Seneka EBDYS

SECURITY TARGET

Mürüvvet Uzun, Fikretcan Erken
SENEKA

Table of Contents

VERSION HISTORY

Version No	Date	Version Description
1.0	04.09.2015	Added DEFINITIONS AND ABBREVIATIONS, SECURITY TARGET INTRODUCTION, DEFINITION OF AIMS AND SCOPE, TOE OWERVIEW
1.1	08.09.2015	Added TOE TYPE, OPERATIONAL ENVIRONMENT COMPONENTS, TYPE OF USERS,
1.1	08.09.2015	Updated TYPE OF USERS
1.2	13.09.2015	Added CONFORMANCE CLAIMS, SECURITY PROBLEM DEFINITION, SECURITY OBJECTIVES, EXTENDED COMPONENTS DEFINITION
1.3	18.09.2015	Added SECURITY REQUIREMENTS
1.4	23.09.2015	Updated SECURITY REQUIREMENTS
1.5	27.09.2015	Added TOE SUMMARY SPECIFICATION
1.6	28.09.2015	Updated TOE SUMMARY SPECIFICATION Added VERSION HISTORY and CONTENTS
1.7.	14.02.2016	Update all document
2.0	02.05.2016	Update all document
3.0	16.05.2016	Update all document
4.0	29.07.2016	Update all document
5.0	23.08.2016	Update Version History, FAU_SAR.3, FDP_SDI.2, FAU_SAR.3, FCS_COP.1(2), FDP_SDI.2, FAU_STG.3, FAU_STG.4,, FCS_COP.1(1), FCS_COP.1(2), FDP_ACF.1, FIA_SOS.1, FIA_USB.1, FMT_MSA.1, FMT_MTD.1(1) , FMT_MTD.1(1,), FMT_MTD.1(2)
6.0	07.10.2016	Update Version history, TOE version, FAU_SAR.3, FAU_STG.4, FIA_UAU.5, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_SMR.1, FPT_TDC.1,Table 5,Table 6, 7.1.1 SECURITY AUDIT, 7.1.3 USER DATA PROTECTION, 7.1.4 IDENTIFICATION AND AUTHENTICATION, 7.1.5 SECURITY MANAGEMENT, 7.1.6 PROTECTION OF THE TSF , 7.1.8 TOE ACCESS
7.0	15.10.2016	Update Version History, Identification Authentication, FAU_STG.4, Identification and Authentication, Securitiy Management.
8.0	21.10.2016	Update Version History, Table 6, TOE Version, FAU_STG.3.1, 7.1.1 SECURITY AUDIT
9.0	11.11.2016	Update Version History, FCS_COP.1(2), FPT_TDC.1
10.0	21.11.2016	Update Version History, 1.1 Reference, ST Version
11.0	01.12.2016	Update Version History, 1.1 Reference ST Version, 6.1.6. FDP_SDI.2 Application Note
12.0	22.12.2016	Update Version History, 7.1.6 Protection of the TSF

13.0	10.01.2017	Update Version History, 6.1.4 FAU_SEL.1 Application Note, 7.1.1 Security Audit, 7.1.2 Cryptographic Support, 7.1.3 User Data Protection
14.0	25.01.2017	Update Version History, 7.1.2 Cryptographic Support
15.0	26.01.2017	Update Version History, 6.1.5 FCS_COP.1(1)
16.0	27.02.2017	Update Version History, 1.1 Reference, 6.1.4 FAU_SAR.3, FAU_STG.4, 6.1.5 FCS_COP.1(1), FCS_COP.1(2), 6.1.3 Dependencies of SFRs
17.0	06.03.2017	Update Version History, 6.1.6 FDP_SDI.2, 7.1.1 Security Audit, 7.1.3 User Data Protection
18.0	09.03.2017	Update Version History, 6.1.5 FCS_COP.1(2)
19.0	03.07.2017	Update Version History, 2.2 PP Claim, 6.1.6 FDP_SDI.2.2, 6.3.1. FCS_COP.1(1) justification, 7.1.2. Cryptographic Support

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 finalized 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.

RDBMS: Relational Database Management System

1. SECURITY TARGET INTRODUCTION

1.1 REFERENCE

Reference information of this security target is shown in the table below.

ST Title	Seneka EBDYS Security Target
ST Version	Version 19.0
TOE Name	Seneka EBDYS
TOE Version	v1.0
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

This document is formed to explain security targets of TOE. This document includes specific and all security targets of TOE according to Electronic Document and Records Management System Protection Profile and CC v3.1 Revision 4.

1.3 TOE OWERVİEW

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 manage 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,
- Dentification 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 features,
- Secure access control mechanisms,
- Safely storing electronic documents,
- Document, data and system integrity,
  When needed, integration with other line of Business applications

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.

1.3.4 TOE DETAILS

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

1.3.4.1. HARDWARE AND SOFTWARE OPERATIONAL ENVIRONMENT COMPONENTS TOE DESCRIPTION

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

1.3.4.2. TOE DESCRIPTION

TOE is a multi-tiered system with separate presentation, business logic and data management layers. Detailed description of physical parts of the TOE and its logical security features are provided below.

1.3.4.2.1. Physical Scope of TOE

Storage Unit: Application records are stored on a separate application server. Documents are stored on database server. Using this method, unauthorized access to the database, because of weakness in the management level of TOE, is obstructed.

Audit Records Unit: Audit records are stored in database.

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 in a database.

Database: TOE is in close interaction with a database for keeping its data. Records and documents are kept in database.

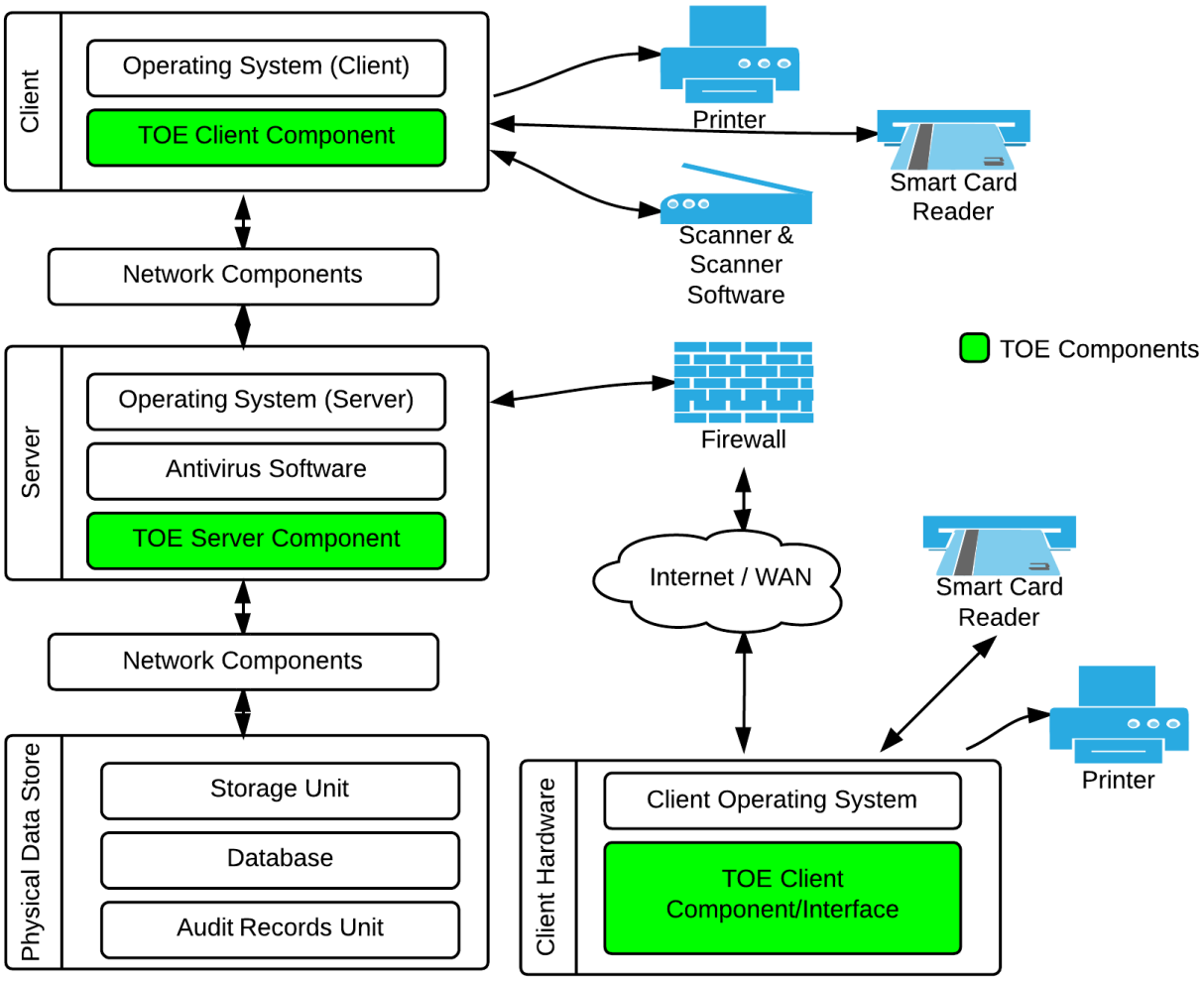
Server: It is the main hardware component that server component of the TOE runs on. It can be physical or virtual. In both cases, security of the server is strongly related with the security

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 security target document. 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 is a secured 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. 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 is used for authentication purposes as well. Especially the authentication of explicitly authorized users profit from this approach.

Antivirus Software: An antivirus software is used to check incoming documents and records. When a digital file like document attachments is uploaded by end user, the file is checked for viruses on the application servers. If virus found, digital file is replaced with a text file which contains the original file name and information about why it is removed from system.

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

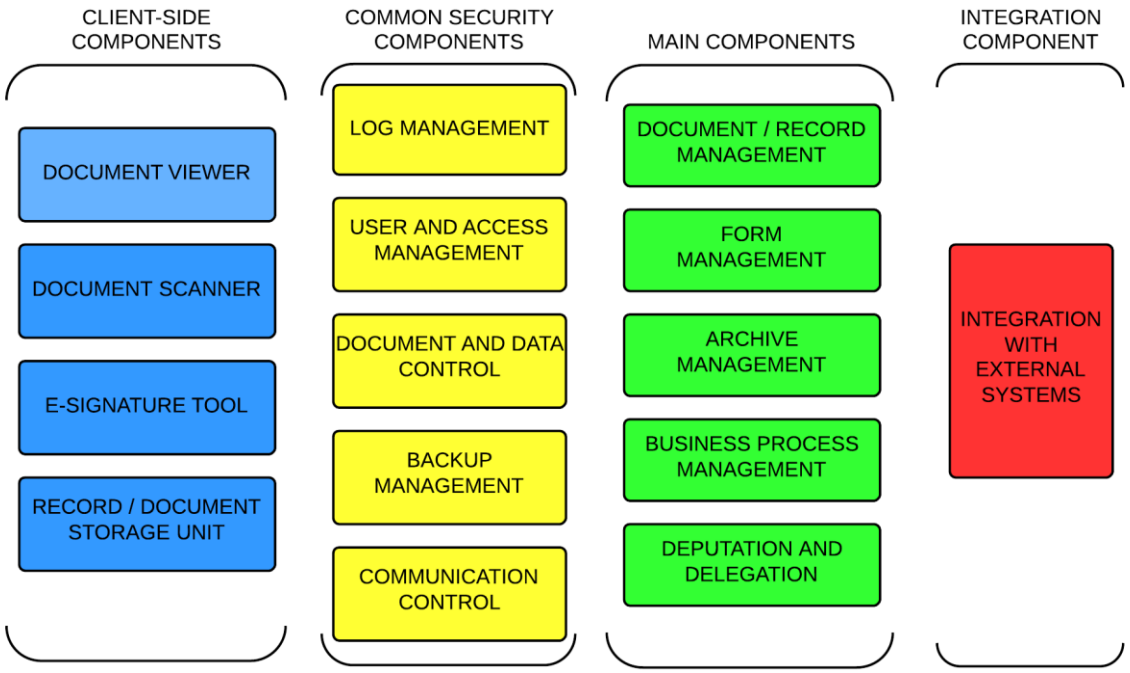
records according to the rules defined in TS 13298 Electronic Document Management Standard and then sends them to the TOE.

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.

1.3.4.2.2. Logical Scope of TOE

Figure 1: Typical Components of an EDRMS System



The logical scope of the TOE is described through the security functionality as follows;

Security Audit: The TSF generates logs that consist of various auditable events. Date and time of events, usernames, and events taken by the authorized users are recorded. Authorized administrators have right to read and view all the recorded logs stated above.

Identification &Authentication: Identification and Authentication is required to ensure that users are associated with the proper security attributes (e.g. identity, group, roles, and security or integrity levels). Each users account only exists in the database that relates to the user organization.

User Data Protection: The access control function permits a user to access a protected resource only if a user ID or role of the user is given permission to perform the requested action on the resource by Administrator. On the other hand, Authorized administrators of the TOE can perform assigning the privileges, modify his/her own authentication data, users' password and other information.

Security Management: Only one administrator is required to have full access rights to manage the TOE. Authorized administrators can assign access privileges to users by user levels based on the functions or resources that they are allowed to perform. Additional functionalities such as modifying access privileges and unlocking password for users are also accessible by authorized administrator.

Toe Access: After a successful authentication, a new session is created for the authenticated user and if another open session for that user exists, it is closed. The TOE is able to deny session establishment once the user status is disabled.

1.3.4.3. TYPE OF USERS

There are three types of users of the TOE. These are:

- Normal User
- Data Entry Operator
- System_Administrator

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, and 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 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 based on client, like database administrator, network administrator, application administrator, etc. Administrator can access the application, database, file system and other entities with all privileges

1.3.5 MAIN SECURITY FEATURES OF THE TOE

Authentication and Authorization: Authorization and authentication operations are carried out effectively. Authentication is carried out by username and password, electronic signature,

mobile signature, and active directory credentials. Firstly, System Administrator or User Administrator define authentication types for each user. There are restrictions on passwords to be used. Passwords are not stored in the storage units as plain texts; hashed passwords are used instead. Cryptographic hash functions are used to secure stored passwords.

Access Control: TOE has the needed capabilities to restrict access, so that only specifically authorized entities have access to TOE functions and data. For authorized users, access control is 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.

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.

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 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. These interfaces simplify fast and accurate decision-making during a security event. Interfaces designed for the management of TOE has subject to more advanced access control mechanisms.

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 be done by an external tool can be used for this purpose. Backup operations be done by SQL Servers and SQL server ensure that there won’t be any information loss and provide security for intentional and unintentional data loss and/or physical damages.

Information and Document Flow Control: Maximum file size 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, hash them. Chosen hashing algorithm is strong enough that original data can't be recovered with today's technology in a reasonable time-period. The TOE updates its hashing algorithm as new algorithms show up to reverse hash tables to get the original value

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 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. The recipient does not regard the received printout as an official record without verifying the original electronic record. E-signature verification is made by TOE environment.

1.4. DOCUMENT OVERVIEW

In Section 1, TOE and Security Target 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, Electronic Document and Records Management System 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 Section 7, TOE summary specification is explained in detail.

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

2. CONFORMANCE CLAIMS

2.1. CC CONFORMANCE CLAIM

This security target conforms to the Common Criteria Standard, Version 3.1, Revision 4.

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

This security target is conformant to the Part 3 of the Common Criteria Standard, Version 3.1, Revision 4.

2.2. PP CLAIM

This security target claim conformance to EDRMS PP Version 1.3.2.

2.3. EAL CONFORMANCE CLAIM

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 STATEMENT

This security fulfill all requirements defined in Section 6 of EDRMS PP.

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 occurs when integrity of audit data is not assured. Another occurrence of this threat is modification of the source codes and audit data of the TOE by the Attacker. Improper 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 improper 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, that he/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 functionality 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 occurrence 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 are 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 are easily monitored with minimal workload.
P.SSL_COMMUNICATION	All communication channels, which are under the control of TSF, use SSL communication protocol.
P.PROPER_CONFIGURATION	Default configuration of the TOE and interacting components that are under the control of the TOE are changed, so that the Attacker can't get information about the TOE and its operational environment. Unused services are 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 are conformant to Turkish Electronic Signature Law numbered 5070. Accordingly, signing procedures are follow the same law.
P.RECORD_VERIFICATION	Record verification mechanism provided to recipients for linking printed versions of digitally signed records and electronic official copies of the records conform to the following criteria: • An access code exists in printouts of the records.

	• Digital versions of the records are verified by recipients. If verification result is unsuccessful, then the record is not accepted (since printed version is not an official record, only a pointer to digitally signed record). • Digital verification feature provided to the recipients are include both e-signature and the record content • Verification interface is implemented in a way that it is able to identify and prevent brute-force attacks. For example, request frequency is monitored, a Captcha string is included in the interface to detect automatic bots, etc. • Filenames of digital signatures are not follow a pattern, verification codes contain at least 16 characters. This measure helps prevent parameter replay attacks. It is also an additional protection against brute-force attacks.

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 have 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_DELIVER	It is assumed that all needed security measures have been taken during the delivery of the TOE. Delivery processes have been carried 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 objectives will be mapped to security functional requirements in Section 6.

4.2. SECURITY OBJECTİVES FOR THE TOE

O.AUDIT	TOE record any event having value in terms of security within the scope of its ownership. TOE protect these records against modification and deletion. TOE 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 explicitly define every user, securely authenticate them and authorize them according to their rights and roles. All requests needing authorization is subject to authentication and authorization processes. The TOE define the rules for user authentication that forces users to have strong passwords. TOE allow classification of records/documents, provide the functionality to define rules with respect to record/document classification. TOE also offer the ability to define rights for individual records/documents. TOE 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 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 are configured to run at minimum authorization level possible. Default parameters of these tools are modified, so that they become unique and aren't affected by automatized attacks.
O.DATA_FLOW_CONTROL	TOE control and manage unauthorized data flow in and/or out. Data to be imported is 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 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 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 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 provide the System_Administrator with all the functionality to manage the system securely and effectively. TOE put proper access control mechanisms in place to protect management interfaces. TOE also ensure that its interfaces support fast and accurate decision making. TOE 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 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 offer an error management mechanism in a secure and efficient way. Errors occurring during the operation of the TOE is shown to the user in a secure and meaningful way. For instance, TOE return a general authentication failure information, not a specific one like "username is not found". Similarly, error details with method and line of code are not exposed to normal users. On the other hand, System_Administrator is informed about critical failures in a fast and efficient way. Errors are detailed enough to lead the System_Administrator to suitable actions. The TOE preserve a secure state in case of an error occurring in the TOE itself.
O.RESIDUAL_DATA_MNG	TOE 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 ensures physical and environmental security of the TOE. Unauthorized access is restricted and all components in the operational environment are secured. Only specifically authorized people is allowed to access critical components. Operational environment of the TOE 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 provides the TOE with secure communication mediums and/or tools.
OE.TRUSTED_ADMIN	Operational environment of the TOE ensures 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 ensures that all users developing the TOE are sufficiently educated and meet the security requirements.
OE.EXPERIENCED_DEVELOPER	Operational environment of the TOE ensures 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 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 are easily monitored with minimal workload.
OE.SECURE_DELIVERY	Delivery and installation of the TOE is carried out without sacrificing any security constraint. Besides, functions

	and/or parameters used for testing purposes are cleared or made inaccessible.
OE.PROPER_BACKUP	Proper backups are created and kept for a reasonable time for all data residing in the operational environment of the TOE. Pre-defined routines may23 be used for this purpose. Storage units and other hardware components are 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 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.TRUSTEDDEVELOPER	A.EXPERIENCED_DEVELOPER	A.COMMUNICATION	A.PROPER_BACKUP	A.DIST_DENIAL_OF_SERVICE	A.SECUREDELIVERY
OBJECTIVES FOR TOE	O.AUDIT			X					X												
	O.AUTH	X	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. 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 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

There are no 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 is shown intact.

Notations used in this section are as follows:

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 (**CC v3.1 Revision 4).** 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))

6.1.2. OVERVIEW

Components included in this security target 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
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 behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
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].**

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 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 behavior 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 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. (basic) Identification of which TSF data have been interpreted. (basic) Detection of modified TSF data.	
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.	

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

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.

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.

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: filtering 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: These 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.

Application Note: Least critical audit selection is left upon the customer's decisions. System administrators can select events not to be audited within the system settings.

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

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: 90% of the disk space].**

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.

Application Note: TOE's Audit Trail records stored on RDBMS. RDBMS has no theoretical limit for data storage

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:TOE will stop working]** if the audit trail is full.

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.

Application Notes: As TOE's Audit Trail Records stored on an RDBMS, available physical disk space can be tracked and managed regularly. Also logs are reported by e-mail with time stamp to authorized administrators. Previously reported by e-mail logs are considered to be less important data. In a case where the disk size limit is reached, the TOE will stop working since the RDBMS would not work. In order to prevent such occurrences, an e-mail is sent to the database administrators (defined by the customer) when the 90% disk limit is reached, urging to add new disk space to the RDBMS environment.

6.1.5. CLASS FCS: CRYPTOGRAPHIC SUPPORT

FCS_COP.1(1)	Cryptographic 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:** SHA-256] and cryptographic key sizes **[assignment: none]** that meet the following: **[assignment: FIPS PUB 180-2]**.

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)	Cryptographic 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: SHA-256]** and cryptographic key sizes **[assignment: none]** that meet the following: **[assignment: FIPS PUB 180-2].**

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: None] e. [assignment: None]].

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
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: None]** **].**
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 authorize 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: None]** **].**
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 threshold value.** **c) Unexpectedly high number of requests coming from an authorized user** **d) Multiple sessions started by the same user that exceeds pre-defined threshold value.** **e) [assignment: None]** **].**

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: 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: none]** 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: display the compromised record data with a red cross and the compromised audit data with a red background].**

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: 5]** 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].**

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: none]
].

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: System_Administrator can define by Regular Expression]].

Rationale: This component defines the rules for secrets. These rules contribute 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. Authentication for this operation is provided by the verification code existing on the printouts of sent records). b) Request for help on the login procedure, password retrieval processes] 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, in addition to username and password verification,** **, [assignment: Active Directory, Mobile Signature]**

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.

Application Note: Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services.

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. Authentication for this operation is provided by the verification code existing on the printouts of sent records).** **b) Request for help on the login procedure, password retrieval processes** **]** 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: None]].
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: None]].
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 behavior
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MOF.1.1:	The TSF shall restrict the ability to [selection: disable, enable, modify the behavior 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: None]]** to restrict the ability to **[selection: change_default, query, modify, delete, [assignment: None]]** 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 initialization
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1:	The TSF shall enforce the **[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]]** the **[assignment: system logs and system settings]** 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,]** 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].**

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].**

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 authorized 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 authorized administrator can change the actions allowed before identification, the managing of the action lists.
FIA_USB.1	a) an authorized administrator can define default subject security attributes. b) an authorized 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.
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 authorized administrator.

* No management actions have 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: None]** **].**
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.

Application Note:

Other authorized identified roles are defined in TS13298, not covered by the TOE.

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: X.509 electronically signed data]** when shared between the TSF and another trusted IT product.
FPT_TDC.1.2:	The TSF shall use **[assignment: SOAP and Tubitak ESYA API**] when interpreting the TSF data from another trusted IT product.

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, hardware failure]**.

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: 1]** sessions per user.

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].**

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.

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: None]** **].**

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 security target document includes all Security Assurance Requirements defined in Common Criteria Part 3, EAL level 2 and Electronic Document and Records Management System Protection Profile Version 1.3.2.

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
	Security Problem Definition	ASE_SPD.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 provided 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	FCS_CKM.1 and FCS_CKM.4 components are not needed since data integrity check is performed by the comparison of hash values and no cryptographic key is generated during this operation.
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.3
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.

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

Component	Dependency	Inclusion
ADV_ARC.1	ADV_FSP.1 Basic functional specification ADV_TDS.1 Basic design	ADV_FSP.2 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	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1

	AGD_PRE.1 Preparative procedures ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing	
AVA_VAN.2	ADV_ARC.1 Security architecture description ADV_FSP.2 Security enforcing functional specification ADV_TDS.1 Basic design AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 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	X						
	FAU_GEN.2	X						
	FAU_SAR.1	X				X		
	FAU_SAR.2	X				X		
	FAU_SAR.3	X				X		
	FAU_SEL.1	X				X		
	FAU_STG.1	X						
	FAU_STG.3	X				X		
	FAU_STG.4	X				X		
	FCS_COP.1(1)				X			
	FCS_COP.1(2)	X	X		X			
	FDP_ACC.1		X			X		
	FDP_ACF.1		X			X		
	FDP_RIP.2							X
	FDP_ITC.2			X	X			
	FDP_ETC.2			X				
	FDP_SDI.2				X			
	FIA_AFL.1		X					
	FIA_ATD.1		X					
	FIA_SOS.1		X					
	FIA_UAU.1		X					
	FIA_UAU.5		X					
	FIA_UID.1		X					
	FIA_USB.1		X					
	FMT_MOF.1					X		
	FMT_MSA.1					X		
	FMT_MSA.3					X		
	FMT_MTD.1(1)					X		
	FMT_MTD.1(2)					X		
	FMT_SMF.1					X		
	FMT_SMR.1		X			X		
	FPT_FLS.1						X	
	FPT_TDC.1			X				
	FRU_FLT.1	X					X	
	FTA_MCS.1		X					X
	FTA_SSL.3		X					X

	FTA_SSL.4		X					X
	FTA_TAH.1		X					
	FTA_TSE.1		X			X		

7. TOE SUMMARY SPECIFICATION

This section provides the TOE summary specification. This section illustrates how the "Seneka Ebdys Elektronik Belge ve Doküman Yönetim Sistemi" features achieve the TOE security functional requirements.

7.1 TOE SECURITY FUNCTIONS

7.1.1 SECURITY AUDIT

Users and administrator access the TOE through the Seneka Ebdys (which will be referred to "System" in the following sections.) login module. The TOE generates audit logs that consist of various auditable events by the users and administrators. The auditable events include user logins, user logouts, failed login attempts. The audit logs contain the following information:

- **User:** The user that made the operation.
  - **Client IP Address**
- **Table Name:** The object that the operation is made on.
- **Operation:** The type of the operation made. This parameter is selected from a combo box containing the following entries:
  - **Delete**
  - **Insert**
  - **Update**
- **Location:** The location of the client making the operation. Displayed as "Inside" or "Outside" according to the operator user's IP Address.
- **User Group (Department):** The department of the operator user.
- **Criticality:** The criticality level of the operation.
- **Connection Method:** The connection protocol used for the operation. Displayed as "HTTP" or "HTTPS".
- **Start Date:** The date when the operation is made on or after.
- **End Date:** The date when the operation is made on or before.

These audit logs can be analyzed by authorized administrators for suspicious activities. The TOE provides the capability for authorized administrators to read and view all the logs stated above through the "System Logs", "Client Logs" or "Server Logs". All types of logs are grouped according to the server address, user Id, date, operation type, operator user's location, operator user's group/department, operation criticality value and operator user's connection method. By this way system administrator can filter audit records. The TSF ensures the integrity and permanency of the audit logs by an electronic signature and a time stamp. Only the administrators can view the audit log. The TSF detect the authorized administrators from modifying or deleting audit logs with electronic signature and time stamp.

As TOE's Audit Trail Records stored on an RDBMS, available physical disk space can be tracked and managed regularly. So, in a case where the disk size limit is reached, the TOE will stop working since the RDBMS would not work. In order to prevent such occurrences, the RDBMS maintenance module

of the TOE periodically controls the remaining disk space and in case where the disk space is 90% full, an e-mail is sent to the database administrators defined by the customer. Also, logs are reported by e-mail with time stamp to authorized administrators in a previously defined schedule determined by the system administrator. Previously reported by e-mail logs are considered to be less important data.

Every audit event can be enabled or disabled to be audited through the system settings. System administrators can select which events to be audited by selecting these events in the respective system setting.

Functional Requirement Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1, FAU_STG.1, FAU_STG3, FAU_STG.4

7.1.2 CRYPTOGRAPHIC SUPPORT

All documents generated in the System are signed with digital certificates. This digital signature guarantees the integrity and non-repudiation of origin. In addition, every digital signature includes a PKI-based time stamp. Versions which are created by different users in a life cycle of a document are stored separately. After the final approval of the document, editable document data is converted to PDF/A format to prevent additional modifications.

A digital time stamp is added to audit logs and automatically e-mailed to System Administrators on a scheduled basis.

Moreover, every user's password information is sent to the server side as a SHA-256 hash. This ensures the protection of the password information between the client and the server side.

Lastly, every audit and record data is stored with an unchangeable digest hash data, calculated with SHA-256. This digest is stored with the data and made unghangable on the RDBMS level with the help of triggers. Upon accessing these data, a SHA-256 hash of the data is calculated and compared to the stored digest. If these two values do not match, the user is informed that the integrity of said data is compromised and no further action is allowed.

Functional Requirement Satisfied: FCS_COP.1(1), FCS_COP.1(2)

7.1.3 USER DATA PROTECTION

System Administrator or an authorized user can create new user accounts in the System. Creation process involves entering detailed information about the user, setting the authorization types which user can use to logon to the System, assigning privileges to the user, and the user accounts validity period.

If a user account has never been used to logon to the system, System Administrator can delete this user. Other user accounts can only be set as disabled by the System Administrator.

Users can request privileges and System Administrator can review requests and assign new privileges to the user.

Only authorized users can import data in to the System. System Administrator can manage which types of data can be imported. Only authorized users can export data form the System.

The integrity of stored data is secured by the database system's authorization and authentication mechanisms. Any data modification can be monitored through the database system's audit functionality. On the other hand, in order to verify the document data integrity, electronic signatures are used. Authorized user can display the electronic signature information of a signed document and

perform a validation in order to ensure the data is not compromised. The validation results are displayed to the authorized user in detail so that the user can determine the cause of the failure in case of an unsuccessful validation. Each signature validation operation is logged and the validation result is included within the respective log item. Also, for audit data integrity, audits are recorded with their respective checksum values and these values are unchangeable due to their definition on the RDBMS. The checksum value is actually a digest of the data calculated with SHA-256 hash algorithm. Every time the audit records are queried, a hash value is calculated with the current audit entry and compared to the checksum value. If these values match, that means the audit records are not tampered.

On specific circumstances, document data can be imported and exported to/from the TOE while communicating with another electronic document management system. Since the imported and exported document data is always electronically signed (and the signature is verified upon import), the imported/exported document unambiguously contains the associated security attributes.

Functional Requirement Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_RIP.2, FDP_ITC.2, FDP_ETC.2, FDP_SDI.2

7.1.4 IDENTIFICATION AND AUTHENTICATION

There are four main kinds of authentication types: Username password, digital signature, mobile signature, active directory authentication. Username password authentication has two sub types. For the first one, users' username and passwords are stored in the system and authentication mechanism checks this username password with the user's input. For the second one, user enters his Active Directory username and password and system authenticates user credentials form Active Directory. In this authentication type, users' passwords are not stored in the System. System Administrators can limit the authentication types for any user.

A remote user can access the TOE if the customer enables this type of access. The remote user access can be disabled by the TOE customer.

System Administrator can limit the authentication failure handling. The TSF provide a mechanism to verify that secret meets with system setting. System administrator can define password rules with the help of a Regular Expression.

Before the authentication operation, The TSF allows the unauthenticated user to see the 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. Authentication for this operation is provided by the verification code existing on the printouts of sent records). Also, the TSF enables an unauthenticated user to request for help on the login procedure, including password retrieval processes on behalf of the user to be performed before the user is authenticated.

In TOE, a corresponding "User" object is created for a user when a user is registered. This object is created by the system administrator and during this creation action the subject security attributes such as user role or department rights can be defined. Every operation made by the system administrator in this scope is logged. With every successful authentication, a session is created for this object that carries the security attributes of the real user.

Functional Requirement Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1, FIA_USB.1

7.1.5 SECURITY MANAGEMENT

There are separate management modules for each entity (user, role, function etc.) in TOE. Only authorized users can access these modules. All TOE functions corresponds to one atomic operation like “update record”, “view record”. Users without rights cannot see the related module menu according to “not need to know” basis.

The TOE provides mechanisms to govern which users can access with resources or functions. The Security Management function allows the administrators to properly configure this functionality.

Authorized administrators can assign access privileges to users by user levels based on the functions or resources that they are allowed to perform or access. Additional functionality such as modifying access privileges is also accessible by authorized administrators. The TSF data can only be modified by authorized administrators. Furthermore, the TOE enforces the Access Control Policy to provide restrictive default values for security attributes that are used to enforce the SFP. Only authorized admisintrators are allowed to change these initially given default values for newly created objects and information.

Functional Requirement Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_SMF.1, FMT_SMR.1

7.1.6 PROTECTION OF THE TSF

TOE offer an error management mechanism in a secure and efficient way. Errors occurring during the operation of the TOE is shown to the user in a secure and meaningful way.

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). The TOE provides the System_Administrator with an easily usable interface to let him/her put filtering mechanisms in place if needed.

In terms of protection regarding accepting data from other trusted IT products, the TOE accepts only electronically signed document data in a special format that contains both the document data and the metadata. (“E-Yazisma Paketi”, Ministry of Development, Turkey). This format contains every information that the TOE requires to constitute a document object and since it is electronically signed with an X.509 Certificate, the authenticity of both the document and the document metadata is verifiable upon the signature verification. This way the TOE is protected from corrupt and unverifiable data input from other tursted IT products.

On the other hand, any document data input requires an authorized user to assign its security properties within the TOE right after the input process is completed. This way the TOE ensures that the input object’s security properties that belongs to other trusted IT products is not passed into the system directly and the TSFs are protected by design.

Functional Requirement Satisfied: FPT_FLS.1, FPT_TDC.1

7.1.7 RESOURCE UTILISATION

TOE error management mechanism ensures the operation, when a software or hardware failure occurs.

Functional Requirement Satisfied: FRU_FLT.1

7.1.8 TOE ACCESS

The TSF restrict the maximum number of concurrent sessions that belong to the same user, only one active session is allowed for a user. When the same user login the system from different devices, first user login is ended by the system.

TOE has a lot of system settings that are managed by the system administrator. System administrator can define the time interval of user inactivity using system settings. TOE allows user-initiated termination of the user's own interactive session. In addition to these system settings, the TOE is able to deny session establishment based on the user’s location, port number, number of unsuccessful authentication attempts, role (or any other security attributes which define a user), time range and IP address.

Authorized users can view previous successful and unsuccessful authentication information. Some users may be given access to the TOE for a specific time period by the system administrator using user management menu and system settings menu.

Functional Requirement Satisfied: FTA_MCS.1, FTA_SSL.3, FTA_SSL.4, FTA_TAH.1, FTA_TSE.1