



**SECURITY MODULE of e-Nabız  
PERSONAL HEALTHCARE SYSTEM**

**COMMON CRITERIA SECURITY  
TARGET**

## REVISION HISTORY

<b>DATE</b>	<b>VERSION</b>	<b>AUTHOR</b>	<b>DESCRIPTION</b>
03.09.2018	1.0		First version
12.12.2018	2.0		SFR's are updated
12.01.2020	2.1		SFR's are updated
28.01.2020	2.1.1		Logical scope is updated.
02.02.2020	2.1.2		FDP_ACF.1 SFR is updated.
17.05.2020	2.1.3		Document contents were updated.
10.06.2020	2.1.4		Document contents were updated.
15.07.2020	2.2		Document contents were updated.
10.08.2020	2.3		Document contents were updated.
11.08.2020	2.4		Document contents were updated.
25.08.2020	2.5		Document contents were updated.
25.08.2020	2.6		Document contents were updated.
07.09.2020	2.7		Document contents were updated.
09.09.2020	2.8		Document contents were updated.
17.09.2020	2.9		Document contents were updated.
22.09.2020	2.10		Document contents were updated.
08.10.2020	2.11		Document contents were updated.
19.10.2020	2.12		Document contents were updated.
22.10.2020	2.13		Document contents were updated.
16.11.2020	2.14		Document contents were updated.
24.11.2020	2.15		Document contents were updated.
22.11.2020	2.16		Document contents were updated.
07.01.2021	2.17		Document contents were updated.
08.01.2021	2.18		Document contents were updated.
15.01.2021	2.19		Document contents were updated.
08.03.2021	2.20		Document contents were updated.

Contents

- 1. INTRODUCTION ..... 5
  - 1.1. TOE Overview..... 6
    - 1.1.1. TOE Usage and Major Security Features ..... 6
    - 1.1.2 TOE Type: ..... 8
    - 1.1.3 ST and TOE reference ..... 8
  - 1.2 Firmware/ Hardware/ Software Required by TOE and Firmware/ Hardware/ Software Required by NON-TOE client..... 9
    - 1.3.1. Physical Scope of TOE ..... 10
    - 1.3.2 Logical Scope of TOE..... 12
    - 1.3.3 Delivery Method and Guidance Parts of TOE ..... 14
- 2. CONFORMANCE CLAIM ..... 16
  - 2.1 Common Criteria Conformance Claim..... 16
  - 2.2 PP Conformance Claim ..... 16
  - 2.3 Package Conformance Claim ..... 16
- 3. SECURITY PROBLEM DEFINITION ..... 16
  - 3.1 Threats ..... 16
  - 3.3.Organizational Security Policy ..... 17
  - 3.4.Assumption..... 17
- 4 SECURITY OBJECTIVES ..... 17
  - 4.1.Security objectives of operational environment of TOE ..... 17
  - 4.2.Security Objectives of TOE..... 18
  - 4.3.Rationale for Security Objectives ..... 18
- 5.EXTENDED COMPONENT DEFINITION ..... 20
- 6 SECURITY REQUIRMENT ..... 20
  - 6.1 Conventions and SFR Formatting ..... 20
  - 6.2 Security Functional Requirements..... 21
    - 6.2.1 CIASS FAU: Security Audit ..... 22

6.2.2 CLASS FIA: Identification and Authentication .....	24
6.2.3 CLASS FCS: Cryptographic Operations .....	25
6.2.4 CLASS FTA: TOE Access .....	26
6.2.5 CLASS FTP: Trusted Path.....	28
6.2.6 CLASS FMT: Security Management.....	29
6.2.7 CLASS FDP: User Data Protection .....	29
7 SECURITY REQUIREMENTS RATIONALE.....	33
7.1 SFR Dependency Rationale.....	33
7.2 SFR – Objective Rationale .....	35
7.3 SAR Rationale .....	37
8. TOE SUMMARY SPECIFICATION .....	37
8.1 Security Audit.....	37
8.2 Authentication and Identification .....	38
8.3 Secure Communication.....	38
8.4 Access Control and TOE Access .....	39
8.5 Cryptographic Operations.....	39

# 1. INTRODUCTION

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the Security Module of e-Nabız Personal Healthcare System v2.0 developed by Republic of Turkey, Ministry of Health and will hereafter be referred to as the TOE throughout this document. The TOE is a security module of personnel healthcare system developed and managed by Ministry of Health. TOE provides required security functions of e-Nabız.

This document is divided into eight sections, as follows:

- **Introduction (Section 1):** Provides a brief summary of the document contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- **Conformance Claims (Section 2):** Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- **Security Problem (Section 3):** Describes the threats, threat agents, organizational security policies, and assumptions that pertain to the TOE and its environment.
- **Security Objectives (Section 4):** Identifies the security objectives that are satisfied by the TOE and its environment.
- **Extended Components (Section 5):** Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- **Security Requirements (Section 6):** Presents the SFRs and SARs met by the TOE.
- **Section 7:** describes the TOE security rationale.
- **TOE Summary Specification (Section 8):** a definition of the security functions claimed to meet the functional requirements.

## ***1.1. TOE Overview***

### **1.1.1. TOE Usage and Major Security Features**

e-Nabız is an application that citizens and health professionals access to health data collected from healthcare facilities via internet and mobile devices. Regardless of where examinations and treatments are held, it is a personal health record system where the users can manage all health information and records, and access personal medical background using internet or mobile applications. It is established and managed by Ministry of Health of Turkish Republic. By using the e-Nabız it is possible for the end users to access their health records from any location, independent of the time. Based on those main features e-Nabız increases the quality and speed of the diagnosis and treatment process and establishes a strong communication between the end users and the physicians. The explanation of roles are below:

**End User:** Citizens who access health data collected from healthcare facilities via Internet and mobile devices.

**Physician:** They are healthcare professionals working in secondary care and tertiary care health facilities that enable to access citizens' health data collected from healthcare facilities.

**Family Physician:** They are healthcare professionals working in primary care health facilities that enable to access citizens' health data collected from healthcare facilities.

**Admin:** It is the Ministry of Health employe who monitors and controls citizens' health data over the e-Nabız system within certain authorizations.

By using the e-Nabız system the end users (citizens) may access their past health records (including, laboratory test results, prescription and medicine data, diagnostic results, information that can be needed in emergency case). In order to access the e-Nabız system the users may use their cellular phones, tablet PCs or PCs. In addition to access the system, an end user may also give authorazition to physicians or other other users to access his/her private health records for a time period and bounded authority of his/her choice. The end users may also upload personal health data recorded by themselves.

e-Nabız is a web-based application and it has a web interface that the users use to Access it. The web address of the application is <https://enabiz.gov.tr>. In addition to web interface, a mobile application is developed for the users. e-Nabız application is also integrated with 112 Emergency System, TELEMedicine Services, MERNİS, Core Resource Management System, Central Physician Appointment System, Bone Marrow and Blood Donation System, Drug Information System, MEDULA, Location Information Services and Ministry of Health Central Physician Appointment System.

e-Nabız system processes the personal health data. e-Nabız also has the visualization features that make the data more readable for the end users.

In addition to e-Nabız, e-Nabız application also keep some personal healthcare records. In general the personal healthcare data collected in the healthcare facilities is kept in e-Nabız. The personal healthcare data uploaded by the end users is kept in e-Nabız application's database.

By using the e-Nabız system an end user may perform the following operations:

- Registration (via e-Nabız portal or e-Devlet)
- Displaying his/her user data and healthcare data,
- Sharing his/her personal healthcare data with others,
- Adding/modifying/displaying the his/her healthcare data, (emergency notes, documents, contact information)
- Displaying the his/her own logs,
- Displaying and uploading his/her personal sensor data (blood pressure, blood glucose level, weight, heart rate, count of step, sleep time sensor data only on mobile)

The TOE is the security module of e-Nabız personal health record system that is used to provide necessary security mechanism is in below to the e-Nabız.

**Major security features of TOE are given below:**

- Audit  
Audit TOE generates audit logs and stores in database. End users can view their audit logs through a user interface. Admin can Access to users' log database.
- Identification and Authentication  
Identification and authentication is performed by multiple authentication that is using their TCKN-password, e-signature, mobile signature and e-Devlet login.
- Secure Communication  
TOE uses SSL protocol (https protocol with TLS 1.2) to prevent sniffing and modification of the transmitted data between other components and TOE.

- Access Control Mechanism

TOE provides access control mechanism to users depending on their roles. The users may access the TOE using a web browser or mobile application. If the web application is preferred, the TOE will terminate an inactive session after 20 minutes of inactivation duration (token duration). This duration is 30 days for mobile application. In every activity on the web, the session time is extended by 10 minutes. Briefly, the web time is between 10 and 20 minutes, and also 10 minutes are added to the active time in each activity. For example, if the end user does not do anything after logging in on the web, the session is terminated after 20 minutes. Also, if the end user does something 3 minutes after logging into the web and then does not do anything again, the session will be terminated after 13 minutes, in other words the session will be terminated 13 minutes after login. On the other hand, there is no such situation on mobile.

- Cryptographic Operation

TOE supports cryptographic operation SHA256 to hash user passwords after encrypted by AES.

### 1.1.2 TOE Type:

TOE is a web based module that is used to protect the personal health records of the e-Nabız system. It provides secure communication between the different components of the e-Nabız system and other third party applications, allows auditing, identification and authentication of the users and manages access control mechanisms.

### 1.1.3 ST and TOE reference

ST Reference	Security Module of e-Nabız Kişisel Sağlık Sistemi V.2.0 Security Target
ST Version	V.2.20
TOE Reference	Security Module of e-Nabız Kişisel Sağlık Sistemi
TOE Version	V.2.0



## ***1.2 Firmware/ Hardware/ Software Required by TOE and Firmware/ Hardware/ Software Required by NON-TOE client***

To operate the TOE and NON-TOE properly, required firmware, hardware and software features are given in the following Table-1.

**Table 1-** Firmware/ Hardware/ Software Required by TOE server and- Firmware/ Hardware/ Software Required by NON-TOE client.

<b>Component</b>	<b>Details</b>
Operating System	Windows Server 2012
Web Server	Windows Service
Server Environments	.NET Core 2.0
Browser	All browsers
Database	Couchbase, MSSQL Server, REDIS
Minimum Server Memory Requirements	8 GB
Minimum Server CPU Requirements	4 virtual CPU(2x2)
Anti-virus/Malware Server	Kaspersky Security Center
Minimum Android Version	Lollipop 5.0
Minimum IOS Version	IOS 8.0

The details of those components are given below:

Web server: This web server use CSharp, .Net, Html, Java Script technology.

Operating system: The server that the TOE runs on has a Windows 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: e-Nabız runs on a total of 83 servers, in which 60 of them are physical and 23 of them are virtual servers.

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.

Database: TOE saves all of the user and patient records in MsSQL Server, Redis and Couchbase.

Communicating with other applications: TOE interacts with the other e-Nabız services and backend services of the e-Nabız system. Besides, those services may also interact with the other healthcare services or databases.

Anti-virus/Malware Server: This component is 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. This server helps TOE to prevent sniffing and data corruption attacks.

File Server: File server is a central server instance in a computer network that enables our connected clients to access the server's storage capacities. As long as they have received the corresponding authorizations, accessing users can open, read, change, and delete files and folders on a file server as well as even upload their own files to the server.

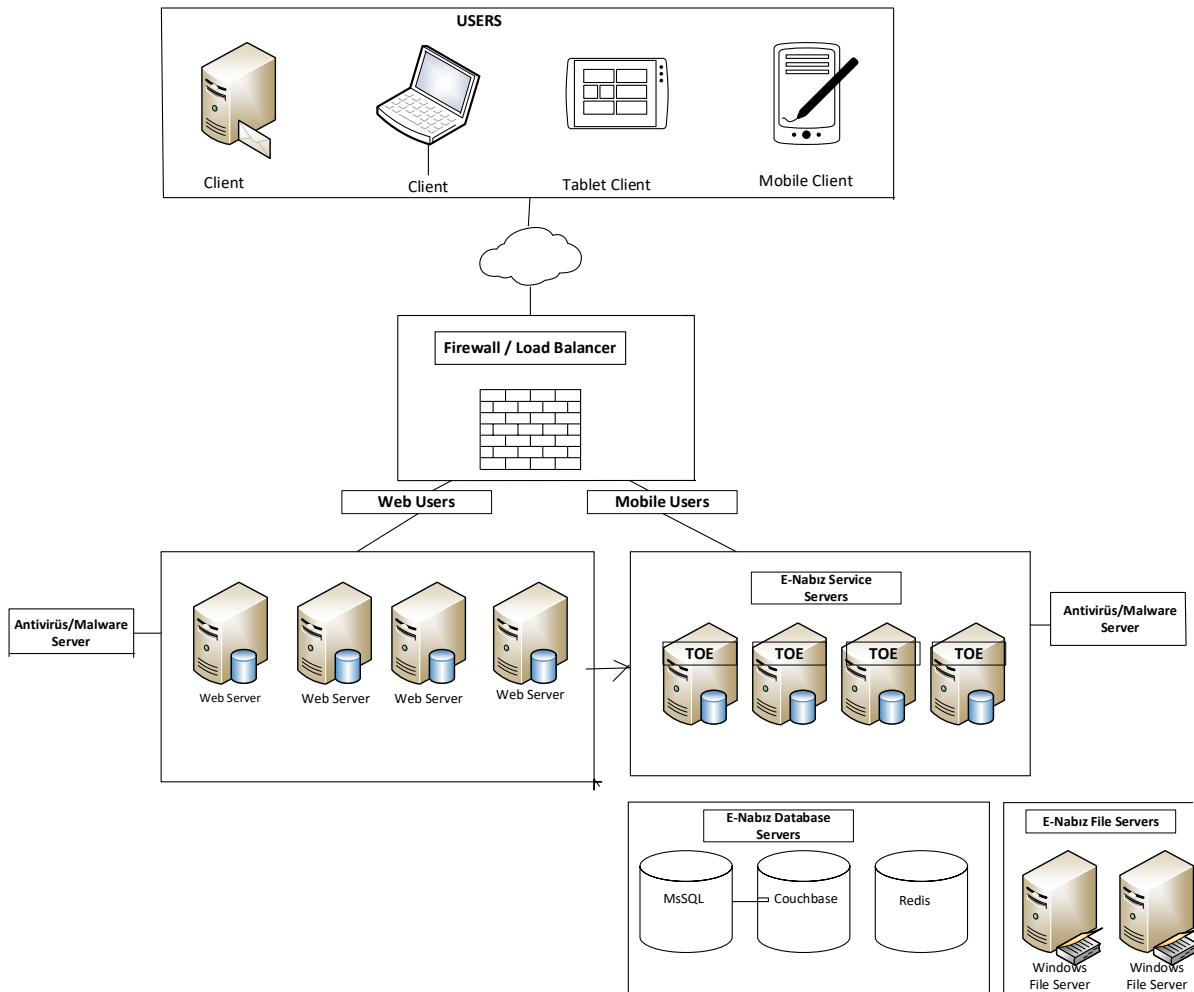
Service Server: The service layer aims at providing middleware that serves third-party value-added services and applications at a higher application layer. For integration, mobile and web application use this Service servers for these purposes. The TOE operates on a service server.

### ***1.3 TOE Description***

#### **1.3.1. Physical Scope of TOE**

TOE is a web based module that is used to protect the personal health records of the e-Nabız system. Since TOE is a web based module, it runs on the web server, as described in Section 1.2.3. So the physical scope of the TOE is not repeated here.

TOE and its scope is represented in Figure 1.



**Figure 1 – TOE and its scope**

End users pass through the firewall and load balancer to access the servers for web or mobile. If the end user wants to log into the web, he / she must first come to the e-Nabiz Web servers. Then, optionally, it accesses appropriate services from e-Nabiz Service servers. If the end user wants to log in on the mobile, he / she can optionally access appropriate services from e-Nabiz Service Servers. Then, appropriate databases are accessed according to the type of data to be accessed or loaded. Responding to end users using web or mobile is done through the services they use. Databases used: Couchbase for NoSQL data type, MsSQL for relational data type, Redis for key-value data type. File servers are also running on two windows servers to keep files received from external sources such as hospitals. Hardware and software requirements are at below:

File Server: Microsoft Windows Server 2012 R2 Standard.  
 Hardware: Virtual Machine 4xCPU,16GB RAM, 600GB DISK

Service Server: Microsoft Windows Server 2016 Standard

Hardware: Virtual Machine 12xCPU,32GB RAM, 200GB DİSK

Database Server: CentOS Linux release 7.8.2003 (Core)

Hardware: 40xCPU,252GB RAM, 3.5TB DİSK

### ***TOE Product Documentation***

The TOE includes the following product documentation:

- e-nabiz User Guidelines: The user guidelines describes the major security features and how to use them securely. The user guidelines also includes the all the functions of the e-nabiz system. The user guidelines is published on the the following web page:  
[https://enabiz.gov.tr/document/KILAVUZ\\_.pdf](https://enabiz.gov.tr/document/KILAVUZ_.pdf)

### **1.3.2 Logical Scope of TOE**

The security functional requirements implemented by the TOE are grouped under the following subtitles:

#### ***Audit***

Audit TOE generates audit logs and stores in database. End User may view their audit logs through a user interface. Admin can access all users' log database. In the audit logs, login of the users name and access type are kept. Also login time of the users are also stored in the audit logs. If a end user authenticates another user to view the healthcare records, and if the authenticated user accesses those records, this is also logged. So end user could monitore reacher to health care data. In this log access method, IP address, access time, numbers of incorrect access, created date, updated date, profile ID, cipher text password, authenticated user, name of the healthcare institution of the authenticated user are logged. The information included in the log records are given below by case basis.

- Login Successfully: Access method, Access time, IP address, Name of the authenticated user
- Login Unsuccessfully: Numbers of incorrect access, Created date, Updated date
- Information of Profile: Profile ID, cipher text Password, Created date,
- View of healthdate: Access method, Access time, IP address, Name of the healthcare institution of the authenticated user.

In each audit record the date and time of the event and subject identity are also kept. Data, creation date and update date of healthcare records are kept. The other informations' creation date and update date are logged. In emergency conditions or according to judicial Orders admins have the right to access and read the end users healthcare data.

### ***TOE Access control/user data protection***

According to the registered user roles, TOE provides rights to the users to access the system and data. An access control list is provided by the TOE to determine which users will access the data. Before the access control, user authentication is required. User authentication approaches are described under the subtitle Identification and authentication. TOE provides access control mechanism to users depending on their roles. TOE also provides necessary means for the termination of active sessions. A session may be terminated by the user. A web initiated session is terminated after between 10 and 20 minutes and a mobile-initiated session is terminated after 30 days. In every activity on the web, the session time is extended by 10 minutes. For example, if the end user does not do anything after logging in on the web, the session is terminated after 20 minutes. Also, if the end user does something 15 minutes after logging into the web and then does not do anything again, the session will be terminated 25 minutes after login. On the other hand, there is no such situation on mobile. TOE also has a mechanism to deny session establishment based on user account status.

### ***Identification and Authentication:***

Identification and authentication is performed by multiple authentication mechanisms for users. An end user may be authenticated by his/her TCKN and password, by e-devlet login or by e-signature or mobile signature login. If the number of unsuccessful authentication attempts reaches 5, then the users are required to enter the Captcha shown to the user. If the number of unsuccessful authentication attempts reaches 10 (with captcha option), that user account is disabled for 24 hours. After 24 hours the user may login the system again, or the user may access the system using the e-devlet authentication without time limitation. The passwords should be composed of at least 10 characters in length and they must include at least two letters. After an accomplished authentication, access rights are provided to the users with regard to predefined user roles. The users are forwarded to e-Nabız system after they are authenticated. The physicians and family physicians can be authenticated by the e-devlet login. The admins are authenticated by Single-Sign On, e-devlet, mobil signature or e-signature.

### ***Secure Communication***

TOE receives data from the users or send private data to the users. Besides TOE requires data transmission between the related healthcare components of the system. In order to provide the integrity of the data transmitted and in order to prevent the disclosure of the data, the TOE uses SSL protocol (https protocol with TLS 1.2) as a secure communication way. TOE uses aforementioned SSL protocol to prevent sniffing, man in the middle attacks and modification of the transmitted data between the TOE and other components (mobile application and browser).

### ***Cryptographic Operations***

TOE supports cryptographic operation SHA256 to hash users' passwords after encrypted by AES to prevent disclosure of the passwords. Key information is generated by hashing a random string of 128 characters using the SHA256 algorithm. Then, using the SHA256 hash algorithm for the value created after AES, a new hash is created. In this way, the password information is encrypted first with AES and then with SHA256.

### **1.3.3 Delivery Method and Guidance Parts of TOE**

TOE is developed and operated inside the Ministry of Health. Source codes are uploaded to TFS. Connection to the servers is made via internal script using username password. Internal script uploads the files that need to be uploaded to the server to the relevant servers over the system. User guidelines describing the how to access and operate the TOE are prepared and published in the web side of the TOE.

### **1.3.4 Users of the TOE and Their Roles**

There are four different user types of the TOE, namely end user, physician, family physician and admin. The user roles of each user are explained below.

***Physician:*** A physician is the personnel that works at the healthcare facilities and examines the end users when they have a health problem. A physician is enrolled to the system by personnel of the Ministry of Health. A physician can log-in to the system by only using the e-Devlet portal. He has the right to read the patient's data according to sharing options' rules.

***Family Physician:*** Family physician is the physician that is assigned to an end user by the Ministry of Health to coordinate healthcare services of that end user. Each end user has an assigned a family physician. Family physician has the same rights with the physician. In addition to that a family physician may enroll an end user to the e-Nabiz system who hasn't enrolled to the system yet. In this enrollment process a disposable access code is sent to the

end user's mobile phone to get the confirmation of the enrollment. If end user confirms the enrollment, then the enrollment is completed. The enrollment process is out of the scope of the TOE.

**Admin:** An admin is a personnel working in Ministry of Health and he is responsible for managing the TOE. He usually performs unusual operations that can not be performed by the family physicians, physicians or end users. Admin can access to users' log database. Those operations are explained below:

System data update: If there is a need to update system data; that data is updated by the admin. In addition to update, an admin also has the right to add system data.

Accessing statistical data: Admins may access the statistical data of TOE.

Accessing end user data: In emergency conditions or according to judicial Orders admins have the right to access and read the end users healthcare data.

Accessing family physicians and physicians data: In emergency conditions admins have the right to access and read the family physicians' and physicians' data (contact informations and informations in core resource management system).

**End User:** An end user is a person who gets services from healthcare facilities and who has private data stored in healthcare databases. In this respect it is natural that the end user may access and read his/her own data. In addition to that an end user may perform the following operations on TOE:

Changing family physician: a family physician is assigned to each end user by the Ministry of Health. The end user may change his/her family physician using the TOE.

Sharing the personal healthcare data: The end user may share his/her personal data with physicians or with other end users, for a limited time period. This operation is performed using the "Share" button of the TOE. The end user may share all of his/her data, or the end user may share a selected group of his/her data.

Adding emergency case notes: The end user may add emergency notes to his/her profile that will be followed by the healthcare personnel in case of any emergency.

Adding, modifying and displaying document: The end user may add healthcare related documents (images of injuries, medical imaging outputs) to the system.

Getting appointment from physicians: The end user may get appointment from physicians. The end user may also get appointment for his/her children. Besides the end user may cancel the appointment using the e-Nabız.

Adding medicine reminder: The end user may add a reminder to the system that will inform the end user when the time to get medicine is approaching.

## **2. CONFORMANCE CLAIM**

### ***2.1 Common Criteria Conformance Claim***

This Security Target claims to be conformant to the Common Criteria 3.1 Revision 5 (April 2017). In order to provide a complete description of the functional requirements addressed by the TOE, functional components of Part 2 of the Common Criteria framework were used. For the description of the requirements due to the trustworthiness of the TOE, only security assurance requirements of CC part 3 were used.

### ***2.2 PP Conformance Claim***

This security target has no claim to any protection profile.

### ***2.3 Package Conformance Claim***

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

## **3. SECURITY PROBLEM DEFINITION**

### ***3.1 Threats***

- **T.DDOS:** An attacker may attempt to make service unavailable by overwhelming it with traffic from multiple sources .
- **T.Brute:** An attacker may repeatedly try to guess authentication data in order to attack TOE by using this information.
- **T.Comm:** An attacker may try to modify the data transmitted between the TOE and other components.



- **T.Password:** An attacker may gain access to the passwords in the database and authenticate to the TOE by using this passwords.
- **T.Access:** An unauthorized person may gain access to resources for which that user is not authorized.
- **T. Masquerade:** An unauthorized user may masquerade via privilege escalation as an authorized user to gain access to data or TOE resources.

### ***3.2 Treat Agents***

**Attackers:** Attackers have knowledge of how the TOE operates and they are assumed to have a basic skill level, and intend to alter TOE configuration settings/parameters.

**Limited User:** Limited user has limited authorisation for viewing and performing.

### ***3.3.Organizational Security Policy***

There is no Organizational Security Policy.

### ***3.4.Assumption***

- **A. Timestamp:**The reliable timestamp is provided in the TOE operation environment.
- **A.Healthcare\_Personnel:** It is assumed that admins, physicians and family physicians are educated and trained to use the TOE securely and will not share patients' records with other users.
- **A.Single\_User:** It assumed that the application is used physically securely by the end user on a single mobile device.

## **4 SECURITY OBJECTIVES**

### ***4.1.Security objectives of operational environment of TOE***

- **OE.Timestamp:** The TOE environment must provide reliable timestamps to the TOE.
- **OE. Healthcare\_Personnel:** It is provided that admins, physicians and family physicians are educated and trained to use the TOE securely and do not share patients' record with other users.
- **OE.SCE:** Operational environment of the TOE shall provide a secure communication environment by using firewall.
- **OE.Single\_User:** The application is used physically securely by the end user on a single mobile device.

#### ***4.2.Security Objectives of TOE***

- **O.Cipher:** TOE ensures that passwords stored in the database are hashed after encrypting.
- **O.Comm:** The TOE must ensure that user data going across the components is protected against disclosure. Besides the integrity of the data should be preserved by the TOE.
- **O.Audit:** TOE will provide the capability to create audit records of security relevant events associated with users and allow capability to review audit information.
- **O.Password:** Passwords used in the TOE will be strong enough to resist most brute force attacks and it will limit the number of unsuccessful authentication attempts in order to protect data.
- **O.Access:** The TOE must ensure that only authorized users are able to access protected resources or functions. Besides TOE also has the secure session termination procedures that will be applied after a session is established. TOE also has the functionalities that can be used to re-activate the account, if the user account is blocked because of the unsuccessful access attempts.
- **O.Auth:** 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.

#### ***4.3.Rationale for Security Objectives***

The relationship between the treats, assumptions and security objectives are given in Table 2.

**Table 2** – Relationship between the treats, assumptions and security objectives

	Threats						Assumptions		
	T.DDOS	T.Brute	T.Comm	T.Password	T.Masquera	T.Access	A.Healthcar e_Personnel	A.Timestam	A.Single_Us er
O.Cipher				x					
O.Comm			x						
O.Audit						x			
O.Password		x							
O.Access						x			
O.Auth					x	x			
OE.Timestamp								x	
OE.Healthcare_Pers onnel							x		
OE.SCE	x								
OE.Single_User									x

**T.DDOS:** *OE.SCE* allows the communication network of the TOE to provide a secure communication environment and by using a firewall it that makes the denial of service attack ineffective.

**T.Brute:** *O.Password* requires the TOE users to get strong passwords which are hard to guess. Besides it will limit the number of unsuccessful authentication attempts in order to prevent brute force attacks.

**T.Comm:** *O.Comm* objective ensures that all user data from the user to the web server will be secured using SSL(https protocol with TLS 1.2), protecting the user data from unauthorized disclosure and loss of integrity. Besides TOE uses secure communication with other components of the e-nabiz system and other third party applications.

**T.Password:** *O.Cipher* objective provides the ciphered text 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 cipher text.

**T.Masquerade :** *O.Auth* objective ensures that each user of the TOE will be successfully authenticated before any actions.

**T.Access:** *O.Access* objective ensures that the TOE restricts access to the TOE objects to the authorized users. *O.Auth* objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions. *O.Audit* objective provides functionality to users of TOE to review their audit logs. By reviewing the audit logs it is possible to detect unauthorized past access to the system.

**A.Healthcare\_Personnel:** *OE.Healthcare\_Personnel* objective ensures that physicians, family physicians and admins are trained so that they use the TOE securely and will not share patient health record with other users.

**A.Timestamp:** *OE.Timestamp* objective ensures that the operational environment will provide reliable timestamps to the TOE and by using the reliable time information it will be possible to generate reliable audit logs.

**A.Single\_User:** *OE.Single\_User* enables the application to be used physically safe by the end user on a single mobile device.

## **5.EXTENDED COMPONENT DEFINITION**

There is no extended component in this Security Target.

## **6 SECURITY REQUIRMENT**

### ***6.1 Conventions and 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*].
- Iteration: The iteration operation allows to iterate a security function for different operations and is applied as /IDENTIFIER.
- Refinement: The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using **bolded text**, for additions and for deletions.

## 6.2 Security Functional Requirements

This section specifies the SFRs for the TOE, organized by CC class. Table 3 identifies all SFRs implemented by the TOE.

**Table 3** - Security Functional Requirements implemented by the TOE

CLASS HEADING	CLASS FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1/ Admin Audit review	Audit Review
	FAU_SAR.1/ End User Audit review	Audit Review
Identification and Authentication	FIA_UID.2	User Identification before any action
	FIA_UAU.2	User authentication before any action
	FIA_AFL.1/CAPTCHA	Authentication failure handling
	FIA_AFL.1/BLOCK	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UAU.5	Multiple authentication mechanism
TOE Access	FTA_TSE.1	TOE session establishment
	FTA_SSL.3/WEB Initial	TSF-Initiated termination
	FTA_SSL.3/WEB Active Session	TSF-Initiated termination
	FTA_SSL.3/MOBILE	TSF-Initiated termination
	FTA_SSL.4	User-initiated termination

Cryptographic Operations	FCS_COP.1/SHA256	Cryptographic operations
	FCS_COP.1/AES	Cryptographic operations
	FCS_CKM.1	Cryptographic Key Generation
Trusted Path	FTP_TRP.1	Trusted path
	FTP_ITC.1	Inter-TSF trusted channel
Security Management	FMT_SMR.1	Security roles
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control

## 6.2.1 CIASS FAU: Security Audit

### 6.2.1.1 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 [*not specified*] level of audit; and
- c) [**successful and unsuccessful authentication attempts, healthcare data viewed by the authenticated users, data with creation date and update date of healthcare records, others kept creation date and update date without data**].

**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, [**Access method, IP address, access time, name of the authenticated user, numbers of incorrect access, created date, updated date, profile ID, hashed**

**ciphered password, access method, access time, authenticated user, name of the healthcare institution of the authenticated user].**

Application Note:

- Login Successfully: Access method, Access time, IP address, name of the authenticated user
- Login Unsuccessfully: Numbers of incorrect access, Created date, Updated date
- Information of Profile: Profile ID, Ciphered Password, Created date, View of healthdate: Access method, Access time, IP address, authenticated user, name of the healthcare institution of the authenticated user.

#### **6.2.1.2 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.

#### **6.2.1.3 FAU\_SAR.1/End User Audit review**

Hierarchical to: No other components.

Dependencies: FAU\_GEN.1 Audit data generation

**FAU\_SAR.1.1** The TSF shall provide [**end user**] with the capability to read [**his/her own audit record and who has viewed his/her healthcare data**] from the audit records.

**FAU\_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

#### **6.2.1.4 FAU\_SAR.1/Admin Audit review**

Hierarchical to: No other components.

Dependencies: FAU\_GEN.1 Audit data generation

**FAU\_SAR.1.1** The TSF shall provide [**admin**] with the capability to read [**end user's audit record and other users' log details**] 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.

## 6.2.2 CIASS FIA: Identification and Authentication

### 6.2.2.1 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.

### 6.2.2.2 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.

### 6.2.2.3 FIA\_AFL.1/CAPTCHA Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA\_UAU.1 Timing of authentication

**FIA\_AFL.1.1** The TSF shall detect when [*5*] unsuccessful authentication attempts occur related to **[login attempt]**.

**FIA\_AFL.1.2** When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall **[create captcha]**.

### 6.2.2.4 FIA\_AFL.1/BLOCK Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA\_UAU.1 Timing of authentication

**FIA\_AFL.1.1** The TSF shall detect when [*10*] unsuccessful authentication attempts occur related to **[login attempt]**.

**FIA\_AFL.1.2** When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall **[block user account for 24 hours]**.

**Application Note:** When the number of unsuccessful login attempts reaches 5, the TOE creates a Captcha in order to prevent automatic login attempts. In this case the user is required to enter Captcha in addition to user identity and password. If the unsuccessful login attempts reaches 10 with Captcha, the user account is blocked for 24 hours. But the user may still use e-devlet



authentication and if he/she successfully logs in to the TOE via e-Devlet login, then his/her account is unblocked.

#### **6.2.2.4 FIA\_SOS.1 Verification of secrets**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA\_SOS.1.1** The TSF shall provide a mechanism to verify that secrets meet [ **the following rules:**

- **Passwords must be at least 10 characters in length,**
- **Passwords must contain at least 2 letters].**

#### **6.2.2.5 FIA\_UAU.5 Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA\_UAU.5.1** The TSF shall provide [**Single-Sign-On, e-Devlet login, TCKN-password, e-signature, mobile signature**] to support user authentication.

**FIA\_UAU.5.2** The TSF shall authenticate any user's claimed identity according to the [**the following rules:**

- **End users may be authenticated by e-Devlet login, TCKN-password, e-signature or mobile signature authentication mechanism.**
- **Admins may be authenticated by Single-Sign-On, e-Devlet login, e-signature or mobile signature authentication mechanism.**
- **Family physicians and physicians can only use e-Devlet authentication mechanism for authentication].**

### **6.2.3 CLASS FCS: Cryptographic Operations**

#### **6.2.3.1 FCS\_COP.1/SHA256 Cryptographic Operation (Hash Algorithm)**

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/SHA256** The TSF shall perform **[hashing]** in accordance with a specified cryptographic algorithm **[SHA-256]** and cryptographic key sizes **[none]** that meet the following: **[FIPS PUB 180-2]**.

### **6.2.3.2 FCS.COP.1/AES Cryptographic Operation (Keyed Hash Algorithm)**

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/AES** The TSF shall perform **[encrypting]** in accordance with a specified cryptographic algorithm **[AES]** and cryptographic key sizes **[256 bits]** that meet the following: **[FIPS PUB 197]**.

### **6.2.3.3 FCS\_CKM.1 Cryptographic key generation**

Hierarchical to: No other components.

Dependencies: [FCS\_CKM.2 Cryptographic key distribution, or

FCS\_COP.1 Cryptographic operation]

FCS\_CKM.4 Cryptographic key destruction

**FCS\_CKM.1.1** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[hashing a random value]** and specified cryptographic key sizes **[256 bits]** that meet the following: **[none]**.

## **6.2.4 CLASS FTA: TOE Access**

### **6.2.4.1 FTA\_TSE.1 TOE session establishment**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FTA\_TSE.1.1** The TSF shall be able to deny session establishment based on **[user account status]**.

**Application Note:** The user's account can be blocked based on the number of unsuccessful authentication mechanisms. If the user's account is blocked, then the TOE will deny session establishment. But if the user uses e-Devlet authentication mechanisms and successfully logs in to the TOE, then his/her account will be unblocked.

#### **6.2.4.2 FTA\_SSL.3/ WEB TSF-initiated termination/ Initial**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FTA\_SSL.3.1** The TSF shall terminate an interactive session after a **[20 min.]**.

#### **6.2.4.3 FTA\_SSL.3/ WEB TSF-initiated termination/Active Session**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FTA\_SSL.3.1** The TSF shall terminate an interactive session after a **[10 min.]**.

**Application Note:** Whenever a web-based session is initiated, that session will be terminated after 20 minutes of inactivation by default. If the user performs an operation during the session, the time interval of user inactivity is set to 10 minutes.

#### **6.2.4.4 FTA\_SSL.3/ MOBILE TSF-initiated termination**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FTA\_SSL.3.1** The TSF shall terminate an interactive session after a **[30 days.]**

**Application Note:** The end user may use mobile application to access the TOE. In the first session establishment the end user is asked to mark "remind me" option by the mobile application. If this option is marked, then the interactive session will be active for 1 month.

#### **6.2.4.4 FTA\_SSL.4 User-initiated termination**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FTA\_SSL.4.1** The TSF shall allow user-initiated termination of the user's own interactive session.

## **6.2.5 CLASS FTP: Trusted Path**

### **6.2.5.1 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]*.

### **6.2.5.2 FTP\_ITC.1 Inter-TSF trusted channel**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FTP\_ITC.1.1** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP\_ITC.1.2** The TSF shall permit *[the TSF]*, **and** *[another trusted IT product]* to initiate communication via the trusted channel.

**FTP\_ITC.1.3** The TSF shall initiate communication via the trusted channel for **[e-Government, Identity Sharing System and Short Message Service Entegrations, Ministry of Health Systems 112 Emergency System, TELEMedicine Services, MERNIS, Core Resource Management System, Central Physician Appointment System, Bone Marrow and Blood Donation System, Drug Information System, MEDULA,**

**Location Information Services and Ministry of Health Central  
Physician Appointment System].**

**6.2.6 CLASS FMT: Security Management**

**6.2.6.1 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 [**admin, physician, family physician, end user**].

**FMT\_SMR.1.2** The TSF shall be able to associate users with roles.

**6.2.7 CLASS FDP: User Data Protection**

**6.2.7.1 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 [**Access control SFP**] on [

**Subjects:**

- **Admin**
- **Physician**
- **Family Physician**
- **End User**

**Objects:**

- **User data**
- **Healthcare data**
- **System data**
- **Audit data**
- **Statistical data**

**Operations:**

- **Read,**
- **Update,**
- **Add**
- **Share].**

**6.2.7.2 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 initialisation

**FDP\_ACF.1.1** The TSF shall enforce the [**Access control SFP**] to objects based on the following:

**Subjects:**

- **Admin**
- **Physician**
- **Family Physician**
- **End User**

**Subject Attributes:**

- **User identity**
- **Status**

**Objects:**

- **User data**
- **Healthcare data**
- **System data**
- **Audit data**
- **Statistical data**


**Object Attributes:**

- **User identity**
- **Object Id**

**FDP\_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Table 4 – Default User Roles].

**Table 4 - Default User Roles**

	USER DATA				HEALTHCARE				SYSTEM DATA				AUDIT DATA				STATISTICAL DATA							
	Account Data		Users		Healthcare Data (*)				System Data				Audit Logs of his/her own data (**)				Statistical Data of Users							
	R	A	U	S	R	A	U	S	R	A	U	S	R	A	U	S	R	A	U	S				
End User	X	X	X						X	X	X	X					X							
Physician									X															
Family Physician						X			X															
Admin					X		X						X	X			X				X			

 **R:** Read – **A:** Add – **U:** Update – **S:** Share

\*End User can add specific health care data which are allergies, emergency notes, documents and medicine reminders. Physician and Family Physician can access to the End User’s healthcare data if the End User permitted.

\*\* End users can view their audit logs through a user interface. Admin can access to users’ log database.

**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].

### 6.3 Security Assurance Requirements (SAR)

The TOE meets the security assurance requirements for EAL2. The following Table 5 is the summary for the requirements.

**Table 5 - Security Assurance Requirements**

Assurance Class	Assurance Components
<b>ADV: Development</b>	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
<b>AGD: Guidance documents</b>	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
<b>ALC: Life-cycle support</b>	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
<b>ASE: Security Target evaluation</b>	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
<b>ATE: Tests</b>	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
<b>AVA: Vulnerability Assessment</b>	AVA_VAN.2 Vulnerability analysis



## 7 SECURITY REQUIREMENTS RATIONALE

### 7.1 SFR Dependency Rationale

The Table 6 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	Although FPT_STM.1 is not included, the TOE Environment provides reliable timestamps to the TOE. That assumption states that the TOE will receive reliable timestamps, thereby satisfying this dependency.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	YES YES (FIA_UID.2 is hierarchical to FIA_UID.1)
FAU_SAR.1 / End User	FAU_GEN.1	YES
FAU_SAR.1 / Admin	FAU_GEN.1	YES
FCS_COP.1/SHA256	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	SHA256 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.
FCS_COP.1/AES	FCS_CKM.1, FCS_CKM.4	YES.  The AES key is physically stored in a safe place. For this reason, it is not destroyed.

<b>FCS_CKM.1</b>	FCS_COP.1  FCS_CKM.4	YES (FCS_COP.1/AES)  The AES key is physically stored in a safe place. For this reason, it is not destroyed.
<b>FDP_ACC.1</b>	FDP_ACF.1	YES
<b>FDP_ACF.1</b>	FDP_ACC.1 FMT_MSA.3	YES NO (FMT_MSA3- Management not allowed for the security attributes specified in FDP_ACF.1 )
<b>FIA_UID.2</b>	-	-
<b>FIA_UAU.2</b>	FIA_UID.1	YES (FIA_UID.2 is hierarchical to FIA_UID.1)
<b>FIA_UAU.5</b>	-	-
<b>FIA_AFL.1/CAPTCHA</b>	FIA_UAU.1	YES (FIA_UAU.2 is hierarchical to FIA_UAU.1)
<b>FIA_AFL.1/Block</b>	FIA_UAU.1	YES (FIA_UAU.2 is hierarchical to FIA_UAU.1)
<b>FIA_SOS.1</b>	-	-
<b>FMT_SMR.1</b>	FIA_UID.1	YES (FIA_UID.2 is hierarchical to FIA_UID.1)
<b>FTA.TSE.1</b>	-	-
<b>FTA_SSL.3/WEB Initial</b>	-	-
<b>FTA_SSL.3/WEB Active Session</b>	-	-
<b>FTA_SSL.3/Mobile</b>	-	-
<b>FTA_SSL.4</b>	-	-

<b>FTP_TRP.1</b>	-	-
<b>FTP_ITC.1</b>	-	-

## 7.2 SFR – Objective Rationale

The relationship between the objectives and SFRs are given in Table 7.

**Table 7 – SFR-Objective Rationale**

	<b>O.Au th</b>	<b>O.Acce ss</b>	<b>O.Passwor d</b>	<b>O.Comm</b>	<b>O.Audit</b>	<b>O.Cipher</b>
<b>FAU_GEN.1</b>					X	
<b>FAU_GEN.2</b>					X	
<b>FAU_SAR.1 / End User</b>					X	
<b>FAU_SAR.1 / Admin</b>					X	
<b>FCS_COP.1/SHA256</b>						X
<b>FCS_COP.1/AES</b>						X
<b>FCS_CKM.1</b>						X
<b>FDP_ACC.1</b>		X				
<b>FDP_ACF.1</b>		X				
<b>FIA_UID.2</b>	X					
<b>FIA_UAU.2</b>	X					
<b>FIA_UAU.5</b>	X					
<b>FIA_AFL.1/Captcha</b>			X			

<b>FIA_AFL.1/Block</b>			X			
<b>FIA_SOS.1</b>			X			
<b>FMT_SMR.1</b>		X				
<b>FTA.TSE.1</b>		X				
<b>FTA_SSL.3/Web Initial</b>		X				
<b>FTA_SSL.3/Web Active Session</b>		X				
<b>FTA_SSL.3/Mobile</b>		X				
<b>FTA_SSL.4</b>		X				
<b>FTP_TRP.1</b>				X		
<b>FTP_ITC.1</b>				X		

**O.Auth:** 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. FIA\_UAU.5 meets the objective by ensuring that the user can login to the application by multiple authentication methods.

**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. FMT\_SMR.1 manages 4 roles (Admin, Physician, Family Physician and End User). Besides FTA\_SSL.3/WEB Initial and FTA\_SSL.3/WEB Active Session, FTA\_SSL.3/Mobile and FTA\_SSL.4 SFRs provide secure session termination procedures. In addition to this FTA\_TSE.1 defines the procedures that can be used to deny session establishment based on user account status.

**O.Password:** FIA\_SOS.1 outlines a quality metric for passwords. FIA\_AFL.1/Captcha and FIA\_AFL.1/Block defines values for number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures.

**O.Audit:** FAU\_GEN.1 generates audit logs. FAU\_GEN.2 is used to associate auditable events to the users. FAU\_SAR.1/End User and FAU\_SAR.1/Admin provides that the audit information can be viewed by the users.

**O.Cipher:** This objective ensures that the user passwords are stored in the database as cipher text passwords. FCS\_COP.1/SHA256, FCS\_COP.1/AES and FCS\_CKM.1 encounters this objective by defining necessary cryptographic operations (SHA256 and AES are used for cryptographic operation).

**O.Comm:** FTP\_TRP.1 helps to meet the objective by establishing an SSL Secure channel from the user's browser to e-Nabiz application protecting the user data from disclosure and modification. Besides FTP\_ITC.1 provides secure communication between the TOE and other components of the e-nabiz system and other third party applications.

### ***7.3 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.

## **8. TOE SUMMARY SPECIFICATION**

This section provides the TOE summary specification, a definition of the security functions claimed to meet the functional requirements.

### ***8.1 Security Audit***

The TOE generates audit logs of successful and start-up and shut down of the audit functions and data view performed by the authenticated users. Moreover, it associates each auditable event with the identity of the user that caused the event and for each auditable event it keeps the data and time of the event, type of the event, and outcome (success or failure) of the event. The TOE provides the capability for all users to read and view his/her own audit record. Admin can Access to end users' log database. In the audit logs the access method, IP address, access time, name of the authenticated user, numbers of incorrect access, created date, updated date, profile ID, ciphered password, name of the healthcare institution of the authenticated user are

also kept. Data, creation date and update date of healthcare records are kept. The information included in the log records are given below by case basis.

- Login Successfully: Access method, Access time, IP address, name of the authenticated user
- Login Unsuccessfully: Numbers of incorrect access, Created date, Updated date
- Information of Profile: Profile ID, Ciphered Password, Created date,
- View of healthdate: Access method, Access time, IP address, name of the healthcare institution of the authenticated user.

The other informations' creation date and update date are logged. In emergency conditions or according to judicial Orders admins have the right to access and read the end users healthcare data.

TOE Security Functional Requirements Satisfied: FAU\_GEN.1, FAU\_GEN.2, FAU\_SAR.1/End User, FAU\_SAR.1/Admin.

## ***8.2 Authentication and Identification***

TOE supports multiple authentication mechanism, that is, authentication of users based on Single-Sign On, TCKN-passwords combinations, e-devlet login and e-signature or mobile signature. Before successful completion of the security function, an user is unable to perform any actions. Once identified and authenticated, the users are able to access the functions or resources available to their roles. TOE maintains 4 roles which are end user, physician, family physician and admin. Passwords are enforced to meet a sufficient amount of complexity. If 5 unsuccessful authentication attempts occur, TOE creates Captcha and if 10 unsuccessful authentication attempts occur after the Captcha is created, then TOE disables the user account for 24 hours for end user authentication. However, user can login to the sytem by e-Devlet login without waiting for 24 hours. In this case user account is automatically unblocked.

TOE Security Functional Requirements Satisfied: FIA\_AFL.1/Captcha, FIA\_AFL.1/Block, FIA\_SOS.1, FIA\_UID.2, FIA\_UAU.2, FIA\_UAU.5, FMT\_SMR.1

## ***8.3 Secure Communication***

TOE needs to communicate with other components databases and user's browsers. Those communications should be done in a secure way, using the SSL protocol (https protocol with TLS 1.2) to protect data traversing across the internet from/to the application from modification

and disclosure. Besides TOE uses secure communication with other components of the e-nabiz system and other third party applications.

Functional Requirement Satisfied: FTP\_TRP.1 and FTP\_ITC.1

#### ***8.4 Access Control and TOE Access***

TOE supports 4 different user types (namely end user, physician, family physician and admin) and their access rights are well-defined. Three of TOE users are healthcare professionals and they are well trained and trusted users. The end users get services from the healthcare facilities. The end user may access his/her own account and update the account, add sensor data or document to the system, read his/her personal healthcare data, give access right of his/her personal healthcare data to others, and read the audit logs of his/her account.

Physicians are the doctors that examines the end user. Physicians may read the end user data if it is allowed by the end user or if the physician examined the end user.

Family physicians are the doctors assigned to each end user by the Ministry of Health to coordinate the end user's healthcare activities. Family physicians have the same rights with the physicians.

Admins are responsible to manage the TOE and they have the rights to read the statistical data from the TOE. That statistical data includes number of users, number of physicians, number of family physicians.

TOE also has the TOE access and session control mechanisms. The TOE deny session establishment based on user account status. After between 10 and 20 minutes, inactive sessions are automatically logged out and returned to the login page on web e-Nabiz application. After 30 days inactive sessions are automatically logged out and returned to the login page on mobile e-Nabiz application. In every activity on the web, the session time is extended by 10 minutes. On the other hand, there is no such situation on mobile. There is a "remind me" option in the mobile application and if this options is checked, then session is terminated automatically after 1 month. The TOE also allows user-initiated termination of the user's own interactive session.

Functional Requirement Satisfied: FDP\_ACC.1, FDP\_ACF.1, FTA\_TSE.1, FTA\_SSL.3/WEB Initial, FTA\_SSL.3/WEB Active Session FTA\_SSL.3/Mobile and FTA\_SSL.4.

#### ***8.5 Cryptographic Operations***

TOE uses cryptographic operations in order to keep the user passwords. By this way TOE protects the users' password from disclosure. TOE uses SHA256 and AES algorithm and it keeps the passwords encrypted and hashed in the database. Key information is generated by

hashing a random string of 128 characters using the SHA256 algorithm. Then, using the SHA256 hash algorithm for the value created after AES, a new hash is created. In this way, the password information is encrypted first with AES and then with SHA256.

TOE Security Functional Requirements Satisfied: FCS.COP.1/SHA256, FCS.COP.1/AES, FCS\_CKM.1