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 v1.7

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	04.09.2013
Version of Report	1
Author	Mehmet Kürşad ÜNAL, Murat ADSIZ
Technical Responsible	Mustafa YILMAZ
Approved	Mariye Umay AKKAYA
Date Approved	04.09.2013
Certification Report Number	21.0.01/13-030
Sponsor and Developer	Revenue Administration Department/Gelir İdaresi Başkanlığı
Evaluation Lab	TUBİTAK BİLGEM OKTEM
PP Name	Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software (NGCRFAS PP)
Pages	20

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
v1	04.09.2013	All	Final 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 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 (CCEF) 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 TUBİTAK 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 (PP version: 1.7) whose evaluation was completed on 03.08.2013 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the PP document with version no 1.7.

The certification report, certificate of PP evaluation and PP document are posted on the STCD 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.

1 - EXECUTIVE SUMMARY

This report describes the certification results by the certification body on the evaluation results applied with requirements of APE(Protection Profile Evaluation) 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(NGCRFAS PP).This report describes the evaluation results and its soundness and conformity.

The evaluation on was conducted Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software (NGCRFAS PP) v1.7 by TÜBİTAK-BİLGEM-OKTEM and completed on 03.08.2013.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. This PP satisfies all APE requirements of the CC, therefore the evaluation results were decided to be “suitable”.

The TOE (TOE is the product described in the PP) is an application which defines 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. FCR may consist of different parts. The TOE being the main item of an FCR, there are also several additional components necessary to get a fully functional FCR. These components are:

- Input/Output Interface,
- Fiscal memory,
- Daily memory,
- Database,
- ERU,
- Fiscal certificate memory.

TOE can provide the following main services:

- TOE supports storing sales data in fiscal memory,
- TOE supports storing for each receipt the total receipt amount and total VAT amount in daily memory,

- TOE supports generating reports (X report, Z report etc.),
- TOE supports transmitting Z reports, receipt information, sale statistics and other information determined by RAD to RAD-IS in RAD messaging protocol [5] format.
- TOE will start the communication with RAD-IS and instantly respond to requests originated from RAD-IS
- TOE stores records of important events as stated in RAD Messaging Protocol document and transmits to RAD-IS in RAD Messaging Protocol format in a secure way.
- TOE supports using by authorized user or authorized manufacturer user and using in secure state mode or maintenance mode.

TOE major security features for operational use

The TOE can provide the following security features:

- TOE supports access control,
- TOE supports secure communication between main processor and fiscal memory,
- However, for the cases where the main processor and the fiscal memory are included within the same electronic seal secure communication is not mandatory. 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 authenticating against RAD-IS and establishing a secure communication with RAD-IS.
- TOE supports secure communication between FCR, RAD-IS and FCR manufacturer.
- TOE ensures the integrity of event data.
- TOE records important events given in RAD Messaging Protocol document and immediately send urgent event data to RAD-IS in a secure way.
- TOE detects physical attacks to FCR and enters into the maintenance mode.

There are 7 assumptions made in the PP regarding the development environment, production environment, initialization and maintenance environment, use environment. The PP contains 6 Organizational Security Policies. There is one threat covered by operational environment and the

other 9 threats are covered by the TOE. The assumptions, the threats and the organizational security policies are described in chapter 3 in PP.

The CB(Certification Body) has examined the evaluation activities, provided the guidance for the technical problems and evaluation procedures, and reviewed each OR(Observation Reports) and ETR(Evaluation Technical Report).The CB confirmed that this PP is complete, consistent and technically sound through the evaluation results. Therefore, the CB certified that observation and evaluation results by evaluator are accurate and reasonable.

2 CERTIFICATION RESULTS

2.1 PP Identification

Project Identifier	TSE-CCCS/PP-002
PP Name and Version	Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software(NGCRFAS PP) v1.7
PP Document Title	Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software(NGCRFAS PP)
PP Document Version	v1.7
PP Document Date	28.08.2013
Assurance Level	EAL 2
Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model,CCMB-2012-09-001, Version 3.1, Revision 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
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology;CCMB-2012-09-004, v3.1 rev4, September 2012
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package Conformant to EAL2
Sponsor and Developer	Gelir İdaresi Başkanlığı/Revenue Administration Department of Turkey
Evaluation Facility	TÜBİTAK-BİLGEM-OKTEM
Certification Scheme	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, Authorized Manufacturer User, Modes of FCR and Assets. These notions are described in Table 1.

Table 1:

External Entities	1. **RAD-IS:** RAD-IS takes sales data and event data from FCR by sending query with parameters to FCR through TSM. 2. **Trusted Service Managing System:** TSM is the system at FCR manufacturer premises which is used to load parameters, update software and manage FCR. 3. **Attacker:** Attacker tries to manipulate the TOE in order to change its expected behavior and functionality. Attacker tries to breach confidentiality, integrity and availability on the FCR. 4. **RAD On-site Auditor:** RAD On-site Auditor is an employee of RAD who performs audits onsite to control the existence of expected FCR functionalities by using the rights of FCR authorized user. 5. **Certificate Storage:** The certificate storage holds certificates and private key used for authentication and secure communication. Certificate storage is protected inside physical and logical tampering system. 6. **Time Information:** FCR gets time information from RAD-IS. Time information is used during receipt, event, fiscal memory record, daily memory record and ERU record creation. 7. **Audit Storage:** Audit storage can be any appropriate memory unit in FCR. Audit storage stores important events according to their critical level (urgent, high, warning, information). List of events can be found in RAD messaging protocol document [5]. 8. **Storage Unit:** Storage units of FCR are database, fiscal memory, daily memory and ERU. 9. **Input Interface:** Input interfaces provide necessary input data from input devices to the TOE. Input devices for FCR may be keyboard, barcode reader, and QR code (matrix barcode) reader, order tracking device or global positioning devices. 10. **Output Interface:** Output interfaces deliver outputs of the TOE to the output devices. Output devices for FCR may be printer, display etc.
Roles	1. **FCR Authorised User:** FCR authorised user is the user who uses the functions of FCR and operates FCR by using his/her own password. It is possible that different FCR authorised users may have different rights. 2. **Authorized Manufacturer User:** Authorized

	Manufacturer User works for FCR manufacturer and conducts maintenance works on FCR.
Modes of FCR	1. **Secure State Mode:** Secure State Mode is the mode that allows FCR authorised user to use the functions of and to operate FCR and allow Authorized Manufacturer User to use maintenance access rights. FCR authorised user can do fiscal sales, configure FCR, take fiscal and FCR reports in this mode. 2. **Maintenance Mode:** Maintenance Mode is the mode that allow only Authorized Manufacturer User to fix FCR in case of any technical problem. FCR does not allow any fiscal transaction in maintenance mode. FCR enters this mode when the following occur; • FCR Certificate check fails, • Mesh cover monitoring check fails, • A disconnection between fiscal memory and main processor occurs, • Electronic seal is opened, or forced by unauthorized persons and • A technical problem is determined by FCR Manufacturer.
Assets	1. **Sensitive Data:** Sensitive data is used for data signing, key sharing and secure communication with RAD-IS and TSM. Confidentiality and integrity of this asset needs to be protected. 2. **Event Data:** Event data is used to obtain information about important events contained in audit storage. The integrity of this asset is crucial while stored in FCR and both integrity and confidentiality of this asset is important while it is transferred from TOE to RAD-IS. Event data is categorized in RAD Messaging Protocol Document[5]. 3. **Sales Data:** Sales data is stored in storage unit. Sales data is required for RAD-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 RAD-IS. 4. **Characterization Data(Identification data for devices):** Characterization data is a unique number assigned to each FCR given by the manufacturer. RAD-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. 5. **Authentication Data:** Authentication data contains authentication information which is required for FCR authorised users and authorized manufacturer user to gain access to

	FCR functionalities. Both integrity and confidentiality of this asset has to be protected. 6. **Time Information:** Time information is stored in FCR and synchronized with RAD-IS. Time information is important when logging important events and sending reports to the RAD-IS. The integrity of this asset has to be protected.

The PP includes 6 OSPs. These are:

- **P.Certificate:** It has to be assured that certificate which is installed at initialization step is compatible with ITU X.509 v3 format.
- **P.Comm - Communication between main processor and fiscal memory:** It has to be assured that communication between main processor and fiscal memory is used to encrypted using 3DES algorithm with minimum 112 bit key length or AES algorithm with 128 bit in case where the fiscal memory and the main processor are not protected by the same electronic seal. There is no need for encrypted communication in case where the fiscal memory and the main processor are protected by the same electronic seal.
- **P.SecureEnvironment:** It has to be assured that environment of TOE provides a mechanism that senses disconnection between fiscal memory and main processor. Then TOE enters into the maintenance mode and logs urgent event. Moreover, it has to be assured that fiscal memory doesn't accept transactions with negative amounts which results in a decrease of total tax value. Also it has to be assured that environment of TOE provides a mechanism that sales data in daily memory which are not reflected to the fiscal memory cannot be deleted and modified in an uncontrolled way. In addition to this, it has to be assured that sales data in ERU cannot be deleted and modified. It has to be assured that FCR stops processing fiscal transactions during maintenance work of authorized manufacturer users.
- **P.PhysicalTamper:** It has to be assured that IT environment provides physical tampering protection system which identifies unauthorized access to the keys (asymmetric key, symmetric key), events, characterization data and fiscal memory data. It has to be assured that IT environment logs this type of events. In addition to logging, FCR blocks fiscal transactions. On the other hand it has to be assured that authorized access such as maintenance work or service works are logged. It also has to be assured that IT environment provides tamper evident system for certificates which is formed by electromechanical keys. Physical tampering protection system also has to be assured that it protects fiscal memory.
- **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-sharing.
- **P.UpdateControl:** TOE is allowed to be updated by TSM. To avoid possible threats in this operation, operating system 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, cash register shall calculate and send the hash value of the TOE to RAD-IS in case of demand.

2.3 Assumptions and Clarification of Scope

This section describes the assumptions must be satisfied by the TOE operational environment, threats satisfied by the TOE and/or operational environment. The PP includes following 7 assumptions:

- **A.TrustedDesigner**

It is assumed that software part of the TOE used in FCR is designed and implemented by trusted designers. They design and implement it in a manner which maintains IT security. It is assumed that they don't leave non-certified test modes and back doors with the software which is used by the end user.

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

- **A.Initialisation**

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. It is assumed that no other application is run during the initialization step. Moreover, it is assumed that environment of TOE provides secure installation of certificate 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**

FCR authorised 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.

The PP includes following 10 threats:

- **T.AccessControl**

Adverse action: Users and systems could try to use functions which are not allowed. (e.g. FCR authorised users gaining access to authorized manufacturer user management functions)

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

Asset: Event data, sales data.

- **T.Identification**

Adverse action: Users could try to bypass identification and authentication.

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

Asset: Sales data, event data.

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

Adverse action: This threat deals with two types of data: event data and sales data.

- 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 RAD-IS and FCR.
- An attacker could try to manipulate or delete the sales data generated by FCRAS which may result in tax fraud. In addition, an attacker also could try to disclose sales data while transmitted between RAD-IS and FCR. Manipulation and deletion of sales data may be caused by magnetic and electronic reasons.

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

Asset: Event data, sales data.

- **T.MCharData-Manipulation of characterization data**

Adverse action: An attacker could try to manipulate the characterization data to cover information about tax fraud; to masquerade the user identity.

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

Asset: Characterization 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 RAD-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, 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 RAD-IS to request information from FCR via the communication channel.

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

Asset: Sales data, and event data.

- **T.Counterfeit - FCR counterfeiting**

Adverse action: An attacker could try to imitate FCR to respond RAD-IS calls via the communication channel to cover information about tax fraud.

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

Asset: Sensitive data.

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

Adverse action: An attacker may try to use FCR out of its normal operational conditions (power, frequency, humidity, temperature) to cause malfunction in FCRAS.

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

Asset : Sales data, event data, authentication data and sensitive data.

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

Adverse action: An attacker may try to obtain sensitive information (private key, session key) when FCR performs encryption operation by side channel attacks like SPA (Simple power analysis), SEMA (Simple Electromagnetic Analysis), DPA (Differential power analysis), DEMA (Differential electromagnetic analysis).

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

Asset: Sensitive 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.

To understand clarification of scope, details can be found in PP section1.2.3, Non-TOE hardware/software/firmware part.

2.4 Architectural Information

Figure 1 shows the TOE and its environment. The detailed information about TOE environment can be found in the TOE Overview Section of the PP document.

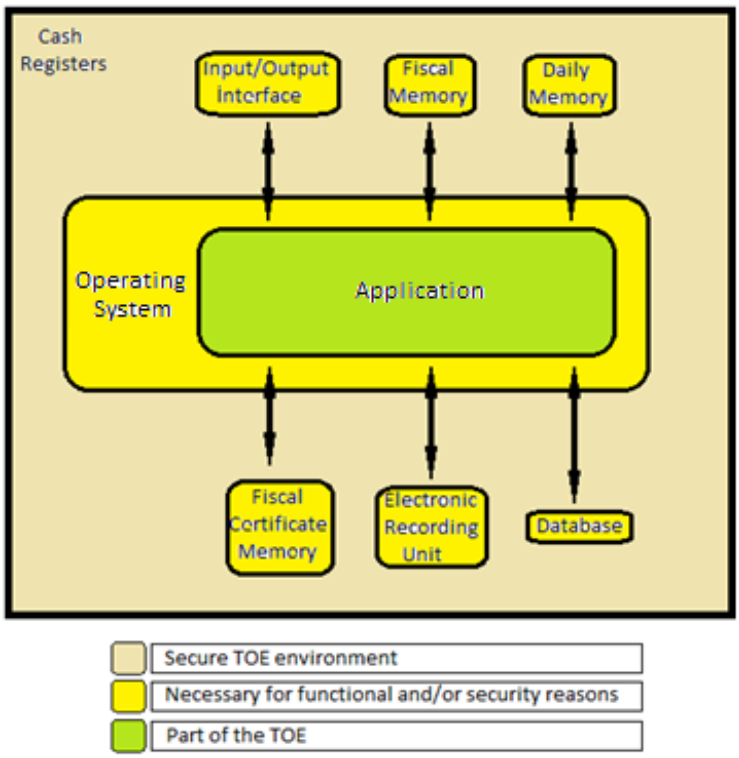

Figure 1

The green part of the figure1 is the TOE and the yellow part is the TOE environment. Operating system, I/O interface, Fiscal memory, Daily Memory, Fiscal Certificate Memory, Electronic Recording Unit and Database are TOE environment as shown in the figure 1.

2.5 Security Functional Requirements

Table 2 describes Security Functional Requirements.

Table 2

Security Functional Class	Security Functional Component
Security Audit (FAU)	FAU_GEN.1-Audit Data Generation FAU_SAR.1-Audit Review FAU_STG.1-Protected Audit Trail Storage FAU_STG.4-Prevention of Audit Data Loss
Communication (FCO)	FCO_NRO.2-Enforced Proof of Origin
Cryptographic Support (FCS)	FCS_CKM.1-Cryptographic Key Generation FCS_CKM.4-Cryptographic Key Destruction FCS_COP.1/ENC-DEC-Cryptographic Operation FCS_COP.1/HASHING-Cryptographic Operation
User Data Protection (FDP)	FDP_ACC.1-Subset Access Control FDP_ACF.1-Security Attribute Based Access Control FDP_ETC.2-Export of User Data with Security Attributes FDP_IFC.1-Subset Information Flow Control FDP_IFF.1-Simple Security Attributes FDP_ITC.2-Import of User Data without Security Attributes FDP_SDI.2-Stored Data Integrity Monitoring and Action
Identification and Authentication (FIA)	FIA_AFL.1-Authentication Failure Handling FIA_UAU.2-User Authentication Before Any Action FIA_UID.2-User Authentication Before Any Action
Security Management (FMT)	FMT_MOF.1-Management of Security Functions Behaviour FMT_MSA.1/USER IDENTITY-Management of Security Attributes FMT_MSA.1/PRIVILEGES-Management of Security Attributes FMT_MSA.3-Static Attribute Initialisation FMT_MTD.1-Management of TSF Data FMT_MTD.2-Management of Limits on TSF Data FMT_SMF.1-Specification of Management Functions FMT_SMR.2-Restrictions on Security Roles
Protection of The TSF (FPT)	FPT_FLS.1-Failure with Preservation of Secure State

	FPT_PHP.2-Notification of Physical Attack FPT_PHP.3-Resistance to Physical Attack FPT_RCV.1-Manual Recovery FPT_RCV.4-Function Recovery FPT_STM.1-Reliable Time Stamps FPT_TDC.1-Inter-TSF basic TSF Data Consistency FPT_TEE.1-Testing of External Entities FPT_TST.1-TSF Testing
Trusted Path/Channels (FTP)	FTP_ITC.1-Inter-TSF Trusted Channel

2.6 Security Assurance Requirements

Assurance requirements of Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software (NGCRFAS 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 (NGCRFAS 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 (NGCRFAS PP) v1.7.

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 (NGCRFAS PP)
Version No.:1.7
Date of Document:28.08.2013

4 GLOSSARY

AES: Advanced Encryption Standard
CC: Common Criteria
CCMB: Common Criteria Management Board
DEMA: Differential Electromagnetic Analysis

DES: Data Encryption Standard
DFA: Differential Fault Analysis
DPA: Differential Power Analysis
EAL: Evaluation Assurance Level
EFTPOS: Electronic Funds Transfer at Point of Sale
EMV: Europay, Mastercard, Visa
ERU: Electronic Recording Unit
FCR: Fiscal Cash Register
FCRAS: Fiscal Cash Register Application Software
GPRS: General Packet Radio Service
GPS: Global Positioning System
IT: Information Technology
ITU: International Telecommunication Union
OSP: Organisational Security Policy
PP: Protection Profile
PKI: Public Key Infrastructure
RAD: Revenue Administration Department
RAD-IS: Revenue Administration Department Information Systems
SAR: Security Assurance Requirements
SEMA: Simple Electromagnetic Analysis
SFR: Security Functional Requirements
SHA: Secure Hash Algorithm
SPA: Simple Power Analysis
SSL-CA: Secure Socket Layer – Client Authentication
TOE: Target of Evaluation
TSF: TOE Security Functionality
TSE: Turkish Standards Institute
TSM: Trusted Service Manager
VAT: Value Added Tax

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] RAD Messaging protocol , version 2.02 , April 2012

[6] Evaluation Technical Report , DTR 26 TR 02 – 28.08.2013

[7] YTBD-01-01-TL-01 Certification Report Writing Instructions

6 ANNEXES

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