Certification Report

EAL 2 Evaluation of

TELE MEDİKAL YAZILIM VE BİLİŞİM TEKNOLOJİ ÜRÜNLERİ SAN. VE TİC. LTD. ŞTİ.

TMYPACS v1.3.18

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-87

TABLE OF CONTENTS

Document Information

Date of Issue	**21/04/2023**
Approval Date	**23/06/2023**
Certification Report Number	**21.0.03/23-004**
Sponsor and Developer	**Tele Medikal Yazılım ve Bilişim Teknoloji Ürünleri Sanayi ve Tic. Ltd. Şti.**
Evaluation Facility	**Beam Teknoloji A.Ş.**
TOE/ PP Name*	**TMYPACS v1.3.18**
Pages	**18**

Prepared by *(Common Criteria Expert)*	**Göktuğ İLISU** **Common Criteria Inspection Expert**
Reviewed by *(Reviewer)*	**Mehmet Kürşad ÜNAL** **Common Criteria Technical Responsible**

The experts whose names and signatures are shown as above prepared and reviewed this report.

Document Change Log

Release	**Date**	**Pages Affected**	**Remarks/Change Reference**
1.0	**11/04/2023**	**All**	**First Release**
2.0	**21/06/2023**	**1, 3, 10, 17**	**Second Release**

DISCLAIMER

This certification report and the IT product/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 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 Teknoloji A.Ş., 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/PP 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 TMYPACS v1.3.18 whose evaluation was completed on February 27th 2023 and whose evaluation technical report was drawn up by BEAM Teknoloji A.Ş. (as CCTL), and with the Security Target document with version no 2.7 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

Developer of the IT product: Tele Medikal Yazılım ve Bilişim Teknoloji Ürünleri San. ve Tic. Ltd. Şti.

Evaluated IT product: TMYPACS

IT Product Version: 1.3.18

Name of IT Security Evaluation Facility: Beam Teknoloji A.Ş.

Completion date of evaluation: 27/02/2023

Assurance Package: EAL 2

1.1. Brief Description

Picture Archiving and Communication Systems (PACS), is a generic name given to the management systems used to store, access, distribute and present images. PACS allows the archiving, management and recall of images provided by imaging devices such as Direct X-ray (CR and DR), Ultrasonography (USG), Magnetic Resonance (MR), Computerized Tomography (CT or CT), Mammography. A radiological information system (RIS) is the core system for the electronic management of imaging departments. The major functions of the RIS can include patient scheduling, resource management, examination performance tracking, examination interpretation, results distribution, and procedure billing. RIS is used to create, store and manage radiological data and images of patients. It is a type of health or hospital information system (HIS), designed to automate and manage the processes in the radiological department.

Typically, the key components of a radiology information system consist of a database and a front-end RIS application. Radiological devices capture radiological tests & data and store it on the database. The front-end RIS application helps in accessing and editing that data. An RIS generally provides:

- Patient registration and management
- Radiology workflow management
- Document and image creation, modification and management
- Billing and reporting

TOE is a security module used for web based PACS / RIS. The TOE architecture is designed for health information systems and is responsible for the security of operations performed through them (HIS). The TOE is also tasked with data protection.

The health information management system refers to an application which hosts and processes all kind of patient data and which can be accessed online. TOE is also tasked with data protection.

Actions created by PACS / RIS are performed securely using the TOE. Thus, unauthorized access to patient and user data is prevented. The TOE provides a way to provide secure connection to the end-to-end. Examples of connection parties are databases and users. Through the TOE, user management, TOE management, event recording monitoring actions can be performed.

The security functionality in the TOE includes:

- user identification and authentication with password management;
- TOE access control;
- management of user access privilages;
- auditing;
- secure communication

1.2. Major Basic Security and Functional Attributes

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 TLS V1.2 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

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.

1.4. Organizational Security Policies (OSPs)

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.

1.5. Assumptions

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 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-87
TOE Name and Version	TMYPACS v1.3.18
Security Target Title	TMYPACS v1.3.18 Security Target
Security Target Version	2.7
Security Target Date	30/03/2023
Assurance Level	EAL 2
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	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	Tele Medikal Yazılım ve Bilişim Teknoloji Ürünleri San. ve Tic. Ltd. Şti.
Evaluation Facility	BEAM Teknoloji A.Ş.
Certification Scheme	TSE CCCS

2.2 Security Policy

TOE Security Policy consists of security functions described in section 2.4 within logical scope.

2.3 Assumptions and Clarification of Scope

- Usage assumptions

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.

- Environmental assumptions

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.

- Clarification of scope

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.

2.4 Architectural Information

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.

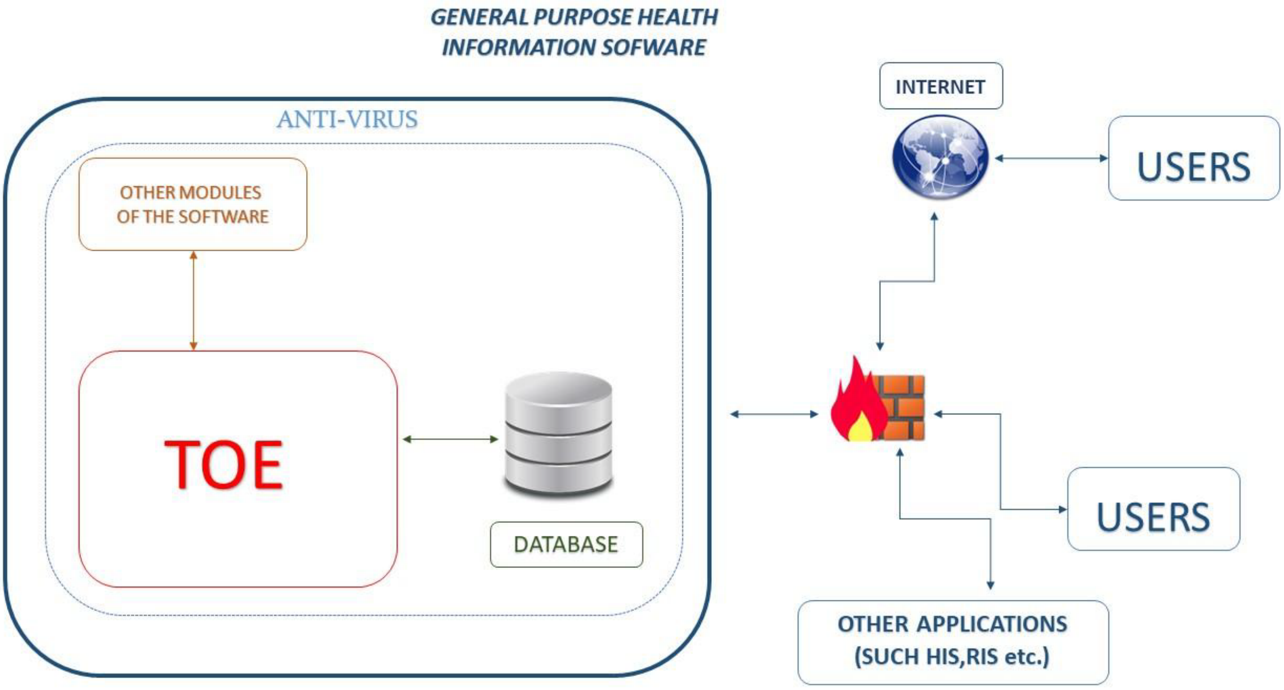
GENERAL PURPOSE HEALTH INFORMATION SOFWARE
ANTI-VIRUS
OTHER MODULES OF THE SOFTWARE
TOE
DATABASE
INTERNET
USERS
USERS
OTHER APPLICATIONS (SUCH HIS,RIS etc.)

Figure 1 *Typical Healtcare Information System*

2.5 Documentation

Document Name	Version	Release Date
TMYPACS v1.3.18 Security Target	v2.7	30/03/2023
User Manual	v1.9	09/12/2022
Installation Procedures	v1.3	13/10/2022

2.6 IT Product Testing

- **Developer Testing:** All TSFIs and module behaviors have been tested by developer. Developer has conducted 14 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted 14 developer tests. Additionally, evaluator has prepared 12 independent tests. TOE has passed all 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, 20 penetration tests have been conducted. TOE proved that it is resistant to “Attacker with Basic Attack Potential”.

2.7 Evaluated Configuration

The structure of operational environment of the TOE. External communication is provided by TLS V1.2.

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.

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

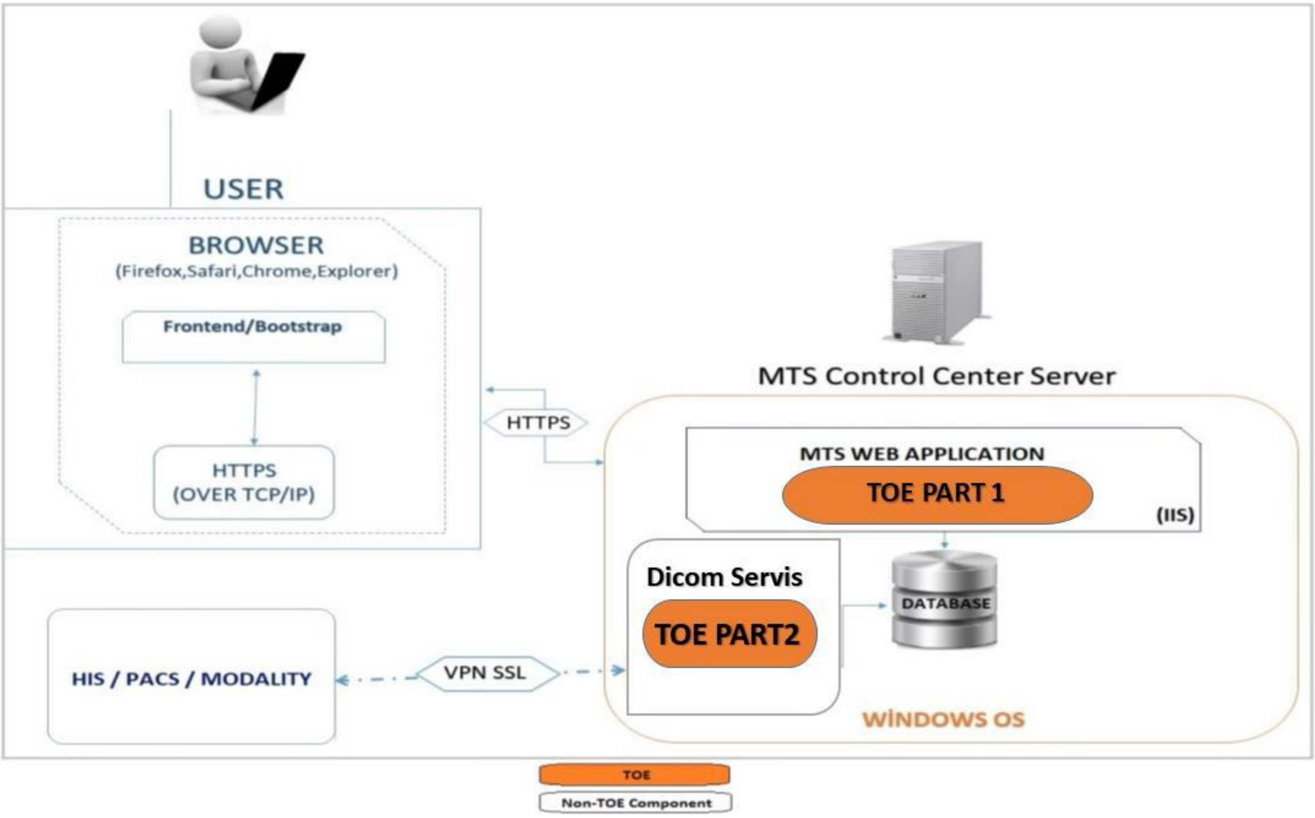

Figure 2 *TMYPACS v1.3.18 Application Software*

WEB SERVER	
CPU	Intel Core i5 6500 Soket
Memory	12 GB
Operating System	Windows Server 2008 R2
Disk	500 GB
Application Server	IIS 7
Connectivity	TCP/ IP
CLIENT	
CPU	Intel Core i3
Memory	4 GB
Operating System	Windows 7,8,10, Mac, Linux
Browser	Explorer, Mozilla, Safari, Chrome
Connectivity	TCP/ IP
DATABASE	
Database	MS Sql Express 2008 R2

***Table 1** Minimum Requirements of Non-TOE hardware/ software/ firmware*

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
	ADV_FSP.2	Complete functional specification	PASS
	ADV_TDS.1	Basic modular design	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC: Lifecycle Support	ALC_CMC.2	Production support, acceptance procedures and automation	PASS
	ALC_CMS.2	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS

Class Heading	Class Family	Description	Result
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	Analysis of coverage	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability Analysis	AVA_VAN.2	Focused 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 “TMYPACS v1.3.18” 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: TMYPACS v1.3.18 Security Target

Version: v2.7

Date of Document: March 30, 2023

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

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

CCRA: Common Criteria Recognition Arrangement

EAL: Evaluation Assurance Level

ITCD: Information Technologies Test and Certification Department

OSP: Organizational Security Policy

PACS: Picture Archiving and Communication Systems

ST: Security Target

TOE: Target of Evaluation

TLS v1.2: Transport Layer Security v1.2

TSF: TOE Security Functionality

5 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] ETR v2.2 of TMYPACS v1.3.18, Rel. Date: February 27, 2023

[4] TMYPACS v1.3.18 Security Target, Version 2.7, Rel. Date: March 30, 2023.

6 ANNEXES

6.1 TOE SPECIFICATIONS

TOE: TMYPACS v1.3.18

TOE Hash (SHA256): 9eccdbd4fd4c99f4838d258d4ed55a108a2372f6e3e548ea03be643490188779

6.2 TEST ENVIRONMENT:

Hardware:

- Windows Server 2008 installed server with 12GB RAM, 500 GB storage, Intel Core i5 6500 socket processor (server side)
- Windows 7, 8, 10 or MAC OS or Linux (as an operating system) installed PC with 4 GB RAM and Intel Core i3i processor. Microsoft Internet Explorer, Mozilla Firefox, Safari or Google Chrome internet browsers may be used for connection to the product. (client side)

Software:

- TOE (supported by developer)
- IIS 7 application server
- MS SQL 2008 R2