



# Certification Report

**EAL 2**  
**Evaluation of**

**Revenue Administration Department of Turkey/Gelir İdaresi**  
**Başkanlığı**

**Common Criteria Protection Profile for New Generation Cash**  
**Register Fiscal Application Software-2**


issued by

**Turkish Standards Institution**  
**Common Criteria Certification Scheme**

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

## **TABLE OF CONTENTS**

TABLE OF CONTENTS.....	2
DOCUMENT INFORMATION .....	3
DOCUMENT CHANGE LOG.....	3
DISCLAIMER.....	3
FOREWORD .....	3
RECOGNITION OF THE CERTIFICATE.....	4
1 EXECUTIVE SUMMARY.....	5
2 CERTIFICATION RESULTS .....	6
2.1 PP IDENTIFICATION .....	6
2.2 SECURITY POLICY.....	7
2.3 ASSUMPTIONS AND CLARIFICATION OF SCOPE .....	13
2.4 ARCHITECTURAL INFORMATION .....	16
2.5 SECURITY FUNCTIONAL REQUIREMENTS .....	17
2.6 SECURITY ASSURANCE REQUIREMENTS.....	21
2.7 RESULTS OF THE EVALUATION .....	21
2.9 EVALUATOR COMMENTS / RECOMMENDATIONS.....	22
3 PP DOCUMENT .....	22
4 GLOSSARY .....	22
5 BIBLIOGRAPHY.....	24
6 ANNEXES.....	24

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

## Document Information

<b>Date of Issue</b>	11.06.2015
<b>Version of Report</b>	1
<b>Author</b>	İbrahim Halil KIRMIZI
<b>Technical Responsible</b>	Zümrüt MÜFTÜOĞLU
<b>Approved</b>	Mariye Umay AKKAYA
<b>Date Approved</b>	12.06.2015
<b>Certification Report Number</b>	21.0.01/15-050
<b>Sponsor and Developer</b>	Revenue Administration Department / Gelir İdaresi Başkanlığı
<b>Evaluation Lab</b>	TÜBİTAK BİLGEM OKTEM
<b>PP Name</b>	Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2 (NGCRFAS-2 PP)
<b>Pages</b>	24

## Document Change Log


<b>Release</b>	<b>Date</b>	<b>Pages Affected</b>	<b>Remarks/Change Reference</b>
v1	22.05.2015	All	First Released

## DISCLAIMER

*This certification report and the PP defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the PP in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the PP by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the PP by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.*

## 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*

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

with a Common Criteria evaluation which is made under the STCD 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) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned PP have been performed by TÜBİTAK BİLGEM OKTEM, which is a public CCTL.

A Common Criteria Certificate given to a PP means that such PP meets the security requirements defined in its PP document that has been approved by the CCCS. The PP document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the PP should also review the PP document in order to understand any assumptions made in the course of evaluations, the environment where the PP will run, security requirements of the PP and the level of assurance provided by the PP.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2 (PP version: 1.3) whose evaluation was completed on 05.06.2015 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the PP document with version no 1.0.


The certification report, certificate of PP evaluation and PP document are posted on the STCD Certified Products List at [bilisim.tse.org.tr](http://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>.

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

## 1 - EXECUTIVE SUMMARY

This report describes the certification results by the certification body on the evaluation results applied with requirements of APE assurance class of the Common Criteria for Information Security Evaluation in relation to Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2 (NGCRFAS-2 PP).

The evaluation was conducted on Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2 (NGCRFAS-2 PP) by TÜBİTAK-BİLGEM-OKTEM and completed on 05.06.2015. Contents of this report have been prepared on the basis of the contents of the ETR submitted by OKTEM. The evaluation was conducted by applying CEM. PP satisfies all APE requirements of the CC.

The TOE addressed by Protection Profile is an application software and crypto library which is the main item of a Fiscal Cash Register (FCR). TOE is used to process the transaction amount of purchases which can be viewed by both seller and buyer. Since transaction amount is used to determine tax revenues; secure processing, storing and transmission of this data is very important.

The TOE is a part of a FCR which is an electronic device for calculating and recording sales transactions and for printing receipts. TOE provides the following services;

- TOE stores sales data in fiscal memory.
- TOE stores total receipt and total VAT amount for each receipt in daily memory.
- TOE is able to generate reports (X report, Z report etc.).
- TOE is able to transmit Z reports, receipt information, sale statistics and other information determined by PRA to PRA-IS in PRA Messaging Protocol format.
- TOE stores records of important events as stated in PRA Messaging Protocol Document [5] and transmits to PRA-IS in PRA Messaging Protocol format in a secure way.
- TOE is able to be used by users in secure state or maintenance mode.

The TOE provides following security features;

- TOE supports access control.
- TOE is able to detect disconnection between main processor and fiscal memory and enter into the maintenance mode.


	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

- c. TOE supports usage of ITU X509 v3 formatted certificate and its protected private key for authentication and secure communication with PRA-IS and TSM.
- d. TOE supports secure communication with EFT-POS/Smart PinPad.
- e. TOE supports secure communication between FCR-PRA-IS and FCR-TSM.
- f. TOE ensures the integrity of event data, sales data, authentication data, characterization data and FCR parameters.
- g. TOE records important events defined in PRA Messaging Protocol Document [6] and sends urgent event data immediately to PRA-IS in a secure way.
- h. TOE detects physical attacks to FCR and enters into the maintenance mode in such cases.

## 2 CERTIFICATION RESULTS

### 2.1 PP Identification

<b>Certificate Number</b>	TSE-CCCS/PP-008
<b>PP Name and Version</b>	Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2 (NGCRFAS-2 PP) v1.3
<b>PP Document Title</b>	Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2 (NGCRFAS-2 PP)
<b>PP Document Version</b>	v1.3
<b>PP Document Date</b>	06.05.2015
<b>Assurance Level</b>	EAL 2
<b>Criteria</b>	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

<b>Methodology</b>	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology;CCMB-2012-09-004, v3.1 rev4, September 2012
<b>Protection Profile Conformance</b>	None
<b>Common Criteria Conformance</b>	CC Part 2 Conformant CC Part 3 Conformant Package Conformant to EAL 2
<b>Sponsor and Developer</b>	Gelir İdaresi Başkanlığı / Revenue Administration Department of Turkey
<b>Evaluation Facility</b>	TÜBİTAK- BİLGEM-OKTEM
<b>Certification Scheme</b>	Turkish Standards Institution Common Criteria Certification Scheme

## 2.2 Security Policy

The PP includes Organizational Security Policies, Threats and Assumptions. Some notions are explained in the PP document to make more understandable document. These notions are categorized External Entities, Roles, Modes of FCR and Assets. These notions are described in Table 1.

External Entities	<p><b>PRA-IS</b></p> <p>PRA-IS takes sales data and event data from FCR by sending query with parameters to FCR through TSM.</p> <p><b>Trusted Service Manager</b></p> <p>TSM is the system which is used to load parameters, update software and manage FCR.</p> <p><b>Attacker</b></p> <p>Attacker tries to manipulate the TOE in order to change its expected behavior and functionality. Attacker tries to breach confidentiality, integrity and availability of the FCR.</p> <p><b>PRA On-site Auditor</b></p> <p>PRA On-site Auditor is an employee of PRA who performs onsite audits to control the existence of expected FCR functionalities by using the rights of FCR Authorised User.</p> <p><b>Certificate storage</b></p>
-------------------	--

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

	<p>The certificate storage holds certificates and private key used for authentication and secure communication. Certificate storage is protected inside a physical and logical tampering system.</p> <p><b>Time Information</b></p> <p>FCR gets time information from trusted server. Time information is used during receipt, event, fiscal memory record, daily memory record and ERU record creation and is also used to send information to PRA-IS according to FCR Parameters.</p> <p><b>Audit storage</b></p> <p>Audit storage can be any appropriate memory unit in FCR. Audit storage stores important events according to their criticality level (urgent, high, warning and information). List of events can be found in PRA messaging protocol document [6].</p> <p><b>Storage unit</b></p> <p>Storage units of FCR are database, fiscal memory, daily memory and ERU.</p> <p><b>Input interface</b></p> <p>Input interfaces provide necessary input data from input devices to the TOE. Input devices for FCR may be keyboard, barcode reader, QR code (matrix barcode) reader, order tracking device and global positioning devices.</p> <p><b>External Device</b></p> <p>External Device is the device which is used to communicate with FCR by using secure channel according to External Device Communication Protocol Document [7]</p> <p><b>Output interface</b></p> <p>Output interfaces deliver outputs of the TOE to the output devices. Output devices for FCR may be printer, display etc.</p>
Modes of FCR	<p><b>Maintenance Mode:</b> Maintenance Mode is the mode that allows only Authorised Manufacturer User;</p>



	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

	<ul style="list-style-type: none"> <li>a. to change date and time information</li> <li>b. to change IP/Port information of TSM</li> <li>c. to review event data</li> <li>d. to start update operation of TOE</li> </ul> <p>FCR does not allow any fiscal transaction in maintenance mode. FCR enters this mode when the following occur;</p> <ul style="list-style-type: none"> <li>a. FCR Certificate check fails,</li> <li>b. Mesh cover monitoring check fails,</li> <li>c. A disconnection between fiscal memory and main processor occurs,</li> <li>d. Electronic seal is opened or forced by unauthorised persons,</li> <li>e. A technical problem is determined by FCR Manufacturer.</li> </ul> <p><b>Secure State Mode:</b> Secure State Mode is the mode that allows;</p> <ul style="list-style-type: none"> <li>a. FCR Authorised User; <ul style="list-style-type: none"> <li>i. to configure FCR,</li> <li>ii. to take fiscal reports</li> </ul> </li> </ul> <p>Secure State Mode is also allows;</p> <ul style="list-style-type: none"> <li>b. Unauthenticated Users; <ul style="list-style-type: none"> <li>i. to do fiscal sales,</li> <li>ii. to get FCR reports (except fiscal reports).</li> </ul> </li> </ul>
Assets	<p><b>Sensitive data</b></p> <p>Sensitive data is used for secure communication with PRA-IS and TSM. Confidentiality and integrity of this asset need to be protected.</p>

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

**Application Note 1:** Sensitive data may consist of symmetric keys (TREK, TRAK, TRMK, TDK and TRMKD).

- TREK is used for provide confidentiality of data transfer to PRA-IS.
- TRAK is used for integrity control of data transferred to the PRA-IS.
- TDK is used for provide confidentiality of data transfer to the TSM.
- TRMK is used for key transportation from PRA-IS to TOE.
- TRMKD is used for key transportation from TSM to TOE.

#### Event data

Event data is used to obtain information about important events saved in audit storage. The integrity of this asset is crucial while stored in FCR and both integrity and confidentiality of this asset are important while it is transferred from TOE to PRA-IS. Event data is categorized in PRA Messaging Protocol Document [6].


#### Sales data

Sales data is stored in storage unit. Sales data is required by PRA-IS to calculate tax amount and to provide detailed statistics about sales. The integrity of this asset has to be protected while stored in FCR; and both integrity and confidentiality have to be protected while it is transferred from TOE to PRA-IS.


#### Characterization data (Identification data for devices)

Characterization data is a unique number assigned to each FCR by the manufacturer. PRA-IS uses characterization data for system calls to acquire sales data or event data of an FCR. Integrity of this asset has to be protected.

#### Authentication data

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

	<p>Authentication data contains authentication information which is required for FCR Authorised User and Authorised Manufacturer User to gain access to FCR functionalities. Both integrity and confidentiality of this asset have to be protected.</p> <p><b>Time Information</b></p> <p>Time information is stored in FCR and synchronized with trusted server. Time information is important when logging important events and sending reports to the PRA-IS. The integrity of this asset has to be protected.</p> <p><b>Server Certificates</b></p> <p>Server certificates contain PRA-IS and TSM certificates (<math>P_{PRA}</math>, <math>P_{PRA-SIGN}</math>, <math>P_{TSM}</math> and <math>P_{TSM-SIGN}</math>)</p> <p><math>P_{PRA}</math> and <math>P_{PRA-SIGN}</math> certificates are used for signing and encryption process during key transport between TOE and PRA-IS.</p> <p><math>P_{TSM}</math> certificate is used for encryption process during key transport between TOE and TSM and <math>P_{TSM-SIGN}</math> is used for signature verification of FCR parameters by TOE.</p> <p><b>FCR Parameters</b></p> <p>FCR parameters stored in FCR are updated by TSM after Z report is printed.</p> <p>FCR parameters set;</p> <ol style="list-style-type: none"> <li>Sales and event data transferring time</li> <li>Criticality level of event data sent to the PRA-IS</li> <li>Maximum number of days that FCR will work without communicating with PRA-IS</li> </ol>
Roles	<p><b>FCR Authorised User</b></p> <p>FCR Authorised User is the user who uses the functions of FCR and operates FCR by accessing the device over an authentication mechanism.</p> <p><b>Authorised Manufacturer User</b></p>

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

	Authorised Manufacturer User works for FCR manufacturer and conducts maintenance works on FCR.
--	--

**Table 1**

The PP includes 8 OPSs;

#### **P.Certificate**

It has to be assured that certificates, which are installed at initialization step, are 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<sub>PRA</sub> and P<sub>TSM</sub> certificates that are used for key transport process between FCR-PRA-IS and FCR-TSM,
- P<sub>PRA-SIGN</sub> and P<sub>TSM-SIGN</sub> certificates which are used by TOE for signature verification,
- UpdateControl certificate that is used to verify the signature of the TOE.

#### **P.Certificates Installation**

It has to be assured that environment of TOE provides secure installation of certificates (P<sub>PRA</sub>, P<sub>PRA-SIGN</sub>, P<sub>TSM</sub>, P<sub>TSM-SIGN</sub>, 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 encrypted 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.

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

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.

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 unauthorised access.

It has to be assured that authorised access such as maintenance work or service works are logged.

It has to be also assured that physical tampering protection system (mesh cover) protects fiscal memory.

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

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

#### **P.UpdateControl**

TOE is allowed to be updated by only TSM or Authorised 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 the latest version.


### **2.3 Assumptions and Clarification of Scope**

This section describes assumptions that must be satisfied by the TOE's operational environment.

The PP includes following 8 assumptions;

#### **A. TrustedManufacturer**

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

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

### **A.Control**

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

### **A.Initialisation**

It is assumed that environment of TOE provides secure initialization steps. Initialization step is consist of secure boot of operating system, 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. AuthorisedService**

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

### **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 Authorised Service.

The PP includes following 8 threats averted by TOE and its environment;

### **T.AccessControl**

Adverse action: Authenticated users could try to use functions which are not allowed.

(e.g. FCR Authorised User gaining access to Authorised 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**

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

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 unauthorised 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 may be caused by magnetic and electronic reasons.
- 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 FC 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, ERU).

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

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

#### **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.

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	Doküman No	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

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

Asset: Sensitive data (TRMK, TRMKD, TREK, TRAK and TDK)

#### **T. Server counterfeiting**

Adverse action: An attacker could try to imitate PRA-IS and TSM by changing server certificates (P<sub>PRA</sub>, P<sub>PRA-SIGN</sub>, P<sub>TSM</sub> and P<sub>TSM-SIGN</sub>) in FCR. In this way, the attacker could try to receive information from FCR while communicating with PRA-IS and to imitate TSM to set parameters to FCR.

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.

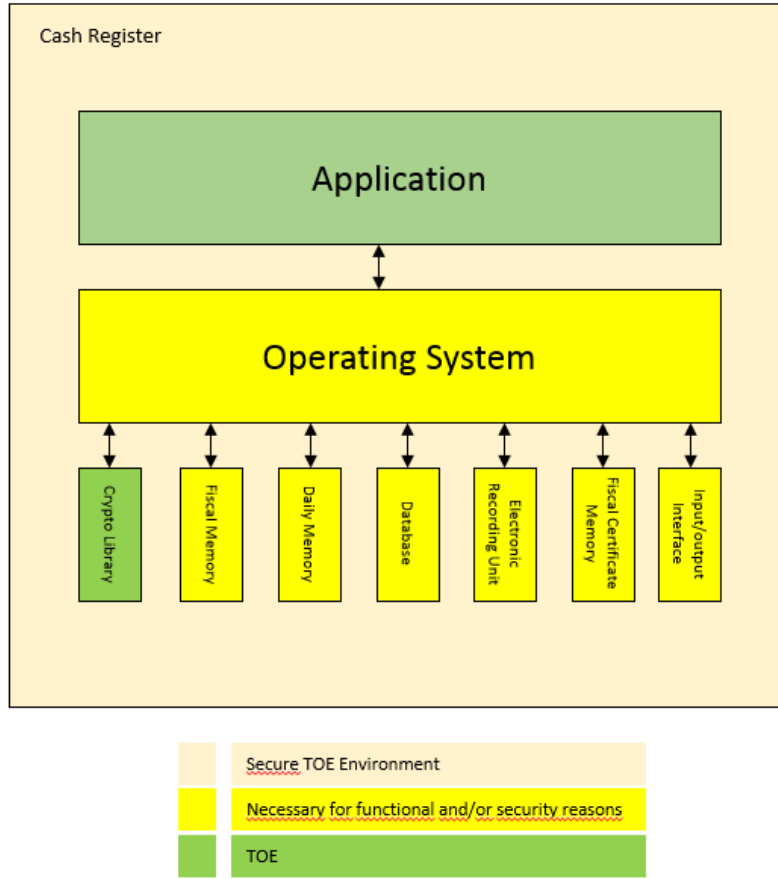
Asset: Time Information.

## **2.4 Architectural Information**

Figure 1 shows the general overview of the TOE and its related components as regarded in PP. The green part of Figure 1 is the TOE. Yellow parts; that are given as input/output interface, fiscal memory, daily memory, database, ERU, fiscal certificate memory; are TOE's environmental components which are crucial for functionality and security. Connections between the TOE and its environment are also subject to evaluation since these connections are made over the interfaces of the TOE.



	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00



**Figure 1** TOE and related components

## 2.5 Security Functional Requirements

Table 2 describes Security Functional Requirements;

Security Functional Class	Functional Family	Security Functional Component
Security Audit (FAU)	FAU_GEN Security audit data generation	FAU_GEN.1 Audit data generation
	FAU_SAR Security audit review	FAU_SAR.1 Audit review
	FAU_STG Security audit event storage	FAU_STG.1 Protected audit trail storage
		FAU_STG.4 Prevention of audit data loss
Communication (FCO)	FCO_NRO Non-repudiation of origin	FCO_NRO.2 Enforced proof of origin

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	Doküman No	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00


Cryptographic Support (FCS)	FCS_CKM Cryptographic key management	FCS_CKM.1/ TRMK Cryptographic key generation
		FCS_CKM.1/ TRMKD Cryptographic key generation
		FCS_CKM.2 Cryptographic key distribution
		FCS_CKM.1/ DHE-KEY Cryptographic key generation
		FCS_CKM.1/ EXT-DEV K <sub>HMAC</sub> Cryptographic key generation
		FCS_CKM.1/ EXT-DEV K <sub>ENC</sub> Cryptographic key generation
		FCS_CKM.4 Cryptographic key destruction
	FCS_COP Cryptographic operation	FCS_COP.1/TREK Cryptographic operation
		FCS_COP.1/TRAK Cryptographic operation
		FCS_COP.1/TDK Cryptographic operation
		FCS_COP.1/HASHING Cryptographic operation
		FCS_COP.1/TRMK-DEC Cryptographic operation
		FCS_COP.1/TRMKD-DEC Cryptographic operation
		FCS_COP.1/PUB-ENC Cryptographic operation
		FCS_COP.1/SIGN-VER Cryptographic operation

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

		FCS_COP.1/ EXT-DEV KEYEXCHANGE Cryptographic operation
		FCS_COP.1/EXT-DEV K <sub>ENC</sub> Cryptographic operation
		FCS_COP.1/ EXT-DEV K <sub>HMAC</sub> Cryptographic operation
User Data Protection (FDP)	FDP_ACC Access control policy	FDP_ACC.1 Subset access control
	FDP_ACF Access control functions	FDP_ACF.1 Security attribute based access control
	FDP_ETC Export from the TOE	FDP_ETC.2/TSM Export of user data with security attributes
		FDP_ETC.2 /EFTPOS/SMARTPINPAD Export of user data with security attributes
	FDP_IFC Information flow control policy	FDP_IFC.1/TSMCOMMUNICATION Subset information flow control
		FDP_IFC.1/EFTPOS/SMARTPINPAD COMMUNICATION Subset information flow control
	FDP_IFF Information flow control functions	FDP_IFF.1/TSMCOMMUNICATION Simple security attributes
		FDP_IFF.1/EFT-POS/SMART PINPAD COMMUNICATION Simple security attributes
	FDP_ITC Import from the outside of the TOE	FDP_ITC.2/TSM Import of user data with security attributes
		FDP_ITC.2/EFTPOS/SMARTPINPAD Import of user data with security attributes
	FDP_SDI Stored data integrity	FDP_SDI.2/MEMORY Stored data integrity monitoring and action
		FDP_SDI.2/DAILY and PRMTR Stored data integrity monitoring and action

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	Doküman No	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

Identification and Authentication (FIA)	FIA_AFL Authentication failures	FIA_AFL.1/MANUFACTURER Authentication failure handling
		FIA_AFL.1/AUTHORISED Authentication failure handling
	FIA_UAU User authentication	FIA_UAU.1 Timing of authentication
		FIA_UAU.4 Single-use authentication mechanisms
	FIA_UID User Identification	FIA_UID.1 Timing of identification
Security Management (FMT)	FMT_MSA Management of security attributes	FMT_MOF.1 Management of security functions behaviour
		FMT_MSA.1/PRIVILEGES Management of security attributes
		FMT_MSA.1/ IP: PORT INFO Management of security attributes
		FMT_MSA.1/FILE NAME and INFO-LABEL Management of security attributes
		FMT_MSA.1/EFTPOS/SMARTPINPAD SOURCE PORT INFO Management of security attributes
		FMT_MSA.1/ EFT-POS/SMART PINPAD LABEL INFO Management of security attributes
		FMT_MSA.3/USERS and SYSTEMS Static attribute initialisation
		FMT_MSA.3/EFTPOS/SMART PINPAD Static attribute initialisation
	FMT_MTD Management of TSF data	FMT_MTD.1/ FCR AUTHORISED USER Management of TSF data
		FMT_MTD.1/ AUTHORIZED MANUFACTURER USER Management of TSF data

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

	FMT_SMF Specification of Management Functions	FMT_SMF.1 Specification of Management Functions
	FMT_SMR Security management roles	FMT_SMR.2 Restrictions on security roles
Protection of the TSF (FPT)	FPT_FLS Fail secure	FPT_FLS.1 Failure with preservation of secure state
	FPT_PHP TSF physical protection	FPT_PHP.2 Notification of physical attack
	FPT_RCV Trusted recovery	FPT_RCV.1 Manual recovery
		FPT_RCV.4 Function recovery
	FPT_STM Time stamps	FPT_STM.1 Reliable time stamps
	FPT_TDC Inter-TSF TSF data consistency	FPT_TDC.1/TSM Inter-TSF basic TSF data consistency
		FPT_TDC.1/EFT-POS/SMART PINPAD Inter-TSF basic TSF data consistency
	FPT_TEE Testing of external entities	FPT_TEE.1/EXT Testing of external entities
		FPT_TEE.1/TIME Testing of external entities
Trusted Path/Channels (FTP)	FTP_ITC Inter-TSF trusted channel	FTP_ITC.1/TSM Inter-TSF trusted channel
		FTP_ITC.1/EFT-POS/SMART PINPAD Inter-TSF trusted channel


**Table 2**

## 2.6 Security Assurance Requirements

Assurance requirements of Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2 (NGCRFAS-2 PP) are consistent with assurance components in CC Part 3 and evaluation assurance level is “EAL 2”.

## 2.7 Results of the Evaluation

The evaluation is performed with reference to the CC v3.1 and CEM v3.1. The verdict of Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	Doküman No	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

(NGCRFAS-2 PP) is the pass as it satisfies all requirements of APE (Protection Profile, Evaluation) class of CC. Therefore, the evaluation results were decided to be "suitable".

## 2.8 Evaluator Comments / Recommendations

There are no recommendations concerning the Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2 (NGCRFAS-2 PP) .

## 3 PP DOCUMENT

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

**Name of Document:** Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2 (NGCRFAS-2 PP)

**Version No.:**1.3

**Date of Document:**06.05.2015

## 4 GLOSSARY

<b>AES</b>	: Advanced Encryption Standard
<b>CC</b>	: Common Criteria
<b>CCMB</b>	: Common Criteria Management Board
<b>DEMA</b>	: Differential Electromagnetic Analysis
<b>DES</b>	: Data Encryption Standard
<b>DFA</b>	: Differential Fault Analysis
<b>DPA</b>	: Differential Power Analysis
<b>EAL</b>	: Evaluation Assurance Level (defined in CC)
<b>EFTPOS</b>	: Electronic Funds Transfer at Point of Sale
<b>EMV</b>	: Europay, MasterCard and Visa
<b>ERU</b>	: Electronic Recording Unit
<b>FCR</b>	: Fiscal Cash Register
<b>GPRS</b>	: General Packet Radio Service
<b>GPS</b>	: Global Positioning System
<b>IT</b>	: Information Technology
<b>ITU</b>	: International Telecommunication Union
<b>OSP</b>	: Organizational Security Policy
<b>PP</b>	: Protection Profile

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	Doküman No	YTBD-01-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

<b>PKI</b>	: Public Key Infrastructure
<b>PRA</b>	: Presidency of Revenue Administration
<b>PRA-IS</b>	: Presidency of Revenue Administration Information Systems
<b>SAR</b>	: Security Assurance Requirements
<b>SEMA</b>	: Simple Electromagnetic Analysis
<b>SFR</b>	: Security Functional Requirements
<b>SHA</b>	: Secure Hash Algorithm
<b>SPA</b>	: Simple Power Analysis
<b>TDK</b>	: Terminal Data Key
<b>TOE</b>	: Target of Evaluation
<b>TREK</b>	: Terminal Random Encryption Key
<b>TRAK</b>	: Terminal Random Authentication Key
<b>TRMK</b>	: Terminal Random Master Key
<b>TRMKD</b>	: Terminal Random Master Key for Data
<b>TSF</b>	: TOE Security Functionality (defined in CC)
<b>TSE</b>	: Turkish Standards Institution
<b>TSM</b>	: Trusted Service Manager
<b>VAT</b>	: Value Added Tax

	<b>YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI</b>	<b>Doküman No</b>	<b>YTBD-01-01-FR-01</b>		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	23/01/2015		
		<b>Revizyon Tarihi</b>		<b>No</b>	00

## 5 BIBLIOGRAPHY

- [1]Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model,CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- [2]Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components,CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- [3]Common Criteria for Information Technology Security Evaluation,Part 3: Security Assurance Requirements,CCMB-2012-09-003,Version 3.1, Revision 4, September 2012
- [4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology;CCMB-2012-09-004, v3.1 rev4, September 2012
- [5] PRA Messaging Protocol Document, current version
- [6] Evaluation Technical Report , DTR 45 TR 01 - 05.06.2015
- [7] BTBD-01-01-TL-01 Certification Report Writing Instructions
- [8] External Device Communication Protocol Document, current version
- [9] Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software-2 (NGCRFAS-2 PP), Rev 1.3, 06.05.2015

## 6 ANNEXES

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