Certification Report

EAL 2 Evaluation of

AKGÜN BİLGİSAYAR PROGRAM ve HİZMET SAN. TİC.LTD.ŞTİ

Akgün HIS v.4.0

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-52

TABLE OF CONTENTS

DOCUMENT INFORMATION

Date of Issue	March 09, 2018
Approval Date	March 09 , 2018
Certification Report Number	21.0.03/18-005
Sponsor and Developer	AKGÜN BİLGİSAYAR PROGRAM ve HİZMET SAN. TİC.LTD.ŞTİ
Evaluation Facility	BEAM TEKNOLOJI A.Ş.
TOE	AKGÜN HIS v.4.0
Pages	17

Prepared by	H.Eda BİTLİSLİ ERDİVAN
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	March 09, 2018	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 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 AKGÜN HIS v.4.0 whose evaluation was completed on 27.02.2018 and whose evaluation technical report was drawn up by Beam Technology (as CCTL), and with the Security Target document with version no 2.1 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 EAL2. 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 logical security module for web-based health information system. The web-based health information management system mentioned here refers to an application which hosts and processes all kinds of patient data and which can be accessed online.
TOE is a general one, which is prepared for Hospital Information Management System which provides online services.

Since the TOE operates on a network, it interacts with the components of that network. There is a web server on which the TOE operates and this web server operates on an operating system, which operates on a hardware server.
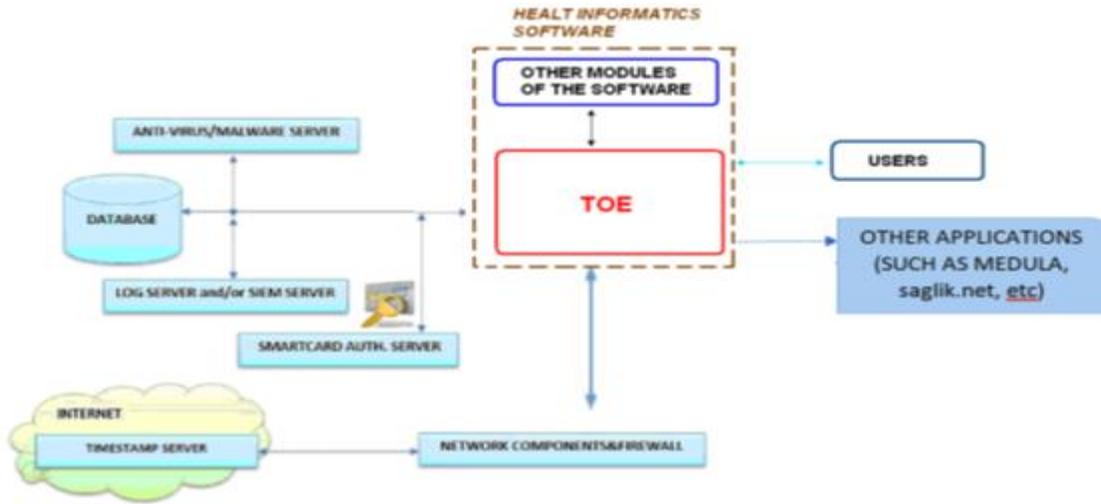
***Figure 1** – The overall structure of typical operational environment of the TOE. TOE components are shown by red. All the communication between the TOE and its environmental components should be done by SSL.*

1.2 TOE major security features

Authentication and authorization: It is because the TOE users may access through an unsecure environment, effective authentication and authorization processes are required to apply. Authentication is performed through user name and password verification. Hash functions (in general) are applied to passwords to prevent them from reversing to the original. After the authentication is successfully completed, then the TOE will authorize the users and give access rights to them based on their user types and roles. The roles are explained in 1.2.4.

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

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

Administration: TOE provides effective control mechanisms for the users responsible for administration of the system. It is important that these mechanisms make decision making process easier and more effective. TOE provides system administrator's authorization and data management functionalities. Administrator is the role that performs functions related to the administration of the TOE. User is the role that uses the TOE within the limits of authorization.

Data protection: TOE keeps records of two kinds of data in general, the patient data and the user data. TOE is responsible for protecting these data. It is noted that protection is being provided not only for storing of the data but also during the transmission of the data. Data protection is performed by an effective authentication and authorization mechanisms, access control policies, and administrative and auditing operations.

Secure Communication: TOE needs to communicate both with its components and with other components such as databases, etc. Those communications are done in a secure way, using the SSL protocol. Secure communication will ensure that sniffing over the network will be prevented and the data transferred between the components are protected against the attackers.

1.3 Threats

Threats averted by TOE and its environment are described in this section. Threats described below results from assets which are protected or stored by TOE or from usage of TOE with its environment.

Threats	Statements
T. COMM	The unauthorized user gains access to the user data and the patient data when it is traversing across the internet from to the application resulting in a loss of confidentiality and integrity of user data.
T.PRVLG_ESC	An attacker/ a limitedly authorized user may modify management data that they are not authorized and gain access to the sensitive like patient data and system data by privilege escalation.
T.UNAUTH	An unauthorized user obtains or modifies stored user data that they are not authorized to access resulting in a loss of confidentiality or integrity of the data.
T.AUDIT_TRAIL	A threat agent may perform a large amount of transactions in order to fill the logs and hence make audit unavailable

T.DoS	An attacker may attempt to make service unavailable by overwhelming it with traffic from multiple sources.
T.PASSWORD	An attacker/unauthorized user may get the passwords in the database and authenticate to the TOE by these passwords causing confidentiality or integrity damage of user or management data.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-52
TOE Name and Version	Akgün HIS v.4.0
Security Target Title	AKGUN HEALTH INFORMATION SYSTEM v4.0 Security Target
Security Target Version	v2.2
Security Target Date	02.03.2018
Assurance Level	EAL2
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	Protection Profile for Security Module of General-Purpose Health Informatics Software v 1.0
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	AKGÜN BİLGİSAYAR PROGRAM ve HİZMET SAN.TİC.LTD.ŞTİ
Evaluation Facility	BEAM TEKNOLOJI A.Ş.
Certification Scheme	TSE CCCS

2.2 Security Policy

The organizational security policies are described in below;

Assumption	Explanation
P.VEM	TOE is able to transfer the available data (if available) stored in the database securely whenever the TOE is installed in the first time. Besides whenever TOE is uninstalled, TOE is able to prepare the data for the transfer to a new software. During this data transfer process, the integrity of the data is provided by the TOE.

Application Note: The format of data for the transfer follow the rules defined by the Republic of Turkey, Ministry of Health. This format is also known as VEM. The details of the VEM can be found on the web site of the Ministry of Health.

2.3 Assumptions and Clarification of Scope

Assumptions made during the preparation are collected under two main headings:

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

Assumptions on Personnel

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

Assumptions on Physical Environment

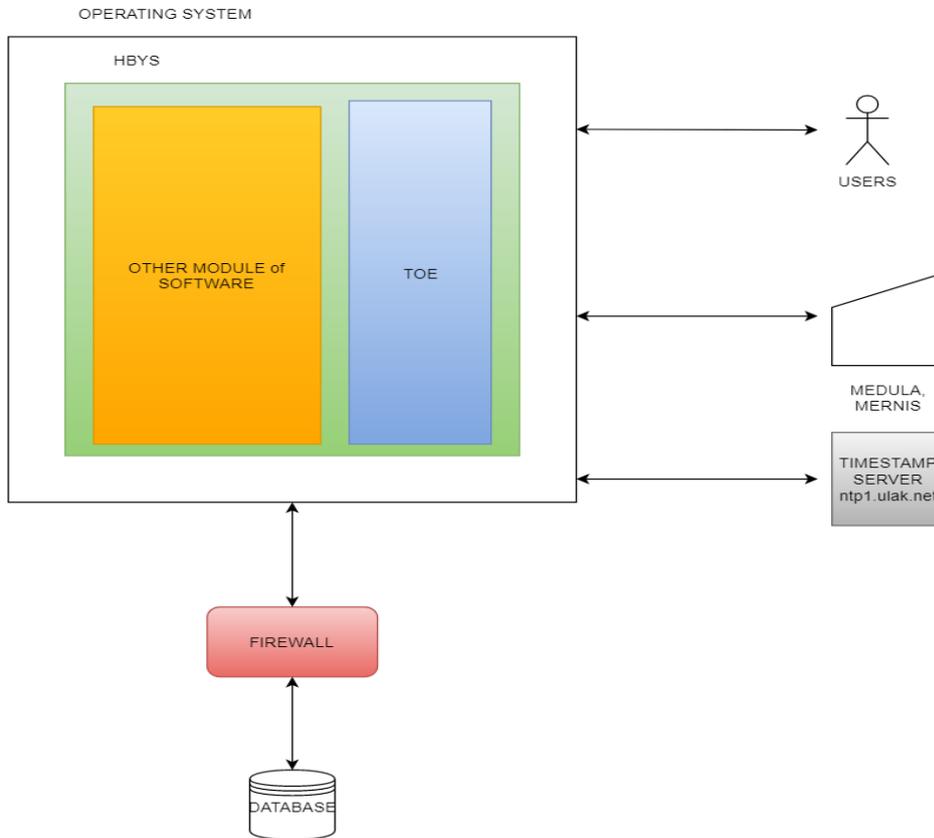| Assumption	Explanation
A.PHYSICAL	It is assumed that the servers that host the web and database servers are hosted in a secure operating facility with restricted physical access with non- shared hardware.

.

2.4 Architectural Information

2.4.1 Logical Scope

TOE allows for auditing the checking in and out of the patients, examinations and reviews, and other related reports and materials. Thus, the TOE allows for accessing the patients' medical history immediately. Additionally the TOE allows saving the individual information (date of birth, place of birth, blood type, etc.), contact information (Social Security Number, citizenship number, etc.) of the patient and the surgeries that the patient had before. The TOE additionally provides basic security functions like authentication, access control, secure communication and security management in order to provide security for the patient information. TOE provides access permissions, TOE automatically audits logs, TOE provides effective control mechanisms, and TOE keeps records. More detailed description of the implementation of security functions is provided in "**Hata! Başvuru kaynağı bulunamadı.**" part of Security Target.

2.4.2 Physical Scope

TOE is a logical security modüle for web-based health information system.

2.5 Documentation

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

Document Name	Version	Release Date
AKGUN HEALTH INFORMATION SYSTEM v4.0 Security Target	2.2	02.03.2018
CAS User Manual	0.4	05.02.2018
Out Patient Module Manual	0.1	24.11.2017
Installation Manual	0.8	24.11.2017

Table-5 Documentation

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 v4.2 of Akgün HIS v4.0. It is concluded that the TOE supports EAL 2.

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 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 28 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 17 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,
- 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

The TOE operates on a web server as a web application. This web server can be any Java container or J2EE container. Application servers that used in evaluation are Tomcat for Akgün HIS and GlassFish for CAS. Server configuration is 32 GB Ram, 250 GB HDD space and 2vCPU. Also DBMS configuration is 32 GB Ram, 2 vCPU, 500 GB HDD space.

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL2 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 system	PASS
	ALC_CMS.2	Parts of the TOE CM coverage	PASS
	ALC_DEL.1	Delivery procedures	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

Table-6 Results of the evaluation

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of "AKGÜN HIS v4.0" 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: AKGUN HEALTH INFORMATION SYSTEM v4.0 Security Target
Version: 2.2
Date of Document: 02.03.2018

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 ACRONYMS

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