COMMON CRITERIA PROTECTION PROFILE

for

NEW GENERATION CASH REGISTER FISCAL APPLICATON SOFTWARE

(NGCRFAS PP)

TSE-CCCS/PP-002

Revision No	1.7
Revision Date	28.08.2013
Document Code	
File Name	NGCRFAS PROTECTION PROFILE
Prepared by	Mehmet YÜCEDAĞ and Oğuz DEMİROĞLU
Approved by	Salih SARI

Revision History

Revision No	Revision Reason	Date of Revision
0.1	First Draft	04.05.2012
1.0	SFRs update	17.10.2012
1.1	"Gözlem raporu_1" update	17.12.2012
1.2	"Gözlem raporu_2" update	29.01.2013
1.3	"Gözlem raporu_3" update	01.04.2013
1.4	"Gözlem raporu_4" update	14.06.2013
1.5	"Gözlem raporu_5" update	02.08.2013
1.6	"Gözlem kararı 3" update	27.08.2013
1.7	"Gözlem kararı 3" update	28.08.2013

CONTENTS

1. PP INTRODUCTION

This Protection Profile (PP) describes the following items:

- The Target of Evaluation (TOE) as a product and its position in production life cycle,
- The security environment of the TOE includes: the assets to be protected, the threats to be encountered by the TOE , the development environment and production utilization phases,
- The security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of application data and programs,
- Protection of the TOE and associated documentation during the development and production phases,
- The Information Technology (IT) security requirements which include the TOE functional requirements and the TOE assurance requirements.

1.1 PP Reference

Title: Common Criteria Protection Profile for New Generation Cash Register Fiscal Application Software (NGCRFAS PP)

Sponsor: Revenue Administration Department (RAD)

Editor(s):

Prepared by Mehmet YÜCEDAĞ and Oğuz DEMİROĞLU

Approved by Salih SARI

CC Version: 3.1 (Revision 4)

Assurance Level: Minimum assurance level for this PP is EAL 2.

General Status: Final

Version Number: 1.7 as of 28th August 2013

Registration: TSE-CCCS/PP-002

Key words : New Generation Cash Register, EMV, EFT-POS, RAD, Electronic Registration Unit.

Note: A glossary of terms used in the Protection Profile is given in GLOSSARY and ACRONYMS section of the document (Section 7).

1.2 TOE Overview

The TOE addressed by this Protection Profile (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, described in Section 1.2.1, 1.2.2. TOEs related components are given in Figure 1. Usage and major security features of TOE are described in section 1.2.3.

1.2.1 General overview of the TOE and related components

Figure 1 shows the general overview of the TOE and related components as regarded in this PP. The green part of Figure 1 is the TOE. Yellow parts given as input/output interface, fiscal memory, daily memory, database, ERU, fiscal certificate memory are TOE environments which are crucial parts of the FCR for functionality and security. Connections between the TOE and its environment are also subject of the evaluation since they are interfaces of the TOE.

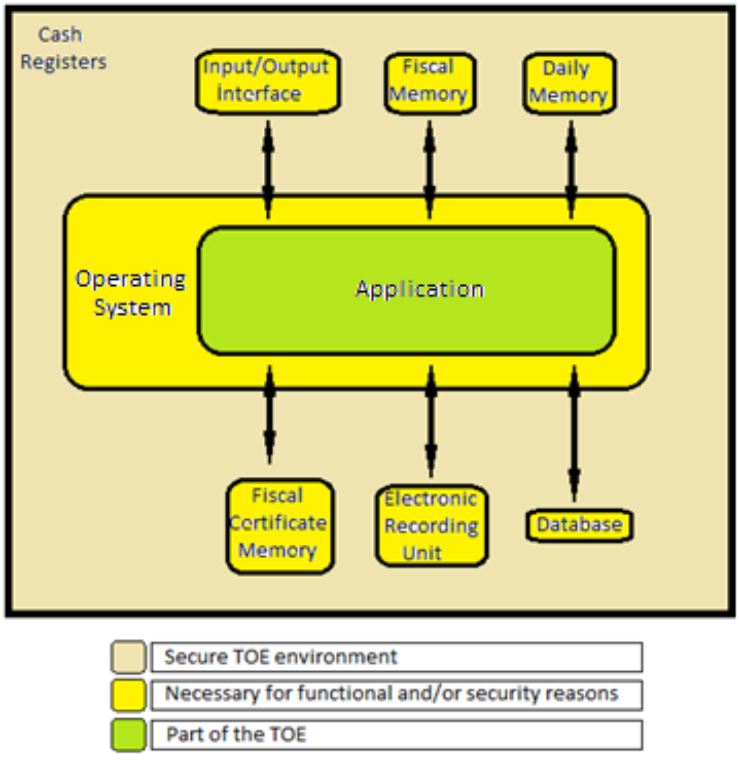

Figure 1 TOE and related components

1.2.2 Required Non-TOE Hardware/Software

Software, hardware environment of the TOE are described below.

1.2.2.1 Software environment of TOE

TOE runs at the top of an operating system, its file-system and software libraries as in a typical software environment. This structure is shown in Table 1.

Table 1 Typical software environment of TOE

File System and Software Libraries
Operating System Kernel

In addition to TOE, following software components are necessary for security and functionality of the FCR:

- Application runs on an **operating system** which supports following features
  - at least 32-bit data processing capacity
  - multi-processing
  - IPv4 and IPv6
  - NTP (Network Time Protocol)
- **Database which is** used to store sales data, has the following features;

i. Database has data recording, organizing, querying, reporting features

ii. Database stores sales records for main product groups (food, clothing, electronics, glassware etc.) and sub-product groups (milk, cigarette, fruit, trousers etc.) in order to track detailed statistics

iii. Database has indexing mechanism

1.2.2.2 Hardware Environment of TOE

In addition to TOE, following hardware components are necessary for security and functionality of the FCR:

- **Fiscal memory**

i. **Fiscal memory** has following features;

a. Fiscal memory has the capacity to store at least 10 years (3650 days) of data,

b. Fiscal memory keeps data at least 5 years after the capacity specified in (a) has been reached,

c. Fiscal memory is to be fixed in FCR in a way that it cannot be removed without damaging the chassis.

d. Fiscal memory is protected with mesh cover,

e. Fiscal memory has the ability to protect against magnetic and electronic threats,

   When the Fiscal memory and main processor interconnection is interrupted, FCR will begin to run in maintenance mode,

f. The data stored in the fiscal memory shouldn't be lost in case of power off,

g. Fiscal Memory accepts only positive amounts from the application and the peripherals,

h. FCR checks "Z" reports from fiscal memory during device start-up. In case there are days for which Z report was not generated, FCR will be able to run in normal mode only after it generates Z reports for the missing days. Seasonal firms can take cumulative Z report by specifying date and time range.

ii. Fiscal Memory includes following data;

a. Fiscal symbol, company code, identification number of the device,

b. Cumulative sum of the total sales amount and Value Added Tax (VAT) amounts of all sales receipts, starting from the device activation (i.e. first use),

c. Date and number of daily "Z" reports with total sales and VAT per day,

d. The number of receipts per day.

- **Daily memory** has following features;

i. Receipt total and total VAT amount for each receipt are to be stored in the daily memory instantly. On demand, this data can be transmitted to RAD information systems (RAD - IS), instantly or daily.

ii. Data in the daily memory which is not already transmitted to fiscal memory, cannot be modified in an uncontrolled way.

iii. Data transmitted from daily memory to fiscal memory is to be kept in daily memory for at least 10 days.

iv. Z reports, taken at the end of the day, and X reports, taken within the present day are produced by the data in the daily memory.

v. Following are to be stored in the daily memory

a. total VAT amount per day,

b. total daily sales values per day grouped by payment type

c. payment type (Cash, credit card etc.)

d. number of receipts.

- FCR supports X.509 formatted digital certificate generated by Authorized Certificate Authority. This **Public Key Infrastructure (PKI)** compatible digital certificate is called **fiscal certificate** and is used for authentication, secure communication between RAD-IS and FCR through Trusted Service Manager (TSM). For physical security FCR is protected by electronic and mechanic systems called **electronic seal**. FCR uses **cryptographic library** for secure communication with RAD-IS.
- **Electronic Record Unit(ERU)** is used to keep second copy of the receipt and has following features;
  i. ERU stores information about receipts and reports (X, Z) in a retrievable form.
  ii. ERU has at least 1.2 million row capacity.ERU may be included in the sealed part of the FCR.In this case ERU must have at least 40 million row capacity.
  iii. Data stored in ERU cannot be modified
  iv. ERU also has features specified in "*Fiscal Cash Register General Communique Serial Number:67"* part A which is about Law No:3100 except item (ii) above.
- FCR devices have at least one of the internal ETHERNET, PSTN or mobile communication technology (GPRS etc.) interfaces and EFTPOS-integrated FCR devices have at least two of these interfaces for communication with RAD-IS (for data transfer) and TSM system (for parameter management and software update). External ETHERNET may be accepted as internal in case the data is encrypted in fiscal unit.
- FCR has a **firewall** to control incoming and outgoing data traffic.
- FCR has a **printer** to print sales receipt.
- FCR supports usage of **EFTPOS**.
- FCR needs some input/output devices for functionalities listed below;
  i. FCR has **keyboard unit**. Additionally, it may optionally use a touch screen.
  ii. FCR has separate displays for **cashier and buyer**.
  iii. FCR has **internal battery** to keep time information.

1.2.3 Major security and functional features

The functional and major security features of the TOE are described below.

1.2.3.1 TOE functional features

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

i. TOE supports storing sales data in fiscal memory.
ii. TOE supports storing for each receipt the total receipt amount and total VAT amount in daily memory.
iii. TOE supports generating reports (X report, Z report etc.).
iv. TOE supports transmitting Z reports, receipt information, sale statistics and other information determined by RAD to RAD-IS in RAD Messaging Protocol [6] format.
v. TOE will start the communication with RAD-IS and instantly respond to requests originated from RAD-IS.
vi. TOE stores records of important events as stated in RAD Messaging Protocol document and transmits to RAD-IS in RAD Messaging Protocol [6] format in a secure way.
vii. TOE supports using by authorized user or authorized manufacturer user and using in secure state mode or maintenance mode. Roles and modes of operation are described in 3.1.2 and 3.1.3 respectively.

1.2.3.2 TOE major security features

The TOE provides following security features;

i. TOE supports access control.
ii. TOE supports secure communication between main processor and fiscal memory.
iii. 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.
iv. 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.
v. TOE supports secure communication between FCR, RAD-IS and FCR manufacturer.
vi. TOE ensures the integrity of event data.
vii. TOE records important events given in RAD Messaging Protocol document and immediately send urgent event data to RAD-IS in a secure way.
viii. TOE detects physical attacks to FCR and enters into the maintenance mode.

1.2.4 TOE type

TOE is a firmware embedded within FCR.

2. CONFORMANCE CLAIMS

2.1 CC Conformance Claim

This protection profile claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [3]

As follows

- Part 2 conformant,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012 [4]

has to be taken into account.

2.2 PP Claim

This PP does not claim conformance to any protection profile.

2.3 Package Claim

The current PP is conformant to the following security requirements package:

- Assurance package EAL2 conformant to CC, part 3.

2.4 Conformance Claim Rationale

Since this PP does not claim conformance to any protection profile, this section is not applicable.

2.5 Conformance Statement

This PP requires demonstrable conformance of any ST or PP claiming conformance to this PP.

3. SECURITY PROBLEM DEFINITION

3.1 Introduction

3.1.1 External Entities

RAD-IS

RAD-IS takes sales data and event data from FCR by sending query with parameters to FCR through TSM.

Trusted Service Managing System

TSM is the system at FCR manufacturer premises which is used to load parameters, update software and manage FCR.

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.

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.

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.

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.

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 [6].

Storage unit

Storage units of FCR are database, fiscal memory, daily memory and ERU.

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 or global positioning devices.

Output interface

Output interfaces deliver outputs of the TOE to the output devices. Output devices for FCR may be printer, display etc.

3.1.2 Roles

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.

Authorized Manufacturer User

Authorized Manufacturer User works for FCR manufacturer and conducts maintenance works on FCR.

3.1.3 Modes of FCR

Secure State Mode : Secure State Mode is the mode that allow 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.

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.

3.1.4 Assets

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.

Application note 1: *Sensitive data may consist of asymmetric private key and symmetric key.*

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[6].

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.

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.

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.

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.

3.2 Threats

Threats averted by TOE and its environment are described in this section. Threats described below results from assets which are protected or stored by TOE or from usage of TOE with its environment.

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.

3.3 OSP

This section describes organizational security policies that must be satisfied.

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.

3.4 Assumptions

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

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.

4. SECURITY OBJECTIVES

This chapter describes security objectives for the TOE and it's operational environment.

4.1 Security Objectives for the TOE

This part describes security objectives provided by the TOE.

O.AccessControl

TOE must control user (FCR Authorised User, Authorized Manufacturer User) access to functions and data.

O.Event

TOE must record important events stated as in RAD Messaging Protocol document.

O.Integrity

TOE must provide integrity for sales data and event data.

O.Authentication

TOE must run authentication mechanism for users and systems.

O.Function

TOE must ensure that processing of inputs to derive sales data and event data is accurate.

O.Transfer

TOE must provide confidentiality and integrity for transferring sales data, event data to the RAD-IS. TOE must provide integrity for characterization data transferred to the RAD-IS. TOE must also provide integrity for sales data and event data transferred from memories to other memories.

4.2 Security Objectives for the Operational Environment

This part describes security objectives provided by the operational environment

OE.Development

Developers must ensure that they implement software part of the TOE in a manner which maintains IT security during development.

OE.Manufacturing

Manufacturer should ensure that FCR is protected against physical attacks during manufacturing.

OE.Delivery

FCR authorised user must ensure that delivery of the TOE is done by a secure way.

OE.KeyGeneration

Asymmetric key generation mechanism shall be accessible only by trusted persons.

OE.KeyTransportation

Asymmetric key private components transportation and installation to the FCR must be done by protecting its confidentiality and integrity.

OE.TestEnvironment

Before FCR activation; test interfaces (functions, parameters) inserted in TOE should be disabled or removed.

OE.StrongAlgorithm

Algorithms used in FCR shall be strong. Also they should have protection against side channel analysis (SPA,DPA,SEMA,DEMA,DFA).

OE.UpgradeSoftware

Updates in software used in FCR should be get pass verdict from Common Criteria maintenance or reevaluation procedures (according to update type) before installed to the FCR. This will be validated by the operating system on the FCR, using the cryptographic signature control methods.

OE.TrustedUser

FCR authorised user and authorised manufacturer user shall act responsibly (use FCR for every sale, use correct VAT rates for sale).

OE.Control

RAD Onsite Auditor must check FCR functionality by controlling tax amount on the receipt and tax amount sent to the RAD-IS.

4.3 Security Objective Rationale

Table provides security problem definition covered by security objectives. Threats and OSPs are addressed by security objectives for the TOE and it's operational environment.
Assumptions are addressed by only security objectives for the operational environment.

Table 2 Security Objective Rationale

	Threats										OSPs						Assumptions						
	T.AccessControl	T.Identification	T.MDData	T.MCharacterizationData	T.Eavesdropping	T.Skimming	T.Counterfeit	T.Malfunction	T.InformationLeakage	T.ChangingTime	P.Certificate	P.Comm	P.SecureEnvironment	P.PhysicalTamper	P.PKI	P.UpdateControl	A.TrustedDesigner	A.TrustedManufacturer	A.Control	A. AuthorizedService	A.Initialisation	A.Activation	A.TrustedUser
O.AccessControl	X					X								X									
O.Event	X	X	X	X			X	X		X			X	X									
O.Integrity			X	X									X	X									
O.Authentication		X				X	X							X	X								
O.Function								X															
O.Transfer			X	X	X	X									X								
OE.Development																	X						
OE.Manufacturing																		X					
OE.Delivery																						X	
OE.KeyGeneration											X										X		
OE.KeyTransportation																					X		
OE.TestEnvironment																	X	X					
OE.StrongAlgorithm									X			X											
OE.UpgradeSoftware																X							

OE.TrustedUser																				X			X
OE.Control																			X				

Justification about Table 2 is given below;

T.AccessControl is addressed by O.AccessControl to control user access to functions and data; O.Event to log uncontrolled accesses.

T.Identification is addressed by O.Authentication to ensure if user identified to the FCR or not; O.Event to log unidentified usage of the FCR.

T.MDData is addressed by O.Integrity to ensure integrity of sales data, event data in fiscal memory, daily memory and ERU; O.Transfer to ensure integrity, confidentiality of sales data, event data during transferring to RAD-IS, O.Event to log unexpected behavior of these memories and unexpected behavior in transferring data.

T.MCharacterizationData is addressed by O.Integrity to ensure integrity of characterization data in memory; O.Transfer to ensure integrity of characterization data during transferring to RAD-IS; O.Event to log unexpected behavior of characterization data storred memory and unexpected behavior in transferring characterization data.

T.Eavesdropping is addressed by O.Transfer to ensure confidentiality of sales data, event data and characterization data during communication with RAD-IS.

T.Skimming is addressed by O.AccessControl to ensure only permitted systems has access to the functions and data; O.Authentication to ensure only permitted users has access to the functions and data; O.Transfer to ensure confidentiality of communication channel.

T.Counterfeit is addressed by O.Authentication to ensure the identity of FCR; O.Event to ensure unchanged in characterization data and sensitive data (private key used for authentication).

T.Malfunction is addressed by O.Function to ensure functions processing accurately ;O.Event to log unexpected behavior of functions.

T.InformationLeakage is addressed by OE.StrongAlgorithm to ensure that cryptographic algorithms have side channel resistances.

T.ChangingTime is addressed by O.Event to log unexpected changes in time information.

P.Certificate is fulfilled by OE.KeyGeneration.

P.Comm is fulfilled by OE.StrongAlgorithm.

P.SecureEnvironment is fulfilled by O.Event and O.Integrity.

P.PhysicalTamper is fulfilled by O.AccessControl, O.Event, O.Integrity and O.Authentication.

P.PKI is fulfilled by O.Transfer and O.Authentication.

P. UpdateControl is upheld by OE.UpgradeSoftware.

A. TrustedDesigner is upheld by OE.Development and OE.TestEnvironment.

A. TrustedManufacturer is upheld by OE.Manufacturing and OE.TestEnvironment.

A.Control is upheld by OE.Control.

A.Initialisation is upheld by OE.KeyGeneration and OE.KeyTransportation.

A.Activation is upheld by OE.Delivery.

A. TrustedUser is upheld by OE.KeyGeneration and OE.TrustedUser.

A.AuthorizedService is upheld by OE.TrustedUser.

5. EXTENDED COMPONENTS DEFINITION

This protection profile does not use any components defined as extensions to CC part 2.

6. SECURITY REQUIREMENTS

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from CC part 2 and the assurance components as defined for the Evaluation Assurance Level 2 from CC part 3.

The following notations are used:

Refinement operation (denoted in such a way that added words are in **bold text** and changed words are ~~**crossed out**~~): is used to add details to a requirement, and thus further restricts a requirement.

Selection operation (denoted by ***italicised bold text*** and placed in square bracket): is used to select one or more options provided by the [CC] in stating a requirement.

Assignment operation (denoted by underlined text and placed in square bracket): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.

Iteration operation are identified with a slash (e.g. "(/)")

6.1 Security Functional Requirements for the TOE

This chapter defines the security functional requirements for the TOE according to the functional requirements components drawn from the CC part 2 version 3.1 revision 4.

6.1.1 Class FAU Security Audit

6.1.1.1 FAU_GEN Security audit data generation

FAU_GEN.1 Audit data generation

Hierarchical to: -

Dependencies: FPT_STM.1 Reliable time stamps.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **[*not specified*]** level of audit; and

c) [the auditable events specified in RAD messaging protocol document [6]].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [none].

6.1.1.2 FAU_SAR Security audit review

FAU_SAR.1 Audit review

Hierarchical to:	-
Dependencies:	FAU_GEN.1 Audit data generation.
FAU_SAR.1.1	The TSF shall provide [Authorized Manufacturer User] with the capability to read [all event data] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.3 FAU_STG Security audit event storage

FAU_STG.1 Protected audit trail storage

Hierarchical to:	-
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to ***[prevent]*** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall ***[overwrite the oldest stored audit records]*** and [none] if the audit trail is full.

6.1.2 Class FCO Communication

6.1.2.1 FCO_NRO Non-repudiation of origin

FCO_NRO.2 Enforced proof of origin

Hierarchical to:	FCO_NRO.1 Selective proof of origin
Dependencies:	FIA_UID.1 Timing of identification
FCO_NRO.2.1	The TSF shall enforce the generation of evidence of origin for transmitted [sales data and event data] at all times.
FCO_NRO.2.2	The TSF shall be able to relate the [originator identity, time of origin] of the originator of the information, and the [body of the message] of the information to which the evidence applies.
FCO_NRO.2.3	The TSF shall provide a capability to verify the evidence of origin of information to [***recipient***] given [immediately].

6.1.3 Class FCS Cryptographic Support

6.1.3.1 FCS_CKM Cryptographic key management

FCS_CKM.1 Cryptographic key generation

Hierarchical to:	-
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment:

	cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following:[assignment: list of standards].

Application note 2 : *For encryption and decryption operations 3DES or AES algorithm is selectable.Generated keys should be minimum 112 bit for 3DES algorithm and minimum 128 bit for AES algorithm. Designer may select one or both of the algorithms. He/she should apply an iteration operation to FCS_CKM.1 when both of the algorithms selected.*

FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].

6.1.3.2 FCS_COP/ ENC - DEC Cryptographic operation

FCS_COP.1 Cryptographic operation

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform [encryption, decryption] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

Application note 3 : *For encryption and decryption operations 3DES or AES algorithm is selectable.Generated keys should be minimum 112 bit for 3DES algorithm and minimum 128 bit for AES algorithm. Designer may select one or both of the algorithms. He/she should apply an iteration operation to FCS_COP.1 when both of the algorithms selected.*

6.1.3.3 FCS_COP/ HASHING Cryptographic operation

FCS_COP.1 Cryptographic operation

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform [hashing] in accordance with a specified cryptographic algorithm [SHA2] and cryptographic key sizes [none] that meet the following: [FIPS PUB 180-2].

6.1.4 Class FDP User Data Protection

6.1.4.1 FDP_ACC Access control policy

FDP_ACC.1 Subset access control

Hierarchical to:	-
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1	The TSF shall enforce the [Administrative Access Control SFP] on [Subjects: FCR Authorised User and Authorized Manufacturer User Objects: Sales and event data, exchange rates,users account attributes, time information. Operations: Secure state mode and maintenance mode actions]

Application note 4 : *FCR Authorised User has access rights to secure state mode and Authorized Manufacturer User has access rights to access maintenance mode.*

Application note 5: *Parameters of new generation cash register fiscal application software functions and exchange rates are specified in RAD messaging protocol document [6].*

6.1.4.2 FDP_ACF Access control functions

FDP_ACF.1 Security attribute based access control	
Hierarchical to:	-
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the [Administrative Access Control SFP] to objects based on the following: [Subjects: FCR Authorised User and Authorized Manufacturer User Subject Attributes:User Identity, Authentication Status, Privileges Objects: Sales and event data, exchange rates ,users account attributes,time information. Object Attributes:Access Control List(secure state mode and maintenance mode access rights). Operations: Secure state mode and maintenance mode actions].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [verify the operator's user identity,authentication status,privileges].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].

6.1.4.3 FDP_ETC Export from the TOE

FDP_ETC.2 Export of user data with security attributes	
Hierarchical to:	-
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1	The TSF shall enforce the [Administrative Access Control SFP and Information Flow Control SFP] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: [none].

Application note 6: *Information Flow Control SFP specified in RAD messaging protocol document [6].*

6.1.4.4 FDP_IFC Information flow control policy

FDP_IFC.1 Subset information flow control

Hierarchical to:	-
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1	The TSF shall enforce the [Information Flow Control SFP] on [subjects (TSM and RAD-IS) and objects (sales data ,event data reports, parameters of new generation cash register fiscal application software functions) as specified in RAD messaging protocol document [6]].

6.1.4.5 FDP_IFF Information flow control functions

FDP_IFF.1 Simple security attributes

Hierarchical to:	-
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1	The TSF shall enforce the [Information Flow Control SFP] based on the following types of subject and information security attributes: [RAD-IS has ability to receive reports related to sales data ,event data reports ; TSM has ability to send parameters of new generation cash register fiscal application software functions to FCR according to technical guidance [5] and RAD messaging protocol document [6]].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [secure communication with SSL CA].
FDP_IFF.1.3	The TSF shall enforce the [none].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [none].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.4.6 FDP_ITC Import from the outside of the TOE

FDP_ITC.2 Import of user data with security attributes

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1	The TSF shall enforce the [Information Flow Control SFP] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data

controlled under the SFP from outside the TOE: [secure communication with SSL CA].

Application note 7: *User data (Parameters of new generation cash register fiscal application software functions) is imported from TSM*

6.1.4.7 FDP_SDI Stored data integrity

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	-
FDP_SDI.2.1	The TSF shall monitor ~~user data~~ **sales data, event data, sensitive data,authentication data, characterization data** stored in containers controlled by the TSF for [integrity errors] ~~on all objects,based on the following attributes: [assignment: user data attributes].~~
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [generate an audit event and transmit it to the RAD-IS according to RAD messaging protocol document [6]].

6.1.5 Class FIA Identification and Authentication

6.1.5.1 FIA_AFL Authentication failures

FIA_AFL.1 Authentication failure handling

Hierarchical to:	-
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when[***TSM configurable positive integer number***]unsuccessful authentication attempts occur related to [FCR Authorised User authentication, Authorized Manufacturer User authentication].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been ***[met],*** the TSF shall [assignment: list of actions].

6.1.5.2 FIA_UAU User authentication

FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.3 FIA_UID User Identification

FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	-
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.6 Class FMT Security Management

6.1.6.1 FMT_MOF Management of security functions behaviour

FMT_MOF.1 Management of security functions behaviour

Hierarchical to:	No other components.

Dependencies:	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to ***[modify the behaviour of]*** the functions [new generation cash register fiscal application software normal operation functions] to ~~[assignment: the authorised identified roles]~~ **nobody**.

Application Note 8 : *No auhtorised user makes the changes on the behaviour of the functions. The TSF itself makes the behavioral changes according to the parameters it receives from TSF.*

Application note 9 : *Ability to Modification of behaviour shall be used according to RAD directives. Normal operation functions includes all FCR parameters that are sent to FCR by TSM.*

6.1.6.2 FMT_MSA Management of security attributes

FMT_MSA.1/USER IDENTITY Management of security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or
	FDP_IFC.1 Subset information flow control]
	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1	The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to ***[modify]*** the security attributes [User Identity] to [FCR Authorised User].

FMT_MSA.1/PRIVILEGES Management of security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or
	FDP_IFC.1 Subset information flow control]
	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1	The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to ***[modify]*** the security attributes [privileges] to [none].

FMT_MSA.3 Static attribute initialisation

Hierarchical to:	-
Dependencies:	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [Administrative Access Control SFP] to provide ***[restrictive]*** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

6.1.6.3 FMT_MTD Management of TSF data

FMT_MTD.1 Management of TSF data

Hierarchical to:	-
Dependencies:	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to ***[modify]*** the [authentication data (user password)] to [FCR Authorised User and Authorized Manufacturer User].

FMT_MTD.2 Management of limits on TSF data

Hierarchical to:	-
Dependencies:	FMT_MTD.1 Management of TSF data FMT_SMR.1 Security roles
FMT_MTD.2.1	The TSF shall restrict the specification of the limits for [authentication data] to [FCR Authorised User,Authorized Manufacturer User].
FMT_MTD.2.2	The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment: actions to be taken].

6.1.6.4 FMT_SMF Specification of Management Functions

FMT_SMF.1 Specification of Management Functions

Hierarchical to:	-
Dependencies:	-
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].

6.1.6.5 FMT_SMR Security management roles

FMT_SMR.2 Restrictions on security roles

Hierarchical to:	FMT_SMR.1 Security roles
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.2.1	The TSF shall maintain the roles:[FCR Authorised User, Authorized Manufacturer User].
FMT_SMR.2.2	The TSF shall be able to associate users with roles.
FMT_SMR.2.3	The TSF shall ensure that the conditions [Authorized Manufacturer User shall take action in maintenance works and FCR authorised user take action in secure state works] are satisfied.

6.1.7 Class FPT Protection of the TSF

6.1.7.1 FPT_FLS Fail secure

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	-
Dependencies:	-
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur:[except maintenance mode events that specified in section 3.1.3]

6.1.7.2 FPT_PHP TSF physical protection

FPT_PHP.2 Notification of physical attack

Hierarchical to:	FPT_PHP.1 Passive detection of physical attack
Dependencies:	FMT_MOF.1 Management of security functions behaviour
FPT_PHP.2.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.2.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3	For [the devices/elements for which active detection is required in technical guidance document[5]], the TSF shall monitor the devices and elements and notify [FCR authorised user] when physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to physical attack

Hierarchical to:	-
Dependencies:	-
FPT_PHP.3.1	The TSF shall resist [physical tampering attacks] to the [private key,session key,authentication data,access control list] by responding automatically such that the SFRs are always enforced.

6.1.7.3 FPT_RCV Trusted recovery

FPT_RCV.1 Manual recovery

Hierarchical to:	-
Dependencies:	AGD_OPE.1 Operational user guidance
FPT_RCV.1.1	After [maintenance mode events which expressed in section 3.1.3 occur] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.4 Function recovery

Hierarchical to:	-
Dependencies:	-
FPT_RCV.4.1	The TSF shall ensure that [except maintenance mode events that specified in section 3.1.3] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

6.1.7.4 FPT_STM Time stamps

FPT_STM.1 Reliable time stamps

Hierarchical to:	-
Dependencies:	-
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

6.1.7.5 FPT_TDC Inter-TSF TSF data consistency

FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to:	-
Dependencies:	-
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret [private key and session key] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use [SSL client authentication] when interpreting the TSF data from another trusted IT product.

6.1.7.6 FPT_TEE Testing of external entities

FPT_TEE.1 Testing of external entities

Hierarchical to:	-
Dependencies:	-
FPT_TEE.1.1	The TSF shall run a suite of tests ***[during initial start-up]*** to check the fulfillment of [proper working of external entities] .

FPT_TEE.1.2	If the test fails, the TSF shall [generate an audit event according to technical guidance [5]]

Application note 10: *External entities are input/output interface,ERU,fiscal memory,daily memory.*

6.1.7.7 FPT_TST TSF self test

FPT_TST.1 TSF testing

Hierarchical to:	-
Dependencies:	-
FPT_TST.1.1	The TSF shall run a suite of self tests ***[during initial start-up]*** to demonstrate the correct operation of ***[the TSF]***.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of ***[TSF data]***.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of ***[TSF]***.

6.1.8 Class FTP Trusted Patch/Channels

6.1.8.1 FTP_ITC Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	-
Dependencies:	-
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit ***[the TSF]*** to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [sending user data(sales and event data) to RAD-IS and receiving user data(parameters of new generation cash register fiscal application software functions and exchange rates) from RAD-IS].

6.2 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE and for its development and operating environment are chosen as the predefined assurance package EAL2.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

Hata! Başvuru kaynağı bulunamadı. provides an overview for security functional requirements coverage and also giving an evidance for sufficiency and necessity of the SFRs chosen.

Table 3 Coverage of security objectives by SFRs for TOE

		O.AccessControl	O.Event	O.Integrity	O.Authentication	O.Function	O.Transfer
FAU_GEN.1	Audit data generation		X				
FAU_SAR.1	Audit review		X				
FAU_STG.1	Protected audit trail storage		X	X			
FAU_STG.4	Prevention of audit data loss		X	X			
FCO_NRO.2	Enforced proof of origin				X		
FCS_CKM.1	Cryptographic key generation						X
FCS_CKM.4	Cryptographic key destruction						X
FCS_COP.1/ ENC - DEC	Cryptographic operation						X
FCS_COP.1/ HASHING	Cryptographic operation						X
FDP_ACC.1	Subset access control	X					
FDP_ACF.1	Security attribute based access control	X					
FDP_ETC.2	Export of user data with security attributes						X
FDP_IFC.1	Subset information flow control					X	
FDP_IFF.1	Simple security attributes	X				X	
FDP_ITC.2	Import of user data without security attributes	X			X		X
FDP_SDI.2	Stored data integrity monitoring and action			X			
FIA_AFL.1	Authentication failure handling	X					

FIA_UAU.2	User authentication before any action	X					
FIA_UID.2	User identification before any action	X					
FMT_MOF.1	Management of security functions behaviour	X				X	
FMT_MSA.1/USER IDENTITIY	Management of security attributes	X				X	
FMT_MSA.1/ PRIVILEGES	Management of security attributes	X				X	
FMT_MSA.3	Static attribute initialisation	X				X	
FMT_MTD.1	Management of TSF data					X	
FMT_MTD.2	Management of limits on TSF data					X	
FMT_SMF.1	Specification of Management Functions	X				X	
FMT_SMR.2	Restrictions on security roles	X					
FPT_FLS.1	Failure with preservation of secure state					X	
FPT_PHP.2	Notification of physical attack		X				
FPT_PHP.3	Resistance to physical attack	X					
FPT_RCV.1	Manual recovery					X	
FPT_RCV.4	Function recovery					X	
FPT_STM.1	Reliable time stamps		X	X		X	
FPT_TDC.1	Inter-TSF basic TSF data consistency				X		X
FPT_TEE.1	Testing of external entities					X	
FPT_TST.1	TSF testing			X		X	
FTP_ITC.1	Inter-TSF trusted channel						X

A detailed justification of required for suitability of the security functional requirements to achieve the security objectives is given in **Hata! Başvuru kaynağı bulunamadı.**.

Table 4 Suitability of the SFRs

Security Objective	**Security Functional Requirement**	
O.AccessControl	FDP_ACC.1	Provides security functional policy for functions and data
	FDP_ACF.1	Defines security attributes for functions and data
	FDP_IFF.1	Provides information flow control policy for data
	FDP_ITC.2	Provides import of new genartion cash register fiscal application software and configuration parameters from outside of the TOE using Information Flow Control SFP
	FIA_AFL.1	Detects and records authentication failure events
	FIA_UAU.2	Defines user authentication before any action
	FIA_UID.2	No allowed actions before identification
	FMT_MOF.1	Restricts the ability to enable the functions to nobody and, thus, prevents an unintended access to data in the operational phase.
	FMT_MSA.1/USER IDENTITIY	Provides the functions to restrict the ability to modify the security attributes to FCR Authorised User
	FMT_MSA.1/ PRIVILEGES	Provides the functions to restrict the ability to modify the security attributes to nobody
	FMT_MSA.3	Provides the functions to provide restrictive default values for security attributes that are used to enforce the SFP and allows FCR Authorised User to specify alternative initial values to override the default values when an object or information is created.
	FMT_SMF.1	Performing all operations being allowed only in the maintenance mode
	FMT_SMR.2	Maintains the roles with restrictions
	FPT_PHP.3	Ensures resistance to physical attack to the TOE software, sales data and event data

O.Event	FAU_GEN.1	Generates correct audit events
	FAU_SAR.1	Allows users to read audit records
	FAU_STG.1	Protects stored audit data from unauthorised deletion
	FAU_STG.4	Prevents loss of audit data loss (overwrite the oldest audit data)
	FPT_PHP.2	Generation of audit event detection of physical tamparing
	FPT_STM.1	Provides accurate time for logging events
O.Integrity	FAU_STG.1	Protects stored audit data integrity from unauthorised deletion
	FAU_STG.4	Prevents loss of audit data loss
	FDP_SDI.2	Monitors user data stored for integrity errors
	FPT_STM.1	Provides accurate time for integrity check
	FPT_TST.1	Detects integrity failures for stored source code, sales data and event data
O.Authentication	FCO_NRO.2	Generates evidence of origin of the data to be transferred to the RAD-IS
	FDP_ITC.2	Provides import of new genartion cash register fiscal application software and configuration parameters from outside of the TOE using the SFP
	FPT_TDC.1	Provides the capability to consistently interpret TSF data(private key and session key)
O.Function	FDP_IFC.1	Provides information flow control for sales data and event data
	FDP_IFF.1	Provides rules of information flow control for sales data and event data
	FMT_MOF.1	Restricts the ability to enable the functions to nobody and, thus, prevents an unintended access to data in the operational phase.
	FMT_MSA.1/USER IDENTITIY	Provides the functions to restrict the ability to modify the security attributes to nobody
	FMT_MSA.1/ PRIVILEGES	Provides the functions to restrict the ability to modify the security attributes to nobody

	FMT_MSA.3	Provides the functions to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	FMT_MTD.1	Provides authorised processing of sales data and event data
	FMT_MTD.2	Provides assignment for try number of authentication
	FMT_SMF.1	Performing all operations being allowed only in the maintenance mode
	FPT_FLS.1	Failure types which makes new generation cash register fiscal application software continue working in secure state
	FPT_RCV.1	Provides new generation cash register fiscal application software start working in maintenance mode in failure. (has ability to switch to the secure state manually)
	FPT_RCV.4	Provides new generation cash register fiscal application software start working in maintenance mode in failure. (has ability to switch to the secure state automatically with functions)
	FPT_STM.1	Provides accurate time for functionalities
	FPT_TEE.1	Provides tests for IT environment for functioning accurately
	FPT_TST.1	Ensures accuracy of its functions working by conducting self test
O.Transfer	FCS_CKM.1	Generates session keys for communication between RAD-IS and new generation cash register fiscal application software, and for communication between TSM and new generation cash register fiscal application software
	FCS_CKM.4	Destroys cryptographic keys in the TOE
	FCS_COP.1/ ENC - DEC	Provides the encryption and decryption operations for secure communication between RAD-IS and new generation cash register fiscal application software, and between TSM and new generation cash register fiscal application software

	FCS_COP.1/ HASHING	Provides the hashing operations for intergrity check in the Fiscal Cash Register
	FDP_ETC.2	Provides export of sale's data and event data from the TOE to the RAD-IS using the SFP
	FDP_ITC.2	Provides protection of sale's data and event data confidentiality during communication with RAD-IS
	FPT_TDC.1	Provides interpretation of private key and session key during communication with RAD-IS and TSM.
	FTP_ITC.1	Provide a communication channel to the RAD-IS.

6.3.2 Rationale for Security Functional Requirements dependencies

Selected security functional requirements include related dependencies. **Hata! Başvuru kaynağı bulunamadı.** below provides a summary of the security functional requirements dependency analysis.

Table 5 Security Functional Requirements dependencies

Component	Dependencies	Included / not included
FAU_GEN.1	FPT_STM.1	included
FAU_SAR.1	FAU_GEN.1	included
FAU_STG.1	FAU_GEN.1	included
FAU_STG.4	FAU_STG.1	included
FCO_NRO.2	FIA_UID.1	included
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 ; FCS_CKM.4	FCS_COP.1 and FCS_CKM.4 included
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FDP_ITC.1 and FCS_CKM.1 included
FCS_COP.1/ ENC - DEC	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ; FCS_CKM.4	FDP_ITC.1, FCS_CKM.1 and FCS_CKM.4 included
FCS_COP.1/HASHING	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ; FCS_CKM.4	FDP_ITC.1, FCS_CKM.1 and FCS_CKM.4 included
FDP_ACC.1	FDP_ACF.1	included
FDP_ACF.1	FDP_ACC.1; FMT_MSA.3	included
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	included
FDP_IFC.1	FDP_IFF.1	included
FDP_IFF.1	FDP_IFC.1; FMT_MSA.3	included
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1 ; FMT_MSA.3	included

FDP_SDI.2	No dependencies	-
FIA_AFL.1	FIA_UAU.1	included
FIA_UAU.2	FIA_UID.1	FIA.UID.2 is hierarchical to FIA.UID.1
FIA.UID.2	No dependencies	-
FMT_MOF.1	FMT_SMR.1; FMT_SMF.1	included
FMT_MSA.1/ USER IDENTITIY	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	included
FMT_MSA.1/ PRIVILEGES	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	included
FMT_MSA.3	FMT_MSA.1; FMT_SMR.1	included
FMT_MTD.1	FMT_SMR.1; FMT_SMF.1	included
FMT_MTD.2	FMT_MTD.1; FMT_SMR.1	FMT_MTD.1 included, FMT_SMR.2 is hierarchical to FMT_SMR.1
FMT_SMF.1	No dependencies	-
FMT_SMR.2	FIA_UID.1	included
FPT_FLS.1	No dependencies	-
FPT_PHP.2	FMT_MOF.1	included
FPT_PHP.3	No dependencies	-
FPT_RCV.1	AGD_OPE.1	included (assurance component)
FPT_RCV.4	No dependencies	-
FPT_STM.1	No dependencies	-
FPT_TDC.1	No dependencies	-
FPT_TEE.1	No dependencies	-
FPT_TST.1	No dependencies	-
FTP_ITC.1	No dependencies	-

6.3.3 Security Assurance Requirements Rationale

The current assurance package was chosen based on the pre-defined assurance packet EAL2. EAL2 is chosen because the threats that were chosen are consistent with an attacker of basic attack potential.

6.3.4 Security Requirements - Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together forms an internally consistent whole.

The dependency analysis in **Hata! Başvuru kaynağı bulunamadı.** shows that the basis for internal consistency between all defined functional requirements is satisfied.

The assurance package EAL2 is a pre-defined set of internally consistent assurance requirements. The assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met. So, there are no inconsistencies between the goals of these two groups of security requirements.

7. ACRONYMS

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
FCRAS	: Fiscal Cash Register Application Software
GPRS	: General Packet Radio Service
GPS	: Global Positioning System
IT	: Information Technology
ITU	: International Telecomunication 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 Sockets Layer - Client Authentication
TOE	: Target of Evaluation
TSF	: TOE Security Functionality (defined in CC)
TSE	: Turkish Standards Institute
TSM	: Trusted Service Manager
VAT	: Value Added Tax

8. BIBLIOGRAPHY

Common Criteria

[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, Version 3.1, Revision 4, September 2012

New Generation Cash Register Directives

[5] Technical Guidance , version 2.0 , March 2012

[6] RAD Messaging protocol , version 2.02 , April 2012