HVL BARİYER v1.0.1

Security Target

Lite

Version No: 2.5

Index

1. ST Introduction

1.1 Security Target & TOE Reference

ST Title: HVL BARİYER v1.0.1 Security Target Lite

ST Version: v 2.5

TOE Reference: HVL BARİYER v1.0.1

CC Conformance: Common Criteria for Information Technology Security Evaluation, Version 3.1 (Revision 5)

Assurance Level: EAL4+ (ALC_FLR.1)

Keywords: DLP, Data Leakage Prevention

1.2 TOE Overview

TOE has been developed to manage the system that is used to prevent authorization disclosure or leakage of corporate information and data, and meets the cyber security needs of civilian and military organizations keeping sensitive data in “SECRET” confidentiality level.

This software, audit accessibility of data on all system units as network traffic, server systems and end user computers by correct users on its supposed place and prevent any type of data leak.

Highlights

-Windows driver implementation

-Big data analysis and management of vast amounts of data

-Dynamic rule set definition

-LDAP integration

-Reporting and visualization

-SIEM integration

File System Monitoring

-File name change

-File extension change

-File move (cut/copy)

-File edit

-File access

-File delete

Media Analysis & Monitoring

Devices which are defined as “SAFE” via the device serial code are monitored and authenticated by the DLP system.

Document Classification System

System allows administrators to classify documents and applications for DLP usage.

Alternate Data Stream (ADS)

The protocol allows every kind of document to be classified and stored.

Text Mining Operations

-Word search in document

-Content search in document

-Label search

-Header / footer search

-Keyword search

-Regular expression search

Screen Capture Monitoring

User screen capturing operations are monitored according to rules set through management server

Document Printing Monitoring

User document printing operations are monitored according to rules set through management server.

Dynamic Rule Set Definition

Through management system interface, rules and authentications can be defined dynamically.

User Based Role Authentication

With the Active Directory integration roles and rules can be applied to users/user groups within the domain.

Integration

-SIEM:

Integration to HAVELSAN SIEM system is available.

-Active Directory:

User / User Group information is retrieved from domain to define rule sets and deploys agents.

Software Black Listing Operation

Software and applications could be tagged and placed into black lists for restricted execution.

Advantages

-Developed not only as a service but also as a windows driver

-Clients serve both as DLP & SIEM Log Collector agent

-Ability to collect event logs & tail text based documents for update operations

-Dynamic reporting infrastructure

-Big Data analysis to handle huge amounts of data

1.2.1 TOE TYPE Usage & Major Security Feautres Of A TOE

Usage: HAVELSAN BARİYER manages the system that provides audit accessibility of data on all system units as network traffic, server systems and end user computers by correct users on its supposed place, and prevents any type of data leak.

The following features are the major security functionality of the TOE;

- **Audit:** TOE will generate audit logs in order to provide accountability for the administrators and users.
- **Cryptographic Support:** TOE should provide mechanisms for securely storage of user passwords using hash function using Bcrypt algorithm. Since hash functions does not require any additional keys no event of key creation or destruction occurs.
- **Identification, Authentication and Authorization:** TOE will successfully identify, authenticate and authorize its users.
- **Data Protection:** Using the access control functions TOE provides confidentiality and integrity of user and TSF data, such as leakage information collected from target computers, based on user roles and their permissions.
- **Security Management:** TOE will manage the security attributes and user roles.

1.2.2 TOE TYPE

TOE is a management web application for a Data Leakage Prevention System, developed by Havelsan, which prevents authorization disclosure or leakage of corporate information and data using agents installed in the targeted machines.

1.2.3 NON-TOE Hardware/Software/Fırmware

Minimum hardware and software requirements of TOE are listed below:

Hardware:

Server:

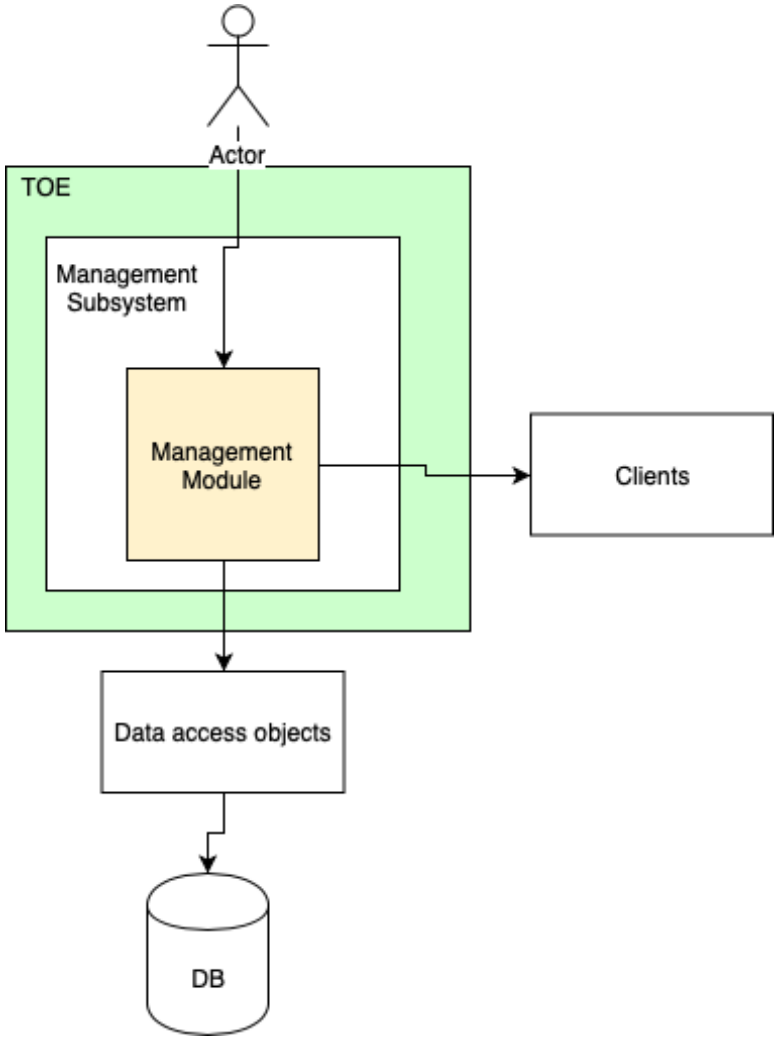
- 8 GB ram
  500 gb Hard Disk
  8 core processor

Software:

- Docker
- Docker Compose
- 64 bit os (Ubuntu 16.04.3)
- 3rd party database (MariaDB)

1.3 TOE Description

1.3.1 TOE Physical Scope



TOE scope is the green area in the figure . Since TOE is a software that works with 3rd party database applications are not included in the TOE Scope.

Delivery and Integration of TOE:

TOE is delivered to customers by a Havelsan representative. Deliverables are listed below:

-dlp-web-buildNumber.tar (Docker Image)

-dlp-db-buildNumber.tar (Docker Image) (out of TOE)

- setup.sh(Setup Script)

-Usage manual.pdf : User guide for TOE

Configuration for the evaluated version of TOE:

-Setup scripts are updated for each setup but all security functions explained in TOE come out of the box with each installation and do not require any other configuration.

1.3.2 TOE Logical Scope

Log Generation :

The TSF generates audit logs that consist of various auditable events. Date and time of events, type of events, usernames, and events taken by the authorized users are recorded.

Cryptographic Operations:

Hashing action is taken by the TSF for storing and authenticating users' passwords. Hashing action does not require any additional keys.

User Login and Authentication:

When a user issues a request to the TOE to access a protected resource, the TOE requires that the user (being a User, Administrator) identify and authenticate themselves before performing any action on behalf of the user. Identification and Authentication is required to ensure that users are associated with the proper security attributes (e.g. identity, group, roles, and security or integrity levels). Once the user attempts administrator defined unsuccessful authentication, his/her status is disabled and s/he will wait the status is enabled again by administrator. Users' passwords are controlled according to the organizational password quality requirements.

Protection of Data

The access control function permits a user to access a protected resource only if a user ID or role of the user is given permission to perform the requested action on the resource by Administrator. On the other hand, Administrators of the TOE can perform assigning the

privileges, modify his/her own authentication data and users' password.

User Roles and Security Rules

Only administrators are allowed to manage and configure security functions. Administrators can assign access privileges to users by user levels based on the functions or resources that they are allowed to perform. Additional functionalities such as modifying access privileges and unlocking password for users are also accessible by authorized administrator. Predefined roles are maintained and can be assigned to users.

Connection via Trusted Path

Users' sessions are forced to be established through trusted path.

TOE Access

If the session inactivity of users exceeds 10 minutes, the authorized users are returned to the login page. The users are also able to terminate their own sessions.

1.3.3 ROLE GROUPS

The TOE supports the following roles, which are subjects of the "User Access Control Policy":

a) User (Default User)
b) Admin Created Role Groups (Authorized User)
c) Administrator

The TOE implements an access control SFP named "User Access Control SFP". Associated roles with this SFP are described below:

a)User (Default User): Role has limited access to TOE. It is actually the most basic role in the TOE and it does not have any privileges. Initially created users have no responsibility unless they are associated with an admin created role group.

b)Admin Created Role Groups: Role groups in this document are created by administrator and users are binded to role groups to have authorizations so users in role groups with appropriate authorizations are referred as Authorized User in this document. This roles allow users to have different organisational responsibilities.

c)Administrator Role: An administrator in the TOE has every authorizations. It can create users, role groups , modify role groups' authorizations and associate users with role groups. Administrators can execute management functions via User Interface. In this document administrator is also referred as Administrator User, Authorised Administrator and Admin.

2. Conformance Claims

2.1 CC Conformance Claim

This Security Target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, CCMB-2017-04-001, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 5, CCMB-2017-04-002, [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 5, CCMB-2017-04-003, [3]

referenced hereafter as [CC].

This Security Target claims the following CC conformance:

- part 2 conformant
- part 3 conformant
- evaluation assurance level (EAL) 4+ (ALC_FLR.1)

2.2 PP Claim

- This ST does not claim conformance to any protection profile

2.3 Package Claim

This ST is conforming to assurance package EAL4 augmented with ALC_FLR.1 defined in CC part 3.

3. Security Problem Definition

This part of the ST defines the security problem that is to be addressed by the TOE. It consists of Organizational Security Policies, Threats and Assumptions.

3.1 Threats

T.UNAUTHORIZED_ACCESS: A malicious user may gain unauthorized access to the TOE and change the TOE configuration.

Threat agent: A malicious user

Assets: the TOE configuration

Adverse action: change the TOE configuration in such a way to result security flaws

T.EAVESDROPPING: Malicious Users could gain the valuable information (passwords and enterprise data) of authorized administrator by sniffing the traffic between agent and management server.

Threat agent: a malicious user

Assets: passwords and enterprise data

Adverse action: gain the valuable information by sniffing

T.NO_ACT_REC: Authorized users may change settings of TOE to not be held accountable for their actions related to the entities checked by the DLP that is controlled by TOE .

Threat agent: Authorized users

Assets: entities controlled by the DLP controlled by TOE

Adverse action: not be held accountable for their actions

3.2 Organizational Security Policies

There are no Organizational Security Policies for the application.

3.3 Assumptions

The assumptions are described in below;

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

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

A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

A.TIME_SERVER It is assumed that trusted time server provides reliable time information.

4. Security Objectives

In this section part-wise solutions are given against the security problem defined in Part 3.

4.1 Security Objectives for the TOE

The security objectives for the TOE are described in below;

O.AUTH : TOE will successfully identify and authenticate its users before allowing any actions. TOE maintains a role based access control and users are restricted with their role groups abilities. It is not allowed to take any action before being logged in. Secrets are verified with a mechanism and authentication failures are handles to maintain a more secure system.

O.PROTECTED_COMMUNICATION : The TOE will provide protected communication channels for administrators and authorized IT entities. TOE and authenticated users' connections are established using an SSL channel.

O.AUDIT : The TOE will provide the capability to generate audit data and match them with timestamps. Each events date, time, username and event name information are logged.

4.2 Security Objectives for the Operational Environment

OE.NETWORK Those responsible for the TOE must ensure that appropriate network layer protection, that there is a firewall in place that only permits access through required ports for external users to access the web-server.

OE.SEC_ENV Operational environment of the TOE shall ensure physical and environmental security of the TOE. Unauthorized access shall be restricted and all components in the operational environment shall be secured. Only specifically authorized people shall be allowed to access critical components.

OE.CREDEN Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users (by complying with organizational policies and procedures disallowing disclosure of user credential information) in a manner which maintains organizational IT security objectives.

OE.ADMIN	Administrator is non-hostile, well-trained, and follow all user guidance, installation guidance and configuration guidance.
OE.PHYSICAL	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system, network and any discrete execution environment provided to the TOE.
OE.TIME	Operational environment shall allow access to a reliable NTP server.

4.3 Security Objectives Ratıonale

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

Rationale tables of Threats, Assumptions and Security Objectives are given below:

Table1: Threats vs. Objectives table

Threats-Objective	O.AUTH	O.PROTECTED_COMMUNICATION	O.AUDIT	OE.NETWORK	OE.SEC_ENV	OE.CREDEN	OE.ADMIN	OE.PHYSICAL	OE.TIME
T.UNAUTHORIZED_ACCESS	X		X			X			
T.EAVESDROPPING		X		X	X			X	
T.NO_ACT_REC			X						X
A.ADMIN							X		
A.SEC_TRANS				X	X			X	
A.PHYSICAL				X	X			X	
A.TIME_SERVER									X

Threat, Assumption, or OSP	**Security Objectives**	**Rationale**

T. UNAUTHORIZED_ACCESS	**O. AUTH** **O.AUDIT** **OE.CREDEN**	The threat T. UNAUTHORIZED_ACCESS is countered by O. AUTH, OE.CREDEN, O.AUDIT where each users of the TOE will be successfully authenticated before any actions, TOE will generate audit logs to review user actions. TOE will provide security management functionality for user management.
T. EAVESDROPPING	**O. PROTECTED_COMMUNICATION** **OE.SEC_ENV** **OE.PHYSICAL** **OE.NETWORK**	The threat T. EAVESDROPPING will be countered by OE.PHYSICAL , OE.SEC_ENV, OE.NETWORK and O.PROTECTED_COMMUNICATION where O.PROTECTED_COMMUNICATION ensures that TOE will communicate via secure channels and information flow to third parties will be under security control , OE.PHYSICAL ensures that there is enough physical security provided to protect TOE from physical interactions with malicious users , OE.SEC_ENV which ensures that all hardware has been configured for the transmitting of secure data and managed securely and OE.NETWORK ensures that TOE relies upon a trustworthy network connection.
T.NO_ACT_REC	**O.AUDIT** **OE.TIME**	The threat T. NO_ACT_REC will be countered by O.AUDIT and OE.TIME which will log every action of users with

		reliable timestamps
A.ADMIN	**OE. ADMIN**	This assumption is addressed by OE. ADMIN which ensures that Administrators are experienced, trained and meet the security conditions.
A. PHYSICAL **A.SEC_TRANS**	**OE. PHYSICAL** **OE.SEC_ENV** **OE.NETWORK**	These assumptions are addressed by OE.PHYSICAL which ensures that TOE's physical environment has a trustworthy physical security , OE.NETWORK ensures that environment has a trustworthy network infrastructure and OE.SEC_ENV which ensures only specifically authorized people shall be allowed to access critical components.
A.TIME_SERVER	**OE.TIME**	This assumption is addressed by OE.TIME , which ensures that a connection to a trusted time server is provided.

Table 2. Security Objectives Rationale

5. Extended Components Definition

There is not any extended components definition within this Security Target.

6. Security Requirements

6.1 Security Functional Requirements

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE. The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Section 8.1 of Common Criteria Part1 [1]. The following operations are used in the ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed are ~~crossed out~~.

The **selection** operation is used to select one or more options provided by the CC instating a requirement. Selections having been made are denoted as underlined text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments are denoted by *italicized* text. If an assignment is done under a selection it will be denoted by ***italicized and bold*** text.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

Requirement Class	Requirement Component

FAU: SECURITY AUDIT	FAU_GEN.1 : Audit Data Generation
	FAU_GEN.2 : User Identity Association
FCS: CRYPTOGRAPHIC SUPPORT	FCS_COP.1 : Cryptographic operation
FDP: USER DATA PROTECTION	FDP_ACC.2 : Complete Access Control
	FDP_ACF.1 : Security attribute based access control
FIA: IDENTIFICATION AND AUTHENTICATION	FIA_AFL.1 : Authentication Failure Handling
	FIA_SOS.1 : Verification of Secrets
	FIA_UAU.2 : User authentication before any action
	FIA_UAU.7 : Protected authentication feedback
	FIA_UID.2 : User identification before any action
	FIA_ATD.1 : User attribute definition
FMT: SECURITY MANAGEMENT	FMT_MSA.1: Management of security attributes
	FMT_SMF.1 : Specification of management functions
	FMT_SMR.1 Security Roles
FTA: TOE ACCESS	FTA_SSL.1: TSF-initiated session locking
	FTA_SSL.4: User-initiated termination
FTP: TRUSTED PATHS	FTP_TRP.1 : Trusted Paths

List of SFRs

6.1.1 Class FAU: Security Audit

6.1.1.1 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 [not specified] level of audit; and

c) [*none*].

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 ST, [*date, time, username , event name*].

6.1.1.2 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.

6.1.2 Class FCS: Cryptographic Support

6.1.2.1 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [*hashing before storing passwords in database*] in accordance with a specified cryptographic algorithm [*Bcrypt*] and cryptographic key sizes [*none**] that meet the following: *[none[4]]*

Application note:
*: Hashing algorithms do not require any additional keys.

6.1.3 Class FDP: USER Data Protection

6.1.3.1 FDP_ACC.2 Complete Access Control

FDP_ACC.2.1 The TSF shall enforce the [*User Access Control SFP*] on [

Subjects:

- *User (Default)*
- *User role group (Admin defined groups)*
- *Administrator*

Objects:

- *User interface web pages' access privileges*] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.1.3.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [*User Access Control SFP*] to objects based on the following: [

-User role settings assigned to administrator defined role groups

-Users that are assigned to an administrator defined user role

-Administrators have all privileges.

].

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

-Administrator can take every action over every object

- Administrator can define User roles

- Administrator can modify user role settings

- Administrator can associate/deassociate User role groups with Users over application.

-User can take actions over objects based on their user role group's settings

].

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*].

6.1.4 Class FIA: Identification and Authentication

6.1.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when **[**an administrator configurable positive integer within *[**greater or equal to 5***]** unsuccessful authentication attempts occur related to [*login*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*block user for an admin defined time interval that is greater than or equal to 5 minutes*].

6.1.4.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*username, password, email, user role group, phone number, job info, sex*].

6.1.4.3 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

password must contain;

-at least 8 characters

-at least 1 lowercase character

-at least 1 uppercase character

-at least 1 numeric character

-at least 1 special character (!@#$%^&()-_=+,.?\/:;{}[]~)*

].

6.1.4.4 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.

6.1.4.5 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *[showing of asterisk characters on password field]* to the user while the authentication is in progress.

6.1.4.6 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.

6.1.5 Class FMT: Security Management

6.1.5.1 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [User Access Control SFP] to restrict the ability to [modify, delete, ***[enable user, disable user, change group]***] the security attributes **[***user group, password***]** to **[***administrator and authorized user***].**

6.1.5.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*create, delete, modify, and read security attributes defined in FIA_ATD.1*].

6.1.5.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [*administrator and admin created role groups*].

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

6.1.6 CLASS FTA: TOE ACCESS

6.1.6.1 FTA_SSL.1 TSF-Initiated Session Locking

FTA_SSL.1.1 The TSF shall lock an interactive session after [*10 minutes*] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: **[***relogin***]**.

6.1.6.2 FTA_SSL.4 User-Initiated Termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.1.7 Class FTP: Trusted Paths

6.1.7.1 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote and local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification ***and deletion***].

FTP_TRP.1.2 The TSF shall permit [remote and local users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***all actions***].

6.2 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 automation
	ALC_CMS.4– Problem tracking CM coverage
	ALC_DEL.1 – Delivery procedures
	ALC_DVS.1 – Identification of security measures
	ALC_LCD.1 – Developer defined life-cycle model
	ALC_TAT.1 – Well defined development tools

	ALC_FLR.1 – Basic Flaw Remediation
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.3 –Focused vulnerability analysis

Table3 . Security Assurance Requirements

6.2.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

Objectives	SFRs	Rationale
O. AUTH	**FIA_UAU.2,** **FIA_UAU.7,** **FIA_UID.2,** **FIA_AFL.1,** **FIA_ATD.1,** **FIA_SOS.1,** **FCS_COP.1 ,** **FTA_SSL.1** **FTA_SSL.4,** **FMT_SMR.1,** **FMT_MSA.1,** **FMT_SMF.1,** **FDP_ACC.2,** **FDP_ACF.1**	Before performing any action, FIA_UAU.2 forces TOE users to authenticate as well as identify provided by FIA_UID.2. FIA_UAU.7 provides multiple authentication mechanism for users. FIA_AFL.1 protects the TOE against brute-force attacks by introducing a protection mechanism. FIA_ATD.1 provides maintaining of security attributes such as: user id, name, e-mail, password, user role. FIA_SOS.1 also contributes to this objective due to the fact that by this component TSF defines the rules for secrets which contribute to the measures taken against unauthorized access. FCS_COP.1 provides hashing of user passwords. FTA_SSL.1 provides session termination after a defined period of inactivity. FTA_SSL.4 allows users to terminate their own session. FMT_SMR.1 associates users with role groups that include static & dynamic authorizations. FMT_MSA.1 applies the specified policy to manage

Objectives	SFRs	Rationale
		security attributes to authorized users. FMT_SMF.1 and FMT_SMR.1 determines the management functions and roles. FDP_ACC.2, FDP_ACF.1 specify access control policy details, information and rules on the management functions.

Objectives	SFRs	Rationale
O. AUDIT	**FAU_GEN.1, FAU_GEN.2**	Auditing requirements of TOE are defined by using FAU_GEN.1 and generated audit records are associated with users of TOE by FAU_GEN.2.
O. PROTECTED_COMMUNICATION	**FTP_TRP.1**	FTP_TRP.1 helps to establish a secure channel from the user's browser to DLP Management application (BARİYER) protecting the user data from disclosure and modification.

Table4. Security Functional Requirements Rationale

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Dependency Rationale

SFRs	Dependency	Dependency Met?
FAU_GEN.1	FPT_STM.1	Time stamps will be provided by operational environment.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Full-fit (FIA_UID.2 is hierarchical to FIA_UID.1)
FIA_AFL.1	FIA_UAU.1	Full-fit (FIA_UAU.2 is hierarchical to FIA_UAU.1)
FIA_ATD.1	-	-
FIA_SOS.1	-	-
FIA_UAU.2	FIA_UID.1	Full-fit (FIA_UID.2 is hierarchical to FIA_UID.1)
FIA_UAU.7	FIA_UAU.1	Full-fit (FIA_UID.2 is hierarchical to FIA_UID.1)
FIA_UID.2	-	-

FMT_MSA.1	[FDP_ACC.2] FMT_SMR.1 FMT_SMF.1	Full-fit
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	Full-fit (FIA_UID.2 is hierarchical to FIA_UID.1)
FTP_TRP.1	-	-
FCS_COP.1	[FCS_CKM.1] FCS_CKM.4	Crypto keys are out sourced.
FDP_ACC.2	FDP_ACF.1	Full-fit
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 is hierarchical to FDP_ACC.1 Default values for security attributes can not be changed
FTA_SSL.1	FIA_UAU.1	Full-fit (FIA_UAU.2 exists and it is hierarchical to FIA_UAU.1)
FTA_SSL.4	-	-

Table 5. Security Functional Requirements Dependency Rationale

6.3.2 Security Functional Requirements Rationale Table

	O.AUTH	O.PROTECTED_COMMUNICATION	O.AUDIT
FAU_GEN.1			X
FAU_GEN.2			X
FCS_COP.1	X		
FDP_ACC.2	x		
FDP_ACF.1	x		
FIA_AFL.1	X		
FIA_ATD.1	X		
FIA_SOS.1	X		
FIA_UAU.2	X		
FIA_UAU.7	X		
FIA_UID.2	X		
FMT_MSA.1	x		
FMT_SMR.1	X		
FMT_SMF.1	x		
FTA_SSL.1	X		
FTA_SSL.4	X		
FTP_TRP.1		X	

Table 6. SFR Rationale Table for TOE

6.3.3 Security Assurance Requirements Rationale

EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs. In addition, ALC_FLR.1 is chosen to provide additional quality assurance to the TOE.

7. TOE Summary Specification

7.1 TOE Security Functions

7.1.1 LOG GENERATION

The TSF generates audit logs for the following events:

All user actions

All admin actions

System actions (info, debug, error, warning)

Date and time of events, type of events and usernames are recorded. Audit logs are not allowed to delete within TOE and protected from unauthorized deletion by physical factors.

Implemented SFR's: FAU_GEN.1, FAU_GEN.2

7.1.2 CRYPTOGRAPHIC KEY MANAGEMENT & OPERATIONS

TOE provides mechanisms for securely storage of user passwords. Cryptographic key generation and destruction mechanisms are out of TOE's scope.

Hashing is provided by the TSF for storing and authenticating users' passwords.

Implemented SFR's: FCS_COP.1

7.1.3 USER LOGIN AND AUTHENTICATION

When a user issues a request to the TOE to access a protected resource, the TOE requires that the user identify and authenticate themselves before performing any action on behalf of the user. Users' passwords are controlled according to the following password quality requirements:

every password must have

at least 8 characters,

at least 1 number,

at least 1 uppercase letter,

at least 1 lowercase letter,

at least 1 special character.

Once the user attempts admin defined times of unsuccessful authentication, his/her status is disabled and her/his IP will be blocked for an admin defined interval.

The TSF shall maintain the following security attributes belonging to individual users:

username, password, email, user role group, phone number, sex and job info.

Implemented SFR's: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2

7.1.4 PROTECTION OF DATA

The access control function permits a user to access a protected resource only if a user ID or role of the user is given permission to perform the requested action on the resource by Administrator. On the other hand, Authorized administrators of the TOE can perform assigning the privileges, modify his/her own authentication data and users' password.

Implemented SFR's FDP_ACC.2, FDP_ACF.1, FMT_MSA.1

7.1.5 User Roles and Security Rules

Only administrators are allowed to manage and configure security functions. Authorized administrators are capable of performing the following management functions:

change active/passive state of a user

changing access control settings of users.

User roles are maintained by the TSF and users can be associated with these roles by authorized administrators. These roles are default user and admin by default. Also admins are able to create custom roles.

The TOE supports the following roles:

a) User (Default)
b) Admin Created Role Groups (Authorized User)
c) Administrator

The TOE implements an access control SFP named "User Access Control SFP".
User Access Control SFP states that:
User(role group) is the default role group and has no privileges. Administrator on the other hand has all the privileges and has ability to create role groups. After creating role groups and setting their authorizations administrator can bind users with role groups. Authorizations are not action based, they are page based and only users with related authorizations can see and use the pages.

Implemented SFR's: FMT_SMF.1, FMT_SMR.1

7.1.6 CONNECTION VIA TRUSTED PATH

TOE has secure connection control functions and it refuses any non secure requests so that users' sessions are always established through trusted path .

Implemented SFR's: FTP_TRP.1

7.1.7 TOE ACCESS

When a session is inactive for 10 minutes, the user session is locked, making the display contents unreadable and users access is disabled. The user has to re-login to gain access and display functions.

The session inactivity of users exceeds 10 minutes, the authorized users are returned to the login page. The users are also able to terminate their own sessions.

Implemented SFR's: FTA_SSL.1, FTA_SSL.4

8. References

[1] :Common Criteria Information Technology Security Evaluation Version 3.1 Rev 5 Part 1:

https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[2] : Common Criteria Information Technology Security Evaluation Version 3.1 Rev 5 Part 2 :

https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

[3] : Common Criteria Information Technology Security Evaluation Version 3.1 Rev 5 Part 3 :

https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[4] : PROVIDING PASSWORD SECURITY BY SALTED PASSWORD HASHING USING BCRYPT ALGORITHM :

ARPN Journal of Engineering and Applied Sciences , Sriramya-Karthika, July 2015 :

http://www.arpnjournals.com/jeas/research_papers/rp_2015/jeas_0715_2288.pdf