

SAMPAŞ A.Ş.

ÇAYBİS SECURITY TARGET

Version 1.9

Emsal Uralcan

2014

1	DOCUMENT INFORMATION	3
	<i>Version History.....</i>	<i>3</i>
1.1	<i>Document Terminology</i>	<i>4</i>
1.2	<i>References</i>	<i>5</i>
1.3	<i>Document Organization.....</i>	<i>5</i>
2	STINTRODUCTION(ASE_INT.1)	5
2.1	<i>ST and TOE Identification.....</i>	<i>5</i>
2.2	<i>TOE Overview.....</i>	<i>6</i>
2.2.1	<i>TOE Type</i>	<i>6</i>
2.2.2	<i>Firmware/Hardware/Software Required by the TOE.....</i>	<i>6</i>
2.3	<i>TOE Description</i>	<i>7</i>
2.3.1	<i>Physical Scope of the TOE</i>	<i>7</i>
2.3.2	<i>Logical Scope of the TOE</i>	<i>9</i>
3	CONFORMANCE CLAIMS(ASE_CCL.1)	10
3.1	<i>CC Conformance Claim</i>	<i>10</i>
4	SECURITY PROBLEM DEFINITION (ASE.SPD.1)	10
4.1	<i>Threats to Security.....</i>	<i>10</i>
4.2	<i>Organizational Security Policies.....</i>	<i>11</i>
4.3	<i>Security Assumptions.....</i>	<i>11</i>
5	SECURITY OBJECTIVES(ASE_OBJ).....	12
5.1	<i>Security Objectives for the Operational Environment (ASE_OBJ.1)</i>	<i>12</i>
5.2	<i>TOE Security Objectives (ASE_OBJ.2).....</i>	<i>13</i>
5.3	<i>Security Objectives Rationale</i>	<i>14</i>
5.3.1	<i>Security Objectives Rationale Relating to Threats</i>	<i>14</i>
5.3.2	<i>Security Objectives Rationale Relating to Policies</i>	<i>15</i>
5.3.3	<i>Security Objectives Rationale Relating to Assumptions.....</i>	<i>15</i>
6	EXTENDED COMPONENTS(ASE_ECD.1)	17
6.1	<i>Extended Components Definition</i>	<i>17</i>
7	SECURITY REQUIREMENTS (ASE_REQ.2).....	17
7.1	<i>SFR Formatting</i>	<i>17</i>
7.2	<i>Security Functional Requirements (SFRs).....</i>	<i>18</i>
7.2.1	<i>Security Audit</i>	<i>18</i>
7.2.2	<i>Cryptographic support</i>	<i>20</i>
7.2.3	<i>User Data Protection</i>	<i>20</i>
7.2.4	<i>Identification and Authentication</i>	<i>21</i>
7.2.5	<i>Security Management</i>	<i>22</i>
7.2.6	<i>TOE Access</i>	<i>24</i>

7.2.7	Protectionthe TSF	24
7.3	<i>TOE Security AssuranceRequirement</i>	25
7.4	<i>Security Requirements Rationale</i>	25
7.4.1	Security Functional Requirements	25
7.4.2	SFR Dependency Rationale.....	26
7.4.3	SFR - Objective Rationale	27
7.4.4	Rationale for Security Assurance Requirements (SARs).....	29
8	TOE SUMMARY SPECIFICATION (ASE_TSS.1)	29
8.1	<i>TOE Security Functions</i>	29
8.1.1	Security Audit	29
8.1.2	User Data Protection	29
8.1.3	Identification and Authorization	30
8.1.4	Security Management	30
8.1.5	TOE Access	30

Security Target ÇAYBİSV1.0

1 DOCUMENT INFORMATION

Version History

Version No	Date	Version Description
1.2	07.01.2014	Added version history, updated version
1.2	07.01.2014	Revised Part 4.1 Threats to security part; added enterprise data to T.DISCLOSURE addition to passwords.
1.2	07.01.2014	Revised Part 5.3.1 Security Objectives Rationale Relating to Threats; added O.LOCKOUT to T.UNAUTH.
1.2	07.01.2014	Revised Part 5.3.1 Security Objectives Rationale Relating to Threats; added descriptions of O.ADMIN, O.AUTH, OE.CREDEN,O.AUDIT,OE.CHANNEL, OE_TRUSTEDCERT, OE.TRANS_PROTECT
1.2	07.01.2014	Revised Part 7.1.1.1 Audit Data Generation (FAU_GEN.1); updated and added dependencies.
1.2	07.01.2014	Added Part 7.3 Security Requirements Rationale
1.3	13.01.2014	Kapakta geçen "Common Criteria :EAL2" kısmı silindi.
1.3	13.01.2014	Revised Part 5.2 TOE Security Objectives (ASE_OBJ.2); "O.AUDIT" description at Table 10: Security Objectives for the TOE.
1.3	13.01.2014	Revised Part 5.3.1 Security Objectives Rationale Relating to Threats; "Rationale of T. DISCLOSURE" at Table 11: Mapping of Threats and Objectives.
1.3	13.01.2014	Added Part 7.2.6 FPT_STM.1 ; "dependency explanation".
1.3	13.01.2014	Added Part 7.1 SFR Formatting; "assignment, selection, iteration ve refinement" explanations.
1.3	13.01.2014	Revised Part 7.2.1.1 Audit Data Generation (FAU_GEN.1); "auditable events of FAU_GEN.1.1" .
1.3	13.01.2014	Deleted Part 7.2.4.3 "Management of TSF Data (FMT_MTD.1)" ; because of the same content with FAU_SAR.1.

1.3	13.01.2014	Added Part 7.4.1 Security Functional Requirements; “Table 15 – Mapping TOE Security Functional Requirements and Objectives” .
1.3	13.01.2014	Added Part 7.4.2 SFR Dependency Rationale; “Table 16 – Mapping of SFR to Dependencies”
1.3	13.01.2014	Added Part 7.4.4 Rationale for Security Assurance Requirements (SARs) .
1.4	14.01.2014	Revisions based on observation report 3
1.5	28.01.2014	Revisions based on observation report 4.
1.6	31.01.2013	Revisions based on observation report 4.
1.7	03.02.14	Revisions based on observation report 6.
1.8	24.03.2014	Revisions on account creation and password reset that are not operations of the TOE, TOE only can make unlock account and admin/users can change their own passwords.
1.9	19.06.2014	Revisions based on observation report 10.

1.1 Document Terminology

Acronym	Meaning
CC	Common Criteria
EAL	Evaluation Assurance Level
GB	Giga bytes
LAN	Local Area Network
PP	Protection Profile
RAM	Random Access Memory
SAR	Security Assurance Requirements
SFP	Security Function Policies
SFR	Security Functional Requirements
SQL	Structured Query Language
SSL	Secure Socket Layer or also known as Transport Layer Security (TLS)
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
TSS	TOE Summary Specification
User	Staff who uses the TOE

Table 1: Acronyms

1.2 References

- Common Criteria Part 1 Version 3.1 Revision 4
- Common Criteria Part 2 Version 3.1 Revision 4
- Common Criteria Part 3 Version 3.1 Revision 4
- Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 4

1.3 Document Organization

This ST contains:

- **TOE Security Target Introduction** :Provides an overview of the TOE security functions and describes the physical and logical scope for the TOE.
- **TOE Security Problem Definition**: Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- **Security Objectives**: Identifies the security objectives that are to be satisfied by the TOE and the TOE environment.
- **TOE Security Functional Requirements**: Presents the Security Functional Requirements (SFRs) met by the TOE.
- **TOE Security Assurance Requirement**: Presents the Security Assurance Requirements (SARs) met by the TOE.
- **TOE Summary Specification**: Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- **TOE Rationale**: Describes the rationale for threats and assumptions and mapping to the security objectives.

2 STINTRODUCTION(ASE_INT.1)

2.1 ST and TOE Identification

ST Title	Security Target ÇAYBİS Version 1.0
ST Version	Version 1.9
ST Publication Date	19.06.2014
ST Author	Sampaş Bilişim
TOE Title	ÇAYBİS
TOE Version	V1.0
Assurance Level	EAL 2
CC Identification	<ul style="list-style-type: none">▪ Common Criteria Part 1 Version 3.1 Revision 4▪ Common Criteria Part 2 Version 3.1 Revision 4


- 
- Common Criteria Part 3 Version 3.1 Revision 4
 - Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 4

Table 2: TOE Reference

2.2 TOE Overview

Çaybis is an online application system that enables ÇAYKUR to buy and sell fresh tea. This application is about how tea is processing from seedling time to processed tea. Farmers brings fresh teas to gathering places that CAYKUR checks teas and buys. Then these teas are transporting processing units.

Office Centre and 60 units, that is running agriculture and personnel program in client server mode locally, in the light of technological opportunities in a centralized manner, it is inevitable transition to a web-based software. Personnel monitoring and the center of agricultural activity and Headquarters units based on this data in real-time monitoring and management decisions, should be taken immediately.

Being the central structure of software and web-based program development, maintenance, support and management processes will be carried out from a single center.

According the descriptions indicated above, major security features of the TOE are listed below;

- Security Audit
 - The TSF generates audit logs that consist of various auditable events
- User Data Protection
 - Access privilege assignments protects user data from unauthorized access
- Identification and Authentication
 - Authorized users can access their relevant resources or functions once they have been successfully identified and authenticated using their usernames and passwords.
- Security Management
 - Assign/modify access privileges
 - unlocking password for users
- TOE Access
 - The TOE is able to deny session establishment once the session has expired.

2.2.1 TOE Type

ÇAYBİS 1.0 is a web based application. The TOE is managed by authorized administrators through the web-based main page.

2.2.2 Firmware/Hardware/Software Required by the TOE

Manage the full cycle of hardware and software product development including requirements gathering, design, development, implementation and maintenance.

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.

Minimum Software Requirements	Details
Operating System	Windows Server 2008 R2 Enterprise
Web Server	IIS version 6.1
Browser	Google Chrome version 15.0
Database	Oracle 11G R2 x64/x86 Edition
Web installer package	Microsoft .Net Framework 4.0

Table 3: Software Requirements

Minimum Hardware Requirements	Details
Server	16 virtual CPU(8x2) or higher processor,16 GB or more RAM,running Win 2008 R2
Client	1.6 GHz or higher processor,2 GB or more RAM ,running Windows 7

Table 4: Hardware Requirements

Firmware :Specific to the Hardware.

2.3 TOE Description

2.3.1 Physical Scope of the TOE

The TOE is the web application (web portal – indicated with red colour in Figure 1) hosted on a web server.

Web portal , database server and user repository (LDAP) are the components of the CAYBIS architecture. Process of authentication walks through on LDAP that will lock the user rights when user entered password incorrectly three times. Database server includes procedures.

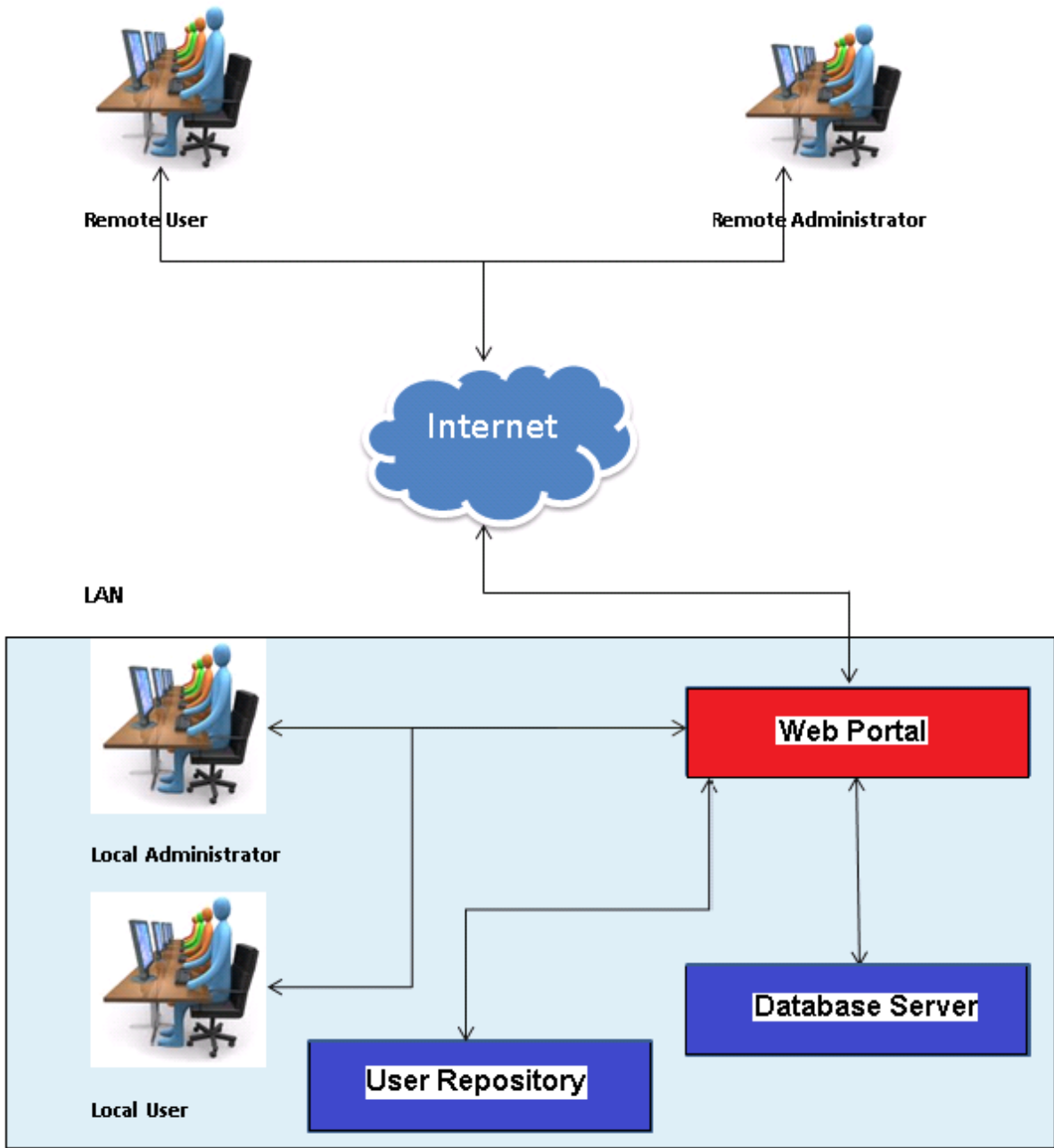



Figure 1 Çaybis v1.0 physical scope

2.3.2 Logical Scope of the TOE

We can explain the logical scope under five main Security Functions headings ;

Security Function	TOE Scope Description
Security Audit	<p>The most logical necessity is to see which user and which progress is in use.</p> <p>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.</p> <p>Authorized administrators have the capability to read and view all the recorded logs stated above through the web portal.</p>
User Data Protection	<p>Authorized administrators of the TOE can perform the following functions to the user or administrator accounts:</p> <ol style="list-style-type: none"> 1. Access privilege assignments by user levels 2. Unlock passwords for authorized users 3. Change password for own administrator
Identification and Authentication	<p>The unambiguous identification and authorised users and the correct association of security attributes with users and subjects is critical to the enforcement of the intended security policies. The families in this class deal with determining their authority to interact with the TOE, and with the correct association of security attributed for each authorised user.</p> <p>Identification and Authentication is required to ensure that users are associated with the proper security attributes (e.g. identity, group, roles, security or integrity levels).</p> <p>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 organisation.</p> <p>Authorized users can access their relevant resources or functions once they have been successfully identified and authenticated using their usernames and passwords.</p> 

Security Management	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.
TOE Access	Duration of the session can be determined by the manager (in minutes). After inactivity of the specified period, the authorized users are then returned to the main page of the ÇAYBIS web portal. The TOE is able to deny session establishment once the session has expired. Re-authentication is required once the session ended.

Table 5: Logical Scope

3 CONFORMANCE CLAIMS(ASE_CCL.1)

3.1 CC Conformance Claim

The following conformance claims are made for the TOE and ST:

Item	Conformance Claim
Applicable Criteria	Common Criteria(CC) version 3.1 Revision 4 Part 2 Conformant Common Criteria(CC) version 3.1 Revision 4 Part 3 Conformant
Protection Profiles	This ST does not claim conformance to any Protection Profiles
Security Assurance Package	EAL 2 security assurance package defined in Common Criteria (CC) version 3.1 Revision 4 Part 3. This ST is EAL2 conformant.

Table 6: Conformance Claims

4 SECURITY PROBLEM DEFINITION (ASE.SPD.1)

This section describes the security aspects of the environment in which the TOE will be used. It provides the statement of the TOE security environment that identifies:

- Known threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical and personnel aspects.

4.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE users are assumed not to be willfully hostile to the TOE).

The TOE address the following threats are applicable listed in Table 7 below.

Threat Name	Description
T.UNAUTH	Users or attackers could gain unauthorized access to the TOE data by bypassing the identification and authentication requirements.
T.DISCLOSURE	Users could gain the valuable information (passwords and enterprise data) of authorized users and administrators by sniffing the traffic
T.INJECT	Users could inject a malicious code inserted into strings (through a SQL query) by inputting data from the forms available in the Web Portal.
T.DATA_ACCESS	An unauthorized person views restricted hosted content compromising the confidentiality and integrity of enterprise data.
T.WEB_ATTACK	An attacker may compromise the integrity, availability and confidentiality of enterprise information by performing web application attacks.
T.RECONFIG	An attacker attempts to reconfigure the TOE to gain access to protected enterprise data compromising integrity and confidentiality.

Table 7: Threats addressed by the TOE

4.2 Organizational Security Policies

The TOE meets no organizational security policies.

4.3 Security Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

The following assumptions, listed in Table 8 below, relate to the operation of the TOE.

Assumption	Description
A.APP	It is assumed that the TOE and third party applications that the TOE relies upon have been configured in accordance with the installation guides. They are securely configured in such a way that the applications provide protection for the TOE from any unauthorized users or processes.
A.PROTECT	It is assumed that all hardware within the environment, including network and peripheral devices, has been approved for the transmitting of secured 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.ADMIN	It is assumed that there are one or more competent individuals that are assigned to manage the TOE and its secured data. Such personnel are assumed not to be careless, willfully negligent or hostile.
A.NO_EVIL	TOE administrators and TOE users are assumed to be non-hostile and trusted to perform all their duties in a competent manner.
A.PHYS_SEC	ÇAYBİS, Active Directory (LDAP) and Database will be hosted inside of a physically secure area.
A.TRANS_PROTECT	The IT environment will provide a secure channel so that all potentially valuable information (including credentials and enterprise data) is protected between the user and application server.
A.CAYBIS_DATA	The ÇAYBİS database is located within the enterprise network boundary and is configured so that only TOE administrators can directly access the interface of the database.
A.FIREWALL	The IT environment will implement gateway filtering, only allowing HTTPS traffic to pass through to ÇAYBİS.

Table 8: Security Assumptions

5 SECURITY OBJECTIVES(ASE_OBJ)

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 4). This section identifies the security objectives for the TOE and its supporting environment.

5.1 Security Objectives for the Operational Environment (ASE_OBJ.1)

The specific security objectives for the TOE environment are those specified in Table 9 below.

Security Objective	Description
OE.NOEVIL	Administrators and Users are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance. The Administrators and users must ensure the physical security of the computers that they use to connect to the TOE to prevent cookie stealing.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE and third party software are delivered, installed, managed, and operated in a manner which maintains the organizational IT security objectives.
OE.RELIABLE	All hardware and third party software supporting the TOE are reliable and operating in good condition. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns. All supporting components' performance is monitored and maintained by administrators.
OE.PHYSICAL	The operational environment of the TOE restricts the physical access to the TOE and non-TOE (hardware and software) to administrative personnel and maintenance personnel accompanied by administrative personnel.

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.NETSEC	The operational environment of the TOE must include a firewall that is configured securely to permit or deny traffic based upon a set of rules. The administrative personnel must configure the firewall rules to block unauthorized access while permitting authorized communications.
OE.CHANNEL	The operational environment of the TOE must protect the transmitted passwords to the Web Portal via usage of HTTPS using a server based SSL.
OE.CAYBIS_DATA	The enterprise administrator shall ensure that the CAYBIS database is located within the enterprises boundary and is configured so that only TOE administrators can directly access the interface of the database.
OE.TRUSTEDCERT	The users (or administrators) of the TOE will 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) are not to trust the server certificate.
OE.TRANS_PROTECT	The IT environment shall provide the server-side of a secure channel so that all potentially valuable information (including credentials and enterprise data) is protected between the user and application server.
OE.FIREWALL	The enterprise administrator shall ensure that gateway filtering is implemented; only allowing HTTPS traffic to pass through to application.

Table 9: Security Objectives for the Operational Environment

5.2 TOE Security Objectives (ASE_OBJ.2)

The security objectives for the TOE are described in below in Table 10.

Security Objective	Description
O.ADMIN	The TOE must provide a method for administrative control of the TOE
O.AUTH	The TOE must 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 must record the login actions taken by users, prevent

	<p>unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.</p> <p>The TOE shall generate audit record of the following auditable events.</p> <ol style="list-style-type: none"> a. Start-up and shutdown of the audit functions; b. User login/ logout and login failures.
O.VALIDATE	The TOE must validate input from users and administrators based on type, length, format and range
O.ACC_CONTROL	The TOE shall ensure that only authenticated and authorized users can access the TOE functionality and protected application resources.
O.DISCLOSURE	The TOE shall ensure that nobody could gain the valuable information by sniffing the traffic.
O.SECURE_CONFIG	The TOE shall ensure that only administrator role can perform the configuration changes in the TOE and enrolment of new users.

Table 10: Security Objectives for the TOE

5.3 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the ST. Sections 5.3.1, 5.3.2, and 5.3.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

5.3.1 Security Objectives Rationale Relating to Threats

Threats	Objectives	Rationale
T.UNAUTH	O.ADMIN	The TOE must provide a method for administrative control of the TOE.
	O.AUTH	The TOE must provide measures to uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE.
	OE.CREDEN	This objective for the environment ensures that the assumption is upheld that all user credentials are protected appropriately by users and they are not negligent.
	O.AUDIT	The TOE shall generate audit reports to trace user and administrator access events.
T. DISCLOSURE	OE.CHANNEL	The operational environment of the TOE must protect the transmitted passwords to the Web Portal via usage of HTTPS using a server based SSL.

	OE.TRUSTEDCERT	The users (or administrators) of the TOE will 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) are not to trust the server certificate.
	OE.TRANS_PROTECT	This objective for the environment ensures that the assumption is upheld that the environment will provide a method for secure transmission of information (and credential) from the user to ÇAYBİS
	O.DISCLOSURE	This objective for the TOE ensures that nobody could gain the valuable information by sniffing.
T.INJECT	O.VALIDATE	mitigates this threat by enforcing the TSF to perform input validation on all fields available for users.
T.DATA_ACCESS	O.ACC_CONTROL	The TOE shall ensure that only authenticated and authorized users can access the TOE functionality and protected application resources.
	O.AUDIT	The TOE shall generate audit reports to trace user and administrator access events.
	OE.CAYBIS_DATA	This objective for the environment ensures that the assumption is upheld that access to the ÇAYBİS database is restricted to TOE administrators.
	OE.NETSEC	This objective for the environment ensures that the assumption is upheld that there exists a firewall that has been configured to block unauthorized access while permitting authorized communications.
T.WEB_ATTACK	O.ACC_CONTROL	The TOE shall ensure that only authenticated and authorized users can access the TOE functionality and protected application resources.
T.RECONFIG	O.SECURE_CONFIG	Only the administrator role can performs configuration changes in the TOE and enrolment of new users.

Table 11: Mapping of Threats and Objectives

5.3.2 Security Objectives Rationale Relating to Policies

There are no policies defined for this Security Target.

5.3.3 Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	Rationale
A.APP	OE.RELIABLE	This objective for the environment ensures that the assumption is upheld that all hardware and software used are reliable and they are in good condition. Their performances are also monitored and maintained by the organization.
	OE.INSTALL	This objective for the environment ensures that the assumption is upheld that the installation and configuration of

		the TOE and third party software are performed in a manner that maintain security objective of the organization. The TOE and third party software installation and configuration are performed by the developer of the application system.
A.PROTECT	OE.PHYSICAL	This objective for the environment ensures that the assumption is upheld that physical security is provided where the access to the servers are controlled.
	OE.INSTALL	This objective for the environment ensures that the assumption is upheld that the installation and configuration of the TOE and third party software are performed in a manner that maintain security objective of the organization. The TOE and third party software installation and configuration are performed by the developer of the application system.
	OE.NOEVIL	This objective for the environment ensures that the assumption is upheld that administrators and users are non-hostile and appropriate trained. It also satisfies this assumption by ensuring the physical security of the computers used to connect to the TOE to prevent cookie stealing.
	OE.NETSEC	This objective for the environment ensures that the assumption is upheld that there exists a firewall that has been configured to block unauthorized access while permitting authorized communications.
A.ADMIN	OE.NOEVIL	This objective for the environment ensures that the assumption is upheld that administrators and users are non-hostile and appropriate trained. It also satisfies this assumption by ensuring the physical security of the computers used to connect to the TOE to prevent cookie stealing.
	OE.CREDEN	This objective for the environment ensures that the assumption is upheld that all user credentials are protected appropriately by users and they are not negligent.
A.NO_EVIL	OE.NOEVIL	This objective for the environment ensures that the assumption is upheld

		that administrators and users are non-hostile and appropriate trained.
A.PHYS_SEC	OE.PHYSICAL	This objective for the environment ensures that the assumption is upheld that physical security is provided where the access to the servers are controlled.
A.TRANS_PROTECT	OE.TRANS_PROTECT	This objective for the environment ensures that the assumption is upheld that the environment will provide a method for secure transmission of information (and credential) from the user to ÇAYBİS
A.CAYBIS_DATA	OE.CAYBIS_DATA	This objective for the environment ensures that the assumption is upheld that access to the ÇAYBİS database is restricted to TOE administrators.
A.FIREWALL	OE.FIREWALL	The objective for the environment ensures that the assumption is upheld that gateway filtering is implemented;only allowing HTTPS traffic to pass through to application.

Table 12: Mapping of Assumptions and Objectives

6 EXTENDED COMPONENTS(ASE_ECD.1)

6.1 Extended Components Definition

There is no extended components.

7 SECURITY REQUIREMENTS (ASE_REQ.2)

7.1 SFR Formatting

The following conventions are set of operations that may be applied to functional requirements; assignment, selection, refinement and iteration.

Assignment:The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows **[assignment]**.

Selection: The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows ***[selection]***

Refinement: The refinement operation is used to add or remove detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by bold text for **additions** and strike through for ~~deletions~~.

Iteration: The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FAU_GEN.1.1a and FAU_GEN.1.1b.

7.2 Security Functional Requirements (SFRs)

This section specifies the security functional requirements for the TOE. It organizes the SFRs by the CC classes.

Requirement Class	Requirement Component
FAU:Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_SAA.3: Simple Attack Heuristics
	FAU_SAR.1: Audit Review
	FAU_STG.1: Protected Audit Trail Storage
FDP:User Data Protection	FDP_ACC.1: Subset Access Control
	FDP_ACF.1: Security Attribute Based Access Control
FCS: CryptographicSupport	FCS_COP.1: CryptographicOperation
FIA:IdentificationandAuthentication	FIA_USB.1: User-subjectbinding
	FIA_ATD.1: User Attribute Definition
	FIA_UAU.2: User authenticationbeforeanyaction
	FIA_UID.2: User identificationbeforeanyaction
FMT:Security Management	FMT_MSA.1: Management of Security Attributes
	FMT_MSA.3: Static Attribute Initialisation
	FMT_MTD.1: Management of TSF data
	FMT_SAE.1: Time-Limited Authorization
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FTA:TOE Access	FTA_LSA.1: Limitation on scope
	FTA_SSL.3: TSF-initiated Termination
FPT: Protection of the TSF	FPT_STM.1: Reliable time stamps

Table 13:TOE Security Functional Requirements

7.2.1 Security Audit

7.2.1.1 Audit Data Generation (FAU_GEN.)

Hierarchical to:	No other components.
FAU_GEN.1.1	

	The TSF shall be able to generate an audit record of the following auditable events: <ul style="list-style-type: none"> a. Start-up and shutdown of the audit functions; b. All auditable events for the [not specified] level of audit; and c. [User login/ user logout and failed login attempts].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: <ul style="list-style-type: none"> a. Date and time of the event, type of event, subject identity, 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, [none].
Dependencies:	FPT_STM.1 Reliable time stamps
Notes:	None.

7.2.1.2 Simple Attack Heuristics (FAU_SAA.3)

Hierarchical to:	No other components.
FAU_SAA.3.1	The TSF shall be able to maintain an internal representation of the following signature events [SQL injections] that may indicate a violation of the enforcement of the SFRs.
FAU_SAA.3.2	The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [inputs by validating data in the specified fields in the Web Portal] .
FAU_SAA.3.3	The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when a system event is found to match a signature event that indicates a potential violation of the enforcement of the SFRs.
Dependencies:	No dependencies.
Notes:	None

7.2.1.3 Audit Review (FAU_SAR.1)

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [TOE Administrators] with the capability to read [all recorded 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.
Dependencies:	FAU_GEN.1 Audit Data Generation
Notes:	None.

7.2.1.4 Protected Audit Trail Storage (FAU_STG.1)

Hierarchical to:	No other components.
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 [prevent] unauthorized modifications to the stored audit records in the audit trail.
Dependencies:	FAU_GEN.1 Audit Data Generation
Notes:	None.

7.2.2 Cryptographic support

7.2.2.1 Cryptographic operation (FCS_COP.1)

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [data encryption and/or decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [256 bit] that meet the following: [FIPS 197].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

7.2.3 User Data Protection

7.2.3.1 Subset Access Control (FDP_ACC.1)

Hierarchical to:	No other components.
FDP_ACC.1.1a	The TSF shall enforce the [administrator access control SFP] on[administrators performing the following operations (or management functions) to the user and administrator accounts: a. access privilege assignments by user levels b. unlock passwords for authorized users c. change password for own administrator account d. view all audit data].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	None.

Hierarchical to:	No other components.
FDP_ACC.1.1b	The TSF shall enforce the [user access control SFP] on [user performing the following operations (or management functions) to the user accounts: a. servicing of HTML pages b. change password for own account].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	None.

7.2.3.2 Security Attribute Based Access Control (FDP_ACF.1)

Hierarchical to:	No other components.
------------------	----------------------

FDP_ACF.1.1a	The TSF shall enforce the [administrator access control SFP] to objects based on the following: [Usernames and user groups] .
FDP_ACF.1.2a	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [users are explicitly granted access to a function or resource if he/she belongs to a user group which has been granted access] .
FDP_ACF.1.3a	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none] .
FDP_ACF.1.4a	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none] .
Dependencies:	FDP_ACC.1 Subset Access Control FMT_MSA.3 Static Attribute Initialization
Notes:	None.

Hierarchical to:	No other components.
FDP_ACF.1.1b	The TSF shall enforce the [user access control SFP] to objects based on the following: [User names, user groups and Access control list] .
FDP_ACF.1.2b	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [users are explicitly granted access to a function or resource if he/she belongs to a user group which has been granted access] .
FDP_ACF.1.3b	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none] .
FDP_ACF.1.4b	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none] .
Dependencies:	FDP_ACC.1 Subset Access Control FMT_MSA.3 Static Attribute Initialization
Notes:	None.

7.2.4 Identification and Authentication

7.2.4.1 User-subject binding (FIA_USB.1)

Hierarchical to:	No other components.
------------------	----------------------

FIA_USB.1.1:	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [user name and user group or role] .
FIA_USB.1.2:	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [Security attributes are assigned from TSF data for each defined user after login operation] .
FIA_USB.1.3:	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [a user access roles assigned to them by an authorized administrator] .
Dependencies:	FIA_ATD.1 User attribute definition
Notes:	None.

7.2.4.2 User Attributes Definition (FIA_ATD.1)

Hierarchical to:	No other components.
FIA_ATD.1.1:	The TSF shall maintain the following list of security attributes belonging to individual users: [<ul style="list-style-type: none"> a. Username b. User group or role].
Dependencies:	No dependencies.
Notes:	None.

7.2.4.3 User authentication before any action (FIA_UAU.2)

Hierarchical to:	FIA_UAU.1 Timing of authentication
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.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

7.2.4.4 User identification before any action (FIA_UID.2)

Hierarchical to:	FIA_UID.1 Timing of identification
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.
Dependencies:	No dependencies
Notes:	None.

7.2.5 Security Management

7.2.5.1 Management of security attributes (FMT_MSA.1)

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [administrator access control SFP] to [modify] the security attributes [access control list, user group and roles, default access rights, mapping of users to roles] to [authorized administrators] .
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
Notes:	None.

7.2.5.2 Static Attribute Initialisation (FMT_MSA.3)

Hierarchical to:	No other components.
FMT_MSA.3.1:	The TSF shall enforce the [administrator access control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2:	The TSF shall allow the [authorized administrators] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

7.2.5.3 Management of TSF data (FMT_MTD.1)

Hierarchical to:	No other components.
FMT_MTD1.1.a	The TSF shall restrict the ability to [unlock] the [user passwords] to [authorised administrators].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

Hierarchical to:	No other components.
FMT_MTD1.1.b	The TSF shall restrict the ability to [modify] the [user password/ administrator password] to [user/authorised administrators].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

7.2.5.4 Time-limited Authorisation (FMT_SAE.1)

Hierarchical to:	No other components.
FMT_SAE.1.1:	The TSF shall restrict the capability to specify an expiration time for [authorized user authentication data in the web portal] to [authorized administrators].
FMT_SAE.1.2:	For each of these security attributes, the TSF shall be able to [log out the associated authorized user account for the web portal] after the expiration time for the indicated security attribute has passed.
Dependencies:	FMT_SMR.1 Security roles

	FPT_STM.1 Reliable time stamps
Notes:	None.

7.2.5.5 Specification of Management Functions (FMT_SMF.1)

Hierarchical to:	No other components.
FMT_SMF.1.1:	The TSF shall be capable of performing the following management functions: [<ul style="list-style-type: none"> a. access privilege assignments by user levels b. viewing of audit data c. unlock passwords for authorized users]
Dependencies:	No dependencies.
Notes:	None.

7.2.5.6 Security Roles (FMT_SMR.1)

Hierarchical to:	No other components.
FMT_SMR.1.1:	The TSF shall maintain the roles [authorized users and administrators].
FMT_SMR.1.2:	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

7.2.6 TOE Access

7.2.6.1 Limitation on Scope of Selectable Attributes (FTA_LSA.1)

Hierarchical to:	No other components.
FTA_LSA.1.1:	The TSF shall restrict the scope of the session security attributes [session timeout], based on [userinactivity].
Dependencies:	No dependencies.
Notes:	None.

7.2.6.2 TSF-Initiated Termination (FTA_SSL.3)

Hierarchical to:	No other components.
FTA_SSL.3.1:	The TSF shall terminate an interactive session after [a logout or a specified time interval of user inactivity set by an authorized administrator. The default session timeout value is 20 minutes].
Dependencies:	No dependencies.
Notes:	None.

7.2.7 Protectionthe TSF

7.2.7.1 Reliable Time Stamps (FPT_STM.1)

Hierarchical to:	No other components.
FPT_STM.1.1:	The TSF shall be able to provide reliable time stamps.
Dependencies:	No dependencies.

Notes:	None.
--------	-------

7.3 TOE Security Assurance Requirement

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

ASSURANCE CLASS	ASSURANCE COMPONENTS
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
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: 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

Table 14: TOE Security Assurance Requirements

7.4 Security Requirements Rationale

7.4.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

Objective	O.ACC_CONTROL	O.AUDIT	O.SECURE_CONFIG	O.AUTH	O.VALIDATE	O.ADMIN	O.DISCLOSURE
SFR							
FDP_ACC.1a	✓			✓			

FDP_ACC.1b	✓			✓			
FDP_ACF.1a	✓			✓			
FDP_ACF.1b	✓			✓			
FCS_COP.1							✓
FAU_GEN.1		✓					
FAU_SAR.1		✓					
FAU_STG.1		✓					
FMT_SMF.1			✓			✓	
FMT_SMR.1			✓			✓	
FMT_MSA.1			✓			✓	
FMT_MSA.3			✓			✓	
FMT_SAE.1			✓			✓	
FMT_MTD.1a				✓			
FMT_MTD.1b				✓			
FIA_USB.1				✓			
FIA_ATD.1				✓			
FIA_UAU.2				✓			
FIA_UID.2				✓			
FAU_SAA.3						✓	
FTA_SSL.3	✓					✓	
FTA_LSA.1						✓	
FPT_STM.1		✓					

Table 15 – Mapping TOE Security Functional Requirements and Objectives.

7.4.2 SFR Dependency Rationale

The ST satisfies all the security functional requirement dependencies of the Common Criteria. The table below lists each SFR to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included.

SFR Claim	Dependencies	Dependency Met
FDP_ACC.1a	FDP_ACF.1	YES
FDP_ACC.1b	FDP_ACF.1	YES
FDP_ACF.1a	FDP_ACC.1 , FMT_MSA.3	YES
FDP_ACF.1b	FDP_ACC.1 , FMT_MSA.3	YES
FTA_SSL.3	N/A	N/A
FAU_GEN.1	FPT_STM.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FAU_STG.1	FAU_GEN.1	YES
FMT_SMF.1	N/A	N/A
FMT_SMR.1	FIA_UID.1	YES (FIA_UID.2 is hierarchical to FIA_UID.1)
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	YES (FDP_ACC.1, FMT_SMR.1, FMT_SMF.1)
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	YES
FMT_MTD.1a	FMT_SMR.1 FMT_SMF.1	YES

FMT_MTD.1b	FMT_SMR.1 FMT_SMF.1	YES
FMT_SAE.1	FMT_SMR.1, FPT_STM.1	YES
FIA_ATD.1	N/A	N/A
FAU_SAA.3	N/A	N/A
FTA_LSA.1	N/A	N/A
FPT_STM.1	N/A	N/A
FCS_COP.1	[FDP_ITC.1,or FDP_ITC.2,or FCS_CKM.1] FCS_CKM.4	<ul style="list-style-type: none"> FDP_ITC.1, FDP_ITC.2, FCS_CKM.1:Cryptographic key import dependency is not met,because the key is hardcoded in code. FCS_CKM.4:Cryptographic key destruction is not dependency met, because the key is hardcoded in code so key should not be deleted.
FIA_USB	FIA_ATD.1	YES
FIA_UAU.2	FIA_UID.1	YES(FIA_UID.2 is hierarchical to FIA_UID.1)
FIA_UID.2	N/A	N/A

Table 16 – Mapping of SFR to Dependencies

7.4.3 SFR - Objective Rationale

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives..

Objectives	SFR	Rationale
O.ACC_CONTROL:	FDP_ACC.1a FDP_ACF.1a FDP_ACC.1b FDP_ACF.1b FTA_SSL.3	<p>O.ACC_CONTROL is fulfilled in the following manner.</p> <p>FDP_ACC.1a enforce the [administrator access control SFP] on [administrators performing the operations (or management functions) to the user and administrator accounts.</p> <p>FDP_ACF.1a enforces the [administrator access control SFP] to objects based on the following: [Usernames and user groups].</p> <p>FDP_ACC.1b enforce the [user access control SFP] on [users performing the operations (or management functions) to the user accounts.</p> <p>FDP_ACF.1b enforces the [user access control SFP] to objects based on the following: [Usernames, user groups and access control list].</p> <p>FTA_SSL.3 terminates an interactive session after [a logout or a specified time interval of user inactivity set by an authorized administrator. The default session timeout value is 20 minutes].</p>
O.AUDIT	FAU_GEN.1 FAU_SAR.1 FAU_STG.1 FPT_STM.1	<p>O.AUDIT is fulfilled in the following manner.</p> <p>FAU_GEN.1 generates the required audit data.</p> <p>FAU_SAR.1 provides [TOE Administrators] with the capability to read [all recorded audit information] from the audit records.</p> <p>FAU_STG.1 protects the stored audit records in the audit trail from unauthorized deletion.</p> <p>FPT_STM.1 provides reliable time for the audit event.</p>
O.SECURE_CONFIG	FMT_SMF.1 FMT_SMR.1 FMT_MSA.1	<p>O.SECURE_CONFIG is fulfilled in the following manner</p> <p>FMT_SMF.1 provides the management functions; access privilege assignments</p>

	FMT_MSA.3 FMT_SAE.1	<p>by user levels, viewing of audit data, unlock passwords for authorized users, change password for own administrator.</p> <p>FMT_SMR.1 maintains the roles and help to associate user with roles.</p> <p>FMT_MSA.1 shall enforce the [administrator access control SFP] to [unlock] the security attributes [passwords] to [authorized administrators].</p> <p>FMT_MSA.3 restrict the ability to provide the default values to security attributes to TOE administrators.</p> <p>FMT_SAE.1 restricts the capability to specify an expiration time for [authorized user authentication data in the web portal] to [authorized administrators].</p>
O.AUTH	FDP_ACC.1a FDP_ACF.1a FDP_ACC.1b FDP_ACF.1b FMT_MTD.1a FMT_MTD.1b FIA_USB.1 FIA_ATD.1 FIA_UAU.2 FIA_UID.2	<p>O. AUTH is fulfilled in the following manner</p> <p>FDP_ACC.1a enforce the [administrator access control SFP] on [administrators performing the operations (or management functions) to the user and administrator accounts.</p> <p>FDP_ACF.1a enforces the [administrator access control SFP] to objects based on the following: [Usernames and user groups].</p> <p>FDP_ACC.1b enforce the [user access control SFP] on [users performing the operations (or management functions) to the user accounts.</p> <p>FDP_ACF.1b enforces the [user access control SFP] to objects based on the following: [Usernames, user groups and access control list].</p> <p>FMT_MTD.1a restricts the ability to unlock user passwords to administrator.</p> <p>FMT_MTD.1b restricts the ability to modify user passwords to user. Also restricts the ability to modify administrator passwords to administrator.</p> <p>FIA_USB.1 provides user-subject bindings with user name and user group or role security attributes.</p> <p>FIA_ATD.1 requires that the TSF maintain the usernames and passwords, user group and role.</p> <p>FIA_UAU.2 requires each user successfully authenticated before any action.</p> <p>FIA_UID.2 requires each user successfully identified before any action.</p>
O.VALIDATE	FAU_SAA.3	<p>O. VALIDATE is fulfilled in the following manner</p> <p>FAU_SAA.3 specifies the TSF to enforce input validation on data input in selective fields in the Web Portal.</p>
O.ADMIN	FMT_MSA.1 FMT_MSA.3 FMT_SAE.1 FMT_SMF.1 FMT_SMR.1 FTA_LSA.1 FTA_SSL.3	<p>O. ADMIN is fulfilled in the following manner</p> <p>FMT_MSA.1 shall enforce the [administrator access control SFP] to [unlock] the security attributes [passwords] to [authorized administrators].</p> <p>FMT_MSA.3 restrict the ability to provide the default values to security attributes to TOE administrators.</p> <p>FMT_SAE.1 restricts the capability to specify an expiration time for [authorized user authentication data in the web portal] to [authorized administrators].</p> <p>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.</p>

		<p>FMT_SMR.1 maintains the roles and help to associate user with roles.</p> <p>FTA_LSA.1 requires the TSF to restrict the session timeout based on user inactivity.</p> <p>FTA_SSL.3 terminates an interactive session after [a logout or a specified time interval of user inactivity set by an authorized administrator. The default session timeout value is 20 minutes].</p>
0.DISCLOSURE	FCS_COP.1	<p>O. DISCLOSURE is fulfilled in the following manner</p> <p>FCS_COP.1 provides encryption mechanism that nobody could gain the valuable information.</p>

Table 17 – Rationale for TOE SFRs to Objectives

7.4.4 Rationale for Security Assurance Requirements (SARs)

The chosen assurance level is appropriate with the threats defined for the environment. The threats that were chosen are consistent with attacker of low attack motivation, therefore EAL2 was chosen for this ST.

8 TOE SUMMARY SPECIFICATION (ASE_TSS.1)

This section provides the TOE summary specification. The table below illustrate how the ÇAYBİS features achieve the TOE security functional requirements.

8.1 TOE Security Functions

8.1.1 Security Audit

Users and administrators access the TOE through the CAYBIS web portal.

The TOE generates audit logs that consist of various auditable events or actionstaken by the users and administrators.

The auditable events include user logins, user logouts, failed login attempts.

The audit contents consist of the date and time of events, usernames, and events taken by the authorized users or administrators.

These audit logs can be analyzed by authorized administrators for suspicious activities, when required.

The TOE provides the capability for authorized administrators to read and view all the recorded logs stated above through the web portal.

Note that onlythe administrators can view the audit log.

The TSF prevents the authorized administrators from modifying or deleting audit logs.

Not validating input is one of the reasons for malicious database manipulation or system crashes.

Functional Requirement Satisfied: FAU_GEN.1, FAU_SAA.3, FAU_SAR.1, FAU_STG.1, FPT_STM.1,

8.1.2 User Data Protection

Authorized administrators of the TOE can perform the following functions to the user or administrator accounts:

Access privilege assignments by user levels.

Unlock passwords for authorized users.

Change password for own administrator.

Users (and administrators) can only access resources (or functions) if they belong to the user group that explicitly have been given access to those resources or functions. Only administrators can give perform the user access privileges.

User Data Protection function provides the TSF with the ability to protect user data by ensuring data sent to the Web Portal is validated prior to processing it. All input to the specified fields available in selective interactive forms in the CAYBIS Web Portal is validated before it is processed.

The input is validated based on size of the input, the sequence of the keystroke, and the list of unacceptable characters (knowns as “black” list) to ensure that no malicious code is inserted into the SQL query or at least keep malicious code from being processed.

User data protection function performs data encryption mechanism that nobody could gain in the valuable information.

Functional Requirement Satisfied: FDP_ACC.1a, FDP_ACC.1b, FDP_ACF.1a, FDP_ACF.1b, FCS_COP.1

8.1.3 Identification and Authorization

The Identification and Authentication security function provides the TOE with the ability to govern access by users and administrators. The TOE ensures that a user (or administrator) identity is established and verified before access to the TOE is allowed. The identity (which is the username) is associated to its proper user group.

An administrator can manage the TOE through the web portal interface.

Prior to allowing access, the TOE requires an administrator to be identified using a username and password. Before successful completion of the security function, an administrator is unable to perform any of the management function.

Users of the TOE must be identified and authenticate prior accessing the functions or resources the web portal. Before successful completion of the security function, a user is unable to perform any of the relevant function.

Once identified and authenticated, the users and administrators are able to access the functions or resources available to their respective groups' access levels.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1,

8.1.4 Security Management

The TOE provides mechanisms to govern which users can access with resources or functions. The Security Management function allows the administrators to properly configure this functionality.

Authorized administrators can assign access privileges to users by user levels based on the functions or resources that they are allowed to perform or access. Additional functionality such as modifying access privileges is also accessible by authorized administrators.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1a, FMT_MTD.1b.

8.1.5 TOE Access

The TSF provides a method for controlling the establishment of a user's (or administrator's) session based on a termination of session after a specified period of user inactivity.

Authorized administrators can define the session expiration time (in minutes) for authorized users and administrators. Inactive sessions are logged out after this defined period of inactivity. The users

are automatically logged out and returned to the login page. The default session timeout is 20 minutes.

The TOE is able to deny session establishment once the session has expired. Re-authentication is required once the session ended.

TOE Security Functional Requirements Satisfied: FTA_LSA.1, FTA_SSL.3, FMT_SAE.1