SECURITY TARGET OF BOER PRODUCT CLASSIFICATION AND AUTOMATION SOFTWARE

Version No	2.0
Release Date	24.05.2019
Document Code	BOER_BPCAS_ST
Language	English
Project	Boer Product Classification and Automation Software
Title	Security Target of Boer Product Classification and Automation Software
Prepared By	Boer Bilişim Sanayi ve Ticaret Anonim Şirketi

CONTENS

FIGURES

TABLES

1 DOCUMENT INFORMATION

1.1 REVISION HISTORY

Version No	Date	Author	Comment	Approve
1.0	13.12.2018	Servet YILDIZ	First Release	Cüneyt GARGİN
2.0	24.05.2019	Servet YILDIZ	Revised based on Observation Report (GK-1)	Cüneyt GARGİN

1.2 DOCUMENT TERMINOLOGY

ACRONYM	DEFINTION
CC	Common Criteria
CEM	Common Evaluation Methodology
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
ST	Security Target
BPCAS	Boer Product Classification and Automation Software
TOE	Target of Evaluation

1.3 REFERENCES

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 5, April 2017
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 5, April 2017

2 ST INTRODUCTION

2.1 ST REFERENCE

Title: Security Target of Boer Product Classification and Automation Software 1.0

2.2 TOE REFERENCE

Boer Product Classification and Automation Software v1.0

- BPCAS Web Panel Application v1.0
- BPCAS Web Admin Service Application :1.0

2.3 TOE OVERVIEW

2.3.1 TOE definitions and operational usage

Boer Product Classification and Automation Software has been developed to follow the classifying and shipping processes of the products. Boer Product Classification and Automation Software provides to users interfaces and communicate and coordinate the connected systems. The software is a service-based application that allows the processing and recording of data from the terminals in a safe and controlled manner.

2.3.2 TOE Major Security Features

- Access Control Mechanism
- Identification and Authentication
- Security Audit
- Security Management

2.3.3 TOE Type

Boer Product Classification and Automation Software is an application software that includes web application and services.

2.3.4 Non-TOE Hardware/Software/Firmware

The TOE operates in a web server environment. In addition to requiring services from the environment to achieve its primary aim, the TOE also relies on the environment to maintain a secure posture so that the application cannot be compromised by factors out of the TSF Scope of Control.

This section identifies peripheral software and hardware components, which TOE needs and interacts.

Mandatory components and their minimum requirements are given below.

Software Components	Usage	Specification
Web Server	The TOE operates on a web server as a web application.	IIS 7.0 .net 4.5
Operating System	The TOE needs an operating system to run. TOE operates on this operating system and uses the sources of this system.	Windows Server 2012
Browser	User need browser to access TOE functions.	HTML 5 compatibilty
Database	TOE saves all corporate data and user credentials in this database.	Oracle min R11

Hardware Components	Usage	Specification
Server	Hosted web Server and operating system run on the server.	Cpu: Min 4 Core 2 ghz Ram: Min 8 Gb Hdd: Min 128 Gb Extra:Ethernet,Usb
Client Computer	Users access the TOE with the browser on Client Computer	Cpu: Min 2 Core 1.5 ghz Ram: Min 2 Gb Hdd: Min 32 Gb

2.4 TOE DESCRIPTION

2.4.1 Physical Scope

Figure 1 shows the physical scope and environment of the TOE interacts.

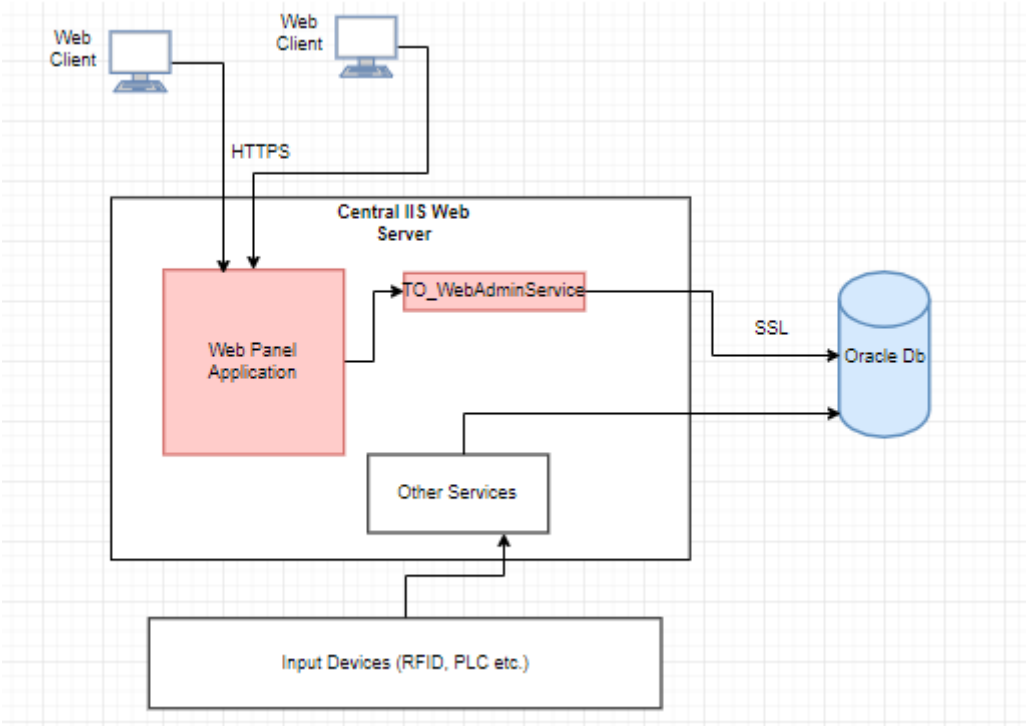

Figure 1 Physical Scope of TOE

The TOE is a software-only and includes following component

- **BPCAS Web Panel Application**

  This is the web application that management users use to define and report in the application. Users' access interfaces are provided by this application. It works on IIS web server.

- **BPCAS Web Admin Service Application**

  This web service is designed to communicate between internal servers. All functions and methods required by the web management application are provided through this service. Access to this service other than servers will not be allowed. IIS is running on web server

The table of TOE deliverables can therefore be described as follows:

Deliverable	Type	Form	Delivery Method
Boer Product Classification and Automation Software • BPCAS Web Panel Application • BPCAS Web Admin Service Application	Software	Binary	Software will be installed by developer. (courier delivery)

Deliverable	Type	Form	Delivery Method
BPCAS Kurulum ve Kullanıcı Kılavuzu Dokümanı	Document	Paper	Courier delivery

2.4.2 Logical Scope

Security Function	**TOE Scope Description**
Access Control	TOE provides access permissions to pre-authorized sources depending on the user name and the password. The data of "which users may have access to what kind of sources" is kept in the access control lists.
Identification and Authentication	When a user issues a request to the TOE to access the modules defined the TOE requires that the user (being User or Administrator) identify and authenticate themselves before performing any TSF mediated action on behalf of the user. The TOE checks the credentials presented by the user upon the login page against the authentication information in the database. Each users account only exists in the database that relates to the user organization. Authenticated users can access their relevant resources or functions once they have been successfully identified and authenticated using their usernames and passwords
Audit Mechanism	The TSF generates audit logs that consist of various auditable events. Date and time of events, usernames, and events taken by the authorized users are recorded. Authorized administrators have the capability to read and view all the recorded logs stated above through the web portal.
Management of TOE Functionality	The TOE provides support functionality that enable users to configure and manage TOE. At least one administrator is required to have full access rights to manage the TOE. Authorized 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 administrators.

3 CONFORMANCE CLAIMS

3.1 CC CONFORMANCE CLAIM

This Security Target and TOE claims conformance to

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

As follows

- Part 2 conformant,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, Revision 5, April 2017

Has to be taken into account during evaluation.

3.2 PP CONFORMANCE CLAIM

The ST does not claim conformance to any Protection Profile.

3.3 PACKAGE CONFORMANCE CLAIM

This Security Target claims conformance to package EAL2

4 SECURITY PROBLEM DEFINITION

This part includes description of roles, assets, threats, organizational security policies and assumptions.

4.1 ROLES

TOE User	: An end user of the TOE who is providing access and management of corporate information.
TOE Admin	: Authorized user who is providing management and configuration of the TOE.

4.2 ASSETS

Table 1: List of User Data

USER DATA	DESCRIPTION
Corporate Information	Any valuable information related to organization accessed through TOE. Production data, etc.
Audit Data	Records are related TOE access, management and configuration.

Table 2: List of TSF Data

TSF DATA	DESCRIPTION
User Credentials	Username and passwords of TOE users.
Group	A definition setting for TOE Group to grant permissions to Clients.
Group Permission	Permission definition granted to a group.

Both of TSF data and user data are named as TOE data. TOE data consists of both TSF data and user data

4.3 ASSUMPTION

This section defines the Assumptions on the TOE.

A.ENV_SEC

It is assumed that latest security settings of environmental components including; operating system, database, web server are completed. All security vulnerabilities are closed and taken all the necessary security measures against potential threats is also assumed.

A.LOCATE

It is assumed that TOE, Web Server and Database will be hosted inside of a physically secure area.

A.TRANS_PROTECT

It is assumed that the IT environment will provide a secure channel so that all potentially valuable information (including credentials and enterprise data) is protected between the client and application server.

A.TRUSTED_USR

It is assumed that the authorized users for TOE, web server and database are not careless, willfully negligent, or hostile.

A.SV_DB

It is assumed that only authorized and trained users can access the web server and database.

4.4 ORGANIZATIONAL SECURITY POLICIES

The TOE meets no organizational security policies.

4.5 THREATS

T.ACCS_CON

Threat Agent	: Attacker
Adverse Action	: An attacker try to unauthorized access TOE sources by web application to compromise TOE data and function
Asset	: TOE data and function

T.DATA_DISCL

Threat Agent	: Attacker
Adverse Action	: An attacker try to compromise the confidentiality of TOE data by manipulating via web application.
Asset	: TOE data

T.RECORDS

Threat Agent	: Attacker, TOE User, TOE Admin
Adverse Action	: Authorized or unauthorized access to TOE data or functions by using web application interface may go undetected. By this way, TOE data and function may be accessed in an uncontrolled way. Unauthorized access trial are also may not detected.
Asset	: TOE data and function

T.RECONFIG

Threat Agent	: Attacker, Unauthorized User
Adverse Action	: An attacker or unauthorized user attempts to reconfigure the TOE to gain access to protected TOE data and service.
Asset	: TOE data and service

5 SECURITY OBJECTIVES

5.1 SECURITY OBJECTIVES FOR TOE

This section defines the Security Objectives for the TOE.

O.ACC_CONTROL

The TOE shall ensure that only authenticated and authorized users can access the TOE functionality and protected application resources.

O.IDAUTH

The TOE shall provide measures to uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE

O.AUDIT

The TOE shall record the login actions taken by users, prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.

O.EADMIN

The TOE shall include a set of functions that allow effective management of its functions and data.

5.2 SECURITY OBJECTIVES FOR TOE OPERATIONAL ENVIRONMENT

This section defines the Security Objectives for the Operational Environment.

OE.ENV_SEC

Necessary configuration and security setting must be provided by qualified person for environmental components including; operating system, database, web server**.**

OE. PHYSICAL_PROTECT

The TOE should be in a secure physical environment that must be preserved and accessible. The Web Server and Database will be hosted inside of a physically secure area. The Only authorized person should be in the environment.

OE.TRUSTED_USR

Authorized users for TOE, web server and database must be well trained, careful and trusted.

OE.SV_DB

Access of the web server and database must be restricted only authorized users.

OE.TRANS_PROTECT

The IT environment shall provide the https communication between the Clients and application server. Application Server and Database communication must be protected by TLS.

OE.TRUSTED_CERT

The users (or administrators) of the TOE must be alerted if the certificate used for establishing the HTTPS session is not the right (or trusted) server certificate. If this happens, users (or administrators) must not to trust the server certificate.

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.TIME

The IT Environment will provide reliable timestamps to the TOE.

5.3 SECURITY OBJECTIVES RATIONALE

The table given below provides security problem definition covered by security objectives. Threats and OSPs are addressed by security objectives for the TOE and its operational environment. Assumptions are addressed by only security objectives for the operational environment

SECURITY OBJECTIVES FOR TOE ENVIRONMENT / THREAT/ ASSUMPTION/POLICY	O.ACC_CONTROL	O.IDAUTH	O.AUDIT	O.EADMIN	OE.ENV_SEC	OE. PHYSICAL_PROTECT	OE.TRUSTED_USR	OE.SV_DB	OE.TRANS_PROTECT	OE.TRUSTED_CERT	OE.CREDEN	OE.TIME
A.ENV_SEC					X							
A.LOCATE						X						
A.TRANS_PROTECT									X		X	
A.TRUSTED_USR							X			X	X	
A.SV_DB								X				
T.ACCS_CON	X	X										
T.DATA_DISCL	X				X			X				
T.RECORDS			X									X
T.RECONFIG	X	X		X	X							

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ENV_SEC	OE.ENV_SEC ensures that Necessary configuration and security setting must be provided by qualified person for environmental components including; operating system, database, web server.
A.LOCATE	OE. PHYSICAL_PROTECT ensures that physical security is provided where the access to the server and database are controlled.
A.TRANS_PROTECT	OE.TRANS_PROTECT ensures that communication between critical IT components are secured. OE.CREDEN ensures that credential security is completed by responsible parties.
A.TRUSTED_USR	OE.TRUSTED_USR ensures that authorized users for TOE, web server and database should be well trained, careful and trusted. OE.CREDEN ensures that credential security is completed by responsible parties OE.TRUSTED_CERT ensures that necessary action will be performed for certificate security.
A.SV_DB	OE.SV_DB ensures that only authorized users can access the Web Server and Database. OE.CREDEN ensures that credential security is completed by responsible parties
T.ACCS_CON	O.ACC_CONTROL ensures that only authenticated and authorized users can access the TOE functionality and protected application resources. O.IDAUTH ensures that uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.DATA_DISCL	O.ACC_CONTROL ensures that only authenticated and authorized users can access the TOE functionality and protected application resources. OE.SV_DB ensures that only authorized users can access the Web Server and Database. OE.TRANS_PROTECT ensures that communication between critical IT components are secured.
T.RECORDS	O.AUDIT ensures that the TOE generates audit reports to trace authorized users access events. OE.TIME ensures that the IT Environment will provide reliable timestamps to the TOE.
T.RECONFIG	The O.EADMIN ensures that the TOE has management functions for secure configuration. OE.ENV_SEC ensures that Necessary configuration and security setting must be provided by qualified person for environmental components. O.ACC_CONTROL ensures that only authenticated and authorized users can access the TOE functionality and protected application resources. O.IDAUTH ensures that uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE

6 EXTENDED COMPONENTS

Extended Components Definition There is no extended components.

7 SECURITY REQUIREMENTS

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from part 2 of [CC] and the assurance components as defined for the Evaluation Assurance Level 4 from part 3 of [CC].

7.1 SECURITY FUNCTIONAL REQUIREMENTS

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were extended.

The following notations are used for the definition of Security Functional Requirements:

Refinement operation (denoted in such a way that added words are in **bold text** and changed words are ~~**crossed out**~~): is used to add details to a requirement, and thus further restricts a requirement.

Assignment operation (denoted by ***italicized bold text*** and placed in square bracket): is used to select one or more options provided by the [CC] in stating a requirement.

Selection operation (denoted by underlined text and placed in square bracket): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.

Iteration operation are identified with a slash (e.g. "(/)"). It should be noted that the requirements in the following chapters are not necessarily be ordered alphabetically. Where useful the requirements have been grouped.

The following table summarizes all TOE security functional requirements of this ST:

FAMILY	DESCRIPTION
FAU: Security Audit	
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_STG.1	Protected Audit Trail Storage
FAU_STG.3	Action in Case of Possible Audit Data Loss
FIA: Identification and Authentication	
FIA_ATD.1	User Attribute Definition
FIA_UID.2	User identification before any action

FAMILY	DESCRIPTION
FIA_UAU.2	User authentication before any action
FIA_AFL.1	Authentication Failure Handling
FMT: Security Management	
FMT_SMR.1	Security Roles
FMT_MTD.1/ADMIN	Management of TSF Data (ADMIN)
FMT_MTD.1/USER	Management of TSF Data (USER)
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialization
FMT_SMF.1	Specification of Management Functions
FDP: User Data Protection	
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control

7.1.1 FAU Requirements (Security Audit)

7.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
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[selection: not specified] level of audit; and

	c) [assignment: • ***User Login*** • ***Log out*** • ***Batch Insert Action*** • ***Failed login attempt*** • ***DB Error*** • ***System Error*** • ***Exceptions*** • ***User Creation*** • ***User deletion*** • ***Application Parameter Modification***].
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, [assignment: ***source IP address].***

7.1.1.2 FAU_GEN.2 User Identity Association

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
FAU_GEN.2.1	The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

7.1.1.3 FAU_SAR.1 Audit Review

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [assignment: ***Authorized TOE Admin***] with the capability to read [assignment: ***all audit information***] 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.

7.1.1.4 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to [selection: prevent] unauthorized modifications to the stored audit records in the audit trail.

7.1.1.5 FAU_STG.3 Action in Case of Possible Audit Data Loss

Hierarchical to:	No other components.
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.3.1	The TSF shall [assignment: ***provide a notification by e-mail to TOE Admin***] if the audit trail exceeds [assignment: ***daily audit storage limit]***.

7.1.2 FIA Requirements (Identification and Authentication)

7.1.2.1 FIA_ATD.1 User Attribute Definition

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: • ***Username*** • ***User Group*** • ***User Role***]

7.1.2.2 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies.
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.

7.1.2.3 FIA_UAU.2 User Authentication Before any Action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
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.

7.1.2.4 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [selection: **[assignment: *an administrator configurable positive integer within [assignment: 3-99]***] unsuccessful authentication attempts occur related to [assignment: ***user authentication***].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [selection: *met*], the TSF shall [assignment**: *disabled the account***].

Application Note 1 Only Authorized TOE Admin unlock the account

7.1.3 FMT Requirements (Security Management)

7.1.3.1 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMR.1.1	The TSF shall maintain the roles [assignment: • ***TOE User*** • ***TOE Admin***].
FMT_SMR.1.2	The TSF shall be able to associate users with roles

7.1.3.2 FMT_MTD.1/ADMIN Management of TSF Data (ADMIN)

Hierarchical to:	No other components
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to [selection: change default] the [assignment: ***Authentication data including user name and password***] to [assignment: ***TOE Admin***].

7.1.3.3 FMT_MTD.1/USER Management of TSF Data (USER)

Hierarchical to:	No other components
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to [selection: modify] the [assignment: ***Own Authentication password***] to [assignment: ***TOE Admin and TOE User***]

7.1.3.4 FMT_MSA.1 Management of Security Attributes

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1	The TSF shall enforce the [assignment: ***BPCAS access control policy***] to restrict the ability to [selection: modify] the security attributes [assignment: ***Access control list***] to [assignment: ***TOE Admin***].

7.1.3.5 FMT_MSA.3 Static Attribute Initialization

Hierarchical to:	No other components
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [assignment: ***BPCAS access control policy***] to provide [selection: restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [assignment: ***TOE Admin***] to specify alternative initial values to override the default values when an object or information is created.

7.1.3.6 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [assignment: ***Access Control List Managements, Authentication Failure Limit Management, Username Password Management***]

7.1.4 FDP Requirements (User Data Protection)

7.1.4.1 FDP_ACC.1 Subset Access Control

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the [assignment: ***BPCAS access control policy***] on [assignment: ***Subject:*** • ***Authenticated TOE User*** • ***Authenticated TOE Admin*** ***Object:*** • ***User data*** ***Operations:*** • ***Read*** • ***Write*** • ***Modify***

Application Note 2 BPCAS access control policy is defined in FDP_ACC.1 and FDP_ACF.1 by subject, object, attributes, rules etc.

7.1.4.2 FDP_ACF.1 Security Attribute Based Access Control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	The TSF shall enforce the [assignment: ***BPCAS access control policy***] to objects based on the following: [assignment :

	Subject: • ***Authenticated TOE User*** • ***Authenticated TOE Admin*** ***Object:*** • ***User data*** ○ ***Corporate Information Data*** ○ ***Audit Data*** ***Subject Attributes*** • ***Authentication Status*** ***Object Attributes*** • ***Access Control List*** ***]***
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: • ***Rule-1: Authenticated TOE Admin allowed to read any User Data*** • ***Rule-2: Authenticated TOE Admin allowed to read, write, modify any Corporate Information Data.*** • ***Rule-3: Authenticated TOE User is allowed to read, write, modify Corporate Information Data according to Access Control List***].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: ***none***].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: ***Nobody is allowed to modify Audit Data***].

7.2 SEURITY ASSURANCE REQUIREMENTS

The TOE meets the security assurance requirements for EAL2 package. The following table is the summary for the requirements.

Table 3: Security Assurance Requirements

ASSURANCE CLASS	ASSURANCE COMPONENTS
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
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures

ASSURANCE CLASS	ASSURANCE COMPONENTS
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis

7.3 SECURITY REQUIREMENTS RATIONALE

7.3.1 Security Functional Security Requirements Rationale

Hata! Başvuru kaynağı bulunamadı. provides an overview for security functional requirements coverage and also giving an evidence for sufficiency and necessity of the SFRs chosen.

Table 4: Coverage of Security Objectives by SFRs for TOE

	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_STG.1	FAU_STG.3	FIA_ATD.1	FIA_UID.2	FIA_UAU.2	FIA_AFL.1	FMT_SMR.1	FMT_MTD.1/ADMIN	FMT_MTD.1/USER	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FDP_ACC.1	FDP_ACF.1
O.ACC_CONTROL																X	X
O.AUDITS	X	X	X	X	X												
O.IDAUTH						X	X	X	X								
O.EADMIN										X	X	X	X	X	X		

A detailed justification of required for suitability of the security functional requirements to achieve the security objectives is given in Table 5.

Table 5 Suitability of SFRs

OBJECTIVES	RATIONALE
O.ACC_CONTROL	FDP_ACC.1 helps to meet the objective by identifying the objects and users subjected to the access control policy. FDP_ACF.1 meets this objective by ensuring the rules for the specific functions that can implement an access control policy.
O.AUDITS	FAU_GEN.1 generates the required audit data. FAU_GEN.2 provides the user association with the events must be recorded FAU_SAR.1 provides [TOE Administrators] with the capability to read [all recorded audit information] from the audit records. FAU_STG.1 protects the stored audit records in the audit trail from unauthorized deletion. FAU_STG.3 provides a notification in the event of audit event storage reaches a predefined limit
O.IDAUTH	FIA_UAU.2 requires each user successfully authenticated before any action. FIA_UID.2 requires each user successfully identified before any action. FIA_ATD.1 requires security attributes for identification and authentication. FIA_AFL.1 provides handling of authentication failure after a predefined limit.
O.EADMIN	FMT_SMF.1 provides the management functions; access privilege assignments by user levels, viewing of audit data, unlock passwords for authorized users, change password for own administrator. FMT_MSA.1 shall enforce the [administrator access control SFP] to [unlock] the security attributes [passwords] to [authorized administrators]. FMT_MSA.3 restrict the ability to provide the default values to security attributes to TOE administrators. FMT_SMF.1 provides the management functions; access privilege assignments by user levels, viewing of audit data, unlock passwords for authorized users, change password for own administrator. FMT_SMR.1 maintains the roles and help to associate user with roles FMT_MTD.1 restrict the ability to provide TSF data in a secure way.

7.3.2 Security Functional Requirement Dependencies

Selected security functional requirements include related dependencies. Table 6 below provides a summary of the security functional requirements dependency analysis.

Table 6: Security Functional Requirements Dependencies

SFR	DEPENDENCY	RATIONALE
FAU_GEN.1	FPT_STM.1	FPT_STM.1 Satisfied by OE.TIME in the environment

SFR	DEPENDENCY	RATIONALE
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied
FAU_SAR.1	FAU_GEN.1	Satisfied
FAU_STG.1	FAU_GEN.1,	Satisfied
FAU_STG.3	FAU_STG.1	Satisfied
FIA_ATD.1	None	-
FIA_UID.2	None	-
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2
FIA_AFL.1	FIA_UAU.1	Satisfied by FIA_UAU.2
FMT_MTD.1/ADMIN	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1/USER	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_MSA.1	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Satisfied FDP_ACC.1 Satisfied Satisfied
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	Satisfied by FIA_UID.2
FDP_ACC.1	FDP_ACF.1	Satisfied
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Satisfied Satisfied

7.3.3 Security Assurance Requirements Rationale Dependencies

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3.

EAL 2 is the general level of assurance for these kind of products. Additionally, The TOE is intended to protect confidential information related to a business's user. This information, while sensitive within an organization, the value to an attacker is relatively low. As such, it is considered that the average motivation of attackers will be

low, which implies that the overall attack potential for this TOE will be LOW.

7.3.4 Security Assurance Requirements Dependencies

Since all dependencies are met internally by the EAL2 package only the augmented assurance components dependencies are analyzed.

8 TOE SUMMARY SPECIFICATION

8.1 SF.1: ACCESS CONTROL

The TOE implements access control policies for the data that it wishes to protect. This first phase of control is concerned with the authentication and authorization of users.

The Access Control List is created for each application.

After this phase, the TOE allows access to the resources protected by the system if an access request is defined for the corresponding user and role when an access request is made.

The TOE restricts access if it is not allowed or not defined for the data or the service on the access control list.

The covered security functional requirements are FDP_ACC.1 and FDP_ACF.1.

8.2 SF.2: IDENTIFICATION AND AUTHENTICATION

The TSF requires users to identify and authenticate themselves before invoking any TSF mediated action and TOE Data. No action can be initiated before proper identification and authentication. The TOE checks the credentials presented by the user upon the login page against the authentication information in the database [FIA_UID.2, FIA_UAU.2].

User security attributes are associated with the user account via User Account management [FIA ATD.1].

The TOE detects the authentication attempts that have failed (administrator configurable positive integer within [3 - 99]) times and takes necessary precautions, disabling the account for a system administrator configurable time. FIA_AFL.1 is fulfilled by this way.

8.3 SF.3: AUDITING MECHANISM

The TOE generates some records showing the actions performed by users. These records include the minimum required logs for the SFRs contained in the ST document.

For each log generated, the following information is also included.

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,

TOE provides association of each auditable event with the identity of the user that caused the event.

These functionality FAU_GEN.1 and FAU_GEN.2 are fulfilled by this way.

The timestamp is used to accurately identify and record the date of the generated logs. For this, the system needs a time server that is guaranteed to be correct. This time server is provided by the operating system of the database server.

Review access to generated audit logs is only performed by certain roles. [FAU.SAR.1]

The TSF does not allow deletion and modification of product log records [FAU_STG.1].

When the log memory reaches a predefinition limit, configured users is automatically informed [FAU_STG.3]

8.4 SF.4: MANAGEMENT OF TOE FUNCTIONALITY

The TOE provides its services for management via the user interfaces. System administrator has capability to perform management function. TOE also has capability to maintain different roles. The covered security functional requirements are FMT_SMF.1, FMT_SMR.1.

The TOE provides mechanisms to change the Authentication data to System Administrator and Other Users. FMT_MTD.1/Admin, FMT_MTD.1/User are fulfilled by this way.

TOE provides restricted initial values for subject attribute (Authorization status and object attribute (Access Control List) to supply necessary access control precautions for new users [FMT_MSA.3].

For Access control list attribute, changing the initial value ability is restricted only for administrator. [FMT_MSA.1]

Table 7 Security Functions Coverage

	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_STG.1	FAU_STG.3	FIA_ATD.1	FIA_UID.2	FIA_UAU.2	FIA_AFL.1	FMT_SMR.1	FMT_MTD.1/ADMIN	FMT_MTD.1/USER	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FDP_ACC.1	FDP_ACF.1
SF.1: ACCESS CONTROL																X	X
SF.2: IDENTIFICATION AND AUTHENTICATION						X	X	X	X								
SF.3: AUDITING MECHANISM	X	X	X	X	X												
SF.4: MANAGEMENT OF TOE FUNCTIONALITY										X	X	X	X	X	X		