	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No



Certification Report

EAL 2 Evaluation of

TURKISH STANDARDS INSTITUTION

**Protection Profile for Security Module of General-Purpose Health
Informatics Software
Version 1.0**

issued by

**Turkish Standards Institution
Common Criteria Certification Scheme**

Certificate Number: TSE-CCCS/PP-011



	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No



TABLE OF CONTENTS

TABLE OF CONTENTS	2
Document Information	3
DISCLAIMER	3
FOREWORD	4
RECOGNITION OF THE CERTIFICATE	4
1 - EXECUTIVE SUMMARY	5
1.1 Introduction	5
1.2 Usage and Major Basic Security and Functional Attributes	5
1.3 Threats	6
2 CERTIFICATION RESULTS	8
2.1 PP Identification	8
2.2 Security Policy	8
2.3 Assumptions and Clarification of Scope	9
2.4 Architectural Information	9
2.5 Security Functional Requirements	10
2.6 Security Assurance Requirements	10
2.7 Results of the Evaluation	11
2.8 Evaluator Comments / Recommendations	11
3 PP DOCUMENT	12
4 BIBLIOGRAPHY	13

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

Document Information

Date of Issue	08.09.2016
Approval Date	09.09.2016
Certification Report Number	21.0.03/16-006
Sponsor and Developer	Turkish Standards Institution
Evaluation Facility	TÜBİTAK BİLGEM OKTEM
PP Name	Protection Profile for Security Module of General-Purpose Health Informatics Software
Pages	13


Prepared by	Cem 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	08.09.2016	ALL	First release

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.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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 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 Protection Profile for Security Module of General-Purpose Health Informatics Software v1.0 whose evaluation was completed on 07.09.2016 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the PP document with version no 1.0 of the relevant product.

The certification report, certificate of PP evaluation and PP 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>.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

1 - EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: Protection Profile for Security Module of General-Purpose Health Informatics Software
PP version: v1.0

Developer's Name: Turkish Standards Institution

Name of CCTL: TÜBİTAK BİLGEM OKTEM

Assurance Package: EAL2

Completion date of evaluation: 07.09.2016

1.1 Introduction

TOE is a logical security module for both desktop and web-based general-purpose health information management system. The health information management system mentioned here refers to an application which hosts and processes all kind of patient data and which can be accessed online.

This protection profile is a general one, which is prepared for Hospital Information Management System, Family Practice Information System, Picture Archiving and Communication System (PACS), Laboratory Information Management System, Digital Document Management System and other health informatics application software, which provides online services. Therefore, in this protection profile the security functional requirements, that are common in those applications above, have been taken into consideration.

The type of the TOE is a logical security module for web based or desktop based general purpose health information systems application.

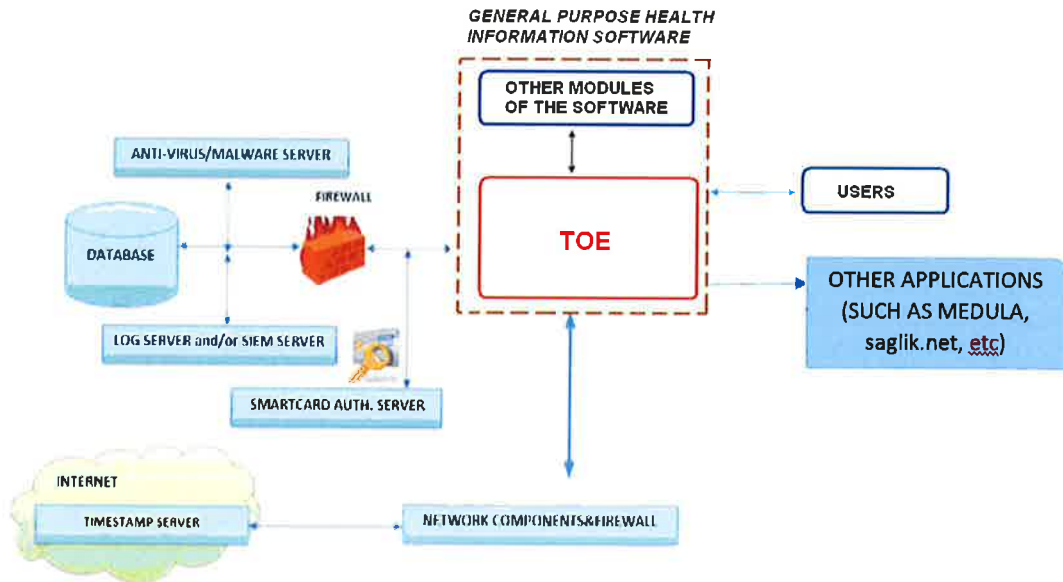



Figure 1: The overall structure of typical operational environment of the TOE. TOE components are shown by red. All the communication between the TOE and its environmental components should be done by SSL.

1.2 Usage and Major Basic Security and Functional Attributes

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

Sayfa 5/13

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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. However it is recommended that hashing information should be 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. The roles are explained in 1.3.4.

Application note: In the context of this protection profile authentication is performed through user name and password verification. When high level of security is needed, additional authentication methods like SMS confirmation, verification through mobile devices, electronic signature, etc. could be used in addition to user name and password verification. In this case the necessary SFRs should be added to the ST of the TOE.

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 as a minimum 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 (structuring settings, reviewing the logs, etc.), 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, etc. 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.


1.3 Threats

The threat agents are described below;


- Attackers who have knowledge of how the TOE operates and are assumed to possess a basic skill level, and intend to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE users who have extensive knowledge about the TOE operations and are assumed to have a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE.

The TOE address the following threats are applicable listed in table below:

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

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

	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.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

2 CERTIFICATION RESULTS


2.1 PP Identification

Certificate Number	TSE-CCCS/PP-011
PP Name and Version	Protection Profile for Security Module of General-Purpose Health Informatics Software v1.0
PP Document Title	Protection Profile for Security Module of General-Purpose Health Informatics Software
PP Document Version	1.0
PP Document Date	07.09.2016
Assurance Level	EAL2
Criteria	<ul style="list-style-type: none"> • 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	None
Common Criteria Conformance	<ul style="list-style-type: none"> • 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, conformant. • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, conformant
Sponsor and Developer	Turkish Standards Institution
Evaluation Facility	TÜBİTAK BİLGEM OKTEM
Certification Scheme	TSE CCCS

2.2 Security Policy

The security policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

- Security Management
- Protection of The TSF
- Trusted Path/Channels

2.3 Assumptions and Clarification of Scope

The organizational security policies are described in below;

P.VEM	TOE should be 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 should be able to prepare the data for the transfer to a new software. During this data transfer process, the integrity of the data should be provided by the TOE.
--------------	---

Application Note: The format of data for the transfer should 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.

The assumptions are described in below;

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.
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.

2.4 Architectural Information

This section provides detailed description of the TOE and discusses the software and hardware components of the TOE (operational environment) and basic security and functional features of the TOE. Since TOE is the logical security module for general purpose health information software, the operational environments components of the TOE is given in the following sections.

Operational Environment Components and Supported Non-TOE Software and Hardware Components for TOE

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.

This section identifies peripheral software and hardware components (typically and some optionally), which interact with the TOE. Figure 1 shows how the TOE interacts with the operational environment. During the interactions all the communications between the TOE and its mandatory/optional components are performed by SSL communication protocol.

The mandatory and optional components of the TOE are explained below:


Web server: The TOE operates on a web server as a web application. This web server may use any technology.

Operating system: The server that the TOE runs on has an operating system. The web server that the TOE runs on, operates on this operating system and uses the sources of this system through this operating system.

Hardware server: The TOE operates on a server. This server may have different features varying from product to product.

Network components and the firewall: The TOE interacts with the network components in order to exchange patient and other related information. This interaction is carried out through the operating system and the server. Internet access of the TOE is controlled by a firewall.

Time stamp server: The TOE requires time stamp server, which is provided by operational environment in order to secure logs. This time stamp server provides timestamps based on electronic signatures (which is hardware created). It is assumed that time server runs on a secure server and time information obtained from this server is also assumed to be secure.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

Database: TOE saves all of the user and patient records in this database. There is a firewall protecting this database.

Communicating with other applications (optional): TOE may need to interact with the other applications such as saglik.net, e-nabiz, MEDULA, etc. In these cases TOE needs to provide a secure communication with these applications.

Log server and/or SIEM server (optional): This component is optional in the TOE environment. A log server will enable the TOE Audit logs to be stored and managed centrally thereby increasing availability of the audit logs. These audit logs can also be correlated by a SIEM server in order to identify and respond to cyber-attacks.

Application note: Log server and/or SIEM server usage is optional in the context of this protection profile. If Log server and/or SIEM server is used in the TOE, then the necessary SFRs should be added to Security Target of the TOE.

Smartcard Authentication server (SAS) (optional): This component is optional in the TOE environment. Smartcard authentication will enable the TOE to utilize strong authentication instead of weak authentication mechanism such as password authentication.

Application note: Smartcard authentication is optional in the context of this protection profile. If smartcard authentication is used in the TOE, then the necessary SFRs should be added to Security Target of the TOE.

Anti-virus/Malware Server (optional): This component is optional in the TOE environment. An anti-virus/malware server will protect the TOE from virus and malware and the threats that can be introduced to the environment by these elements such as sniffing, data corruption etc.


Application note: Anti-virus/Malware server usage is optional in the context of this protection profile. If Anti-virus/Malware server is used in the TOE, then the necessary SFRs should be added to Security Target of the TOE.

2.5 Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit Review
	FAU_STG.1: Protected Audit Trail Storage
	FAU_STG.4: Prevention of audit data loss
FCS: Cryptographic Support	FCS_COP.1: Cryptographic Operation
FDP: User Data Protection	FDP_ACC.1: Subset Access Control
	FDP_ACF.1: Security Attribute Based Access Control
FIA: Identification and Authentication	FIA_AFL.1: Authentication failure handling
	FIA_UID.2: User identification before any action
	FIA_UAU.2: User authentication before any action
FMT: Security Management	FMT_MSA.1: Management of Security Attributes
	FMT_MSA.3: Static Attribute Initialization
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of The TSF	FPT_STM.1: Reliable time stamps
FTP: Trusted Path/Channels	FTP_TRP.1: Trusted Path

2.6 Security Assurance Requirements

Assurance requirements for Protection Profile for Security Module of General-Purpose Health Informatics Software v1.0 are consistent with assurance components in CC Part 3 and evaluation assurance level is EAL2.


	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

2.7 Results of the Evaluation

The evaluation is performed with reference to the CC v3.1 and CEM v3.1. The verdict of Common Criteria Protection Profile for Security Module of General-Purpose Health Informatics Software v1.0 is “pass” as it satisfies all requirements of APE class of CC. Therefore, the evaluation results were decided to be “suitable”.

2.8 Evaluator Comments / Recommendations

There are no recommendations concerning the Common Criteria Protection Profile for Security Module of General-Purpose Health Informatics Software v1.0.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No


3 PP DOCUMENT

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

Name of Document: Common Criteria Protection Profile for Security Module of General-Purpose Health Informatics Software
Version No: 1.0

Date of Document: 07.09.2016

C. C. 

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

4 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: August,4,2015
- [4] Criteria Protection Profile for Security Module of General-Purpose Health Informatics Software Version No: 1.0, 07.09.2016
- [5] ETR 58 TR 01 /07.09.2016