	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

PERKON Personel Barkod Sistemleri Bil. Yaz. Elek. Tic. Ltd. Şti.

IPT-360 Pico FiscalApp V3.152.1256

issued by

**Turkish Standards Institution
Common Criteria Certification Scheme**

Certificate Number: 21.0.03/TSE-CCCS-41



	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

DOCUMENT INFORMATION	3
DOCUMENT CHANGE LOG	3
DISCLAIMER	4
FOREWORD	4
RECOGNITION OF THE CERTIFICATE	5
1. EXECUTIVE SUMMARY	6
1.1 BRIEF DESCRIPTION	6
1.2 MAJOR SECURITY FEATURES	7
1.3 THREATS	8
2. CERTIFICATION RESULTS	10
2.1 IDENTIFICATION OF TARGET OF EVALUATION	10
2.2 SECURITY POLICY	11
2.3 ASSUMPTIONS AND CLARIFICATION OF SCOPE	14
2.4 ARCHITECTURAL INFORMATION	15
2.5 DOCUMENTATION	16
2.6 IT PRODUCT TESTING	16
2.7 EVALUATED CONFIGURATION	17
2.8 RESULTS OF THE EVALUATION	17
2.9 EVALUATOR COMMENTS / RECOMMENDATIONS	18
3. SECURITY TARGET	19
4. GLOSSARY	20
5. BIBLIOGRAPHY	21
6. ANNEXES	21

	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>	21.06.2017
<i>Approval Date</i>	22.06.2017
<i>Certification Report Number</i>	21.0.03/17-004
<i>Sponsor and Developer</i>	PERKON Personel Barkod Sistemleri Bil. Yaz. Elek. Tic. Ltd. Şti.
<i>Evaluation Lab</i>	TÜBİTAK BİLGEM TDBY OKTEM
<i>TOE</i>	IPT-360 Pico FiscalApp V3.152-1256
<i>Pages</i>	21

<i>Prepared by</i>	İbrahim Halil KIRMIZI
<i>Reviewed by</i>	Zümrüt MÜFTÜOĞLU

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	21.06.2017	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/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 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.

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 ITCDC 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 TÜBİTAK BİLGEM TDBY OKTEM 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

Sayfa 4/21

	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

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 IPT-360 Pico FiscalApp V3.152-1356 whose evaluation was completed on 07.06.2017 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM TDBY OKTEM (as CCTL), and with the Security Target document with version no 1.6 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 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: Perkon IPT-360 Pico FiscalApp V3.152-1256

IT Product version: V3.152-1256

Developer's Name: PERKON Personel Barkod Sistemleri Bil. Yaz. Elek. Tic. Ltd. Şti.

Name of CCTL: TÜBİTAK BİLGEM TDBY OKTEM

Assurance Package: EAL 2

Completion date of evaluation: 07.06.2017

Serial Number of the TOE: SHA-256


(a1145c0b68447b61c6ce1abb875fc9b55f9e3636d51e578dafa7876c2c38bd8e)

1.1 Brief Description

The TOE is a Fiscal Application Software and Software Crypto Library which are the main items of a Fiscal Cash Register (FCR). TOE is used to process transaction amount of purchases to be viewed by both seller and buyer. This transaction amount is used to determine tax revenues. Therefore, secure processing, storing and transmitting of this data is very important.

The FCR is mandatory for first-and second-class traders. FCR is not mandatory for sellers who sell the goods back to its previous seller completely the same as the purchased good.

Figure 1 shows the general overview of the TOE and related components as regarded in this ST. The green part of Figure 1 is the TOE. The operational environment is also shown in the figure including Input/output interface, fiscal memory, daily memory, database, ERU, fiscal certificate memory. These components are non-TOE environments which are crucial parts of the FCR for functionality and security. Connections between the TOE and its environment are also subject of the evaluation since they are interfaces of the TOE.

	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

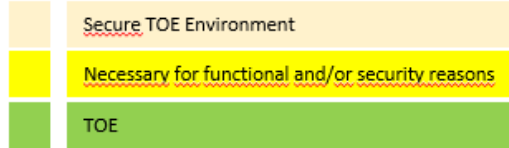
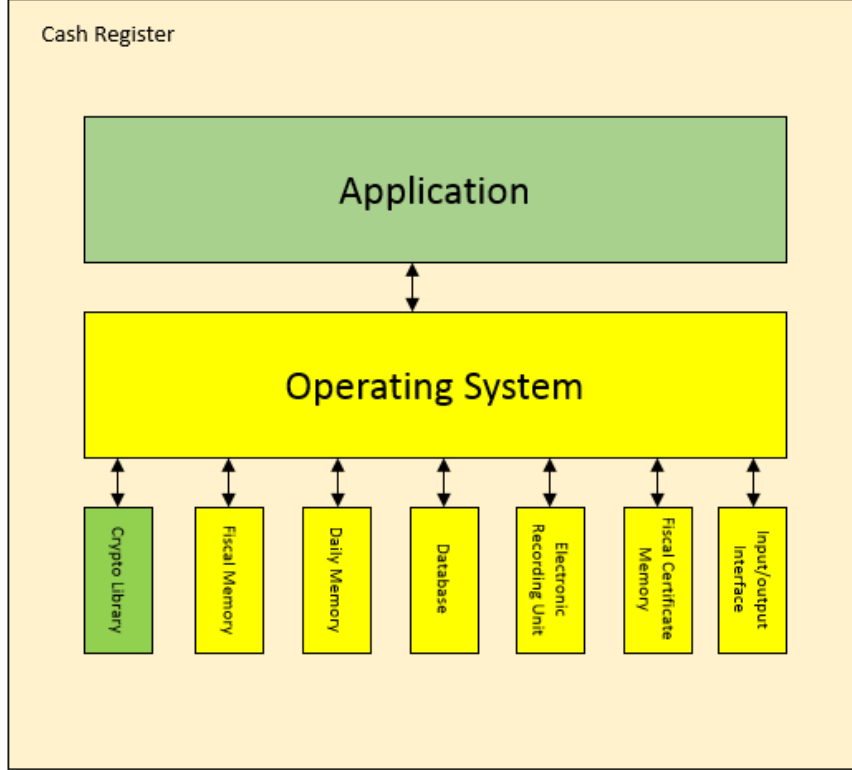



Figure 1 - TOE and Related Components

1.2 Major Security Features

TOE Security Functions are;

- TOE supports access control.
- TOE has the ability to detect disconnection between main processor and fiscal memory and should enter into the maintenance mode.
- TOE supports usage of ITU X509 v3 formatted certificate and its protected private key for authentication and secure communication with PRA- IS and TSM.
- TOE supports secure communication between FCR, PRA-IS and FCR TSM.
- TOE supports secure communication with EFT-POS /SMART PINPAD

	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

- TOE ensures the integrity of event data, sales data, authentication data, characterization data and FCR parameters.
- TOE records important events given in PRA Messaging Protocol document and send urgent event data to PRA-IS in a secure way.
- TOE detects physical attacks to FCR and enters into the maintenance mode.

1.3 Threats

The threats are;

- **T.AccessControl**

Adverse action: Authenticated users could try to use functions which are not allowed. (e.g. FCR Authorized Users gaining access to Authorized Manufacturer User functions)

Threat agent: An attacker who has basic attack potential has physical and logical access to FCR.

Asset: Event data, sales data, time information.

- **T.Authentication**

Adverse action: Unauthenticated users could try to use FCR functions except doing fiscal sales and taking reports which are not fiscal.


Threat agent: An attacker who has basic attack potential, has logical and physical access to the FCR.

Asset: Sales data, event data, time information

- **T.MDData – Manipulation and disclosure of data**

Adverse action: This threat deals with five types of data: event data, sales data, characterization data, authentication data and FCR parameters.

- An attacker could try to manipulate the event data to hide its actions and unauthorized access to the FCR, failure reports, and deletion of logs. An attacker also could try to disclose important events while transmitted between PRA-IS and FCR.
- An attacker could try to manipulate or delete the sales data generated by TOE which may result in tax fraud. In addition, an attacker also could try to disclose sales data while transmitted between PRA-IS and FCR. Manipulation and deletion of sales data located in FCR may be caused by magnetic and electronic reasons.

	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

- An attacker could try to manipulate the characterization data to cover information about tax fraud; to masquerade the user identity.
- An attacker could try to manipulate the FCR parameters to use FCR in undesired condition.
- An attacker also could try to disclose and modify authentication data in FCR to gain access to functions which are not allowed to his/her.

Threat agent: An attacker who has basic attack potential, has physical and logical access to the FCR.

Asset: Event data, sales data, characterization data, FCR parameters and authentication data.

- **T.Eavesdrop – Eavesdropping on event data, sales data and characterization data**

Adverse action: An attacker could try to eavesdrop event data, sales data and characterization data transmitted between the TOE and the PRA-IS and also between the TOE and the distributed memory units (Fiscal Memory, Database, Daily Memory and ERU).

Threat agent: An attacker who has basic attack potential, has physical access to the FCR and physical access to the FCR communication channel.

Asset: Characterization data, sales data, and event data.

- **T.Skimming – Skimming the event data, sales data and characterization data**

Adverse action: An attacker could try to imitate TSM to set parameters to FCR via the communication channel.

Threat agent: An attacker who has basic attack potential and logical access to the FCR.

Asset: FCR parameters

- **T.Counterfeit – FCR counterfeiting**


Adverse action: An attacker could try to imitate FCR by using sensitive data while communicating with PRA-IS and TSM to cover information about tax fraud.

Threat agent: An attacker who has basic attack potential and has physical and logical access to the FCR.

Asset: Sensitive data

- **T.Server counterfeiting**

Adverse action: An attacker could try to imitate PRA-IS by changing server certificates (P_{PRA} and P_{PRA-SIGN}) in FCR. In this way, the attacker could try to receive information from FCR.

	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

Threat agent: An attacker who has basic attack potential, has physical and logical access to the FCR.

Asset: Server Certificates

- **T.Malfunction – Cause malfunction in FCR**

Adverse action: An attacker may try to use FCR out of its normal operational conditions to cause malfunction without the knowledge of TOE.

Threat agent: An attacker who has basic attack potential, has physical access to the FCR.

Asset: Sales data, event data

- **T.ChangingTime**

Adverse action: An attacker may try to change time to invalidate the information about logged events and reports in FCR.


Threat agent: An attacker who has basic attack potential, has physical and logical access to the FCR.

Asset: Time Information.

2. CERTIFICATION RESULTS

2.1. Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-41
TOE Name and Version	IPT-360 Pico FiscalApp v3.152-1256
Security Target Title	Perkon IPT-360 Pico New Generation FCR Fiscalapp Security Target
Security Target Version	v1.6
Security Target Date	02.06.2017
Assurance Level	EAL 2
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

	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

Criteria	<ul style="list-style-type: none"> • 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	Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software TSE-CCCS/PP-007, version 2.0, 06 May 2015


2.2. Security Policy

Organizational Security Policies are;

- **P.Certificate**

It has to be assured that certificate which is installed at initialization step is compatible with ITU X.509 v3 format. FCR contains;

- FCR certificate,
- Certification Authority root and sub-root (subordinate) certificates that are used for verification of all certificates that are produced by Certification Authority,
- P_{PRA} certificate that is used for key transport process between FCR and PRA-IS,
- P_{PRA-SIGN} certificate that is used by TOE for signature verification
- UpdateControl certificate that is used to verify the signature of the TOE.

	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

- **P.Certificates Installation**

It has to be assured that environment of TOE provides secure installation of certificates (PPRA PPRA-SIGN, Certification Authority root and sub-root certificates, UpdateControl certificate, FCR certificates if handled as soft) into the FCR at initialization phase. Before the installation of certificates, it has to be assured that asymmetric key pair is generated in a manner which maintains security posture.

- **P. Comm_EXT - Communication between TOE and External Device**

It has to be assured that communication between TOE and External Devices is used to encrypt using AES algorithm with 256 bits according to External Device Communication Protocol Document [7]

- **P. InformationLeakage - Information leakage from FCR**

It has to be assured that TOE's environment provides a secure mechanism which prevents attacker to obtain sensitive information (private key) when FCR performs signature operation; i.e by side channel attacks like SPA (Simple power analysis), SEMA (Simple Electromagnetic Analysis), DPA (Differential power analysis), DEMA (Differential electromagnetic analysis).

- **P. SecureEnvironment**

It has to be assured that environment of TOE senses disconnection between fiscal memory and main processor. Then TOE enters into the maintenance mode and logs urgent event.


It has to be assured that fiscal memory doesn't accept transactions with negative amounts which results in a decrease of total tax value.

It has to be assured that environment of TOE provides a mechanism that sales data in daily memory which is not reflected to the fiscal memory cannot be deleted and modified in an uncontrolled way.

It has to be assured that sales data in ERU cannot be deleted and modified.

- **P. PhysicalTamper**

It has to be assured that TOE environment and TOE provide a tamper respondent system which is formed by electromechanical seals.

	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

It has to be assured that physical tampering protection system protects the keys (asymmetric key, symmetric key), the certificates, event data, characterization data, FCR parameters and sales data in FCR.

It has to be assured that TOE logs this type of events and enters into the maintenance mode when physical tampering protection system detect unauthorized access.

It has to be assured that authorized access such as maintenance work or service works are logged. It has to be assured that physical tampering protection system (mesh cover) protects fiscal memory.

- **P. SecureEnvironment**

It has to be assured that environment of TOE senses disconnection between fiscal memory and main processor. Then TOE enters into the maintenance mode and logs urgent event.

It has to be assured that fiscal memory doesn't accept transactions with negative amounts which results in a decrease of total tax value.

It has to be assured that environment of TOE provides a mechanism that sales data in daily memory which is not reflected to the fiscal memory cannot be deleted and modified in an uncontrolled way.


It has to be assured that sales data in ERU cannot be deleted and modified.

- **P. PKI - Public key infrastructure**

It has to be assured that IT environment for the TOE provides public key infrastructure for encryption, signing and key agreement.

- **P. UpdateControl**

TOE is allowed to be updated by TSM or Authorized Manufacturer User to avoid possible threats during this operation, FCR shall verify the signature of the new version of TOE to ensure that the TOE to be updated is signed by the correct organisation. Thus, the TOE to be updated is ensured to be the correct certified version because only the certified versions will be signed. In addition, FCR shall check version of TOE to ensure that it is in latest version.

	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

2.3. Assumptions and Clarification of Scope

Assumptions for the operational environment of the composite TOE are;

- **A.TrustedManufacturer**

It is assumed that manufacturing is done by trusted manufacturers. They process manufacturing step in a manner which maintains IT security.

- **A.Control**

It is assumed that PRA-IS personnel performs random controls on FCR. During control PRA-IS should check if tax amount, total amount printed on receipt and sent to PRA-IS is the same. In addition to this, a similar check should be processed for events as well.

- **A.Initialization**

It is assumed that environment of TOE provides secure initialization steps. Initialization step consists of secure boot of operating systems, and integrity check for TSF data. Moreover, if certificate is handled as soft (not in the smartcard) it is assumed that environment of TOE provides secure installation of it to the FCR in initialization phase. Before certificate installation it is assumed that asymmetric key pair generated in a manner which maintains security posture.

- **A.TrustedUser**


User is assumed to be trusted. It is assumed that for each sale a sales receipt is provided to the buyer.

- **A.Activation**

It is assumed that environment of TOE provides secure activation steps at the beginning of the TOE operation phase and after each maintenance process.

- **A.AuthorizedService**

It is assumed that repairing is done by trusted authorized services. The repairing step is processed in a manner which maintains legal limits.

	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.Ext_Key**

It is assumed that External Device (EFT-POS/SMART PINPAD) generates strong key for communicating with TOE and stores it in a secure way.

- **A.Ext_Device Pairing**

It is assumed that External Device and TOE are paired by Authorized Service.

2.4. Architectural Information

TOE is implemented in FCR in a plastic case protected by the tampering switches. The main architecture of the FCR is given in Figure 2. The fiscal application is running on an operating system whose functionality is accessed through drivers.

All components within the FCR are physically located in the area protected by the Electronic Seal. The Electronic Seal is being monitored by the TOE.

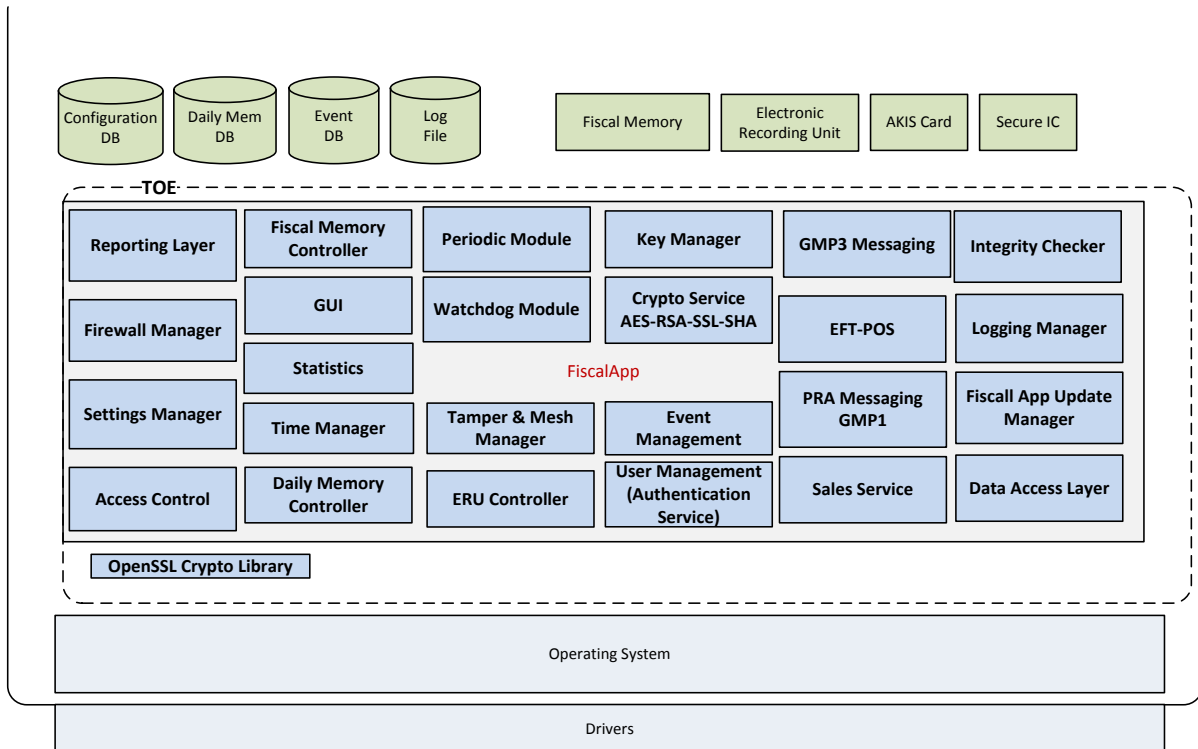



Figure 2 – Basic Architecture Model

	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

2.5. Documentation

During the evaluation; the configuration of evaluation evidences which are composed of Software source code, Common Criteria related documents, sustenance documents and guides are shown below;

Name of Document	Version Number	Date
Perkon IPT-360 Pico New Generation FCR Fiscalapp Security Target	v1.6	02.06.2017
Perkon IPT-360 Pico New Generation FCR Guidance and Procedures Document	v1.8	02.06.2017

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 IPT-360 Pico Fiscalapp v3.152-1256

It is concluded that the TOE supports EAL 2. There are 19 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. Developer has done total of 32 functional tests.

2.6.2. Evaluator Testing

- Independent Testing: Evaluator has done total of 26 test. 10 of them were selected from developer's tests. The other 16 of them were evaluator's independent tests.
- Penetration Testing: Evaluator has done 9 penetration tests to find out TOE's vulnerabilities that can be used for malicious purposes.

	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. Evaluated Configuration


During the evaluation; the configuration of evaluation evidences which are composed of Common Criteria documents, sustenance documents and guides are shown below;

Name of Document	Version Number	Publication Date
IPT-360 Pico Fiscalapp	3.152-1256	
Perkon IPT-360 Pico New Generation FCR Fiscalapp Security Target	1.6	02.06.2017
Perkon IPT-360 Pico New Generation FCR Functional Specification Document	1.5	02.06.2017
Perkon IPT-360 Pico New Generation FCR Design Specification Document	1.6	02.06.2017
Perkon IPT-360 Pico New Generation FCR Security Architecture Document	1.4	02.06.2017
Perkon IPT-360 Pico New Generation FCR Guidance and Procedures	1.8	02.06.2017
Perkon IPT-360 Pico New Generation FCR Lifecycle Definition Document	1.6	02.06.2017
Perkon IPT-360 Configuration Items List	1.1	02.06.2017
Perkon_FiscalApp_Repo_CI_List	1.1	15.03.2017
Perkon IPT-360 Pico New Generation FCR Test Records Document	1.2	22.02.2017

2.8. Results of the Evaluation

Table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 2 (EAL 2) components as specified in Part 3 of the Common Criteria.

Assurance Class	Component	Component Title
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic Design
	AGD_OPE.1	Operational User Guidance


	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

Guidance Documents	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery 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.1	Evidence of coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing
Vulnerability Analysis	AVA_VAN.2	Vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 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 “IPT-360 Pico”, the results of the assessment of all evaluation tasks are “Pass”.

2.9.Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “IPT-360 Pico” product, result of the evaluation, or the ETR.

	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: Perkon IPT-360 Pico New Generation FCR Fiscalapp Security Target

Version: 1.6


Date of Document: 02.06.2017

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

Title: Perkon IPT-360 Pico New Generation FCR Fiscalapp Security Target-Lite

Version: 1.0

Date of Document: 15.06.2017

	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. 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

BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

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

DEL : Delivery

EAL : Evaluation Assurance Level

FCR: Fiscal Cash Register

GR : Observation Report

OKTEM : Ortak Kriterler Test Merkezi

OPE : Operational User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

PRE : Preparative Procedures

SAR : Security Assurance Requirements


SFR : Security Functional Requirements

ST : Security Target

TDBY: Test ve Değerlendirme Başkan Yardımcılığı

TOE : Target of Evaluation

TSF : TOE Security Functionality

	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

TSFI : TSF Interface

5. 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: February 8th 2016
- [4] DTR 62 TR 01 PERKON OPT-360 Pico Fiscalapp V3.152-1256 Evaluation Technical Report
- [5] Technical Guidance (TK1), v4.0, October 20th 2016
- [5] PRA Messaging Protocol, v4.0, May 18th 2015
- [6] Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software (NGCRFAS PP) 2.0, TSE-CCCS/PP-007, 06.05.2015
- [7] External Device Communication Protocol (GMP3), v3.0, April 12th 2016

6. ANNEXES

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