Certification Report

EAL 2 + (ALC_FLR.1, ALC_LCD.1)
Evaluation of

Turkish Standards Institution

Electronic Document and Records Management, Records Management, Electronic Document Management
(EDRMS PP)

Protection Profile
V1.3.1

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	06.08.2014
Version of Report	1
Author	Kerem KEMANECİ
Technical Responsible	Mustafa YILMAZ
Approved	Mariye Umay AKKAYA
Date Approved	06.08.2014
Certification Number	21.0.01/14-021
Sponsor and Developer	Turkish Standards Institution
Evaluation Lab	TÜBİTAK BİLGEM OKTEM
PP Name	Electronic Document and Records Management, Records Management, Electronic Document Management (EDRMS PP) v1.3.1
Pages	22

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
V1	06.08.2014	All	Final Released

DISCLAIMER

This certification report and the PP defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the PP in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the PP by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the PP by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the STCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCCS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned PP have been performed by TÜBİTAK BİLGEM OKTEM, which is a public CCTL.

A Common Criteria Certificate given to a PP means that such PP meets the security requirements defined in its PP document that has been approved by the CCCS. The PP document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the PP should also review the PP document in order to understand any assumptions made in the course of evaluations, the environment where the PP will run, security requirements of the PP and the level of assurance provided by the PP.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Electronic Document and Records Management, Records Management, Electronic Document Management (EDRMS PP) v1.3.1 whose evaluation was completed on 25.07.2014 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the PP document with version no 1.3.1.

The certification report, certificate of PP evaluation and PP document are posted on the STCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

This report describes the certification results by the certification body on the evaluation results applied with requirements of APE(Protection Profile Evaluation) assurance class of the Common Criteria for Information Security Evaluation in relation to Electronic Document and Records Management, Records Management, Electronic Document Management Protection Profile (EDRMS PP) v1.3.1. This report describes the evaluation results and its soundness and conformity.

The evaluation on Electronic Document and Records Management, Records Management, Electronic Document Management Protection Profile (EDRMS PP) v1.3.1 was conducted by TÜBİTAK-BİLGEM-OKTEM and completed on 25.07.2014. Contents of this report have been prepared on the basis of the contents of the ETR submitted by OKTEM. The evaluation was conducted by applying CEM. This PP satisfies all APE requirements of the CC, therefore the evaluation results were decided to be “suitable”.

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

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

- Registration of electronic records,
- Scanning of paper-based documents,
- definition and management of file classification plans and their elements,
- Identification of document attributes and document metadata,
- Workflow management of electronic records,
- Creation of retention plans, definition of retention criteria and periods, resolution of retention plan inconsistencies (when users enter a wrong categorization value for retention plan, high level authorized users are given permission to change retention plan categorization),
- Creation and management of archival processes,

- Performing common tasks like efficiently indexing, searching, listing, viewing, editing, printing of documents and records, as well as reporting, user management, etc.
- Providing the infrastructure for secure e-signature and electronic seal features,
- Secure access control mechanisms,
- Sefely storing electronic documents,
- Document, data and system integrity,
- When needed, integration with existing paper-based systems,

Main Security Features of the TOE;

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

Access Control: TOE has the needed capabilities to restrict access, so that only specifically authorized entities has access to TOE functions and data. For authorized users, access control is usually carried out by using authorization data. TOE may also control IP addresses of active connections, only allow for connections from pre-defined IP addresses, allow connections for a specific time interval for critical operations, include session and cookie data to the verification process for cross-checking. If the administrator(s) of the TOE use definite communication channels or locations to access to the TOE, then some restrictions may be in place to further control access to sensitive TOE functionality.

Audit: TOE automatically collects audit records to keep track of and control user activities on assets, access control and configuration changes, specifically documents and records. Contents of audit records and record keeping methods and intervals can be configured by a TOE interface.

Nobody can change or delete contents of audit records except users authorized by the TOE for these operations, including administrators. Contents of audit records can only be changed by using the functionality offered by the TOE to explicitly authorized users.

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

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

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

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

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

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

Hashing/Encryption of Sensitive Data: Examples of sensitive data are passwords or confidential

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

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

There are 8 assumptions made in the PP. The PP contains 5 Organizational Security Policies. There are 7 threats covered by operational environment and the TOE. The assumptions, the threats and the organizational security policies are described in chapter 3 in PP.

The CB(Certification Body) has examined the evaluation activities, provided the guidance for the technical problems and evaluation procedures, and reviewed each OR(Observation Reports) and ETR(Evaluation Technical Report). The CB confirmed that this PP is complete, consistent and technically sound through the evaluation results. Therefore, the CB certified that observation and evaluation results by evaluator are accurate and reasonable.

2 CERTIFICATION RESULTS

2.1 PP Identification

Project Identifier	TSE-CCCS/PP-003
PP Name and Version	Electronic Document and Records Management, Records Management, Electronic Document Management Protection

	Profile (EDRMS PP) v1.3.1
PP Document Title	Electronic Document and Records Management System Protection Profile
PP Document Version	V1.3.1
PP Document Date	24thJuly 2014
Assurance Level	EAL2+ (ALC_FLR.1, ALC_LCD.1)
Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 4, September 2012
Methodology	Common Methodology for Information Technology Security Evaluation v3.1 rev4, September 2012
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package Conformant to EAL2 + (ALC_FLR.1, ALC_LCD.1)
Sponsor and Developer	TSE
Evaluation Facility	TÜBİTAK-BİLGEM-OKTEM
Certification Scheme	Turkish Standards Institution Common Criteria Certification Scheme

2.2 Security Policy

The PP includes 6 Organizational Security Policies. These are;

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

2.3 Assumptions and Clarification of Scope

This section describes the assumptions must be satisfied by the TOE operational environment, threats satisfied by the TOE and/or operational environment. The PP includes following 8 assumptions. These are;

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

The PP includes 7threats. These are;

T.UNAUTHORIZED_ACCESS	Attacker can make an attempt to get access to TOE by using a fake/stolen identity. This attempt can be made by using a stolen identity, a faked IP address, etc. The Attacker can get unauthorized access to the TOE by making use of security breaches like keeping default usernames and passwords unchanged, use of simple passwords, not disabling test accounts on real system, unsatisfactorily controlled uploading feature. Besides, the Attacker can benefit from residual data of a previous or an active user or residual data that is created during internal or external TOE operation and communication. These data can be a critical data about the users of the TOE or the TOE itself. Attacker can have access to these data and can ease his/her/its access to the TOE, cause damage depending on the content of the data. Attacker can also access confidential data used for authentication by misguiding System_Administrator, Data_Entry_Operator or Normal_User. For instance, Attacker can have access to confidential data by redirecting System_Administrator, Data_Entry_Operator or Normal_User to a web address which doesn't belong to TOE and make the users believe that they are protected by the TOE.
T.DATA_ALTERATION	Records, documents and data protected by the TOE can be modified without permission. The Attacker can misguide System_Administrator, Data_Entry_Operator or Normal_User, to obtain TSF data or data of a specific user. The Attacker can also authorize itself illegally and change records, documents and/or other data protected by the TOE. This threat generally occurs when the integrity of the records and documents is not assured. The Attacker can also try to alter audit data. This threat occur when integrity of audit data is not assured. Another occurence of this threat is modification of the source codes and audit data of the TOE by the Attacker. Inproper file permissions or insufficient control of incoming data/files may be the cause of this threat. The Attacker may get unauthorized access to the TOE by benefiting from this threat.
T.REPUDIATION	An action or a transaction (a queue of actions) made on the TOE can be repudiated. It is relatively easier to

	repudiate actions on the TOE when insufficient or inproper audit mechanisms exist. It is usually the last task of the Attacker on the TOE, to make sure that the System_Administrator doesn't become aware of the attacking and so doesn't have the ability to take the needed actions. Additionally the Attacker can prevent audit records to be in place (for instance, by causing an overflow in audit trail). Or the Attacker can add false / high number of records to audit trail to mislead the System_Administrator.
T.DATA_DISCLOSURE	Confidential data protected by the TOE can be disclosed without permission. For instance, Normal_User can access to a record, document or data, thathe/she is unauthorized to access. Insufficient parameter controls may cause this threat. A Normal_User or Data_Entry_Operator can intentionally or unintentionally disclose confidential information by using the functinality offered by the TOE. For instance, existence of confidential user data on statistical reports is a kind of this threat. Showing credit card information of any user along with other information in user details interface is another kind of this threat. Yet another kind of this threat is that allowing bulk export /view of user data or TSF data using TOE functionality to the users having limited privileges. Another occurence of this threat is the possibility of an Attacker to disclose TSF data by using his/her attack potential.
T.DENIAL_OF_SERVICE	The Attacker can cause the TOE to become unavailable or unusable for a period of time. This is usually done by sending too many requests in a small period of time that the TOE becomes unable to respond. Simple type of denial of service includes sending too many request from a specific IP range. This is called Denial of Service (DoS). A more advanced type of denial of service threat is Distributed Denial of Service (DDoS). For DDoS attacks, no specific IP range is used. Usually BOTNETs are used for DDoS attacks. Since there is not a restriction on incoming IP addresses, it is either hard or too expensive to distinguish between normal and malicious requests.

T.HARMFUL_DATA	The Attacker can import a harmful record, document or data into the TOE. By using this threat, the Attacker can have access the data of a specific user, can take over the account of a user or can access to a part or the whole of the TOE functionality. It is a quite common fact that when the Attacker gains access, he/she/it tries to form new ways (back doors) to access to the TOE by changing TSF parameters or parameters in working environment, by defining a new user account, opening an alternative port, etc. Even when the cause of the threat is cured, the Attacker may continue to access to the TOE using the back door.

2.4 Architectural Information

Figure 1 shows the TOE and its environment. The detailed information about TOE environment can be found in the TOE Overview Section of the PP document.

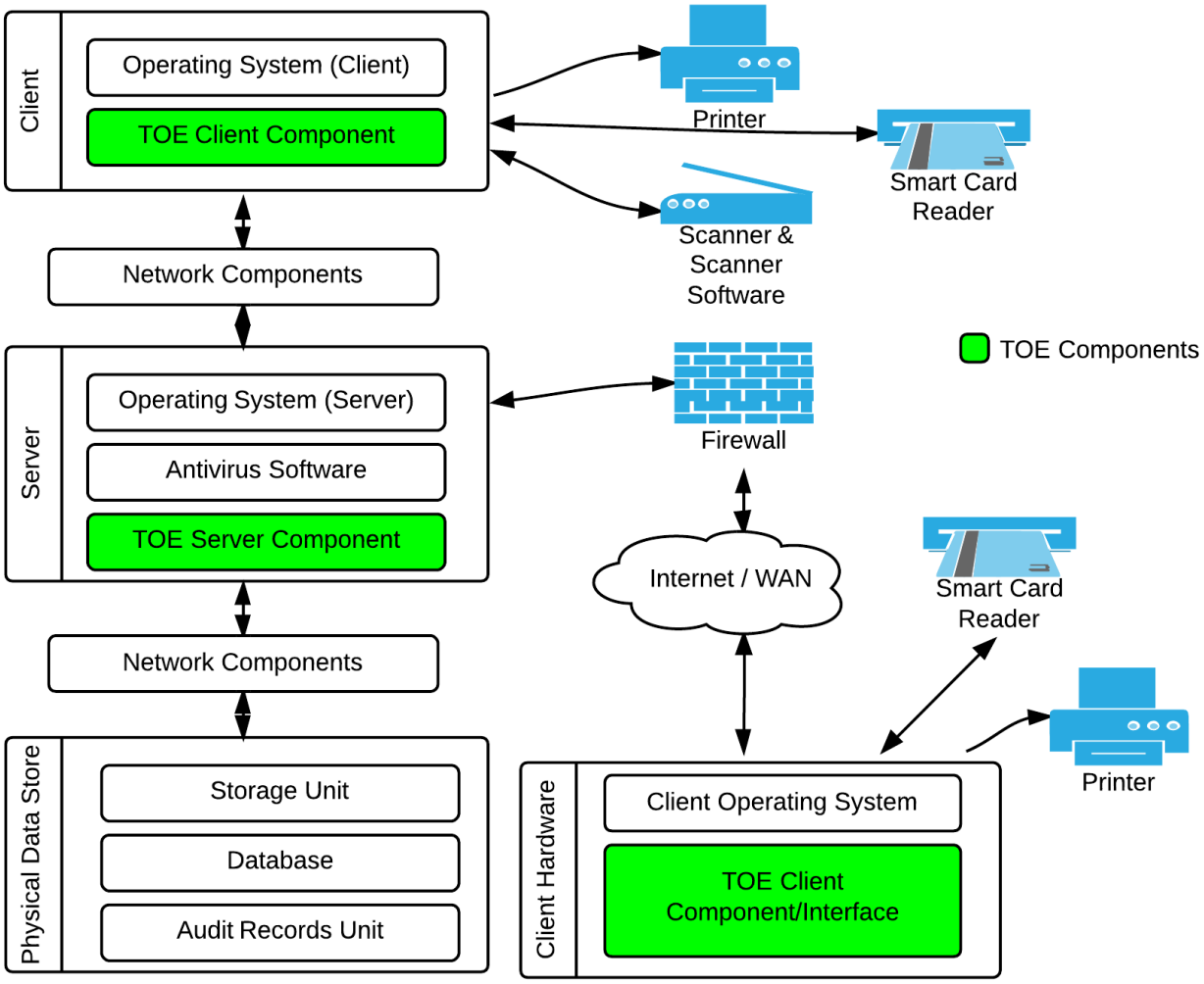

Figure 1

The green parts of the Figure 1 are the TOE and the other parts are the TOE environment. Audit Records Unit, Record/Document Storage, Database, Server, Client, Firewall, Network Components, Smart Card Reader, Antivirus Software, Scanner and Scanner Software, Storage Unit, Printer and Operating System are TOE environment as shown in the figure 1.

2.5 Security Functional Requirements

Security Functional Requirements are;

Security Audit (FAU)	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
Cryptographic Support (FCS)	FCS_COP.1(1)	Cryptographic operation (Audit Data and Record Data Integrity)
	FCS_COP.1(2)	Cryptographic operation (Generation of Hash Values)
User Data Protection (FDP)	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
Identification and Authentication (FIA)	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
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1(1)	Management of TSF data (System_Administrator)
	FMT_MTD.1(2)	Management of TSF data (Normal_User, Data Entry Operator)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_TDC.1	Inter-TSF basic TSF data consistency
Resource Utilisation (FRU)	FRU_FLT.1	Degraded fault tolerance
TOE Access (FTA)	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

2.6 Security Assurance Requirements

Assurance requirements of Electronic Document and Records Management System Protection Profile (EDRMS PP) are consistent with assurance components in CC Part 3 and evaluation assurance level is "EAL 2+". The augmented assurance components are ALC_FLR.1 and ALC_LCD.1

2.7 Results of the Evaluation

The evaluation is performed with reference to the CC v3.1 and CEM v3.1.The verdict of Electronic Document and Records Management System Protection Profile (EDRMS PP) is the pass as it satisfies all requirements of APE (Protection Profile, Evaluation) class of CC. Therefore, the evaluation results were decided to be suitable.

2.8 Evaluator Comments / Recommendations

There are no recommendations concerning the Electronic Document and Records Management System Protection Profile (EDRMS PP) v1.3.1.

3 PP DOCUMENT

Information about the Protection Profile document associated with this certification report is as follows:

Name of Document: Electronic Document and Records Management System Protection Profile (EDRMS PP)

Version No.:1.3.1

Date of Document: 24.07.2013

4 GLOSSARY

AES: Advanced Encryption Standard

BİLGEM: Informatics and Information Security Research Center

CC: Common Criteria

CCCS: Common Criteria Certification Scheme

CCEF: Common Criteria Evaluation Facility

CCMB: Common Criteria Management Board

CEM: Common Methodology for Information Technology Security Evaluation

EDRMS: Electronic Document and Records Management System

EAL: Evaluation Assurance Level

IS: Information Security

IT: Information Technology

OKTEM: Common Criteria Test and Evaluation Center

OSP: Organisational Security Policy

PP: Protection Profile

SAR: Security Assurance Requirements

SFR: Security Functional Requirements

SHA: Secure Hash Algorithm

SSL: Secure Socket Layer

TOE: Target of Evaluation

TSF: TOE Security Functionality

TSE: Turkish Standards Institution

TÜBİTAK: The Scientific and Technological Research Council Of Turkey

5 BIBLIOGRAPHY

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

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

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

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology;CCMB-2012-09-004, v3.1 rev4, September 2012

[5] Evaluation Technical Report , DTR 29 TR 01 – 25.07.2014

[6] YTBD-01-01-TL-01 Certification Report Writing Instructions

[7] Electronic Document and Records Management System Protection Profile, v1.3.1, 24.07.2014

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections.