ProMedArt Biyoteknoloji ve Özel Sağlık Hizmetleri Ltd.Şti.

Yazılım Geliştirme Bölümü

Promedart HIS and LIS Güvenlik Modülü Uygulamaları v1.0.5.14

SECURITY TARGET

Document Name	: Promedart HIS and LIS Güvenlik Modülü Uygulamaları v1.0.5.14 Security Target
Document Version	: 1.11
Revision Date	: 05.04.2019
Prepared by	: İsmet Turgut / Technical Director Gökhan Kaya / Consultant
Approved by	: Gürsel Turgut / Project Manager

Revision History

Revision No	Revision Reason	Date of Revision
1.0	First Release	07.12.2017
1.1	Physical and logical scopes of TOE are updated.	18.04.2018
1.2	Physical scope of TOE, FDP_ACF.1.4 and FMT_SMF.1 are updated.	31.05.2018
1.3	Physical scope of TOE is updated.	05.06.2018
1.4	FDP_ACF.1 and FAU_SAR.1, Operational Environment Components are updated.	02.01.2019
1.5	TOE Overview, Physical Scope, Logical Scope of TOE, Access Control, Audit, Management are updated	16.01.2019
1.6	Updated according to the remarks from the evaluation facility	28.01.2019
1.7	Updated according to the remarks from the evaluation facility	04.02.2019
1.8	Updated according to the remarks from the evaluation facility	21.02.2019
1.9	Updated according to the remarks from the evaluation facility	02.04.2019
1.10	Updated according to the remarks from the evaluation facility	03.04.2019
1.11	Updated according to the remarks from the evaluation facility	05.04.2019

ACRONYMS

CC	: Common Criteria
CCMB	: Common Criteria Management Board
EAL	: Evaluation Assurance Level (defined in CC)
OSP	: Organizational Security Policy
PACS	: Picture Archiving and Communication Systems
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

1.1 ST Reference

ST Title	Promedart HIS and LIS Güvenlik Modülü Uygulamaları v1.0.5.14 Security Target
ST Version	1.11
ST Publication Date	05.04.2019
CC version	Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 5)

1.2 TOE Reference

TOE Identification	Promedart HIS and LIS Güvenlik Modülü Uygulamaları v1.0.5.14
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

1.3 TOE Overview

TOE is online application and used for tracking Patients who visit Polyclinics / Hospitals. Patients visit Polyclinic and their treatments are performed inside. During this period, radiological operations and laboratory tests are performed. Patients reports, patients anamnesis are processed with this software in addition to patients data and invoice details. Branch users, Doctors and all office centres use software by n-tier structure

HIS modüles :

Patient acceptance
Invoice
Stores and Drugs Control
Operations
Doctor's Treatments & Tracking.

LIS Modules :

Patients Sample Requests & Acceptance
Barcode Generation
Analyzers Integration & Results Entry
Medical Validation
Reports Generation

The TOE is a logic security module in this system with the following basic security functions.

- Identification and Authentication (Application can be used only after user identified and validated by password and they can use / do only their assigned functions).

- Security Management (assign / modify privileges by Administrators. Password generation and unlocking).
- User Data Protection (Privilege assignments protects user data against modification and unauthorized access).
- Security Audit (The TSF generates audit logs that consists of various auditable events)
- Secure comminication (TOE provides secure comminication between TOE and other components)

These functions will be handled by using WCF (Windows Communication Foundation) service in n-tier structure. All database operations, logs generations and security operations will be done at WCF service. Main functions of this service is token generation for connection, loading user's authorization, database connections and executions by security checking.

1.3.1 Introduction

TOE is a logical security module for desktop 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 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.

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 ProServis Server on which the TOE operates and this application 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

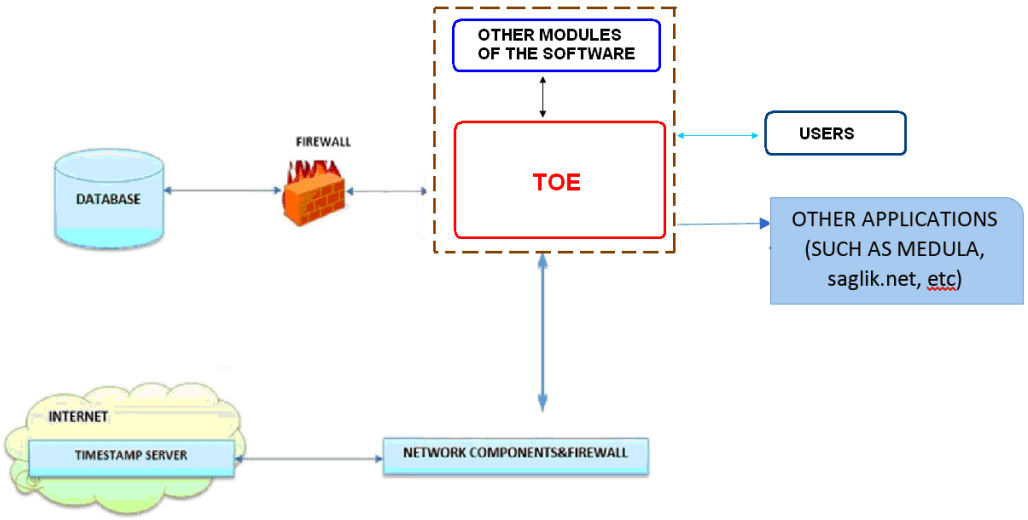

Figure 1 The structure of operational environment of the TOE. TOE components are shown by red. All the communication between the TOE and its environmental components done by SSL.

Database Server	
CPU	2 Core 2.6 Ghz
Memory	6 GB
Disk for TOE	500 GB
Disk for TOE Log	500 GB
Operating System	Windows Server R2008 or Higher
RDBMS	MySQL v5.1 or higher
Connectivity	TCP/IP
ProServis Server	
CPU	2 Core 2.6 Ghz
Memory	6 GB
Disk for Logs	500 GB
Operating System	Windows Server R2008 or Higher (if server preferred) Windows 7 or Higher (otherwise) .Net Framework 4.5.2
Connectivity	TCP/IP
Client	
CPU	2.6 GHz
Memory	4 GB
Operating System	Windows XP or Later

	.Net Framework 4.5.2
Disk	100 GB
Connectivity	TCP/IP
Software	t-HIS or i-LIS

ProServis server: The TOE operates on a ProServis server as a WCF Service (WCF: Windows Communication Foundation). This web server may use any technology on Windows Server Environment. This service uses .Net Framework 4.5.2 or higher.
Operating system: The server that the TOE runs on has an operating system. The ProServis server that the TOE runs on, operates on this operating system and uses the sources of this system through this operating system. This operating system may be one of the following operating system as it is based on MySQL: Windows, Linux. Windows is prefarable.

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. The TOE will use Database built-in timestamp functions.

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

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.. 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
  - ➢ Promedart HIS and LIS Güvenlik Modülü Uygulamaları Desktop Application
    Part 1: ProServis
    Part 2: Trigger

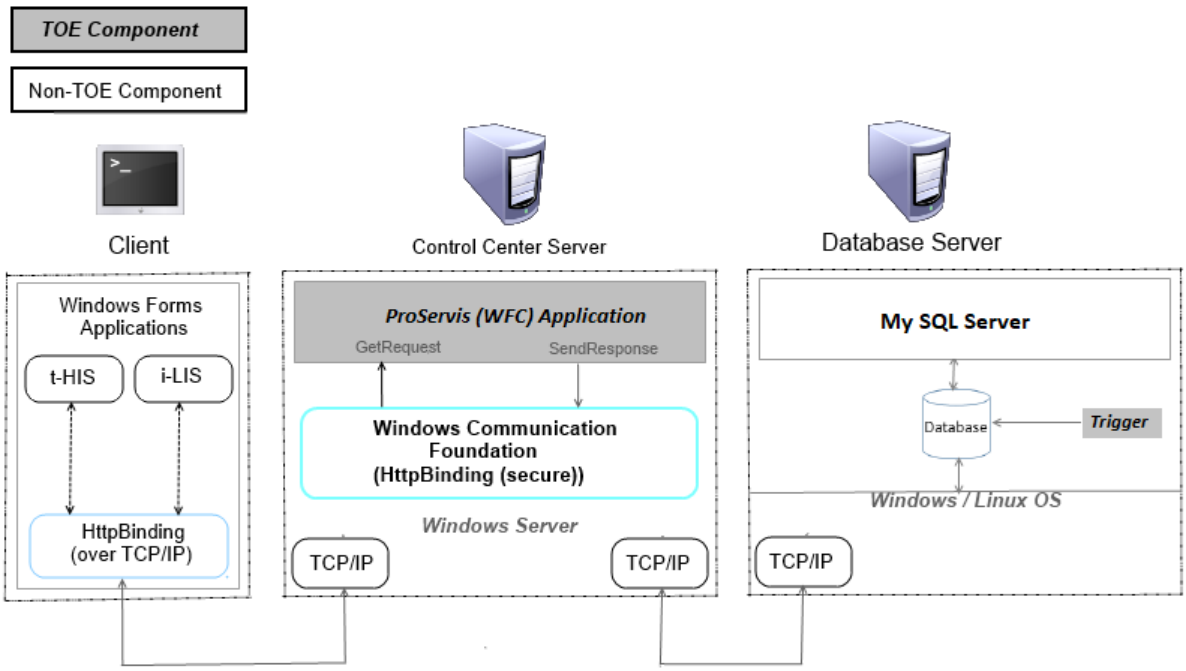

Figure 2 Promedart HIS and LIS Güvenlik Modülü Uygulamaları v1.0.5.14 Application Software

The TOE composed of multiple applications (ProServis and Triggers). And they run as single IT products at Control Center Server. Products are developed as n-tier structure. The Client computers must run with an operating system platform on which the t-HIS or i-LIS executes and Data are stored at database server (Please refer to "Operational Environment Components"). Clients uses TOE via t-HIS or i-LIS for user identitfication and autohorization. Users, Privileges and all data are stored at Database Server and identifications, authorizations and audit trails are performed at database server.

The TOE with applications (t-HIS and/or i-LIS) are delivered to customers with users manuals (t-HIS

User Manual and/or i-LIS User Manual). Applications and Manuals are only delivered electronically and setup files and manuals are stored at customers server. If installation is performed at customer location, files are uploaded by flash disk or by using local network. If installation is performed remotely, files are uploaded by using remote connection tools (VPN, RDP, TeamViewer, AnyDesk).

TOE part 1:Main part of the TOE is ProServis which uses WCF. All database connections and authorization are done through ProServis and there is no direct connection between Clients and Database. Logs are created by ProServis (part 1) and Trigger (part 2). All security functions are executed TOE part 1 and only some audit records are generated in TOE part 2.

1.4.2 Logical Scope of TOE

All users are required to perform identification and authentication before any information flows are permitted. After authorization users can reach only their authorized area and can perform only authorized functions.

The TOE provides a wide range of security management functions. Administrator can manage users identificaitons, rules, roles, security groups access rights. Administrators can assign access privileges to users by user levels based on the functions or resources that they are allowed to perform. Additional functionalities such as modifying access privileges and unlocking or generate password for users are also accessible by administrators.

The TOE provides specifying requirements for TOE security functions and TOE security function policies related to protecting user data.

The TOE generates audit records for security events. The auditor and Administrator roles are allowed to view the audit trail. The TOE protects the protection of its resources not only in the place where it is stored, but also during transmission.

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 and exceeds 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 ProServis server 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 ProServis server and database 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 ProServis 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 ProServis 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: 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_MSA.1: Management of Security Attributes

FMT: Security Management	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

Table 3 Minimum 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.

Application Note: The system administrator is the top level administrator of the TOE. System administrator can read all audit records, like the system auditor.

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: The TOE strictly prevents unauthorized modification of audit records. The TOE does not provide an interface for authorized / unauthorized users to delete or modify

audit records., so unauhorized updates / deletions are not needed to control.

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 [*ignore audited events*] and [**will raise exception / give message to user about 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 of 256 bits]** and cryptographic key sizes [**none**] that meet the following: [**FIPS PUB 180-2].**

6.2.3 User Data Protection

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 [**Promedart Medical Service Manager access control SFP**] on
[
Subjects: end user, system user, system administrator, system auditor.
Objects: Individual Information, Contact Information, Health Information, Authentication Data, Access Control List, AuditData
Operations: Create, Add, Update, Delete/Cancel, View
].

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 [**Promedart Medical Service Manager access control SFP**] to objects based on the following: [

Subjects:

System Administrator, Sytem User, End User, System Auditor

Objects:

Individual Information, Contact Information, Health Information, Authentication Data, Access Control List, AuditData

Subject Attributes:

User Role, Security Group, Security List Group

Object Attributes:

Accessible list of forms / menus and special function lists

Buttons: Add, Update, Cancel / delete choices

Security Group Lists: List of Branches, Stores, Appointment Areas, Surgery Rooms

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

1. **If the operator is associated with a user role or security group that authorizes an operation, then the operation is allowed. Otherwise, the operation is denied or button / menu choice is invisible.**
2. **If a Security List Group's element is specified / choosed, this element's details and contents are accesible and operatable with respect to user role, otherwise these details are denied to user / operator.**

Table 4 Subject-Object-Operation Relationship

Subject	Object	Operation
End User	Individual Information, Contact Information, Health Information Authentication Data	View Update
System User	Individual Information, Contact Information, Health Information Authentication Data	Add, Update, Delete/Cancel, View Update
System Administrator	Authentication Data, Access Control List Audit Data All User's Authentication Data	Create, Add, Update, Delete/Cancel, View View Update
System Auditor	Audit Data Authentication Data	View Update

].

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 within [*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 [**disable the user**].

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 [**Promedart Medical Service Manager access control SFP**] to restrict the ability to [*modify*] the security attributes [**user identification, system configurations, user group and roles, access rights, mapping of users to roles**] 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 [**Promedart Medical Service Manager access control SFP**] to provide [*restictive*] 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:
[
Manage Accounts
Generate Passwords
Lock / Unlock accounts
Define privilege levels
Manange security groups access rights
Manage rules
].

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 5 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 6 SFR 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 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

Table 7 provides an overview for security functional requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen.

Table 7 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 EAL2 was 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

All users credentials (like password) are stored in database with salted hash. When a TOE user change the his/her password or during authentication, salted hashing action do by the TOE. Any user can't enter / use system who doesn't exist in user account tables.
All user login attempts will generate audit logs. Authentication failures will be tracked by a specific table, successful logins will reset counters and each successive failures will set counters. When desired counter is reached user will be set as passive and this user will not enter until it is active and it will get a message "user is passive".

The TOE identify and authenticate all users. Any user can't use the TOE and its resource before these operations.

This Security Function is satisfying the following SFRs;
FCS_COP.1, FIA_AFL.1, FIA_UAU.2, FIA_UID.2,

7.1.2 Access Control

User accounts are stored in database. Each user has their own departments, stores. User's departments and allowable departments, stores, surgery rooms and appointment areas are selected at user definition form, and user can reach only allowed areas.

Access attributes / privilege headers are stored in database. And there are relation between insert, update and delete operation, these operations are not listed separately, they shown as link (checkboxes) at user privilige forms. At these forms priviliges can be determined by system administrator.

Access control rights of all users are defined at the Table 4 Subject-Object-Operation Relationship. In this way, users cannot perform any action other than defined operations.

This Security Function is satisfying the following SFRs;
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; Computer Name on which event was performed; type of event; outcome (success or failure) of the event.

Three different log tables will be used for general purpose logging (above data is based for all tables):

- If SQL statement is successful, SQL statement is logged at first table. Duration of SQL statement execution as milliseconds are stored. So performance of system is also stored.
- If SQL statement is failed, SQL statement is logged at second table.Reason / error message is stored at another column. So all failed SQL statements are logged.

- Any special events related to user (Menu selections, Opening Forms, Button clicks, Grid Clicks, Grid current rows changes, Grid loadings, Generated / produced messages.) are logged. So all user operations are logged.

In addition to general purpose logs, table based logs will be generated by TOE. Timestamp, Computer Name, User name is similar to general purpose logs. These tables names will be start "l" and rest will be same as table name. Log table columns will be same as original tables. TOE generate logs for Modified / changed data (old values) at these tables.

Date and Time values at logs are stored as TimeStamps. Database built-in TimeStamp funcitons are used for this purpose.

The TSF shall ignore audited events and will raise exception / give message to user about failure if the audit trail is full.

The TOE shows 3 kinds of audit logs to System Auditor and System Administrator.

- **User based operations audit logs**. At this form auditor will choose user and time period and will see all operations performed by user during this period.

- **Login attempts audit logs**. Auditor will choose a date, and they will see all Daily login actions (Number of logins and logouts, Failed attempts, successive failed attempts count, user based login logout details).

- **Table based audit logs**. Auditor will choose a table and time period and will see all transactions (modify, delete) performed during this period.

Audit log tables contents generated only by the TOE and there is no point to modify them through TOE. Modification of audit records are prevented by Log Tables Authorization (only inserts can be performed to Log Tables).

This Security Function is satisfying the following SFRs;
FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FAU_STG.4, FPT_STM.1,

7.1.4 Management

User Account Management: System administrator will handle user accounts by using User Account Form. This form allows new user definitions, modifications and make them passive. When a new user is created, the TOE generates random password for user. User's Roles / Security Group assigned here. User and doctors associations shall be done here. Following type of lists that defined in the system shall be shown and administrator will determine to allow them:

- Branches / Departments
- Stores
- Appointment Areas

User / Security Group Privileges: System Administrator will handle user and security group privileges by using this form. The TOE will use user security privileges if priviliges defined by user basely. Otherwise the TOE will use security group privileges for users. All possible security attributes will be listed at this form. Authorization will be given by choosing checkboxes of attributes. If insert Modify and delete/cancel operation is available related to security attribute / privilege, extra checkboxes will be shown respectively, the administrator will be able to set these authorizations too.

When user logins, the TOE will produce security privileges and areas. the TOE will generate / show forms with respect to user definitions and security privileges. Unauthorized functions, forms, menus and buttons will be invisible to user. Empty places (when buttons are made invisible) will be filled by sliding buttons when necessary. Unauthorized brancehes and other areas can not be modified by users. These details are not shown at lists of user's operation area.

HIS & LIS applicaitions running strategy can be different for customers. This is done by using system parameters. Softwares decides working strategy by these parameters values. Some of these parameters are settled at initial setup. And some of them is dynamic and can be changed by only System Administrators. On the other hand, TOE provides restictive default values for security attributes and only system administrator can override default values to manage security attributes.

There are 4 main roles in the TOE and system administrator associates roles with the users. These roles are defined end user, system user, system administrator and system auditor.

This Security Function is satisfying the following SFRs;
FMT_SMF.1, FMT_SMR.1, 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.

This Security Function is satisfying the following SFR;
[FTP_TRP.1]

7.2 Security Enforcing Functions Coverage

Table 8 provides an overview for security enforcing functions coverage also giving an evidence for covarage of the SEFs defined.

Table 8 Security 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
Identificatii/Authentication						X			X	X	X						
Access Control							X	X									
Audit	X	X	X	X	X											X	
Management												X	X	X	X		
Secure Communication																	X