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

TABLE of CONTENTS

Document Information

Date of Issue	29.12.2014
Version of Report	1
Author	Zümrüt MÜFTÜOĞLU
Technical Responsible	Mustafa YILMAZ
Approved	Mariye Umay AKKAYA
Date Approved	30.12.2014
Certification Report Number	21.0.01/14-51
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 2 (NGCRFAS PP 2)
Pages	23

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
v1	21.12.2014	All	First Released
v2	29.12.2014	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: 1.1) whose evaluation was completed on 25.12.2014 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the PP document with version no 1.1.

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 2(NGCRFAS PP 2).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 2 (NGCRFAS PP 2) by TÜBİTAK-BİLGEM-OKTEM and completed on 25.12.2014.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 software 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 FCR is mandatory for first-and second-class traders and is not mandatory for sellers who sell the goods back to their previous seller as completely the same as the purchased good. In addition to TOE, which is the main item of FCR, FCR may consist of several other hardware and software components.
These components are:

- Input/Output Interface,
- Fiscal Memory,
- Daily Memory,
- Database,
- Electronic Recording Unit,
- Fiscal Certificate Memory.

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 [5] format.
- TOE is able to start the communication with PRA-IS and instantly respond to requests originated from PRA-IS.
- 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 mode or maintenance mode.

TOE major security features

The TOE provides 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 is able to detect disconnection between main processor and fiscal memory and 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 ensures the integrity of event data, sales data, authentication data, characterization data and FCR parameters.
- TOE records important events defined in PRA Messaging Protocol Document [6] and send urgent event data immediately to PRA-IS in a secure way.
- TOE detects physical attacks to FCR and enters into the maintenance mode in such cases.

There are 7 assumptions that must be satisfied by the TOE's operational environment. The PP contains 8 Organizational Security Policies.There are 8 threats covered by operational environment and the TOE. The assumptions, the threats and the organizational security policies are described in chapter 3 in the 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-005
PP Name and Version	Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software 2(NGCRFAS PP 2) v1.1
PP Document Title	Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software 2(NGCRFAS PP 2)
PP Document Version	v1.1
PP Document Date	25.12.2014
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/ Presidency of Revenue Administration
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, Modes of FCR and Assets. These notions are described in Table 1.

Table 1:

External Entities	**1. PRA-IS :** PRA-IS takes sales data and event data from FCR by sending query with parameters to FCR through TSM. **2.Trusted Service Manager:**TSM is the system 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 of the FCR. **4.PRA On-site Auditor:**PRA On-site Auditor is an employee of PRA who performs onsite audits onsite to control the existence of expected FCR functionalities by using the rights of FCR Authorised 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 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. **7.Audit storage:** 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 [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, QR code (matrix barcode) reader, order tracking device and global positioning devices. **10.External Device:** External device is the device which is used to communicate with FCR by using secure channel according to External Device Communication Protocol Document [8] **11.Output interface:** Output interfaces deliver outputs of the TOE to the output devices. Output devices for FCR may be printer, display etc. **12.Main Unit:** Main Unit is an external device

	which is used for following actions; □Provides visual interface for fiscal transaction, □Provides input interface for fiscal transaction, □Provides secure communication with TOE according to External Device Communication Protocol Document [8](Please see Application Note 1 in the PP)
Roles	**1.FCR Authorised User:** FCR Authorised User is the user who uses the functions of FCR and operates FCR by accessing the device over an authentication mechanism. **2.Authorised Manufacturer User:** Authorised Manufacturer User works for FCR manufacturer and conducts maintenance works on FCR. **3.FCR User (Cashier):** FCR user is the user who uses the sale functionality of FCR by using his/her identity.(Please see Application Note 2 in the PP)
Modes of FCR	**1.Maintenance Mode:** Maintenance Mode is the mode that allows only Authorised Manufacturer User to fix FCR in case of any technical problem, to change date and time information; to review event data and to start update operation of TOE.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 unauthorised persons, ✓ A technical problem is determined by FCR Manufacturer. **2.Secure State Mode:** Secure State Mode is the mode that allows; FCR Authorised User; ✓ to configure FCR, ✓ to take fiscal and FCR reports FCR User; ✓ to do fiscal sales(Please see Application Note 3 in the PP)
Assets	**1.Sensitive data** Sensitive data is used for secure communication with PRA-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 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 [5]. **3.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. **4.Characterization data (Identification data for devices)** Characterization data is a unique number assigned to each FCR given 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. **5.Authentication data** 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. **6.Time Information** 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.

7.FCR Parameters

FCR parameters stored in FCR are updated by TSM after Z report is printed.

FCR parameters set;

- Sales and event data transferring time
- Criticality level of event data sent to the PRA-IS
- Maximum number of days that FCR will work without communicating with PRA-IS

8.Server Certificates

Server certificates contain PRA-IS and TSM certificates (P_{PRA}, $P_{PRA\text{-}SIGN}$, P_{TSM} and $P_{TSM\text{-}SIGN}$) P_{PRA} and $P_{PRA\text{-}SIGN}$ certificates are used for signing and encryption process during key transport between TOE and PRA-IS.

P_{TSM} certificate is used for encryption process during key transport between TOE and TSM and $P_{TSM\text{-}SIGN}$ is used for signature verification of FCR parameters by TOE.

The PP includes 8 OSPs :

- **P.Certificate:** It has to be assured that certificates which are installed at initialization step, are compatible with ITU X.509 v3 format.
- **P.Certificates Installation:** It has to be assured that environment of TOE provides secure installation of certificates (P_{PRA}, $P_{PRA-SIGN}$, P_{TSM}, $P_{TSM-SIGN}$) 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 encrypted using AES algorithm with 256 bits according to External Device Communication Protocol Document [8]
- **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 (secret key) when FCR performs encryption 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. 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 is 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.
- **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. On the other hand 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 7 assumptions:

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 these controls PRA-IS personnel should check that if 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, 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

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, Main Unit) generates strong key for communicating with TOE.

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 Users gaining access to FCR Authorised User management 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: Unauthorized users could try to use FCR functions.
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 four types of data: event data, sales data, characterization 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.

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.

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(TREK,TRAK and TDK) data while communicating with PRA-IS and TSM to cover information about tax fraud.
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_{PRA}, $P_{PRA\text{-}SIGN}$, P_{TSM} and $P_{TSM\text{-}SIGN}$) 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 TOE and its environment. The detailed information about TOE environment can be found in the TOE Overview Section of the PP document.

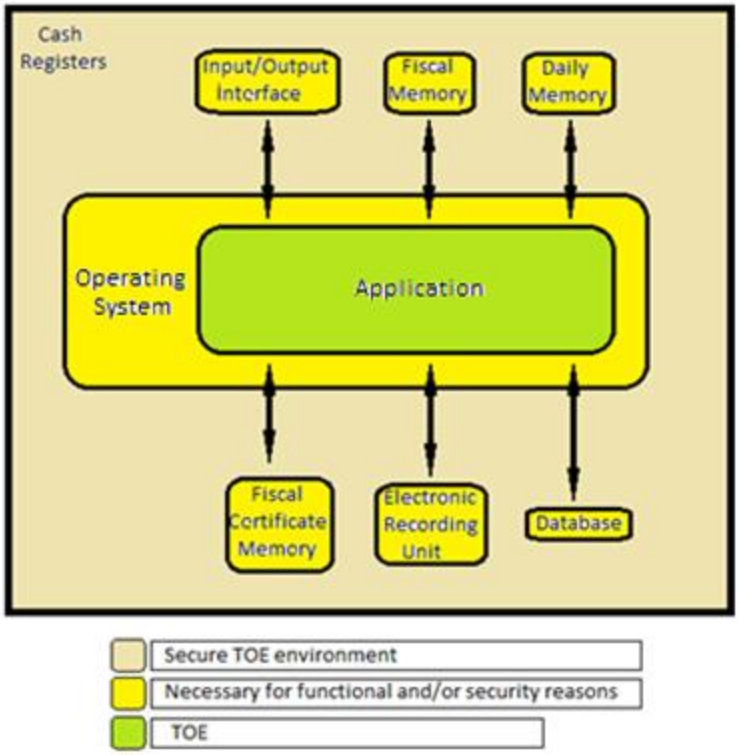

Figure 1

The green part of the figure1 is the TOE and the yellow parts are the TOE's environmental components which are crucial for functionality and security.

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/TRMK -Cryptographic Key Generation FCS_CKM.1/ TRMKD Cryptographic key generation FCS_CKM.1/ DHE-KEY Cryptographic key generation FCS_CKM.1/ EXT-DEV K_{HMAC} Cryptographic key generation FCS_CKM.1/ EXT-DEV K_{ENC} Cryptographic key generation FCS_CKM.2 Cryptographic key distribution FCS_CKM.4-Cryptographic Key Destruction FCS_COP.1/ TREK -Cryptographic Operation FCS_COP.1/TRAK-Cryptographic Operation FCS_COP.1/ TDK Cryptographic operation FCS_COP.1/HASHING Cryptographic key generation FCS_COP.1/TRMK-DEC Cryptographic key generation FCS_COP.1/TRMKD-DEC Cryptographic key generation FCS_COP.1/ PUB-ENC Cryptographic key generation FCS_COP.1/ SIGN-VER Cryptographic key generation FCS_COP.1/ EXT-DEV K_{ENC} Cryptographic key generation FCS_COP.1/ EXT-DEV K_{HMAC} Cryptographic key generation FCS_COP.1/ EXT-DEV KEYEXCHANGE Cryptographic key generation

User Data Protection (FDP)	FDP_ACC.1-Subset Access Control FDP_ACF.1-Security Attribute Based Access Control FDP_ETC.2/TSM-Export of User Data with Security Attributes FDP_ETC.2 /EFTPOS Export of user data with security attributes FDP_ETC.2 /MAIN UNIT Export of user data with security attributes (Please see Application Note 9 in the PP) FDP_IFC.1/TSMCOMMUNICATION-Subset Information Flow Control FDP_IFC.1/EFTPOSCOMMUNICATION-Subset Information Flow Control FDP_IFC.1/MAIN UNIT-Subset Information Flow Control(Please see Application Note 10 in the PP) FDP_IFF.1/TSMCOMMUNICATION-Simple Security Attributes FDP_IFF.1/EFT-POSCOMMUNICATION-Simple Security Attributes FDP_IFF.1/MAIN UNIT-Simple Security Attributes(Please see Application Note 11 in the PP) FDP_ITC.1 Import of user data without security attributes FDP_ITC.2/TSM-Import of User Data without Security Attributes FDP_ITC.2/EFTPOS-Import of User Data without Security Attributes FDP_ITC.2/MAIN UNIT-Import of User Data without Security Attributes(Please see Application Note 13 in the PP) FDP_SDI.2/MEMORY Stored Data Integrity Monitoring and Action FDP_SDI.2/DAILY and PRMTR Stored data integrity monitoring and action

Identification and Authentication (FIA)	FIA_AFL.1/MANUFACTURER Authentication Failure Handling FIA_AFL.1/AUTHORISED Authentication failure handling FIA_UAU.1 Timing of Authentication FIA_UAU.2-User Authentication Before Any Action(Please see Application Note 15 in the PP) FIA_UAU.4 Single-use authentication mechanisms FIA_UID.1 Timing of identification FIA_UID.2-User Authentication Before Any Action(Please see Application Note 16 in the PP)
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.1/ IP:PORT INFO Management of security attributes FMT_MSA.1/FILE NAME and INFO-LABEL Management of security attributes FMT_MSA.1/ INFO-LABEL Management of security attributes(Please see Application Note 19 in the PP) FMT_MSA.1/MAIN UNIT SOURCE PORT INFO Management of security attributes(Please see Application Note 19 in the PP) FMT_MSA.1/EFTPOS SOURCE PORT INFO Management of security attributes FMT_MSA.1/ EFT-POS LABEL INFO Management of security attributes FMT_MSA.3/USERS and SYSTEMS Static attribute initialization FMT_MSA.3/EFTPOS Static attribute initialization FMT_MSA.3/MAIN UNIT Static attribute initialisation(Please see Application Note 20 in the PP) FMT_MTD.1/ FCR AUTHORİSED USER Management of TSF data FMT_MTD.1/AUTHORİZED MANUFACTURER USER Management of

	TSF data FMT_MTD.1/ FCR USER Management of TSF data(Please see Application Note 22 in the PP) 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_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/EXT Testing of external entities FPT_TEE.1/TIME 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 2 (NGCRFAS PP 2) 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 (NGCRFAS PP 2) 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 PP 2) .

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 PP 2)

Version No.:1.1

Date of Document:25.12.2014

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 (defined in CC)

EFTPOS : Electronic Funds Transfer at Point of Sale

EMV : Europay, MasterCard and Visa

ERU : Electronic Recording Unit

FCR : Fiscal Cash Register

GPRS : General Packet Radio Service

GPS : Global Positioning System

IT : Information Technology

ITU : International Telecommunication Union

OSP : Organizational Security Policy

PP : Protection Profile

PKI : Public Key Infrastructure

PRA : Presidency of Revenue Administration

PRA-IS : Presidency of Revenue Administration Information Systems

SAR : Security Assurance Requirements

SEMA : Simple Electromagnetic Analysis

SFR : Security Functional Requirements

SHA : Secure Hash Algorithm

SPA : Simple Power Analysis

TDK : Terminal Data Key

TOE : Target of Evaluation

TREK : Terminal Random Encryption Key

TRAK : Terminal Random Authentication Key

TRMK : Terminal Random Master Key

TRMKD : Terminal Random Master Key for Data

TSF : TOE Security Functionality (defined in CC)

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] PRA Messaging Protocol Document, version 2.2

[6] Evaluation Technical Report , DTR 35 TR 03 - 27.12.2014

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

[8] External Device Communication Protocol Document, version 1.0

[9] Common Criteria Protection Profile for New Generation Cash Register Fiscal Application software 2 (NGCRFAS-2 PP),Rev 1.1,25.12.2014

6 ANNEXES

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