çizim, metre içeren bir resim

Açıklama otomatik olarak oluşturuldu

**SISOHIS SECURITY TARGET**

Sisoft HIS 2.0.4

Security Target v.1.33

# DOCUMENT HISTORY

|  |  |  |
| --- | --- | --- |
| v.1.0 | 01.05.2020 | Released for internal review |
| v.1.1 | 19.06.2020 | Content improvement |
| v.1.2 | 03.07.2020 | Content improvement |
| v.1.3 | 07.07.2020 | Content improvement |
| v.1.4 | 07.07.2020 | Content improvement |
| v.1.5 | 30.09.2020 | Content improvement |
| v.1.6 | 10.11.2020 | Content improvement |
| v.1.7 | 27.11.2020 | Content improvement |
| v.1.8 | 04.12.2020 | Content improvement |
| v.1.9 | 14.01.2021 | Content improvement |
| v.1.10 | 18.01.2021 | Content improvement |
| v.1.11 | 08.02.2021 | Content improvement |
| v.1.12 | 26.04.2021 | Content improvement |
| v.1.13 | 04.06.2021 | Content improvement |
| v.1.14 | 23.06.2021 | Content improvement |
| v.1.15 | 07.07.2021 | Content improvement |
| v.1.16 | 07.12.2021 | Content improvement |
| v.1.17 | 20.12.2021 | Content improvement |
| v.1.18 | 21.12.2021 | Content improvement |
| v.1.19 | 27.01.2022 | Content improvement |
| v.1.20 | 03.10.2022 | Content improvement |
| v.1.21 | 10.05.2023 | Content improvement |
| v.1.22 | 07.07.2023 | Content improvement |
| v.1.23 | 27.07.2023 | Content improvement |
| v.1.24 | 28.07.2023 | Content improvement |
| v.1.25 | 22.09.2023 | Content improvement |
| v.1.26 | 12.12.2023 | TOE Version and document revision number have been updated. |
| v.1.27 | 11.01.2024 | TOE TITLE updated  Cover title updated  1.2. explanation updated  Document name updated |
| v.1.28 | 16.02.2024 | FDP\_ACF.1.2 updated. |
| v.1.29 | 27.02.2024 | FDP\_ACF.1.2 updated. |
| v.1.30 | 07.05.2024 | FAU\_STG.3 and FIA\_AFL.1 updated. |
| v.1.31 | 12.06.2024 | 1.3.2.1, 7.1 and FIA\_AFL.1 updated. |
| v.1.32 | 24.06.2024 | FIA\_AFL.1, 7.3 and 1.3.2.4 are updated. |
| v.1.33 | 02.07.2024 | FIA\_AFL.1, 7.3 and 1.3.2.4 are updated. |

ındex

[DOCUMENT HISTORY 1](#_Toc141368786)

[1. ST INTRODUCTION (ASE\_INT) 4](#_Toc141368787)

[1.1. ST AND TOE REFERENCES 4](#_Toc141368788)

[1.2. TOE OVERVIEW 4](#_Toc141368789)

[1.2.1. TOE SECURITY FEATURES 5](#_Toc141368790)

[1.2.2. TOE TYPE 5](#_Toc141368791)

[1.2.3. HARDWARE/SOFTWARE REQUIRED BY TOE 5](#_Toc141368792)

[1.3. TOE DESCRIPTION 5](#_Toc141368793)

[1.3.1. PHYSICAL SCOPE OF TOE 6](#_Toc141368794)

[1.3.2. LOGICAL SCOPE OF TOE 6](#_Toc141368795)

[1.3.2.1. AUDIT 6](#_Toc141368796)

[1.3.2.2. SECURE COMMUNICATION 6](#_Toc141368797)

[1.3.2.3. CRYPTOGRAPHIC SUPPORT 6](#_Toc141368798)

[1.3.2.4. IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION 7](#_Toc141368799)

[1.3.2.5. SECURITY MANAGEMENT 7](#_Toc141368800)

[1.3.2.6. TOE ACCESS 7](#_Toc141368801)

[2. CONFORMANCE CLAIMS (ASE\_CCL) 7](#_Toc141368802)

[2.1. CC CONFORMANCE CLAIM 7](#_Toc141368804)

[2.2. PP CLAIM 7](#_Toc141368805)

[2.3. PACKAGE CLAIM 7](#_Toc141368806)

[3. SECURITY PROBLEM DEFINITION (ASE\_SPD) 7](#_Toc141368807)

[3.1. THREATS 8](#_Toc141368809)

[3.1.1. T. UNAUTHORIZED ACCESS 8](#_Toc141368814)

[3.1.2. T. DISABLING USER LOGIN LOGOUT LOG RECORDS 8](#_Toc141368815)

[3.1.3. T. INFORMATION 8](#_Toc141368816)

[3.1.4. T. DATA CHANGE 8](#_Toc141368817)

[3.1.5. T. BRUTE FORCE 8](#_Toc141368818)

[3.1.6. T. DENIAL OF SERVICE (DoS) 8](#_Toc141368819)

[3.1.7. T. MODIFY AUDIT 8](#_Toc141368820)

[3.1.8. T. COMMUNICATION 8](#_Toc141368821)

[3.2. ORGANIZATIONAL SECURITY POLICIES (OSPs) 8](#_Toc141368822)

[3.2.1. P. SECURITY 8](#_Toc141368824)

[3.2.2. P. SECURE COMMUNICATION 8](#_Toc141368825)

[3.2.3. P. MAINTENANCE 9](#_Toc141368826)

[3.3. ASSUMPTIONS 9](#_Toc141368827)

[3.3.1. A. PROPER ADMIN (PROGRAM ADMIN & SUPER ADMIN) 9](#_Toc141368829)

[3.3.2. A. PROPER SERVICE USER 9](#_Toc141368830)

[3.3.3. A. BACKUP 9](#_Toc141368831)

[3.3.4. A. ENVIRONMENT SECURITY- ENVSEC 9](#_Toc141368832)

[3.3.5. A. PHYSICAL 9](#_Toc141368833)

[3.3.6. A. RELIABLE TIME STAMP 9](#_Toc141368834)

[3.4. ASSETS 9](#_Toc141368835)

[4. SECURITY OBJECTIVES (ASE\_OBJ) 9](#_Toc141368837)

[4.1. SECURITY OBJECTIVES FOR TOE 10](#_Toc141368839)

[4.1.1. O. IDENTIFICATION & AUTHENTICATION 10](#_Toc141368842)

[4.1.2. O. AUDIT 10](#_Toc141368843)

[4.1.3. O. ACCESS 10](#_Toc141368844)

[4.1.4. O. HASH 10](#_Toc141368845)

[4.1.5. O. COMMUNICATION 10](#_Toc141368846)

[4.1.6. O. MANAGEMENT 10](#_Toc141368847)

[4.2. SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT 10](#_Toc141368848)

[4.2.1. OE. SECURITY 10](#_Toc141368855)

[4.2.2. OE. TAKING BACKUPS OF DATA 10](#_Toc141368856)

[4.2.3. OE.WEB APPLICATION FIREWALL 10](#_Toc141368857)

[4.2.4. OE. ADMIN 10](#_Toc141368858)

[4.2.5. OE. RELIABLE TIME STAMP 11](#_Toc141368859)

[4.3. SECURITY OBJECTIVE RATIONALE 11](#_Toc141368860)

[5. EXTENDED COMPONENT DEFINITION (ASE\_ECD) 13](#_Toc141368861)

[6. SECURITY REQUIREMENTS (ASE\_REQ) 13](#_Toc141368862)

[6.1. SECURITY FUNCTIONAL REQUIREMENTS (SFRS) 13](#_Toc141368865)

[6.1.1. SECURITY AUDIT 14](#_Toc141368866)

[6.1.1.1. FAU\_GEN.1: AUDIT DATA GENERATION 14](#_Toc141368875)

[6.1.1.2. FAU\_GEN.2: USER IDENTITY ASSOCIATION 14](#_Toc141368876)

[6.1.1.3. FAU\_SAR.1: AUDIT REVIEW 14](#_Toc141368877)

[6.1.1.4. FAU\_STG.1: PROTECTED AUDIT TRAIL STORAGE 15](#_Toc141368878)

[6.1.1.5. FAU\_STG.3: ACTION IN CASE OF POSSIBLE AUDIT DATA LOSS 15](#_Toc141368879)

[6.1.2. CRYPTOGRAPHIC SUPPORT 15](#_Toc141368880)

[6.1.2.1. FCS\_COP.1: CRYPTOGRAPHIC OPERATION 15](#_Toc141368882)

[6.1.3. USER DATA PROTECTION 15](#_Toc141368883)

[6.1.3.1. FDP\_ACC.1: SUBSET ACCESS CONTROL 15](#_Toc141368885)

[6.1.3.2. FDP\_ACF.1: SECURITY ATTRIBUTE BASED ACCESS CONTROL 15](#_Toc141368886)

[6.1.4. PROTECTION OF THE TSF 16](#_Toc141368887)

[6.1.4.1. FPT\_ITT.1: BASIC INTERNAL TRANSFER PROTECTION 16](#_Toc141368889)

[6.1.5. IDENTIFICATION AND AUTHENTICATION 16](#_Toc141368890)

[6.1.5.1. FIA\_AFL.1: AUTHENTICATION FAILURE HANDLING 16](#_Toc141368892)

[6.1.5.1.1. FIA\_AFL.1: AUTHENTICATION FAILURE HANDLING / USER BLOCKING 16](#_Toc141368893)

[6.1.5.1.2. FIA\_AFL.1: AUTHENTICATION FAILURE HANDLING / IP BLOCKING 17](#_Toc141368894)

[6.1.5.1.3. FIA\_UAU.2: USER AUTHENTICATION BEFORE ANY ACTION 17](#_Toc141368895)

[6.1.5.1.4. FIA\_UID.2: USER IDENTIFICATION BEFORE ANY ACTION 17](#_Toc141368896)

[6.1.6. SECURITY MANAGEMENT 17](#_Toc141368897)

[6.1.6.1. FMT\_MSA.1: MANAGEMENT OF SECURITY ATTRIBUTES 17](#_Toc141368899)

[6.1.6.2. FMT\_MSA.3: STATIC ATTRIBUTE INITIALIZATION 18](#_Toc141368900)

[6.1.6.3. FMT\_SMF.1: SPECIFICATION OF MANAGEMENT FUNCTIONS 18](#_Toc141368901)

[6.1.6.4. FMT\_SMR.1 SECURITY ROLES 18](#_Toc141368902)

[6.1.7. TOE ACCESS 18](#_Toc141368903)

[6.1.7.1. FTA\_SSL.1: TSF-INITIATED 18](#_Toc141368905)

[6.1.7.2. FTA\_SSL.3: TSF-INITIATED 19](#_Toc141368906)

[6.1.7.3. FTA\_SSL.4: USER-INITIATED 19](#_Toc141368907)

[6.1.7.4. FTA\_TSE.1: TOE SESSION ESTABLISHMENT 19](#_Toc141368908)

[6.1.8. TRUSTED PATH/CHANNELS 19](#_Toc141368909)

[6.1.8.1. FTP\_TRP.1: TRUSTED PATH 19](#_Toc141368911)

[6.2. SECURITY ASSURANCE REQUIREMENTS (SARS) 19](#_Toc141368912)

[6.3. SECURITY REQUIREMENT RATIONALE 20](#_Toc141368913)

[6.3.1. SFR RATIONALE 20](#_Toc141368923)

[6.3.1.1. SFR DEPENDENCY RATIONALE 20](#_Toc141368934)

[6.3.1.2. SFR OBJECTIVE RATIONALE 21](#_Toc141368935)

[6.3.1.3. SAR RATIONALE 22](#_Toc141368936)

[7. TOE SUMMARY SPECIFICATION 22](#_Toc141368937)

[7.1. SECURITY AUDIT 22](#_Toc141368940)

[7.2. CRYPTOGRAPHIC SUPPORT 22](#_Toc141368941)

[7.3. IDENTIFICATION AND AUTHENTICATION 22](#_Toc141368942)

[7.4. SECURITY MANAGEMENT 23](#_Toc141368943)

[7.5. TOE ACCESS 23](#_Toc141368944)

[7.6. TRUSTED PATH/CHANNELS 23](#_Toc141368945)

[8. REFERENCES 23](#_Toc141368946)

table ındex

[*Table 1 ST AND TOE REFERENCES* 4](#_Toc90978896)

[*Table 2 Hardware / Software Requirements* 5](#_Toc90978897)

[*Table 3 SECURITY OBJECTIVE RATIONALE* 11](#_Toc90978898)

[*Table 4 SECURITY FUNCTIONAL REQUIREMENTS (SFRS)* 14](#_Toc90978899)

[*Table 5 SECURITY ASSURANCE REQUIREMENTS (SARS)* 20](#_Toc90978900)

[*Table 6 SFR DEPENDENCY TABLE* 20](#_Toc90978901)

[*Table 7 SFR OBJECTIVE RATIONALE* 21](#_Toc90978902)

fıgure ındex

[*Figure 1 TOE* 6](#_Toc90903263)

# ST INTRODUCTION (ASE\_INT)

## ST AND TOE REFERENCES

|  |  |
| --- | --- |
| ST TITLE | SISOHIS SECURITY TARGET |
| ST VERSION | v.1.19 |
| TOE TITLE | Sisoft HIS |
| TOE VERSION | 2.0.4 |
| ASSURANCE LEVEL | EAL4+ ALC\_FLR.2 |
| CC IDENTIFICATION | Common Criteria Part 2 Version 3.1 Revision 5  Common Criteria Part 3 Version 3.1 Revision 5  Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 5 |

*Table 1 ST AND TOE REFERENCES*

## TOE OVERVIEW

The Sisoft HIS 2.0.4 (TOE) forms the infrastructure of the products developed by SISOFT. TOE provides tools and service functions that will ensure the correct management of the basic security requirements of the Hospital Information Management System (HIMS).

Software components that make up the TOE are responsible for the security of the processes applied in the stages of creating, transporting, storing, and processing data contents. Patient health data created with HIMS application, medical results from device integrations, physician decisions, reports, medical and other financial inputs are managed using TOE security functions.

**USER:** USER" specifies a program user that is created on the application (HIMS) in which the TOE works, uses this application, whose authorities are determined by another user (ADMIN), and can be used by those who work within the institution where the application is run.

The "USER" carries out its activities in accordance with the user job descriptions and roles on the screens that are granted access on the application, cannot access other screens or pages owned by the application, and cannot change the user roles or authorizations.

**SERVICE USER:** User account is given to machines running 24 hours a day as kiosks. Devices that interact with the TOE constitute TOE Service users and they are constantly connected to the system. These users can only read and write within the privileges given to them and are not thrown out of the system due to time limits.

**TOE ADMINS:**

**PROGRAM ADMIN:** "ADMIN" specifies a program user that is created on the application where the TOE works, can use the application within the limits specified in the ADMIN role, can create new users, edit their authorizations, and can be used by those who work within the institution where the application is running.

The IT manager or administrative staff in the institution where the application works have an "ADMIN" program user. Users with admin role have the authority to access and define all screens in the application unless their authority is limited.

**SUPER ADMIN:** The Super Admin manages all Program Administrator rights. Refers to the person responsible for all global settings of the system. It manages the level of access and responsibility of program admin.

### TOE SECURITY FEATURES

TOE provides the following security functions.

* Audit
  + Audit Data Generation and User Identity Association
  + Audit Review
  + Protected Audit Storage
  + Action in case of possible audit data loss
* Secure Communication
  + Secure Communication between TOE components
  + Secure Communication between TOE and remote or local users
* Cryptographic Support
  + Password Hashing
* Data protection
  + Access Control
* Identification and Authentication
  + Identification and authentication before any action
  + Authentication failure handling
* Security Management
  + Management functions
  + Security Roles
* Toe Access
  + Session Management

### TOE TYPE

TOE is health application framework.

### HARDWARE/SOFTWARE REQUIRED BY TOE

|  |  |
| --- | --- |
| OS | Min, Windows 2008 and above; Oracle Enterprise Linux 5 and above, RedHat Enterprice Linux 5 and above, SUSE Linux Enterprise Server 11 and above, Oracle Solaris 10 and above. |
| HARDWARE SERVER | Min. 8 Core CPU, 256GB Ram, 4TB HDD, SAS SSD. |
| DATABASE | Min. Oracle Database 12C and above |
| WEB SERVER | Tomcat (9 or above) or Weblogic (12c or above) |
| BROWSER | Min. Chrome (v.93 or above) or Firefox (v.90 or above) or Safari (v.12 or above) or Edge (v.90 or above) |

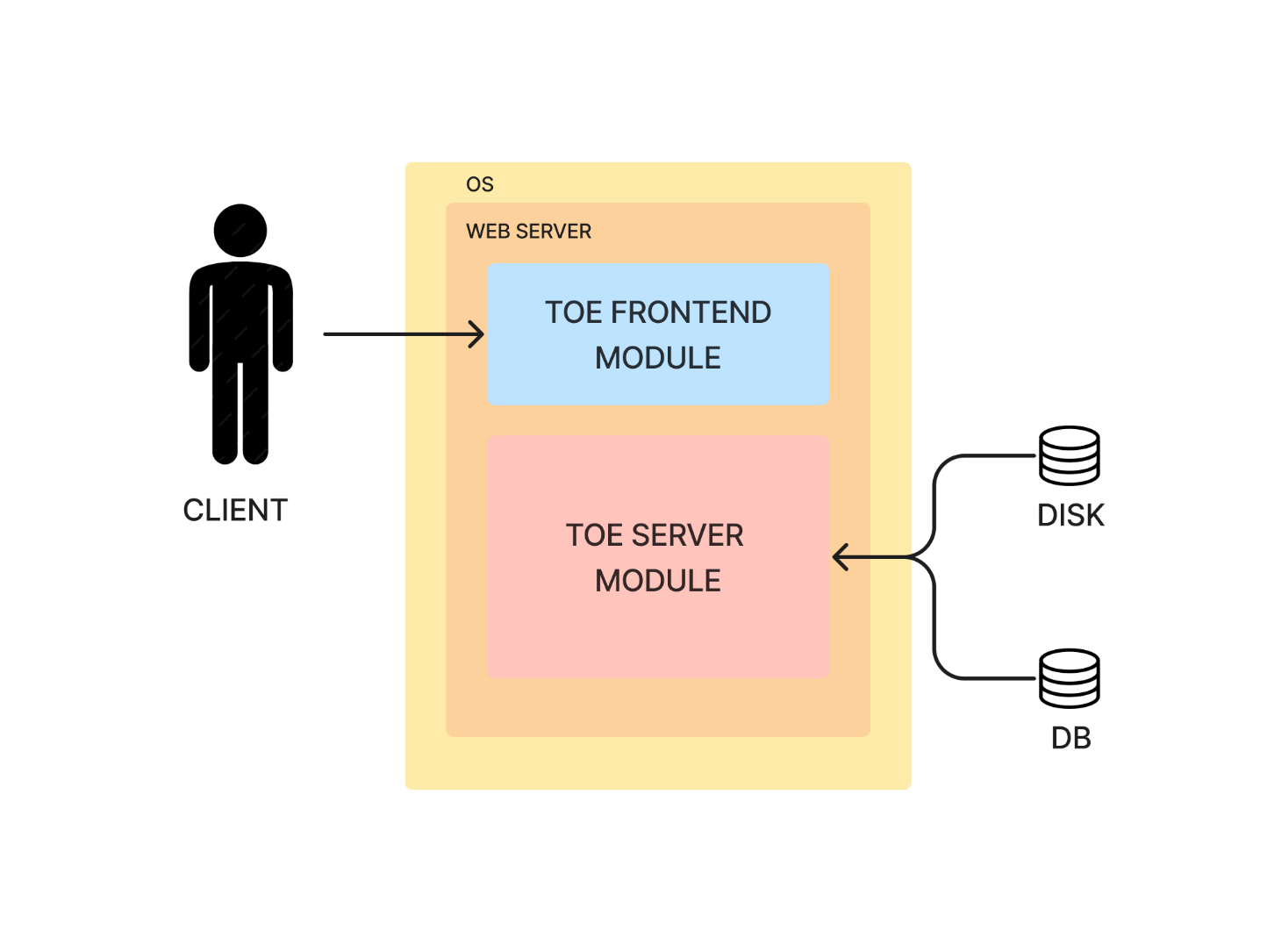
*Table 2 Hardware / Software Requirements*

## TOE DESCRIPTION

This part of the ST is analyzed under two headings, namely physical scope and logical scope.

### PHYSICAL SCOPE OF TOE

TOE is the web application framework of the products that developed by Sisoft and it is delivered electronically with the MD5 Checksum information via the download link. TOE consists of the following two parts and guidance documents.



*Figure 1 TOE*

### LOGICAL SCOPE OF TOE

#### AUDIT

TOE generates log records for security events. This log records contains Date and time of the event, type of event, and the outcome of the event, subject identity and accessing IP. Log records can be viewed by TOE Admins. TOE does not provide any permission to modify or delete any view or recorded data, for the records covered by the Security audit.

#### SECURE COMMUNICATION

Communication protocols provide a secure communication path between TOE and [local and remote] users that are logically distinct from other communication paths and provides assured identification of its endpoints and protection of the communicated data. The TOE structure supports encrypted data communication over the Internet with TLS **1.2**

In addition, TOE protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.

#### CRYPTOGRAPHIC SUPPORT

User passwords are stored after with PBKDF2 [RFC2898] algorithm with NumberOfIterations : 25 and Salt Bit Length: 128 hashing. Hashing action is taken by the TSF when storing passwords and authenticating users

#### IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION

When a user requests to access the TOE, the TOE prompts the user to identify and authenticate themselves before taking any action. When 3 unsuccessful authentication attempts have been met, user account is blocked for 30 minutes (can be adjusted by TOE Admins). The TSF shall detect when [an administrator configurable positive integer within [0-10]] unsuccessful authentication attemps occur related to [authentication]. When the “8” [an administrator configurable positive integer within [0-10]] authentication attempts have been met from same IP block, IP and user account is blocked for 20 minutes (can be adjusted by TOE Admins). After the authentication is successfully completed, then the TOE will authorize the users to access data and functions based on their user types.

#### SECURITY MANAGEMENT

The TOE maintains the following roles: User, Service User, Program Admin and Super Admin. Admins can modify and delete user status. TOE is capable of the following management functions: Delete, Modify and Create User, Read Audit Data, Read, Create, Modify Management Data, Read and Create Authentication and Authorization configurations. TOE also provides restrictive default values for security attributes and ability to override the default values to Super Admin.

#### TOE ACCESS

TOE locks interactive sessions after 2 minutes and require to re-login prior to unlocking the session. TOE allows user-initiated session termination and terminates interactive sessions after 15 minutes. TOE also has a mechanism to deny session establishment based on user status.

# CONFORMANCE CLAIMS (ASE\_CCL)



## CC CONFORMANCE CLAIM

The ST are conformant to version 3.1 (Revision 5) of the Common Methodology for Information Technology Security Evaluation.

The following conformance claims are made for the ST:

* Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 Revision 5, April 2017.
* Part 3 conformant, Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 5, April 2017.

## PP CLAIM

This ST does not claim conformance to any PP.

## PACKAGE CLAIM

The current ST is conformant to the Assurance package EAL 4+ augmented with ALC\_FLR.2 as defined in the CC, part 3.

# SECURITY PROBLEM DEFINITION (ASE\_SPD)

This part of the ST describes the security issue that needs to be addressed by the TOE and consists of the following subsections:

* Threats
* Organizational Security Policies (OSPs)
* Assumptions
* Assets



## THREATS

Threat agents are described below.

* Attackers who have knowledge of the TOE and are supposed to have an enhanced-basic skill level
* TOE users who have extensive knowledge about the use of TOE and are assumed to have a high level of skill to change TOE settings, parameters and change access to TOE.



### T. UNAUTHORIZED ACCESS

The attacker may get the passwords in database and gain access to user data and TSF data.

### T. DISABLING USER LOGIN LOGOUT LOG RECORDS

A threat agent may perform a large number of transactions in order to fill the logs and hence make audit unavailable.

### T. INFORMATION

Unauthorized TOE Users may access to user data or TSF data that they are not authorized to

### T. DATA CHANGE

The attacker may try to access and/or modify records, documents or data protected in TOE.

### T. BRUTE FORCE

Unauthorized TOE Users or attackers may try to repeatedly guess password to access TOE.

### T. DENIAL OF SERVICE (DoS)

The attacker may try to make the TOE inaccessible or unavailable for some time by sending many HTTP GET requests in a short period of time.

### T. MODIFY AUDIT

An attacker or TOE user may try to manipulate the audit data.

### T. COMMUNICATION

An attacker may try to access and/or modify the data transmitted between the TOE components or between TOE and other components.

## ORGANIZATIONAL SECURITY POLICIES (OSPs)



### P. SECURITY

This product is protected by a firewall in line with the needs of the user in the environment in which it works.

### P. SECURE COMMUNICATION

Communication with the web services provided should be secured. This secure communication should be done over TLS **1.2** protocol by TOE. The web service provider should ensure communication with server certificates that are not expired, revoked, or repealed. The web service user must also verify the certificate provided by the web service provider during each use and then request the web service. Web service communication should be provided using secure communication protocol.

### P. MAINTENANCE

Necessary security updates should be made on TOE by trained TOE Admins, according to changing technology and needs.

## ASSUMPTIONS



### A. PROPER ADMIN (PROGRAM ADMIN & SUPER ADMIN)

It is assumed that the TOE Admins who are responsible for setting up, configuring, and operating the TOE, are experienced, well trained, and not careless, deliberate negligent or unfriendly. It is assumed that the TOE installation, configuration, and operation are performed correctly by TOE Admins as specified in the guidance documents

### A. PROPER SERVICE USER

It is assumed that service users are not misconfigured

### A. BACKUP

It is assumed that any data generated by the TOE and/or its users are backed up regularly.

### A. ENVIRONMENT SECURITY- ENVSEC

It is assumed that the TOE's working environment has a web application firewall and runs on an operating system that has no security flaw.

### A. PHYSICAL

It is assumed that the servers hosting the web and database are hosted in a secure operating facility with unshared hardware and limited physical access.

### A. RELIABLE TIME STAMP

It is assumed that the reliable time stamp provided by operational environment

## ASSETS

* User data: All records, documents, or data within the TOE
* TSF Data
  + Audit data
  + Management data
  + Authentication Authorization data

# SECURITY OBJECTIVES (ASE\_OBJ)

Security objectives are a brief statement of the intended response to the security problem described in Chapter 3. There are security objectives for the TOE to address and additional objectives that provide specific directions for those intended for the environment in which the TOE will operate.



## SECURITY OBJECTIVES FOR TOE



### O. IDENTIFICATION & AUTHENTICATION

TOE must identify and authenticate all users before they access protected resources or functions. In addition, login attempts must be limited and when these limits are passed necessary actions must be taken.

### O. AUDIT

The TOE must record security related events with ability to review and ensure that these records are not changed. When the log record area is full, necessary measures must be taken.

### O. ACCESS

The TOE must ensure that "User", "Service User", "Program Admin" and "Super Admin" roles are defined, and only authorized users are able to access protected resources or functions. TOE must terminate sessions when user initiates it and terminate or lock sessions automatically after some time. If user status is disabled, TOE must reject the access.

### O. HASH

TOE must ensure that passwords stored in the database are hashed with PBKDF2 [RFC2898] algorithm with NumberOfIterations: 25 and Salt Bit Length: 128 hashing.

### O. COMMUNICATION

The TOE must ensure the user data and TSF data going across the components (between TOE components or other components) is protected from disclosure and integrity deprivation.

### O. MANAGEMENT

TOE must provide necessary management functions in order to TOE Admins manage the system securely and effectively.

## SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT



### OE. SECURITY

Security objectives for the operational environment shall provide physical security of the IT entities within the domain. Unauthorized entries and exits to and from this environment need to be blocked.

### OE. TAKING BACKUPS OF DATA

Any data generated by the TOE and/or its users are backed up regularly.

### OE.WEB APPLICATION FIREWALL

The TOE environment has a web application firewall and runs on an operating system that has no security flaw.

### OE. ADMIN

TOE Admins are competent, not hostile, and appropriately trained. TOE installation, configuration and operation are performed correctly by TOE Admins as specified in the guidance documents.

### OE. RELIABLE TIME STAMP

The TOE environment provides reliable timestamps.

## SECURITY OBJECTIVE RATIONALE

The following table demonstrates that all security objectives trace back to the threats, OSPs and assumptions in the security problem definition:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **O. IDENTIFICATION & AUTHENTICATION** | **O. AUDIT** | **O. ACCESS** | **O. HASH** | **O. COMMUNICATION** | **O. MANAGEMENT** | **OE. SECURITY** | **OE. TAKING BACKUPS OF DATA** | **OE. WEB APPLICATION FIREWALL** | **OE. ADMIN** | **OE. RELIABLE TIME STAMP** |
| **THREATS** | T. UNAUTHORIZED ACCESS |  |  |  | X |  |  |  |  |  |  |  |
| T. DENIAL OF SERVICE (DOS) |  |  |  |  |  |  |  |  | X |  |  |
| T. MODIFY AUDIT |  | X |  |  |  |  |  |  |  |  |  |
| T. COMMUNICATION |  |  |  |  | X |  |  |  |  |  |  |
| **OS POLICY** | P. SECURITY |  |  |  |  |  |  | X |  | X |  |  |
| P. SECURE COMMUNICATION |  |  |  |  | X |  |  |  |  |  |  |
| P. MAINTENANCE |  |  |  |  |  | X |  |  |  |  |  |
| **ASSUMPTIONS** | A. PROPER ADMIN |  |  |  |  |  |  |  |  |  | X |  |
| A. PROPER SERVICE USER |  |  |  |  |  |  |  |  |  | X |  |
| A. ENVIRONMENT SECURITY- ENVSEC |  |  |  |  |  |  |  |  | X |  |  |
| A. PHYSICAL |  |  |  |  |  |  | X |  |  |  |  |
| A. RELIABLE TIME STAMP |  |  |  |  |  |  |  |  |  |  | X |

*Table 3 SECURITY OBJECTIVE RATIONALE*

|  |  |  |
| --- | --- | --- |
| THREATS | SECURITY OBJECTIVES | RATIONALE |
| **T. UNAUTHORIZED\_ACCESS** | *O. HASH* | O. HASH objective ensures that user passwords are not stored in clear text. |
| **T. DISABLING USER LOGIN LOGOUT LOG RECORDS** | *O. AUDIT* | *O. AUDIT* objective that necessary measures are taken in case of log storage is full |
| **T. INFORMATION** | *O. AUDIT*  *O. ACCESS*  *O. MANAGEMENT* | *O. AUDIT* objective ensures that all operations related with accessing to system functionalities and security be audited.  *O. ACCESS* objective ensures that the TOE restricts access to the TOE objects only authorized users.  *O. MANAGEMENT* objective ensures TOE provides the tools necessary for the TOE Admins to manage the security‐related functions and that those tools are usable only by users with appropriate authorizations |
| **T. DATA\_CHANGE** | *O. IDENTIFICATION & AUTHENTICATION*  *O. AUDIT* | *O. IDENTIFICATION & AUTHENTICATION* objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions**.**  *O. AUDIT* objective ensures that all operations related with accessing to system functionalities and security be audited. |
| **T. BRUTE\_FORCE** | *O. IDENTIFICATION & AUTHENTICATION* | *O. IDENTIFICATION & AUTHENTICATION* objective ensures that the login attempts are limited. |
| **T. DENIAL\_OF\_SERVICE(DOS)** | *OE. WEB APPLICATION FIREWALL* | *OE. WEB\_APPLICATION\_FIREWALL* objective ensures that the TOE to protect from Internet threats and malicious attacks. |
| **T. MODIFY AUDIT** | *O. AUDIT* | O. AUDIT objective ensures that all operations related with accessing to system functionalities and security be audited. |
| **T. COMMUNICATION** | *O. COMMUNICATION* | *O. COMMUNICATION* objective ensures that the user data and TSF data going across the components (between TOE components or other components) is protected from disclosure and integrity deprivation. |

|  |  |  |
| --- | --- | --- |
| OS POLICY | SECURITY OBJECTIVES | RATIONALE |
| **P. SECURITY** | *OE. SECURITY*  *OE. WEB APPLICATION FIREWALL* | *OE. SECURITY* objectives for the operational environment shall provide physical security of the IT entities within the domain. Unauthorized entries and exits to and from this environment need to be blocked.  *OE. WEB\_APPLICATION\_FIREWALL* objective ensures that the TOE environment have a web application firewall and OS has no security flaw. |
| **P. SECURE\_COMMUNICATION** | *O. COMMUNICATION* | *O. COMMUNICATION* objective ensures that the user data and TSF data going across the components (between TOE components or other components) is protected from disclosure and integrity deprivation. |
| **P. MAINTENANCE** | *O. MANAGEMENT* | *O. MANAGEMENT* objective ensures TOE provides the tools necessary for the TOE Admins to manage the security‐related functions and that those tools are usable only by users with appropriate authorizations |

|  |  |  |
| --- | --- | --- |
| ASSUMPTIONS | SECURITY OBJECTIVES | RATIONALE |
| **A. PROPER\_ADMIN** | *OE. ADMIN* | *OE. ADMIN* objective ensures that the TOE Admins who are managing the TOE are competent, not hostile and acts as specified in guidance documents. |
| **A. PROPER\_SERVICE\_USER** | *OE. ADMIN* | *OE. ADMIN* objective ensures that TOE Admins are trained thus do not misconfigure the service user. |
| **A. BACKUP** | *OE. TAKING BACKUPS OF DATA* | *OE. TAKING BACKUPS OF DATA* objective ensures that data produced by the TOE are backed up. |
| **A. ENVIRONMENT SECURITY- ENVSEC** | *OE. WEB APPLICATION FIREWALL* | *OE. WEB\_APPLICATION\_FIREWALL* objective ensures that the TOE environment have a web application firewall and OS has no security flaw. |
| **A. PHYSICAL** | *OE. SECURITY* | *OE. SECURITY* objectives for the operational environment shall provide physical security of the IT entities within the domain. Unauthorized entries and exits to and from this environment need to be blocked. |
| **A. RELIABLE TIME STAMP** | *OE. RELIABLE TIME STAMP* | *OE. RELIABLE TIME STAMP* objective ensures that TOE environment provides reliable time stamp. |

# EXTENDED COMPONENT DEFINITION (ASE\_ECD)

There are no extended components.

# SECURITY REQUIREMENTS (ASE\_REQ)

This chapter describes the security requirements which must be fulfilled by the TOE. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of CC. The following notations are used:

* **Assignment:** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using **bolded text** and are surrounded by square brackets as follows [**assignment**].
* **Selection:** The selection operation allows the specification of one or more items from a list. Selections are depicted using *italics text* and are surrounded by square brackets as follows [*selection*].
* **Refinement:** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using **bolded text**, for additions, and ~~strike‐through~~, for deletions.
* **Iteration:** The iteration operation allows a component to be used more than once with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.



## SECURITY FUNCTIONAL REQUIREMENTS (SFRS)

The security functional requirements (SFRs): a translation of the security objectives for the TOE into a standardized language.

The following table shows the safety functional requirements for TOE and the operations performed on components according to CC part 2.

|  |  |
| --- | --- |
| **CLASS** | **REQUIREMENT COMPONENT** |
| **FAU: SECURITY AUDIT** | FAU\_GEN.1: AUDIT DATA GENERATION |
| FAU\_GEN.2: USER IDENTITY ASSOCIATION |
| FAU\_SAR.1: AUDIT REVIEW |
| FAU\_STG.1: PROTECTED AUDIT TRAIL STORAGE |
| FAU\_STG.3: ACTION IN CASE OF POSSIBLE AUDIT DATA LOSS |
| **FCS: CRYPTOGRAPHIC SUPPORT** | FCS\_COP.1: CRYPTOGRAPHIC OPERATION |
| **FDP: USER DATA PROTECTION** | FDP\_ACC.1: SUBSET ACCESS CONTROL |
| FDP\_ACF.1: SECURITY ATTRIBUTE BASED ACCESS CONTROL |
| **FPT: PROTECTION OF THE TSF** | FPT\_ITT.1: BASIC INTERNAL TRANSFER PROTECTION |
| **FIA: IDENTIFICATION AND AUTHENTICATION** | FIA\_AFL.1: AUTHENTICATION FAILURE HANDLING |
| FIA\_UAU.2: USER AUTHENTICATION BEFORE ANY ACTION |
| FIA\_UID.2: USER IDENTIFICATION BEFORE ANY ACTION |
| **FMT: SECURITY MANAGEMENT** | FMT\_MSA.1: MANAGEMENT OF SECURITY ATTRIBUTES |
| FMT\_MSA.3: STATIC ATTRIBUTE INITIALIZATION |
| FMT\_SMF.1: SPECIFICATION OF MANAGEMENT FUNCTIONS |
| FMT\_SMR.1 SECURITY ROLES |
| **FTA: TOE ACCESS** | FTA\_SSL.1 TSF-INITIATED |
| FTA\_SSL.3 TSF-INITIATED |
| FTA\_SSL.4 USER-INITIATED |
| FTA\_TSE.1: TOE SESSION ESTABLISHMENT |
| **FTP: TRUSTED PATH/CHANNELS** | FTP\_TRP.1: TRUSTED PATH |

*Table 4 SECURITY FUNCTIONAL REQUIREMENTS (SFRS)*

### SECURITY AUDIT



#### FAU\_GEN.1: AUDIT DATA GENERATION

|  |  |
| --- | --- |
| Hierarchical to: | No other components. |
| Dependencies: | FPT\_STM.1 Reliable time stamp |
| 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*[minimum]* level of audit; and  c) [**none**]. |
| FAU\_GEN.1.2 | The TSF shall record within each audio 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, [**accessing IP**]**.** |

#### FAU\_GEN.2: USER IDENTITY ASSOCIATION

|  |  |
| --- | --- |
| Hierarchical to: | No other components. |
| Dependencies: | FAU\_GEN.1 Audit data generation  FIA\_UID.1 Timing of identification |
| FAU\_GEN.2.1 | For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event. |

#### FAU\_SAR.1: AUDIT REVIEW

|  |  |
| --- | --- |
| Hierarchical to: | No other components |
| Dependencies: | FAU\_GEN.1 Audit data generation |
| FAU\_SAR.1.1 | The TSF shall provide [**Super Admin and Program Admin**] with the capability to read [**all audit information**] from the audit records. |
| FAU\_SAR.1.2 | The TSF shall provide the audit records in a manner suitable for the user to interpret the information. |

#### FAU\_STG.1: PROTECTED AUDIT TRAIL STORAGE

|  |  |
| --- | --- |
| Hierarchical to: | No other components |
| Dependencies: | FAU\_GEN.1 Audit data generation |
| FAU\_STG.1.1 | The TSF shall protect the stored audit records in the audit trail from unauthorized deletion |
| FAU\_STG.1.2 | The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail. |

**Application Note:** Edit, update, or delete any log files from system by “any type” of users is not provided by TSF

#### FAU\_STG.3: ACTION IN CASE OF POSSIBLE AUDIT DATA LOSS

|  |  |
| --- | --- |
| Hierarchical to: | No other components |
| Dependencies: | FAU\_STG.1 Protected audit trail storage |
| FAU\_STG.3.1 | The TSF shall [**related via system interfaces any action is not allowed**] if the audit trail exceeds [**when system is full**]. |

### CRYPTOGRAPHIC SUPPORT



#### FCS\_COP.1: CRYPTOGRAPHIC OPERATION

|  |  |
| --- | --- |
| Hierarchical to: | No other components |
| Dependencies: | [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation]  FCS\_CKM.4 Cryptographic key destruction |
| FCS\_COP.1.1 | The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**PBKDF2**] and cryptographic ~~key~~ **salt** sizes [**128 bits**] that meet the following: [**RFC2898**] |

### USER DATA PROTECTION



#### FDP\_ACC.1: SUBSET ACCESS CONTROL

|  |  |
| --- | --- |
| Hierarchical to: | No other components |
| Dependencies: | FDP\_ACF.1 Security attribute-based access control |
| FDP\_ACC.1.1 | The TSF shall enforce the [**Access Control Policy**] on [**subjects: Program Admin, Super Admin, User, Service User; objects: User Data, Audit Data, Management Data, Authentication / Authorization Data; operations: Read, Delete, Modify and Create**] |

#### FDP\_ACF.1: SECURITY ATTRIBUTE BASED ACCESS CONTROL

|  |  |
| --- | --- |
| Hierarchical to: | No other components |
| Dependencies: | FDP\_ACC.1 Subset access control  FMT\_MSA.3 Static attribute initialization |
| FDP\_ACF.1.1 | The TSF shall enforce the [**Access Control Policy**] to objects based on the following:  [  **Subjects: Super Admin, Program Admin, User, Service User**  **Objects: User Data, Audit Data, Management Data, Authentication / Authorization Data**  **Subjects Attribute: User ID**  **Objects Attribute: 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: [**users are explicitly granted access to a function or resource if he/she belongs to a user group which has been granted access**]**.**   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | User | Object | Read | Create | Modify | Delete | | Super Admin | User Data | X | X | X | X | | Audit Data | X |  |  |  | | Management Data | X | X | X | X | | Authentication / Authorization Data | X | X | X |  | | Program Admin | User Data | X | X | X |  | | Audit Data | X |  |  |  | | Management Data | X | X | X | X | | Authentication / Authorization Data | X | X | X |  | | User | User Data | X |  | X |  | | Audit Data |  |  |  |  | | Management Data |  |  |  |  | | Authentication / Authorization Data |  |  |  |  | | Service User | User Data | X |  | X |  | | Audit Data |  |  |  |  | | Management Data |  |  |  |  | | Authentication / Authorization Data |  |  |  |  | |
| 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**] |

### PROTECTION OF THE TSF



#### FPT\_ITT.1: BASIC INTERNAL TRANSFER PROTECTION

|  |  |
| --- | --- |
| Hierarchical to: | No other components |
| Dependencies: | No dependencies |
| FPT\_ITT.1.1 | The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between separate parts of the TOE. |

### IDENTIFICATION AND AUTHENTICATION



#### FIA\_AFL.1: AUTHENTICATION FAILURE HANDLING

#### FIA\_AFL.1: AUTHENTICATION FAILURE HANDLING / USER BLOCKING

|  |  |
| --- | --- |
| Hierarchical to: | No other components. |
| Dependencies: | FIA\_UAU.1 Timing of authentication |
| FIA\_AFL.1.1 | The TSF shall detect when [*[****3****]*]unsuccessful authentication attempts occur related to [**authentication**] |
| FIA\_AFL.1.2 | When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [**disable the user for 30 minutes, this period can be manually adjusted by TOE Admins**]**.** |

#### FIA\_AFL.1: AUTHENTICATION FAILURE HANDLING / IP BLOCKING

|  |  |
| --- | --- |
| Hierarchical to: | No other components. |
| Dependencies: | FIA\_UAU.1 Timing of authentication |
| FIA\_AFL.1.1 | The TSF shall detect when [***an administrator configurable positive integer within* [0-10]**] unsuccessful authentication attemps occur related to [**authentication**]. |
| FIA\_AFL.1.2 | When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [**disable the IP and User Account for 20 minutes, this period can be manually adjusted by TOE Admins**]**.** |
|  |  |

**Application Note:** Default configurable positive integer is 8.

#### FIA\_UAU.2: USER AUTHENTICATION BEFORE ANY ACTION

|  |  |
| --- | --- |
| Hierarchical to: | FIA\_UAU.1 Timing of authentication |
| Dependencies: | FIA\_UID.1 Timing of identification |
| FIA\_UAU.2.1 | The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user |

#### FIA\_UID.2: USER IDENTIFICATION BEFORE ANY ACTION

|  |  |
| --- | --- |
| Hierarchical to: | FIA\_UID.1 Timing of identification |
| Dependencies: | No dependencies |
| FIA\_UID.2.1 | The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. |

### SECURITY MANAGEMENT



#### FMT\_MSA.1: MANAGEMENT OF SECURITY ATTRIBUTES

|  |  |
| --- | --- |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP\_ACC.1 Subset access control, or FDP\_IFC.1 Subset information flow control]  FMT\_SMR.1 Security roles  FMT\_SMF.1 Specification of Management Functions |
| FMT\_MSA.1.1 | The TSF shall enforce the [**Access Control Policy**] to restrict the ability to [ *delete*, *modify*] the security attributes [**user status**] to [**TOE Admins**]**.** |

#### FMT\_MSA.3: STATIC ATTRIBUTE INITIALIZATION

|  |  |
| --- | --- |
| Hierarchical to: | No other components |
| Dependencies: | FMT\_MSA.1 Management of security attributes  FMT\_SMR.1 Security roles |
| FMT\_MSA.3.1 | The TSF shall enforce the [**Access Control Policy**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP. |
| FMT\_MSA.3.2 | The TSF shall allow the [**Super Admin**] to specify alternative initial values to override the default values when an object or information is created. |

#### FMT\_SMF.1: SPECIFICATION OF MANAGEMENT FUNCTIONS

|  |  |
| --- | --- |
| Hierarchical to: | No other components |
| Dependencies: | No dependencies. |
| FMT\_SMF.1.1 | The TSF shall be capable of performing the following management functions: [  **Delete, Modify and Create User,**  **Read Audit Data,**  **Read, Create, Modify Management Data,**  **Read and Create Authentication and Authorization configurations**  ] |

#### 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 [**User, Service User, Program Admin, Super Admin**]. |
| FMT\_SMR.1.2 | The TSF shall be able to associate users with roles |

### TOE ACCESS



#### FTA\_SSL.1: TSF-INITIATED

|  |  |
| --- | --- |
| Hierarchical to: | No other components. |
| Dependencies: | FIA\_UAU.1 Timing of authentication |
| FTA\_SSL.1.1 | The TSF shall lock an interactive session after [**2 minutes**] by:  a) clearing or overwriting display devices, making the current contents unreadable.  b) disabling any activity of the user's data access/display devices other than unlocking the session. |
| FTA\_SSL.1.2 | The TSF shall require the following events to occur prior to unlocking the session: [**re-login**]. |

#### FTA\_SSL.3: TSF-INITIATED

|  |  |
| --- | --- |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FTA\_SSL.3.1 | The TSF shall terminate an interactive session after a [**15 minutes**] |

#### FTA\_SSL.4: USER-INITIATED

|  |  |
| --- | --- |
| 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. |

#### 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 [**status of the user**] |

### TRUSTED PATH/CHANNELS



#### 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 [*local and remote users*] 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 [*local and 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*]. |

**Application Note:** TLS **1.2** is used for secure communication.

## SECURITY ASSURANCE REQUIREMENTS (SARS)

The TOE meets the security assurance requirements for EAL4+ALC\_FLR.2. The following table is the summary for the requirements.

|  |  |
| --- | --- |
| Assurance Classes | Assurance Components |
| ADV: Development | ADV\_ARC.1 SECURITY ARCHITECTURE DESCRIPTION |
| ADV\_FSP.4 COMPLETE FUNCTIONAL SPECIFICATION |
| ADV.IMP.1 IMPLEMENTATION REPRESENTATION OF THE TSF |
| ADV\_TDS.3 BASIC MODULAR DESIGN |
| AGD: Guidance Documents | AGD\_OPE.1 OPERATIONAL USER GUIDANCE |
| AGD\_PRE.1 PREPARATIVE PROCEDURES |
| ALC: Life Cycle Support | ALC\_CMC.4 PRODUCTION SUPPORT, ACCEPTANCE PROCEDURES AND AUTOMATION |
| ALC\_CMS.4 PROBLEM TRACKING CM COVERAGE |
| ALC\_DVS.1 IDENTIFICATION OF SECURITY MEASURES |
| ALC\_FLR.2 FLAW REPORTING PROCEDURES |
| ALC\_TAT.1 WELL-DEFINED DEVELOPMENT TOOLS |
| ALC\_DEL.1 DELIVERY PROCEDURES |
| ALC\_LCD.1 DEVELOPER DEFINED LIFE-CYCLE MODEL |
| ASE: Security Target Evaluation | ASE\_CCL.1 CONFORMANCE CLAIMS |
| ASE\_ECD.1 EXTENDED COMPONENTS DEFINITION |
| ASE\_INT.1 ST INTRODUCTION |
| ASE\_OBJ.2 SECURITY OBJECTIVES |
| ASE\_REQ.2 DERIVED SECURITY REQUIREMENTS |
| ASE\_SPD.1 SECURITY PROBLEM DEFINITION |
| ASE\_TSS.1 TOE SUMMARY SPECIFICATION |
| ATE: Tests | ATE\_COV.2 ANALYSIS OF COVERAGE |
| ATE\_DPT.1 – TESTING: BASIC DESIGN |
| ATE\_FUN.1 FUNCTIONAL TESTING |
| ATE\_IND.2 INDEPENDENT TESTING – SAMPLE |
| AVA: Vulnerability Assessment | AVA\_VAN.3 –FOCUSED VULNERABILITY ANALYSIS |

*Table 5 SECURITY ASSURANCE REQUIREMENTS (SARS)*

## SECURITY REQUIREMENT RATIONALE



### SFR RATIONALE



#### SFR DEPENDENCY RATIONALE

The following table shows how the dependencies for each SFR are satisfied.

|  |  |  |
| --- | --- | --- |
| SFR | DEPENDENCY | INCLUSION |
| FAU\_GEN.1: AUDIT DATA GENERATION | FPT\_STM.1 | NO (Reliable time stamp provided by the TSF operational environment) |
| FAU\_GEN.2: USER IDENTITY ASSOCIATION | FAU\_GEN.1 FIA\_UID.1 | YES YES (FIA\_UID.2 is Hierarchical to FIA\_UID.1)) |
| FAU\_SAR.1: AUDIT REVIEW | FAU\_GEN.1 | YES |
| FAU\_STG.1: PROTECTED AUDIT TRAIL STORAGE | FAU\_GEN.1 | YES |
| FAU\_STG.3: ACTION IN CASE OF POSSIBLE AUDIT DATA LOSS | FAU\_STG.1 | YES |
| FCS\_COP.1: CRYPTOGRAPHIC OPERATION | [FDP\_ITC.1 or FDP\_ITC.2 or FCS\_CKM.1] FCS\_CKM.4 | PBKDF2 [RFC2898] is a hashing algorithm and is a one‐way function. Therefore, it does not use any key for hashing and there is no FCS\_CKM.1 and FCS\_CKM.4 involved for the function. Therefore, the dependencies are not applicable. |
| FDP\_ACC.1: SUBSET ACCESS CONTROL | FDP\_ACF.1 | YES |
| FDP\_ACF.1: SECURITY ATTRIBUTE BASED ACCESS CONTROL | FDP\_ACC.1 FMT\_MSA.3 | YES YES |
| FPT\_ITT.1: BASIC INTERNAL TSF DATA TRANSFER PROTECTION | - | - |
| FIA\_AFL.1: AUTHENTICATION FAILURE HANDLING/USER BLOCKKING | FIA\_UAU.1 | YES (FIA\_UID.2 is Hierarchical to FIA\_UID.1) |
| FIA\_AFL.1: AUTHENTICATION FAILURE HANDLING/IP Blocking | FIA\_UAU.1 | YES (FIA\_UID.2 is Hierarchical to FIA\_UID.1) |
| FIA\_UAU.2: USER AUTHENTICATION BEFORE ANY ACTION | FIA\_UAU.1 | YES (FIA\_UID.2 is Hierarchical to FIA\_UID.1) |
| FIA\_UID.2: USER IDENTIFICATION BEFORE ANY ACTION | - | - |
| FMT\_MSA.1: MANAGEMENT OF SECURITY ATTRIBUTES | [FDP\_ACC.1 or FDP\_IFC.1] FMT\_SMR.1  FMT\_SMF.1 | FDP\_ACC.1 YES YES |
| FMT\_MSA.3: STATIC ATTRIBUTE INITIALIZATION | FMT\_MSA.1  FMT\_SMR.1 | YES YES |
| FMT\_SMF.1: SPECIFICATION OF MANAGEMENT FUNCTIONS | - | - |
| FMT\_SMR.1: SECURITY ROLES | FIA\_UID.1 | YES (FIA\_UID.2 is Hierarchical to FIA\_UID.1) |
| FTA\_SSL.1: TSF-INITIATED | FIA\_UAU.1 | YES (FIA\_UAU.2 SFR is included because FIA\_UAU.2 SFR is hierarchical to FIA\_UAU.1 SFR.) |
| FTA\_SSL.3: TSF-INITIATED | - | - |
| FTA\_SSL.4: USER-INITIATED | - | - |
| FTA\_TSE.1: TOE SESSION ESTABLISHMENT | - | - |
| FTA\_TRP.1: TRUSTED PATH | - | - |

*Table 6 SFR DEPENDENCY TABLE*

#### SFR OBJECTIVE RATIONALE

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **SFR** | **O. IDENTIFICATION & AUTHENTICATION** | **O. AUDIT** | **O. ACCESS** | **O. HASH** | **O. COMMUNICATION** | **O. MANAGEMENT** |
| **FAU\_GEN.1:** |  | X |  |  |  |  |
| **FAU\_GEN.2:** |  | X |  |  |  |  |
| **FAU\_SAR.1:** |  | X |  |  |  |  |
| **FAU\_STG.1:** |  | X |  |  |  |  |
| **FAU\_STG.3:** |  | X |  |  |  |  |
| **FCS\_COP.1:** |  |  |  | X |  |  |
| **FDP\_ACC.1:** |  |  | X |  |  |  |
| **FDP\_ACF.1:** |  |  | X |  |  |  |
| **FPT\_ITT.1:** |  |  |  |  | X |  |
| **FIA\_AFL.1:/User Blocking** | X |  |  |  |  |  |
| **FIA\_AFL.1/IP Blocking** | X |  |  |  |  |  |
| **FIA\_UAU.2:** | X |  |  |  |  |  |
| **FIA\_UID.2:** | X |  |  |  |  |  |
| **FMT\_MSA.1:** |  |  |  |  |  | X |
| **FMT\_MSA.3:** |  |  |  |  |  | X |
| **FMT\_SMF.1:** |  |  |  |  |  | X |
| **FMT\_SMR.1:** |  |  | X |  |  |  |
| **FTA\_SSL.1:** |  |  | X |  |  |  |
| **FTA\_SSL.3:** |  |  | X |  |  |  |
| **FTA\_SSL.4:** |  |  | X |  |  |  |
| **FTA\_TSE.1:** |  |  | X |  |  |  |
| **FTP\_TRP.1:** |  |  |  |  | X |  |

*Table 7 SFR OBJECTIVE RATIONALE*

|  |  |
| --- | --- |
| **O. IDENTIFICATION & AUTHENTICATION** | FIA\_AFL.1/User Blocking and FIA\_AFL.1/IP Blocking defines values for some number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures. FIA\_UAU.2 confirms the authentication before any other TSF-mediated action. FIA\_UID.2, confirms identification before allowing any other TSF-mediated action. |
| **O. AUDIT** | FAU\_GEN.1 meets the objective by generating the minimum level of auditable events and specifies the list of data that shall be recorded in each record. FAU\_GEN.2 meets the objective by associate auditable events to individual user identities. FAU\_SAR.1 meets the objective by provides that the user with TOE Admin roles can view all audit information. FAU\_STG.1 meets the objective by protecting the audit trail from unauthorized deletion and modification. FAU\_STG.3 specifies actions in case the audit trail is full. |
| **O. ACCESS** | FDP\_ACC.1 identifies objects and users subject to access control policy. FDP\_ACF.1 provides rules for certain functions that can implement an access control policy. FMT\_SMR.1 manages user roles for an authentication. FTA\_SSL.1 locks the interactive session when it has not been used for a certain period of time. FTA\_SSL.3, end the session if the user has not been used for a while. FTA\_SSL.4 authorizes Users to end users their interactive session. FTA\_TSE.1 denies users' access based on user status FMT\_SMR.1 manages 4 roles. |
| **O. HASH** | FCS\_COP.1 helps to meet the objective by hashing all the passwords using PBKDF2 before they are written into the database performs. |
| **O. COMMUNICATION** | FPT\_ITT.1 ensures that the TOE protects user data from disclosure when it is transmitted between separate parts of the TOE. FTP\_TRP.1 meets the target by establishing secure channel between TOE and local/remote users. |
| **O. MANAGEMENT** | FMT\_MSA.1 encounters this objective by allowing the TOE Admins to manage the specified security attributes. FMT\_MSA.3 ensures that the default values of security attributes are restrictive in nature. FMT\_SMF.1 allows the specification of the management functions to be provided by the TOE. |

#### SAR RATIONALE

EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs. The augmentation of ALC\_FLR.2 was chosen to give greater assurance of the developer’s on-going flaw remediation processes.

# TOE SUMMARY SPECIFICATION



## SECURITY AUDIT

TOE generates audit logs of all auditable events for minimum level, start-up and shutdown of the audit functions. These logs that are associated by users are produced with a reliable time stamp provided by operational environment. TOE provides TOE Administrators with the ability to read and view all log files. TSF prevents audit logs from being modified or deleted, and TOE disables all actions if the audit store is full.

Functional Requirement Satisfied: FAU\_GEN.1, FAU\_GEN.2, FAU\_SAR.1, FAU\_STG.1, FAU\_STG.3

## CRYPTOGRAPHIC SUPPORT

The TOE performs hashing to the user passwords with PBKDF2 [RFC2898] algorithm with NumberOfIterations : 25 and Salt Bit Length: 128 of the TOE users.

Functional Requirement Satisfied: FCS\_COP.1

## IDENTIFICATION AND AUTHENTICATION

Prior to allowing access, the TOE requires User, System User, Program Admin and Super Admin to be identified and authenticated using a username and password. Before successful completion of the security function, a User or System User or Program Admin or Super Admin is unable to perform any of the relevant function. When 8 unsuccessful authentication attempts have been met, user account is blocked for 30 minutes (can be adjusted by TOE Admins). The TSF shall detect when [an administrator configurable positive integer within [0-10]] unsuccessful authentication attemps occur related to [authentication]. When the “8” [an administrator configurable positive integer within [0-10]] unsuccessful authentication attempts have been met from same IP block, IP and user account is blocked for 20 minutes (can be adjusted by TOE Admins) Once identified and authenticated, the User, System User, Program Admin and Super Admin can access the functions or resources available to their roles which is defined in Table 5 - TOE Access Control Policy.

Functional Requirement Satisfied: FIA\_AFL.1/User Blocking, FIA\_AFL.1/IP Blocking, FIA\_UAU.2, FIA\_UID.2, FDP\_ACC.1, FDP\_ACF.1

## SECURITY MANAGEMENT

TOE is capable of the following management functions: Delete, Modify and Create User, Read Audit Data, Read, Create, Modify Management Data, Read and Create Authentication and Authorization configurations (FMT\_SMF.1). Access control policy restricts the ability of deleting and modifying the user status to TOE Admins (FMT\_MSA.1). The TOE maintains four 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, Service User, Program Admin, Super Admin. The TOE does not allow to change the default values of the security attributes of the Access Control Policy except Super Admin (FMT\_MSA.3).

Functional Requirement Satisfied: FMT\_MSA.1, FMT\_MSA.3, FMT\_SMF.1, FMT\_SMR.1

## TOE ACCESS

The TSF shall lock an interactive session after within the 2 minutes and terminate the session after 15 minutes. The users are automatically logged out and returned to the login page. User must be re-login after locking process. The TOE also allows user-initiated termination of the user's own interactive session. The TOE can deny session establishment of users with disabled status.

Functional Requirement Satisfied: FTA\_SSL.1, FTA\_SSL.3, FTA\_SSL.4, FTA\_TSE.1

## TRUSTED PATH/CHANNELS

TOE communicates with local and remote users using a secure channel. This secure communication is provided with TLS **1.2.** Besides TOE prevents the disclosure and modification of TSF data when it is transmitted between separate parts of the TOE.

Functional Requirement Satisfied: FTP\_TRP.1, FPT\_ITT.1

# REFERENCES

[1] Common Criteria for Information Technology Security Evaluation Part I: Introduction and General Model; Version 3.1 Revision 5 CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation Part II: Security Functional Requirements; Version 3.1 Revision 5 CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation Part III: Security Assurance Requirements; Version 3.1 Revision 5 CCMB-2017-04-003

[4] Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, CCMB-2017-04-004