	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 4+ (ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5 and
ALC_FLR.2)**

Evaluation of

Güvenpark Bilişim Teknolojileri Ar-GE Tic. Ltd. Şti.

ProCrypt KM-3000 Hardware Security Module v1.0

issued by


**Turkish Standards Institution
Common Criteria Certification Scheme**

Certificate Number: 21.0.03/TSE-CCCS-61

	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
DOCUMENT CHANGE LOG.....	3
DISCLAIMER.....	4
FOREWORD.....	5
RECOGNITION OF THE CERTIFICATE.....	6
1 - EXECUTIVE SUMMARY.....	7
1.1 TOE Overview.....	7
1.2 Threats	7
2 CERTIFICATION RESULTS.....	8
2.1 Identification of Target of Evaluation	8
2.2 Security Policy.....	8
2.3 Assumptions and Clarification of Scope	8
2.4 Architectural Information	9
2.4.1 Logical Scope	9
2.4.2 Physical Scope.....	10
2.5 Documentation.....	11
2.6 IT Product Testing	12
2.7 Evaluated Configuration.....	12
2.8 Results of the Evaluation	12
2.9 Evaluator Comments / Recommendations.....	13
3 SECURITY TARGET	14
4 BIBLIOGRAPHY	15

	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

<i>Date of Issue</i>	July 10th, 2019
<i>Approval Date</i>	July 10th, 2019
<i>Certification Report Number</i>	21.0.03/18-007
<i>Sponsor and Developer</i>	Güvenpark Bilişim Teknolojileri Ar-GE Tic. Ltd. Şti.
<i>Evaluation Facility</i>	Beam Technology Test Center
<i>TOE</i>	ProCrypt KM-3000 Hardware Security Module v1.0
<i>Pages</i>	15

<i>Prepared by</i>	Cem ERDİVAN Common Criteria Inspection Expert 
<i>Reviewed by</i>	Zümrüt MÜFTÜOĞLU Common Criteria Technical Responsible (Hardware 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

<i>Release</i>	<i>Date</i>	<i>Pages Affected</i>	<i>Remarks/Change Reference</i>
1.0	July 10th, 2019	All	First Release

	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

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.

	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 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 ProCrypt KM-3000 Hardware Security Module v1.0 whose evaluation was completed on July 7th, 2019 and whose evaluation technical report was drawn up by Beam Technology (as CCTL), and with the Security Target document with version no 1.0 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).

C.Ş

7M

	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	05

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>.

C-8

70

	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 05

1 - EXECUTIVE SUMMARY

1.1 TOE Overview

The TOE is a general purpose hardware security module (HSM) which provides cryptographic processing (encryption/decryption, signature generation/verification, message digest generation/verification, MAC generation/verification), key generation and key management services to connected host systems, which might be SSL/TLS web servers, application servers, authentication servers and other IT systems that need secure storage of cryptographic keys and secure use of cryptographic operations.

The TOE communicates with host systems through its network interface (100/1000 Base-T) and PKCS#11 protocol. This enables integration to either existing system environments or future projects, for wide range of applications. In addition to the ethernet interface, a smartcard interface (ISO7876) is also available for importing/exporting cryptographic keys and for user authentication using smartcards.

The TOE is physically defined as a set of hardware and firmware, which is contained within the cryptographic boundary. The TOE is in system on module (SOM) form with a card edge connection and it is typically located within a custom carrier/host system(non-TOE).

The TOE has a tamper resistant casing and constantly monitors against physical tamper attempts that including drilling, breaking or removing its casing. The whole module, except the card edge connection area, is covered by the mentioned tamper resistant casing and hard, opaque potting material (epoxy resin) is also used to fill the gap between the module electronics and the casing. Additionally, the TOE also monitors temperature and input voltage, to harden its tamper resistance capability. Optionally, the TOE can be configured to output a separate tamper trigger signal, which can be used to protect case of its carrier/host system, making it difficult to open its enclosure without detection. The TOE zeroizes plaintext key material and security parameters in case of a tamper event.

The TOE records audit logs for all operational events and security relevant events.

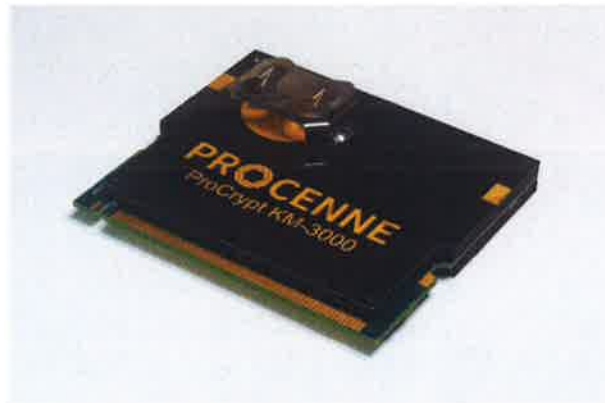


Figure 1 - TOE

1.2 Threats

Threats are provided in Section 3.2 of Security Target Document v1.0.

C.E. 7M

	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 Identification of Target of Evaluation


<i>Certificate Number</i>	21.0.03/TSE-CCCS-61
<i>TOE Name and Version</i>	ProCrypt KM-3000 Hardware Security Module v1.0
<i>Security Target Title</i>	ProCrypt KM-3000 Hardware Security Module v1.0 Security Target
<i>Security Target Version</i>	v1.0
<i>Security Target Date</i>	July 10th, 2019
<i>Assurance Level</i>	EAL4+ (ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2)
<i>Criteria</i>	<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 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
<i>Methodology</i>	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
<i>Protection Profile Conformance</i>	None
<i>Common Criteria Conformance</i>	<ul style="list-style-type: none"> • 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
<i>Sponsor and Developer</i>	Güvenpark Bilişim Teknolojileri Ar-GE Tic. Ltd. Şti.
<i>Evaluation Facility</i>	Beam Technology Test Center
<i>Certification Scheme</i>	TSE CCCS

2.2 Security Policy

TOE Security Policy consists of security functions described in section 2.4.1 Logical Scope.

2.3 Assumptions and Clarification of Scope

Please refer to Security Target Document v1.0 Section 3.3 for OSPs and Section 3.4 for Assumptions.

	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	05

2.4 Architectural Information

2.4.1 Logical Scope

Security Function	Description
User Authentication	The TOE provides pre-defined user roles and each user role has access to certain TOE functionality.
Secure Key Management	The TOE provides functionality to securely generate, store, exchange, use and destroy cryptographic keys for supported cryptographic functions.
Cryptographic Services	The TOE provides access to several cryptographic algorithms such as asymmetric and symmetric encryption algorithms, hash algorithms, key generation algorithms and signature generation and verification algorithms. A full list of the supported cryptographic algorithms is provided in the Security Target Document.
Auditing	The TOE has a logging mechanism to record significant events along with date/time information and status code.
Self-Test	The TOE performs various self-tests on system start up and provides the ability to re-run the same tests on user request. The self-tests are performed to verify functionality of the TOE's hardware components, cryptographic IP cores and soft cores and integrity of the firmware packages and other software.
Tamper Detection	The TOE has tamper detection mechanisms and it is designed to destroy content of its secure memory in case of tamper detection. The tamper detection mechanisms are battery backed and continues to operate when the system power is lost.

C-8

7M



2.4.2 Physical Scope

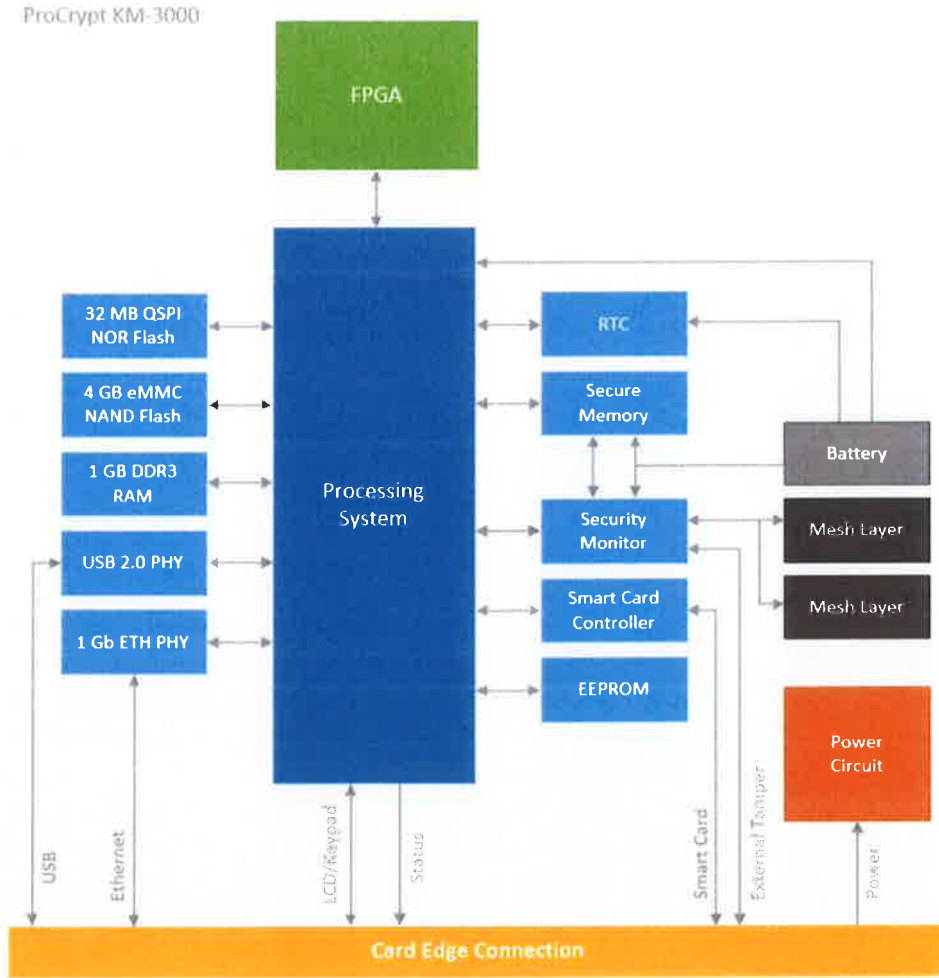


Figure 2 – TOE Hardware Architecture

Component	Description
Processing System	Processing system is a microcontroller which consists of dual core CPUs (Central Processing Unit) and auxiliary units like memory interface units, storage elements and I/O peripherals. It runs main firmware of the TOE and is responsible of management of all other hardware components. In addition, the processing system has a key memory to store firmware encryption key which is backed by the battery.
FPGA	FPGA hosts cryptographic IP cores which are used to accelerate cryptographic operations.
QSPI NOR Flash	NOR Flash is used to store bootloader files in addition to some system configuration files which are needed on system startup.
eMMC NAND Flash	It is used to store filesystem of the operating system(OS). All cryptographic keys, key components and CSPs are encrypted using master key and also stored in the NAND memory.
USB 2.0 PHY	It is a physical layer interface component which generates USB 2.0 compliant electrical interface, in order to enable the processing system to communicate with

	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

	USB devices.
1 Gb ETH PHY	It is a physical layer interface component which enables the processing system to communicate over computer networks.
RTC	Real time clock component is used to provide date/time information to the system. It is battery backed to retain data/time information when system power is lost.
Secure Memory	Secure memory is used to store master key of the device. It is battery backed to retain its content when system power is lost. It is able to rapidly destroy stored key data when tamper alarm signal is received by the security monitor.
Security Monitor	It constantly monitors the mesh layers and makes sure that they are physically intact. It also monitors module temperature and voltage supply inputs to detect abnormal events. In case of tamper event detection, it broadcasts an alarm signal. It is battery backed and continues its operation when system power is lost.
Smart Card Controller	It is an interface component that enables the processing system to communicate with smart cards.
EEPROM	It stores constant and unique module identification data which are set during manufacturing.
Battery	It is used to provide power to volatile memory components and security monitor, when system power is not present.
Mesh Layer	It provides protection against possible electrical and mechanical attacks. It covers the whole module electronics and enables the module to detect physical damage.
Power Circuit	It consists of several power regulators, power supervisor circuits and auxiliary components that regulate and monitor the power rails.


Software and IP components of the TOE are listed below:

- Processing System Bootloader
- Operating System
- Device Drivers
- Firmware Packages
- FPGA IP Cores
- Secure SoC Bootloader
- Secure SoC Firmware

2.5 Documentation

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

Document Name	Version	Release Date
ProCrypt KM-3000 Hardware Security Module v1.0 Security Target	v1.0	July 10, 2019
Key Management Manual	v1.0	April 5, 2019
KM-3000 Manager Installation Manual	v1.0	May 8, 2019
Command Reference Manual	v1.0	December 22, 2018
Management Manual	v1.0	May 3, 2019

	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

2.6 IT Product Testing

- **Developer Testing:** All TSFIs and subsystem/module behaviors have been tested by developer. Developer has conducted 21 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted all 21 developer tests. Additionally, evaluator has prepared 11 independent tests. TOE has passed all 32 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, 9 penetration tests have been conducted. TOE proved that it is resistant to attackers with “High Attack Potential”.

2.7 Evaluated Configuration

TOE configuration:

ProCrypt KM-3000 Hardware Security Module v1.0


Hardware and software requirements for “ProCryptManager Setup (non-TOE management software)” are listed below:

- Operating System:
 - Microsoft Windows 7 or higher (x86 and x64)
 - Microsoft Windows Server 2012 or higher (x64)
 - Linux (x64)
- Processor: 1.5 GHz, 2 cores or higher
- Memory: 2 GB RAM for x86 systems, 4 GB RAM for x64 systems
- HDD: 500 MB of free disk space
- Network interface

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL4+ (ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2) 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.4	Complete functional specification	PASS
	ADV_IMP.2	Complete mapping of the implementation representation of the TSF	PASS
	ADV_TDS.3	Basic modular design	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC:	ALC_CMC.5	Advanced support	PASS

	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	05

Class Heading	Class Family	Description	Result
Lifecycle Support	ALC_CMS.4	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
	ALC_DVS.2	Sufficiency of security measures	PASS
	ALC_LCD.1	Developer defined life-cycle model	PASS
	ALC_TAT.1	Well-defined development tools	PASS
	ALC_FLR.2	Flaw reporting 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.2	Analysis of coverage	PASS
	ATE_DPT.1	Testing: basic design	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability Analysis	AVA_VAN.5	Advanced methodical vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

Some recommendations have been communicated to CCCS by the evaluators, related to the evaluation process of "ProCrypt KM-3000 Hardware Security Module v1.0" product in the ETR. Certification Body has reviewed those recommendations and decided that they are not crucial for the results of the evaluation. Nevertheless, should a customer wishes to see those recommendations anyway, can apply the Certification Body (TSE) with a formal request.

	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 SECURITY TARGET


The security target associated with this Certification Report is identified by the following terminology:

Title: ProCrypt KM-3000 Hardware Security Module v1.0 Security Target

Version: v1.0

Date of Document: July 10, 2019

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.

	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 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 v1.2 of ProCrypt KM-3000 Hardware Security Module v1.0, Rel. Date: July 7, 2019
- [5] ProCrypt KM-3000 Hardware Security Module v1.0 Security Target, Version 1.0, Rel. Date: July 10, 2019

c.s



Sayfa 15/15