Certification Report

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

SENEKA YAZILIM DONANIM BİLİŞİM TİCARET TAAHHÜT VE SAN. LTD. ŞTİ.

Seneka EBDYS v1.0

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-43

TABLE OF CONTENTS

DOCUMENT INFORMATION

Date of Issue	July 20, 2017
Approval Date	July 21, 2017
Certification Report Number	21.0.03/17-006
Sponsor and Developer	SENEKA Yazilim Donanim Bilişim Ticaret Taahhüt Ve San. Ltd. Şti.
Evaluation Facility	Beam Teknoloji A.Ş
TOE	Seneka EBDYS v1.0
Pages	21

Prepared by	Halime Eda BİTLİSLİ
Reviewed by	İbrahim Halil KIRMIZI

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.

DOCUMENT CHANGE LOG

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
1.0	July 20, 2017	All	First Release

DISCLAIMER

This certification report and the IT product 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 product 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 product 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 product 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 ITCD 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 (CCSS) 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 = Common Criteria Testing Laboratory) 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 product have been performed by Beam Technology Testing Facility, which is a commercial CCTL.

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

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Seneka EBDYS v1.0 whose evaluation was completed on 14 July, 2017 and whose evaluation technical report was drawn up by Beam Technology Testing Center (as CCTL), and with the Security Target document with version no 19.0 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD 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

1.1 TOE Overview

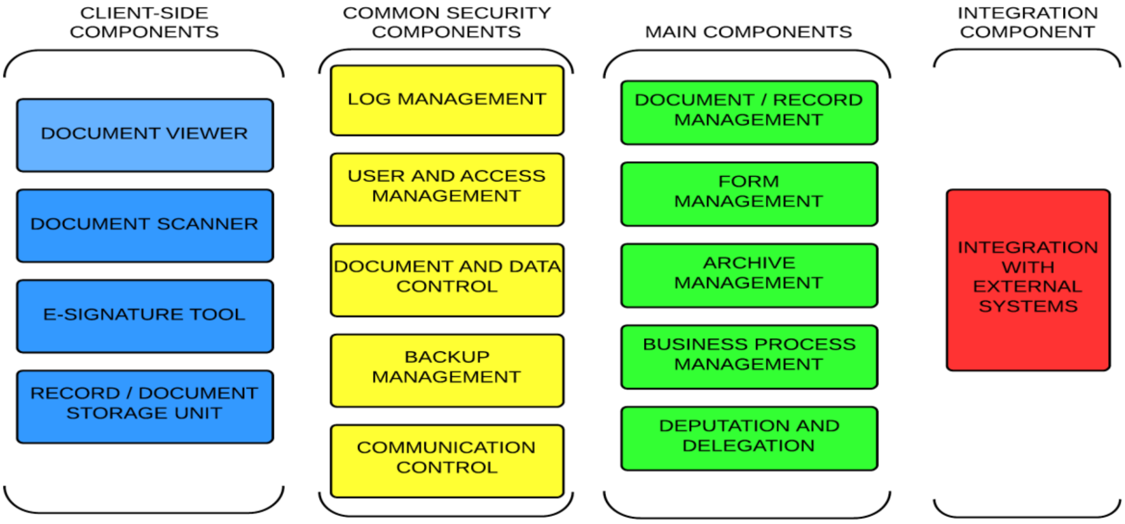
TOE is a web-based application of electronic document and records management system. Aim of the TOE is to manage documents which are a part of the evidences of organizational processes, to protect these documents in terms of content and form and manage these documents from creation to the archival processes. 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.



CLIENT-SIDE COMPONENTS
DOCUMENT VIEWER
DOCUMENT SCANNER
E-SIGNATURE TOOL
RECORD / DOCUMENT STORAGE UNIT
COMMON SECURITY COMPONENTS
LOG MANAGEMENT
USER AND ACCESS MANAGEMENT
DOCUMENT AND DATA CONTROL
BACKUP MANAGEMENT
COMMUNICATION CONTROL
MAIN COMPONENTS
DOCUMENT / RECORD MANAGEMENT
FORM MANAGEMENT
ARCHIVE MANAGEMENT
BUSINESS PROCESS MANAGEMENT
DEPUTATION AND DELEGATION
INTEGRATION COMPONENT
INTEGRATION WITH EXTERNAL SYSTEMS

Figure 1: Typical Components of an EDRMS System

1.2 Main Security Features

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.

1.3 Threats

Assumption	Definition
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.

Table 1: Threats

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-43
TOE Name and Version	Seneka EBDYS v1.0
Security Target Title	Seneka EBDYS Security Target
Security Target Version	v.19.0
Security Target Date	July 3, 2017
Assurance Level	EAL 2+ (ALC_FLR.1, ALC_LCD.1)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	Electronic Document and Records Management System Protection Profile Version 1.3.2
Common Criteria Conformance	• 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, extended • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, conformant
Sponsor and Developer	SENEKA Yazılım Donanım Bilişim Ticaret Taahhüt ve San. Ltd. Şti.
Evaluation Facility	BEAM Teknoloji A.Ş.
Certification Scheme	TSE CCCS

2.2 Security Policy

Policy	Definition
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.

Table 2: Organizational Security Policies

2.3 Assumptions

Assumption	Definition
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

Table 3: Assumptions

2.4 Architectural Information

2.4.1 Logical Scope

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.

2.4.2 Hardware and Software Operational Environment Components

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.

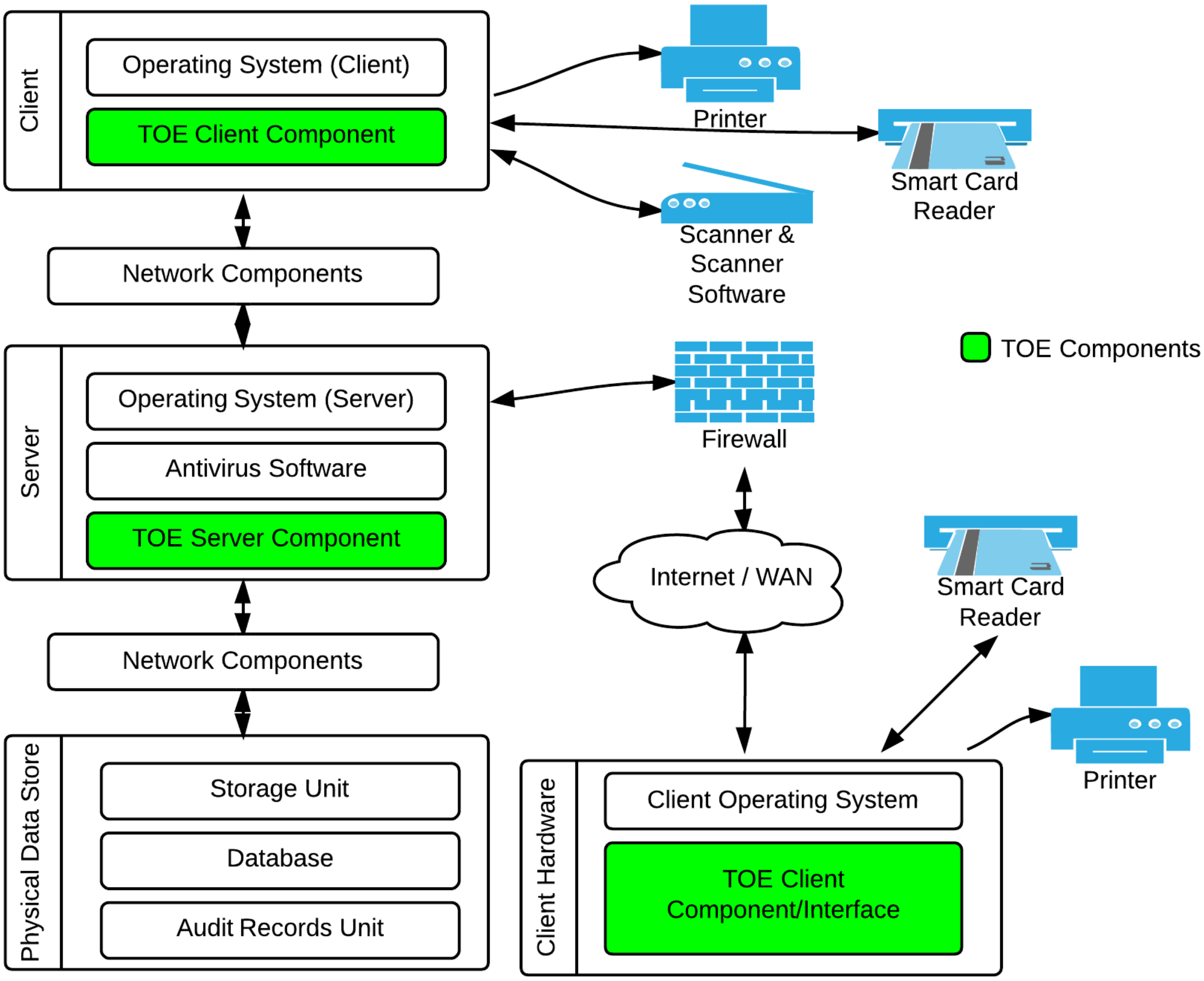


Figure 2: TOE and its Operational Environment

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.

2.5 Documentation

These documents listed below are provided to customer by the developer alongside the TOE:

Document Name	Version	Release Date
Seneka EBDYS Security Target	19.0	03.07.2017
Seneka EBYS Teknik Kurulum Kılavuzu	3.0	08.03.2017
Seneka EBYS Yönetim Ekranı Yardım Kılavuzu	14.0	28.04.2017
Seneka EBYS Son Kullanıcı Yardım Kılavuzu	8.0	03.07.2017

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report v3.2 of Seneka EBDYS v1.0 . It is concluded that the TOE supports EAL 2+ (ALC_FLR.1, ALC_LCD.1)

IT Product Testing is mainly realized in two parts:

1-Developer Testing:

Developer has done total of 32 functional tests.

- **TOE Test Coverage:** Developer has prepared TOE Test Document according to the TOE Functional Specification documentation.
- **TOE Test Depth:** Developer has prepared TOE Test Document according to the TOE Design documentation which includes TSF subsystems and its interactions.
- **TOE Functional Testing:** Developer has made functional tests according to the test documentation. Test plans, test scenarios, expected test results and actual test results are in the test documentation.

2- Evaluator Testing:

Independent Testing: The evaluator conducted testing using all of developer tests found in the developer’s test plan and procedures. Additionally, the evaluator conducted 15 independent tests prepared by the evaluators themselves. All off these tests have ensured that TOE is capable of demonstrating the functional requirements stated in security document. TOE has successfully passed all tests.

Penetration Testing: Evaluator has done 12 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. During devising the tests, a flaw hypothesis was prepared considering:

- SFRs in security target,
- Modules in design document,
- Architectural elements in architecture document,
- Guidance documents,
- Internet search for publicly known vulnerabilities of TOE and tools used to create TOE etc.

TOE has successfully passed all tests.

2.7 Evaluated Configuration

System Requirements:

- Microsoft Visual C++ 2010x86 (e-signature)
- Microsoft Visual C++ 2010x64 (e- signature)
- Microsoft .NET Framework 4.5
- Kamu SM Drivers , Card Reader ve AKİS Smart Card
- Java Runtime Environment 7 for AKİS Smart Card

Server Requirements:

- Intel(R) Xenon(R) CPU E5-2420 0 @ 1.90GHz,
- 64.0 GB RAM,
- 64-bit Operating System

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL2+ (ALC_FLR.1, ALC_LCD.1) and the security target evaluation) is summarized in the following table:

Assurance Class	Component ID	Component Title	Verdict
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.2	Security- enforcing functional specification	PASS
	ADV_TDS.1	Basic design	PASS
AGD: Guidance documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC: Life-cycle support	ALC_CMC.2	Use of a CM coverage	PASS
	ALC_CMS.2	Parts of TOE CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
	ALC_LCD.1	Developer defined life-cycle model	PASS
	ALC_FLR.1	Basic flaw remediation	PASS
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims	PASS
	ASE_ECD.1	Extended components definition	PASS
	ASE_INT.1	ST introduction	PASS
	ASE_OBJ.2	Security objectives	PASS
	ASE_REQ.2	Security requirements	PASS

	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS
ATE: Tests	ATE_COV.1	Evidence of coverage	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “Seneka EBDYS v1.0” product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The security target associated with this Certification Report is identified by the following terminology:
Title: Seneka EBDYS Security Target
Version: 19.0
Date of Document: July 3, 2017

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

4 GLOSSARY

ADV : Assurance of Development

AGD : Assurance of Guidance Documents

ALC : Assurance of Life Cycle

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCRA : Common Criteria Recognition Arrangement

CCTL :Common Criteria Test Laboratory

CEM :Common Evaluation Methodology

CMC : Configuration Management Capability

CMS : Configuration Management Scope

DEL : Delivery

EAL : Evaluation Assurance Level

OPE : Opretaional User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

PRE : Preperative Procedures

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012

[3] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel. Date: February 8, 2016

[4] BTTM-CCE-005 ETR v3.2, Rel. Date: July 14,2017

[5] Seneka EBDYS Security Target, Version 19.0, Rel. Date: July 3, 2017