CHANGE v 01.00

SECURITY TARGET LITE

Version 1.0

April 13th 2015

Table of Contents

Version History

Version No	Reason for Change	Release Date
1.0	First Release	13/04/2015

Approvals

Name	Role
Mehmet Çakır	ST Author (BEAM Teknoloji)
Emre Çakır	ST Author (BEAM Teknoloji)
Selçuk Doğu	ST Author (EDATA Elektronik)

1. ST INTRODUCTION

This section presents the following information:

- Identifies the Security Target (ST) and Target of Evaluation (TOE);
- Specifies the ST conventions,
- Defines the terminology and acronyms used in the ST,
- Defines TOE overview and TOE description.

1.1. ST Reference and TOE Reference

ST Title:	CHANGE v 01.00 Security Target Lite v 1.0
ST Version:	v 1.0
TOE Identification:	CHANGE v 01.00
CC Identification:	Common Criteria for Information Technology Security Evaluations, version 3.1R4
Keywords:	Revenue Administration, Fiscal Application Software, New Generation Cash Register, EMV, EFT-POS, PRA, Electronic Registration Unit.

ST and TOE References

1.2. Document Conventions, Terminology & Acronyms

This section specifies the formatting information used in the ST.

1.2.1. Conventions

In this Security Target some notations and conventions which are taken from the Common Criteria v3.1R4 have been used in order to guide to the reader.

During the specification of the functional requirements under the Section 4, the functional components are interpreted according to the “assignment” and “selection” operations.

The outcome of the assignment operations are shown with <u>underlined</u> identified between “[<u>brackets</u>]”.

The outcome of the selection operations are shown with **bold** and **italic** and identified between “***[brackets]***”.

Iterated functional requirement components are shown with a “**/IDENTIFIER”** for the components which used more than once with varying operations.

Refinement operations are used in the ST. Removed parts of the requirements shown with ~~strikethrough.~~

Under the term “**Application Note**”, an informal explanation added under some of the functional requirements in order to highlight or to describe the component in detail.

1.2.2. Terminology

The following terminology is used in this Security Target:

MPU	: Microprocessor Unit

1.2.3. 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
GPRS	: General Packet Radio Service
IT	: Information Technology
ITU	: International Telecomunication Union
OSP	: Organisational 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
SFP	: Security Function Policy
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	: Türk Standartları Enstitüsü
TSM	: Trusted Service Manager
VAT	: Value Added Tax

1.3. TOE Overview

The TOE addressed by this Security Target (ST) is an application software which is the main items 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 as described in section 1.3.2 for full functionality. TOE and related components are given in Figure 1. Usage and major security features of TOE are described in section 1.3.3.

1.3.1. General overview of the TOE and related components

Figure 1 shows the general overview of the TOE and its related components as regarded in this ST. 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 non-TOE environments which are crucial parts of the FCR for functionality and security. Connections between the TOE and its environment are also subject to evaluation since since these connections are made over the interfaces of the TOE.

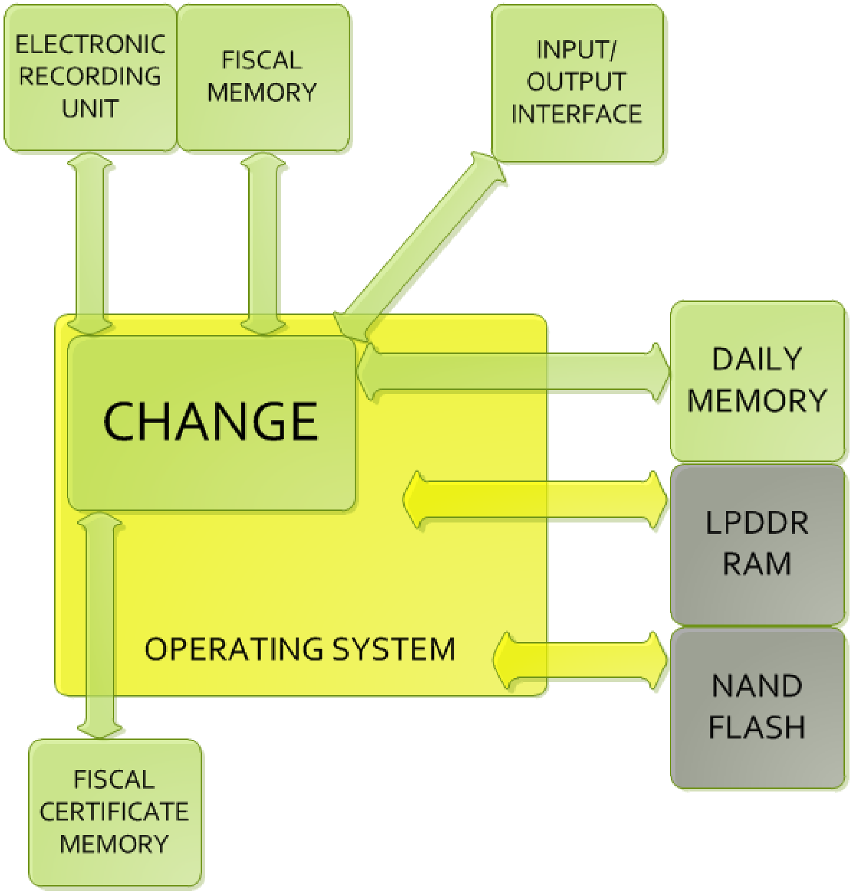

Figure 1 TOE(CHANGE v 01.00) and Related Components

CHANGE Software is released with an FCR device and the certified version of the TOE can be used with different FCR brands and models.

1.3.2. Required Non-TOE Hardware/Software

Software and hardware environment of the TOE are described below.

1.3.2.1. Software Environment of TOE

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

Table 1 Typical Software Environment of the TOE

File System and Software Libraries
Operating System Kernel

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

- Application runs on Linux **operating system** which supports following features
    - at least 32 bit data processing capacity
    - multi-processing
    - IPv4 and IPv6 support
    - NTP (Network Time Protocol)

Linux is a monolithic kernel. Linux supports true preemptive multitasking (both in user mode and kernel mode), virtual memory, shared libraries, demand loading, shared copy-on-write executables (via KSM), memory management, Internet Protocol Suite and threading.

A cryptographic API is provided for use by kernel subsystems. It provides support for a wide range of cryptographic algorithms and operating modes, including commonly deployed ciphers, hash functions, and limited support for asymmetric cryptography. There are synchronous and asynchronous interfaces, supporting cryptographic hardware, which offloads processing from general CPUs.

- As a database, in our system a relational database is used.It 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

Database system features:

- Even after power outages and system crashes, operations are processing as atomic (Atomic), consistent (consistent), isolated (Isolated) and durable (Durable) (ACID).
- No configuration or installation it does not need to configuration or authorization.
- It is stored in a database at Single Class-platform disk file.
- Supports terabyte-sized databases and gigabyte-sized strings and blobs. (refer to limits.html)
- Written in ANSI-C.TCL connections are added.

- Source codes are explained very good to meet all steps of test items.
- It can be used as a single ANSI-C source code file which is easily transferred to another project.
- There is no any external dependency.

1.3.2.2. Hardware Environment of TOE

In addition to TOE, following hardware components are also 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 has to be fixed within FCR in a way that it cannot be removed without damaging the chassis.

  d) Fiscal memory is protected by mesh cover,

  e) Fiscal memory has the ability to be protected against magnetic and electronic threats,

  When the connection between fiscal memory and main processor is broken, FCR enters in maintenance mode,

  f) The data stored in the fiscal memory is not 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 where 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 and identification number of the device,

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

Fiscal memory data retention is guaranteed to be more than 20 years.

Because of the mesh protection fiscal memory can not be accessed directly and also cannot be erased or modified.

- **Daily memory has following features;**

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

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 current day are produced by using the data in the daily memory.

v. Following values 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

Daily memory uses dedicated SRAM memory.

- 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 and secure communication with PRA-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 PRA-IS and TSM.

- **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.

  iii. Data stored in ERU cannot be modified

  iv. ERU also supports features specified in "Fiscal Cash Register General Communique Serial Number: 67, Part A” which is about Law No:3100 except item (ii) above.

The ERU uses flash memory with sufficient size to supply the requirements.

- FCR devices either with one or more of the following interfaces; an internal ETHERNET, PSTN or mobile communication technology (GPRS etc.)

FCR supports one or more of the physical communication interfaces.

- Incoming and outgoing data traffic for FCR passes over a **firewall**.

IP firewall runs on FCR that ignores all unwanted incoming traffic and allows only FCR initiated connections. Linux Iptables is used as firewall.

- FCR has a printer to print sales receipt.

FCR uses 2” thermal printer with minimum 56mm paper width.

- FCR supports the use of EFTPOS.

- FCR needs some input/output devices for functionalities listed below;

  i. FCR has keyboard unit.

  ii. FCR has separate displays for cashier and buyer.

  iii. FCR has internal battery to keep time information.

1.3.3. Major security and functional features

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

1.3.3.1. 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 stores sales data in fiscal memory.
ii. TOE stores total receipt and total VAT amount for each receipt in daily memory.
iii. TOE is able to generate reports (X report, Z report etc.).
iv. TOE is able to transmit Z reports, receipt information, sale statistics and other information determined by PRA to PRA-IS in PRA Messaging Protocol format.
v. TOE is able to start the communication with PRA-IS and instantly respond to requests originated from PRA-IS.
vi. TOE stores records of important events as stated in PRA Messaging Protocol Document [6] and transmits to PRA-IS in PRA Messaging Protocol format in a secure way.
vii. TOE is able to be used by users in secure state mode or maintenance mode. Roles and modes of operation are described in 3.1.2 and 3.1.3 respectively.

1.3.3.2. TOE major security features

The TOE provides following security features;

i. TOE supports access control.
ii. 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.
iii. TOE supports usage of ITU X509 v3 formatted certificate and its protected private key for authentication and secure communication with PRA- IS and TSM.
iv. TOE supports secure communication between FCR-PRA-IS and FCR–TSM.
v. TOE ensures the integrity of event data, sales data, authentication data, characterization data and FCR parameters.
vi. TOE records important events defined in PRA Messaging Protocol Document [6] and send urgent event data immediately to PRA-IS in a secure way.

vii. TOE detects physical attacks to FCR and enters into the maintenance mode in such cases.

1.3.4. TOE Type

TOE is a software application embedded within FCR.

1.4. TOE Description

1.4.1. Physical Scope

TOE is the fiscal application software which runs on Linux operating system. A secure microcontroller is used in the system. Main MPU has the following features:

- 32 bit
- Supports mesh protection
- Secure memory area for key storage
- Temperature, voltage, die shield sensor

Flash memory is used to store the operating system, TOE and the user data. DDR RAM is used as operating memory.

For daily memory, a dedicated SRAM memory is used.

Flash memories are used for fiscal memory and ERU.

FCR has matrix keyboard to manage keyboard operations.

FCR has 2 displays, namely clerk and customer displays.

For long time work, FCR uses li-ion battery.

In order to keep the time information active, Lithium coin battery is used.

FCR supports use of USB ports.

FCR supports ethernet communication.

FCR supports GPRS communication.

FCR supports serial communication for EFT-POS, serial barcode and scale.

1.4.2. Logical Scope

The logical scope of the TOE consists of the security functional features of the fiscal application software which is subject to a common criteria evaluation. The following security functions are in the logical scope of TOE;

- Audit/Event Log: The function which generates and stored the events data according to the PRA Messaging Protocol and the SFRs stated in this Security Target.
- Cryptography: The Cryptographic Libraries which are used by TSF for cryptographic operations like encrypting and decrypting of imported and exported data.This function also covers the key generation and destruction.
- Identification and Authentication: TOE has varios user roles and access rights during normal operation and an identification and authentication function controls the user identification and authentication securely. This function also covers the usage of SSL CA to communicate securely with TSM and PRA-IS.
- Access Control: The access rights in the TOE are controlled with an access control policy which is enforced during authentication of FCR User, FCR Authorized User and Authorized Manufacturer User.
- Data Integrity: TOE protects the integrity of stored and exported data with the support of a TSF.
- Import/Export: Data import and export are handled securely with an enforced policy with the control of a TSF.
- TSF Protection: TSF protects the secure operation and in any case of defined corruptions TOE switches to maintenance mode to continue protecting its core functionality.
- Data Preparation: The data integrity and reliability of transmitted data is provided via a data preparation method which is enforced by TSF.
- TOE Self Testing: TOE conducts self testing of its functionality during initial startup.
- Security Management: TSF provides the security functions and restrict the access to these functions with specific capabilities defined in this security target.

2. CONFORMANCE CLAIM

2.1. CC Conformance Claim

This Security Target 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,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1, Revision 4, September 2012,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1, Revision 4, September 2012,

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

has to be taken into account.

2.2. PP and Package Claim

2.2.1. Protection Profile (PP) Claim

This Security Target claims conformance to New Generation Fiscal Application Software Protection Profile TSE-3C1S/PP-006.

2.2.2. Package Claim

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

- Assurance package EAL2 conformant to CC, part 3.

2.3. Conformance Claim Rationale

The type of TOE defined in this ST is consistent with the TOE type defined in the PP which is claimed in the section 2.2.1.

The security problem definition defined in this ST is equivalent with the security problem definition in the PP which the TOE claims conformance.

TOE includes all the security objectives defined in the PP which the TOE claims conformance.

TOE demonstably meets and exceeds all the requirements defined in the PP which the TOE claims conformance.

3. SECURITY PROBLEM DEFINITION

3.1. TOE Security Policy

3.1.1. External Entities

PRA-IS

PRA-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 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.

PRA On-site Auditor

PRA On-site Auditor is an employee of PRA 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 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.

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, information). List of events can be found in PRA 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.

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 [7].

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 User (Cashier):

FCR User is the user who uses the sales functionality of FCR by using his/her identity

FCR Authorised User

FCR Authorised User is the user who uses the functions of FCR and operates FCR by using authentication mechanism.

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 User;
  - ✓ to do fiscal sales
- ❖ FCR Authorised User;
  - ✓ to configure FCR,
  - ✓ to take fiscal and FCR reports

Maintenance Mode: Maintenance Mode is the mode that allow only Authorized Manufacturer User to fix FCR in case of any technical problem; to change time information and 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 unauthorized persons and
- A technical problem is determined by FCR Manufacturer.

3.1.4. Assets

Sensitive data

Sensitive data is used for secure communication with PRA-IS and TSM. Confidentiality and integrity of this asset needs to be protected.

Application Note 1: *Sensitive data may consist of symmetric keys.*

Event data

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

Sales data

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

Characterization data (Identification data for devices)

Characterization data is a unique number assigned to each FCR 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.

Authentication data

Authentication data contains authentication information which is required for FCR Authorised User and Authorized Manufacturer User to gain access to FCR functionalities. Both integrity and confidentiality of this asset have to be protected.

Time Information

Time information is stored in FCR and synchronized with PRA-IS. Time information is important when logging important events and sending reports to the PRA-IS. The integrity of this asset is to be protected.

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

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

Threat agent: An attacker who has basic attack potential and 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, 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 unauthorized access to the FCR; failure reports and deletion of logs. An attacker also could try to disclose important events while transmitted between PRA-IS and FCR.
- An attacker could try to manipulate or delete the sales data generated by TOE which may result in tax fraud. In addition, an attacker also could try to disclose sales data while transmitted between PRA-IS and FCR. Manipulation and deletion of sales data 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, physical and logical access to the FCR.

Asset: Event data, sales data, characterization data, FCR parameters

T.Eavesdropping - 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.Skimming - Skimming the event data, sales data and characterization data

Adverse action: An attacker could try to imitate PRA-IS to receive information from FCR and to imitate TSM to set parameters to FCR via the communication channel.

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

Asset : Sales data, and event data, FCR parameters

T.Counterfeit - FCR counterfeiting

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

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

Asset : Sensitive data(session keys)

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

3.3. OSP

This section describes organizational security policies that must be satisfied.

P.Certificate

It has to be assured that certificates which are installed at initialization step, are compatible with ITU X.509 v3 format. FCR contains FCR certificate, Certification Authority root certificate, Certification Authority sub-root (subordinate) certificate and UpdateControl certificate. UpdateControl certificate is used to verify the signature of the TOE.

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 [7].

P.InformationLeakage - Information leakage from FCR

It has to be assured that TOE's environment provides a secure mechanism which prevents attacker to obtain sensitive information (secret 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).

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, signing and key aggreement.

P.Update Control

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.

3.4. Assumptions

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

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.AuthorizedService

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

A.Ext_Key

It is assumed that External Device (EFT-POS) generates strong key for communicating with TOE.

4. SECURITY OBJECTIVES

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

4.1. Security Objectives for the TOE

This part describes security objectives provided by the TOE.

O.AccessControl

TOE must control authenticated user’s access to functions and data by using authorization mechanism.

O.Event

TOE must record important events stated as in PRA Messaging Protocol Document[6].

O.Integrity

TOE must provide integrity for sales data, event data, characterization data, authentication data, sensitive data(session keys) and FCR parameters.

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.

TOE must ensure that time information is accurate by doing anomaly detection.

TOE must enter a maintenance mode when maintenance mode events occur in section 3.1.3.

O.Transfer

TOE must provide confidentiality, integrity and authenticity for sales data, event data, characterization data transferred to the PRA-IS and FCR parameters transferred from TSM.TOE also provides integrity for sales data and event data transferred from memories to other memories. TOE must provide confidentiality, integrity and authenticity for information send/received during external device communication.

4.2. Security Objectives for the Operational Environment

This part describes security objectives provided by the operational environment

OE.External Device

External Device should generate strong key for communicating with TOE.

OE.Manufacturing

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

OE.Delivery

Authorized Manufacturer User must ensure that delivery and activation of the TOE done by a secure way.

OE.KeyGeneration

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

OE.SecureStorage

Asymmetric private key shall be stored within smartcard or Secure-IC’s.

Keys (asymmetric key, symmetric key), certificates, event data, characterization data and sales data shall be stored within secure environment protected by electronic seal.

OE.KeyTransportation

Transportation and installation of asymmetric private key and certificates to the FCR must be done by protecting its confidentiality and integrity.

OE.TestEnvironment

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

OE.StrongAlgorithm

Environment of TOE shall use asymmetric private keys for signature operation by using libraries of smartcard and Secure-IC’s. These libraries used in FCR shall be strong. They should also have protection against side channel analysis (SPA, DPA, SEMA, DEMA, and DFA).

OE.UpgradeSoftware

FCR software updates should be get passed verdict from Common Criteria maintenance or reevaluation procedures (according to update type) before installed to the FCR. This will be validated by the FCR, using the cryptographic signature control methods.

OE.TrustedUser

Users shall act responsibly.

OE.Control

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

OE.SecureEnvironment

Fiscal memory shall not accept transactions with negative amounts which results in a decrease of total tax value.

Tampering protection system shall protect fiscal memory with mesh cover.

Environment of TOE provides secure initialization steps. Initialization step is consist of secure boot of operating system, and integrity check for TSF data.

4.3. Security Objective Rationale

Table-2 provides security problem definition covered by security objectives. Threats and OSPs are addressed by security objectives of the TOE and it's environment. Assumptions are addressed by only security objectives of the operational environment.

Table 2 Security Objectives Rationale

	Threats								OSPs								Assumptions					
	T.AccessControl	T. Authentication.	T.MDData	T.Eavesdropping	T.Skimming	T.Counterfeit	T.Malfunction	T.ChangingTime	P.Certificate	P.SecureEnvironment	P.PhysicalTamper	P.PKI	P.InformationLeakage	P.Comm_EXT	P.UpdateControl	A.Ext_Key	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	X											
O.Authentication	X	X			X										X							
O.Function							X	X		X												
O.Transfer			X	X										X								
OE.External Device																X						
OE.Manufacturing																	X					
OE.Delivery												X									X	
OE.KeyGeneration									X											X		
OE.SecureStorage											X											
OE.KeyTransportation												X								X		
OE.TestEnvironment																	X					
OE.StrongAlgorithm													X									

OE.UpgradeSoftware															X							
OE.TrustedUser																			X			X
OE.Control																		X				
OE.SecureEnvironme			X	X		X				X	X									X		

Justification about Table 2 is given below;

T.AccessControl is addressed by O.AccessControl to control user access to functions and data; O.Authentication to provide authentication mechanism for users; O.Event to log all access attempts.

T.Authentication is addressed by O.Authentication to ensure that if user is authenticated to the FCR; O.Event to log successful/unsuccessful authentication attempts.

T.MDData is addressed by O.Integrity to ensure integrity of sales data, event data, characterization data and FCR parameters in FCR with logical and physical security features; O.Transfer to ensure integrity, confidentiality and authenticity of sales data, event data and characterization data during transferring to PRA-IS and parameters during transfering from TSM to FCR ; O.Event to log unexpected behavior of these memories and unexpected behavior in transferring data; OE.SecureEnvironment to provide electronic seal.

T.Eavesdropping is addressed by O.Transfer to ensure confidentiality of sales data, event data and characterization data during communication with PRA-IS; O.Integrity to ensure the integrity of event data, sales data and characterization data; O.Event to log physical tamper; by OE.SecureEnvironment to provide electronic seal.

T.Skimming is addressed by O.Authentication to establish communication only with permitted systems.

T.Counterfeit is addressed by O.Integrity to ensure the integrity of sensitive data (session keys); O.Event to log physical tamper; OE.SecureEnvironment to provide electronic seal.

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

T.ChangingTime is addressed by O.Event to log unexpected changes in time information; by O.Access Control to control user access to time information; by O.Function to ensure accuracy of time information.

P.Certificate is fulfilled by OE.KeyGeneration.

P.SecureEnvironment is fulfilled by OE.SecureEnvironment, O.Event, O.Integrity and O.Function.

P.PhysicalTamper is fulfilled by OE.SecureEnvironment, O.AccessControl, O.Event, O.Integrity and OE.SecureStorage

P.PKI is fulfilled by OE.Delivery and OE.KeyTransportation

P.InformationLeakage is fulfilled by OE.StrongAlgorithm to ensure that cryptographic algorithms used by FCR have side channel protection.

P.Comm_EXT is fulfilled by O.Transfer.

P. UpdateControl is upheld by OE.UpgradeSoftware and O.Authentication.

A.Ext_Key is upheld OE.External Device.

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

A.Control is upheld by OE.Control.

A. AuthorisedService is upheld by OE.TrustedUser.

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

A.Activation is upheld by OE.Delivery.

A. TrustedUser is upheld by OE.TrustedUser.

5. EXTENDED COMPONENT DEFINITION

This Security Target does not use any components defined as extensions to CC part 2.

6. SECURITY REQUIREMENTS

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 3.

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: No other components.

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 PRA 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: No other components.

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: No other components.

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/TLS_AES Cryptographic key generation

Hierarchical to: No other components.

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 [PRF] and specified cryptographic key sizes [AES:128 bit and AES:256 bit] that meet the following: [RFC 5246].

FCS_CKM.1/TLS_HMAC Cryptographic key generation

Hierarchical to: No other components.

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 [PRF] and specified cryptographic key sizes [128 bit and 256 bit] that meet the following: [RFC 5246].

FCS_CKM.1/DHE-KEY Cryptographic key generation

Hierarchical to: No other components.

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 [RNG] and specified cryptographic key sizes [2048 bits] that meet the following: [none].

FCS_CKM.1/EXT-DEV KHMAC Cryptographic key generation

Hierarchical to: No other components.

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 [PRF] and specified cryptographic key sizes [256 bits] that meet the following: [RFC 5246].

FCS_CKM.1/EXT-DEV KENC Cryptographic key generation

Hierarchical to: No other components.

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 [PRF] and specified cryptographic key sizes [AES: 256 bits] that meet the following: [RFC 5246].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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 [assigning 0 to the area that stores the key] that meets the following: [none].

6.1.3.2. FCS_COP Cryptographic operation

FCS_COP.1/ENC-DEC Cryptographic operation

Hierarchical to: No other components.

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 and decryption] in accordance with a specified cryptographic algorithm [AES in CBC mode] and cryptographic key sizes [AES:128 bits and AES:256 bits] that meet the following: [RFC 3602].

FCS_COP.1/INT-AUTH Cryptographic operation

Hierarchical to: No other components.

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 [authentication and integrity protection] in accordance with a specified cryptographic algorithm [HMAC-SHA256] and cryptographic key sizes [256 bits] that meet the following: [FIPS 198-1 and NIST FIPS PUB 180-2].].

FCS_COP.1/HASHING Cryptographic operation

Hierarchical to: No other components.

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: [NIST FIPS PUB 180-2].

FCS_COP.1/EXT-DEV KEYEXCHANGE Cryptographic operation

Hierarchical to: No other components.

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 [key agreement] in accordance with a specified cryptographic algorithm [DHE] and cryptographic key sizes [2048 bits] that meet the following: [NIST SP 800-56A].

FCS_COP.1/EXT-DEV KENC Cryptographic operation

Hierarchical to: No other components.

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 [AES with CBC] and cryptographic key sizes [256 bits] that meet the following: [NIST SP800-38A(CBC.AES256)].

FCS_COP.1/EXT-DEV KHMAC Cryptographic operation

Hierarchical to: No other components.

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 and decryption for integrity protection] in accordance with a specified cryptographic algorithm [HMAC-SHA256] and cryptographic key sizes [256 bits] that meet the following: [FIPS 198-1 and NIST 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: No other components.

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, time information

Operations: Secure state mode and maintenance mode actions],

[Subjects:FCR User(Cashier),

Objects: Sales data,

Operations: Secure state mode actions].

Application Note 2: FCR User(Cashier) and FCR Authorised User have access rights to secure state mode and Authorized Manufacturer User has access rights to access maintenance mode.

Application Note 3: Parameters of new generation cash register fiscal application software functions and exchange rates are specified in PRA Messaging Protocol Document [6].

6.1.4.2. FDP_ACF Access control functions

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

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,Privileges

Objects: Sales and event data, exchange rates, time information

Object Attributes: Access Control List (Secure State Mode and maintenance mode access rights)

Operations: Secure State Mode and Maintenance Mode actions describe in 3.1.3],

[Subjects: FCR User(Cashier

Objects: Sales data

Object Attributes: Access Control List (Secure State Mode Access Rights),

Operations: Secure State Mode describe in 3.1.3]

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 and 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/TSM Export of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1 The TSF shall enforce the [Information Flow Control SFP with TSM and PRA-IS] 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: [secure communication with SSL CA].

FDP_ETC.2 /EFTPOS Export of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1 The TSF shall enforce the [Information Flow Control SFP with EFT-POS Device] 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: [Communication with secure messaging according to External Device Communication Protocol Document [7]].

6.1.4.4. FDP_IFC Information flow control policy

FDP_IFC.1/TSMCOMMUNICATION Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [Information Flow Control SFP with TSM and PRA-IS] on [subjects (TSM and PRA-IS) and objects (sale's data, event data reports, FCR parameters) as specified in PRA Messaging Protocol Document [6]].

FDP_IFC.1/EFTPOSCOMMUNICATION Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [Information Flow Control SFP with EFT-POS Device] on [subjects (EFT-POS) and objects (amount information in sale's data) as specified in External Device Communication Protocol Document [7]].

6.1.4.5. FDP_IFF Information flow control functions

FDP_IFF.1/TSMCOMMUNICATION Simple security attributes

Hierarchical to: No other components.

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 with TSM and PRA-IS] based on the following types of subject and information security attributes: [TOE has ability to send reports related to sales data and event data reports to PRA-IS by using subject identifier(IP/Port information) and object identifier (file name); TOE has ability to receive FCR parameters from TSM by using subject identifier (IP/Port information) and object identifier (information label) according to PRA 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].

FDP_IFF.1/EFT-POSCOMMUNICATION Simple security attributes

Hierarchical to: No other components.

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 with EFT-POS Device] based on the following types of subject and information security attributes: [TOE has ability to send amount information to EFT-POS Device by using subject identifier(EFT-POS label and source port),

TOE has ability to receive outcome of the operation conducted by the EFT-POS Device by using subject identifier(source port)]

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: [Communication with secure messaging according to External Device Communication Protocol Document [7]].

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/TSM Import of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSD 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 with TSM and PRA-IS] 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 4: User data (FCR parameters) is imported from TSM.

FDP_ITC.2/EFTPOS Import of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSD 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 with EFT-POS Device] 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

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: [Communication with secure messaging according to External Device Communication Protocol Document [7]].

6.1.4.7. FDP_SDI Stored data integrity

FDP_SDI.2/MEMORY Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor ~~user data~~ **sales data stored in fiscal memory and ERU; event data, authentication data and 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 PRA-IS according to PRA Messaging Protocol Document [6] and then enter into the maintenance mode].

FDP_SDI.2/DAILY and PRMTR Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor ~~user data~~ **sales data** stored in ~~containers~~ **daily memory and FCR parameters 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 PRA-IS according to PRA Messaging Protocol Document [6] and and print Z report automatically].

6.1.5. Class FIA Identification and Authentication

6.1.5.1. FIA_AFL Authentication failures

FIA_AFL.1/MANUFACTURER Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when ***[5]*** unsuccessful authentication attempts occur related to [Authorized Manufacturer User authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[met]***, the TSF shall [lock Authorized Manufacturer User Account for 3 hours].

FIA_AFL.1/AUTHORISED Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when ***[5]*** unsuccessful authentication attempts occur related to [FCR Authorised User].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[met]***, the TSF shall [lock FCR Authorised User Account for 3 hours].

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.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

[the authentication mechanism employed to authenticate Authorized Manufacturer 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: No 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 5: No authorised user makes the changes on the behaviour of the functions. The TSF itself makes the behavioral changes according to the FCR parameters received from TSM.

Application Note 6: Ability to modify the behaviour shall be used according to PRA 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.1/FILE NAME and INFO-LABEL 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 [Information Flow Control SFP with TSM and PRA-IS] to restrict the ability to ***[modify]*** the security attributes [file name and information label] to [none].

FMT_MSA.1/ IP:PORT INFO 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 [Information Flow Control SFP with TSM and PRA-IS] to restrict the ability to ***[modify]*** the security attributes [IP:Port Information] to [Authorized Manufacturer User].

FMT_MSA.1/EFTPOS SOURCE PORT INFO 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 [Information Flow Control SFP with EFT_POS Device] to restrict the ability to ***[modify]*** the security attributes [Source Port] to [none].

FMT_MSA.1/ EFT-POS LABEL INFO 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 [Information Flow Control SFP with EFT_POS Device] to restrict the ability to ***[modify]*** the security attributes [EFT-POS Label] to [none].

FMT_MSA.3/USERS and SYSTEMS Static attribute initialisation

Hierarchical to: No other components.

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, Information Flow Control SFP with TSM and PRA-IS] 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.

FMT_MSA.3/EFTPOS Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [Information Flow Control SFP with EFT-POS Device] to provide ***[permisive]*** 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/ FCR USER Management of TSF data

Hierarchical to: No other components.

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 [FCR User's authentication data] to [FCR Authorised User].

FMT_MTD.1/ FCR AUTHORİSED USER Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to ***[reset]*** the [FCR Authorised User's authentication data] to [*Authorized Manufacturer User*].

FMT_MTD.1/ AUTHORİZED MANUFACTURER USER Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to ***[create]*** the [Authorized Manufacturer User's authentication data] to ~~[assignment: the authorised identified roles]~~ [**nobody**].

Application Note 7: *No* authorised identified roles *make the changes on Authorized Manufacturer User's authentication data, but TSM does.*

6.1.6.4. FMT_SMF Specification of Management Functions

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [Authorised Manufacturer User modifies IP:Port Information. FCR Authorised User modifies User Identity],[FCR Authorised User modifies FCR User's Authentication Data, Authorised Manufacturer User modifies modifies time information and resets FCR Authorised User's Authentication Data].

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], [FCR User(Cashier)].

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, FCR Authorised User takes action in secure state works], [FCR User(Cashier) takes 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: No other components.

Dependencies: No 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 User and FCR Authorised User] when physical tampering with the TSF's devices or TSF's elements has occurred.

6.1.7.3. FPT_RCV Trusted recovery

FPT_RCV.1 Manual recovery

Hierarchical to: No other components.

Dependencies: AGD_OPE.1 Operational user guidance

FPT_RCV.1.1 After [maintenance mode events which expressed in section 3.1.3] 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: No other components.

Dependencies: No 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: No other components.

Dependencies: No 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: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [CheckSum] 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/EXT Testing of external entities

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TEE.1.1 The TSF shall run a suite of tests ***[during initial start-up and during fiscal transactions]*** 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 Document [5]].

Application Note 8: External entities are input/output interface,ERU,fiscal memory,daily memory,mesh cover,electronic seal.

FPT_TEE.1/TIME Testing of external entities

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TEE.1.1 The TSF shall run a suite of tests ***[during time synchronization with NTP]*** to check the fulfillment of [<u>accuracy of time information</u>].

FPT_TEE.1.2 If the test fails, the TSF shall [not execute time syncronization with NTP].

6.1.7.7. FPT_TST TSF self test

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests ***[during initial start-up and periodically during normal operation]*** to demonstrate the correct operation of <u>[parts of TSF].</u>

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of <u>[parts of TSF data].</u>

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of <u>[parts of TSF].</u>

6.1.8. Class FTP Trusted Path/Channels

6.1.8.1. FTP_ITC Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No 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 [<u>sending user data (sales and event data) to PRA-IS and receiving user data (FCR parameters and exchange rates) from TSM</u>].

6.2. Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE, 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

Table 3 provides an overview for security functional requirements coverage also giving an evidance for sufficiency and necessity of the SFRs chosen.

Table 3 Coverage of security objectives for TOE by SFRs

		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			
FAU_STG.4	Prevention of audit data loss			X			
FCO_NRO.2	Enforced proof of origin						X
FCS_CKM.1/TLS_AES	Cryptographic key generation						X
FCS_CKM.1/TLS_HMAC	Cryptographic key generation						X
FCS_CKM.1/ DHE-KEY	Cryptographic key generation						X
FCS_CKM.1/ EXT-DEV K_{ENC}	Cryptographic key generation						X
FCS_CKM.1/ EXT-DEV K_{HMAC}	Cryptographic key generation						X
FCS_CKM.4	Cryptographic key destruction						X
FCS_COP.1/ENC-DEC	Cryptographic operation						X
FCS_COP.1/INT-AUTH	Cryptographic operation						X

FCS_COP.1/HASHING	Cryptographic operation				X		
FCS_COP.1/EXT-DEV K_{ENC}	Cryptographic operation						X
FCS_COP.1/EXT-DEV K_{HMAC}	Cryptographic operation						X
FCS_COP.1/EXT-DEV KEYEXCHANGE	Cryptographic operation						X
FDP_ACC.1	Subset access control	X					
FDP_ACF.1	Security attribute based access control	X					
FDP_ETC.2/TSM	Export of user data with security attributes						X
FDP_ETC.2/EFTPOS	Export of user data with security attributes						X
FDP_IFC.1/TSMCOMMUNICATION	Subset information flow control						X
FDP_IFF.1/ TSMCOMMUNICATION	Simple security attributes						X
FDP_IFC.1/EFTPOSCOMMUNICATION	Subset information flow control						X
FDP_IFF.1/EFTPOS COMMUNICATION	Simple security attributes						X
FDP_ITC.2/TSM	Import of user data with security attributes						X
FDP_ITC.2/EFTPOS	Import of user data with security attributes						X
FDP_SDI.2/ MEMORY	Stored data integrity monitoring and action			X			
FDP_SDI.2/DAILY AND PRMTR	Stored data integrity monitoring and action			X			
FIA_AFL.1/MANUFACTURER	Authentication failure handling				X		
FIA_AFL.1/AUTHORISED	Authentication failure handling				X		
FIA_UAU.2	User Authentication before any action				X		
FIA_UAU.4	Single Use Authentication Mechanisms				X		
FIA_UID.2	User identification before any action				X		

FMT_MOF.1	Management of security functions behaviour					X	
FMT_MSA.1/USER IDENTITY	Management of security attributes	X					
FMT_MSA.1/PRIVILEGES	Management of security attributes	X					
FMT_MSA.1/FILENAME and INFO-LABEL	Management of security attributes						X
FMT_MSA.1/IP:PORT INFO	Management of security attributes						X
FMT_MSA.1/EFTPOS SOURCE PORT INFO	Management of security attributes						X
FMT_MSA.1/EFTPOS LABEL INFO	Management of security attributes						X
FMT_MSA.3/USERS and SYSTEMS	Static attribute initialisation	X					X
FMT_MSA.3/EFTPOS	Static attribute initialisation						X
FMT_MTD.1/FCR USER	Management of TSF data	X			X		
FMT_MTD.1/FCR AUTHORISED USER	Management of TSF data	X			X		
FMT_MTD.1/AUTHORIZED MANUFACTURER USER	Management of TSF data	X					
FMT_SMF.1	Specification of Management Functions	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			X
FPT_RCV.1	Manual recovery					X	
FPT_RCV.4	Function recovery					X	
FPT_STM.1	Reliable time stamps		X				
FPT_TDC.1	Inter-TSF basic TSF data consistency			X			
FPT_TEE.1/EXT	Testing of external entities					X	
FPT_TEE.1/TIME	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 Table 4.

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
	FAU_SAR.1	Allows users to read audit records
	FMT_MSA.1/USER IDENTITY	Provides the functions to restrict the ability to modify the security attribute(User Identity) to FCR Authorised User
	FMT_MSA.1/PRIVILEGES	Provides the functions to restrict the ability to modify the security attributes (privileges) to nobody.
	FMT_MSA.3/USERS and SYSTEMS	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_SMF.1	Descripe the specification of management functions being allowed to use in maintenance mode and secure state mode.
	FMT_SMR.2	Maintains the roles with restrictions
	FMT_MTD.1/ FCR USER	Provides authorised processing of FCR User’s authentication data
	FMT_MTD.1/ FCR AUTHORİSED USER	Provides authorised processing of FCR Authorised User’s authentication data
	FMT_MTD.1/ AUTHORİZED MANUFACTURER USER	Provides authorised processing of FCR Manufacturer User’s authentication data
O.Event	FAU_GEN.1	Generates correct audit events
	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
	FPT_PHP.2	Generation of audit event detection of

		physical tampering
	FDP_SDI.2/MEMORY	Monitors user data stored for integrity errors
	FDP_SDI.2/DAILY and PRMTR	Monitors user data stored for integrity errors
	FPT_TST.1	Ensures accuracy of its functions working by conducting self test
	FPT_TDC.1	Provides the capability to consistently interpret TSF data (checksum)
O.Authentication	FIA_AFL.1/MANUFACTURER	Detects and records authentication failure events for Autharised Manufacturer User
	FIA_AFL.1/ AUTHORISED	Detects and records authentication failure events for FCR Authorised User
	FIA_UAU.2	Defines user authentication before any action
	FIA_UAU.4	Provides single use authentication mechanism for Autharised Manufacturer User
	FIA_UID.2	No allowed actions before identification

	FMT_MTD.1/ FCR AUTHORİSED USER	Provides authorised processing of FCR Authorised User's authentication data
	FMT_MTD.1/ FCR USER	Provides authorised processing of FCR User's authentication data
	FCS_COP.1/HASHING	Provides authentication operation for PRA-IS and TSM
O.Function	FMT_MOF.1	Restricts the ability to enable the functions to nobody and, thus, prevents an unintended access to data in the operational phase.
	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_TEE.1/EXT	Provides test for IT environment for functioning accurately
	FPT_TEE.1/TIME	Provides test for IT environment for functioning accurately
	FPT_TST.1	Ensures accuracy of its functions working by conducting self test
O.Transfer	FCS_CKM.1/TLS_AES	Generates session keys for communication between FCR-PRA-IS and FCR–TSM
	FCS_CKM.1/TLS_HMAC	Generates session keys for communication between FCR-PRA-IS and FCR–TSM
	FMT_MSA.1/ EFT-POS LABEL INFO	Provides the functions to restrict the ability to modify the security attribute(EFT-POS label) to nobody
	FMT_MSA.1/FILE NAME and INFO-LABEL	Provides the functions to restrict the ability to modify the security attribute(file name) to nobody

	FMT_MSA.1/ IP:PORT INFO	Provides the functions to restrict the ability to modify the security attribute(IP/Port)to Authorized Manufacturer User
	FMT_MSA.1/EFTPOS SOURCE PORT INFO	Provides the functions to restrict the ability to modify the security attribute(EFT-POS source port) to nobody
	FMT_MSA.3/USERS and SYSTEMS	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_MSA.3/EFTPOS	Provides the functions to provide permisive 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
	FCS_CKM.4	Destroys cryptographic keys in the TOE

	FCS_COP.1/ENC-DEC	Provides the cryptographic operation for secure communication between PRA-IS and new generation cash register fiscal application software, and between TSM and new generation cash register fiscal application software
	FCS_COP.1/INT-AUTH	Provides authentication and integrity protection for comminication between FCR-PRA-IS and FCR–TSM
	FPT_PHP.2	Generation of audit event detection of physical tampering
	FCO_NRO.2	Generates evidence of origin of the data to be transferred to the PRA-IS
	FCS_CKM.1/ DHE-KEY	Generates private key for DHE key agreement
	FCS_COP.1/EXT-DEV K_{ENC}	Provides symmetric encryption in order to establish secure communication with EFT-POS Devices.
	FCS_COP.1/ EXT-DEV K_{HMAC}	Provides authentication and integrity protection for comminication with External Devices.

	FCS_CKM.1/ EXT-DEV K_{ENC}	Generates keys for communication between TOE and External Devices
	FCS_CKM.1/ EXT-DEV K_{HMAC}	Generates keys for communication between TOE and External Devices
	FCS_COP.1/EXT-DEV KEYEXCHANGE	Provides agreement operation with External Devices
	FDP_ETC.2/TSM	Provides export of sale's data and event data from the TOE to the PRA-IS using the information flow control SFP with TSM and PRA-IS
	FDP_ETC.2/EFTPOS	Provides export of amount information in sale’s data from the TOE to the EFT-POS using the information flow control SFP with EFT-POS Devices
	FDP_IFC.1/TSMCOMMUNICATION	Provides information flow control policy for TSM and PRA-IS communication
	FDP_IFC.1/EFTPOSCOMMUNICATION	Provides information flow control policy for EFT-POS communication
	FDP_IFF.1/TSMCOMMUNICATION	Provides information flow control policy rules for TSM and PRA-IS

		communication
	FDP_IFF.1/EFTPOSCOMMUNICATION	Provides information flow control policy rules for EFT-POS communication
	FDT_ITC.2/TSM	Provides protection of FCR Parameters confidentiality and integrity during import from TSM
	FDT_ITC.2/EFTPOS	Provides protection of confidentiality and integrity of outcome of the operation conducted by the EFT-POS device and AES keys (KENC and KHMAC) during import from EFT-POS device
	FTP_ITC.1	Provides protection of sale's data and event data (confidentiality+integrity) during communication with PRA-IS by the help of secure channel

6.3.2.Rationale for Security Functional Requirements dependencies

Selected security functional requirements include related dependencies. Table 5 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	FIA_UID.2 is hierarchical to FIA_UID.1
FCS_CKM.1/TLS_AES	FCS_CKM.2 or FCS_COP.1; FCS_CKM.4	FCS_COP.1/ENC-DEC and FCS_CKM.4 included
FCS_CKM.1/TLS_HMAC	FCS_CKM.2 or FCS_COP.1; FCS_CKM.4	FCS_COP.1/INT-AUTH and FCS_CKM.4 included
FCS_CKM.1/ EXT-DEV K_{ENC}	FCS_CKM.2 or FCS_COP.1; FCS_CKM.4	FCS_COP.1/EXT-DEV KENC and FCS_CKM.4 included
FCS_CKM.1/ EXT-DEV K_{HMAC}	FCS_CKM.2 or FCS_COP.1; FCS_CKM.4	FCS_COP.1/ EXT-DEV K_{HMAC} and FCS_CKM.4 included
FCS_CKM.1/ DHE-KEY	FCS_CKM.2 or FCS_COP.1; FCS_CKM.4	FCS_COP.1/ EXT-DEV KEYEXCHANGE and FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1(FCS_CKM.1/ EXT-DEV K_{ENC}, FCS_CKM.1/ EXT-DEV K_{HMAC}, FCS_CKM.1/TLS_HMAC, FCS_CKM.1/TLS_AES and FCS_COP.1/ EXT-DEV KEYEXCHANGE) included
FCS_COP.1/ENC-DEC	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ; FCS_CKM.4	FCS_CKM.1/TLS_AES and FCS_CKM.4 included
FCS_COP.1/INT-AUTH	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ; FCS_CKM.4	FCS_CKM.1/TLS_HMAC and FCS_CKM.4 included
FCS_COP.1/HASHING	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1;	No need to include any dependencies because there is no need to use any key

	FCS_CKM.4	for HASHING
FCS_COP.1/EXT-DEV K_{ENC}	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ;FCS_CKM.4	FCS_CKM.1/ EXT-DEV K_{ENC} ; FCS_CKM.4 included
FCS_COP.1/ EXT-DEV K_{HMAC}	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ;FCS_CKM.4	FCS_CKM.1/ EXT-DEV K_{HMAC}; FCS_CKM.4 included
FCS_COP.1/ EXT-DEV KEYEXCHANGE	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ;FCS_CKM.4	FCS_CKM.1/ DHE-KEY and FCS_CKM.4 included
FDP_ACC.1	FDP_ACF.1	included
FDP_ACF.1	FDP_ACC.1; FMT_MSA.3	FDP_ACC.1; FMT_MSA.3/USERS and SYSTEMS included
FDP_ETC.2/TSM	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1; FDP_IFC.1/TSMCOMMUNICATION included
FDP_ETC.2/EFTPOS	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1; FDP_IFC.1/EFTPOSCOMMUNICATION included
FDP_IFC.1/TSMCOMMUNICATION	FDP_IFF.1	FDP_IFF.1/TSMCOMMUNICATION included
FDP_IFF.1/TSMCOMMUNICATION	FDP_IFC.1; FMT_MSA.3	FDP_IFC.1/TSMCOMMUNICATION; FMT_MSA.3/USERS and SYSTEMS included
FDP_IFC.1/EFT-POSCOMMUNICATION	FDP_IFF.1	FDP_IFF.1/EFT-POSCOMMUNICATION included

FDP_IFF.1/ EFT-POSCOMMUNICATION	FDP_IFC.1; FMT_MSA.3	FDP_IFC.1/EFTPOSCOMMUNICATION; FMT_MSA.3/EFTPOS included
FDP_ITC.2/TSM	FDP_ACC.1 or FDP_IFC.1 ;FTP_ITC.1 or FTP_TRP.1 ;FPT_TDC.1	FDP_IFC.1/TSMCOMMUNICATION; FTP_ITC.1; FPT_TDC.1 included
FDP_ITC.2/EFTPOS	FDP_ACC.1 or FDP_IFC.1 ;FTP_ITC.1 or FTP_TRP.1 ;FPT_TDC.1	FDP_IFC.1/EFTPOSCOMMUNICATION; FTP_ITC.1; FPT_TDC.1 included
FDP_SDI.2/MEMORY	No dependencies	-
FDP_SDI.2/DAILY and PRMTR	No dependencies	-
FIA_AFL.1/MANUFACTURER	FIA_UAU.1	FIA_UAU.2 is hierarchical to FIA_UAU.1
FIA_AFL.1/AUTHORISED	FIA_UAU.1	FIA_UAU.2 is hierarchical to FIA_UAU.1
FIA_UAU.1	FIA_UID.1	FIA_UID.2 is hierarchical to FIA_UID.1
FIA_UAU.4	No dependencies	-
FIA.UID.1	No dependencies	-
FMT_MOF.1	FMT_SMR.1; FMT_SMF.1	FMT_SMR.2 is hierarchical to FMT_SMR.1; FMT_SMF.1
FMT_MSA.1/USER IDENTITY	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	FDP_ACC.1 included
FMT_MSA.1/PRIVILEGES	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	FDP_ACC.1 included
FMT_MSA.1/FILENAME and INFO-LABEL	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	FDP_IFC.1/TSMCOMMUNICATION included
FMT_MSA.1/IP:PORT INFO	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1;	FDP_IFC.1/TSMCOMMUNICATION included

	FMT_SMF.1	

FMT_MSA.1/EFTPOS SOURCE PORT INFO	FDP_ACC.1 or FDP_IFC.1;
	FMT_SMR.1;
	FMT_SMF.1
		FDP_IFC.1/EFTPOSCOMMUNICATION included

FMT_MSA.1/EFTPOS LABEL INFO	FDP_ACC.1 or FDP_IFC.1;
	FMT_SMR.1;
	FMT_SMF.1
		FDP_IFC.1/EFTPOSCOMMUNICATION included

FMT_MSA.3/USERS and SYSTEMS	FMT_MSA.1; FMT_SMR.1	FMT_MSA.1 (FMT_MSA.1/USER IDENTITY, FMT_MSA.1/PRIVILEGES, FMT_MSA.1/IP:PORT INFO, FMT_MSA.1/FILE NAME and INFO-LABEL) ; FMT_SMR.1 is hierarchical to FMT_SMR.1 included
FMT_MSA.3/EFTPOS	FMT_MSA.1; FMT_SMR.1	FMT_MSA.1/ EFT-POS LABEL INFO) ; FMT_SMR.2 is hierarchical to FMT_SMR.1 included
FMT_MTD.1/FCR USER	FMT_SMR.1; FMT_SMF.1	FMT_SMR.2 is hierarchical to FMT_SMR.1 ; FMT_SMF.1 included
FMT_MTD.1/FCR AUTHORISED USER	FMT_SMR.1; FMT_SMF.1	FMT_SMR.2 is hierarchical to FMT_SMR.1 ; FMT_SMF.1 included
FMT_MTD.1/AUTHORIZED MANUFACTURER USER	FMT_SMR.1; FMT_SMF.1	FMT_SMR.2 is hierarchical to FMT_SMR.1 ; FMT_SMF.1 included
FMT_SMF.1	No dependencies	-
FMT_SMR.2	FIA_UID.1	FIA_UID.2 is hierarchical to FIA_UID.1 included
FPT_FLS.1	No dependencies	-
FPT_PHP.2	FMT_MOF.1	included
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/EXT	No dependencies	-
FPT_TEE.1/TIME	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 Table 5 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. TOE SUMMARY SPECIFICATIONS

The following security functions are implemented in order to satisfy the Security Functional Requirements in Section 6.1 of this Security Target.

7.1. Audit/Event Log Function

Audit/Event Function is going to generate the events specified in PRA Messaging Protocol Document[6] at minimum.

For each auditable event in the list, TSF will add Date and Time of the event and identity of the subject to the stored event.

TSF will protect the stored events data and prevent any unauthorised modifications to the stored audit records. To prevent unauthorised modification, TSF checks the integrity of event database. This Security Function is satisfying the following SFRs;

FAU_GEN.1, FAU_SAR.1,FAU_STG.1, FAU_STG.4,
FPT_STM.1,FDP_SDI.2/MEMORY

7.2. Cryptography Function

Cryptography function is going to encrypt the exported event and sales data from TOE to PRA-IS. Function will also be used for decrypting the imported FCR parameters from TSM. This function supports usage of hashing for data export and import operations with TSM and PRA-IS.

TOE also establishes a secure communication with third party devices like EFT-POS.

This Security Function is satisfying the following SFRs;

FCS_CKM.1/TLS_AES,FCS_CKM.1/TLS_HMAC, FCS_CKM.1/DHE-KEY, FCS_CKM.1/EXT-DEV KENC, FCS_CKM.1/EXT-DEV KHMAC, FCS_CKM.4, FCS_COP.1/ENC-DEC, FCS_COP.1/INT_AUTH, FCS_COP.1/HASHING, FCS_COP.1/EXT-DEV K_{ENC}, FCS_COP.1/EXT-DEV K_{HMAC}, FCS_COP.1/EXT-DEV KEYEXCHANGE, FDP_ITC.2/EFTPOS, FTP_ITC.1, FDP_ETC.2/EFTPOS, FDP_ITC.2/TSM, FDP_ETC.2/TSM

7.3. Identification and Authentication Function

Identification and Authentication Function will support the following features;

- Enforce identification and authentication mechanism for the following users;
  - FCR User
  - FCR Authorised User

  - Authorized Manufacturer User

- Enforce identification and authentication mechanism for the following systems;
  - PRA-IS
  - TSM

This Security Function is satisfying the following SFRs;

FIA_AFL.1/MANUFACTURER, FIA_AFL.1/AUTHORISED, FIA_UAU.2, FIA_UAU.4, FIA_UID.2, FDP_ITC.2/TSM, FDP_ETC.2/TSM

7.4. Access Control

Access Control Function will support the following features;

- Enforce an access control policy for FCR User, FCR Authorized User and Authorized Manufacturer User according to their security attributes.

This Security Function is satisfying the following SFRs;

FDP_ACC.1, FDP_ACF.1

7.5. Data Integrity Function

The memory space for sales data, event data, authentication data, characterization data and FCR parameters will be subject to a integrity check in order to provide the integrity of the data.

This Security Function is satisfying the following SFRs;

FDP_SDI.2/MEMORY, FDP_SDI.2/DAILY AND PRMTR

7.6. Import/Export Function

The TOE will import following data from TSM according to the protocol defined in PRA Messaging Protocol Document [6] :

- FCR parameters
- Communication Table
- Currency Table

The imported data will be saved in the FCR for use. TOE exports the event, receipt and sales data to PRA-IS according to the FCR parameters securely.

The TOE will export data to EFT-POS according to the protocol defined in External Device Communication Protocol Document [7].

The TOE will import data from EFT-POS according to the protocol defined in External Device Communication Protocol Document [7].

This Security Function is satisfying the following SFRs;

FDP_ETC.2/TSM, FDP_ITC.2/TSM,FDP_IFF.1/TSMCOMMUNICATION, FDP_IFC.1/TSMCOMMUNICATION,FDP_IFF.1/EFTPOSCOMMUNICATION,FDP_IFC.1/EFTPOSCOMMUNICATION, FDP_ETC.2/EFTPOS,FDP_ITC.2/EFTPOS, FTP_ITC.1

7.7. TSF Protection

TSF will protect the secure operation of the TOE by conduction the following functionality;

- In case of generation of an event with the event type "Urgent", the function or module make the TOE switch to "Maintenance Mode".
- With the support of Electronic Seal, TOE Security Functions will check the external switches frequently for a possible tampering.
- In case of an internal tampering to the mesh cover inside electronic seal, main MPU will erase session keys. Upon tampering of the mesh cover, TOE will switch to Maintenance Mode.

This Security Function is satisfying the following SFRs;

FPT_FLS.1, FPT_PHP.2, FPT_RCV.1, FPT_RCV.4, FPT_TDC.1

7.8. Data Preparation Function

Data Preparation Function reverts the sales and event data to a data package specified in PRA Messaging Protocol before the export operation. It calculates the LRC of the package and adds it to the exported message. This will provide integrity control during transmission.

This Security Function is satisfying the following SFRs;

FCO_NRO.2

7.9. TOE Self-Testing Function

TOE will conduct self testing during initial startup and periodically during normal operation and conduct tests on event data, sales data and external entities.

Upon unsuccessful test results, TSF will generate an event log and take the necessary actions.

When fiscal memory is disconnected, FCR will switch to maintenance mode. When ERU is disconnected, FCR will stop operation and wait for ERU reconnection.

TOE will try to make time syncronization with NTP before every Z report. When time information is acquired from NTP server, TOE will check if time information is valid before executing NTP time syncronization.

This Security Function is satisfying the following SFRs;

FPT_TST.1, FPT_TEE.1/EXT, FPT_TEE.1/TIME

7.10. TSF Management Function

The following functions can be managed by the TOE :

authentication data, user identities, communication tables, limits of user functions, time.

FCR Authorized User has the right to read, write, modify and delete FCR User authentication data and FCR User identities.

TSM is forwarding the communication tables to the TOE from PRA and with these tables, the destination adress and content of the data which will be exported outside the TOE can be modified.

This Security Function is satisfying the following SFRs;

FMT_MOF.1, FMT_MSA.1/USER IDENTITY, FMT_MSA.1/PRIVILEGES, FMT_MSA.1/FILENAME and INFO-LABEL, FMT_MSA.1/IP:PORT INFO, FMT_MSA.1/EFTPOS LABEL INFO, FMT_MSA.3/USERS and SYSTEMS, FMT_MSA.3/EFTPOS, FMT_MTD.1/FCR USER, FMT_MTD.1/FCR AUTHORISED USER, FMT_MTD.1/AUTHORIZED MANUFACTURER USER, FMT_SMF.1, FMT_SMR.2

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: SecurityFunctional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: SecurityAssurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

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

New Generation Cash Register Directives

[5] Technical Guidance Document(TK1), version 2.0

[6] PRA Messaging Protocol Document(TK1), version 2.02

[7] External Device Communication Protocol Document, version 1.0