# Certification Report

## EAL 4+ (ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2) Evaluation of

**Güvenpark Bilişim Tek. Ar. Ge. Tic. Ltd. Şti.**

## ProCrypt KM-X Hardware Security Module v1.0

**issued by**

**Turkish Standards Institution**

**Common Criteria Certification Scheme**

*Certificate Number: 21.0.03/TSE-CCCS-75*

# TABLE OF CONTENTS

# Document Information

| | |
|---|---|
| **Date of Issue** | *29.07.2021* |
| **Approval Date** | *30.07.2021* |
| **Certification Report Number** | *21.0.03/21-007* |
| **Sponsor and Developer** | *Güvenpark Bilişim Tek. Ar. Ge. Tic. Ltd. Şti.* |
| **Evaluation Facility** | *Beam Teknoloji A.Ş.* |
| **TOE** | *ProCrypt KM-X Hardware Security Module v1.0* |
| **Pages** | *16* |

| | | |
|---|---|---|
| **Prepared by** | *İbrahim Halil KIRMIZI* | |
| **Reviewed by** | *Halime Eda BİTLİSLİ ERDİVAN* | |

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* | *29.07.2021* | *All* | *First Release* |

# DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformant 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.

# 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 (CCCS) provides an evaluation and certification service to ensure the reliability of Information Security products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCTL 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 CCTL 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 public/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-X Hardware Security Module v1.0* whose evaluation was completed on *30.06.2021* and with the Security Target document with version no *0.23* 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

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:** *ProCrypt KM-X Hardware Security Module*

**IT Product version**: *v1.0*

**Developer's Name**: *Güvenpark Bilişim Tek. Ar. Ge. Tic. Ltd. Şti.*

**Name of CCTL**: *Beam Teknoloji A.Ş.*

**Assurance Package**: *EAL 4+ (ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2)*

**Completion date of evaluation**: *30.06.2021*

## 1.1. Brief Description

The TOE is a general-purpose hardware security module (HSM) which provides cryptographic processing. The It's physically defined as a set of hardware and firmware.

## 1.2. Major Security Features

The TOE provides the following security services;

- User Authentication,
- Access Control,
- Secure Key Management,
- Cryptographic Services,
- Audit,
- Self-Test,
- Tamper Detection,
- Secure Communication

### 1.3. Threats

The threats are;

- **T.Compro_CSP** – Compromise of Confidential CSP
- **T.Modif_CSP** – Modification of Integrity Sensitive CSP
- **T.Abuse_Func** – Abuse of Function
- **T.Inf_Leakage** – Information Leakage
- **T.Malfunction** – Malfunction of TSF
- **T.Physical_Tamper** – Physical Tampering
- **T.Masquerade** – Masquerade Authorized Data Source of Receiver

## 2. CERTIFICATION RESULTS

### 2.1. Identification of Target of Evaluation

| | |
|---|---|
| **Certificate Number** | *21.0.03/TSE-CCCS-75* |
| **TOE Name and Version** | *ProCrypt KM-X Hardware Security Module v1.0* |
| **Security Target Title** | *KMX-TD050-A-023 ProCrypt KM-X Hardware Security Module Security Target* |
| **Security Target Version** | *0.23* |
| **Security Target Date** | *23.06.2021* |
| **Assurance Level** | *EAL 4+ (ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2)* |

| | |
|---|---|
| **Criteria** | • *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017*<br>• *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017*<br>• *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017* |
| **Methodology** | *Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017* |
| **Protection Profile Conformance** | *None* |
| **Sponsor and Developer** | *Güvenpark Bilişim Tek. Ar. Ge. Tic. Ltd. Şti.* |
| **Evaluation Facility** | *Beam Teknoloji A.Ş.* |
| **Certification Scheme** | *TSE CCCS* |

## *2.2. Security Policy*

Organizational Security Policies are;

- **OSP.User_Data_Prot** - Protection of User Data by Cryptographic Functions
- **OSP.Endorsed_Crypto** - Endorsed Cryptographic Functions
- **OSP.Key_Man** - Cryptographic Key Management
- **OSP.Key_Personal** – Personal Security for Cryptographic Keys

## 2.3. Assumptions and Clarification of Scope

Assumptions for the operational environment of the TOE are;

- **A.User_Data** - Protection of User Data by the IT System
- **A.Data_Sep** - Separation of Cryptographically Protected and Unprotected Data
- **A.Key_Generation** - Key Generation and Import to the Cryptographic Module
- **A.Audit_Analysis** - Analysis of Audit Trails
- **A.Availability** - Availability of Keys
- **A.Environmental_Security** – Environmental Security of systems accessing TOE interfaces

## 2.4. Architectural Information

The TOE is physically defined as a set of hardware and firmware. The TOE is in system on module (SOM) form with PCIe card edge connection and it is typically located within a custom carrier or host system(non-TOE). The TOE communicates with host systems through its PCIe card edge connection.

The TOE uses a Linux based operating system running on the processing system. The operating system just provides an environment for the firmware packages to run and it does not play a direct role at meeting security functional requirements.

The device drivers are mainly developed for interfacing the IP cores, which are hosted on the FPGA portion of the TOE. Their primary objective is to provide an abstraction layer between the devices and the firmware packages.

## 2.5. Documentation

Documents below are provided to the customer by the developer alongside the TOE;

| Name of Document | Version Number | Date |
|---|---|---|
| *KMX-TD050-A-023 ProCrypt KM-X Hardware Security Module Security Target* | *V0.23* | *23.06.2021* |
| *KMX-KL059-A-05 ProCrypt KM-X Hardware Security Module Manager Installation Guide* | *V0.5* | *11.06.2021* |

| | | |
|---|---|---|
| *KMX-KL060-A-07 ProCrypt KM-X Hardware Security Module Management Guide* | *V0.7* | *11.06.2021* |
| *KMX-KL061-A-02 ProCrypt KM-X Hardware Security Module Command Reference Guide* | *V0.2* | *25.09.2020* |
| *KMX-KL062-A-03 ProCrypt KM-X Hardware Security Module Key Management Guide* | *V0.3* | *03.12.2020* |

## 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 (ETR) of *ProCrypt KM-X Hardware Security Module v1.0.*

It is concluded that the TOE supports EAL 4+ (*ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2*). There are 25 assurance families which are all evaluated with the methods detailed in the ETR.

IT Product Testing is mainly described in two parts:

### 2.6.1. Developer Testing

Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE Design documentation which includes TSF subsystems and its interactions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 25 functional tests in total.

### 2.6.2. Evaluator Testing

- Independent Testing: Evaluator has chosen all 25 developer tests to conduct by itself. Additionally, evaluator has prepared 23 independent tests. TOE has passed all 48 functional tests to demonstrate that its security functions work as it is defined in the ST.

- Penetration Testing: TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 8 penetration tests have been conducted.

## 2.7. Evaluated Configuration

The evaluated TOE configuration is composed of;

- the TOE itself,
- ProCrypt Manufacturer Application,
- ProCrypt Admin Application,
- ProCrypt Key Manager Application,
- ProCryptoki,
- Pkcs11-testing tool,
- BP Application,
- Guidance documents

## 2.8. Results of the Evaluation

The table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2 components.

| Assurance Class | Component | Component Title |
|---|---|---|
| Development | ADV_ARC.1 | Security Architecture Description |
| | ADV_FSP.4 | Complete functional specification |
| | ADV_IMP.2 | Complete mapping of the implementation representation of the TSF |
| | ADV_TDS.3 | Basic Modular Design |
| Guidance Documents | AGD_OPE.1 | Operational User Guidance |
| | AGD_PRE.1 | Preparative Procedures |
| Life-Cycle Support | ALC_CMC.5 | Advanced Support |
| | ALC_CMS.4 | Problem tracking CM coverage |
| | ALC_DEL.1 | Delivery Procedures |
| | ALC_DVS.2 | Sufficiency of security measures |
| | ALC_LCD.1 | Developer defined life-cycle model |
| | ALC_TAT.1 | Well-defined development tools |
| | ALC_FLR.2 | Flaw reporting procedures |
| Security Target Evaluation | ASE_CCL.1 | Conformance Claims |
| | ASE_ECD.1 | Extended Components Definition |

| | | |
|---|---|---|
| | ASE_INT.1 | ST Introduction |
| | ASE_OBJ.2 | Security Objectives |
| | ASE_REQ.2 | Derived Security Requirements |
| | ASE_SPD.1 | Security Problem Definition |
| | ASE_TSS.1 | TOE Summary Specification |
| Tests | ATE_COV.2 | Analysis of Coverage |
| | ATE_DPT.1 | Testing: Basic Design |
| | ATE_FUN.1 | Functional Testing |
| | ATE_IND.2 | Independent Testing - Sample |
| Vulnerability Analysis | AVA_VAN.5 | Advanced Methodical Vulnerability Analysis |

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4+ (ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2) assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE "ProCrypt KM-X Hardware Security Module v1.0", the results of the assessment of all evaluation tasks are "Pass".

### *2.9. Comments / Recommendations*

It is recommended that all guidance outlined in the Guidance Documents be followed and all assumptions are fulfilled in order to the secure usage of the TOE.

## 3. SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:

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

Version: *0.23*

Date of Document: *23.06.2021*

A public version has been created and verified according to ST-Santizing:

Title: *ProCrypt KM-X Hardware Security Module v1.0 Security Target - Lite*

Version: 1.0

Date of Document: 26.07.2021

# 4. GLOSSARY

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

CSF : Critical Security Perimeter

DEL : Delivery

DVS : Development Security

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 5, April 2017,

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

[3] BTTM-CCE-055 DTR v.1.2 ProCrypt KM-X Hardware Security Module v1.0 EAL4+ (ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2) Evaluation Technical Report

# 6. ANNEXES

There is no additional information which is inappropriate for reference in other sections