SISOFT HEALTHCARE INFORMATION SYSTEMS

SİSOFT SAĞLIK BİLGİ SİSTEMLERİ

SOFTWARE RESEARCH and DEVELOPMENT

Common Criteria: EAL2+(ALC_FLR.1)

Sisoft WEBHBYS Version 2.0.0.3
16-JULY-13

Document management

Document identification

Document ID	Sisoft WEBHBYS _EAL2_ST
Document title	Sisoft WEBHBYS Security Target
Document date/version	1.9, 16-JULY-13

Document History

Version	Date	**Description**
0.1	16-AUG-11	Released for internal review
0.2	19-AUG-11	Updated to address internal comments
0.3	06-SEP-11	Updated to reflect the scope of the TOE.
1.0	15-SEP-11	Updated to address EORs.
1.1	13-NOV-11	Updated from draft ETR
1.2	24-NOV-11	Updated to address EORs
1.3	01-DEC-11	Updated to address changes for Product Version
1.4	18-OCT-12	ST-document update
1.5	12-NOV-12	ST-document update
1.6	03-DEC-12	ST-document update
1.7	08-JUNE-13	Updated to reply Onbservation Report 4
1.8	09-JULY-13	Updated according to mismatches with interface document
1.9	16-JULY-13	Updated according to mismatches with design document

Table of Contents

1 Security Target introduction (ASE_INT.1)

1.1 ST reference

ST Title	Sisoft WebHBYS of Security Target
ST Identifier	Sisoft WEBHBYS Version 2.0.0.3
ST Version/Date	1.9 (16-JULY-13)

1.2 TOE reference

TOE Title	Sisoft WEBHBYS
TOE Version	2.0.0.3

1.3 Document organisation

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 TOE overview

1.4.1 TOE usage and major security functions

- Provide access to application-oriented access to external systems in environments where information is stored as encrypted. Managing the authority assigned to SisoftWebHBYS application, rule-based application-oriented access controls can significantly mitigate the threats posed by malicious code due to software vulnerabilities.
- SHA-2 checksum verification to ensure the integrity of releases are published values. These subprograms generate SHA-2 hashes of data. The SHA-2 algorithm ensures data integrity by generating a 128-bit cryptographic message digest value from given data confidence in the oracle.
- Version to update the license informationare tracked by individual users, version of the update process details are recorded. Version updates is based on the feedbacks from our customers and the Republic of Turkey Ministry of Health. Each customer is determined by the license code number and password. In addition, ethernet and mac id is taken from customer application server.
- The SisoftWebHBYS application has the ability to work with SSL. Users have the optionto log on with the application of qualified electronic signatures. Electronic data are used for the purpose of any change or modification. Qualified electronic certificates X.509 standards that meet this standard are produced and web browsers, smart cards and tokens that respect and are supported by SisoftWebHBYS.
- Powers of access and operation by the user control is provided on the basis of the definitions. SisoftWebHBYS contained in user and group definitions section for making authority, which authority will be determined user. This authorization can only be perform by administrator.
- The activity does not present a specific period of time the application automatically terminated user sessions. If the user is authenticated, the server then verifies that the user has the privilege to access the requested page against a file. If the user has access, the Web server then serves the page. If the user is denied access, the server either requests the username/password combination again or presents an error message on the browser window. Sisoft WEBHBYS application user input incorrectly three times for 15 minutes in appreciation of his entry closes.

Security function	Description
Access control	The TOE manages access control within each organisation based on user IDs, user roles and access control lists. The TOE maintains access control lists for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.
Identification and authentication	The TOE requires that each user is successfully identified (user ID) and authenticated (password) before any interaction with protected resources is permitted.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

1.4.2 TOE type

SisoftWebHBYS provides reuse of electronic registers of patients' examination, etude, medicine, material, operation, admission, reports and of all healthcare corporation/organization services with nice ties, **examining quickly every application of a patient**. All personal informations of a patient (Name, Surname, Date/Place of Birth, Blood Group etc.) and all operation informations with contact information of a patient (Social Security, Referral, Corporation, Register No etc.) are being kept safely. (Speed taped in emergency service and primary operation realization feature are being provided.)

The TOE is a specialist software module designed to be used as a core security controlling module for a web-based application environment. The TOE provides core security functionality such as authentication, access control, secure communications and application security management.

1.4.3 Supporting hardware, software and/or firmware

The TOE operates in a web server environment. In addition to requiring services from the environment to achieve its primary aim, the TOE also relies on the environment to maintain a secure posture so that the application cannot be compromised by factors out of the technology services.

The TOE requires the following from the environment to function:

Type	Description	
Operating System	Suse Enterprise Server 11 or MS Windows 2008 EntEdt.	
Web Server	Oracle Weblogic 11g	
Database (RDBMS)	Oracle 11g R2	
VTYS Server	Processor	2 x Intel XEON Processor x5670 2.93 GHz 12MB Cache
	RAM	32 GB
	HDD	2 x 146 GB 10K 6Gbps SAS | 3 x 600 GB 10K 6Gbps SAS
	RAID Card	512 MB
	RAID Support	0 / 1 / 5 / 10
	Network	4 x gigabit LAN (10 /100 / 1000)
	Power Supply	2x 800W
APP Server	Processor	2 x Intel XEON Processor x5670 2.40 GHz 12MB Cache
	RAM	16 GB
	HDD	2 x 146 GB 10K 6Gbps SAS | 3 x 600 GB 10K 6Gbps SAS
	RAID Card	512 MB
	RAID Support	0 / 1 / 5 / 10
	Network	4 x gigabit LAN (10 /100 / 1000)
	Power Supply	2x 800W
Client	Processor	P4 CELERON 2.8 İŞLEMCİ
	RAM	512 MB DDR400 RAM
	HDD	40 GB RPM 7200 HDD
	Network	Ethernet (10 /100 / 1000)
	Power Supply	350W
	OEM	Klavye Mouse Barkode Writer and Reader

The TOE requires, specifically, that the underlying environment provide appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server). The TOE also requires that the underlying environment, primarily the Client browser and Web Server, provide protection for authentication details traversing the network. In addition, the TOE requires that the underlying environment is free of vulnerabilities that allow an attacker to bypass the TOE security functions.

1.5 TOE description

1.5.1 Physical scope of the TOE

The TOE is a java module which is part of the Sisoft WebHBYS Healthcare information Management System is a web application hosted on a web server. A typical architecture of the TOE can be found in below and identifies the various components of the Sisoft architecture. It is assumed there is appropriate network layer protection, that there is a firewall in place that only permits access through required ports for external users to access the web-server.

1.5.2 Logical scope of the TOE

The logical scope of the TOE is described through the security functionality that the Sisoft Security Module provides for the Sisoft WebHBYS, this functionality is as follows:

Identification &Authentication: When a user issues a request to the TOE to access a protected resource, the TOE requires that the user (being an User, Administrator) identify and authenticate themselves before performing any action on behalf of the user. The TOE checks the credentials presented by the user upon the login page against the authentication information in the database. Each users account only exists in the database that relates to the user organisation.

Access Control: The access control function permits a user to access a protected resource only if a user ID or role of the user has permission to perform the requested action on the resource. Access rules are stored in Access Control Lists.

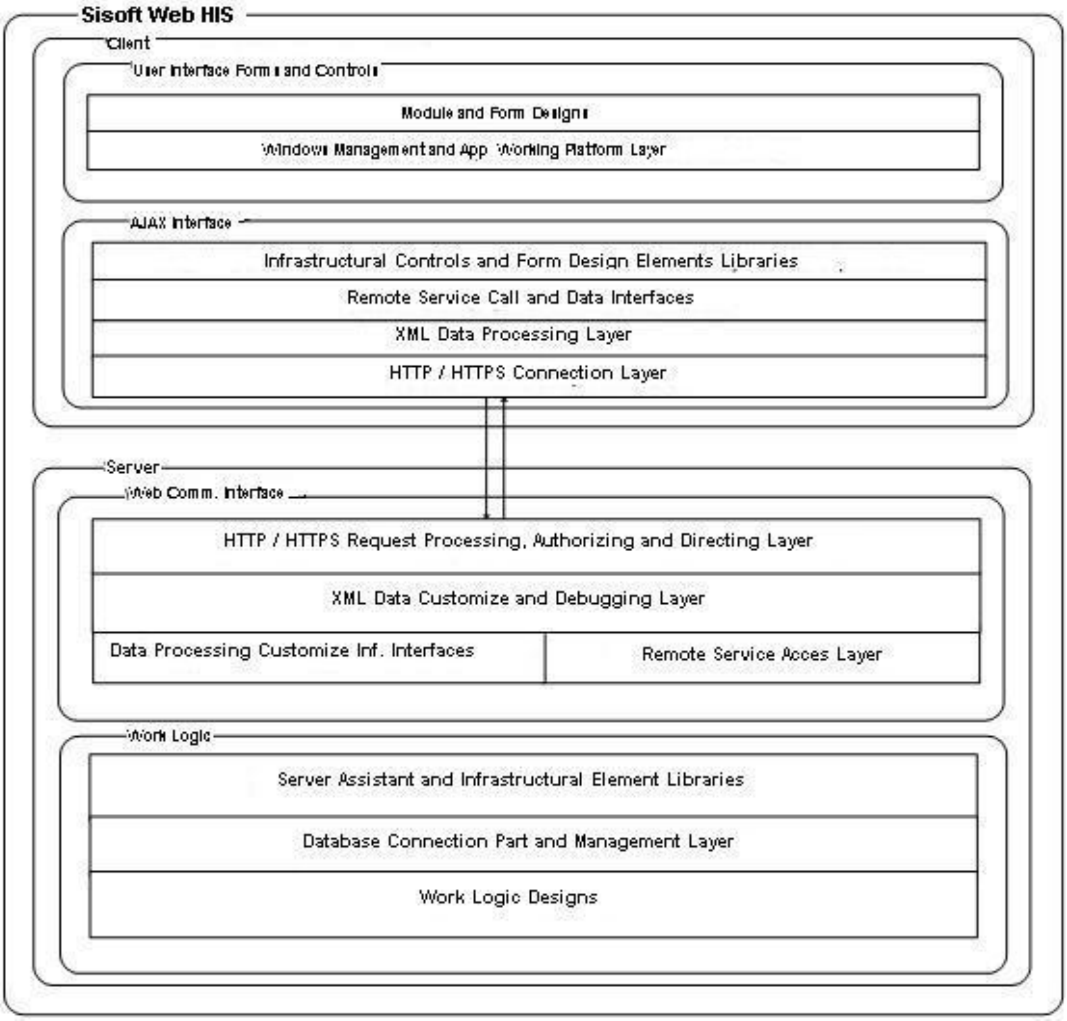
Security Management: The Sisoft WebHBYS contains various management functions to ensure efficient and secure management of the TOE: user management, permission management for functions and data management. The TOE maintains two roles within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: User and Administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

1.5.3 TOE Environment

SSL provides secure data communication over the Internet encrypted. The TOE supports SSL protocol. Sets the SSL protocol for use with the product are made on the application server. SSL protocol allows communication confidential and integrity

1.5.4 Healtcare Information System Architecture

Sisoft WEBHBYS (Healthcare Information System), system and communications architecture, as shown in Schema 1A.

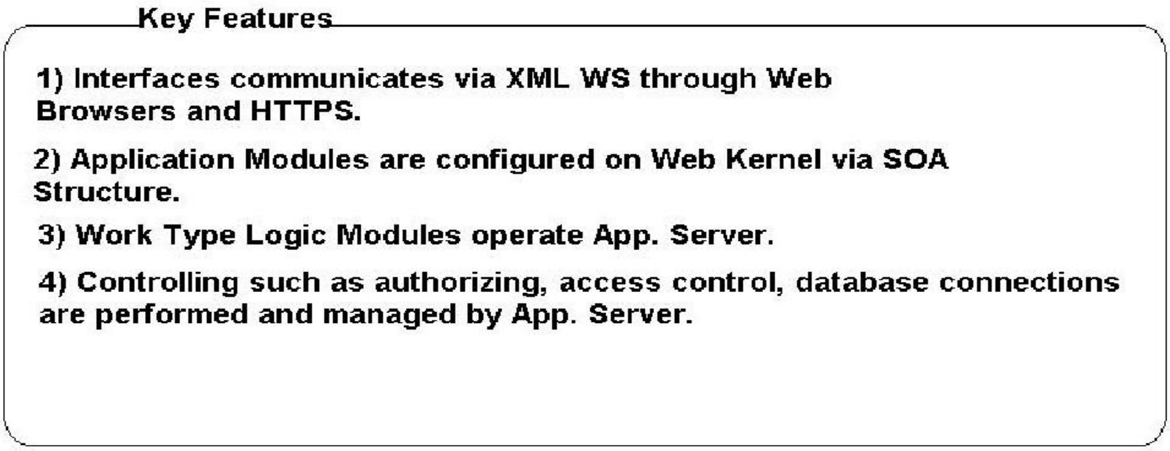

Sisoft Web HIS
Client
User Interface Forms and Controls
Module and Form Designs
Windows Management and App. Working Platform Layer
AJAX Interface
Infrastructural Controls and Form Design Elements Libraries
Remote Service Call and Data Interfaces
XML Data Processing Layer
HTTP / HTTPS Connection Layer
Server
Web Comm. Interface
HTTP / HTTPS Request Processing, Authorizing and Directing Layer
XML Data Customize and Debugging Layer
Data Processing Customize Inf. Interfaces
Remote Service Acces Layer
Work Logic
Server Assistant and Infrastructural Element Libraries
Database Connection Part and Management Layer
Work Logic Designs

Schema 1A – Communication Interface

Sisoft WEBHBYS (Healthcare Information System) architecture is formed with two primary structure such as server and client. The work type (logic) and code items in server part connect with user interfaces through XML Web Services.

Sisoft Healthcare Information Systems' Web-based Corporate Applications: It has highly strong and flexible architecture formed with infrastructures on server part such as load-balancing, authorizing, database connection management, etc... and web interface that connects XML Web Services that abstracts wholly work logic from user interfaces found on server part and powered by AJAX on WEB 2.0 standards and RIA (Rich Internet Applications) without needing any software set-up on updated Internet Browsers (E.g. Internet Explorer, Firefox, etc...)

There are some kind of structures that provides data connection between server and client and that provides the transformation of objective data to XML or XML to objective data. Starting from HTTP connection, authorizing, directing and data processing structures are composed in project core as infrastructural interfaces. Client is able to set-up synchronous and asynchronous connections through connection layer server. The results can be obtained by transmitting HTTP request to the server through those connections.



Key Features

1) Interfaces communicates via XML WS through Web Browsers and HTTPS.

2) Application Modules are configured on Web Kernel via SOA Structure.

3) Work Type Logic Modules operate App. Server.

4) Controlling such as authorizing, access control, database connections are performed and managed by App. Server.

Schema 1B- HTTP request

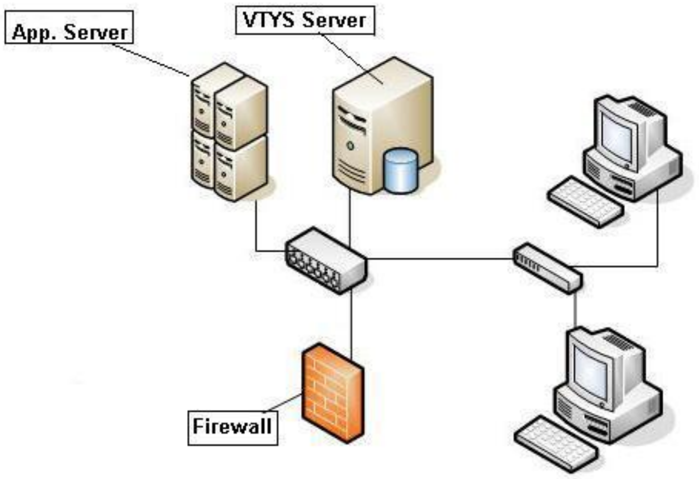
Server Connection Layer transmits the request to a upper layer so as to provide the transformation XML to objective data following the analyze of HTTP request via various filters in a basis of an authorization by using HTTP session.

Then it's assigned to remote service access points so as to transmit upper design codes or other remote XML Web Services by using fundamental structures in Web Connection Interface. Now it's the role of work logic. The work logic forms a work type routine for all structural software library and a targeted processing in a easier, securer and quicker way in a common standard.

It's thought between a fundamental infrastructure parts for database connection repository and work logic forming in order to realize a high productivity database processing under control. Software code elements are found on topping layer in the system by leveling in the basis of modules.

It forms a multi-layered platform that can operate on Internet Browser without needing any set-up with a high level of accessibility and easier-to-use. It enables a high level of design and easier-to-use for code elements and XML Web Service Call and feedback process on application server. The Interface Design Library which is formed dynamically operates as integrated via AJAX by working with data processing and connection layer.

Securer and Broad Accessibility via HTTPS Protocol



Schema 1C - HTTPS Protocol

2 Conformance Claim (ASE_CCL.1)

2.1CC Conformance Claim

The ST and TOE are conformant to version 3.1 (Revision 3) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

a) Part 1 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 1: Security functional requirements, version 3.1 Revision 4, September 2012.
b) Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 Revision 4, September 2012.
c) Part 3 conformant,Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 4, September 2012.

2.2 PP Claim

This ST does not claim conformance to any PP.

2.3 Package Claim

The current ST is conformant to the Assurance package EAL2 augmented with ALC_FLR.1 as defined in the CC, part 3.

3 Security Problem Definition (ASE_SPD.1)

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,
b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and
c) any relevant ***organisational security policies*** are any statements made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

Threats	Statements
T.ACCESS	An unauthorized user obtains or modifies stored user data that they are not authorised to access resulting in a loss of confidentiality or integrity of the data.
T.MANAGEMENT	An unauthorized user modifies management data that they are not authorised to access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.
T.PASSWORD	An unauthorized user gains access to the passwords in the database and use them to authenticate to the TOE resulting in a loss of confidentiality or integrity of user or management data.

3.3 Assumptions

Assumption	Statements
A.ENVIRONMENT	The TOE environment will provide appropriate authentication and authorisation controls for all users and administrators under environment (including the Operating System, DataBase, and Web Server)
A.ADMIN	It is assumed that the administration who manages the TOE is not hostile and is competent.
A.PHYSICAL	It is assumed that the servers that host the web and database servers are hosted in a secure operating facility with restricted physical access with non-shared hardware.
A.DATABASE	It is assumed that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
A.NETWORK	It is assumed there is appropriate network layer protection, that there is a firewall in place that only permits access through required ports for external users to access the web-server.
A.PATCH	It is assumed that the underlying operating system, web-server, application server and DBMSs and are patched and hardened to protect against known vulnerabilities and security configuration issues.
A.SSL_CONFIG	It is assumed that the web-server has SSL certificates installed and are valid (not revoked or expired), are sourced from a trusted entity.
A.MANAGEMENT	All management of the TOE will be performed through the management interfaces of the TOE and not through the under environment.
A.COMM	It is assumed that the web-server uses SSL when user data is traversing accross the internet from to the Sisoft WebHBYS application.

3.4 Organisational security Policies

Security problem definition does not contain any organisational security policy.

4 Security objectives (ASE_OBJ.2)

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. There are security objectives for the TOE to address and additional objectives that provide specific direction for the intended in environment in which the TOE is to operate.

4.2 Security objectives for the TOE

Identifier	Objective statements
O.ACCESS	The TOE must ensure that only authorised users are able to access protected resources or functions.
O.USER	The TOE must ensure that all users are identified and authenticated before they access a protected resources or functions.
O.MANAGE	The TOE must allow administrators to effectively manage the TOE, while ensuring that appropriate control is maintained over those functions.
O.PASSWORD	The TOE must ensure that passwords stored in the database are not in clear plaintext.

4.3 Security objectives for the environment

Identifier	Objective statements
OE.ENVIRONMENT	Those responsible for the TOE must ensure that appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, Oracle DataBase and Web Server)
OE.ADMIN	The owners of the TOE must ensure that the administrator who manages the TOE is not hostile and is competent.
OE.PHYSICAL	Those responsible for the TOE must ensure that the servers that host the web and database servers are hosted in a secure operating facility with restricted physical access with non-shared hardware.
OE.DATABASE	Those responsible for the TOE must ensure that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
OE.MANAGEMENT	Those responsible for the TOE must ensure that all management of the TOE is performed through the management interfaces of the TOE and not through the underlying environment.
OE.NETWORK	Those responsible for the TOE must ensure that appropriate network layer protection, that there is a firewall in place that only permits access through required ports for external users to access the web-server.
OE.PATCH	Those responsible for the TOE must ensure that the underlying operating system, web-server, application server and DBMSs and are patched and hardened to protect against known vulnerabilities and security configuration issues.
OE.SSL_CONFIG	Those responsible for the TOE must ensure that the web-server has SSL certificates installed and are valid (not revoked or expired), are sourced from a trusted entity.
OE.COMM	Those responsible for the TOE must ensure that the web server uses SSL to protect user data traversing across the network from disclosure and loss of integrity.

4.4 TOE security objectives rationale

The following table demonstrates that all security objectives for the TOE trace back to the threats in the security problem definition.

Threats/OSPs	Objectives	Rationale
T.ACCESS	O.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users.
	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
T.MANAGEMENT	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
	O.MANAGE	This 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.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users
T.PASSWORD	O.PASSWORD	The objective ensures that all passwords stored in the database are hashed using SHA-2 before written to the database. No one can see the password in plaintext and will not be able to use the password toauthenticate to the TOE.

4.5 Environment security objectives rationale

The following table demonstrates that all security objectives for the operational environment all trace back to assumptions or OSPs in the security problem definition.

Assumptions	Objective	Rationale
A.ENVIRONMENT	OE.ENVIRONMENT	This objective ensures that those responsible for the TOE ensure that appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, Oracle DataBase, and Web Server)
A.ADMIN	OE.ADMIN	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
A.PHYSICAL	OE.PHYSICAL	This objective ensures that those responsible for the TOE ensure that the servers that host the web and database servers are hosted in a secure operating facility with restricted physical access with non-shared hardware.
A.DATABASE	OE.DATABASE	This objective ensures that those responsible for the TOE ensure that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
A.MANAGEMENT	OE.MANAGEMENT	This objective ensures that those responsible for the TOE ensure that all management of the TOE is performed through the management interfaces of the TOE and not through the underlying environment.
A.NETWORK	OE.NETWORK	This objective ensures that those responsible for the

		TOE ensure that appropriate network layer protection, that there is a firewall in place that only permits access through required ports for external users to access the web-server.
A.PATCH	OE.PATCH	This objective ensures that those responsible for the TOE ensure that the underlying operating system, web-server, application server and DBMSs and are patched and hardened to protect against known vulnerabilities and security configuration issues.
A.SSL_CONFIG	OE.SSL_CONFIG	This objective ensures that those responsible for the TOE ensure that the web-server has SSL certificates installed and are valid (not revoked or expired), are sourced from a trusted entity.
A.COMM	OE.COMM	The objective ensures that all user data from the user to the web server will be secured using SSL protecting the user data from unauthorized disclosure and loss of integrity.

5 Security requirements (ASE_REQ.2)

5.1 Overview

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 bold 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~~.~~

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_ACC.1/a

5.2 Security functional requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and itemised in the table below.

Identifier	Title
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1/a	Management of TSF data (Default)
FMT_MTD.1/b	Management of TSF data (Configuration)
FMT_MTD.1/c	Management of TSF data (Password)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FTP_TRP.1	Trusted path
FTA_SSL.1	TSF-initated session locking

FTA_SSL.3	TSF-initiated termination
FAU_GEN.1	Audit data generation
FIA_AFL.1	Authentication failure handling
FIA_USB.1	User-subject binding
FIA_ATD.1	User attribute definition
FTA_TSE.1	TOE session establishment
FPT_STM.1	Reliable time stamp

5.2.2 FCS_COP.1 Cryptographic Operation

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**secure hashing**][1] in accordance with a specified cryptographic algorithm [**SHA-2**] and cryptographic key sizes [**none**] that meet the following: [**FIPS 180-2**][2].
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

5.2.3 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**Access Control SFP**] on [**Subjects:** **a) HTTP request on behalf of users** **Objects:** **a) Protected resources (methods and HTML pages)** **Operations:** **a) Methods execution** **b) Serving of HTML pages**]
Dependencies:	FDP_ACF.1 – Security attribute based access control

5.2.4 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**Access Control SFP**] to objects based on the following: [**Subject attribute:** **a) ID of the user** **b) corresponding user role** **Object attributes:** **a) Access Control List**]
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**The operation is allowed, if:** **a) The Access Control List for an object permits the user ID to access that**

[1] Assignment : List of cryptografic operations
[2] Assignment : Secure Hash Signature Standard

	object; OR **b) The Access Control List for an object permits the User Role to access that Object**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**the Administrator role can access all records and functions**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

5.2.5 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
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.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	User Credentials for User only exist within a specific organisation.

5.2.6 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
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.
Dependencies:	No dependencies.

5.2.7 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**Access Control SFP**] to restrict the ability to [[**write]** ***or delete***] the security attributes [**Subject attribute:** **a) ID of the user** **b) corresponding user role** **Object attributes:** **a) Access Control List**] to [**administrator**].
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

5.2.8 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow ~~the~~ [**none**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

5.2.9 FMT_MTD.1/a Management of TSF data (Default)

Hierarchical to:	No other components.

FMT_MTD.1a.1	The TSF shall restrict the ability to [***change_default***] the [**all TSF data**] to [**None**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

5.2.10 FMT_MTD.1/b Management of TSF data (Configuration)

Hierarchical to:	No other components.
FMT_MTD.1b.1	The TSF shall restrict the ability to [***query, modify, delete, clear,*** [**Create**]] the [**Access Control Lists, Mapping of users to Roles, User accounts**] to [**Administrator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

5.2.11 FMT_MTD.1/c Management of TSF data (Password)

Hierarchical to:	No other components.
FMT_MTD.1c.1	The TSF shall restrict the ability to [***modify***] the [**User Password**] to [**User (that is related to the password), Administrator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

5.2.13 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) mapping user roles** **b) creation of users with default passwords/ changing of passwords** **c) deletion of users** **d) management of Access Control lists**
Dependencies:	No dependencies

5.2.14 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**User, Administrator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification

5.2.15 FAU_GEN.1: Audit data generation

Hierarchical to:	No other components.
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) [**Login (successful - unsuccessful), prescription delivery, Records are traded, xml logs of some web services**].
FAU_GEN.1.2	The TSF shall record within each audi 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**].
Dependencies:	FPT_STM Reliable time stamp

5.2.16 FIA_AFL.1: Authentication failure handling

Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when [**3**] 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 account until unlocked by the authorized security administrator or until a configurable number of minutes have elapsed**].
Dependencies:	FIA_UAU.1 Timing of authentication

5.2.17 FIA_USB.1: User-subject binding

Hierarchical to:	No other components.
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**user identity and active access roles**].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**subject security attributes are derived from TSF data maintained for each defined user after a successful login with the defined user identity**].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**a user can set the active access role to any or all access roles assigned to them by an authorized security administrator**].
Dependencies:	FIA_ATD.1 User attribute definition

5.2.18 FIA_ATD.1: User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**user identity, access control list, access roles as defined by an authorized security administrator**].
Dependencies:	No dependencies

5.2.19 FTA_TSE.1: TOE session establishment

Hierarchical to:	No other components.
FTA_TSE.1.1	The TSF shall be able to deny session establishment based on [**attributes that can be set explicitly by authorized administrator(s), including user identity and/or group identity, database name, Host IP address, and/or subnet address**].
Dependencies:	No dependencies

5.2.203 FPT_STM: Reliable time stamp

Hierarchical to:	No other components.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Dependencies:	No dependencies

5.3 TOE security assurance requirements

EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behavior.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
	ALC_FLR.1 Flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4 Defined terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements.

Term/Acronym	Definition
Authentication Data	It is information used to verify the claimed identity of a user.
FIPS 180-2	It is a Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology for Secure Hash Standard

SHA-2	SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512) designed by the National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard. For the evaluation, SHA-256 is implemented only.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE
Unauthorized users	Unauthorized users can mean a legitimate user with access rights to certain web resource, an external entity that has no rights to any protected web resource/data.
Users	It means any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In this case, there are end users (Administrator) of the TOE access the TOE through a web browser.
User data	Data created by and for the user, that does not affect the operation of the TSF
TSC	TOE Scope of Control, the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP
TSP	TOE Security Policy, a set of rules that regulate how assets are managed, protected and distributed.

5.5 Security requirements rationale

5.5.1 SFR dependency rationale

Below demonstrates the mutual supportiveness of the SFR's for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE, and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level EAL2 as defined in Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

SFR	Dependency	Inclusion
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FMT_SMF.1	No dependencies	N/A
FMT_MSA.1	[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	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FMT_MTD.1a	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1b	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1c	FMT_SMR.1 Security roles	FMT_SMF.1

	FMT_SMF.1 Specification of Management Functions	FMT_SMR.1
FAU_GEN.1	FPT_STM.1 Reliable time stamp	FPT_STM.1
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FIA_ATD.1	No dependencies	N/A
FTA_TSE.1	No dependencies	N/A
FPT_STM.1	No dependencies	N/A
FCS_COP.1	[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	SHA-2 algorithm does not use any key. So there is no need to generate, destruct or share keys.

5.5.2 Mapping of SFRs to security objectives for the TOE

Objective	SFR and Demonstration
O.ACCESS	**FDP_ACC.1**: The requirement helps meets the objective by identifying the objects and users subjected to the access control policy. **FDP_ACF.1**:The requirement meets this objective by ensuring the TOE only allows access to objects based on the defined access control policy. **FIA_AFL.1**: Authenticationfailurehandling **FIA_USB.1**: Successorfailure of bindingusersecurityattributesto adatabasesubject **FIA_ATD.1**: User attributedefinition
O.USER	**FIA_UID.2**: The requirement helps meets the objective by identifying the users before any TSF mediated actions. **FIA_UAU.2**: The requirement helps meets the objective by authenticating the users before any TSF mediated actions. **FMT_SMR.1**: The TOE manages 2 roles: User, Administrator.
O.PASSWORD	**FCS_COP.1:** The requirement helps to meet the objective by hashing all the passwords using SHA-2 before they are written into the database.
O.MANAGE	**FMT_MSA.1**: The TOE allows the administrator to determine who will have access to the folder and the folder's contents and what actions the user can be perform. **FMT_MSA.3**: The TOE enforces a restrictive access when a new object is created. The TOE has a default ACL which is assigned to all newly-created objects. This default ACL cannot be altered by any user. **FMT_MTD.1a:** This requirements helps meet the objective by allowing no one to change the default values of the TSF data. **FMT_MTD.1c:** This requirement helps meet the objective by allowing users of all roles to change their passwords. **FMT_MTD.1b:** This requirements helps meet the objective by allowing only the administrator roles to create, delete, modify access control list, mapping of users to roles and user accounts to the respective organisation database. **FMT_SMF.1**: The TOE allows the mapping of user to roles, creation of users,deletion of users, changing of passwords, management of ACL and managing organisation.. **FMT_SMR.1**: The TOE manages 2 roles: User, Administrator. **FAU_GEN.1**: Audit data generation

	FPT_STM.1: Time stamp used in audit data generation. **FTA_TSE:** TSF manages Session establishment policy

5.5.3 Explanation for selecting the SARs

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 [EAL2 + (ALC_FLR.1)].

The TOE is intended to protect confidential information related to a business's user. This information, while sensitive within an organization, the value to an attacker is relatively low. As such, it is considered that the average motivation of attackers will be low, which implies that the overall attack potential for this TOE will be LOW. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a LOW attack potential.

In addtition to provides additional quality assurance to the product ALC_FLR.1 provides well defined update procedure.

6 TOE summary specification (ASE_TSS.1)

6.1 Overview

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements. s

The TOE security functions include the following:

- Access Control
- Identification and Authentication
- Security Management

6.2 Access Control

The TOE enforces an access control policy on protected resource. After a user identifies and authenticates to the TOE, the TOE will check all HTTP request to the protected resource from the user. The TOE will permit a user to access a protected resource only if a user ID or role of the user has permission to perform the requested action on the resource (**FDP_ACC.1, FDP_ACF.1**). The TOE maintains access control lists for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

There are 2 users maintained by the TOE. They are User, Administrator (**FMT_SMR.1**). Each type of user will have different access rights to a protected resource. All users will have a unique user ID.

TOE satisfies TSF_FIA.1 administrator identification and certification by defining the security properties of authorized administrator at the time of executing security policy on the basis of management.**(FIA_ATD.1)**

TOE manages session by session establishment policy described in **FTA_TSE.1.**

6.3 Identification and Authentication

When a user issues a request to the TOE to access a protected resource (methods or HTML pages), the TOE requires that the user (being an User, Administrator) identify and authenticate themselves before performing any TSF mediated action on behalf of the user (**FIA_UID.2, FIA_UAU.2**). The TOE checks the credentials presented by the user upon the login page against the authentication information in the database. Each users account only exists in the database that relates to the user organisation.

All users presented passwords are hashed before being used to authenticate the user or when users change their passwords (**FMT_MTD.1c**) and is being written to the database. This is all done by the TOE (**FCS_COP.1**).

in the event of occurrence of certification attempts that have failed 3 times (within 1 minute) in relations to [attempt of user], detect such. **(FIA_AFL.1)**

Success or failure of binding user security attributes to a database subject (e.g., success and failure to create a database subject)**(FIA_USB.1)**

6.4 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE **(FMT_SMF.1)**:

a) User Management

The TOE only Administrator to query, create, delete, and modify users into the respective in organization.

(FMT_MTD.1b).

b) Permission Management for Functions and Data
Administrator role can modify the access control list, mapping of users to roles as well as modifying the user accounts. **(FMT_MTD.1b, FMT_MSA.1)**.

c) **Organization Management**
The TOE maintains two roles **(FMT_SMR.1)** within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: User, Administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

The TOE allows no one to change the default values of the TSF data and security attributes of the TOE (**FMT_MTD.1a, FMT_MSA.3**).
TOE assures ability to define case to be subjected to audit and generation of audit record**(FAU_GEN.1).** TOE supports obtain time stamp need to be used for reliable audit records **(FPT_STM.1)**