Certification Report

EAL 2 Evaluation of

Mergen Yazılım A.Ş

Mergen HBYS Security Module v1.18.1

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-55

TABLE OF CONTENTS

DOCUMENT INFORMATION

Date of Issue	February 20th, 2019
Approval Date	February 20th, 2019
Certification Report Number	21.0.03/19-001
Sponsor and Developer	Mergen Yazılım A.Ş
Evaluation Facility	Beam Technology Test Center
TOE	Mergen HBYS Security Module v1.18.1
Pages	13

Prepared by	Cem ERDİVAN Common Criteria Inspection Expert
Reviewed by	İbrahim Halil KIRMIZI Common Criteria Technical Responsible (Software Product Group)

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	February 20th, 2019	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 5, using Common Methodology for IT Products Evaluation, version 3.1, revision 5. 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 Mergen HBYS Security Module v1.18.1 whose evaluation was completed on February 20th, 2019 and whose evaluation technical report was drawn up by Beam Technology (as CCTL), and with the Security Target document with version no 1.5 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 general-purpose health information management system. The health information management system refers to an application which hosts and processes all kind of patient data and which can be accessed online.

Security module, as TOE, is responsible for protecting health information management system data. So TOE ensures that user and patient information are protected towards unauthorized access. Along with that, any users' security activities are recorded via audit logs and communication path between peer to peer is securely protected by using secure protocols like HTTPS. TOE serves GUI to manage users, user roles and security attributes to system administrator and serves GUI to view user and system activities (logs) to auditor.

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.

1.2 Threats

Threats are defined in Section 3.1.1 of Security Target Document v1.5.

2 - CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-55
TOE Name and Version	Mergen HBYS Security Module v1.18.1
Security Target Title	Mergen HBYS Security Module v1.18.1 Security Target
Security Target Version	V1.5
Security Target Date	November 27th, 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 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 5, April 2017
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
Protection Profile Conformance	TSE-CCS/PP-011 Protection Profile for Security Module of General-Purpose Health Informatics Software v1.0

Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, conformant • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, conformant
Sponsor and Developer	Mergen Yazılım A.Ş.
Evaluation Facility	Beam Technology Test Center
Certification Scheme	TSE CCCS

2.2 Security Policy

TOE Security Policy consists of security functions described in section 1.4.2 Logical Scope of Security Target Document v1.5.

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, contact information 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. The explanation of these security related attributes of the TOE are as follows:

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. Hashing information saved together with the salt variant. 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.

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 should be 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 should make decision-making process easier and more effective. TOE provides system administrator's authorization and data management functionalities. Only the authorized users can access interfaces provided for administration of the TOE and more strict security measures are applied to those interfaces. Roles defined for the TOE are administrator, end user, system user and the auditor.

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. Auditor is the role that can use only auditing functions, which are used in audits.

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 should be noted that protection should be 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. Those communications should be 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.

2.3 Assumptions and Clarification of Scope

Please refer to Security Target Document v1.5 Section 3.1.2 for OSPs and Section 3.1.3 for Assumptions.

2.4 Architectural Information

2.4.1 Logical Scope

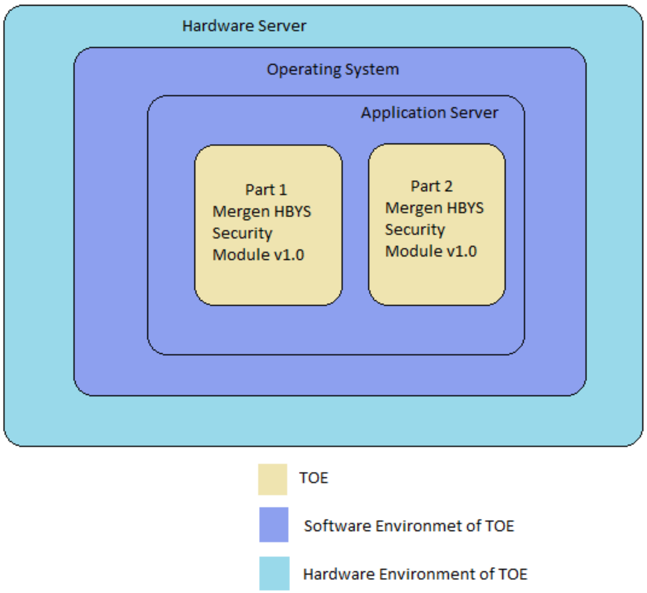
TOE enforces the users for identification and authentication. If the identification and authentication processes are successful, the authorization mechanism will provide access rights. TOE resources are restricted with an effective authorization mechanism. At the same time, passwords are stored in the database with salted hash. Access rights are restricted for users to access operations. Only authorized users can access defined resources.

The activities of the users can be monitored by the system auditor. At the same time, audit records are read only record. Audit records can not be deleted or updated by any role. When the audit records are full, the up to date audit records overwrite the oldest audit record.

TOE provides efficient interfaces for managing the system for administrator with special access rights. The system administrator can assign roles to the users. There are four roles defined in the TOE. These roles are end user, system user, system administrator and system auditor.

The TOE provides security for all data stored in the system, which are private data of the users, system options/references and logs. TOE does identification by using username, authentication with password, authorization by user’s capability and system hierarchy to access control and auditing of these. At the same time, the TOE provides secure communication for data transfer using network protocols; HTTPS (Secure Hypertext Transfer Protocol) for Presentation layer, IIOP (Internet Inter-ORB Protocol) for Business layer, JDBC (Java Database Connectivity) Protocol for Data Access layer.

2.4.2 Physical Scope



Hardware Server
Operating System
Application Server
Part 1 Mergen HBYS Security Module v1.0
Part 2 Mergen HBYS Security Module v1.0
TOE
Software Environmet of TOE
Hardware Environment of TOE

Figure-1 TOE Architecture

TOE is a web based application which runs on a web server and there is no need any hardware components.

TOE uses web server connection pool to connect database.
The TOE is shown in two parts:

Part 1 includes authentication mechanism. All users are identified and authenticated from here. Part 1 serves as a Central Authentication Server to check username and password. If username and password are ok to success login, a session token is generated to be used by HBYS modules and so user is able to access modules.

Part 2 does all other operations except authentication and that is a interceptor layer to filter and do operations about requests. Authorization, management, auditing, access control are the main tasks which are handled by that.

TOE is a part of the HBYS product which is served by JAR and WAR packages to the customer companies. Product is uploaded to "Mergen Yazılım" FTP servers. Customer's IT Professional downloads packages using username, password and ftp address which is given by Mergen Yazılım, and deploys to their application servers.

2.5 Documentation

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

Document Name	Version	Release Date
Mergen HBYS Security Module v1.18.1 Security Target	V1.5	November 27th, 2018
Mergen HBYS Security Module v1.18.1 Operational User Manual	v1.3	November 20th, 2018

2.6 IT Product Testing

- **Developer Testing:** All TSFIs have been tested by developer. Developer has conducted 29 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted all 29 developer tests. Additionally, evaluator has prepared 8 independent tests. TOE has passed all 37 functional tests to demonstrate that its security functions work as it is defined in the ST.
- **Penetration Tests:** TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 17 penetration tests have been conducted. TOE proved that it is resistant to “Attackers with Basic Attack Potential”.

2.7 Evaluated Configuration

TOE Configuration:

Mergen HBYS Security Module v1.18.1

Required Minimum Hardware Configuration:

Web Server	
CPU	2 Core 2.6 Ghz
Memory	16 GB
Operating System	Debian 9.2 / Windows 10
Disk	60 GB
Application Server	Glassfish 4.1 Build 13
Connectivity	TCP/IP
Database Server	
CPU	2 Core 2 Ghz
Memory	32 GB
Disk	300 GB
Operating System	Oracle Linux 6.x, Oracle Linux 7.x
RDBMS	Oracle 11gR2
Connectivity	JDBC

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:

Class Heading	Class Family	Description	Result
ADV: Development	ADV_ARC.1	Security architecture description	PASS

Class Heading	Class Family	Description	Result
	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: Lifecycle 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	Derived 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 Analysis	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 “Mergen HBYS Security Module v1.18.1” 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: Mergen HBYS Security Module v1.18.1 Security Target
Version: v1.5
Date of Document: November 27th, 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 - BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017

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

[4] ETR v2.2 of Mergen HBYS Security Module v1.18.1, Rel. Date: February 19th, 2019

[5] Mergen HBYS Security Module v1.18.1 Security Target, Version 1.5, Rel. Date: November 27th, 2018