Health Informatics Software Protection Profile

TURKISH STANDARDS INSTITUTION

DECEMBER 2013

Contents

1. PP Introduction

1.1. PP Reference

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

Title	Health Informatics Software Protection Profile
Version	1.0
Publication date	
Authors	Turkish Standards Institution
Evaluation Assurance Level (EAL)	EAL2

1.2. Goal and the Scope

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

The purpose of this protection profile, which is designed to use in web-based health information systems, is to identify minimal security requirements for the software used in public and private hospitals.

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

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

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

1.3. Target of Evaluation (TOE) Overview

This section defines Target of Evaluation of the protection profile.

1.3.1. Introduction

TOE is a web-based health information management system. The web-based health information management system mentioned here refers to an application which hosts and processes all kinds of patient data and which can be accessed online.

This protection profile is a general one, which is prepared for Hospital Information Management System, Family Practice Information System, Picture Archiving and Communication System (PACS), Laboratory Information Management System, Digital Document Management System and other health informatics application software, which provides online services. Therefore, in this protection profile the security functional requirements, that are common in those applications above, have been taken into consideration.

1.3.2. TOE Type

The type of the TOE is a web-based health information systems application. In this sense TOE allows for auditing the checking in and out of the patients, examinations and reviews, and other related reports and materials. Thus, the TOE allows for reviewing the patients' medical history immediately. Additionally the TOE saves the individual information (date of birth, place of birth, blood type, etc.), contact information (Social Security Number, citizenship number, etc.) of the patient and the surgeries that the patient had before.

The TOE additionally provides basic security functions like authentication, secure communication and security management in order to provide security for the patient information.

1.3.3. Operational Environment Components

This section provides detailed description of the TOE and discusses the software and hardware components of the TOE (operational environment) and basic security and functional features of the TOE.

Since the TOE operates on a network, it interacts with the components of that network. There is a web server on which the TOE operates and this web server operates on an operating system, which operates on a hardware server.

1.3.3.1. TOE Software and Hardware Components

This section identifies peripheral software and hardware components, which interact with the TOE. Figure 1 shows how the TOE interacts with the operational environment.

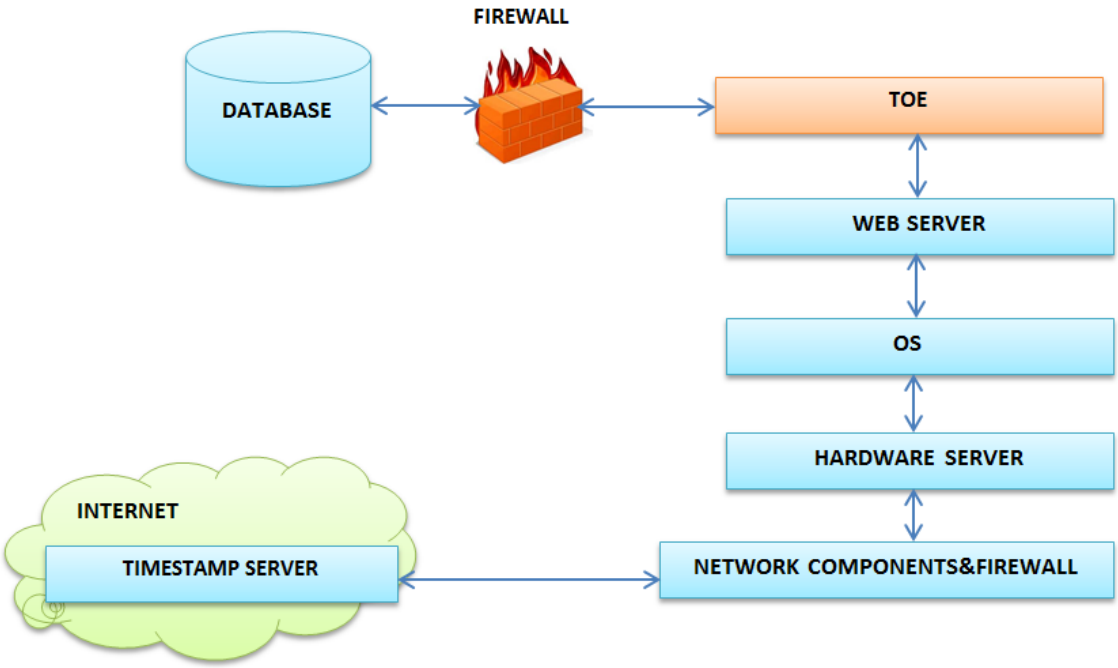

Figure 1 – The overall structure of the operational environment of the TOE

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

Operating system: The server that the TOE operates on has an operating system. The web server that the TOE operates on operates on this operating system and uses the sources of this system through this operating system.

Hardware server: The TOE operates on a server. This server may have different features from product to product.

Network components and the firewall: The TOE interacts with the network components in order to exchange patient and other related information. This interaction is carried out through the operating system and the server. Internet access of the TOE is controlled by a firewall.

Time stamp server: The TOE requires time stamp server, which is provided by operational environment in order to secure logs. This time stamp server has the feature of being electronic signature-based (which is created by the hardware).

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

1.3.4. Usage and Major Basic Security and Functional Attributes

Security related attributes of the TOE are as follows:

Authentication and authorization: It is because the TOE may operate in an Internet free environment, effective authentication and authorization processes are required to apply. Authentication is generally performed through user name and password verification. When high level of security is needed, additional authentication methods like SMS confirmation, verification through mobile devices, electronic signature, etc. could be used in addition to user name and password verification. Hash functions (in general) are applied to passwords to prevent them from reversing to the original. However it is recommended that hashing information should be saved together with the salt variant.

Access control: TOE provides access permissions to pre-authorized sources depending on the user name and the password. The data of "which users may have access to what kind of sources" is kept in the access control lists.

Auditing: TOE automatically audits logs in order to record user activities over the system assets, access control and modifications. Content of the audit logs and the method of auditing should be easily understood and configurable through a user interface. TOE stamps the logs with a time stamp to prevent them from unauthorized modification. Thus, TOE could detect unauthorized modification of the logs.

Administration: TOE provides effective control mechanisms for the users responsible for administration of the system. It is important that these mechanisms should make decision-making process easier and more effective. TOE provides system administrators authorization and data management functionalities. Only the authorized users can access interfaces provided for administration of the TOE and more strict security measures are applied to those interfaces. Roles defined as a minimum for the TOE are administrator, user and the auditor. Administrator is the role that performs functions related to the administration of the TOE. User is the role that uses the TOE within the limits of authorization. Auditor is the role that can use only auditing functions (structuring settings, reviewing the logs, etc.), which are used in audits.

Data protection: TOE keeps records of two kinds of data in general, the patient data and the user data. TOE is responsible for protecting these data. It should be noted that protection should be provided not only for saving of the data but also during the transmission of the data.

1.5. Document Overview

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

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

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

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

Part 5 identifies security requirements including functional and Assurance requirements that meets the security objectives.

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

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

2. Conformance Claims

2.1. Common Criteria Conformance Claim

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

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

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

2.2. PP Conformance Claim

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

2.3. Package Conformance Claim

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

2.4. Conformance Claim Rationale

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

2.5. Conformance Statement

This protection profile requires "strict conformance".

3. Security Problem Definition

3.1. Introduction

This section identifies security threats related to the TOE and defines actions should be taken against these threats. Other threats, which are out of the scope of the TOE, are discussed in the assumptions. These threats are assumed to avoid independent from this protection profile. Organizational security policies are discussed in this section as well.

3.2. Assets

Table 1: Assets

Definition	Explanation
D.User_Data	Individual information belonging to the users of the TOE (Name, surname, identity number, contact information and so on of the users of the TOE like physician, nurse, administrator, data entry operator, etc.)
D.Patient_Data	Sensitive information of patients processed and saved by the TOE (Type of illness, status of patient, medical intervention applied to the patient, individual information of the patient, etc.)

D.Authentication_Data	User name and password information used by the authorized users to gain access to the functionalities of the TOE
D.System_Data	Structuring data and logs hosted in the system

3.3 Threats

3.3.1. Threat Agents (Actors)

Attacker	Individual or IT entity that doesn't have user authorization but has access to the TOE through interfaces logically or physically. Attacker is malicious and has strong motives, knowledge, system resources and time to harm the system

3.3.2. Threats

T.UNAUTHORISED_ ACCESS	An unauthorized user or an attacker may try to gain access to the data that someone doesn't have access permission for. If this attacker/user gains access then he/she may compromise or modify these sensitive data **(D.Patient_Data, D.User_Data, D.Authentication_Data, D.System_Data)**. This causes exfiltration, losing confidentiality and integrity of the data. Attacker may gain unauthorized access to the TOE by exploiting vulnerabilities like unchanged user names/passwords, using simple passwords, keeping test accounts in the actual system.
T. SPOOFING	Attacker may attempt to compromise user name and password information by directing the user of the TOE to a different address. This attempt may be perform by using a bogus address or domain name or a similar interface. Directing User or System_Administrator to an address different from the address of the application and giving the impression of this address belonging to the TOE and compromising the information (**D.Authentication_Data**) that used to get access to the system by the attacker can be an example to this threat.
T.DATA_ALTERING	Unauthorized individuals can modify data being protected by the TOE without having permission. For instance, attacker can modify the data **(D.Patient_Data, D.User_Data, D.System_Data),** which is transmitted between TOE and the components of the TOE's operational environment or once the attacker has access to the data may try to disappear without a trace by modifying the logs. Preferring protocols, which are not ensuring data integrity, makes it easy for this threat being realized.
T.DATA_ COMPROMISING	This kind of threat is compromising the user **(D.User_Data)** and the patient data **(D.Patient_Data)** without permission. For instance, having access to the content of a table or a file or monitoring open text passing over the network could be considered within this scope. Especially transmitting sensitive data without encrypting it makes it easy that this threat is being realized. These kind of threats can be easily realized from the network that the TOE operates in.
T.PRIVACY	This kind of threat is disclosing patient and user data **(D.Patient_Data and D.User_Data)** by an authorized user through using the functionalities of the

	TOE. For example, if an authorized user includes the data identifying patient's identities to a statistical report that is prepared, this can be considered within this scope. Especially saving sensitive data without encrypting it makes the threat being easily realized.
T.DENIAL_OF_SERVICE	In this threat the service provided by the TOE or the TOE system itself is made unusable or inaccessible for a period of time. For example, the attacker's constantly and heavily demands can make the TOE unanswerable. Distributed denial of service attacks, which is a kind of denial of service, should be considered separately. Even though some measures can be taken to prevent from these kinds of attacks, those measures taken in the software layer generally falls behind.
T.PRIVILAGE_ESCALATION	Privilege escalation is the situation where a limitedly authorized user gains more privileges. An attacker can access the system by using the methods related to the T.SPOOFING threat and then may become more privileged through privilege escalation. Thus, the attacker may gain access to the sensitive **D.Patient_Data** and **D.System_Data.**
T.MALICIOUS_UPDATE	The attacker may try to update the software of the TOE with malicious software. Thus, the attacker may modify **D.System_Data** and/or compromise **D.Patient_Data D.User_Data** through a covert channel**.**
T.CORRUPTING_LOGS	Attacker may deactivate the logging function (for example, by making storage space insufficient). Attacker may decrease reliability of **D.System_Data** by adding erroneous data or deleting data from the logs kept by the TOE.

3.4. Organizational Security Policies

No organizational security policy has been identified within the scope of this protection profile.

3.5. Assumptions

Assumptions made during the preparation of this protection profile are collected under three main headings:

- ✓ Assumptions related to the personnel,
- ✓ Assumptions related to the physical environment,
- ✓ Assumptions related to the connection.

3.5.1 Assumptions on Personnel

A.TRUSTED_ADMINISTRATOR	It is assumed that all users who is responsible to install, configure and operate the TOE and the IT entities in the operational environment of the TOE are experienced, trained and meet the security conditions.

3.5.2 Assumptions on Physical Environment

A.PHYSICAL_SECURITY	It is assumed that required physical and environmental security is provided for the components of the operational environment of the TOE. It is

required that entries to the room that host the server should be controlled and registered according to pre-defined authorization rules

3.5.3 Assumptions on Communications

A.SECURE_COMMUNICATION	It is assumed that the communication, which is not protected by TSF, between the TOE and remote IT systems that the TOE interacts with and the transmission between the separately located parts of the TOE and the network are protected against different kinds of threats (distributed denial of service, penetration attempts to the network, malicious software attacks, etc.). In this sense it is assumed that integrity and confidentiality of the transmitted data is provided and sources of communication end points are verified. Secure transmission is ensured on the web commonly through SSL connection and https protocol. Application note: If the TOE consist separate parts and if the TOE applies mechanisms, which provide security for the transmitted data between these parts, ST author may choose using FPT_ITT.1 to support or remove A.SECURE_COMMUNICATION.

4. Security Objectives

4.1. Introduction

This section discusses the security objectives for the TOE and the security objectives for the Operational Environment of the TOE.

Security objectives are discussed in two parts: the security objectives for the TOE (security objectives that addressed directly by the TOE) and the security objectives for the Operational Environment of the TOE (security objectives that addressed by IT environment, which are not technical).

4.2. Security Objectives for the TOE

O.AUDIT	TOE shall audit data access, access to the system functionalities and all the operations related with security, save these logs and ensure that these logs are not modified. These logs should be monitored constantly and it is allowed to review these when needed.
O.AUTHENTICATION	TOE shall ensure all pre-defined users have been defined uniquely and authenticate user identity before giving permission to access.
O.AUTHORISATION	TOE shall ensure all pre-defined users have been defined uniquely and authorized them in different levels. TOE shall check the authorization level of the user when accessing the system and allow access in accordance with this authorization.
O.DATA_FLOW_CONTROL	TOE shall control and manage unauthorized data flow in and out the system. Any data received by the TOE shall be controlled through a control mechanism.

O.MANAGEMENT	TOE shall provide all necessary means and functions in order that the users, which have administrator authorization, manage the system securely and effectively. TOE shall restrict using these means and functions against unauthorized use and take necessary precautions.
O.DATA_PROTECTION	TOE shall provide necessary security measures against that the data on the system cannot be displayed, modified or deleted.
O.PRIVACY	TOE shall provide necessary security measures against that the patients data on the system cannot be displayed and copied unnecessarily even by an authorized user.
O.ERROR_MANAGEMENT	TOE shall ensure that error management is applied and correct processes operated on the system. The TOE shall manage all possible error types and these errors should be displayed to the users in a more secure and meaningful way.
O.UPDATE	TOE shall verify manufacturer's signature on the update package and Thus, prevent unauthorized updates.

4.3. Security Objectives for the Operational Environment

OE.PHSICAL_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.TRUSTED_ADMINISTRATOR	Security objectives for the operational environment shall ensure that all authorized users have been trained as needed and meet all security requirements.
OE.CONTROL_AND_MONITOR	All entries and exits to and from the operational environment of the TOE shall be controlled and registered. These records shall be monitored constantly and it is allowed to review these records when needed.
OE.TIME_STAMP	Security objectives for the operational environment of the TOE shall ensure establishing of time stamps in order to record security related incidents sensitively. This time stamp should be digital signature-based.
OE.SECURE_COMMUNICATION	Operational environment of the TOE shall provide a secure communication environment. Taking network security precautions should do this.

4.4. Security Objectives Rationale

Security objectives rationale shows that defined security objectives are necessary, suitable and enough to deal with the security problems.

- For each threat, organizational security policy and assumption at least one security objective has been defined.
- Each security objective encompasses at least one threat, organizational security policy and assumption.

4.4.1. Security Objectives Coverage

Table 1 presents which security problem definition is encompassed by which security objective. Threats and organizational security objectives are considered together with security objectives for the TOE and security objectives for the operational environment of the TOE. Assumptions on the other hand are considered only with security objectives for the operational environment of the TOE.

Table 2:Mapping of Security Problems to Security Objectives

		Threats									Assumptions		
		T.UNAUTHORISED_ACCESS	T.SPOOFING	T.DATA_ALTERING	T.DATA_COMPROMISING	T.PRIVACY	T.DENIAL_OF_SERVICE	T.PRIVILAGE_ESCALATION	T.MALICIOUS_UPDATE	T.CORRUPTING_LOGS	A.TRUSTED_ADMINISTRATOR	A.PHYSICAL_SECURITY	A.SECURE_COMMUNICATION
Security objectives	O. AUDIT				X			X		X			
	O.VERIFICATION	X		X									
	O. AUTHORIZATION		X	X				X					
	O. DATA_FLOW_CONTROL			X	X				X				
	O. MANAGEMENT			X									
	O. DATA_PROTECTION	X		X	X			X					
	O.PRIVACY					X							
	O. ERROR_ MANAGEMENT				X			X					
	O.UPDATE								X				
Operational Environment Security Objectives	OE. PHYSICAL _SECURITY											X	
	OE. TRUSTED_ADMINISTRATOR										X		
	OE. CONTROL_AND_MONITORING											X	
	OE. TIME_STAMP			X						X			
	OE.SECURE_ COMMUNICATION						X						X

4.4.2. Rationale for the Security Objectives for the TOE

TOE SECURITY OBJECTIVE	RATIONALE
O.AUDIT	TOE ensures that all operations related with accessing to system functionalities and security be audited. It allows protecting these logs in a secure way and monitoring them when needed. TOE provides functionality for taking action when the audit log is full. Generating audit logs allows TOE to detect the identity of the attacker by using the audit data during the attacker's successive authentication attempts. Audit logs prevent security problems like spoofing by using a false identity, denying an operation or overall operations, denial of the service, blocking the system, privilege escalation without permission and malicious use of logs. Thus, this security objective provides countermeasures against T.DATA_ COMPROMISING, T.PRIVILAGE_ESCALATION, and T.CORRUPTING_LOGS threats.

0.AUTHENTICATION	This security objective ensures that the TOE is verifying the identity of the user before giving access permission. Using the user name/password queries generally performs authentication. However in some special occasions biometric systems may be used for authentication. Authentication for accessing the TOE may only be vulnerable to an external attacker's successive authentication attempts. Thus, the TOE provides a defense mechanism against external successive authentication attempts. The authentication mechanism provided by this security objective will ensure blocking unauthorized access to the system and correspondingly protecting the data integrity. Thus, this security objective provides countermeasures against T.UNAUTHORİSED_ACCESS and T.DATA_MODIFICATION.
O.AUTHORISATION	This security objective allows for authorization of the users. This is required to manage security issues. TOE allows all users to access the system, after verifying their identities, within their privileges. System administrators are to be defined in order that they take responsibility of all operations performed in the system. Thus, this security objective provides countermeasures against T.SPOOFING, T.DATA_MODIFICATION and T.PRIVILAGE_ESCALATION.
O.DATA_FLOW_CONTROL	This security objective allows for controlling data flow in and out of the system. Attacks, which may come through data flow, are detected and prevented by this way. It might be an attack in which malicious data or an unauthorized access to the web application is used. Thus, this security objective provides countermeasures against T.DATA_MODIFICATION, T.DATA_COMPROMISING and T.MALICIOUS_UPDATE.
O.MANAGEMENT	This security objective provides all kinds of means and functionalities, which are needed by the users having administrator privileges to manage the system in a secure and efficient way. Thanks to this security objective TOE's security functionality allows for keeping the data up to date. Thus, this security objective provides countermeasures against T.DATA_MODIFICATION.
O.DATA_PROTECTION	This security objective provides countermeasures for preventing TOE's security functions data from being displayed, modified and deleted by an unauthorized user. Thus, this security objective provides countermeasures against T.DATA_MODIFICATION, T.DATA_COMPROMISING T.UNAUTHORISED_ACCESS and T.PRIVILAGE_ESCALATION.
O.PRIVACY	This security objective provides countermeasures for preventing patient data on the system from being displayed and copied unnecessarily even by an authorized user. Thus, this security objective provides countermeasures against T.PRIVACY.
O.ERROR_MANAGEMENT	This security objective allows for managing all errors and presenting these errors to the users in a meaningful way without the data of security functions. Displaying the data and having unauthorized access by performing an attack right after a system gives errors is avoided through error management by this way. Thus, this security objective provides countermeasures against T.DATA_COMPROMISING and T.PRIVILAGE_ESCALATION.
O.UPDATE	Sometimes updates might be necessary for a TOE. These updates shall be performed using update packages endorsed by the supplier. TOE shall verify reliability of these packages and avoid unauthorized updates. Malicious updates, which might be performed by unauthorized entities, may harm the system integrity and cause data loss. This security objective ensures that only the updates endorsed by the supplier can be applied. Thus, this security objective provides countermeasures against T.MALICIOUS_UPDATE.

4.4.3. Rationale for the Security Objectives for the Operational Environment

OE.PHYSICAL_SECURITY	This security objective for the operational environment ensures that the TOE exists and operates in a physically secure environment. It prevents unauthorized individuals from entering in and exiting out of this environment. Thus, this security objective satisfies A.PHYSICAL_SECURITY.
OE.TRUSTED_ADMINISTRATOR	This security objective for the operational environment ensures that all users having administrator privileges have passed security controls and been selected from among experienced individuals. These users have to be trained on security as well. Thus, this security objective satisfies A. TRUSTED_ADMINISTRATOR.
OE.CONTROL_AND_MONITOR	This security objective for the operational environment ensures that all entrances and exits, in and out of the operational environment of the TOE to be recorded. It also allows these records to be protected and monitored when needed. It blocks unauthorized access to the operational environment. This security objective for the operational environment also ensures all security related accesses to the IT entities in the operational environment to be recorded. It allows these records to be protected and monitored when needed. Thus, this security objective satisfies A. PHYSICAL_SECURITY.
OE.TIME_STAMP	This security objective for the operational environment ensures recording of the time of the security related incidents sensitively enough and establishing the time stamps in order to detect modifications. Thus, this security objective provides countermeasures against T.DATA_COMPROMISING and T.PRIVILAGE_ESCALATION as well.
OE.SECURE_COMMUNICATION	This security objective for the operational environment allows the communication network of the TOE to provide a secure communication environment. Thus, this security objective satisfies A.SECURE_COMMUNICATION. A secure communication environment additionally makes the distributed denial of service attack ineffective. Thus, this security objective provides countermeasures against T.DENIAL_OF_SERVICE as well.

5. Extended Components Definition

This protection profile does not need any extended component.

6. Security Requirements and Rationale

6.1. Security Functional Requirements

6.1.1. Overview

Components encompassed by this protection profile are presented in Table 3.

Table 3: List of Security Functional Requirements Encompassed by this Protection Profile

Code	Long title
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review

FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute-based access control
FIA_AFL.1	Authentication failure handling
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.1	Timing of identification
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MTD.1	Managing TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_STM.1	Reliable time stamps
FRU_FLT.1	Degraded fault tolerance
FTA_MCS.1	Basic limitation on multiple concurrent sessions
FTA_SSL.3	TSF-initiated termination
FTA_SSL.4	User-initiated termination
FTA_TAH.1	TOE access history
FTA_TSE.1	TOE session establishment
FTP_TRP.1	Trusted path

6.1.2. Organizational Security Policies

Access control policy

Access control policy governs issues regarding to access the data saved by the web application. The details related to this policy are identified under FAU_ACC.1 and FAU_ACF.1 components.

6.1.3. Security Audit (FAU)

FAU_GEN.1	**Audit data generation**
Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 reliable time stamps.
FAU_GEN.1.1:	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [basic] level of audit; b) All authentication attempts [successful and failed];

c) Authorization and role changes of the administrator level users and,

d) [See Table-3 for the other auditable events].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: this kind of information shall be saved: session information of the subject, application parameters sent by the subject].

Application note: System_Administrator must have the chance to select events, which would be the subject of the audit. Since this requirement makes it necessary that the list of selected events to be dynamic, changing these events also requires auditing. The result of the actions performed through the TOE can be a one-digit success or failure expression as well as a wider set of results depending on the system design of the TOE. Besides that, successful and failed actions shall be monitored easily and immediately and shall be discerned automatically. All authorization attempts shall be controlled. But if the System_Administrator wants to filtrate these attempts by specific users/user groups or specific authorization methods and thus, prevent them from occupying too much space, FAU_SEL.1 should be considered to select in addition to FAU_GEN.1.2.

Application note: Date and time information provided through the server, on which the web application operates, is used as the date and time of the event. This information may have a margin for error but if this error is at a level that can be disregarded then it does not constitute a security problem.

System_Administrator is responsible for the time coordination between separate components of the TOE and the time difference between these components to be as accurate as possible.

Rationale: This component contributes the security objective O.AUDIT because it includes details about auditing.

Table 4: Auditable Events

Component	Auditable Events	Detailed Information
FAU_SAR.1	Reading of information from the audit records.	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records.	
FAU_SEL.1	Identification of the user trying modifies audit events.	
FAU_STG.3	Actions to be taken if a threshold on the audit trail are exceeded.	
FAU_STG.4	Actions to be taken in case of audit storage failure.	
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP.	Description information related to the entity
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken in this case, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	
FIA_ATD.1	Verification of user attribute definition	
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret.	Identification of

		modifications in the defined quality metrics.
FIA_UAU.2	Unsuccessful use of the authentication mechanism; All use of the authentication mechanism.	
FIA_UID.1	Unsuccessful use of the user identification mechanism, including the user identity provided; All use of the user identification mechanism, including the user identity provided.	User identity provided, the source of the attempt (e.g. node identifier connected, source address)
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided; All use of the user identification mechanism, including the user identity provided.	User identity provided, the source of the attempt (e.g. node identifier connected, source address)
FMT_MOF.1	All modifications in the behavior of the functions in the TSF.	
FMT_MSA.1	All modifications of the values of security attributes.	
FMT_MTD.1	All modifications to the values of TSF data.	
FMT_SMF.1	Use of the management functions.	
FMT_SMR.1	Modifications to the group of users that are part of a role.	
FPT_FLS.1	Failure of the TSF.	
FPT_STM.1	Setting date/time to a specific value	Old and new values of date/time
FRU_FLT.1	Any failure detected by the TSF. All TOE capabilities being discontinued due to a failure.	
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions.	
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	
FTA_SSL.4	Termination of an interactive session by the user.	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism. All attempts at establishment of a user session.	
FTP_TRP.1	Failures of the trusted path functions. Identification of the user associated with all trusted path failures, if available. All attempted uses of the trusted path functions. Identification of the user associated with all trusted path invocations, if available.	

FAU_GEN.2 **User identity association**

Hierarchical to: No hierarchical 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 causes the event.

Rationale: This component contributes the security objective O.AUDIT because it allows for associating audit data with the users.

FAU_SAR.1	**Audit review**
Hierarchical to:	No hierarchical components
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1:	The TSF shall provide [assignment: authorized users] with the capability to read [assignment: list of 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.

PP author's note: The purpose of this component is to prevent the user from the complexity of audit logs and to ensure the users to use audit logs immediately and efficiently in taking decision in case of an event. This functionality can be achieved through different means. However by taking into consideration of the purpose of this component, be sure that these means ensures accessing audit logs immediately and effectively and supporting the System_Administrator in taking decisions immediately and easily. Achieving this functionality through external tools means conformance with this component is achieved. The functionality intended with this component shall be design through considering this component together with FAU_SAR.3. The method of authorizing the users to read audit logs shall be determined and identified (e.g. defining a role for reading the audit logs or defining a separate role for reading only some of the audit logs).

Rationale: This component contributes the security objectives O.AUDIT and O.MANAGEMENT because it allows the audit logs being able to read by the users easily.

FAU_SAR.2	**Restricted audit review**
Hierarchical to:	No hierarchical components
Dependencies:	FAU_SAR.1 Audit review
FAU_SAR.2.1:	The TSF shall prohibit all users to access the audit records, except for those that have been granted explicit read-access.

Application note: It is intended with this component to block access at the application level. It is assumed that actions needed to block access at the level of operating system and storage unit have been taken.

Rationale: This component contributes the security objectives O.AUDIT and O.AUTHORISATION because it ensures that only defined users can see audit logs.

FAU_SAR.3	**Selectable audit review**
Hierarchical to:	No other components
Dependencies:	FAU_SAR.1 Audit review

FAU_SAR.3.1:	The TSF shall provide the ability to apply [assignment: methods of selection and/or ordering] of audit data, based on [assignment: criteria with logical relations].

PP author's note: The purpose of this component is to prevent the user from the complexity of audit logs and to ensure the users to use audit logs immediately and efficiently in taking decision in case of an event. This functionality can be achieved through different means. However by taking into consideration of the purpose of this component, be sure that these means ensures accessing audit logs immediately and effectively and supporting the System_Administrator in taking decisions immediately and easily. Achieving this functionality through external tools means conformance with this component is achieved.

Rationale: This component contributes the security objectives O.AUDIT and O.MANAGEMENT because it allows for presenting audit logs to the users selectively.

FAU_STG.1	**Protected audit trail storage**
Hierarchical to:	No hierarchical components
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to [detect] unauthorized modifications to the stored audit records in the audit trail.

PP author's note: The most efficient countermeasures to protect audit logs from unauthorized deletion and modification are those that can be taken at the level of operating system. It is assumed that these countermeasures had been taken precisely. On the other hand, it is possible to detect deletion and modification at the level of application. FAU_STG.1.1 intends to protect audit logs from unauthorized deletion but if one or more components of the operational environment of the TOE provide this functionality then the conformance to this component is achieved. Detection of modification of audit logs shall be fulfilled by TSF in any case.

Application note: In some cases TOE might monitor audit logs by using an external component. In this case it will be useful using a buffer storage within the TOE to preclude the possibility of the external component is inaccessible. Buffer storage used within the TOE is to comply with this component.

Rationale: This component contributes security objectives O.AUDIT and O.DATA_PROTECTION because it protects audit logs from unauthorized deleting and modifying.

FAU_STG.3	**Action in case of possible audit data loss**
Hierarchical to:	No hierarchical components
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.3.1	**Development:** The TSF shall take the decision of **[assignment: actions to be taken in case of possible audit storage failure]**, **[assignment: Informing System_Administrator through e-mail]**, **[selection: using a method of SMS or equivalent informing method, informing the users logged in with a status code]**, if **[the pre-defined limit determined by the System_Administrator]** will be **exceeded after a certain amount of time.**

Rationale: This component intends generating solutions to keep audit logs uninterruptedly. Thus, this component contributes the security objective O.AUDIT. Besides that, it contributes the security objective O.MANAGEMENT because it supports System_Administrator in event management in case of a possible breakdown.

FAU_STG.4	**Prevention of audit data loss**
Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall take the decision of [selection: "ignore audited events", "prevent audited events, except those taken by the authorized user with special rights", "overwrite the oldest stored audit records", **"creating additional space by selecting and deleting old audit records which can be considered relatively insignificant"**] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

Rationale: This component intends reducing audit data loss when the storage space allocated for audit logs became full. Thus, this component contributes security objective O.AUDIT.

6.1.4. User Data Protection (FDP)

FDP_ACC.1	**Subset access control**
Hierarchical to:	No hierarchical components
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce **access control policy** for; **1. Subjects: [assignment: user types or other subjects covered by the access control policy],** **2. Objects:** **a. Data satisfying following criteria [assignment: criteria related with data],** **b. [Assignment: other objects covered by the access control policy], in the operations among subjects and objects covered by the access control policy**.

PP author's note: The list of the interactions between subjects and objects shall include establishing a new object, removing an object, all alternative actions of accessing the object and actions on the TSF data, which is saved together with the object and related to the object (e.g. access control list associated with the object). If some of these actions have been defined in SFRs related with the management of TSF data, ST author shall provide the information needed to direct the readers of this document. If different access control mechanisms are to define for different objects, FDP_ACC.1 component shall be written for each mechanism separately to define these components.

Rationale: This component identifies data access control policy. It uses authorization-based permissions in this sense. Thus, this component contributes security objectives O.DATA_PROTECTION and O.AUTHORISATION.

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No hierarchical components
Dependencies:	FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	The TSF shall enforce access control policy over objects by taking subjects and objects into consideration; **Subject attributes;** **a) User identity, group ID that the user belongs to, roles given to the user,** **b) Roles and privileges of the user,** **c) Cross-verification code, which will ensure that the user has made the access request for the web page/method from the right source through correct procedures,** **d) Session information regarding the user and parameters sent with the request,** **e) [Assignment: Other attributes belong to the subject]** **Attributes of the object: 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: **[Operation is allowed only for the following conditions: If an access list defined for an object allows user ID, group ID that the user belongs to or the role that was given to the user to access the object].**
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the rule of the TSF **[all users having the System_Administrator role have the right to access all records and methods]**.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the **[user IDs or requests made by the IP ranges, detected that using the system maliciously]**.

Rationale: This component identifies the details of access control policy, which is defined under the component FDP_ACC.1. Thus, this component also contributes security objectives O.DATA_PROTECTION and O.AUTHORISATION.

6.1.5. Identification and Authentication (FIA)

FIA_AFL.1	**Authentication failure handling**
Hierarchical to:	No hierarchical components
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when the number of unsuccessful authentication attempts [assignment: authentication operations belongs to the TOE roles] reach a [selection: [assignment: positive integer number].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been **[selection: met]**, the TSF shall **[assignment: blocking accessing to the functions of the TOE]**.

Rationale: This component identifies the details of access control policy, which is defined under the component FDP_ACC.1. Thus, this component also contributes the security objective O.AUTHENTICATION.

FIA_ATD.1	**User attribute definition**
Hierarchical to:	No hierarchical components
Dependencies:	No dependencies
FIA_ATD.1	The TSF shall have a mechanism verifying that it satisfies **[assignment**: a) User Identity (UID), b) Authentication mechanism, used, c) Verifying information for the authentication mechanism, used, d) User identity or PIN/Password for the T.R. Electronic Identity Card, e) T.R. Electronic Identity Card number, f) Role.

Rationale: This component identifies the details of access control policy, which is defined under the component FDP_ACC.1. Thus, this component also contributes the security objective O.AUTHENTICATION.

FIA_SOS.1	**Verification of secrets**
Hierarchical to:	No hierarchical components
Dependencies:	No dependencies
FIA_SOS.1	The TSF shall have a mechanism verifying that it satisfies the following conditions **[assignment:** **Must include,**

a) **One upper case as a minimum,**
b) **One lower case as a minimum,**
c) **One number as a minimum,**
d) **One symbol as a minimum.**
e) **Shall be seven characters as a minimum.**
f) **Must not include recurring predictable strings.**

Application note: This SFR, as an authentication mechanism, is only valid when using passwords, not for T.R. Electronic Identity Cards.

Rationale: This component identifies the details of access control policy, which is defined under the component FDP_ACC.1. Thus, this component also contributes the security objective O.AUTHENTICATION.

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.

Rationale: This component identifies the details of access control policy that is defined under the component FDP_ACC.1. Thus, this component also contributes the security objective O.AUTHENTICATION.

FIA_UAU.5	**Multiple authentication mechanisms**
Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification

FIA_UAU.5.1 The TSF shall provide **[assignment:**
a) User code and password,
b) Token (including smart cards) authentication]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **[assignment: authentication mechanism defined by the Authorized Administrator]**.

Rationale: This component identifies the details of access control policy, which is defined under the component FDP_ACC.1. Thus, this component also contributes the security objective O.AUTHENTICATION.

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

FIA_UID.1.1	The TSF shall allow **[accessing the pages, functions and entities open to public by the TOE]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Rationale: This component identifies the details of access control policy that is defined under the component FDP_ACC.1. Thus, this component also contributes the security objective O.AUTHORISATION.

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.

Rationale: This component identifies the details of access control policy, which is defined under the component FDP_ACC.1. Thus, this component also contributes the security objective O.AUTHORISATION.

FIA_USB.1	**User-subject binding**
Hierarchical to:	No hierarchical components
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[assignment: user identity code (UID) User role].**
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: **[assignment: after a successful identification and authentication user name will become the user name of the user authenticated successfully]**.
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: **[assignment: no changes is allowed].**

Rationale: This component identifies the details of access control policy, which is defined under the component FDP_ACC.1. Thus, this component also contributes security objectives O.AUTHENTICATION and O.AUTHORISATION.

6.1.6. Security Management (FMT)

FMT_MOF.1	**Management of security functions behavior**
Hierarchical to:	No other components
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1 :	The TSF shall restrict the ability to **[selection: determine the behavior of, disable, enable, modify the behavior of]** the functions **[assignment: list of functions]** to **[assignment: the authorized administrators]**.

Rationale: This component allows authorized users to control security attributes. This component intends satisfying security objectives O.MANAGEMENT and O.AUDIT.

FMT_MSA.1	**Management of security attributes**
Hierarchical to:	No other components
Dependencies:	[FDR_ACC.1 Access control subset or FDP_IFC.1 Data flow control subset] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1 :	The TSF shall enforce the [assignment: **access control policy**, information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete] the security attributes [assignment: list of security attributes] to [assignment: the authorized administrators].

Rationale: This component allows authorized users to control security attributes. This may include attributes, which are for monitoring and modification of security attributes. This component intends satisfying security objectives O.MANAGEMENT and O.AUDIT.

FMT_MTD.1	**Management of TSF data**
Hierarchical to:	No other components
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1 :	The TSF shall restrict the ability to [selection: change_default, query, modify, delete] the [list of TSF data] with the [**authorized administrators**].

Rationale: This component allows users to be authorized by the TOE to manage TSF data within the defined rules. This component intends satisfying the security objective O.MANAGEMENT.

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: **[list of security management functions to be provided by the TSF, listed in Table 4]**

Rationale: This component requires TOE to determine management features. This component intends satisfying the security objective O.MANAGEMENT.

Table 5: Security Management Functions Provided by the TSF

Component*	**Management Functions**
FAU_SAR.1	Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.
FAU_SEL.1	Maintenance of the rights to view/modify the audit events.
FAU_STG.3	a) Maintenance of the threshold; b) Maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit storage failure.
FAU_STG.4	Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.
FDP_ACF.1	Managing the attributes used to make explicit access or denial based decisions.
FDP_RIP.2	The choice of when to perform residual information protection (i.e. upon allocation or reallocation) could be made configurable within the TOE.
FMT_MOF.1	Managing the group of roles that can interact with the functions in the TSF;
FMT_MSA.1	a) Managing the group of roles that can interact with the security attributes; b) Management of rules by which security attributes inherit specified values.
FMT_MTD.1	Managing the group of roles that can interact with the TSF data.
FMT_SMR.1	Managing the group of users that are part of a role.
FPT_STM.1	Management of the time.
FTA_MCS.1	Management of the maximum allowed number of concurrent user sessions by an administrator.
FTA_SSL.3	a) Specification of the time of user inactivity after which termination of the interactive

	session occurs for an individual user; b) Specification of the default time of user inactivity after which termination of the interactive session occurs.
FTA_TSE.1	Management of the session establishment conditions by the authorized administrator.
FTP_TRP.1	Configuring the actions that require trusted path, if supported.

* There is no management activity for FAU_GEN.1, FAU_GEN.2, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FDP_ACC.1, FMT_SMF.1, FPT_FLS.1, FRU_FLT.1, FTA_SSL.4, FTA_TAH.1 components.

FMT_SMR.1	**Security roles**
Hierarchical to:	No hierarchical components
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1:	The TSF shall maintain the roles, a) authorized administrator b) User, c) Auditor.
FMT_SMR.1.2:	The TSF shall be able to associate users with roles.

Rationale: This component requires defining different roles and designating these different roles to the users. This component intends satisfying security objectives O.MANAGEMENT and O.AUTHORISATION.

6.1.7. Protection of the TSF (FPT)

FPT_FLS.1	**Failure with preservation of secure state**
Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_FLS.1.1:	The TSF shall preserve a secure state when the following types of failures occur: [assignment: application errors, user faults].

Rationale: This component ensures the TOE operates properly even in the case of application and software errors. This component intends satisfying the security objective O.ERROR_MANAGEMENT.

FPT_STM.1	**Reliable time stamps**
Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_STM.1.1:	The TSF shall be able to provide reliable time stamps for itself.

Rationale: This component provides a reliable time stamp feature for management and audit features in the TOE. This component intends satisfying security objectives O.AUDIT and O.TIME_STAMP.

6.1.8. Resource Utilization (FRU)

FRU_FLT.1	**Degraded fault tolerance**
Hierarchical to:	No other components
Dependencies:	FPT_FLS.1 Failure with preservation of secure state
FRU_FLT.1.1:	The TSF shall ensure the operation of [assignment: list of TOE faults] when the following failures occur: [assignment: list of type of failures].

Rationale: This component ensures the TOE operates properly even in the case of a TSF error. This component intends satisfying the security objective O.ERROR_MANAGEMENT.

6.1.9. TOE Access (FTA)

FTA_MCS.1	**Basic limitation on multiple concurrent sessions**
Hierarchical to:	No other components
Dependencies:	FIA_UID.1 Timing of identification
FTA_MCS.1.1:	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

Rationale: TSF ensures that the number of multiple concurrent sessions that a user can establish is limited in order to establish a secure session. This component intends satisfying the security objective O.AUTHORISATION.

FTA_SSL.3	**TSF-initiated termination**
Hierarchical to:	No other components
Dependencies:	No dependencies.
FTA_SSL.3.1:	The TSF shall terminate an interactive session after a [assignment: time interval of user inactivity].

Rationale: This component provides requirements for terminating of the session by TSF at the end of a certain of a time, if the user doesn't take any action. This component intends satisfying the security objective O.AUTHORISATION.

FTA_SSL.4	**User-initiated termination**
Hierarchical to:	No other components

Dependencies:	No dependencies.
FTA_SSL.4.1 :	The TSF shall allow user-initiated termination of the user's own interactive session.

Rationale: The user is needed to have capabilities of terminating its own interacted sessions in order to terminate a secure session. This component intends satisfying the security objective O.AUTHORISATION.

FTA_TAH.1 TOE access history

Hierarchical to:	No other components
Dependencies:	No dependencies.
FTA_TAH.1.1:	Upon successful session establishment, the TSF shall display the [selection: date, time, method, location] of the last successful session establishment to the user.
FTA_TAH.1.2:	Upon successful session establishment, the TSF shall display the [selection: date, time, method, location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.
FTA_TAH.1.3:	The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

Rationale: This component allows TSF to present successful and failed access attempts of the user when the user log in. This component intends satisfying the security objective O.AUTHORISATION.

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 [assignment: location, time, number of session establishment attempts].

Rationale: This component determines in which kind of situations establishing a session by a user is not allowed. This component intends satisfying the security objective O.AUTHORISATION.

6.1.10. Trusted Paths /Channels (FTP)

FTP_TRP.1 Trusted path

Hierarchical to:	No other components

Dependencies:	No dependencies.
FTP_TRP.1.1:	The TSF shall provide a communication path between itself and [remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]].
FTP_TRP.1.2:	The TSF shall permit [the TSF, local users, 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, management functions, data transfer].

Rationale: This component ensures establishing and sustaining a secure session from the users to TSF and from the TSF to the users. Any interaction related with security requires a trusted access path. A user shall establish a trusted access path during its interaction with TSF, or the TSF shall communicate by using a trusted path. This component intends satisfying the security objective O.DATA_FLOW_CONTROL.

6.2. TOE Security Assurance Requirements

This protection profile encompasses Security Assurance Requirements written in the CC, section 3 which are applicable for the level of EAL 2. In addition it addresses the following issues:

ASE_CCL.1, defined in the CC, section 3 has been re-written as follows: All developer action elements, content and presentation elements and evaluator action elements have been prevented. However the following section has been re-written:

In determination and verification of ASE_CCL.1.10C conformance claim rationale, the requirements defined under the subtitles, “ST author’s note” (if available), in the functional security components determined by the protection profile shall be taken into consideration.

Table 6: TOE Security Assurance Requirements Components List

Assurance Class	Assurance Components	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives

	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification.
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Dependencies

Table 7 provides the dependencies of selected Functional Security Requirements, defined in the CC and how these dependencies are covered in this protection profile.

Table 7: Security Functional Requirements Dependency List

Component	Dependency	Coverage
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1 Audit review	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1 Audit review	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1 Audit data generation FMT_MTD.1 TSF Management of TSF data	FAU_GEN.1 FMT_MTD.1
FAU_STG.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.3	FAU_STG.1 Protected audit trail storage	FAU_STG.1
FAU_STG.4	FAU_STG.1 Protected audit trail storage	FAU_STG.1
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 initialization	FDP_ACC.1 FMT_MSA.1
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	-	-
FIA_SOS.1	-	
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.5	-	FIA_UID.1
FIA_UID.1	-	-
FIA_UID.2	-	-
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[FDR_ACC.1 Subset access control or Subset information flow control FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.	FDR_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Timing of identification	-
FPT_FLS.1	-	-

FPT_STM.1	-	-
FRU_FLT.1	FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1
FTA_MCS.1	FIA_UID.1 Timing of identification	FIA_UID.1
FTA_SSL.3	-	-
FTA_SSL.4	-	-
FTA_TAH.1	-	-
FTA_TSE.1	-	-
FTP_TRP.1	-	-

6.3.2. Security Assurance Requirements Dependencies

Table 8 provides the dependencies of selected Security Assurance Requirements, defined in the CC and how these dependencies are covered in this protection profile.

Table 8: Security Assurance Requirements Dependency List

Component	Dependency	Coverage
ADV_ARC.1	ADV_FSP.1 Basic functional specification ADV_TDS.1 Basic design	ADV_FSP.1 ADV_TDS.1
ADV_FSP.2	ADV_TDS.1 Basic design	ADV_TDS.1
ADV_TDS.1	ADV_FSP.2 Security-enforcing functional specification.	ADV_FSP.2
AGD_OPE.1	ADV_FSP.1 Basic functional specification	ADV_FSP.1
AGD_PRE.1	-	
ALC_CMC.2	ALC_CMS.1 TOE CM coverage	ALC_CMS.1
ALC_CMS.2	-	
ALC_DEL.1	-	
ASE_CCL.1	ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements	ASE_INT.1 ASE_ECD.1 ASE_REQ.1
ASE_ECD.1	-	
ASE_INT.1	-	
ASE_OBJ.2	ASE_SPD.1 Security problem definition	ASE_SPD.1
ASE_REQ.2	ASE_OBJ.2 Security objectives ASE_ECD.1 Extended components definition	ASE_OBJ.2 ASE_ECD.1
ASE_TSS.1	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification	ASE_INT.1 ASE_REQ.1 ADV_FSP.1
ATE_COV.1	ADV_FSP.2 Security-enforcing functional specification ATE_FUN.1 Functional testing	ADV_FSP.2 ATE_FUN.1
ATE_FUN.1	ATE_COV.1 Evidence of coverage	ATE_COV.1
ATE_IND.2	ADV_FSP.2 Security-enforcing functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 Security architecture description	ADV_ARC.1

	ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_FSP.2 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1

6.3.3. Security Functional Requirements Coverage

Table 9 presents the matching between the Functional Security Requirements and the Security objectives. Each Functional Security Requirement covers at least one security objective and each security objective is covered by at least one Functional Security Requirement.

This table also establishes sufficiency and necessity of selected Functional Security Requirements.

6.3.4. EAL Selection Rationale

In selecting the level of EAL, security requirements level that is required by the product group have been taken into consideration. EAL levels preferred for commercial products are EAL2, EAL3 and EAL4. EAL5 and above are for critical hardware IT products like smart cards.

Another factor taken into consideration in determining the EAL level is the need for update of the products covered by this protection profile. These products should be updated more frequently when compared to other product groups. Because these products are accessible through web and security threats can be changed in time. Even if the security threats do not change the need for frequent update of these products makes it necessary to select an EAL level in which it is possible to get the result fast.

Table 9: Security Functional Requirement Components

	Objectives

		O.AUDIT	O.AUTHENTICATION	O.AUTHORISATION	O.DATA_FLOW_CONTROL	O.MANAGEMENT	O.DATA_PROTECTION	O.PRIVACY	O.ERROR_MANAGEMENT	O.UPDATE
Security Functional Requirements	FAU_GEN.1	X								
	FAU_GEN.2	X								
	FAU_SAR.1	X			X					
	FAU_SAR.2	X	X							
	FAU_SAR.3	X			X					
	FAU_SEL.1	X			X					
	FAU_STG.1	X				X				
	FAU_STG.3	X			X					
	FAU_STG.4	X								
	FDP_ACC.1		X			X				
	FDP_ACF.1		X			X				
	FDP_RIP.2						X			
	FIA_AFL.1	X	X							
	FIA_SOS.1		X							
	FIA_ATD.1			X						
	FIA_UAU.2		X							
	FIA_UAU.5		X							
	FIA_UID.1		X	X						
	FIA_UID.2		X	X						
	FIA_USB.1	X	X	X						
	FMT_MOF.1	X			X					
	FMT_MSA.1	X			X					
	FMT_MTD.1				X					
	FMT_SMF.1				X					
	FMT_SMR.1		X		X					
	FPT_FLS.1						X		X	
	FPT_STM.1	X								
	FRU_FLT.1						X	X	X	
	FTA_MCS.1		X		X					
	FTA_SSL.3		X		X					
	FTA_SSL.4		X							
	FTA_TAH.1		X							
	FTA_TSE.1		X		X					
	FTP_TRP.1			X						X

References

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

Web Application Security Consortium, (online) <http://www.webappsec.org> (last access: 10 December 2013)