Electronic Document and Records Management System Protection Profile

Version 1.3.1

TURKISH STANDARDS INSTITUTION

May 2014

DEVELOPERS

Muhammed Rasit Ozdas

Feyzullah Koray Atsan

CONTRIBUTORS

Mevlut Kus

Eser Cengiz

Uluc Efe Ozturk

CONTENTS

DEFINITIONS AND ABBREVIATIONS

Assets: Entities that the owner of the TOE presumably places value upon.

Assignment: The specification of an identified parameter in a component (of the CC) or requirement.

Attack Potential: A measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation.

Authentication Data: Information used to verify the claimed identity of a user.

Authorized Administrator: An authorized user who may, in accordance with the SFRs, operation and manage Firewall.

Authorized User: A user who may, in accordance with the SFRs, perform an operation.

Class: A grouping of CC families that share a common focus.

Common Criteria (CC): The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) through the use of Protection Profiles (PPs), vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.

Component: The smallest selectable set of elements on which requirements may be based.

Dependency: A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.

Document: The term “document” is used to describe any document created, edited and stored by an end user prior to being finalised as a “record”. Document could be an electronic record in any format such as e-mails, word documents, PowerPoint presentations, PDFs, TIFs, etc.

Electronic Document Management System (EDMS): Computer system (or set of computer programs) used to track and store electronic documents. It is usually also capable of keeping track of the different versions modified by different users (history tracking).

Electronic Seal (e-Seal): A type of electronic signature, which uses the same technology with electronic signature and can be issued for organizations, rather than individuals. Electronic seal shall be seen as a supplementary of electronic signature, not an alternative.

Electronic Signature (e-Signature): Binary code that, like a handwritten signature, authenticates and executes a document and identifies the signatory. A digital signature is practically impossible to forge and cannot be sent by itself but only as a part of an electronic document or message.

Element: An indivisible statement of security need.

Evaluation Assurance Level (EAL): An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

External Entity: any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Family: A grouping of components that share a similar goal but may differ in emphasis or rigor.

Identity: A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Iteration: The use of the same component to express two or more distinct requirements.

Metadata: This is information about documents or records. It is either automatically generated when a document is created or it may require the user to fill in some fields. For example the metadata for a word document might include title, author, date created etc.

Object: A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Operation (on a component of the CC): Modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection.

Operation (on an object): A specific type of action performed by a subject on an object.

Organizational Security Policy (OSP): A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.

Protection Profile (PP): An implementation-independent statement of security needs for a TOE type.

Qualified Certificate: Qualified Certificate that is suitable with electronic signatures law of Turkey (Electronic Signature Law numbered 5070).

Record: Document that memorializes and provides objective evidence of activities performed, events occurred, results achieved, or statements made. Records are created/received by an organization in routine transaction of its business or in pursuance of its legal obligations. A record may consist of two or more documents.

Records Management: The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records. It includes processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Refinement: The addition of details to a component.

Role: A predefined set of rules establishing the allowed interactions between a user and the TOE.

Security Assurance Requirement (SAR): descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality.

Security Functional Requirement (SFR): Specification of individual security functions which may be provided by a product.

Security Function Policy (SFP): A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.

Security Target (ST): An implementation-dependent statement of security needs for a specific identified TOE.

Selection: The specification of one or more items from a list in a component.

Subject: An active entity in the TOE that performs operations on objects.

Target Of Evaluation (TOE): A set of software, firmware and/or hardware possibly accompanied by guidance.

Threat Agent: An unauthorized user that brings assets under such threats as illegal access, modification or deletion.

TOE Security Functionality (TSF): A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

TSF Data: Data created by and for the TOE, that might affect the operation of the TOE.

Turkish Standards Institution (Türk Standardları Enstitüsü - TSE): TSE has been established by the law numbered 132 dated 18.11.1960 for the purpose of preparing standards for every kind of item and products together with procedure and service. The Institute is responsible to the Prime Ministry. The Institute is a public founding which is conducted according to the special rules of law and has a juristic personality. Its abbreviation and trademark is TSE.

User: See definition of “external entity”

Workflow: Automation of business processes, in whole or in part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules.

1. PROTECTION PROFILE INTRODUCTION

1.1. REFERENCE

Reference information of this protection profile is shown in the table below.

Protection Profile Name	Electronic Document and Records Management System Protection Profile
Document Version	1.3.1
Publication Date	2014-07-24
Conforming CC Version	CC v3.1 Revision 4
Conforming EAL	EAL 2+. In addition to EAL 2 components, ALC_FLR.1 (Basic flaw remediation) and ALC_LCD.1 (Developer defined life-cycle model) components are added.
Keywords	Electronic Document and Records Management, Records Management, Electronic Document Management, EDRM, EDRMS, EDMS.

1.2. DEFINITION OF AIMS AND SCOPE

In National Cyber Security Strategy and Action Plan, which went in effect by being published Turkish Official Gazette dated 06/20/2013 and numbered 28683, in the direction of Council of Ministers Decision numbered 2013/4890, TSE was assigned to preparing national standards in the field of information security. Within this scope, National Cyber Security Specialists Committee has been formed under the administration of TSE and standards and guidance documents have been prepared in many technical topics. This protection profile is one of the outputs of these efforts. All outputs of National Cybersecurity Specialists Committee are listed under http://bilisim.tse.org.tr (turkish).

This protection profile conforms to Turkish standard numbered 13298, named “Electronic Records Management”, which defines processes, procedures and quality metrics for records. This protection profile should be seen as a complementary effort to 13298 Standard.

This protection profile is based on “Web Application Protection Profile”, which is another output of the aforementioned Committee. Electronic document and records management systems (EDRMS) are a type of web applications, therefore all threats within the scope of web applications are also valid for EDRMS. Besides, EDRMS require additional security measures like communication security, integrity and confidentiality of documents and records, etc. Hence, in this protection profile, related parts of the “Web Application Protection Profile” has been adapted to EDRMS to fulfill its needs. In order to conform to this protection profile, there is no need to conform to web application protection profile, since both works are presented as standalone works.

This protection profile addresses moderate security issues. It ignores some time-consuming and/or expensive security measures to ensure that the protection profile can be harmonized with dynamic nature of the web environment and to shorten the certification period to comply to adapt to business environment. Similarly, a relatively low level of EAL has been chosen.

In this protection profile, functionality that is shared by all EDRMSs has been taken into consideration. Features that is unique to a specific EDRMS should be addressed by Security Target (ST) authors separately.

Within the scope of this protection profile, it is assumed that EDRMS uses internet for external communication. There may be some types of EDRMSs that some parts are isolated from the internet. In such situations, either internet-enabled parts can conform to this protection profile, or all parts can conform to it to ensure high level security.

1.3. TOE OVERVIEW

In this section, Target of Evaluation (TOE) of the Protection Profile is explained.

1.3.1. USAGE OF TOE

TOE is a web-based application of electronic document and records management system. Aim of the TOE is to filter documents which are a part of the evidences of organizational processes, to protect these documents in terms of content and form and manage these documents from creation to the archival processes. Document and data security is of primary concern while the TOE performs given tasks.

TOE is used for performing following tasks about electronic documents and records:

- Registration of electronic records,
- Scanning of paper-based documents,
- definition and management of file classification plans and their elements,
- Identification of document attributes and document metadata,
- Workflow management of electronic records,
- Creation of retention plans, definition of retention criteria and periods, resolution of retention plan inconsistencies (when users enter a wrong categorization value for retention plan, high level authorized users are given permission to change retention plan categorization),
- Creation and management of archival processes,
- Performing common tasks like efficiently indexing, searching, listing, viewing, editing, printing of documents and records, as well as reporting, user management, etc.
- Providing the infrastructure for secure e-signature and electronic seal[1] features,
- Secure access control mechanisms,
- Sefely storing electronic documents,
- Document, data and system integrity,
- When needed, integration with existing paper-based systems,

TOE performs aforementioned tasks with the help of components shown in Figure 1.

1.3.2. TOE TYPE

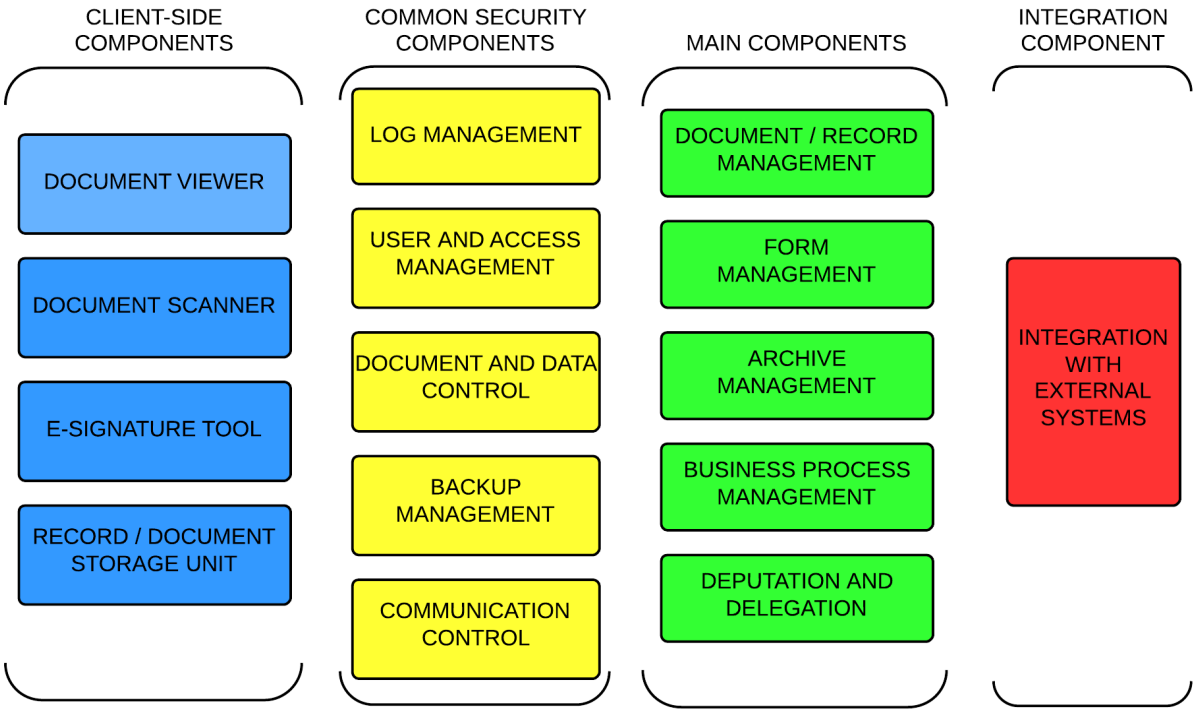
TOE type is a “web-based document and records management system application having moderate security needs”.

1.3.3. OPERATIONAL ENVIRONMENT COMPONENTS

TOE interacts with the network components, since it runs on a network. TOE runs on an operating system and this operating system runs on a server environment. TOE also interacts with storage unit/units which keeps TOE records. This storage unit is generally a relational database. In addition to these, TOE also interacts with an audit component which keeps audit records of the TOE. In the following section, these components are explained in detail.

[1] In Turkey, electronic seal is not yet officially supported as of publication date of this protection profile. Since electronic seal is an advantage for document integrity, it is recommended that EDRMSs provide the functionality to electronically seal digital documents.

Figure 1: Typical Components of an EDRMS System



1.3.4. TOE DETAILS

In this section, TOE will be explained in detail. Operational environment of the TOE, including hardware and software components, as well as main security and functional features will be addressed.

1.3.4.1. HARDWARE AND SOFTWARE OPERATIONAL ENVIRONMENT COMPONENTS

In Figure 2, hardware and software components interacting with TOE are shown. The figure depicts how TOE interacts with the operational environment.

Audit Records Unit: Similar to storage unit(s), audit records unit can reside on the same server which TOE runs on. It can be a standalone component or it can be a part of the storage unit.

Record/Document Storage: TOE is in interaction with a storage, which securely keeps all records and documents created within the TOE or imported from outside. This storage can be in database form or it can be based on file-system.

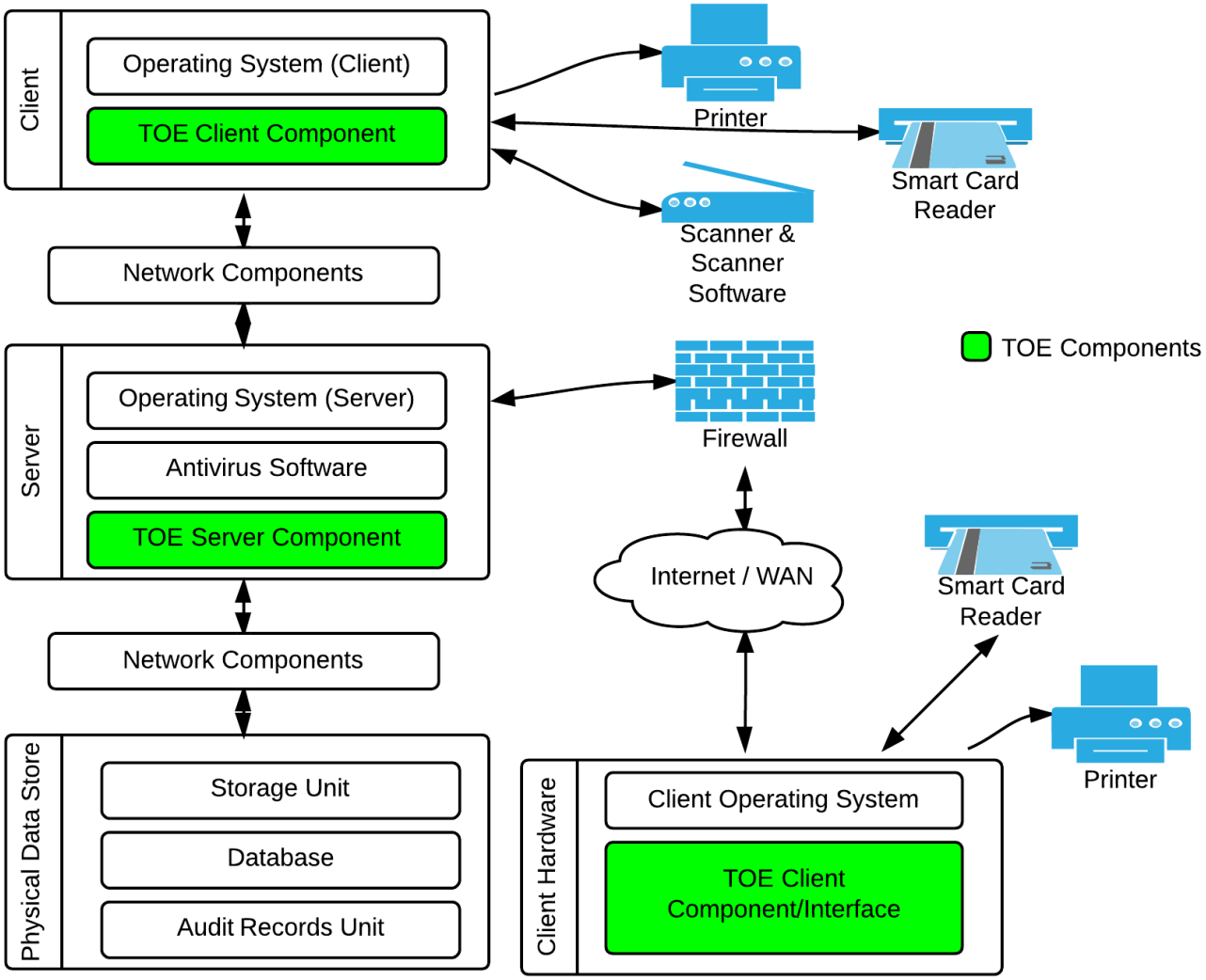
Database: TOE is in close interaction with a database for keeping its data. Records and documents can also be kept in database or can be kept separately. When a specific structured data set is needed, a query is sent to database and results are get. Commonly, TOE uses a cache mechanism to store frequently used query results for fast access.

Server: It is the main hardware component that server component of the TOE runs on. It can be physical or virtual. In both cases, security of the server is strongly related with the security of the TOE. The configuration and capability of the server can vary with respect to number of users, multiple connections, etc.

Client: Client component is the hardware and operating system that lets the users access to the TOE. This component is usually a computer. It can also be a tablet or a smart phone, but it is assumed that it is a computer within the scope of this protection profile. There are two types of client component. One type is for end users. Another type is for users that imports the records and documents into the TOE. Connection between the clients and central component of the TOE can be intranet, virtual private network or internet.

Firewall: Internet access is secured by means of this component. It can be a software and/or a hardware.

Figure 2: TOE and its Operational Environment



Network Components: TOE is in interaction with network components. This interaction is carried out by means of operating system and server. Network components can be as simple as a component to connect to the internet, or it may contain sophisticated components for advanced features. In either case, there need to be a secure network connection between client and server components of the TOE. One client of the TOE is capable of actions like printing, scanning, etc. The connection between this component and the server component is usually a local area network (LAN).

Smart Card Reader: Smart card reader holds a trusted certificate and is used for signing electronic documents. It is a hardware component. As of writing this protection profile, most common type of smart card reader is a usb token. Since this component is hardware-based and is not connected to network, it provides a higher level of security. Hence, it may be used for authentication purposes as well. Especially the authentication of explicitly authorized users will profit from this approach.

Antivirus Software: An antivirus software is used to check incoming documents and records.

Scanner and Scanner Software: Users who are authorized for scanning feature scans records and documents that are received in paper form. Scanning software scans documents and records according to the rules defined in TS 13298 Electronic Document Management Standard and then sends them to the TOE. There may be some specific features of scanning software, like OCR processing and bulk scanning, but these features will not be explained detailly, since they are not security features.

Storage Unit: Application records and documents can be stored in separate storage units or they can be stored in a single storage unit. In case they are stored separately, they can reside in the same server which TOE runs on. For simple web-based applications, it is quite often for storage units and TOE to be on the same server. On the other hand, it is recommended that TOE and storage units are separated, so that TOE is not easily affected by a potential security vulnerability in storage units.

Printer: It is the component that lets the users of the TOE to print any record or document, according to privileges given to the user.

Operating System: TOE runs on an operating system. The communication between TOE and storage unit, audit records unit, server and network components are provided by operating system.

1.3.4.2. TYPE OF USERS

Basically there are three types of users of the TOE. These are:

- Normal User
- Data Entry Operator
- System_Administrator

In addition to the roles listed above, the TOE may have additional roles. In case an additional role is needed by ST Author, it shall be listed and explained here.

Normal User: Normal user uses the TOE as a black box. Normal user is able to manage the data which is in his/her ownership. Normal user can search, list, see documents and records, only when he/she is given explicit authorization. Normal user can create a new document or record and can only delete a data/document/record if he/she is the owner of it. Normal user can archive documents and shall be able to access any archived document. TOE may send a record to national archive authority after a defined period depending on the type of the record.

Data Entry Operator: Data entry operator has the same privileges with the normal user. In addition to these, data entry operator can also register/scan/import incoming documents/records into the TOE. He/she has the needed capabilities to effectively and securely use importing tools like scanners.

System_Administrator: Administrator has explicit authorization on management of the TOE. Administrator can be one person, or there may be specific administrators for the different parts of the TOE, like database administrator, network administrator, application administrator, etc. Administrator can access the application, database, file system and other entities with all privileges.

1.3.4.3. MAIN SECURITY FEATURES OF THE TOE

Authentication and Authorization: Authorization and authentication operations should be carried out effectively. Authentication is generally carried out by means of verification of username and password. There should be restrictions on passwords to be used. If TOE needs a higher level of security, a stronger authentication mechanism or a combination of two or more authentication mechanisms may be used. Some examples of authentication mechanisms are username and password verification, SMS verification, authentication via a mobile application, e-signature, biometric verification, etc. If a strong authentication mechanism like e-signature verification is used, then verification with username and password can be omitted. Passwords are generally not stored in the storage units as plain texts, hashed passwords are used instead. It is recommended that hashing of password is more secured using variables like SALT.

Access Control: TOE has the needed capabilities to restrict access, so that only specifically authorized entities has access to TOE functions and data. For authorized users, access control is usually carried out by using authorization data. TOE may also control IP addresses of active connections, only allow for connections from pre-defined IP

addresses, allow connections for a specific time interval for critical operations, include session and cookie data to the verification process for cross-checking. If the administrator(s) of the TOE use definite communication channels or locations to access to the TOE, then some restrictions may be in place to further control access to sensitive TOE functionality.

Audit: TOE automatically collects audit records to keep track of and control user activities on assets, access control and configuration changes, specifically documents and records. Contents of audit records and record keeping methods and intervals can be configured by a TOE interface. Nobody can change or delete contents of audit records except users authorized by the TOE for these operations, including administrators. Contents of audit records can only be changed by using the functionality offered by the TOE to explicitly authorized users.

The creator of a record attaches a standard file plan to the record, which defines the category of the document (personnel assignment, meeting invitation, private analysis report, etc.). These standard file plans correspond to specific retention periods. A record having a standard file plan "meeting invitation" may be deleted after a short period, whereas a private analysis report may need a longer period. TOE shall preserve the record with all attributes and related audit records at least until the end of retention period of the record.

TOE presents audit records to the users with a human readable and clear format. TOE provides the user with ergonomic searching and filtering features, as well as reporting mechanisms to support usage of these records. Audit records related with critical operations are marked as "critical" and authorized users are informed timely via appropriate communication channels.

Management: TOE provides privileged authorized users with needed management interfaces. It is important that these interfaces ease fast and accurate decision-making during a security event. Dynamic features are favorable in terms of efficient management, but they may also become causes of security vulnerabilities if not properly restricted. Interfaces designed for the management of TOE are subject to more advanced access control mechanisms. For instance, changing a parameter about audit records is not regarded as any normal operation.

Integrity of Records and Verification of Source: Deletion or modification of any classified document is not allowed by the TOE. Within this scope, access to document and/or its metadata is restricted. Integrity of the records and verification of source is provided by e-signatures.

Backup: Backup operations on the data, documents and audit records that TOE protects can be done by the TOE itself or an external tool can be used for this purpose. Backup operations ensure that there won't be any information loss, provided that proper backup procedures are used. Backup operations provide security for intentional and unintentional data loss and/or physical damages.

Information and Document Flow Control: Maximum file size can be defined dynamically for any type of document. TOE takes care of free storage space and takes precautions against storage overflow. Incoming records and documents are subject to malicious code control. Explicitly authorized users are allowed to export any record or document.

Hashing/Encryption of Sensitive Data: Examples of sensitive data are passwords or confidential records. Sensitive data are kept on the TOE as not plain text, its hash or encrypted values are stored instead.Since some types of sensitive data like passwords don't require any recovery operation, it is better to hash them. Chosen hashing algorithm should be strong enough that original data can't be recovered with today's technology in a reasonable time-period. There is a possibility that hashes are looked up in reverse hash tables to get the original value. To prevent this, the TOE shall update its hashing algorithm as new algorithms show up.

Record Verification: Records can be transferred to another entity. If the receiving entity doesn't have an EDRMS system, then printed version of the record should be sent. This necessity requires that the TOE provides recipients a mechanism to verify digital versions of the records. This is usually done by providing a verification interface to recipients with an access code, which can be found in printed version of the record. Recipient can enter the access

code of the record to the interface provided and have access to the digital version of the record. The recipient can then verify the signature of the record. E-signature verification is made by TOE environment.

1.4. DOCUMENT OVERVIEW

In Section 1, TOE and Protection Profile are identified. With this introduction, security requirements and functions will be more easily understood.

In Section 2, conformance claims are explained. Conformance claims are Common Criteria conformance claim, Protection Profile conformance claim and EAL package conformance claim. Rationale of conformance claim and conformance statement defining type of the conformance are also explained in this chapter.

In Section 3, security problem definition is made and threats, assumptions and organizational security policies are listed to give an overall picture of the TOE with a security focus.

In Section 4, security objectives addressing threats, assumptions and organizational security policies explained in Section 3 will be explained and rationales are given accordingly.

Section 5 is supposed to explain extended components. Since this protection profile doesn't require any extended components, this section is leaved blank.

In Section 6, security requirements are explained in detail, making use of the components and assurance classes of Common Criteria Standard Part 2 and Part 3.

In the section named "References", some remarkable reference documents are cited.

2. CONFORMANCE CLAIMS

2.1. CC CONFORMANCE CLAIM

This protection profile conforms to the Common Criteria Standard, Version 3.1, Revision 4.

This protection profile is conformant to the Part 2 of the Common Criteria Standard, Version 3.1, Revision 4.

This protection profile is conformant to the Part 3 of the Common Criteria Standard, Version 3.1, Revision 4. All EAL2 level requirements are included, additionally ALC_FLR.1 (Basic flaw remediation) and ALC_LCD.1 (Developer defined life-cycle model) components are added as they are defined in Part 3 of the Standard. Evaluation Assurance Level is EAL2+.

2.2. PP CLAIM

This protection profile doesn't claim conformance to any other protection profiles.

2.3. EAL CONFORMANCE CLAIM

This protection profile is conformant to the Part 3 of the Common Criteria Standard, Version 3.1, Revision 4. All EAL2 level requirements are included, additionally ALC_FLR.1 (Basic flaw remediation) and ALC_LCD.1 (Developer defined life-cycle model) components are added as they are defined in Part 3 of the Standard. Evaluation Assurance Level is EAL2+.

2.4. CONFORMANCE RATIONALE

This part is non-applicable, since it doesn't claim any conformance to any other protection profiles.

2.5. CONFORMANCE STATEMENT

This protection profile requires "strict conformance". Strict conformance requires that ST documents which will conform to this protection profile will need to fulfill all requirements defined in Section 6 of this protection profile.

3. SECURITY PROBLEM DEFINITION

3.1. INTRODUCTION

In this section, scope and form of the possible threats, organizational security policies and assumptions for the TOE, as well as related counter-measures (security objectives) are explained.

3.2. THREATS

3.2.1. THREAT AGENTS

Attacker	Attacker is the entity that is not an authorized user of the TOE... but uses his/her/its abilities to illegally become authorized. Attacker has a bad intent, motivation, system resources and time to cause damage on the TOE. The most dangerous kind of Attackers have advanced abilities and knowledge to cause damage. Another group of Attackers have limited ability and knowledge, but they are capable of using ready-to-use software tools to attack the TOE.
Normal_User	This threat agent doesn't have management role on the TOE. Normal_User is allowed to use some functions on the TOE. Normal_User uses the TOE functionality as a black box. Although it can be said that generally Normal_User doesn't have any malicious intent when using TOE, it can be otherwise as well. This threat agent can cooperate with the Attacker or can unintentionally fall into a trap of an Attacker.
Data_Entry_Operator	This threat agent has the same privileges with the normal user. In addition to these, this agent can also register/scan/import incoming documents/records into the TOE. It is assumed that he/she has the needed capabilities to effectively and securely use importing tools like scanners. Although it can be said that generally Data_Entry_Operator doesn’t have any malicious intent when using TOE, it can be otherwise as well. This threat agent can cooperate with the Attacker or can unintentionally fall into a trap of an Attacker.

3.2.2. THREATS

T.UNAUTHORIZED_ACCESS	Attacker can make an attempt to get access to TOE by using a fake/stolen identity. This attempt can be made by using a stolen identity, a faked IP address, etc. The Attacker can get unauthorized access to the TOE by making use of security breaches like keeping default usernames and passwords unchanged, use of simple passwords, not disabling test accounts on real system, unsatisfactorily controlled uploading feature. Besides, the Attacker can benefit from residual data of a previous or an active user or residual data that is created during internal or external TOE operation and communication. These data can be a critical data about the users of the TOE or the TOE itself. Attacker can have access to these data and can ease his/her/its access to the TOE, cause damage depending on the content of the data. Attacker can also access confidential data used for authentication by misguiding System_Administrator, Data_Entry_Operator or Normal_User. For instance, Attacker can have access to confidential data by redirecting System_Administrator, Data_Entry_Operator or Normal_User to a web address which doesn't belong to TOE and make the users believe that they are protected

	by the TOE.
T.DATA_ALTERATION	Records, documents and data protected by the TOE can be modified without permission. The Attacker can misguide System_Administrator, Data_Entry_Operator or Normal_User, to obtain TSF data or data of a specific user. The Attacker can also authorize itself illegally and change records, documents and/or other data protected by the TOE. This threat generally occurs when the integrity of the records and documents is not assured. The Attacker can also try to alter audit data. This threat occur when integrity of audit data is not assured. Another occurence of this threat is modification of the source codes and audit data of the TOE by the Attacker. Inproper file permissions or insufficient control of incoming data/files may be the cause of this threat. The Attacker may get unauthorized access to the TOE by benefiting from this threat.
T.REPUDIATION	An action or a transaction (a queue of actions) made on the TOE can be repudiated. It is relatively easier to repudiate actions on the TOE when insufficient or inproper audit mechanisms exist. It is usually the last task of the Attacker on the TOE, to make sure that the System_Administrator doesn't become aware of the attacking and so doesn't have the ability to take the needed actions. Additionally the Attacker can prevent audit records to be in place (for instance, by causing an overflow in audit trail). Or the Attacker can add false / high number of records to audit trail to mislead the System_Administrator.
T.DATA_DISCLOSURE	Confidential data protected by the TOE can be disclosed without permission. For instance, Normal_User can access to a record, document or data, thathe/she is unauthorized to access. Insufficient parameter controls may cause this threat. A Normal_User or Data_Entry_Operator can intentionally or unintentionally disclose confidential information by using the functinality offered by the TOE. For instance, existence of confidential user data on statistical reports is a kind of this threat. Showing credit card information of any user along with other information in user details interface is another kind of this threat. Yet another kind of this threat is that allowing bulk export /view of user data or TSF data using TOE functionality to the users having limited privileges. Another occurence of this threat is the possibility of an Attacker to disclose TSF data by using his/her attack potential.
T.DENIAL_OF_SERVICE	The Attacker can cause the TOE to become unavailable or unusable for a period of time. This is usually done by sending too many requests in a small period of time that the TOE becomes unable to respond. Simple type of denial of service includes sending too many request from a specific IP range. This is called Denial of Service (DoS). A more advanced type of denial of service threat is Distributed Denial of Service (DDoS). For DDoS attacks, no specific IP range is used. Usually BOTNETs are used for DDoS attacks. Since there is not a restriction on incoming IP addresses, it is either hard or too expensive to distinguish between normal and malicious requests.
T.HARMFUL_DATA	The Attacker can import a harmful record, document or data into the TOE. By using this threat, the Attacker can have access the data of a specific user, can take over the account of a user or can access to a part or the whole of the TOE functionality. It is a quite common fact that when the Attacker gains access, he/she/it tries to form new ways (back doors) to access to the TOE by changing TSF parameters or parameters in working environment, by defining a new user

	account, opening an alternative port, etc. Even when the cause of the threat is cured, the Attacker may continue to access to the TOE using the back door.
T.ELEVATION_OF_PRIVILEGES	The Attacker can gain limited access to the TOE by benefiting from the threats like T.UNAUTHORIZED_ACCESS, T.HARMFUL_DATA and T.DATA_ALTERATION, and then try to gain a higher level of privilege, or a Normal_User can try to gain higher level of privilege by using his/her existing privileges. This threat is usually caused by the fact that interfaces for authorized users are not secured as strong as the interfaces not requiring an authorization.

3.3. ORGANIZATIONAL SECURITY POLICIES

P.COMPLEMENTARY_AUDIT	All events on the working environment of the TOE should be recorded, records are protected and regularly reviewed in order to detect and prevent security breaches, and also to collect the needed evidences after the breach. All audit records shall be easily monitored with minimal workload.
P.SSL_COMMUNICATION	All communication channels, which are under the control of TSF, should use SSL communication protocol.
P.PROPER_CONFIGURATION	Default configuration of the TOE and interacting components that are under the control of the TOE shall be changed, so that the Attacker can't get information about the TOE and its operational environment. Unused services shall be deactivated. Configuration parameters include (but not limited to) default root directories, default error and 404 pages, default authentication values, default usernames, default ports, default pages that reveal internal information like version number, etc. This organizational security policy is especially important when the TOE or any interacting component is widely used. By ensuring unique configuration parameters, the Attacker can be prevented from attacking with the information gained by a similar IT product.
P.E_SIGNATURE	e-Signatures that are used for electronically signing operations shall be conformant to Turkish Electronic Signature Law numbered 5070. Accordingly, signing procedures shall follow the same law.
P.RECORD_VERIFICATION	Record verification mechanism provided to recipients for printed versions of digitally signed records shall conform to the following criteria: • An access code shall exist in printed version of the records. • Digital versions of the records shall be verified by recipients. If verification result is unsuccessful, then the record shall not be accepted (since printed version is not an official record, only a pointer to digitally signed record). • Digital verification provided to the recipients shall include both e-signature and the record content. • Verification interface shall be implemented in a way that it is able to identify and prevent brute-force attacks. For example, request frequency shall be monitored, a Captcha string shall be included in the interface to detect automatic bots, etc. • Filenames of digital signatures shall not follow a pattern to prevent

record disclosure by using parameter changing.

3.4. ASSUMPTIONS

A.TRUSTED_ADMIN	It is assumed that all users responsible for installation, configuration and management of the TOE are sufficiently qualified and educated, and they are following the rules properly.
A.TRUSTED_DEVELOPER	It is assumed that people responsible for the development of the TOE (like coder, designer, etc.) are trusted entities and they follow the rules properly without any malicious intentions.
A.EXPERIENCED_DEVELOPER	It is assumed that all users developing the TOE are experienced in the field of security and they take all the needed counter-measures for all known security vulnerabilities.
A.SECURE_ENVIRONMENT	It is assumed that needed physical and environmental precautions has been taken for the working environment of the TOE. It is also assumed that access to the working environment of the TOE is properly restricted and access records are kept for a reasonable amount of time. It is also assumed that there is a mechanism to properly detect records/documents illegally taken out of the TOE. It is also assumed that proper measures has been taken against denial of service attacks.
A.PROPER_BACKUP	It is assumed that any data created or imported by the TOE, storage unit(s) and other hardware components have proper backups, so that no data loss or service interruption occurs because of a system failure.
A.COMMUNICATION	It is assumed that all communication and communication channels used by the TSF to communicate external entities, which are not under the protection of TSF, are sufficiently secured against attacks like distributed denial of service, network sniffing, etc.
A.SECURE_DELIVERY	It is assumed that all needed security measures have been taken during the delivery of the TOE. Delivery processes have been caried out by qualified and trusted entities.
A.DIST_DENIAL_OF_SERVICE	It is assumed that all needed security measures have been properly taken against Distributed Denial of Service (DDoS) attacks.

4. SECURITY OBJECTIVES

4.1. INTRODUCTION

In this section, security objectives for the TOE and its working environment are explained.

Security objectives are separated into two parts as security objectives for the TOE and security objectives for the operational environment. Security objectives for the TOE are addressed by the TSF, others are not. These security objectives define the requirements that the TOE and/or its operational environment should meet. These objectives will be mapped to security functional requirements in Section 6.

4.2. SECURITY OBJECTIVES FOR THE TOE

O.AUDIT	TOE shall record any event having value in terms of security within the scope of its ownership. TOE shall protect these records against modification and deletion. TOE shall provide explicitly authorized users the functionality to review the records easily and quickly, making it possible for System_Administrator to be timely informed about critical security events.
O.AUTH	TOE shall explicitly define every user, securely authenticate them and authorize them according to their rights and roles. All requests needing authorization shall be subject to authentication and authorization processes. The TOE shall define the rules for user authentication that forces users to have strong passwords. TOE shall allow classification of records/documents, provide the functionality to define rules with respect to record/document classification. TOE shall also offer the ability to define rights for individual records/documents. TOE shall provide a record/document level access control mechanism to individual users or groups of users. An Attacker can try to benefit from T.ELEVATION_OF_PRIVILEGE threat. To help prevent this threat, TOE shall authenticate the System_Administrator using stronger mechanisms. Examples of such mechanisms are IP-range restriction, time-period restriction, token-based authentication, multi-factor authentication, a combination of these, etc. Third party tools used by the TOE shall be configured to run at minimum authorization level possible. Default parameters of these tools shall be modified, so that they become unique and aren't affected by automatized attacks.
O.DATA_FLOW_CONTROL	TOE shall control and manage unauthorized data flow in and/or out. Data to be imported shall be subject to content filtering. A high number of requests from a definite IP range can be a signal of denial of service attack. The TOE shall provide the System_Administrator with an easily usable interface to let him/her keep the network traffic under observation and let the System_Administrator put filtering mechanisms in place if needed. Additionally, TOE shall take precautions against viewing, exporting, modifying and deleting TSF or user data without a reasonable aim, even if these operations are carried out by using the functions provided by the TOE itself.
O.DATA_INTEGRITY	TOE shall ensure data integrity for audit data and record data by detecting any modification on these data, takes needed actions when any modification occurs.
O.MANAGEMENT	TOE shall provide the System_Administrator with all the functionality to manage the system securely and effectively. TOE shall put proper access control mechanisms in place to protect management interfaces. TOE shall also ensure that its interfaces support fast and accurate decision making. TOE shall provide the System_Administrator with the ability to change rights and roles of the users, and can explicitly set rights and roles for a specific user and/or group. System_Administrator shall give the users rights and roles according to "need to know" basis.This security objective also ensures that proper protection mechanisms against Denial of Service are taken.

O.ERROR_MANAGEMENT	TOE shall offer an error management mechanism in a secure and efficient way. Errors occuring during the operation of the TOE shall be shown to the user in a secure and meaningful way. For instance, TOE shall return a general authentication failure information, not a specific one like “username is not found”. Similarly, error details with method and line of code shall not be exposed to normal users. On the other hand, System_Administrator shall be informed about critical failures in a fast and efficient way. Errors shall be detailed enough to lead the System_Administrator to suitable actions. The TOE shall preserve a secure state in case of an error occuring in the TOE itself.
O.RESIDUAL_DATA_MNG	TOE shall ensure that any residual data is removed from the TOE or made inaccessible to users when it is no longer needed.

4.3. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

OE.SECURE_ENVIRONMENT	Operational environment of the TOE shall ensure physical and environmental security of the TOE. Unauthorized access shall be restricted and all components in the operational environment shall be secured. Only specifically authorized people shall be allowed to access critical components. Operational environment of the TOE shall ensure that the TOE is properly protected against any denial of service or distributed denial of service attacks. Possible protection mechanisms include, but not limited to: • Deactivation of unused services, ports, etc. • Creation of IDS and IPS signatures • Shorter period of DNS timeout • A policy to ensure additional bandwidth to be in place in a short period of time • Static web page copies • IP address blocking and black listing • Activation of DoS protection modules that exist in web server • Using reverse proxy
OE.COMMUNICATION	Operational environment of the TOE shall provide the TOE with secure communication mediums and/or tools.
OE.TRUSTED_ADMIN	Operational environment of the TOE shall ensure that all users using the management functions of the TOE are sufficiently educated and meet the security requirements.
OE.TRUSTED_DEVELOPER	Operational environment of the TOE shall ensure that all users developing the TOE are sufficiently educated and meet the security requirements.
OE.EXPERIENCED_DEVELOPER	Operational environment of the TOE shall ensure that all users developing the TOE are experienced in the field of security and they take all the needed counter-measures for all known security vulnerabilities.
OE.COMPLEMENTARY_AUDIT	Operational environment of the TOE shall ensure that any security related event for the components other than the TOE itself is subject to audit operations. This

	operational environment security objective complements O.AUDIT security objective and does its job on the operational environment of the TOE. Audit records for the TOE are more meaningful if they are combined with the remaining audit records. Hence, all audit records shall be easily monitored with minimal workload.
OE.SECURE_DELIVERY	Delivery and installation of the TOE shall be carried out without sacrificing any security constraint. Besides, functions and/or parameters used for testing purposes shall be cleared or made inaccessible.
OE.PROPER_BACKUP	Proper backups shall be created and kept for a reasonable time for all data residing in the operational environment of the TOE. Pre-defined routines may be used for this purpose. Storage units and other hardware components shall also be backed up for the TOE to be reliable enough.

4.4. SECURITY OBJECTIVES RATIONALE

Security objectives rationale verifies that identified security objectives are necessary, suitable and sufficient for addressing security problems.

These points have been verified by security objectives rationale:

- At least one security objective is defined for each threat, organizational security policy and/or assumption.
- Each security objective is addressing at least one threat, organizational security policy and/or assumption.

Please refer to Table 1 for a general overview.

4.4.1. RATIONALE OVERVIEW

Table 1 shows the relation between security objectives and security problem definition elements (threats, OSPs and assumptions). Threats are generally addressed by security objectives for the TOE, whereas OSPs and assumptions are addressed by security objectives for the operational environment of the TOE.

Table 1: Relation Between Security Problem Definition and Security Objectives

		THREATS							OSPs					ASSUMPTIONS							
		T.UNAUTHORIZED_ACCESS	T.DATA_ALTERATION	T.REPUDIATION	T.DATA_DISCLOSURE	T.DENIAL_OF_SERVICE	T.ELEVATION_OF_PRIVILEGE	T.HARMFUL_DATA	P.COMPLEMENTARY_AUDIT	P.SSL_COMMUNICATION	P.PROPER_CONFIGURATION	P.RECORD_VERIFICATION	P.E_SIGNATURE	A.SECURE_ENVIRONMENT	A.TRUSTED_ADMIN	A.TRUSTED_DEVELOPER	A.EXPERIENCED_DEVELOPER	A.COMMUNICATION	A.PROPER_BACKUP	A.DIST_DENIAL_OF_SERVICE	A.SECURE_DELIVERY
OBJECTIVES FOR TOE	O.AUDIT			X					X												
	O.AUTH	X	X		X		X														
	O.DATA_FLOW_CONTROL		X		X	X		X		X	X	X									
	O.DATA_INTEGRITY		X										X								
	O.MANAGEMENT	X			X	X	X				X										
	O.ERROR_MANAGEMENT						X				X										
	O.RESIDUAL_DATA_MNG	X					X														
OBJECTIVES FOR OPER. ENV.	OE.SECURE_ENVIRONMENT				X	X					X			X						X	
	OE.TRUSTED_ADMIN														X						
	OE.TRUSTED_DEVELOPER															X					
	OE.EXPERIENCED_DEVELOPER	X			X												X				
	OE.COMPLEMENTARY_AUDIT								X												
	OE.COMMUNICATION									X			X					X			
	OE.PROPER_BACKUP																		X		
	OE.SECURE_DELIVERY										X										X

4.4.2. RATIONALE FOR THE TOE

O.AUDIT

O.AUDIT security objective offers an audit mechanism. This mechanism helps the System_Administrator to identify any repudiation attempt by ensuring audit records to be kept and by providing integrity of the records. This security objective addresses **T.REPUDIATION**threat. This security objective is also strongly related with **P.COMPLEMENTARY_AUDIT**, since audit mechanism of the TOE and audit mechanism of the operational environment are helping each other to solve security issues.

O.AUTH

This security objective ensures a proper authentication and authorization mechanism and therefore it is directly addressing **T.UNAUTHORIZED_ACCESS**. Besides, a strong authentication and authorization mechanism prevents data alteration. Since it is ensured that System_Administrator is subject to more advanced authentication mechanisms, this security objective is also addressing elevation of privilege threat. Therefore, this security objective addresses **T.ELEVATION_OF_PRIVILEGE**. This security objective is also in relationship with **T.DATA_ALTERATION**, since it ensures the integrity of the audit records. This security objective is also related with **T.DATA_DISCLOSURE**, since a good authentication mechanism is a means of data disclosure prevention. It is also

	related with **P.RECORD_VERIFICATION** OSP, since record verification policy introduces some measures for authentication.
O.DATA_FLOW_CONTROL	This security objective secures the communication channels and defines data control principles. Hence, it addresses **T.HARMFUL_DATA**. Since this objective tries to manage data flow, it can also detect unusual number of data flow or data requests from a specific IP range. Hence, it addresses **T.DENIAL_OF_SERVICE** threat. This security objective can prevent unauthorized access by allowing authentication data to be securely sent. It also prevents data alteration and data disclosure during transmission. This security objective addresses **T.DATA_ALTERATION** and **T.DATA_DISCLOSURE** threats as well. Besides, it is addressing **P.SSL_COMMUNICATION**, since this OSP has some restrictions on communication channels. **P.PROPER_CONFIGURATION** can also be related with this security objective, since configuration parameters help prevent unauthorized data flow. It is also related with **P.RECORD_VERIFICATION** OSP, since record verification policy introduces some measures against information disclosure.
O.DATA_INTEGRITY	This security objective ensures that the TOE is able to detect and take needed actions against any data modification on audit data and record data. This security objective addresses **T.DATA_ALTERATION** threat. Additionally, since usage of e-signatures is included in data integrity operations, this security objective also addresses **P.E_SIGNATURE** OSP.
O.MANAGEMENT	This security objective provides the System_Administrator with all needed management functions to securely manage the TOE. Provided management functions addresses issues related with authentication, authorization and data disclosure. Hence, this security objective addresses **T.UNAUTHORIZED_ACCESS**, **T.DATA_DISCLOSURE** and **T.ELEVATION_OF_PRIVILEGE**. Access Control Policy defined in management functions provide mechanisms to take needed measures against denial of service attacks. Hence, this objective addresses **T.DENIAL_OF_SERVICE** threat as well. This security objective is also related with **P.PROPER_CONFIGURATION**, since configuration management is a branch of TOE management.
O.ERROR_MANAGEMENT	This security objective supports the TOE with error management functionality. Content of error messages can be used for elevation of privilege. Hence, this security objective addresses **T.ELEVATION_OF_PRIVILEGE** threat. This security objective is also related with **P.PROPER_CONFIGURATION**, since a proper configuration helps for a better error management.
O.RESIDUAL_DATA_MNG	This security objective manages the residual data existing on the TOE. Residual data can be used for unauthorized access and elevation of privilege. It is also a kind of data disclosure. Hence, this security objective addresses **T.UNAUTHORIZED_ACCESS** and **T.ELEVATION_OF_PRIVILEGE** threats.

4.4.3. RATIONALE FOR THE OPERATIONAL ENVIRONMENT

OE.SECURE_ENVIRONMENT	This security objective for the operational environment is directly addressing **A.SECURE_ENVIRONMENT** assumption. This security objective is also related with **P.PROPER_CONFIGURATION**, since a proper configuration is a core component of a secure environment. This security objective for the operational environment also addresses **T.DATA_DISCLOSURE** and **T.DENIAL_OF_SERVICE** threats, since both threats need additional measures which are need to be taken by the operational environment of the TOE. Since proper protection against distributed denial of service attacks need precautions for operational environment, this security objective for operational environment is addressing **A.DIST_DENIAL_OF_SERVICE** assumption.
OE.TRUSTED_ADMIN	This security objective for the operational environment is directly addressing **A.TRUSTED_ADMIN** assumption.
OE.TRUSTED_DEVELOPER	This security objective for the operational environment is directly addressing **A.TRUSTED_DEVELOPER** assumption.
OE.EXPERIENCED_DEVELOPER	This security objective for the operational environment is directly addressing **A.EXPERIENCED_DEVELOPER** assumption. Besides, this security objective also addresses **T.UNAUTHORIZED_ACCESS** and **T.DATA_DISCLOSURE** threats, since an experienced developer is the only means for a high-level security in terms of access control and data protection.
OE.COMPLEMENTARY_AUDIT	This security objective for the operational environment is directly addressing **P.COMPLEMENTARY_AUDIT** organizational security policy. Since this security objective is mapped to an organizational security policy, it is evidence based. In other words, it should be proven that proper audit mechanisms exist for the operational environment of the TOE.
OE.COMMUNICATION	This security objective for the operational environment is directly addressing **A.COMMUNICATION** assumption. This security objective is also related with **P.SSL_COMMUNICATION**. Although P.SSL_COMMUNICATION is meant to secure communication channels under the control of the TSF, it has a positive impact on the security of communication channels of the operational environment. Because TOE owns / is part of some of communication channels. This security objective is also related with **P.E_SIGNATURE**, since e-signature helps some degree of reliability to the communication.
OE.PROPER_BACKUP	This security objective for the operational environment is directly addressing **A.PROPER_BACKUP** assumption.
OE.SECURE_DELIVERY	This security objective for the operational environment is directly addressing **A.SECURE_DELIVERY** assumption. This security objective is also related with **P.PROPER_CONFIGURATION**, since a proper configuration helps for the secure delivery of the TOE.

5. EXTENDED COMPONENTS DEFINITION

This protection profile does not require any extended component definitions.

6. SECURITY REQUIREMENTS

6.1. SECURITY FUNCTIONAL REQUIREMENTS

6.1.1. USED NOTATIONS

This section explains needed security functional requirements. Rewritten parts to the component definition are shown as bold text. Unchanged content are shown intact.

Notations used in this section are as follows:

“Application Note” is added when there is a need to clarify possible misunderstanding about the application of component requirements. Besides, “PP Author Note” is added when it is needed to give extra information to ST Author or to make further restrictions on the components.

After every component definition, rationale of the component has been given to improve readability.

There are some allowed operations in protection profiles, which are defined in reference documents of Common Criteria Standard. A brief explanation about the operations are explained below. For further information please refer to the reference documents.

Refinement operation (denoted in such a way that added words are in **bold text** and changed words are ~~crossed out~~): is used to add details to a requirement, and thus further restricts a requirement.

Selection operation (denoted by **bold text** starting with “selection:” and placed in square bracket): is used to select one or more options provided by the [CC] in stating a requirement.

Assignment operation (denoted by **bold text** starting with “assignment:” and placed in square bracket): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.

Iteration operation are identified with a number in round bracket (e.g. (1) , (2))

When editing security functional components, bold assignments are filled out by PP author. Those are not meant to be changed by ST author. But there are some assignments that is left to ST author. These assignments may be changed by ST author. These fields are not made bold to distinguish between remaining assignments.

6.1.2. OVERVIEW

Components included in this Protection Profile are shown in Table 2.

Table 2: List of Included Security Functional Components

Component Code	Component Name
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_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage

Component Code	Component Name
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FCS_COP.1(1)	Cryptographic operation (Audit Data and Record Data Integrity)
FCS_COP.1(2)	Cryptographic operation (Generation of Hash Values)
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.2	Full residual information protection
FDP_ITC.2	Import of user data with security attributes
FDP_ETC.2	Export of user data with security attributes
FDP_SDI.2	Stored data integrity monitoring and action
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1(1)	Management of TSF data (System_Administrator)
FMT_MTD.1(2)	Management of TSF data (Normal_User, Data Entry Operator)
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_TDC.1	Inter-TSF basic TSF data consistency
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

6.1.3. SECURITY FUNCTIONAL POLICIES

Access Control Policy

Access Control Policy is a policy that defines actions and restrictions about access to information protected by the TOE. Details about this policy can be found in the definitions of the components FDP_ACC.1 and FDP_ACF.1.

6.1.4. CLASS FAU: SECURITY AUDIT

FAU_GEN.1	**Audit data generation**
Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1:	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the **[selection: basic (**These events are listed in Table 3 below)**]** level of audit; and c) **[assignment: none]**
FAU_GEN.1.2:	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: session information of the subject, operation parameters sent by the subject via TOE interfaces]**.

Application Note: System_Administrator shall have the possibility to choose among auditable event groups/types. Since this capability requires that auditable events can be selected dynamically, any change in the list of auditable events shall be auditable as well and marked as "critical". Results of the auditable events can be a one digit indicating success/failure or can be a wider range, according to the auditing procedure provided by the TOE. On the other hand, success or failure of events shall be easily observable and automatically sortable/filterable/groupable. It is indicated that all authentication events are subject to audit, however, a more flexible approach can be chosen by using FAU_SEL.1 component.

Application Note: Date and time of the server that the TOE runs on may be used as event date and time, provided that there is no significant difference between the date and time of the server and exact date and time. There may be small amounts of time differences, but this doesn't have a remarkable effect on the security of the TOE. System_Administrator is responsible for the accuracy of the date and time of the server.

> ***Rationale:*** *This component is the main component defining the auditing requirements of the TOE. This component makes contribution to O.AUDIT security objective.*

Table 3: List of Auditable Events

Component	**Auditable Event**	**Details**
FAU_SAR.1	(basic) Reading of information from the audit records.	
FAU_SAR.2	(basic) Unsuccessful attempts to read information from the audit records.	
FAU_SEL.1	(minimal) All modifications to the audit configuration that occur while the audit collection functions are operating.	
FAU_STG.3	(basic) Actions taken due to exceeding of a threshold.	
FAU_STG.4	(basic) Actions taken due to the audit storage failure.	
FCS_COP.1(1)	(minimal) Success and failure, and the type of cryptographic operation. (basic) Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
FCS_COP.1(2)	(minimal) Success and failure, and the type of cryptographic	

Component	Auditable Event	Details
	operation. (basic) Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
FDP_ACF.1	(minimal) Successful requests to perform an operation on an object covered by the SFP. (basic) All requests (successful and unsuccessful) to perform an operation on an object covered by the SFP.	Identification data of the object.
FDP_ITC.2	(minimal) Successful import of user data, including any security attributes. (basic) All attempts to import user data, including any security attributes.	
FDP_ETC.2	(minimal) Successful export of information. (basic) All attempts to export information.	
FDP_SDI.2	(minimal) Successful attempts to check the integrity of user data, including an indication of the results of the check. (basic) All attempts to check the integrity of user data, including an indication of the results of the check, if performed.	
FIA_AFL.1	(minimal) The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	
FIA_SOS.1	(minimal) Rejection by the TSF of any tested secret; (basic) Rejection or acceptance by the TSF of any tested secret.	For example, rejection or acceptance of user password.
FIA_UAU.1	(minimal) Unsuccessful use of the authentication mechanism; (basic) All use of the authentication mechanism.	
FIA_UAU.5	(minimal) The final decision on authentication; (basic) The result of each activated mechanism together with the final decision	
FIA_UID.1	(minimal) Unsuccessful use of the user identification mechanism, including the user identity provided; (basic) All use of the user identification mechanism (successful and unsuccessful), including the user identity provided.	Provided user identity, source of attempt (identity of connected endpoint, source address, etc.)
FIA_USB.1	(minimal) Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). (basic) Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	
FMT_MOF.1	(basic) All modifications in the behaviour of the functions in the TSF.	
FMT_MSA.1	(basic) All modifications of the values of security attributes.	
FMT_MSA.3	(basic) Modifications of the default setting of permissive or restrictive rules. (basic) All modifications of the initial values of security attributes.	
FMT_MTD.1(1)	(basic) All modifications to the values of TSF data.	Especially changes in record/document access

Component	Auditable Event	Details
		rights shall be subject to audit.
FMT_MTD.1(2)	(basic) All modifications to the values of TSF data.	Especially changes in record/document access rights shall be subject to audit.
FMT_SMF.1	(minimal) Use of the management functions.	
FMT_SMR.1	(minimal) Modifications to the group of users that are part of a role;	
FPT_FLS.1	(basic) Failure of the TSF.	
FPT_TDC.1	(minimal) Successful use of TSF data consistency mechanisms. (basic) Use of the TSF data consistency mechanisms.	
FRU_FLT.1	(minimal) Any failure detected by the TSF. (basic) All TOE capabilities being discontinued due to a failure.	
FTA_MCS.1	(minimal) Rejection of a new session based on the limitation of multiple concurrent sessions.	
FTA_SSL.3	(minimal) Termination of an interactive session by the session locking mechanism.	
FTA_SSL.4	(minimal) Termination of an interactive session by the user.	
FTA_TSE.1	(minimal) Denial of a session establishment due to the session establishment mechanism. (basic) All attempts at establishment of a user session.	

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.

Rationale: *This component associates the audit records of the TOE with the users of the TOE. This component makes contribution to O.AUDIT security objective.*

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 **[assignment: System_Administrator]** with the capability to read **[assignment: all audit information]** from the audit records.
FAU_SAR.1.2:	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: When implementing the rules of this component, it should be noted that this component is in strong relationship with FAU_SAR.3 component.

> ***Rationale:*** *This component provides the users of the TOE with a human-readable interface to the audit records. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

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

Application Note: Application level access prohibition is aimed with this component. It is assumed that access restriction mechanisms for operating system and storage unit(s) are provided.

> ***Rationale:*** *This component restricts audit reviewing functionality to explicitly authorized users. This feature contributes to audit and management of the TOE. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

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 ordering]** of audit data based on **[assignment: user account, connection method, date/time, location, records/documents involved in the event (if applicable), event type, user group (if applicable), and/or criticality level of audit records]**.

> ***Rationale:*** *This components introduces an ability to TOE, with which audit records can be shown to the user in a selectable format. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

FAU_SEL.1	**Selective audit**
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FMT_MTD.1 Management of TSF data
FAU_SEL.1.1:	The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: **a) [selection: subject identity, event type]** **b) [assignment: only the least critical audit events shall be selected not to be audited]**

Rationale: *This component ensures that it is possible to manage the volume of the audit trail by allowing least critical audit events not to be audited. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

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 unauthorised deletion.
FAU_STG.1.2:	The TSF shall be able to **[selection: detect]** unauthorised modifications to the stored audit records in the audit trail.

Application Note: The most important precautions for the protection of audit records against removal or modification can be taken in operating system level. It is assumed that these precautions has been properly taken. In the software level, it is possible to "detect" any modifications or removals, but preventing is not possible. In some cases, TOE can use an external component to track and protect audit records. In such cases, it is possible that the TOE can't access to that external component. Since availability of audit records is an important functionality of the TOE, TOE shall take the needed precautions against the probability that the TOE can't access external audit recording unit.

Rationale: *This component protects audit records against unauthorized deletion. This component makes contribution to O.AUDITsecurity objective.*

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 **[assignment: use a communication channel, SMS or equivalent, inform related users via system interfaces]** if the audit trail exceeds [assignment: a pre-defined limit].

Rationale: *This component defines the actions to be taken in case of an audit data loss. It also helps System_Administrator be informed about the situation. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

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 **[selection: overwrite the oldest stored audit records]** **marked as "less important"** and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

Application Note: Importancy of an audit record can be determined by calculating the possibility that it will be of use after a period of time. Some types of records keep its importance, whereas some others may be less important after some time. Determination of the importancy of any record is made by the System_Administrator.

Rationale: *This component aims to minimize the loss in case of the fact that audit trail is full. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

6.1.5. CLASS FCS: CRYPTOGRAPHIC SUPPORT

FCS_COP.1(1)	**Cyrptographic operation (Audit Data and Record Data Integrity)**
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(1):	The TSF shall perform **[assignment: audit data and record data integrity verification]** in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

PP Author Note: Methods for ensuring audit data and record data integrity is left to ST Author. ST Author shall include additional components if they are needed for data integrity. FCS_CKM.4 component may or may not be needed, according to data integrity method chosen by the ST Author.

Rationale: *This component introduces features for audit data and record data integrity. This component makes contribution to O.DATA_INTEGRITY security objective.*

FCS_COP.1(2)	**Cyrptographic operation (Generation of Hash Values)**
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(2):	The TSF shall perform **[assignment: hash data generation]** in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes **[assignment: none]** that meet the following: [assignment: list of standards].

Application Note: Hash algorithms don't require cryptographic keys, hence no restriction has been made on assignments. FCS_CKM.1 and FCS_CKM.4 component has not been added, since it is not definite that there will be a need for cryptographic keys.

Rationale: *This component introduces features for document verification and audit integrity. This component makes contribution to O.DATA_INTEGRITY, O.AUTH and O.AUDIT security objectives.*

6.1.6. CLASS FDP: 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 **[assignment: Access Control Policy]** on **[assignment:** **a) Subjects: [assignment: System_Administrator, Normal_User, Data_Entry_Operator and other subjects included by Access Control Policy]** **b) Objects:** **a. Records, documents and metadata** **b. Data belong to or identifiying registered users** **c. Authentication data** **d. Data with these criteria:** [assignment: criteria of data] **e.** [assignment: other objects included in Access Control Policy] **].**

PP Author Note: List of operations between subjects and objects should contain creation of a new object, removal of an object, all accesses including access methods, operations on TSF data binded to the object (for instance, access control list binded to the object). If a part or all of these operations are defined in SRFs, then ST author should support the readers with sufficient explanation. If there is a need to define more than one access control policy, then ST author should FDP_ACC.1 should be repeated for every new access control policy.

> ***Rationale:*** *This component defines the information access control policy and specifies the methods of rights-based access control. This component makes contribution to O.MANAGEMENT and O.AUTH security objectives.*

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1:	The TSF shall enforce the **[assignment: Access Control Policy]** to objects based on the following: **[assignment:** **a) User identity** **b) Roles and rights of the authenticated user,** **c) Cross-check mechanism ensuring that the user uses appropriate methods from appropriate sources when requesting a web page or a method,** **d) User session information and parameters sent with the request,** **e)** [Assignment: Other attributes of the subject] **].**
FDP_ACF.1.2:	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: Operation is only allowed if Access Control List has a record that gives right to the user with User ID or associated Group ID or user's role definition to access the object]**.
FDP_ACF.1.3:	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment:** **a) Users having System_Administrator privileges have access to any records and methods provided by the TSF.** **b) Unauthorized users have access to any publicly available information**

without needing an authentication process.

c) [Assignment: other rules]

].

FDP_ACF.1.4: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment:**

a) Unexpectedly high number of requests from one or more specific IPs.

b) Authentication attempts of a specific user exceeding pre-defined treshold value.

c) Unexpectedly high number of requests coming from an authorized user

d) Multiple sessions started by the same user that exceeds pre-defined treshold value.

e) [assignment: other rules]

].

PP Author Note: Some systems may prefer to keep track of location of an authenticated user. If there is a significant change in the location of the user, then the system may require additional authentication information before authenticating the user. Since this method needs convertion of IP-ranges to location information, it is not included as an additional rule. But ST author may include this additional security feature.

Application Note: Precautions in software level are usually not enough to sufficiently prevent denial of service threats. Hence, a distinction made between DoS and DDoS threats. While some measures for DoS has been included in this protection profile, A.DIST_DENIAL_OF_SERVICE assumption is used for covering all types of denial of service attacks.

> ***Rationale:*** *This component defines the details of the access control policy defined in FDP_ACC.1. This component makes contribution to O.MANAGEMENT and O.AUTH security objectives.*

FDP_RIP.2	**Full residual information protection**
Hierarchical to:	FDP_RIP.1 Subset residual information protection
Dependencies:	No dependencies.
FDP_RIP.2.1:	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] all objects.

> ***Rationale:*** *This component aims to protect residual information on the TOE. Protection of residual information is the core feature of a residual data management mechanism. This component makes contribution to O.RESIDUAL_DATA_MNG security objective.*

FDP_ITC.2	**Import of user data with security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
	FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1:	The TSF shall enforce the **[assignment: Access Control Policy]** when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2:	The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3:	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4:	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5:	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: When importing electronic records, TOE shall verify integrity of the records by using e-signature verification]**.

Rationale: *This component aims to provide a functionality to verify imported data. This component makes contribution to O.DATA_FLOW_CONTROL and O.DATA_INTEGRITY security objectives.*

FDP_ETC.2	**Export of user data with security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1:	The TSF shall enforce the **[assignment: Access Control Policy]** when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2:	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3:	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4:	The TSF shall enforce the following rules when user data is exported from the TOE: **[assignment: System_Administrator shall restrict exporting of records, so that users of the TOE are not able to carry out an export operation without a reasonable aim]**.

Rationale: *This component aims to provide a functionality to apply some security measures for exported data. This component makes contribution to O.DATA_FLOW_CONTROL security objective.*

FDP_SDI.2	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1:	**Refinement:**The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: integrity errors] ~~on all objects~~ **record data and audit data**, based on the following attributes: **[assignment: hash of stored user data]**.
FDP_SDI.2.2:	Upon detection of a data integrity error, the TSF shall [assignment: action to be taken].

Rationale: *This component aims to provide a functionality to verify the integrity of TSF data. This component makes contribution to O.DATA_INTEGRITY security objective.*

6.1.7. CLASS FIA: IDENTIFICATION AND AUTHENTICATION

FIA_AFL.1	**Authentication failure handling**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1:	The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to **[assignment: user attempting to authenticate]**.
FIA_AFL.1.2:	When the defined number of unsuccessful authentication attempts has been **[selection: met]**, the TSF shall **[assignment: prevent access to TOE functions]**.

PP Author Note: When the defined number of unsuccessful authentication attempts has been met, it is secure to prevent the access to TOE functions. But it can easily be abused by users and may cause administrative overload. In addition to blocking access to TOE functions, the TOE may prefer to provide the user with an alternative authentication method like SMS verification, so that the user can continue to work without an interruption, without waiting for the account to be unblocked.

> ***Rationale:*** *This component protects the TOE against brute-force attacks by introducing a protection mechanism. This component makes contribution to O.AUTH security objective.*

FIA_ATD.1	**User attribute definition**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1.1:	The TSF shall maintain the following list of security attributes belonging to individual users: **[assignment:** **a) User identity code (user id) or PIN/password for Turkish Smart Identity Card** **b) Authentication method used** **c) Verification information for authentication method used** **d) Assigned roles of the user** **e) Status of the account of the user (active, passive, blocked, etc.)** **f)** [assignment: other security attributes] **]**.

> ***Rationale:*** *This component defines the security attributes belonging to the users of the TOE. Security attributes are associated with the user during Authentication phase and kept in the TOE afterwards (until the session ends or longer, depending on the design of the TOE). This component makes contribution to O.AUTH security objective.*

FIA_SOS.1	**Verification of secrets**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.1.1:	The TSF shall provide a mechanism to verify that secrets meet **[assignment:** **a) Should contain at least one uppercase letter,** **b) Should contain at least one lowercase letter,**

c) **Should contain at least one number,**
d) **Should contain at least one symbol,**
e) **Should be at least 7 characters long,**
f) **Should not contain repetitive or iterative character groups,**
g) **When changed, should not be the same as last 3 secrets.**
h) [assignment: other quality metrics]

].

PP Author Note: If the TOE prefers using stronger authentication mechanisms like Turkish Republic Smart Identity Card, e-Signature Token, Biometric Verification, etc., then this component may be fully ignored. In such situations, ST Author shall demonstrate that preferred verification mechanism provides a verification that is stronger than what is offered by this component.

> ***Rationale:*** *This component defines the rules for secrets. These rules contributes to the measures taken against unauthorized access. This component makes contribution to O.AUTH security objective.*

FIA_UAU.1	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1:	The TSF shall allow **[assignment:** **a) e-Signature verification page for the records, which is offered to the receivers of the record (they don't need to be authorized to view the e-signature).** **b) Request for help on the login procedure** **]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2:	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 defines the rules for the timing of authentication. This component makes contribution to O.AUTH security objective.*

FIA_UAU.5	**Multiple authentication mechanisms**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1:	The TSF shall provide **[assignment:** **a) Username and password,** **b) Digital signature based authentication or an alternative authentication method providing equivalent or better security.** **]** to support user authentication.
FIA_UAU.5.2:	The TSF shall authenticate any user's claimed identity according to the **[assignment: Remote users shall use the second authentication method defined above, other than / in addition to username and password verification,** [assigment: rules describing how the multiple authentication mechanisms provide authentication]**]**

Rationale: *This component requires that the TOE has multiple authentication mechanisms. Multiple authentication makes unauthorized access harder. This component makes contribution to O.AUTH security objective.*

FIA_UID.1	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1:	The TSF shall allow **[assignment:** **a) e-Signature verification page for the records, which is offered to the receivers of the record (they don't need to be authorized to view the e-signature).** **b) Request for help on the login procedure** **]** 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 defines which actions require authentication. This component makes contribution to O.AUTH security objective.*

FIA_USB.1	**User-subject binding**
Hierarchical to:	No other 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:** **a) User identity code (user id)** **b) Roles assigned to the user** **c) Client interface details** **d) Authentication history (time of last successful and unsuccessful authentication attempts)** **e) Recent record/document access history** **f)** [assignment: list of other user security attributes] **]**.
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:** **a) A clear session shall be established, information exists from the previous sessions shall be removed,** **b) Authentication history information shall be updated,** **c)** [assignment: other rules for the initial association of attributes] **]**.
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 change is allowed during an active session]**.

Rationale: *This component explains the details about user and subject binding. Since user attributes are also identified in this component, this component is complementary to auditing components. This component makes contribution to O.AUTH security objective.*

6.1.8. CLASS FMT: SECURITY MANAGEMENT

FMT_MOF.1	**Management of security functions behaviour**
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 behaviour of, disable, enable, modify the behaviour of] the functions **[assignment: all functions related with the management of the TOE]** to **[assignment: System_Administrator]**.

Rationale: *This component restricts the ability to manage security features to the authenticated System_Administrator. This component makes contribution to O.MANAGEMENT security objective.*

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 **[assignment: Access Control Policy,** [assignment: other access control SFP(s)]**]** to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes **[assignment: list of security attributes defined in FIA_USB.1.1]** to **[assignment: System_Administrator]**.

Rationale: *This component restricts the ability to manage security attributes to the authenticated System_Administrator. This component makes contribution to O.MANAGEMENT security objective.*

FMT_MSA.3	**Static attribute initialisation**
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 **[assignment: Access Control Policy]** to provide **[selection: restrictive]** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2:	The TSF shall allow the **[assignment: System_Administrator]** to specify alternative initial values to override the default values when an object or information is created.

Rationale: *This component restricts the ability to manage security attributes to the authenticated System_Administrator. This component makes contribution to O.MANAGEMENT security objective.*

FMT_MTD.1(1)	Management of TSF data (System_Administrator)
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of management functions
FMT_MTD.1.1(1):	The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: **create,** other operations]] the [assignment: list of TSF data] to **[assignment: System_Administrator]**.

> ***Rationale:*** *This component lets users authorized by the TOE to manage TSF data within the rules. This component makes contribution to O.MANAGEMENT security objective.*

FMT_MTD.1(2)	Management of TSF data (Normal_User, Data_Entry_Operator)
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of management functions
FMT_MTD.1.1(2):	The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: **create,** other operations]] the **[assignment: TSF data that is under the ownership of a Normal_User or Data_Entry_Operator]** to **[assignment: Owning Normal_User or Data_Entry_Operator]**.

PP Author Note: If other users are also involved in the data, then there may be some restrictions on the allowed operations on the data.

> ***Rationale:*** *This component lets users authorized by the TOE to manage TSF data within the rules. This component makes contribution to O.MANAGEMENT security objective.*

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: **[assignment: list of management functions to be provided by the TSF, which are listed in Table 4]**.

Application Note: The list of management actions in Table 4 is a collection of management actions defined under component definitions in Common Criteria Standard – Part 2. Please refer to the Part 2 of the Standard for further information.

> ***Rationale:*** *This component defines management actions on the TOE for chosen components. This component makes contribution to O.MANAGEMENT security objective.*

Table 4: List of Security Management Functions Provided by the TSF

Component*	Management Action
FAU_SAR.1	a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.
FAU_SEL.1	a) 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	a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.
FDP_ACF.1	a) Managing the attributes used to make explicit access or denial based decisions.
FDP_RIP.2	a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.
FDP_ITC.2	a) The modification of the additional control rules used for import.
FDP_SDI.2	a) The actions to be taken upon the detection of an integrity error could be configurable.
FIA_AFL.1	a) management of the threshold for unsuccessful authentication attempts; b) management of actions to be taken in the event of an authentication failure.
FIA_ATD.1	a) if so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users.
FIA_SOS.1	a) the management of the metric used to verify the secrets.
FIA_UAU.1	a) management of the authentication data by an administrator; b) management of the authentication data by the associated user; c) managing the list of actions that can be taken before the user is authenticated.
FIA_UAU.5	a) the management of authentication mechanisms; b) the management of the rules for authentication.
FIA_UID.1	a) the management of the user identities; b) if an authorised administrator can change the actions allowed before identification, the managing of the action lists.
FIA_USB.1	a) an authorised administrator can define default subject security attributes. b) an authorised administrator can change subject security attributes.
FMT_MOF.1	a) 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_MSA.3	a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values.
FMT_MTD.1(1)	a) managing the group of roles that can interact with the TSF data.
FMT_MTD.1(2)	a) managing the group of roles that can interact with the TSF data.

Component*	Management Action
FMT_SMR.1	a) managing the group of users that are part of a role.
FTA_MCS.1	a) 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	a) management of the session establishment conditions by the authorised administrator.

* No management actions has been foreseen for other components.

FMT_SMR.1	**Security roles**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of authentication
FMT_SMR.1.1:	The TSF shall maintain the roles **[assignment:** **a) System_Administrator** **b) Normal_User** **c) Data_Entry_Operator** **d)** [assignment: other authorised identified roles] **]**.
FMT_SMR.1.2:	The TSF shall be able to associate users with roles.

Rationale: *This component defines security roles for the users. This component makes contribution to O.MANAGEMENT and O.AUTH security objectives.*

6.1.9. CLASS FPT: PROTECTION OF THE TSF

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 failures, user failures].

Rationale: *This component ensures that the TSF shall preserve a secure state in case of defined types of failures. This functionality is a core component of error management, besides it can help for a better TOE management as well. This component makes contribution to O.ERROR_MANAGEMENT security objective.*

FPT_TDC.1	Inter-TSF basic TSF data consistency
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TDC.1.1:	The TSF shall provide the capability to consistently interpret [assignment: list of TSF data types] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2:	The TSF shall use [assignment: list of interpretation rules to be applied by the TSF] when interpreting the TSF data from another trusted IT product.

ST Author Note: There are some circumstances that the TOE accepts data from external entities, like registered e-mail and database of government entities (DTVT Project of Turkey). For each of these entities, a new iteration has to be made to this component.

> ***Rationale:*** *This component ensures a secure communication between the TOE and a trusted external IT entity. This component makes contribution to O.DATA_FLOW_CONTROL security objective.*

6.1.10. CLASS FRU: RESOURCE UTILISATION

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: all critical TOE capabilities]** when the following failures occur: **[assignment: software failure,** [assignment: list of other type of failures]**]**.

Application Note: "Critical" TOE capabilities mean any capability that is a part of the core functionality of the TOE. Software failures occuring because of hardware and/or operating system failures are out of scope.

> ***Rationale:*** *This component ensures the operation of the TOE even some kind of failures occur. Since audit records are important inputs for determining failures, this functionality is strongly related with O.AUDIT security objective. Besides, the functionality offered by this component is helpful for a better TOE management and error management. This component makes contribution to O.AUDIT and O.ERROR_MANAGEMENT security objectives.*

6.1.11. CLASS FTA: TOE ACCESS

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

FTA_MCS.1.2	The TSF shall enforce, by default, a limit of [assignment: default number] sessions per user.

PP Author Note: No determination has been made on the default number of sessions per user. However, if there is no need to provide a user with more than one session, it is recommended that only one active session is allowed for a user. If the TOE has a mobile interface as well, then maximum number of active sessions should be restricted to 2 or 3.

> ***Rationale:*** *This component limits the number of multiple concurrent sessions for a user. This functionality helps for a better authentication. Besides, it prevents the Attacker to use residual data of an active session by initiating a parallel session. This component makes contribution to O.AUTH and O.RESIDUAL_DATA_MNG security objectives.*

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 that is defined by System_Administrator]**.

PP Author Note: ST author should be aware that background processing should also be taken into consideration when considering user inactivity time interval. After the determined time interval, user session should be terminated regardless of background processes binded to that specific user. Time interval should not be too long to allow the Attacker to give harm, but also should not be too short, as it may prevent rational use.

> ***Rationale:*** *This component defines a time period for inactivity of the users. This functionality protects authenticated users and provides a mechanism against unwanted use of residual data. This component makes contribution to O.AUTH and O.RESIDUAL_DATA_MNG security objectives.*

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:*** *This component provides the user with a mechanism to protect his/her session data. Management of session data is a part of authentication and it is also a kind of residual data. This component makes contribution to O.AUTH and O.RESIDUAL_DATA_MNG security objectives.*

FTA_TAH.1	**TOE access history**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TAH.1.1	**Refinement:** Upon successful session establishment, the TSF shall display the [selection: date, time, method, location] of the last **three** 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.

Application Note: In FTA_TAH.1.1 and FTA_TAH1.2; "Method" means communication protocol/method used. It may have values like ftp, http, etc. Access from different mediums like desktop and mobile shall also be indicated in this column.

> ***Rationale:*** *This component provides authorized users with previous successful authentication information, so that they may determine possible misuse of their user account. This functionality provides a method to prevent unauthorized access. This component makes contribution to O.AUTH security objective.*

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:** **a) Location** **b) Port number** **c) Number of unsuccessful authentication attempts** **d) User ID, Role of the user or any other security attributes which define users** **e) Time range** **f) IP range** **g)** [assignment: any other attributes] **]**.

Application Note: Denial of session establishment based on time range means that some users may be given access to the TOE for a specific time period. This can be a definite time period, or any repeating time interval. This is especially useful for third party users of the TOE. This constraint provides protection against actions that occur at a time where proper monitoring may not be in place.

> ***Rationale:*** *This component defines restrictions on session establishment request of the users. This component makes contribution to O.AUTH and O.MANAGEMENT security objectives.*

6.2. SECURITY ASSURANCE REQUIREMENTS

This protection profile includes all Security Assurance Requirements defined in Common Criteria Part 3, EAL level 2. In addition to this, this protection profile also take into account following points:

ASE_CCL.1.10C section of ASE_CCL.1, which is defined in Common Criteria Part 3, has been rewriten to include "PP Author Note" subtitles of the included components. The new content is:

ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which

conformance is being claimed. **When determining and verifying conformance claim rationale, subtitles named "PP Author Note" (if exist) should also be taken into account.**

Security Assurance Requirements of EAL 2 assurance level, extended with ALC_FLR.1 and ALC_LCD.1 has been shown in the table below (Table 5).

Table 5: List of Security Assurance Requirements

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

6.3. SECURITY REQUIREMENTS RATIONALE

6.3.1. DEPENDENCIES OF SECURITY FUNCTIONAL REQUIREMENTS

Table 6 lists the dependencies of Security Functional Requirements and how they are included.

Table 6: List of the Dependencies of Security Functional Requirements

Component	Dependency	Inclusion
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FAU_GEN.1 requires that FPT_STM.1 is included as a component. However, the TOE is not capable of providing this functionality. This functionality will be proovided by a trusted server. Hence, FPT_STM.1 is not included.
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 Management of TSF data	FAU_GEN.1 FMT_MTD.1(1) FMT_MTD.1(2)
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
FCS_COP.1(1)	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Methods for ensuring audit data and record data integrity is left to ST Author. ST Author shall include additional components if they are needed for data integrity. FCS_CKM.4 component may or may not be needed, according to data integrity method chosen by the ST Author.
FCS_COP.1(2)	[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	Hash algorithms don't require cryptographic keys, hence no restriction has been made on assignments. FCS_CKM.1 and FCS_CKM.4 component has not been added, since it is not definite that there will be a need for cryptographic keys.
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	FDP_ACC.1 FMT_MSA.1
FDP_RIP.2	-	-
FDP_ITC.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1 FPT_TDC.1 FPT_ITC.1 or FTP_TRP.1 is not included, since this P.SSL_COMMUNICATION already provides a secure channel between TOE and external entities.

Component	Dependency	Inclusion
FDP_ETC.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1
FDP_SDI.2	-	-
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	-	-
FIA_SOS.1	-	-
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.5	-	-
FIA_UID.1	-	-
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	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.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	FIA_UID.1
FPT_FLS.1	-	-
FPT_TDC.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	-	-

6.3.2. DEPENDENCIES OF SECURITY ASSURANCE REQUIREMENTS

Table 7 lists the dependencies of Security Assurance Requirements and how they are included.

Table 7: List of the Dependencies of Security Assurance Requirements

Component	Dependency	Inclusion
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	-	
ALC_FLR.1	-	
ALC_LCD.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_FSP.2 Security enforcing functional specification ADV_TDS.1 Basic design	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1

Component	Dependency	Inclusion
	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	AGD_OPE.1 AGD_PRE.1

6.3.3. SCOPE OF SECURITY FUNCTIONAL REQUIREMENTS

Table 8 presents a mapping of SFRs and security objectives. Every SFR corresponds to at least one security objective. Similarly, every security objective corresponds to at least one SFR. The table also verifies that chosen SFRs are required and they are sufficiently addressing all security objectives.

6.3.4. RATIONALE OF EAL PACKAGE

When choosing EAL level, security requirements of the document and record management system applications has been considered. These applications require a moderate level of security. Attack potential is relatively low, when compared to smart cards and/or banking applications.

Another consideration made during EAL decision is relatively more frequent update needs of web-based applications. Since web-based applications can be reached from the internet and internet threats change quickly, they should be reflected to the products as fast as possible. A higher assurance level would need longer certification periods, which may result in a shrinking demand.

Table 8: Coverage of Security Functional Requirements

		SECURITY OBJECTIVES						
		O.AUDIT	O.AUTH	O.DATA_FLOW_CONTROL	O.DATA_INTEGRITY	O.MANAGEMENT	O.ERROR_MANAGEMENT	O.RESIDUAL_DATA_MNG
SECURITY FUNCTIONAL REQUIREMENTS	FAU_GEN.1	✓						
	FAU_GEN.2	✓						
	FAU_SAR.1	✓				✓		
	FAU_SAR.2	✓				✓		
	FAU_SAR.3	✓				✓		
	FAU_SEL.1	✓				✓		
	FAU_STG.1	✓						
	FAU_STG.3	✓				✓		
	FAU_STG.4	✓				✓		
	FCS_COP.1(1)				✓			
	FCS_COP.1(2)	✓	✓		✓			
	FDP_ACC.1		✓			✓		
	FDP_ACF.1		✓			✓		
	FDP_RIP.2							✓
	FDP_ITC.2			✓	✓			
	FDP_ETC.2			✓				
	FDP_SDI.2				✓			
	FIA_AFL.1		✓					
	FIA_ATD.1		✓					
	FIA_SOS.1		✓					
	FIA_UAU.1		✓					
	FIA_UAU.5		✓					
	FIA_UID.1		✓					
	FIA_USB.1		✓					
	FMT_MOF.1					✓		
	FMT_MSA.1					✓		
	FMT_MSA.3					✓		
	FMT_MTD.1(1)					✓		
	FMT_MTD.1(2)					✓		
	FMT_SMF.1					✓		
	FMT_SMR.1		✓			✓		
	FPT_FLS.1						✓	
	FPT_TDC.1			✓				
	FRU_FLT.1	✓					✓	
	FTA_MCS.1		✓					✓
	FTA_SSL.3		✓					✓
	FTA_SSL.4		✓					✓

		SECURITY OBJECTIVES						
		O.AUDIT	O.AUTH	O.DATA_FLOW_CONTROL	O.DATA_INTEGRITY	O.MANAGEMENT	O.ERROR_MANAGEMENT	O.RESIDUAL_DATA_MNG
	FTA_TAH.1		✓					
	FTA_TSE.1		✓			✓		

RESOURCES

TS 13298 Elektronik Belge Yönetimi Standardı, Türk Standardları Enstitüsü, TS 13298/T1, Ankara, Turkey, April 2012.

20 Critical Security Controls, version 4.1, SANS Institute, (online) <http://www.sans.org/critical-security-controls/> (last access: 10 December 2013)

OWASP Top 10 - 2013: The Ten Most Critical Web Application Security Risks, The Open Web Application Security Project (OWASP), 2013, (online) <https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project> (last access: 10 December 2013)

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

PRONI, General Guidelines for Implementing an Electronic Document and Records Management System, Public Record Office of Northern Ireland (PRONI), March 2009.