AKGUN HEALTH INFORMATION SYSTEM v4.0

Security Target

AKGUN HEALTH INFORMATION SYSTEM (AKGUN HIS)

Akgun HIS v4.0
02-03-2018

Document management

Document identification

Document Id	KALITE-02_Web40HIS_ST_EAL2_v2.2
Document title	Akgun HIS Security Target
Document date/version	2.2, 02.03.2018

Document History

Version	Date	Description
0.1	29.02.2016	Released for internal review
0.2	02.04.2016	Content improvement
0.3	28.04.2016	Some Corrections and Improvements
0.4	07.06.2016	Some Corrections and Improvements
0.5	28.06.2016	Contents of the TOE description updated, some corrections and improvements
0.6	02.09.2016	Contents of the TOE description updated, some corrections and improvements
0.7	03.10.2016	Contents of the Security Target updated according to released PP
0.8	04.11.2016	Some Corrections and Improvements
0.9	23.12.2016	Some Corrections
1.0	26.12.2016	TOE version updated
1.1	31.01.2017	FCS_COP.1.1 updated
1.2	20.04.2017	FDP_ACC.1.1 updated
1.3	26.04.2017	FDP_ACC.1.1 and FDP_ACF.1.1 updated
1.4	09.05.2017	Some Corrections and Improvements
1.5	16.05.2017	Some Corrections and Improvements
1.6	30.05.2017	FIA_AFL.1.1 updated and TOE Description updated and Physical Scope of TOE updated
1.7	19.06.2017	FAU_STG.4.1 updated
1.8	01.12.2017	FAU_STG.4 updated
1.9	05.02.2017	ST Reference updated, Target of Evaluation (TOE) Overview updated, TOE Description updated, Usage and Major Basic Security and Functional Attributes updated, PP Conformance Claim updated, Security Problem Definitions updated, FAU_STG.4 updated
2.0	08.02.2018	Type of Users updated
2.1	23.02.2018	TOE Type updated, Physical Scope of TOE updated, FAU_SAR.1 updated
2.2	02.03.2018	Physical Scope of TOE updated, Operational Environment Components and Supported Non-TOE Software and Hardware Components for TOE updated

Table of Contents

Document management 2

Document identification 2

Document History 2

Table of Contents 4

List of Figures 6

1. ST Introduction 7

1.1 ST Reference 7

1.2 Target of Evaluation (TOE) Overview 7

1.2.1 Introduction 7

1.2.2 TOE type 7

1.2.3 Operational Environment Components 7

1.2.3.1 Operational Environment Components and Supported Non-TOE Software and Hardware Components for TOE 7

1.2.3.2 Usage and Major Basic Security and Functional Attributes 9

1.2.4 Type of Users 10

1.2.5 TOE Description 10

1.2.5.1 Physical Scope of TOE 11

1.2.5.2 Logical Scope 11

2. Conformance Claims 12

2.1 Common Criteria Conformance Claim 12

2.2 PP Conformance Claim 12

2.3 Package Conformance Claim 12

3. Security Problem Definitions 12

3.1 Introduction 12

3.2 Threats 12

3.2.1 Threat Agents 12

3.2.2 Threats 12

3.3 Organizational Security Policies 13

3.4 Assumptions 13

3.4.1 Assumptions on Personnel 13

3.4.2 Assumptions on Physical Environment 14

4. Security Objectives 14

4.1 Introduction 14

4.2 Security Objectives for the TOE 14
4.3 Security Objectives for the Operational Environment 15
4.4 Security Objectives Rationale 15
5. Extended Components Definition 16
6. Security Requirements 17
6.1 SFR Formatting 17
6.2 Security Functional Requirements (SFR) 17
6.2.1 Security Audit 18
6.2.2 Cryptographic Operation 20
6.2.3 User Data Protection 20
6.2.4 Identification and Authentication 22
6.2.5 Security Management 22
6.2.6 Protection of TOE 23
6.2.7 Trusted Path 23
6.3 Security Assurance Requirements 24
6.4 Security Requirements Rationale 24
6.4.1 SFR Dependency Rationale 24
6.4.2 SFR – Objective Rationale 25
6.4.3 SAR Rationale 27
7. Toe Summary Specification 27
7.1 Security Audit 27
7.2 Cryptographic Operation 27
7.3 User Data Protection 27
7.4 Identification and Authentication 28
7.5 Security Management 28
7.6 Trusted Path 28

List of Figures

Figure 1 : The overall structure of the operational environment of the TOE. TOE components are shown by red. All the communication between the TOE and its environmental components is done by SSL. 8
Figure 2 : The major security objectives of the TOE 11

1. ST Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) references, document organization, TOE Overview and TOE Description.

1.1 ST Reference

The following table presents reference information related to this security target.

Title	AKGUN HEALTH INFORMATION SYSTEM v4.0 Security Target
ST Version	2.2
TOE Version	4.0
Publication Date	02.03.2018
Authors	Zeki DEMİRCİ
Evaluation Assurance Level(EAL)	EAL2
TOE Reference	Akgun HIS

1.2 Target of Evaluation (TOE) Overview

AKGUN HIS is the set of web based software systems necessary for health management, such as patient management, hospital stock, account management, laboratory services etc.

1.2.1 Introduction

TOE is a logical security modüle for web-based health information system. The web-based health information management system mentioned here refers to an application which hosts and processes all kinds of patient data and which can be accessed online.

TOE is a general one, which is prepared for Hospital Information Management System which provides online services.

1.2.2 TOE type

The type of the TOE is a logical security module for web based general purpose health information systems application.
Application Note: The type of the TOE is a logical security module for web based general purpose health information systems application. Sentence is came from protection profile but TOE is only web based.

1.2.3 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.

1.2.3.1 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 mandatory/optional components are performed by SSL communication protocol

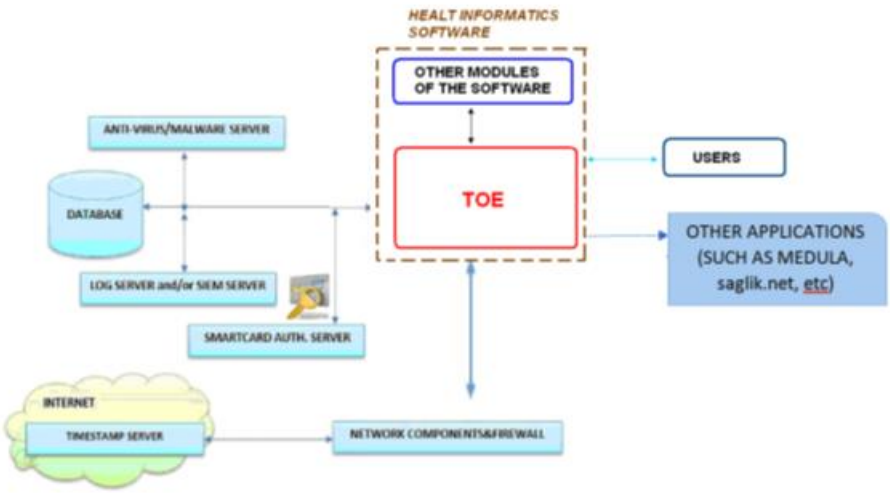

Figure 1 : The overall structure of the operational environment of the TOE. TOE components are shown by red. All the communication between the TOE and its environmental components is done by SSL.

Application Servers: Application server is the environment that running Akgun HIS application. Number of application server can be multiple.

CAS APP Servers: Both identification/authentication process and managing user role and their authorities process are running on this environment. This environment has two services which are CAS Server and CAS Client:

- **CAS Server:** Identification and authentication processes are running on this environment. Either successful or failed login attempts, all user login activities are logged.
- **CAS Client:** The environment is that creating user, managing their status, roles and authorities. Also, CAS Client provides effective control mechanisms for the users responsible for administration of the system. It is important that these mechanisms are make decision-making process easier and more effective. 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 as a minimum 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 (structuring settings, reviewing the logs, etc.), which are used in audits.

Web server: The TOE operates on a web server as a web application. This web server can be any Java container or J2EE container.

Operating system: The server that the TOE operates on Oracle Linux. The web server that the TOE operates 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 from product to product. Bur at least 2 virtual servers one for web server, another for DBMS. Web server configuration will be 32 GB Ram, 2 vCPU, 250 GB HDD space, DBMS configuration will be 32 GB Ram, 2 vCPU, 500 GB HDD space.

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 has the feature of being electronic signature-based (which is created by the hardware).

Database: TOE saves all of the user and patient records in this database.

Medula: TOE gets patient social security convenience. TOE send to Medula social security number, assurance type, province code, provision date etc.

Saglik-net: TOE sends patient medical record information. TOE send to Saglik-net Patient pursuit information, Patient prescription information, Patient report information, Medical information etc.

1.2.3.2 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 (date of birth, place of birth, blood type, etc.), contact information (Social Security Number, citizenship number, etc.) 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. 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 1.2.4.

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 are 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 make decision making process easier and more effective. TOE provides system administrator's authorization and data management functionalities. 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.

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 is noted that protection is being 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, etc. Those communications are 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.

1.2.4 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, etc. Administrator can access the application, database, file system and other entities with all privileges.

System Auditor: System auditors have read only access privileges 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.

1.2.5 TOE Description

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

1.2.5.1 Physical Scope of TOE

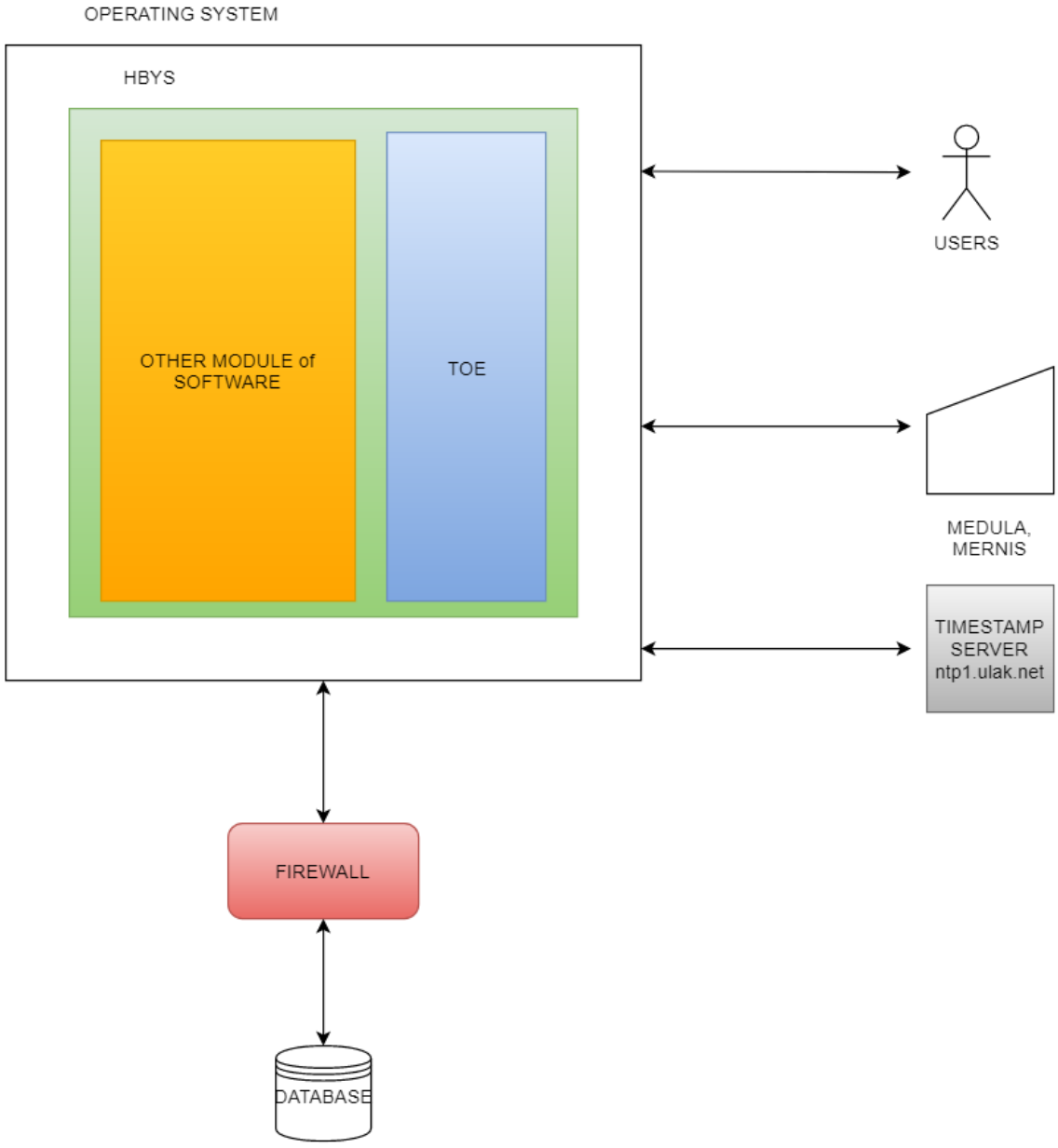

Figure 2 Physical scope of TOE

1.2.5.2 Logical Scope

Akgun HIS is a software program. 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 (date of birth, place of birth, blood type, etc.), contact information (Social Security Number, citizenship number, etc.) 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. TOE provides access permissions, TOE

automatically audits logs, TOE provides effective control mechanisms, and TOE keeps records.

2. Conformance Claims

2.1 Common Criteria Conformance Claim

This security target is developed using Common Criteria Version 3.1, Revision 4.

This security target has strict conformance with Common Criteria Part 2.

This security target has strict conformance with Common Criteria Part 3.

2.2 PP Conformance Claim

The security target conforms to TSE Protection Profile for Security Module of General-Purpose Health Informatics Software v 1.0.

2.3 Package Conformance Claim

This security target conforms to the assurance package EAL 2, which is defined in Common Criteria Part 3.

3. Security Problem Definitions

3.1 Introduction

This section identifies security threats. Other threats, which are out of the scope of the TOE, are discussed in the assumptions. Organizational security policies are discussed in this section as well.

3.2 Threats

This section includes list of the threats which effects

3.2.1 Threat Agents

Threat Agents (Actor)	Explanation
Attacker	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	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.

3.2.2 Threats

Threats	Statements
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.

3.3 Organizational Security Policies

The organizational security policies are described in below;

Assumption	Explanation
P.VEM	TOE is 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 is able to prepare the data for the transfer to a new software. During this data transfer process, the integrity of the data is provided by the TOE.

Application Note: The format of data for the transfer follow the rules defined by the Republic of Turkey, Ministry of Health. This format is also known as VEM. The details of the VEM can be found on the web site of the Ministry of Health.

3.4 Assumptions

Assumptions made during the preparation are collected under two main headings:

- ✓ Assumptions related to the personnel,
- ✓ Assumptions related to the physical environment,

3.4.1 Assumptions on Personnel

Assumption	Explanation

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.

3.4.2 Assumptions on Physical Environment

Assumption	Explanation
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.

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, which are not technical).

4.2 Security Objectives for the TOE

Assumption	Explanation
O.ACCESS	The TOE must ensure that only authorized users are able to access protected resources or functions.
O.USER	The TOE must ensure that all users are identified and authenticated before they access any/ some a protected resources or functions
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

Identifier	Objective statements
OE.PHSICAL	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 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.

	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		

Identifier	Explanation
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 Components Definition

This ST does not need any extended component

6. Security Requirements

6.1 SFR Formatting

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from TSE Health Informatics Software protection profile, providing assurance requirements.
TSE Health Informatics Software protection profile 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.

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: Identification and Authentication	FIA_AFL.1: Authentication failure handling

	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; c) [**none**].
FAU_GEN.1.2	The TSF shall record at least one of the following information within each audit record: 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, [**object of event**].

Component	**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

Table 1 : Auditable Events

FAU_GEN.2	**User identity association**
Hierarchical to:	No hierarchical 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 causes the event.

FAU_SAR.1	**Audit review**
Hierarchical to:	No hierarchical 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 data**] 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.

Application Note: Log records can also be viewed by the system administrator.

FAU_STG.1	***Protected audit trail storage***

Hierarchical to:	No hierarchical 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: Beside detecting unauthorized modifications, the TSF prevents any action (modify and delete) to the stored audit records in the audit trail. Audit records can be only read by system auditor. Even if system auditor has no permission to modify audit records.

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 hierarchical 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 [**SHA2-512**] and cryptographic key sizes [**none**] that meet the following: [**none**].

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 hierarchical components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the [**Access Control Policy**] on [**subjects: System Administrator, End User, System Auditor ,System User; object: TOE Modules, user data', user status, user attributes, audit logs, authentication and authorization configurations; operations: read, delete, modify, and create**].

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No hierarchical components
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1	The TSF shall enforce the [**Access Control Policy**] to objects based on the following: [**End User, System User, System Administrator and System Auditor].**
	• **System Administrator can**
	  ○ **Have access right for all TOE modules**
	  ○ **Read/Write/Delete/Modify user attributes**
	  ○ **Modify secrets of each users including his/hers**
	  ○ **Create or delete authorized users**
	  ○ **Modify users' status**
	• **End User can**
	  ○ **Read his/her own user attribute, assigned role**
	  ○ **Modify his/her own secret**
	• **System Auditor can**
	  ○ **Read audit logs**
	  ○ **Reads authentication and authorization configurations**
	• **System User**
	  ○ **Have access right for all HIS modules**
	  ○ **Read user attributes**
	  ○ **Read and modify module parameters**
	  ]

FDP_ACF.1.2	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 has the**

	right role which has been granted access].
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 [1] unsuccessful authentication attempts occur related to [**user attempting to authenticate within a three seconds**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [**disable the user in a period of time. This period can be adjust manually**]

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 [**Access Control Policy**] to restrict the ability to [*change_default, query, modify, delete,* [**none**]] the security attributes [**associated roles, user status**] to [**System Administrator**].

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 [**Access Control Policy**] to provide [*restrictive,* [**none**]] 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: [**create, delete, modify, and read security attributes**].

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,* [**none**]].
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,*[**none**]]

6.3 Security Assurance Requirements

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_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	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_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
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

Component	Dependency	Dependency Met?
FAU_GEN.1	FPT_STM.1 Reliable time stamps	YES
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	YES YES(FIA_UID.2 is hierarchical to FIA_UID.1))
FAU_SAR.1	FAU_GEN.1 Audit data generation	YES
FAU_STG.1	FAU_GEN.1 Audit data generation	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 Security attribute-based access control	YES
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	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 FMT_SMR.1	YES, YES
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Timing of identification	YES(FIA_UID.2 is hierarchical to FIA_UID.1)
FPT_STM.1	-	-
FTP_TRP.1	-	-

6.4.2 SFR – Objective Rationale

	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 appropriately either permissive or restrictive in nature. 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 EAL2 was chosen for this ST.

7. Toe Summary Specification

7.1 Security Audit

All of the users (End User, System User, System Administrator and System Auditor) access the TOE via web. The TOE generates audit logs that consist of Start-up and shutdown of the audit functions, All auditable events for the minimum level of audit. These logs that are associated by users are produced with a reliable time stamp provided by the TSF operational environment. The TOE detects the capability for system audit to read and view all the recorded logs. The TSF prevents the system auditor from modifying or deleting audit logs. When audit trail becomes full, TOE ignores audited events by deleting audit logs which are older than 1 year.

Functional Requirement Satisfied: *FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FAU_STG.4, FPT_STM.1*

7.2 Cryptographic Operation

The TOE encrypts the passwords of the TOE users. While doing this encryption, the TOE perform secure hashing with a cryptographic algorithms SHA2 to protection of user passwords.

Functional Requirement Satisfied: *FCS_COP.1*

7.3 User Data Protection

System Administrator of the TOE can perform the following functions: accessing all TOE Modules, reading user attributes, modifying user status and secrets, adding or removing authorized users.

End User of the TOE can perform the following functions: reading his/her own user attributes, modifying his/her own secrets.

System Auditor of the TOE can perform the following functions: read audit logs, reads authentication and authorization configurations.

System User of the TOE can perform the following functions: accessing all TOE HIS Modules, reading user attributes, read and modify module parameters

Functional Requirement Satisfied: FDP_ACC.1, FDP_ACF.1

7.4 Identification and Authentication

The Identification and Authentication security function provides each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. The TOE ensures that a user (or administrator) identity is established and verified before access to the TOE is allowed. Prior to allowing access, the TOE requires administrator and users to be identified using a username and password. Before successful completion of the security function, a user or administrator 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 roles. When unsuccessful authentication attempts reached the limit (this limit is a configurable value by administrator 1), user can not try any authentication attempt in a 3 seconds. This time can be configurable also.

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

7.5 Security Management

The TOE provides necessary roles to govern which users can access with resources or functions. The Security Management function allows the system administrator to properly configure this functionality. System administrator can assign roles to users by user levels based on the functions or resources that they are allowed to perform or access. Hence ability of the changing security attributes is restricted. On the other hand, System Administrator is allowed to specify alternative initial values to override the default values when an object or information is created. Also these values can be created, deleted, modified and read.

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

7.6 Trusted Path

All of the users (End User, System User, System Administrator and System Auditor) access the TOE via web. Hence, the TOE provide a secure communication path between itself and users by using a standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. Hence a trusted path is being permitted between remote users. For the initial user authentication, the trusted path is required by the TOE.

TOE Security Functional Requirements Satisfied: FTP_TRP.1