TOE shall implement such a Keypair Access Control Policy for secure importation of cryptographic keys and generation of IV pairs for each connection/session encryption.
OSP.MACP	O.MACP OE.USERID_PROVIDER	The OSP.MACP requires the implementation of an access control policy to restrict the accessibility to a set of maintenance functions directly through the **vag-int** or **vag- ext**. The TOE implements the access control policy for the set of functions as defined in O.MACP using the UserID of the user authenticated by the operating system. This UserID is to be provided to the TOE by the operating system (OE.USERID_PROVIDER).
A.PHYSICAL	OE.PHYSECURE	This objective is to ensure that TOE will be protected against physical attacks.

© All rights reserved.

Threat / Policy / Assumption	Security Objective	Rationale
A.TIME	OE.TIME	This objective assures operational environment to provide reliable timestamps.
A.NOEVIL	OE.NOEVIL	This objective ensures that the administrator of the management interface and the Maintenance User are trained and do not intentionally cause threats on TOE.
A.SINGEN	OE.SINGEN	This objective ensures that TOE cannot be bypassed during communication with external network.
OSP.LOCK	OE.INITIALIZATION	This objective ensures that Maintenance User initializes TOE with the correct cryptographic keys on USB Flash Memory. Flash memory must be under the sole control of the Maintenance User.
A.INITIALIZATION	OE.INITIALIZATION	This objective ensures that Maintenance User initializes TOE with the correct cryptographic keys according to user guidance, and that the secure media containing the cryptographic keys will be under the sole control of this user.
A.PLATFORM	OE.PLATFORM	This objective states that TOE is not protected against a compromise in the operational environment.

© All rights reserved.

5 SECURITY REQUIREMENTS

5.1 Security Functional Requirements

The following table summarizes the Security Functional Requirements stated in this Security Target including their dependencies. The first column indicates the SFR, the second column specifies the dependencies for that SFR, and the third column indicates the way the dependencies have been satisfied. For the non-satisfied dependencies, a rationale (identified by a cardinal) is included under the table.

SFR	Dependencies	Satisfied (Y or N)
FAU_ARP.1	FAU_SAA.1	**Y** (FAU_SAA.1)
FAU_GEN.1	FPT_STM.1	(FPT_STM.1) **N (1)**
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	**Y** (FAU_GEN.1) (FIA_UID.2) **N (2)**
FAU_SAA.1	FAU_GEN.1	**Y** (FAU_GEN.1)
FAU_SAR.1	FAU_GEN.1	**Y** (FAU_GEN.1)
FAU_SAR.2	FAU_SAR.1	**Y** (FAU_SAR.1)
FCS_COP.1/a	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	**Y** (FCS_CKM.1) **Y** (FCS_CKM.4/a)
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	**Y** (FCS_CKM.2/a) **Y** (FCS_COP.1/a) **Y** (FCS_CKM.4/a)
FCS_CKM.2/a	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	**Y** (FDP_ITC.2) **Y** (FCS_CKM.1) **Y** (FCS_CKM.4/a)
FCS_CKM.4/a	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	**Y** (FDP_ITC.2) **Y** (FCS_CKM.1)
FCS_COP.1/b	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	**Y** (FDP_ITC.2) (FCS_CKM.4/b) **N (4)**
FCS_CKM.4/b	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	**Y** (FDP_ITC.2)
FCS_COP.1/c	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	**Y** (FDP_ITC.2) (FCS_CKM.4/c) N **(4)**
FCS_CKM.4/c	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	**Y** (FDP_ITC.2)

© All rights reserved.

SFR	Dependencies	Satisfied (Y or N)
FDP_ITC.2	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	**Y** (FDP_ACC.1/MAINTENANCE) (FTP_ITC.1) **N (8)** (FPT_TDC.1) **N (7)**
FDP_ACC.1/MANAGEMENT	FDP_ACF.1	**Y** (FDP_ACF.1/MANAGEMENT)
FDP_ACF.1/MANAGEMENT	FDP_ACC.1 FMT_MSA.3	**Y** (FDP_ACC.1/MANAGEMENT) **Y** (FMT_MSA.3)
FDP_ACC.1/MAINTENANCE	FDP_ACF.1	**Y** (FDP_ACF.1/MAINTENANCE)
FDP_ACF.1/MAINTENANCE	FDP_ACC.1 FMT_MSA.3	**Y** (FDP_ACC.1/MAINTENANCE) (FMT_MSA.3) **N (5)**
FDP_ETC.1	[FDP_ACC.1 or FDP_IFC.1]	**Y** (FDP_ACC.1/MAINTENANCE)
FDP_IFC.1	FDP_IFF.1	**Y** (FDP_IFF.1)
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	**Y** (FDP_IFC.1) (FMT_MSA.3) **N (6)**
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	**Y** (FDP_ACC.1/MAINTENANCE) (FMT_MSA.3) **N (5.1)**
FIA_AFL.1	FIA_UAU.1	**Y** (FIA_UAU.2)
FIA_ATD.1	None.	N/A
FIA_SOS.1	None.	N/A
FIA_UAU.2	FIA_UID.1	(FIA_UID.1) **N (2)**
FIA_UID.2	None.	N/A
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	**Y** (FDP_ACC.1/MANAGEMENT) **Y**(FMT_SMR.1) **Y** (FMT_SMF.1)
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	**Y** (FMT_MSA.1) **Y** (FMT_SMR.1)
FMT_SMF.1	None.	N/A
FMT_SMR.1	FIA_UID.1	(FIA_UID.1) **N (5)**

Non-Satisfied Dependencies Rationale

(1) The dependency for FPT_STM.1 Reliable Time Stamps is not met given that the TOE does not generate time stamps for audit logs. As stated in OE.TIME, the responsible entity for the generation of time stamps is the operational environment.

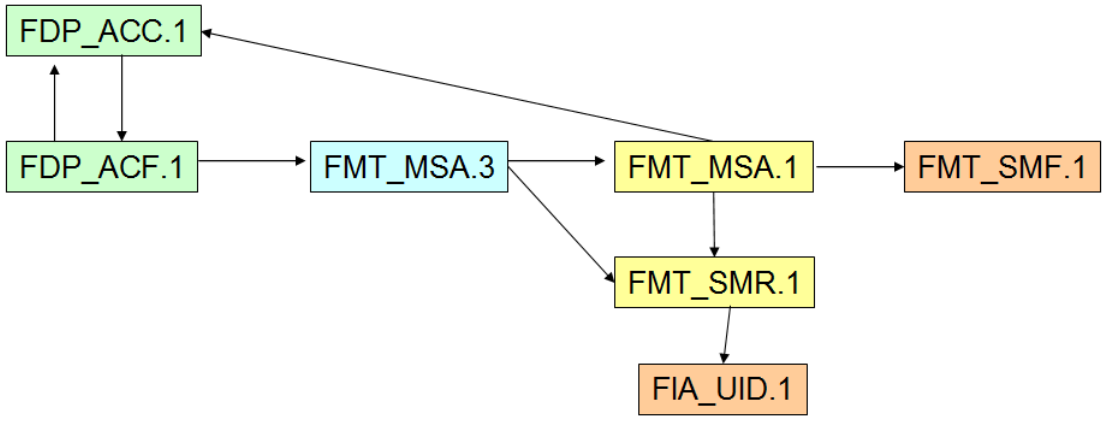
(2) The user identification for the Maintenance User is not performed by the TOE. As stated in OE.USERID_PROVIDER, the operational environment is responsible for providing the user ID of the Maintenance User to the TOE.

(3) The importation of the keys used for the cryptographic operations is performed by the initialization and start-up of the system and is defined as part of the TOE security architecture.

(4) The dependency for FCS_CKM.4 is not met for this component since the keys are not destructed by the TOE. However, the Maintenance User is able to regenerate asymmetric cryptographic keys and write them to USB Flash Memory (Token) as frequent as (s)he wishes. This operation would overwrite the previous keys, hence destructing them.

© All rights reserved.

(5) The FDP_ACC.1 and FDP_ACF.1 used to define an access control policy require the existence by dependencies of the following SFRs as depicted in the following chart:



The following dependencies have not been satisfied in the frame of the specification of the **maintenance access control policy**:

(5.1) FMT_MSA.3 & FMT_MSA.1 (FDP_ACC.1 and FDP_ACF.1). The policy attribute -UserID of the subject- is provided by the OS and not managed by the TOE.

(5.2) FIA_UID.1 (FMT_SMR.1). Although FMT_MS3.1 is not satisfied, the TOE maintains a set of roles including the maintenance role involved in this policy. For the user holding this role and allowed to access the objects defined in this policy, the UserID attribute needed is provided by the operating system (out of the scope of the evaluation) obtained in its login process (see OE.USERID_PROVIDER). Therefore the dependency with FIA_UID.1 is not satisfied.

(6) The dependency with FMT_MSA.3 is not satisfied, given that the security attributes of the data flow control policy are not configurable, and therefore, no management operations over security attributes for this data flow control policy is to be performed.

(7) The dependency with FPT_TDC.1 is not satisfied, since the TOE does not share any internal information or data with any third party IT product.

(8) The dependency with FTP_ITC.1 is not satisfied, since the key material is manually generated and imported by an authorized individual within a secure operational environment, without relying on any communication with an external trusted IT product.

© All rights reserved.

5.1.1 Security Audit

FAU_ARP.1 Security Alarms

FAU_ARP.1.1 The TSF shall take [**generate log, send notification for all alarms, stop data flow (put the system in passive mode) for critical alarms**] upon detection of a potential security violation.

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **[minimum]** level of audit;
and

c) [**the following Audited Events**

System alarms
Actions derived from potential security violations
Proxy accepted requests
Proxy denied requests
Users access to the TOE
Successful/Unsuccessful authentication attempts
Dataflow filters results
All management functionality of FMT_SMF.1
]

Application Note: *Start-up of audit functions is performed at the TOE initialization phase, and then is never shutdown while the TOE is up and running; i.e., audit functionality is always ON.*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~**PP**~~**/ST**, [**none**].

© All rights reserved.

FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note: *The TOE associates users with the auditable events, whenever these events are generated by an Administrative User's or the Maintenance User's action. Otherwise, the TOE will only log the event itself, such as the information flow of supported APs between internal and external networks.*

FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of **[**

Rule Name	Definition
ALRM_CRIT	Any message by any TOE component containing ”CRIT” or ”VAG_CRIT” keyword Any message by any TOE (Management) component containing ”MGMT_CRIT” and ”Critical Disk Space” keyword
ALRM_ERR	Any message by any TOE component containing ”ERROR” or ”VAG_ERR” keyword
ALRM_LOG	Any message by any component containing ”VAG_ALRT” or ”VAG_CRIT” or ”VAG_ERR” or ”VAG_BUG” or ”ERROR” or ”CRIT” keyword
ALRM_VAG	Any message by VAG containing ”[VAG]” keyword
ALRM_MGMT	Any message by any TOE (Management) component
ALRM_LOGIN	Any message by OS containing ”login” keyword

© All rights reserved.

Rule Name	Definition
ALRM_HIDS	Any message by HIDS software containing keyword ”CRIT” or ”ERROR”
ALRM_NIDS	Any message by NIDS software
ALRM_KERNEL	Any message by OS containing ”kernel:” keyword
ALRM_MALWARE	Any message by OS containing ”malware” keyword

] that are known to indicate a potential security violation;

b) [none] .

FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [**all administrative users**] with the capability to read [**list of audited events in FAU_GEN.1**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users’ read accesses to the audit records, except those users that have been granted explicit read-access.

5.1.2 Cryptographic Support

FCS_COP.1/a Cryptographic Operation **Invocation**

FCS_COP.1.1/a The TSF shall **invoke the OpenSSL library to** perform [**encryption and decryption of session messages**] in accordance with a specified cryptographic algorithm [**AES-256-CBC**] and cryptographic key sizes [**256-bits**] that meet the following: [**FIPS 197 and NIST SP 800-38A**].

Application Note: *Encryption and decryption operations use ED-Key set* ***(sk, IVin, IVout)*** *that is generated for that particular session.*

© All rights reserved.

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RAND_bytes()**] and specified cryptographic key sizes [**256 bits**] that meet the following: [**OpenSSL Library**].

Application Note: *Encryption and decryption operations for messages (payload) of a connection/session uses different pairs of sk and IV for a particular direction ("in" or "out"). That is,* ***(sk, IVin)*** *is used for messages of "in" direction,* ***(sk, IVout)*** *is used for messages of "out" direction.*

FCS_CKM.2/a Cryptographic Key Distribution

FCS_CKM.2.1/a The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**message passing on a secure channel**] that meets the following: [**none**].

Application Note: *Generated ED-Key set sk, IVin, IVout items are encrypted by peer's public key (ppk) as described in FCS_COP.1.1/c, and then sent to the peer by inserting them into the connection message.*

FCS_CKM.4/a Cryptographic Key Destruction

FCS_CKM.4.1/a The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**clearing the memory**] that meets the following: [**none**].

Application Note: *Generated ED-Key set sk, IVin, IVout is used only for a single particular session. Once that particular session is terminated, the associated key set is no longer used, and is also cleared in memory.*

FCS_COP.1/b Cryptographic Operation **Invocation**

FCS_COP.1.1/b The TSF shall **invoke the OpenSSL library to** perform [**signing and signature verification of session messages**] in accordance with a specified cryptographic algorithm [**DSA** or **RSA**] and cryptographic key sizes [**1024-bits**] that meet the following: [**FIPS 186-4 (for DSA) and RFC 8017 (for RSA)**].

© All rights reserved.

FCS_CKM.4/b Cryptographic Key Destruction

FCS_CKM.4.1/b The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**regenerate and rewrite**] that meets the following: [**none**].

Application Note: *The Maintenance User is able to regenerate asymmetric cryptographic keys and write them to USB Flash Memory (Token) as frequent as (s)he wishes. This operation would overwrite the previous keys, hence destructing them.*

FCS_COP.1/c Cryptographic Operation **Invocation**

FCS_COP.1.1/c The TSF shall **invoke the OpenSSL library to** perform [**encryption and decryption of generated ED-Key set**] in accordance with a specified cryptographic algorithm [**DSA or RSA**] and cryptographic key sizes [**1024-bits**] that meet the following: [**FIPS 186-4 (for DSA) and RFC 8017 (for RSA)**].

FCS_CKM.4/c Cryptographic Key Destruction

FCS_CKM.4.1/c The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**regenerate and rewrite**] that meets the following: [**none**].

Application Note: *Exactly the same process described in FCS_CKM.4.1/b is used here.*

5.1.3 User Data Protection

FDP_ACC.1/MANAGEMENT Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [**management interface access control policy**] on **[**

List of Subjects;

Administrative Users

© All rights reserved.

List of Objects;

System Information
Configuration Data
Other Administrative Users
Administrative User List
Own Password
Audit Logs
Backups and Snapshots

List of Operations;

Read
Modify
Delete
Create
Restore].

FDP_ACF.1/MANAGEMENT Security Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [**management interface access control policy**] to objects based on the following: [

List of Subjects;

Administrative Users

List of Objects;

System Information
Configuration Data
Other Administrative Users
Administrative User List
Own Password
Audit Logs
Backups and Snapshots

List of Security Attributes for Subjects:

Administrative user Role

© All rights reserved.

List of Security Attributes for Objects:

None

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine whether a subject n operation among controlled subjects and controlled objects is allowed: [

The list of subjects is only granted access for list of operations on the list of objects according to their security attributes shown in table given below;

	System Info	Config Data[2]	Other Admin Users	Admin User List	Own Password	Audit Logs	Backups and Snapshots
Administrator	R	C R M D	C M D	R	M	R	R C RS
Manager(s)	R	C R PM D	NA	R	M	R	R C
Operator(s)	R	R	NA	NA	M	R	NA

].

Application Note: *The operations (privileges) are to be interpreted as follows:*

Read (R): *Can read the content.*

Modify (M): *Can modify the content.*

Partial Modify (PM): *Can partially modify (not all) the content.*

Create (C): *Can create an instance of the object (a user or a partial backup).*

Delete (D): *Can delete an instance of an object.*

Restore (RS): *Can restore a backup.*

NA: *Subject has no privilege over the object.*

[2] See Application Note in FDP_ACF.1.3

© All rights reserved.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].

Application Note (*): *The operator user can only read (i) the IDS status, (ii) the web status and parameters, (iii) the mail status and parameters from Configuration data.*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

Application Note: *The modification of "Other Administrative Users" includes the password change and the role change.*

FDP_ACC.1/MAINTENANCE Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [**maintenance access control policy**] on [

List of Subjects;

Maintenance User *(consolemaintenance)*

List of Objects;

USB Device
Certificates
Patch files
Own Password
Audit Logs
Backups
Network Configuration
Shared Storage Configuration
Partial Firewall Configuration
Service Status

List of Operations;

Read
Mount
Unmount
Modify
Install
Export
Restore
Start
Stop
].

FDP_ACF.1/ MAINTENANCE Security Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [**maintenance access control policy**] to objects based on the following: [

List of Subjects;

Maintenance User *(consolemaintenance)*

List of Objects;

- **USB Device**
- **Licence**
- **Certificates**
- **Patch files**
- **Own Password**
- **Audit Logs**
- **Backups**
- **Network Configuration**
- **Shared Storage Configuration**
- **Partial Firewall Configuration**
- **Service Status**
- **HTTP (L7) / Malware Config**
- **Management Interface (ETH) Config**
- **Admin Password**
- **Liveness / Delay**
- **Debug Mode**

List of Security Attributes for Subjects:

User ID

List of Security Attributes for Objects:

None

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

The list of subjects is only granted access for a list of operations that can be performed on the list of objects according to their security attributes. This is shown in the two tables given below;

	USB Device	**License**	**Certificates**	**Patch Files**	**Own Password**	**Audit Logs**
Maintenance User	Mount Unmount	Read	Read Modify	Install	Modify	Export

	Backup and Snapshot	**NW Config**	**Shared Storage Config**	**Partial FW Config**	**Service Status**
Maintenance User	Export Restore	Modify	Modify	Modify	Read Modify

	HTTP (L7) / Malware Config	**Managenent Interface (ETH) Config**	**Admin Password**	**Liveness and Delay**	**Debugging Mode**
Maintenance User	Modify	Modify	Reset	Read	Modify

].

© All rights reserved.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

> **Application Note - 1:** *As detailed in the SPD (OSP.MACP), the entity responsible for the Maintenance User Identification and Authentication is the Debian/Linux Operating System, on which the TOE runs. Once identification and authentication of the user have been performed by the operational environment (Debian/Linux), the User ID is provided to the TOE that uses this information to exercise the access control policy.*

> **Application Note - 2:** *The Maintenance User can access both parts of the TOE, **vag-int** and **vag-ext**, and therefore, this access control policy is applicable to both interfaces.*

FDP_ETC.1 Export of User Data without Security Attributes

FDP_ETC.1.1 The TSF shall enforce the [**maintenance access control policy**] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

> **Application Note:** *The TOE provides user data protection while exporting audit logs and full backups. This action can be performed by the Maintenance User through the Linux Shell.*

FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [**data flow control policy**] on [

List of Subjects:

VAG Users

Information (Data/Payload):

All data flow between internal and external network through the TOE and subject to cryptographic operations.

Operation:

Data Input/Output with cryptographic operations

].

FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [**data flow control policy**] based on the following types of subject and information security attributes: [

List of Subjects:

VAG Users

List of Subject Attributes:

Source IP Address

List of Information:

All data flow between internal and external network through the TOE

List of Information Attributes:

Destination IP Address
HTTP Header Contents
HTTPS Header Contents
FTP Header Contents
FTPS Header Contents
NTP Header Contents
SIP Header Contents
RTP Header Contents

SMTP Header Contents
TLS Header Contents
WS Header Contents

].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

For the data input, the access is granted if the Source IP address is allowed to access to the Destination IP address, and if the SIP, RTP, FTP, FTPS, TLS, HTTPS, HTTP, WS, NTP or SMTP header pass through the application filter.

For the data output, the access is granted if the Source IP address is allowed to access to the Destination IP address, and if the SIP, RTP, FTP, FTPS, TLS, HTTPS, HTTP, WS, NTP or SMTP header pass through the application filter.

].

FDP_IFF.1.3 The TSF shall enforce the [**none**].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [**none**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**none**].

FDP_ITC.1 Import of User Data without Security Attributes

FDP_ITC.1.1 The TSF shall enforce the [**maintenance access control policy**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].

Application Note: *The TOE provides user data protection while importing patch files and full backups. Import action can be performed by the Maintenance User via Linux Shell interface.*

FDP_ITC.2 Import of User Data with Security Attributes

© All rights reserved.

FDP_ITC.2.1 The TSF shall enforce the [**keypair flow control policy**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].

> **Application Note:** *Own Public/Private key pair and peer's public key are located on the USB Flash Memory (Token), and imported by the initialization process of the TOE. These keys are initially provided during first installation and could be regenerated and written on USB Flash Memory as many times as necessary by the Maintenance User.*

5.1.4 Identification and Authentication

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [**[3]**] unsuccessful authentication attempts occur related to [**authentication for administrative users (administrator, operator, manager)**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [**detected**], the TSF shall [**lock the administrative user account**].

> **Application Note - 1:** *This requirement is only applicable for administrative users that access the TOE through the management interface.*

> **Application Note - 2:** *The Administrator have the capability of unlocking Managers or Operators.*

> **Application Note - 3:** *Unlocking the Administrator is only possible by a reboot of the system. However, once the system is rebooted, all administrative users (including the Administrator) are unlocked.*

© All rights reserved.

FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user role, user credential**].

These attributes are securely maintained to support user authentication and role-based access control within the TOE.

FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**the following metric: the minimal password length is 8 characters**].

Application Note: *This requirement is only applicable for administrative users that access the TOE through the management interface.*

Application Note: *This requirement is not applicable for the default administrative user (administrator) account which has "admin" as username in default system.*

FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: *Authentication of administrative users is performed by the TOE. Authentication of the Maintenance User is performed by the operational environment (Debian/Linux).*

FIA_UID.2 User Identification Before any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

© All rights reserved.

Application Note: *The identification of Administrative users is performed by the TOE. The identification of the Maintenance User is performed by the environment (Debian/Linux).*

5.1.5 Security Management

FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [**management interface access control policy**] to restrict the ability to [**change_default** , **modify**] the security attributes [**administrative user role**] to [**administrator**].

TOE restricts access to the management interface and limits changes to security attributes, specifically the administrative user role, to authorized administrators only. Other users are not allowed to modify these attributes, which helps maintain the integrity and security of the TOE's user access management system.

FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [**management interface access control policy**] to provide [**permissive**] default values for security attributes that are used to enforce the SFP.

The TOE enforces the management interface access control policy by setting permissive default values for security attributes. These values are applied to ensure that the security attributes required for the enforcement of the Security Function Policy (SFP) are initialized in a flexible way, allowing easier management and access control.

FMT_MSA.3.2 The TSF shall allow the [**administrator**] to specify alternative initial values to override the default values when an object or information is created.

The administrator is allowed to specify alternative initial values for security attributes when creating objects or information, overriding the default values as needed.

© All rights reserved.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- **Configuration Data and Service Management**
- **Network Management**
- **Firewall Management**
- **Administrative Users Management**
- **Passwords Management**
- **Backup and Snapshot Management**
- **Audit Logs Management**
- **USB Device Management**
- **Read Licence**
- **Patch Management**
- **Certificate Management**
- **Shared Storage Management**

].

FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [**administrator, manager, operator, maintenance**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles

Application Note - 1: *The unique kind of users that can be created and associated to a role during the normal operation of the TOE is the administrative users. The administrator is able to associate the operator or manager role to new administrative users.*

Application Note - 2: *The maintenance role contemplates only a user, the Maintenance User, and there is no way of creating more users associated to this role.*

Application Note - 3: *There is a virtual user called "LOGWATCH" observed only in management interface alarm messages area, which is not an actual user but just an internal process identifier.*

© All rights reserved.

5.2 Security Assurance Requirements

The Security Assurance Requirements for the TOE are the Evaluation Assurance Level 4 augmented with ALC_FLR.2 and AVA_VAN.5. EAL4 is the highest mutually recognized level and TOE could be able to comply. The requirements for this level are listed below.

Table 1 ***Security Assurance Requirements***

Assurance Class	Assurance Component
ADV: 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
AGD:Guidance Documents	AGD_OPE.1 – Operational user guidance AGD_PRE.1 – Preparative procedures
ALC: 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_FLR.2 – Flaw reporting procedures ALC_LCD.1 – Development defined life-cycle model ALC_TAT.1 – Well-defined development tools
ASE: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
ATE: Test	ATE_COV.2 – Analysis of coverage ATE_DPT.1 – Testing: basic design ATE_FUN.1 – Functional testing ATE_IND.2 – Independent testing – sample
AVA:Vulnerability Assessment	AVA_VAN.5 – Advanced methodical vulnerability analysis

5.3 Security Functional Requirements Rationale

The following table shows that all SFRs contribute to at least one objective and all objectives are met at least by one SFR.

© All rights reserved.

	AUDIT	AUTH	ALARM	ACCESS CONTROL	FLOW	CRYPTOOP	KACP	MACP
FAU_ARP.1			X					
FAU_GEN.1	X		X					
FAU_GEN.2	X		X					
FAU_SAA.1			X					
FAU_SAR.1	X							
FAU_SAR.2	X							
FCS_COP.1/a						X		
FCS_CKM.1							X	
FCS_CKM.2/a						X		
FCS_CKM.4/a							X	
FCS_COP.1/b						X		
FCS_CKM.4/b							X	
FCS_COP.1/c						X		
FCS_CKM.4/c							X	
FDP_ACC.1/MG				X				
FDP_ACF.1/MG				X				
FDP_ACC.1/MT								X
FDP_ACF.1/MT								X
FDP_ETC.1								X
FDP_IFC.1					X			
FDP_IFF.1					X			
FDP_ITC.1								X
FDP_ITC.2							X	
FIA_AFL.1		X						
FIA_ATD.1		X						
FIA_SOS.1		X						
FIA_UAU.2		X						
FIA_UID.2	X	X		X				
FMT_MSA.1				X				
FMT_MSA.3				X				
FMT_SMF.1				X				X
FMT_SMR.1				X				X

The following table shows how the SFRs satisfy the security objectives.

Objective	Rationale
O.AUDIT	The generation of audit records is performed by FAU_GEN.1. FAU_GEN.2 is responsible for assigning the user identification provided by FIA_UID.2 to the records generated by identified users of the TOE. FAU_SAR.1 and FAU_SAR.2 provide the review capability to authorized users.

© All rights reserved.

Objective	Rationale
O.AUTH	The identification and authentication of administrative user that access through the management interface is conducted by FIA_UAU.2 and FIA_UID.2. The security attributes for each administrative user is maintained with FIA_ATD.1. The administrative user passwords follow the restrictions stated in FIA_SOS.1. The authentication attempts are controlled under FIA_AFL.1.
O.ALARM	FAU_GEN.1 and FAU_GEN.2 generate the audit records to be inspected by FAU_SAA.1 to detect potential violations. FAU_ARP.1 is the responsible of perform certain actions is case of detecting potential violations.
O.ACCESSCONTROL	The access control policy for administrative users is performed by FDP_ACC.1/MANAGEMENT and FDP_ACF.1/MANAGEMENT. The user identity of the administrative users is provided by FIA_UID.2. The management of the access control policy security attributes is conducted by FMT_MSA.1 and FMT_MSA.3. FMT_SMF.1 provides the management functionality available for each role after the access control. The security roles are maintained by FMT_SMR.1.
O.FLOW	The dataflow control policy is conducted by FDP_IFC.1, FDP_IFF.1. The data is subject to cryptographic operations with secure keys.
O.CRYPTOOP	The cryptographic operations invocation is conducted by FCS_COP.1/a, FCS_COP.1/b and FCS_COP.1/c. Key management functions are conducted by FCS_CKM.1, FCS_CKM.2/a, FCS_CKM.4/a, FCS_CKM.4/b and FCS_CKM.4/c.
O.KACP	Keypair Access Control Policy is enforced by the key import function, as defined in FDP_ITC.2, and supported by key management operations in CKM.1 and CKM.4 for secure key handling.
O.MACP	The access control for Maintenance User is conducted by FDP_ACC.1/MAINTENANCE, FDP_ACF.1/MAINTENANCE. The accessible functionality after the access control for the Maintenance User is defined in FDP_ITC.1, FDP_ETC.1 and FMT_SMF.1. The TOE maintains the maintenance role with FMT_SMR.1.

5.4 Security Assurance Requirements Rationale

The overall security claim of this Security Target is that the specified TOE is compliant with assurance level EAL4 with the augmentation of ALC_FLR.2 and AVA_VAN.5.

EAL4 is accepted as the suitable assurance level where TOE can be conformant. While the TOE will be connecting secure networks with public networks, it would be better to claim high attack potential and also in order to demonstrate the maintenance capability ALC_FLR.2 claimed.

© All rights reserved.

All the dependencies and requirements of the selected assurance level and augmented components are satisfied during the life cycle of the TOE.

© All rights reserved.

6 TOE SUMMARY SPECIFICATIONS

6.1 Audit (AUD)

Audit Alarms (AUD_ALR)

Automatic alarms will be generated in the audit logs, which can be seen via web interface when defined regular patterns are caught . According to the level of the pattern (either critical or non-critical) TOE will either put the TOE in passive mode or just send an information message to the administrators of the management console.

This functionality is satisfying the requirement FAU_ARP.1.

Audit Data (AUD_DAT) The TOE generates audit logs according to a predefined policy. The recorded events in the audit logs are the included in FAU_GEN.1. Where applicable, the events will be associated to their subjects.

This functionality satisfies the requirements stated in FAU_GEN.1 and FAU_GEN.2 by generating audit logs.

Audit Analysis (AUD_ANL) Audit logs will be automatically analyzed searching for predefined patterns and an alarm will be generated if any dangerous pattern is found.

This functionality satisfies the requirements stated in FAU_SAA.1 by collecting the audit logs from **vag-int** and **vag-ext** and then searching the logs against potential violations and generating alarms.

Audit Review (AUD_REV) Audit logs can be reviewed via management interface and only the authorized administrative users can be able to review the audit logs.

This functionality satisfies the requirements stated in FAU_SAR.1 and FAU_SAR.2 by allowing only administrative users with sufficient access rights to review audit logs according to their role.

6.2 Cryptographic Operation Invocation (CRP)

The TOE Environment will encrypt/decrypt, sign/verify the data flow between **vag-int** and **vag-ext** by using algorithms provided by the OpenSSL library upon invocation by the TOE.

Cryptographic operations on data flow is carried out on three different contexts: (i) key generation for symmetric cipher, and key encryption/decryption symmetric ciphering (FCS_COP.1/a, FCS_CKM.1, FCS_CKM.2/a, FCS_CKM.4/a), (ii) encryption/decryption of

© All rights reserved.

generated symmetric keys (FCS_COP.1/b, FCS_CKM.4/b), and (iii) signing/verifying messages (FCS_COP.1/c, FCS_CKM.4/c).

Public/private keys used in (ii) and (iii) are stored on USB Flash Memory (Token) and imported by initialization process (FDP_ITC.2).

6.3 Data Protection (DPT)

DP Management Access Control (DPT_ACT)

Three types of administrative user can access and configure certain TOE functions through the management interface. These three types are: administrator, manager and operator. Depending on their role, the will be able to access a certain set of management functions. The **management interface access control policy** is the responsible of providing access rights to administrative users taking into account the type of that administrative user. The accessible functionality for each type of user is the following:

Operator: This kind of users can open multiple sessions from different client browsers.

They are able to perform the following actions:

- Read system information.
- Partially read configuration data.
- Change its password.
- Read audit logs.

Manager: Managers can perform all the operations that an operator can, plus the following actions:

- Read complete configuration data and modify partial configuration data.
- Read administrative users list
- Create partial backups.
- Get list of available partial backups.

Administrator: Administrator of the system is a single entity having full control over allavailable functionalities of the management interface. S/he can perform all the operations that a manager can, and additionally can perform the following actions:

- Create/Modify/Delete administrative users.

- Change the password of any administrative user.
- Restore partial backups.

This functionality satisfies the requirements stated in FDP_ACC.1/MANAGEMENT and FDP_ACF.1/MANAGEMENT by enforcing access control policy for management interface.

DP Maintenance Access Control (DPT_ACM)

A Linux Shell access is provided for certain management purposes. This access is only available for the Maintenance User. This Maintenance User must perform an authentication and identification before conducting any action in the TOE. The responsibility of this authentication and identification belongs to the TOE environment (Debian Linux OS), which after this process will provide the user ID to the TOE. This user ID will be used by the TOE when exercising the **Maintenance Access Control Policy** to grant access to the Maintenance User to access the functionality described in **Administrative Functions Performed by the Maintenance User** subsection of Logical Scope.

This functionality satisfies the requirements stated in FDP_ACC.1/MAINTENANCE and FDP_ACF.1/MAINTENANCE by enforcing access control policy for Linux Shell.

DP Flow Control (DPT_FCT)

The TOE provides a **data flow control policy** between the internal and the external network. This **data flow control policy** allows only permitted packets flow through the TOE. This includes a malware detection and a packet filtering system. TOE uses white-list method which means only the permitted IP/protocol/ports can be used.

This functionality satisfies the requirements FDP_IFC.1 and FDP_IFF.1.

DP Import (DPT_IMP)

Maintenance User can import patch files and full backups to the TOE according to the **maintenance access control policy** .

This functionality satisfies the requirements stated in FDP_ITC.1.

DP Export (DPT_EXP)

Maintenance User can export audit logs and full backups from the TOE according to the **maintenance access control policy** .

This functionality satisfies the requirements stated in FDP_ETC.1.

© All rights reserved.

6.4 Identification and Authentication (IAU)

IA Authentication Failures (IAU_AUF)

The TOE provides login functionality in the management interface. The credentials of the administrative users are checked before granting access to the management interface accessible functionality. The TOE will disable the administrative user account if three (3) unsuccessful authentication attempts are reached. This functionality will limit the number of unsuccessful attempts, and therefore, it protects the management interface of the TOE against brute force attacks.

This functionality satisfies the requirements stated in FIA_AFL.1.

IA Password Quality (IAU_PQL)

Administrative users of the TOE can only choose passwords satisfying a certain quality metrics which will make the password powerful. During the modification of administrative user passwords, the TOE checks if the new password satisfies the password policy.

This functionality satisfies the requirements stated in FIA_SOS.1.

IA User Attributes (IAU_ATD)

The TOE controls, for each administrative user that access to the TOE through the management interface, its password and its role.

This functionality satisfies the requirements stated in FIA_ATD.1.

IA User Authentication (IAU_UAU)

Administrative users of the TOE are authenticated before conducting any action through the management interface.

This functionality satisfies the requirements stated in FIA_UAU.2.

IA User Identification (IAU_UID)

Administrative users of the TOE are identified through the management interface before conducting any action.

This functionality satisfies the requirements stated in FIA_UID.2

6.5 Security Management (SEM)

SM Security Attributes (SEM_SAT)

Only the administrator can modify the default value of administrative user role according to the management interface access control policy. The administrator is also able to

modify the role of other administrative users.

This functionality satisfies the requirements stated in FMT_MSA.1 and FMT_MSA.3.

SM Functions (SEM_FUN)

The following management functions are performed by TSF;

- Configuration Data management
- Administrative Users management
- Passwords management
- Backup/Snapshot management
- Audit logs management
- Patch management
- USB devices management
- Read License
- Service Management
- Network Management
- Firewall Management
- Snapshot Management
- Certificate Management
- Shared Storage Management

This functionality satisfies the requirements stated in FMT_SMF.1.

SM Roles (SEM_ROL)

TOE maintains four types of users that are named as *administrator*, *manager*, *operator* and *maintenance*. An administrative user can be administrator, manager or operator while the Maintenance User has the maintenance role using Linux tty terminal.

This functionality satisfies the requirements stated in FMT_SMR.1.

© All rights reserved.

7 Document Revision History

VAG Version	Revision No	Revision Reason	Date of Revision(s)
2.5.0			
	1.0a	First Draft	2021-01-22
	1.0b	Prepare to submit for Lab Evaluation	2021-01-30
	1.0c	After Evaluation Fixes	2024-06-24
	1.0d	Minor changes	2024-09-02
2.6.0			
	1.0e	After Evaluation (GR01) Fixes	2024-07-24
	1.1	Minor changes	2024-08-07
	1.1a	Minor changes	2024-08-08
	1.1b	Minor changes	2024-08-24
	1.1c	After Evaluation (GR01) Fixes	2024-09-02
	1.1d	After Evaluation (GR01) Fixes	2024-09-02
	1.1e	After Evaluation (GR01) Fixes	2024-09-02
	1.2	After Evaluation (GR01) Fixes	2024-10-22
	1.2a	Minor changes	2024-10-22
	1.2b	GR1 Fixes	2025-05-02
	1.2c	GR1 Fixes	2025-05-02
	1.2d	GR1 Fixes	2025-05-09
	1.2e	GR1 Fixes	2025-05-12
	1.2f	GR1 Fixes	2025-05-14
	1.2g	GR1 Fixes	2025-05-22
	1.2h	GR1 Fixes	2025-05-28
	1.2i	figure-2 fix	2025-06-02
	1.3	Minor changes	2025-06-10
	1.3a	Minor fix	2025-06-17
3.0.0			
	1.0	Version Update	2025-09-12
	1.0a	Minor change	2025-12-16
	1.0b	Minor change	2025-12-29
	1.0c	Minor change	2026-01-20
	1.0d	Minor change	2026-03-06
3.0.3			
	1.0	Environmental components updated	2026-05-13
	1.0a	SFR matchings and typos fixed	2026-06-05