Protection Profile for Security Module of General-Purpose Health Informatics Software

Version 1.0

TURKISH STANDARDS INSTITUTION

07.09.2016

DEVELOPERS

Feyzullah Koray ATSAN

Gökhan ŞENGÜL

REVISION HISTORY

Revision No	Revision Date	Reason for Change	Prepared By
0.1	01.12.2015	First Draft	Feyzullah Koray ATSAN, Gökhan ŞENGÜL
0.2	26.01.2016	Update according to OKTEM meetings	Feyzullah Koray ATSAN, Gökhan ŞENGÜL
0.3	13.07.2016	Update according to Observation Report 1	Feyzullah Koray ATSAN, Gökhan ŞENGÜL
1.0	07.09.2016	Update according to Observation Reports 2 and 3 (Release Version)	Feyzullah Koray ATSAN, Gökhan ŞENGÜL

Contents

1 PP Introduction

1.1 PP Reference

The following table presents reference information related to this protection profile.

Title	Protection Profile for Security Module of General-Purpose Health Informatics Software
Version	1.0
Publication date	
Authors	Feyzullah Koray ATSAN, Gökhan ŞENGÜL
Evaluation Assurance Level (EAL)	EAL2

1.2 Goal and the Scope

In accordance with the developments in the recent years, newer information technology equipment and software has been developed and put into practice. Health is one of the areas that those technological products are used in. In order to use the data and the sources of the health facilities, various software applications are used. Hospital Information Management Systems, Family Practice Information Systems, Picture Archiving and Communication Systems (PACS), Laboratory Information Management Systems, Digital Document Management Systems and other health informatics software applications, which provide online services, are the most important ones. As these software applications need to interact and communicate with different applications, they usually operate online. This protection profile discusses security modules of health information software.

The purpose of this protection profile, which is designed to provide a security outline to general-purpose health information systems, is to identify a security module which can be applied to all kind of health information software (including Hospital Information Management Systems, Family Practice Information Systems, Picture Archiving and Communication Systems (PACS), Laboratory Information Management Systems, Digital Document Management Systems). Besides this protection profile defines the minimal security requirements for the software used in public and private healthcare institutions.

In parallel with the technological developments, health information systems, which host and process all kinds of information related to human health are now developed as web-based or desktop based systems. Both systems (web based or desktop based) need to interact and exchange information with the other applications such as saglik.net or MEDULA through the Internet. Taken into consideration that the Internet is vulnerable to threats, it is obvious that these software must have sufficient security measures. Ensuring that organizations take necessary security measures efficiently is only possible when these organizations comply with the standards and related certifications. The purpose of this protection profile is to cover the need for a guideline document, which can be used in certification processes of security modules of web-based and desktop based health information systems. This protection profile discusses medium-level security measures related to health information system applications.

This protection profile is intended for the desktop based and web-based health information system applications in general. In other words, functional features and components which are valid for all desktop-based and web-based health information systems were taken into consideration and those features and components which are specific to the applications were left out of the scope. There are two options for security features and components, which are out of scope of this protection profile if they wanted to be included in certification processes. The first option is to cover these security features and components in the Security Target document. The second and recommended option is to refer the protection profile of the specific product.

When developing a protection profile; some issues that the application is responsible to protect, such as the level of criticality and confidentiality of the data, the tangible and intangible damage could occur by the loss and disclosure or unwanted modification of the data, shall be taken into consideration. In applications, which are the subject of this protection profile, patient records are processed. Additionally personal information related to the workers in the health sector (incumbent physicians, the department that they work, the patients that they treat, etc.) is stored in these applications as well. In the case that the information (on the basis of individually or statistically) mentioned here is accessed by illegal parties, serious damage might be caused. Therefore when security is not provided for the TOE, critical tangible and intangible damages may occur. What is more is the loss of prestige. In consequence, in both private and public health sectors, it is vital to provide security for the applications.

1.3 Target of Evaluation (TOE) Overview

This section defines Target of Evaluation of the protection profile.

1.3.1 Introduction

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

This protection profile is a general one, which is prepared for Hospital Information Management System, Family Practice Information System, Picture Archiving and Communication System (PACS), Laboratory Information Management System, Digital Document Management System and other health informatics application software, which provides online services. Therefore, in this protection profile 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 or desktop 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. Since TOE is the **logical security module** for general purpose health information software, the operational environments components of the TOE is given in the following sections.

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 (typically and some optionally), 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

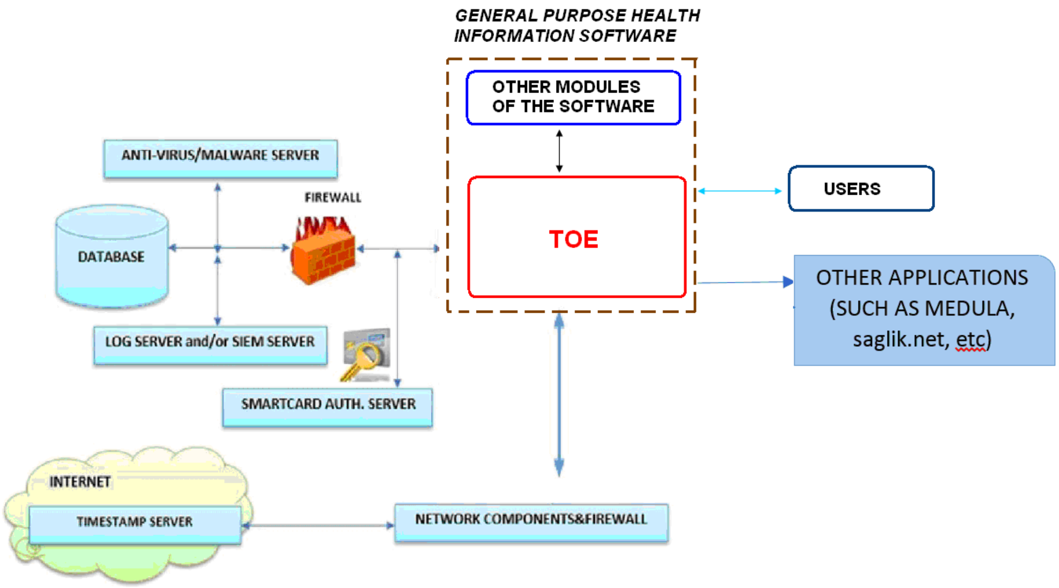

Figure 1 – *The overall structure of typical operational environment of the TOE. TOE components are shown by red. All the communication between the TOE and its environmental components should be done by SSL.*

The mandatory and optional components of the TOE are explained below:

Web server: The TOE operates on a web server as a web application. This web server may use any technology.

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.

Communicating with other applications (optional): TOE may need to interact with the other applications such as saglik.net, e-nabiz, MEDULA, etc. In these cases TOE needs to provide a secure communication with these applications.

Log server and/or SIEM server (optional): This component is optional in the TOE environment. A log server will enable the TOE Audit logs to be stored and managed centrally thereby increasing availability of the audit logs. These audit logs can also be correlated by a SIEM server in order to identify and respond to cyber-attacks.

Application note: Log server and/or SIEM server usage is optional in the context of this protection profile. If Log server and/or SIEM server is used in the TOE, then the necessary SFRs should be added to Security Target of the TOE.

Smartcard Authentication server (SAS) (optional): This component is optional in the TOE environment. Smartcard authentication will enable the TOE to utilize strong authentication instead of weak authentication mechanism such as password authentication.

Application note: Smartcard authentication is optional in the context of this protection profile. If smartcard authentication is used in the TOE, then the necessary SFRs should be added to Security Target of the TOE.

Anti-virus/Malware Server (optional): This component is optional in the TOE environment. An anti-virus/malware server will protect the TOE from virus and malware and the threats that can be introduced to the environment by these elements such as sniffing, data corruption etc.

Application note: Anti-virus/Malware server usage is optional in the context of this protection profile. If Anti-virus/Malware server is used in the TOE, then the necessary SFRs should be added to Security Target of the TOE.

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 (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. However it is recommended that hashing information should be 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.

Application note: In the context of this protection profile authentication is performed through user name and password verification. When high level of security is needed, additional authentication methods like SMS confirmation, verification through mobile devices, electronic

signature, etc. could be used in addition to user name and password verification. In this case the necessary SFRs should be added to the ST of the TOE.

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 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.

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, etc. 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

In addition to the roles listed above, the TOE may have additional roles. In case an additional role is needed, it shall be listed and explained in ST by ST Author.

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 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 Document Overview

Part 1 provides the definitions of TOE and the Protection Profile. Thanks to this preliminary information security requirements and functions will be understood better.

Part 2 identifies conformance claims. Among these conformance claims are there common criteria conformance claims, Protection Profile conformance claims and package conformance claims. In addition, conformance claims rationale and which kind of conformance that a ST (Security Target) must conform this protection profile is expressed in this part as well.

Part 3 provides the definition of security policy and identifies threats, assumptions and organizational security policies, which are within the scope of TOE.

Part 4 defines security targets that correspond to the threats, assumptions and organizational security policies, which were identified in Part 3.

Part 5 identifies extended components for extended security requirements.

Part 6 discusses security functional requirements, security Assurance requirements and security Assurance requirements rationale under the general title of security requirements.

In the last section, bibliography, supportive noteworthy references are given.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

This protection profile is developed using Common Criteria Version 3.1, Revision 4.

This protection profile has strict conformance with Common Criteria Part 2.

This protection profile has strict conformance with Common Criteria Part 3.

2.2 PP Conformance Claim

This protection profile was not prepared as to conform to another protection profile.

2.3 Package Conformance Claim

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

2.4 Conformance Claim Rationale

As this protection profile doesn’t claim conformance to another protection profile, this part is not applicable.

2.5 Conformance Statement

This protection profile requires “strict conformance”.

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 protection profile. Organizational security policies are discussed in this section as well.

3.2 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 in table 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.

3.3 Organizational Security Policy

The organizational security policies are described 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.

Application Note: The format of data for the transfer should 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

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.

	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 Protection Profile

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.

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; and

c) [assignment: other specifically defined auditable events].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

Application Note: Minimum level of auditable events are given below

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.

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 [selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by the authorized user with special rights”, “overwrite the oldest stored audit records”] and [assignment: other actions to be taken in case of audit storage failure] 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 [selection, choose one of: “224”, “256”, “384”, “512”]**]and cryptographic key sizes [**none**] that meet the following: [assignment: list of standards].

Application note: SHA-2 algorithm has different implementations using the digest size of 224, 256, 384, or 512. The developers may choose one of the alternatives and they are not restricted about the digest sizes.

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 [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes that explicitly authorize access of subjects to objects].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes that explicitly deny access of subjects to objects.

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 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of authentication events].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [assignment: list of actions].

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 [assignment: access control SFP(s), information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] 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 [assignment: access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: the authorized identified roles] 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: [assignment: list of management functions to be provided by the TSF].

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.

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

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 FMT_SMR.1	YES, 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

	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.