Mergen Yazılım A.Ş

Mergen HBYS Security Module v1.18.1

SECURITY TARGET

Document Name	: Mergen HBYS Security Module v1.18.1 SECURITY TARGET
Document Version	: 1.5
Revision Date	: 27.11.2018
Prepared by	: Yusuf KARTAL / Project Manager Fatih GÖKEN / Software Developer Elif BÜYÜKKAYA / Consultant
Approved by	: Ekrem Küçük / System Manager

Revision History

Revision No	Revision Reason	Date of Revision
1.0	First Release	07.12.2017
1.1	Updated according to the remarks from the evaluation facility	22.02.2018
1.2	Updated according to the remarks from the evaluation facility	05.03.2018
1.3	Updated according to the remarks from the evaluation facility	20.03.2018
1.4	Updated according to Mergen quality document template to add headers	30.03.2018
1.5	Updated according to remarks from the avaluation facility	27.11.2018

ACRONYMS

CC	: Common Criteria
CCMB	: Common Criteria Management Board
DAO	: Data Access Object
EAL	: Evaluation Assurance Level (defined in CC)
IIOP	: Internet Inter-ORB Protocol
ORB	: Object Request Broker
ORM	: Object Relational Mapping
OSP	: Organizational Security Policy
PP	: Protection Profile
SAR	: Security Assurance Requirements
SFR	: Security Functional Requirements
SHA	: Secure Hash Algorithm
SSL	: Secure Sockets Layer
TOE	: Target of Evaluation
TSF	: TOE Security Functionality (defined in CC)
TSE	: Turkish Standards Institute

TABLES

FIGURES

TABLE OF CONTENT

1. ST INTRODUCTION

1.1ST Reference

ST Title	Mergen HBYS Security Module v1.18.1 Security Target
ST Version	1.4
ST Publication Date	30.03.2018
CC version	Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 5)

1.2TOE Reference

TOE Identification	Mergen HBYS Security Module v1.18.1
CC Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 5)
PP Conformance	Protection Profile for Security Module of General-Purpose Health Informatics Software
Assurance Level Evaluation	Assurance Level 2

1.3TOE Overview

As well as in many areas, the health sector in Turkey has its own unresolved issues. Providing regular registries, accurate analyzes and a systematic work environment are the first step in reducing the problems of both hospital staff and hospital patients. Software programs that can solve the problems of hospitals become inevitable with "Information Technology" which directs our future. From this point of view, our main goal is closely monitoring the progress occurring in information technology, health, culture and health institutions according to Turkey's Hospital Information Systems (HIS) is to develop. It was aimed to minimize the problems of the health sector by reducing the work load of the healthcare personnel and the hospital management with the financial and administrative modules within the scope of the software programs that we gave the name of HBYS and with its medical modules. HBYS is a software program that will enable more efficient use of hospital resources, patient satisfaction, reduction of the most loss of service losses and increase profitability and enable the hospital to be financially strong.

Security module, as TOE, is responsible for protecting HBYS data. So TOE ensures that user and patient informations are protected towards unauthorized access. Along with that, any users' security activities are recorded via audit logs and communication path between peer to peer is securely protected by using secure protocols like HTTPS. TOE serves GUI to manage users, user roles and security attributes to system administrator and serves GUI to view user and system activities(logs) to auditor.

1.3.1 Introduction

TOE is a logical security module for web-based general-purpose health information management system. The health information management system refers to an application which hosts and processes all kind of patient data and which can be accessed online.

ST is prepared for Hospital Information Management System, which provides online services. Therefore, in this ST the security functional requirements, that are common in those applications above, have been taken into consideration.

1.3.2 TOE Type

The type of the TOE is a logical security module for web based general purpose health information systems application.

1.3.3 Operational Environment Components

This section provides detailed description of the TOE and discusses the software and hardware components of the TOE (operational environment) and basic security and functional features of the TOE.

1.3.3.1 Operational Environment Components and Supported Non-TOE Software and Hardware Components for TOE

Since the TOE operates on a network, it interacts with the components of that network. There is a web server on which the TOE operates and this web server operates on an operating system, which operates on a hardware server.

This section identifies peripheral software and hardware components, which interact with the TOE. Figure 1 shows how the TOE interacts with the operational environment. During the interactions all the communications between the TOE and its components are performed by SSL communication protocol

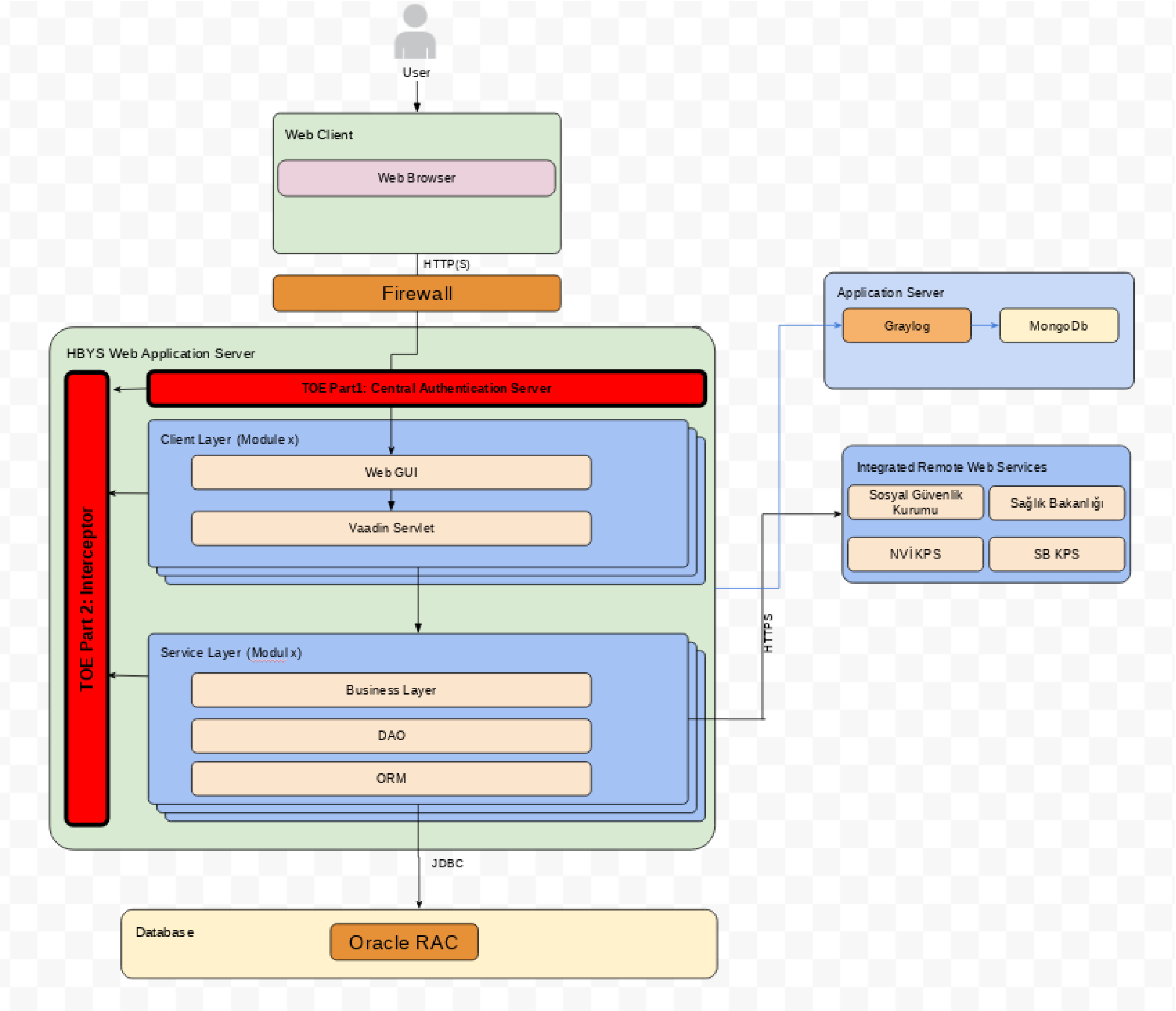

Figure 1The structure of operational environment of the TOE. TOE components are shown by red. All the communication between the TOE and its environmental components done by SSL.

Web server: The TOE operates on a web server as a web application. This web server may use any technology. Like TOE, HBYS modules and components are operates on a web server.

- TOE Part 1: Central Authentication Server, authenticates users to access HBYS modules.
- TOE Part 2: Interceptor, filters requests to verify and validate security requirements and generates logs about operations.
- Client Layer, includes Web GUI and Vaadin Servlets.
  - Web GUI, generates graphical user interface to assure interaction between user and modules.
  - Vaadin Servlets, receive the user requests via HTTPS and forward requests to Service Layer via IIOP in Web Server.
- Service Layer, includes Business Layer, DAO and ORM.
  - Business Layer, handles request and decides operation about that request in a transaction. This layer uses DAO to do operations about database.

- ○ DAO, includes SQL and HQL codes and scripts to access database.
- ○ ORM, is a object to table and table to object mechanism between DAO and database.

Operating system: The server that the TOE runs on has an operating system. The web server that the TOE runs on, operates on this operating system and uses the sources of this system through this operating system.

Hardware server: The TOE operates on a server. This server may have different features varying from product to product.

Network components and the firewall: The TOE interacts with the network components in order to exchange patient and other related information. This interaction is carried out through the operating system and the server. Internet access of the TOE is controlled by a firewall.

Time stamp server: The TOE requires time stamp server, which is provided by operational environment in order to secure logs. This time stamp server provides timestamps based on electronic signatures (which is hardware created). It is assumed that time server runs on a secure server and time information obtained from this server is also assumed to be secure.

Database: TOE saves all of the user and patient records in this database. There is a firewall protecting this database.

TOE's minimum hardware requirements and software versions are given on below table

Web Server	
CPU	2 Core 2.6 Ghz
Memory	16 GB
Operating System	Debian 9.2 / Windows 10
Disk	60 GB
Application Server	Glassfish 4.1 Build 13
Connectivity	TCP/IP
Database Server	
CPU	2 Core 2 Ghz
Memory	32 GB
Disk	300 GB
Operating System	Oracle Linux 6.x, Oracle Linux 7.x
RDBMS	Oracle 11gR2
Connectivity	JDBC

1.3.3.2 Usage and Major Basic Security and Functional Attributes

TOE allows for auditing the checking in and out of the patients, examinations and reviews, and other related reports and materials. Thus, the TOE allows for accessing the patients' medical history immediately. Additionally the TOE allows saving the individual information, contact information of the patient and the surgeries that the patient had before. The TOE additionally provides basic security functions like authentication, access control, secure communication and security management in order to provide security for the patient information. The explanation of these security related attributes of the TOE are as follows:

Authentication and authorization: It is because the TOE users may access through an unsecure environment, effective authentication and authorization processes are required to apply. Authentication is performed through user name and password verification. Hash functions (in general) are applied to passwords to prevent them from reversing to the original. Hashing information saved together with the salt variant. After the authentication is successfully completed, then the TOE will authorize the users and give access rights to them based on their user types and roles. The roles are explained in 1.3.4.

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.

Auditing: TOE automatically audits logs in order to record user activities over the system assets, access control and modifications. Content of the audit logs and the method of auditing should be easily understood and configurable through a user interface. TOE stamps the logs with a time stamp to prevent them from unauthorized modification. Thus, TOE could detect unauthorized modification of the logs.

Administration: TOE provides effective control mechanisms for the users responsible for administration of the system. It is important that these mechanisms should make decision-making process easier and more effective. TOE provides system administrator's authorization and data management functionalities. Only the authorized users can access interfaces provided for administration of the TOE and more strict security measures are applied to those interfaces. Roles defined for the TOE are administrator, end user, system user and the auditor. Administrator is the role that performs functions related to the administration of the TOE. User is the role that uses the TOE within the limits of authorization. Auditor is the role that can use only auditing functions, which are used in audits.

Data protection: TOE keeps records of two kinds of data in general, the patient data and the user data. TOE is responsible for protecting these data. It should be noted that protection should be provided not only for storing of the data but also during the transmission of the data. Data protection is performed by an effective authentication and authorization mechanisms, access control policies, and administrative and auditing operations.

Secure Communication: TOE needs to communicate both with its components and with other components such as databases, Sosyal Güvenlik Bakanlığı, NVI/KPS, SB KPS, Sağlık Bakanlığı. Those communications should be done in a secure way, using the SSL protocol. Secure communication will ensure that sniffing over the network will be prevented and the data transferred between the components are protected against the attackers.

1.3.4 Type of Users

The TOE shall have the following four types of users as a minimum requirement. These roles are organized on a need to know basis and have segregation requirements. These are as follows:

- End User
- System User
- System Administrator
- System Auditor

End User: End user sees the TOE as a black box. He is able to deal with the data for which he is authorized to. Typical functions that the end user is authorized to use are: search, list, view documents and records. End users are not authorized to update patient records or such other critical data.

System User: System user has the same privileges with the normal user. In addition to these, data entry operator can also register/scan/import incoming documents/records into the TOE. He/she has the needed capabilities to effectively and securely use importing tools like scanners.

System_Administrator: System Administrator has explicit authorization on management of the TOE. Administrator can be one person, or there may be specific administrators for the different parts of the TOE, like database administrator, network administrator, application administrator. Administrator can access the application, database, file system and other entities with all privileges.

System Auditor: System auditors have read only access priviliges to audit logs and authentication and authorization configurations provided by the TOE. They are entitled to check any audit logs that the applications produces and authentication and authorization configurations for the TOE. A user may have a single role or multiple roles at the same time, based on the role type.

1.4 TOE Description

1.4.1 Physical Scope

TOE physically consists of the following software component;

✓ Software components

➢ Mergen HBYS Security Module v1.18.1 WEB Application

- Part 1: Web Application (only Authentication mechanism)
- Part 2: Web Application (excluding authentication mechanism)

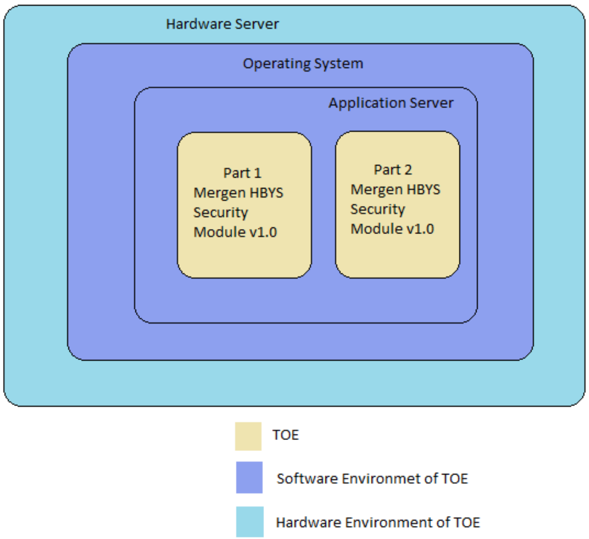
Hardware Server
Operating System
Application Server
Part 1 Mergen HBYS Security Module v1.0
Part 2 Mergen HBYS Security Module v1.0
TOE
Software Environmet of TOE
Hardware Environment of TOE

Figure 2Mergen HBYS Security Module v1.18.1 Application Software

TOE is a web based application which runs on a web server and there is no need any hardware components. TOE uses web server connection pool to connect database.

The TOE is shown in two parts.

Part 1 includes authentication mechanism. All users are identified and authenticated from here. Part 1 serves as a Central Authentication Server to check username and password. If username and password are ok to success login, a session token is generated to used by HBYS modules and so user is able to access modules.

Part 2 does all other operations except authentication and that is a interceptor layer to filter and do operations about requests. Authorization, management, auditing, access control are the main tasks which are handled by that.

TOE is a part of the HBYS product which is served by JAR and WAR packages to the customer companies. Product is uploaded to Mergen Yazılım FTP servers. Customer's IT Professional downloads packages using username, password and ftp adress which is given by Mergen Yazılım, and deploys to their application servers.

1.4.2 Logical Scope of TOE

TOE enforces the users for identification and authentication. If the identification and authentication processes are successful, the authorization mechanism provide access rights. TOE resources are restricted with an effective authorization mechanism. At the same time passwords are stored in the database with salted hash. Access rights are restricted for users to access operations. Only authorized users can access defined resources.

The activities of the users can be monitored by the system auditor. At the same time, audit records are read only record. Audit records can not be deleted or updated by any role. When the audit records are full, the up to date audit records overwrite the oldest audit record.

TOE provides efficient interfaces for managing the system for administrator with special access rights. The system administrator can assign roles to the users. There are four roles defined in the TOE. These roles are end user, system user, system administrator and system auditor.

The TOE provides security for all data stored in the system, which are private data of the users, system options/references and logs. TOE does identification by using username, authentication with password, authorization by users capability and system hierarchy to Access control and auditing of these. At the same time, the TOE provides secure communication for data transfer using network protocols; HTTPS (Secure Hypertext Transfer Protocol) for Presentation layer, IIOP (Internet Inter-ORB Protocol) for Bussiness layer, JDBC (Java Database Connectivity) Protocol for Data Access layer.

2 CONFORMANCE CLAIM

2.1 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, April 2017

has to be taken into account during evaluation.

2.2 PP Claim

This Security Target claims strict conformance to Protection Profile for Security Module of General-Purpose Health Informatics Software v1.0

2.3 Package Claim

This Security Target claims conformance to package EAL2.

2.4 Conformance Claim Rationale

This security target (ST) claims strict conformance with the protection profile (PP) TSE-CCS/PP-011 referenced in 2.2 PP Conformance Claims. The type of TOE defined in this ST is consistent with the TOE type defined in the PP which is claimed in the section 2.2

TOE meets all the requirements defined in the PP which the TOE claims conformance.

Security problem definition and security objectives contained in this ST are consistent with those in the PP.

3 SECURITY PROBLEM DEFINITION

3.1 Introduction

This section identifies security threats related to the TOE and defines actions that should be taken against these threats. Other threats, which are out of the scope of the TOE, are discussed in the assumptions. These threats are assumed to avoid independent from this ST. Organizational security policies are discussed in this section as well.

3.1.1 Threats

The threat agents are described below;

- Attackers who have knowledge of how the TOE operates and are assumed to possess a basic skill level, and intend to alter TOE configuration settings/parameters and no physical access to the TOE.

- TOE users who have extensive knowledge about the TOE operations and are assumed to have a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE.

The TOE address the following threats are applicable listed below

T. COMM The unauthorized user gains access to the user data and the patient data when it is traversing across the internet from to the application resulting in a loss of confidentiality and integrity of user data.

T.PRVLG_ESC An attacker/ a limitedly authorized user may modify management data that they are not authorized and gain access to the sensitive like patient data and system data by privilege escalation.

T.UNAUTH An unauthorized user obtains or modifies stored user data that they are not authorized to access resulting in a loss of confidentiality or integrity of the data.

T.AUDIT_TRAIL A threat agent may perform a large amount of transactions in order to fill the logs and hence make audit unavailable

T.DoS An attacker may attempt to make service unavailable by overwhelming it with traffic from multiple sources.

T.PASSWORD An attacker/unauthorized user may get the passwords in the database and authenticate to the TOE by these passwords causing confidentiality or integrity damage of user or management data.

3.1.2 Organizational Security Policy (OSP)

The organizational security policies are defined for secure use of the Healthcare information system in below;

P.VEM TOE should be able to transfer the available data (if available) stored in the database securely whenever the TOE is installed in the first time. Besides whenever TOE is uninstalled, TOE should be able to prepare the data for the transfer to a new software. During this data transfer process, the integrity of the data should be provided by the TOE.

3.1.3 Assumptions

The assumptions are described in below;

A.PHYSICAL It is assumed that the servers that host the web and database servers are hosted in a secure operating facility with restricted physical access with non- shared hardware.

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

4 SECURITY OBJECTIVES

4.1 INTRODUCTION

This section discusses the security objectives for the TOE and the security objectives for the Operational Environment of the TOE.

Security objectives are discussed in two parts: the security objectives for the TOE (security objectives that addressed directly by the TOE) and the security objectives for the Operational Environment of the TOE (security objectives that addressed by IT environment.

4.2 Security Objectives for the TOE

The security objectives for the TOE are described in below;

O.ACCESS The TOE must ensure that only authorized users are able to access protected resources or functions.

O.USER The TOE must provide an identification and authentication mechanism such that there will be no access to protected resources or functions before presenting user credentials.

O.MANAGE TOE shall provide all necessary means and functions in order that system administrators manage the system securely and effectively.

O.COMM The TOE must ensure that user data going across the network to the web server is protected from disclosure and integrity deprivation.

O.AUDIT TOE ensures that all operations related with accessing to system functionalities and security be audited.

O.HASH TOE ensures that passwords stored in the database are hashed.

4.3 Security objectives for the Operational Environment

The security objectives for operational environment are defined in below;

OE.PHYSICAL Security objectives for the operational environment shall provide physical security of the IT entities within the domain. Unauthorized entries and exits to and from this environment need to be blocked.

OE.ADMIN The owners of the TOE must ensure that the administrator who manages the TOE is not hostile and is competent.

OE.SEC_COMM Operational environment of the TOE shall provide a secure communication environment. Taking network security precautions should do this.

4.4 Security Objectives Rationale

The following table demonstrates that all security objectives trace back to the threats, OSPs and assumptions in the security problem definition.

*Table 1*Security Objectives Covarage

	THREATS						OSP	ASSUMPTIONS	
	T. COMM	T.PRVLG_ESC	T.UNAUTH	T.AUDIT_TRAIL	T.DoS	T.PASSWORD	P.VEM	A.PHYSICAL	A.ADMIN
O.ACCESS			X						
O.USER		X	X						
O.MANAGE		X							
O.COMM	X						X		
O.AUDIT		X		X					
O.HASH						X			
OE.PHYSICAL								X	
OE.ADMIN									X
OE.SEC_COMM					X		X		

T.COMM *O.COMM* objective ensures that all user data from the user to the web server will be secured using SSL protecting the user data from unauthorized disclosure and loss of integrity**.**

T.PRVLG_ESC *O.USER* objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions. *O.MANAGE* objective ensures that the TOE provides the tools necessary for the authorized administrator to manage the security-related functions and that those tools are usable only by users with appropriate authorizations. *O.AUDIT* objective ensures that all operations related with accessing to system functionalities and security be audited. It allows protecting these logs in a secure way and monitoring them when needed.

T.UNAUTH *O.ACCESS* objective ensures that the TOE restricts access to the TOE objects to the authorized users. *O.USER* objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.

T.AUDIT_TRAIL *O.AUDIT* objective provides functionality for taking action when the audit log is full.

T.DoS *OE.SEC_COMM* allows the communication network of the TOE to provide a secure communication environment that makes the denial of service attack ineffective.

T.PASSWORD *O.HASH* provides the hashed passwords presented by the users are stored in the database. Thus, to authenticate a user, the password provided by the user is compared with the stored hash.

P.VEM *O.COMM* objective ensures that all user data from the user to the web server will be secured using SSL protecting the user data from unauthorized disclosure and loss of integrity. *OE.SEC_COMM* allows the communication network of the TOE to provide a secure communication environment

A.PHYSICAL *OE.PHYSICAL*objective ensures that the TOE exists and operates in a physically secure environment. It prevents unauthorized individuals from entering in and exiting out of this environment.

A.ADMIN *OE.ADMIN*objective ensures that all users having administrator privileges have passed security controls and been selected from among experienced individuals.

5 EXTENDED COMPONENT DEFINITION

There is not any extended component in this Security Target.

6 SECURITY REQUIREMENT

6.1 SFR Formatting

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application.

- **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 *italics text* and are surrounded by square brackets as follows [*selection*].

- **Refinement:** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using **bolded text**, for additions, and ~~strike-through~~, for deletions.

6.2 Security Functional Requirements (SFR)

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

*Table 2*Security Functional Requirements

Requirement Class	Requirement Component
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.4: Prevention of audit data loss
FCS: Cryptographic Support	FCS_COP.1: Cryptographic Operation
FDP: User Data Protection	FDP_ACC.1: Subset Access Control
	FDP_ACF.1: Security Attribute Based Access Control
	FIA_AFL.1: Authentication failure handling

FIA: Identification and Authentication	FIA_UID.2: User identification before any action
	FIA_UAU.2: User authentication before any action
FMT: Security Management	FMT_MSA.1: Management of Security Attributes
	FMT_MSA.3: Static Attribute Initialization
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of The TSF	FPT_STM.1: Reliable time stamps
FTP: Trusted Path/Channels	FTP_TRP.1: Trusted Path

6.2.1 Security Audit

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 [*minimum*] level of audit; and
c) [**none**].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].

Application Note: Minimum level of auditable events are given below

Table3Minimum Level of Auditable Events

SFR	Auditable Events
FCS_COP.1	Success and failure, and the type of cryptographic operation

FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal)
FIA_UAU.2	Unsuccessful use of the authentication mechanism
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided
FMT_SMF.1	Use of the management functions
FMT_SMR.1	Modifications to the group of users that are part of a role
FPT_STM.1	Changes to the time
FTP_TRP.1	● Failures of the trusted path functions, ● Identification of the user associated with all trusted path failures, if available

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

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 [**System Auditor**] with the capability to read [**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.

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 [*detect*] unauthorized modifications to the stored audit records in the audit trail.

Application Note: Editing and deleting any log files from system by any type of users is not provided by TSF.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [*overwrite the oldest stored audit records*] and [**none**] if the audit trail is full

6.2.2 Cryptographic Operation

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform [**secure hashing**] in accordance with a specified cryptographic algorithm [**SHA-2 with the digest size of 512]** and cryptographic key sizes [**none**] that meet the following: [**FIPS PUB 180-4 Secure Hash Standard**].

6.2.3 User Data Protection

Application note: The access control policy which determines the objects and actions associated with identified roles are described here.

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 [**administrative access control policy**] on [
subjects: end user, system user, system administrator, system auditor
objects: Healthcare Information System Data
operations: Read, Write, Modify, Delete].

Application Note: The access control policy which determines the objects and actions associated with identified roles are described onTable4.

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 [**administrative access control policy**] to objects based on the following: [
subjects: end user, system user, system administrator, system auditor
objects: Healthcare Information System Data
subject attribute: User ID
object attribute: Module ID (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:
[

a) **If users is successfully authenticated according to access privilege assigned, then access are granted based on privilege allocated for that users**
b) **If user attempt are not successful, therefore, access permission is denied**

Table 4Access Control Policy

	Authentication Data	Audit Data	Configuration Data	Health Information	Contact Information	Individual Information
End user	**Read** and **Modify** his/her authentication data in TOE	**X**	**X**	**Read** his/her health information	**Read** **Modify** his/her contact information	**Read**
System user	**Read** and **Modify** his/her authentication data in TOE	**X**	**X**	**Read** **Write** **Modify**	**Read** **Write** **Modify**	**Read**
Sytem administrator	**Read, Write** and **Modify** authentication data of all users in TOE	X	**Read** **Write** **Modify**	X	**Read** **Write** **Modify**	X
System auditor	**Read** and **Modify** his/her authentication data in TOE	**Read**	X	X	X	X

Application Note: End user has Read Access on Health Informationonly forLaboratory Results, Diagnosis, Reports, Prescriptions.
].

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

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

6.2.4 Identification and Authentication

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 [*an administrator configurable positive integer within* **[3-10]** *default is* **[5]**] unsuccessful authentication attempts occur related to [**User Authentication**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [**block the user from the same ip address for 5 minutes**].

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.

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.

6.2.5 Security Management

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 [**administrative access control policy**] to restrict the ability to [*modify*, *delete*, **[create]**] the security attributes [**listed on table 5**] to [**System Administrator**].

Table 5Security Management

Authorised Role	Operations	Security Attribute
System Administrator	Modify	Users Groups User Status (Active/Pasive) User Access Rights Unsuccessfull Authetication Attempts
	Create	Users Groups
	Delete	Users Groups

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 [**administrative access control policy**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

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

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:
[**management of user groups,**
Management of user status
Management of user access rights
management of users unsuccessful authentication attempts].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [**End User, System User, System Administrator and System Auditor**].

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

6.2.6 Protection of TOE

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The ~~TSF~~**operational environment** shall be able to provide reliable time stamps

6.2.7 Trusted Path

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*initial user authentication*]

6.3 Security Assurance Requirements (SAR)

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

Table 6*Security Assurance 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

6.4 Security Requirements Rationale

6.4.1 SFR Dependency Rationale

The table below lists each SFR to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included

Table 7SFR Dependency Rationale

SFR	Dependency	Dependency Met?
FAU_GEN.1	FPT_STM.1	YES
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	YES YES(FIA_UID.2 is hierarchical to FIA_UID.1)
FAU_SAR.1	FAU_GEN.1	YES
FAU_STG.1	FAU_GEN.1	YES
FAU_STG.4	FAU_STG.1	YES
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	SHA-2 is a hashing algorithm and is a one-way function. Therefore it does not use any key for hashing and there is no FCS_CKM.1 and FCS_CKM.4 involved for the function. Therefore the dependencies are not applicable.
FDP_ACC.1	FDP_ACF.1	YES
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	YES YES
FIA_UID.2	-	-
FIA_UAU.2	FIA_UID.1	YES(FIA_UID.2 is hierarchical to FIA_UID.1)
FIA_AFL.1	FIA_UAU.1	YES(FIA_UAU.2 is hierarchical to FIA_UAU.1)
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1, YES YES
FMT_MSA.3	FMT_MSA.1	YES,

	FMT_SMR.1	YES
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	YES(FIA_UID.2 is hierarchical to FIA_UID.1)
FPT_STM.1	-	-
FTP_TRP.1	-	-

6.4.2 SFR – Objective Rationale

Table 8provides an overview for security functional requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen.

Table 8 *SFR Covarage*

	O.ACCESS	O.USER	O.MANAGE	O.COMM	O.AUDIT	O.HASH
FAU_GEN.1					X	
FAU_GEN.2					X	
FAU_SAR.1					X	
FAU_STG.1					X	
FAU_STG.4					X	
FCS_COP.1						X
FDP_ACC.1	X					
FDP_ACF.1	X					
FIA_UID.2		X				
FIA_UAU.2		X				
FIA_AFL.1	X					
FMT_MSA.1			X			
FMT_MSA.3			X			
FMT_SMF.1			X			
FMT_SMR.1		X	X			
FPT_STM.1					X	
FTP_TRP.1				X		

O.ACCESS

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. *FIA_AFL.1* defines values for some number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures.

O.USER

FIA_UAU.2 meets the objective by confirming that the user is authenticated before any TSF-mediated action. *FIA_UID.2* meets the objective by ensuring that the user is identified before any TSF-mediated action. *FMT_SMR.1* manages 4 roles (End User, System User, System Administrator and System Auditor).

O.MANAGE *FMT_MSA.1* encounters this objective by allowing the system administrator to manage the specified security attributes. *FMT_MSA.3* ensures that the default values of security attributes are restrictive. FMT_SMF.1 allows the specification of the management functions to be provided by the TOE. *FMT_SMR.1* manages 4 roles (End User, System User, System Administrator and System Auditor).

O.COMM FTP_TRP.1 helps to meet the objective by establishing an SSL Secure channel from the user's browser to health informatics system application protecting the user data from disclosure and modification.

O.AUDIT With reliable time stamps provided by *FPT_STM.1*, *FAU_GEN.1* generates the minimum level of auditable events, and specifies the list of data that shall be recorded in each record and *FAU_GEN.2* associate auditable events to individual user identities. *FAU_SAR.1* provides that the user with system auditor role can view the all audit information. *FAU_STG.1* protects audit trail from unauthorized deletion and/or modification. *FAU_STG.4* specifies actions in case the audit trail is full.

O.HASH *FCS_COP.1* helps to meet the objective by hashing all the passwords using SHA- 2 before they are written into the database.

6.4.3 SAR Rationale

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 EAL2was chosen for this ST.

7 TOE SUMMARY SPECIFICATION

7.1 Security Enforcing Functions

TOE carries out its security related operations with security enforcing functions which defined below sections.

7.1.1 Identification /Authentication

TOE users are forced to identification and authentication operations before doing any action. Users who fail to identify and authenticate can not perform any action in the TOE. User name and password are used for identification and authentication operations. [FIA_UID.2, FIA_UAU.2]

Users credential/password are stored in database with salted hash. When a TOE user change his/her password or during authentication, salted hashing action do by the TOE. [FCS_COP.1]

User from the same ip will be blocked for 5 minutes if user attempt count is reached to defined invalid attempt count which is defined by system administrator between 3 and 10. Invalid attempt count's default value is 5. [FIA_AFL.1]

7.1.2 Access Control

All users are able to operate on healthcare information system data according to access control policy which is defined in Table 4. Any user attempt to access an operation is granted or blocked based on privilege defined in access control policy. The access control policy gives permissions to user with a user id and a module id pair. [FDP_ACC.1, FDP_ACF.1]

7.1.3 Audit

The TOE generates audit logs that consist of various auditable events or actions taken by the users and administrators. TOE has ability to record the following information into each audit logs that is generated: Date and time on which the event was logged; username of the user for whom the log entry was made; the outcome (success or failure) of the event for which the check that generated the log entry was performed; indication as to whether the access request succeeded or failed. [FAU_GEN.1, FAU_GEN.2]

The time stamps are taken from operational environment (operating system) to use on records. [FPT_STM.1]

A user with System Auditor role is able to read all audit information in a suitable form from the audit records. [FAU_SAR.1]

Any type of users are not allowed to modify and delete audit records by the TOE to block unauthorized modifications to the stored audit records in the audit trail. If the audit trail is full, the oldest audit records are overwriten. [FAU_STG.1, FAU_STG.4]

7.1.4 Management

System Administrator associates roles with users. There roles have been identified end user, system user, system administrator and system auditor. TOE can be capable of performing management function listed below;

- management of user groups,
- management of user status,
- management of user access rights
- management of users unsuccessful authentication attempts.

[FMT_SMF.1, FMT_SMR.1]

System administrator is able to override default values with a minimal values to manage security attributes. TOE provides effective interfaces for management of security attributes. These attributes are Users Groups, User Status, User Access Rights, Unsuccessfull Authetication Attempts. [FMT_MSA.1, FMT_MSA.3]

7.1.5 Secure Communication

When the TOE communicates other applications and system, communications should be done in a secure way, using the SSL protocol to protect data traversing across the internet from/to the application from modification and disclosure. Users are always authenticated, authorized and given access to the operations and data via trusted path. [FTP_TRP.1]

7.2 Security Enforcing Functions Coverage

Table 9 provides an overview for security enforcing functions coverage also giving an evidence for covarage of the SEFs defined.

Table 9Security Enforcing Functions Covarage

	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_STG.1	FAU_STG.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FIA_AFL.1	FIA_UAU.2	FIA_UID.2	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_STM.1	FTP_TRP.1
Identification/Authentication						X			X	X	X						
Access Control							X	X									
Audit	X	X	X	X	X											X	
Management												X	X	X	X		
Secure Communication																	X