|  |
| --- |
|  |
| **CHANGE v 06.00** |
| **SECURITY TARGET LITE** |
| Version 1.0Copyright © 2017 by E Data Elektronik San. ve Tic. A.Ş. All rights reserved. |
|  |
|  |

|  |
| --- |
| August 21 2017 |

Table of Contents

[1. ST INTRODUCTION 5](#_Toc422229685)

[1.1. ST Reference and TOE Reference 5](#_Toc422229686)

[1.2. Document Conventions, Terminology & Acronyms 5](#_Toc422229687)

[1.2.1. Conventions 5](#_Toc422229688)

[1.2.2. Terminology 6](#_Toc422229689)

[1.2.3. Acronyms 6](#_Toc422229690)

[1.3. TOE Overview 8](#_Toc422229691)

[1.3.1. General overview of the TOE and related components 8](#_Toc422229692)

[1.3.2. Required Non-TOE Hardware/Software 9](#_Toc422229693)

[1.3.3. Major security and functional features 14](#_Toc422229694)

[1.3.4. TOE Type 15](#_Toc422229695)

[1.4. TOE Description 15](#_Toc422229696)

[1.4.1. Physical Scope 15](#_Toc422229697)

[1.4.2. Logical Scope 16](#_Toc422229698)

[2. CONFORMANCE CLAIM 18](#_Toc422229699)

[2.1. CC Conformance Claim 18](#_Toc422229700)

[2.2. PP and Package Claim 18](#_Toc422229701)

[2.2.1. Protection Profile (PP) Claim 18](#_Toc422229702)

[2.2.2. Package Claim 18](#_Toc422229703)

[2.3. Conformance Claim Rationale 18](#_Toc422229704)

[3. SECURITY PROBLEM DEFINITION 20](#_Toc422229705)

[3.1. TOE Security Policy 20](#_Toc422229706)

[3.1.1. External Entities 20](#_Toc422229707)

[3.1.2. Roles 21](#_Toc422229708)

[3.1.3. Modes of FCR 21](#_Toc422229709)

[3.1.4. Assets 22](#_Toc422229710)

[3.2. Threats 25](#_Toc422229711)

[3.3. OSP 28](#_Toc422229712)

[3.4. Assumptions 30](#_Toc422229713)

[4. SECURITY OBJECTIVES 31](#_Toc422229714)

[4.1. Security Objectives for the TOE 31](#_Toc422229715)

[4.2. Security Objectives for the Operational Environment 33](#_Toc422229716)

[4.3. Security Objective Rationale 34](#_Toc422229717)

[5. EXTENDED COMPONENT DEFINITION 39](#_Toc422229718)

[6. SECURITY REQUIREMENTS 40](#_Toc422229719)

[6.1. Security Functional Requirements for the TOE 40](#_Toc422229720)

[6.1.1. Class FAU Security Audit 40](#_Toc422229721)

[6.1.2. Class FCO Communication 42](#_Toc422229722)

[6.1.3. Class FCS Cryptographic Support 42](#_Toc422229723)

[6.1.4. Class FDP User Data Protection 50](#_Toc422229724)

[6.1.5. Class FIA Identification and Authentication 57](#_Toc422229725)

[6.1.6. Class FMT Security Management 58](#_Toc422229726)

[6.1.7. Class FPT Protection of the TSF 63](#_Toc422229727)

[6.1.8. Class FTP Trusted Path/Channels 65](#_Toc422229728)

[6.2. Security Assurance Requirements for the TOE 67](#_Toc422229729)

[6.3. Security Requirements Rationale 67](#_Toc422229730)

[7. TOE SUMMARY SPECIFICATIONS 92](#_Toc422229731)

[7.1. Audit/Event Log Function 92](#_Toc422229732)

[7.2. Cryptography Function 92](#_Toc422229733)

[7.3. Identification and Authentication Function 92](#_Toc422229734)

[7.4. Access Control 93](#_Toc422229735)

[7.5. Data Integrity Function 93](#_Toc422229736)

[7.6. Import/Export Function 93](#_Toc422229737)

[7.7. TSF Protection 94](#_Toc422229738)

[7.8. Data Preparation Function 94](#_Toc422229739)

[7.9. TOE Self-Testing Function 95](#_Toc422229740)

[7.10. TSF Management Function 95](#_Toc422229741)

[8. BIBLIOGRAPHY 97](#_Toc422229742)

[Common Criteria 97](#_Toc422229743)

[New Generation Cash Register Directives 97](#_Toc422229744)

**Version History**

|  |  |  |
| --- | --- | --- |
| Version No | Reason for Change | Release Date |
| 1.0 | First Release | 21/08/2017 |

**Approvals**

|  |  |
| --- | --- |
| Name | Role |
| Volkan HEKİMOĞLU | Project Manager |
| Emre ÖZSAN | SW Specialist |
| Egemen ÖZTAMAZ | Junior SW Specialist |

# 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.

## ST Reference and TOE Reference

|  |  |
| --- | --- |
| ST Title: | CHANGE v 06.00 Security Target Lite v 1.0 |
| ST Version: | v 1.0 |
| TOE Identification: | CHANGE v 06.00 |
| 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

## Document Conventions, Terminology & Acronyms

This section specifies the formatting information used in the ST.

### 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 underlinedidentified between *“*[brackets]”.

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.

### Terminology

The following terminology is used in this Security Target:

MPU : Microprocessor Unit

### 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

## TOE Overview

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

The 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 1.3.1, 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.

### 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 parts of Figure 1 compose the TOE. Yellow parts; that are given as input/output interface, fiscal memory, daily memory, database, ERU, fiscal certificate memory; are TOE’s environmental components which are crucial for functionality and security. Connections between the TOE and its environment are also subject to evaluation since these connections are made over the interfaces of the TOE.



Figure 1 TOE (CHANGE and Crypto Library ) and Related Components

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

### Required Non-TOE Hardware/Software

Software and hardware environment of the TOE are described below.

#### Software Environment of TOE

CHANGE Software 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  |
| 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](http://en.wikipedia.org/wiki/Computer_multitasking#Preemptive_multitasking.2Ftime-sharing) (both in [user mode](http://en.wikipedia.org/wiki/User_mode) and [kernel mode](http://en.wikipedia.org/wiki/Kernel_mode)), [virtual memory](http://en.wikipedia.org/wiki/Virtual_memory), [shared libraries](http://en.wikipedia.org/wiki/Library_%28computer_science%29), [demand loading](http://en.wikipedia.org/wiki/Demand_paging), shared [copy-on-write](http://en.wikipedia.org/wiki/Copy-on-write) executables (via [KSM](http://en.wikipedia.org/wiki/Kernel_SamePage_Merging_%28KSM%29)), [memory management](http://en.wikipedia.org/wiki/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;
1. Database has data recording, organizing, querying, reporting features
2. 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
3. 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.

#### Hardware Environment of TOE

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

* **Fiscal memory**
1. Fiscal memory has following features;
2. Fiscal memory has the capacity to store at least 10 years (3650 days) of data,
3. Fiscal memory keeps data at least 5 years after the capacity specified in (a) has been reached,
4. Fiscal memory has to be fixed within FCR in a way that it cannot be removed without damaging the chassis.
5. Fiscal memory is protected by mesh cover,
6. 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,

1. The data stored in the fiscal memory is not be lost in case of power off,
2. Fiscal memory accepts only positive amounts from the application and the peripherals,
3. 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.
4. Fiscal Memory includes following data;
5. Fiscal symbol, company code and identification number of the device,
6. 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),
7. Date and number of daily "Z" reports with total sales and VAT per day,
8. 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;**
1. 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.
2. Data in the daily memory which is not already transmitted to fiscal memory, cannot be modified in an uncontrolled way.
3. Data transmitted from daily memory to fiscal memory is to be kept in daily memory for at least 10 days.
4. 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.
5. Following values are to be stored in the daily memory
6. total VAT amount per day,
7. total daily sales values per day grouped by payment type
8. payment type (Cash, credit card etc.)
9. 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;
1. ERU stores information about receipts and reports (X, Z) in a retrievable form
2. ERU has at least 1.2 million row capacity. ERU may be included in the sealed part of the FCR. In this case ERU must have at least 40 million row capacity.
3. Data stored in ERU cannot be modified
4. 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/SMART PINPAD.
* FCR needs some input/output devices for functionalities listed below;
1. FCR has keyboard unit.
2. FCR has separate displays for cashier and buyer.
3. FCR has internal battery to keep time information.

### Major security and functional features

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

#### 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](http://en.wikipedia.org/wiki/Receipt). TOE provides the following services;

1. TOE stores sales data in fiscal memory.
2. TOE stores total receipt and total VAT amount for each receipt in daily memory.
3. TOE is able to generate reports (X report, Z report etc.).
4. 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.
5. TOE is able to start the communication with PRA-IS and instantly respond to requests originated from PRA-IS.
6. 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.
7. 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.

#### TOE major security features

The TOE provides following security features;

1. TOE supports access control.
2. TOE is able to detect disconnection between main processor and fiscal memory and enter into the maintenance mode.
3. TOE supports usage of ITU X509 v3 formatted certificate and its protected private key for authentication and secure communication with PRA- IS and TSM.
4. TOE supports secure communication with EFT-POS/Smart PinPad.
5. TOE supports secure communication between FCR-PRA-IS and FCR–TSM.
6. TOE ensures the integrity of event data, sales data, authentication data, characterization data and FCR parameters.
7. TOE records important events defined in PRA Messaging Protocol Document [6] and send urgent event data immediately to PRA-IS in a secure way.
8. TOE detects physical attacks to FCR and enters into the maintenance mode in such cases.

### TOE Type

TOE is a Fiscal Application software (CHANGE) and Hardware Crypto library embedded within FCR.

## TOE Description

### 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
* Hardware Crypto library (part of the TOE)

Flash memory is used to store the operating system, Fiscal Application software (part of the 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 optionally supports GPRS communication.

FCR optionally supports PSTN communication.

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

### Logical Scope

The logical scope of the TOE consists of the security functional features of the Fiscal Application software and Crypto Library 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, encryption/decryption 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 secure communication with TSM and PRA-IS according to PRA Messaging Protocol Document[6].
* Access Control: The access rights in the TOE are controlled with an access control policy which is enforced during authentication of 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.

# CONFORMANCE CLAIM

## 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.

## PP and Package Claim

### Protection Profile (PP) Claim

This Security Target claims demonstrable conformance to New Generation Cash Register Fiscal Applicaton Software 2 Protection Profile TSE-3C1S/PP-008.

### Package Claim

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

* Assurance package EAL2 conformant to CC, part 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.

# SECURITY PROBLEM DEFINITION

## TOE Security Policy

### 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 Manager**

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 of 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 and 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.

### Roles

**FCR Authorised User**

FCR Authorised User is the user who uses the functions of FCR and operates FCR by accessing the device over an authentication mechanism.

**Authorized Manufacturer User**

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

**Unauthenticated Users**

Unauthenticated Users are users who do ficsal sales or get nonfiscal FCR reports. However, they are unable to get fiscal FCR reports and configure FCR.

### Modes of FCR

**Secure State Mode:** Secure State Mode is the mode that allows;

* FCR Authorised User;
* to configure FCR,
* to take fiscal and FCR reports
* Unauthenticated Users;
* to do fiscal sales,
* to get FCR reports (except fiscal reports).

**Maintenance Mode:** Maintenance Mode is the mode that allows only Authorised Manufacturer User;

* to change date and time information
* to change IP/Port information of TSM
* to review event data
* 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,
* When server certificates or root certificates check fails,
* Mesh cover monitoring check fails,
* A disconnection between fiscal memory and main processor occurs,
* Electronic seal is opened or forced by unauthorised persons,
* Daily maximum events log limit is reached,
* A technical problem is determined by FCR Manufacturer.

### Assets

**Sensitive data**

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

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

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

**Event data**

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

**Sales data**

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

**Characterization data (Identification data for devices)**

Characterization data is a unique number assigned to each FCR 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 trusted server. Time information is important when logging important events and sending reports to the PRA-IS. The integrity of this asset has to be protected.

**Server Certificates**

Server certificates contain PRA-IS and TSM certificates (PPRA, PPRA-SIGN, PTSM and PTSM-SIGN).

PPRA and PPRA-SIGN certificates are used for signing and encryption process during key transport between TOE and PRA-IS.

PTSM certificate is used for encryption process during key transport between TOE and TSM and PTSM-SIGN is used for signature verification of FCR parameters by TOE.

**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

## 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 Authorised User gaining access to Authorised Manufacturer User 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: Unauthenticated users could try to use FCR functions except doing fiscal sales and taking reports which are not fiscal.

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

Asset: Sales data, event data, time information

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

Adverse action: This threat deals with five types of data: event data, sales data, characterization data, authentication data and FCR parameters.

* An attacker could try to manipulate the event data to hide its actions and 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.
* An attacker also could try to disclose and modify authentication data in FCR to gain access to functions which are not allowed to his/her.

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

Asset: Event data, sales data, characterization data, FCR parameters and authentication data.

**T.Eavesdrop - Eavesdropping on event data, sales data and characterization data**

Adverse action : An attacker could try to eavesdrop event data, sales data and characterization data transmitted between the TOE and the PRA-IS and also between the TOE and the distributed memory units (Fiscal memory, Database, Daily memory, ERU).

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

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

**T.Counterfeit - FCR counterfeiting**

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

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

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

**T. Server counterfeiting**

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

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

Asset: Server Certificates

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

Adverse action : An attacker may try to use FCR out of its normal operational conditions to cause malfunction without the knowledge of TOE.

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

Asset : Sales data, event data.

**T.ChangingTime**

Adverse action : An attacker may try to change time to invalidate the information about logged events and reports in FCR.

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

Asset : Time information

## 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 and sub-root (subordinate) certificates that are used for verification of all certificates that are produced by Certification Authority,
* PPRA and PTSM certificates that are used for key transport process between FCR-PRA-IS and FCR-TSM,
* PPRA-SIGN and PTSM-SIGN certificates which are used by TOE for signature verification,
* UpdateControl certificate that is used to verify the signature of the TOE.

**P.Certificates Installation**

It has to be assured that environment of TOE provides secure installation of certificates (PPRA, PPRA-SIGN, PTSM, PTSM-SIGN, Certification Authority root and sub-root certificates, UpdateControl certificate) into the FCR at initialization phase. Before the installation of certificates, it has to be assured that asymmetric key pair is generated in a manner which maintains security posture.

**P.Comm\_EXT - Communication between TOE and External Device**

It has to be assured that communication between TOE and external devices is used to encrypted using AES algorithm with 256 bits according to External Device Communication Protocol Document [7].

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

It has to be assured that TOE’s environment provides a secure mechanism which prevents attacker to obtain sensitive information (private key) when FCR performs signature operation 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.

 It has to be assured that fiscal memory doesn't accept transactions with negative amounts which results in a decrease of total tax value.

It has to be assured that environment of TOE provides a mechanism that sales data in daily memory which is not reflected to the fiscal memory cannot be deleted and modified in an uncontrolled way.

It has to be assured that sales data in ERU cannot be deleted and modified.

**P.PhysicalTamper**

It has to be assured that TOE environment and TOE provide a tamper respondent system which is formed by electromechanical seals.

It has to be assured that physical tampering protection system protects the keys (asymmetric key, symmetric key), the certificates, event data, characterization data, FCR parameters and sales data in FCR.

It has to be assured that TOE logs this type of events and enters into the maintenance mode when physical tampering protection system detect unauthorised access.

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

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

**P.PKI - Public key infrastructure**

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

**P.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.

## 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/SMART PINPAD) generates strong key for communicating with TOE and stores it in a secure way.

**A.Ext\_Device Pairing**

It is assumed that External Device and TOE are paired by Authorised Service.

# SECURITY OBJECTIVES

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

## 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 (TRMK, TRMKD, TREK, TRAK and TDK) , server certificates and FCR parameters located in the FCR and between the distributed memory units.

**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 must provide confidentiality, integrity and authenticity for information send/received during external device communication.

## Security Objectives for the Operational Environment

This part describes security objectives provided by the operational environment.

**OE.Manufacturing**

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

**OE.Delivery**

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

**OE.KeyGeneration**

Asymmetric key and certificate generation mechanism shall be compatible with ITU X.509 format and accessible only by trusted persons.

**OE.SecureStorage**

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

Sensitive Data, all 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 to the FCR must be done by protecting their confidentiality and integrity. In addition to this, transportation and installation of server certificates, Certification Authority root and sub-root certificates, FCR certificates and update control certificates must be done by protecting their 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 generation 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).

**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.External Device**

External Device should generate strong key for communicating with TOE and should store it in a secure way.

**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.

**OE.Ext\_Pairing**

External Device should be paired with TOE by only Authorised Service.

## 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.Server Counterfeiting | T.Counterfeit | T.Malfunction | T.ChangingTime | P.Certificate | P.Certificate Installation | P.SecureEnvironment | P.PhysicalTamper | P.PKI | P.InformationLeakage | P.Comm\_EXT | P.UpdateControl | A.Ext\_Key | A.TrustedManufacturer | A.Control | A. AuthorisedService | A.Initialisation | A.Activation | A.Ext\_Device Pairing  | A.TrustedUser |
| O.AccessControl | X |  |  |  |  |  |  | X |  |  |  | X |  |  |  | X |  |  |  |  |  |  |  |  |
| O.Event | X | X | X | X | X | X | X | X |  |  | X | X |  |  |  |  |  |  |  |  |  |  |  |  |
| O.Integrity |  |  | X | X | X | X |  |  |  |  | X | X |  |  |  |  |  |  |  |  |  |  |  |  |
| O.Authentication |  | 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 | X | X | X |  |  |  | X |  | X |  |  |  |  |  |  |  |  |  |  |  |  |
| OE.KeyTransportation |  |  |  |  |  |  |  |  |  | X |  |  | X |  |  |  |  |  |  |  | X |  |  |  |
| OE.TestEnvironment |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |
| OE.StrongAlgorithm |  |  |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |
| OE.UpgradeSoftware |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |  |  |  |
| OE.TrustedUser |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  | X |
| OE.Control |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
| OE.SecureEnvironment |  |  |  |  |  |  |  |  |  |  | X | X |  |  |  |  |  |  |  |  | X |  |  |  |
| OE.Ext\_Pairing |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | X |  |

Justification about Table 1 is given below;

**T.AccessControl** is addressed by O.AccessControl to control user access to functions and data; O.Event to log all access attempts.

**T.Authentication** is addressed by O.Authentication to ensure that 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, authentication 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 FCR parameters during transfering from TSM to FCR; O.Event to log unexpected behavior of these memories and unexpected behavior in transferring data; OE. SecureStorage to provide secure environment for Sensitive Data, all certificates, event data, characterization data and sales data.

**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. SecureStorage to provide secure environment for event data, characterization data and sales data

**T.Counterfeit** is addressed by O.Integrity to ensure the integrity of sensitive data ( TREK,TRAK,TDK); O.Event to log physical tamper; OE. SecureStorage to provide secure environment for sensitive data.

**T.Server Counterfeiting** is addressed by O.Integrity to ensure the integrity of server certificates (PPRA, PPRA-SIGN, PTSM and PTSM-SIGN); O.Event to log physical tamper;OE. SecureStorage to provide secure environment for server certificates.

**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.AccessControl to control user access to time information; by O.Function to ensure accuracy of time information.

**P.Certificate** is fulfilled by OE.KeyGeneration.

**P.Certificate Installation** is fulfilled OE.KeyTransportation and OE.SecureStorage.

**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.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.AccessControl.

**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.

**A.Ext\_Device Pairing** is upheld byOE.Ext\_Pairing.

# EXTENDED COMPONENT DEFINITION

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

# SECURITY REQUIREMENTS

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

The following notations are used:

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

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

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

**Iteration** operation are identified with a slash (e.g. “(/)”)

## Security Functional Requirements for the TOE

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

### Class FAU Security Audit

#### 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 security 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].

#### 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.

#### 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.

### Class FCO Communication

#### 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].

### Class FCS Cryptographic Support

#### FCS\_CKM Cryptographic key management

**FCS\_CKM.1/ TRMK 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 [256 bits] that meet the following: [none].

**FCS\_CKM.1/ TRMKD 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 [256 bits] that meet the following: [none].

**FCS\_CKM.2 Cryptographic key distribution**

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\_CKM.2.1** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [according to PRA Messaging Protocol Document [6] ] that meets the following: [none].

**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].

***Application Note 2:*** *Keys shall be deleted according to below Table 3.*

Table 3 Key Management Table

|  |  |
| --- | --- |
| **Keys** | **When** |
| TREK | * The usage number that is specified PRA Messaging Protocol Document [6] is exceeded
* Electronic seal is opened by authorized/unauthorized user
 |
| TRAK | * The usage number that is specified PRA Messaging Protocol Document [6] is exceeded
* Electronic seal is opened by authorized/unauthorized user
 |
| TDK | * The usage number that is specified PRA Messaging Protocol Document [6] is exceeded
* Electronic seal is opened by authorized/unauthorized user
 |
| TRMK | After key transport from PRA-IS to TOE for TREK and TRAK |
| TRMKD | After key transport from TSM to TOE for TDK |
| KENC | * Conditions specified in External Device Communication Protocol Document [7] occur
* The usage number that is specified External Device Communication Protocol Document [7] is exceeded
 |
| KHMAC | * Conditions specified in External Device Communication Protocol Document [7] occur
* The usage number that is specified External Device Communication Protocol Document [7] is exceeded
 |
| DHE-KEY | After key agrement between TOE and External Device |

#### FCS\_COP Cryptographic operation

**FCS\_COP.1/TREK 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] in accordance with a specified cryptographic algorithm [AES in CBC mode] and cryptographic key sizes [AES:256 bits ] that meet the following: [NIST SP800-38A (CBC.AES256)].

**FCS\_COP.1/TRAK 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 [AES in CBC mode] and cryptographic key sizes [AES:256 bits ] that meet the following: [NIST SP800-38A (CBC.AES256)].

**FCS\_COP.1/TDK 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] and cryptographic key sizes [AES:256 bits] that meet the following: [NIST SP800-38A (CBC.AES256)].

**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: [FIPS 180-2].

**FCS\_COP.1/TRMK-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 [decryption] in accordance with a specified cryptographic algorithm [AES in CBC mode] and cryptographic key sizes [256 bits] that meet the following: [NIST SP800-38A (CBC.AES256)].

**FCS\_COP.1/TRMKD-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 [decryption] in accordance with a specified cryptographic algorithm [AES in CBC mode] and cryptographic key sizes [256 bits] that meet the following: [NIST SP800-38A (CBC.AES256)].

**FCS\_COP.1/PUB-ENC 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] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [2048 bits] that meet the following: [PKCS#1 v2.1 (RSAES-PKCS1-v1\_5) ].

**FCS\_COP.1/SIGN-VER 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 [signature verification] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [2048 bits] that meet the following: [PKCS#1 v1.5, SHA256 Type 2 (random padding)].

**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 and 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].

### Class FDP User Data Protection

#### 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],

[none].

***Application Note 3:*** *FCR Authorised User have access rights to secure state mode and Authorized Manufacturer User has access rights to access maintenance mode.*

***Application Note 4:*** *Parameters of new generation cash register fiscal application software functions and exchange rates are specified in PRA Messaging Protocol Document [6].*

#### 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],

[none]

**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 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].

#### 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: [Communication with secure messaging according to PRA Messaging Protocol Document [6]].

***Application Note 5:*** *User data (sales data, event data and TRMK) are exported from FCR to the PRA-IS via TSM and TRMKD are exported from FCR to TSM.*

**FDP\_ETC.2 /EFTPOS/SMARTPINPAD 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/SMART PINPAD 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]].

#### 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, TREK, TRAK and TDK, TRMK and TRMKD) as specified in PRA Messaging Protocol Document [6]].

**FDP\_IFC.1/EFTPOS/SMARTPINPAD** **COMMUNICATION 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/SMART PINPAD Device] on [subjects (EFT-POS/SMART PINPAD) and objects (amount information in sale's data and outcome of the operation) as specified in External Device Communication Protocol Document [7]].

#### 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, event data reports and TRMK to PRA-IS by using subject identifier(IP/Port information) and object identifier (file name); TOE has ability to receive TREK and TRAK from PRA-IS by using subject identifier (IP/Port information) and object identifier (information label)according to PRAMessaging ProtocolDocument[6];TOE has ability to receive FCR parameters and TDK from TSM by using subject identifier (IP/Port information) and object identifier (information label) according to PRA Messaging Protocol Document [6]; TOE has ability to send TRMKD to 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: [Communication with secure messaging according to PRA Messaging Protocol Document [6]].

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

TOE has ability to receive outcome of the operation conducted by the EFT-POS/SMART PINPAD 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].

#### 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: [Communication with secure messaging according to PRA Messaging Protocol Document [6]].

***Application Note 6:*** *FCR parameters and TDK are imported from TSM to TOE. TREK and TRAK are imported from PRA-IS to TOE.*

**FDP\_ITC.2/EFTPOS/SMARTPINPAD 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/SMART PINPAD 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 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: [Communication with secure messaging according to External Device Communication Protocol Document [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 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].

### Class FIA Identification and Authentication

#### 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].

#### FIA\_UAU User authentication

**FIA\_UAU.1 Timing of authentication**

Hierarchical to: No other components.

Dependencies: FIA\_UID.1 Timing of identification

**FIA\_UAU.1.1** The TSF shall allow [to do fiscal sales and to get FCR reports (except fiscal reports)] on behalfof the user to be performed before the user is authenticated.

**FIA\_UAU.1.2** 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].

#### FIA\_UID User Identification

**FIA\_UID.1 Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA\_UID.1.1** The TSF shall allow [to do fiscal sales and to get FCR reports (except fiscal reports)] on behalf of the user to be performed before the user is identified.

**FIA\_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

### Class FMT Security Management

#### 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 7:*** *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 8:*** *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.*

#### FMT\_MSA Management of security attributes

**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 and Access Control List] 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/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/EFTPOS/SMARTPINPAD 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/SMARTPINPAD Device] to restrict the ability to ***[modify]*** the security attributes [Source Port] to [none].

**FMT\_MSA.1/ EFT-POS/SMARTPINPAD 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/SMARTPINPAD 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/SMARTPINPAD 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.

#### FMT\_MTD Management of TSF data

**FMT\_MTD.1/** **FCR AUTHORISED 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/ AUTHORIZED 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’sauthentication data ] to ~~[assignment: the authorised identified roles]~~ [**nobody**].

***Application Note 9:*** *No* authorised identified roles *make the changes on Authorized Manufacturer User’s**authentication data, but TSM creates it.*

#### 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], [Authorised Manufacturer User modifies time information and resets FCR Authorised User’s Authentication Data].

#### FMT\_SMR Security management roles

**FMT\_SMR.2 Restrictions on security roles**

Hierarchical to: FMT\_SMR.1 Security roles

Dependencies: FIA\_UID.1 Timing of identification

**FMT\_SMR.2.1** The TSF shall maintain the roles:[FCR Authorised User, Authorized Manufacturer User].

**FMT\_SMR.2.2** The TSF shall be able to associate users with roles.

**FMT\_SMR.2.3** The TSF shall ensure that the conditions [Authorized Manufacturer User shall take action in maintenance works, FCR Authorised User takes action in secure state works] are satisfied.

### Class FPT Protection of the TSF

#### 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].

#### 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 [all users] when physical tampering with the TSF's devices or TSF's elements has occurred.

#### 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 occur] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

**FPT\_RCV.4 Function recovery**

Hierarchical to: 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.

#### 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.

#### FPT\_TDC Inter-TSF TSF data consistency

**FPT\_TDC.1/TSM 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 [Communication with secure messaging according to PRA Messaging Protocol Document [6]] when interpreting the TSF data from another trusted IT product.

**FPT\_TDC.1/EFT-POS/SMART PINPAD 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 [Communication with secure messaging according to External Device Communication Protocol Document [7]] when interpreting the TSF data from another trusted IT product.

#### 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 PRA Messaging Protocol Document [6]].

***Application Note 10:*** *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 [accuracy of time information].

**FPT\_TEE.1.2** If the test fails, the TSF shall [not execute time syncronization with NTP].

### Class FTP Trusted Path/Channels

#### FTP\_ITC Inter-TSF trusted channel

**FTP\_ITC.1/TSM 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 [sending user data (sales, event data and TRMK) to PRA-IS and receiveing user data (FCR parameters, exchange rates and TDK) from TSM; receiveing user data (TREK and TRAK) from PRA-IS; sending user data (TRMKD) to TSM].

**FTP\_ITC.1/EFT-POS/SMART PINPAD 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 [sending amount information to EFT-POS/SMART PINPAD and receiving outcome of the operation from EFT-POS/SMART PINPAD].

## 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.

## Security Requirements Rationale

#### .Security Functional Requirements Rationale

Table 4 provides an overview for security functional requirements coverage also giving an evidance for sufficiency and necessity of the SFRs chosen.

Table 4 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/TRMK | Cryptographic key generation |  |  |  |  |  | X |
| FCS\_CKM.1/TRMKD | Cryptographic key generation |  |  |  |  |  | X |
| FCS\_CKM.2 | Cryptographic key distribution |  |  |  |  |  | X |
| FCS\_CKM.1/ DHE-KEY | Cryptographic key generation |  |  |  |  |  | X |
| FCS\_CKM.1/EXT-DEV KENC  | Cryptographic key generation |  |  |  |  |  | X |
| FCS\_CKM.1/ EXT-DEV KHMAC | Cryptographic key generation |  |  |  |  |  | X |
| FCS\_CKM.4 | Cryptographic key destruction |  |  |  |  |  | X |
| FCS\_COP.1/TREK | Cryptographic operation |  |  |  |  |  | X |
| FCS\_COP.1/TRAK | Cryptographic operation |  |  |  |  |  | X |
| FCS\_COP.1/TDK | Cryptographic operation |  |  |  |  |  | X |
| FCS\_COP.1/HASHING | Cryptographic operation |  |  |  | X |  |  |
| FCS\_COP.1/TRMK-DEC | Cryptographic operation |  |  |  |  |  | X |
| FCS\_COP.1/TRMKD-DEC | Cryptographic operation |  |  |  |  |  | X |
| FCS\_COP.1/PUB-ENC | Cryptographic operation |  |  |  |  |  | X |
| FCS\_COP.1/SIGN-VER | Cryptographic operation |  |  |  |  |  | X |
| FCS\_COP.1/EXT-DEV KENC | Cryptographic operation |  |  |  |  |  | X |
| FCS\_COP.1/EXT-DEV KHMAC | 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/SMART PINPAD | Export of user data with security attributes |  |  |  |  |  | X |
| FDP\_IFC.1/TSMCOMMUNICATION | Subset information flow control |  |  |  |  |  | X |
| FDP\_IFC.1/EFTPOS/SMART PINPADCOMMUNICATION | Subset information flow control |  |  |  |  |  | X |
| FDP\_IFF.1/TSMCOMMUNICATION | Simple security attributes |  |  |  |  |  | X |
| FDP\_IFF.1/EFT-POS/SMART PINPAD COMMUNICATION | Simple security attributes |  |  |  |  |  | X |
| FDP\_ITC.2/TSM | Import of user data with security attributes |  |  |  |  |  | X |
| FDP\_ITC.2/EFTPOS/SMART PINPAD | 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.1 | Timing of authentication |  |  |  | X |  |  |
| FIA\_UAU.4 | Single-use authentication mechanisms |  |  |  | X |  |  |
| FIA\_UID.1 | Timing of identification |  |  |  | X |  |  |
| FMT\_MOF.1 | Management of security functions behaviour |  |  |  |  | X |  |
| FMT\_MSA.1/PRIVILEGES | Management of security attributes | X |  |  |  |  |  |
| FMT\_MSA.1/IP:PORT INFO | Management of security attributes |  |  |  |  |  | X |
| FMT\_MSA.1/FILE NAME and INFO-LABEL | Management of security attributes |  |  |  |  |  | X |
| FMT\_MSA.1/EFTPOS/SMART PINPAD SOURCE PORT INFO | Management of security attributes |  |  |  |  |  | X |
| FMT\_MSA.1/EFT-POS/SMART PINPAD LABEL INFO | Management of security attributes |  |  |  |  |  | X |
| FMT\_MSA.3/USERS and SYSTEMS | Static attribute initialisation | X |  |  |  |  | X |
| FMT\_MSA.3/EFTPOS/SMART PINPAD | Static attribute initialisation |  |  |  |  |  | X |
| FMT\_MTD.1/FCR AUTHORİSED USER | Management of TSF data | X |  |  | X |  |  |
| FMT\_MTD.1/ AUTHORİZED 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/TSM | Inter-TSF basic TSF data consistency |  |  | X |  |  |  |
| FPT\_TDC.1/ EFT-POS/SMART PINPAD | 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 |  |
| FTP\_ITC.1/TSM | Inter-TSF trusted channel |  |  |  |  |  | X |
| FTP\_ITC.1/EFT-POS/SMART PINPAD | 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 5 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/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 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\_TDC.1/TSM | Provides the capability to consistently interpret TSF data (checksum)  |
| FPT\_TDC.1/EFT-POS/SMART PINPAD | 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.1 | Defines user authentication before allowing to do fiscal sales |
| FIA\_UAU.4 | Provides single use authentication mechanism for Autharised Manufacturer User |
| FIA\_UID.1 | Defines user identification before allowing to do fiscal sales |
| FMT\_MTD.1/ FCR AUTHORİSED USER | Provides authorised processing of FCR Authorised User’s authentication data |
| 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 registerfiscal application software start workingin maintenance mode in failure. (hasability to switch to the secure stateautomatically with functions) |
| FPT\_TEE.1/EXT | Provides test for IT environment for functioning accurately |
| FPT\_TEE.1/TIME | Provides test for time information for accuracy |
| O.Transfer | FCS\_CKM.1/TRMK | Generates session keys for communication between FCR-PRA-IS and FCR–TSM |
| FCS\_CKM.1/TRMKD | Generates session keys for communication between FCR-PRA-IS and FCR–TSM |
| FCS\_CKM.2 | Provides cryptographic key distribution to genarate keys  |
| FMT\_MSA.1/ EFT-POS/SMART PINPAD LABEL INFO | Provides the functions to restrict the ability to modify the security attribute(EFT-POS/SMART PINPAD 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/SMART PINPAD SOURCE PORT INFO | Provides the functions to restrict the ability to modify the security attribute(EFT-POS/SMART PINPAD 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/SMART PINPAD  | Provides the functions to provide permissive 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/TREK | Provides the cryptographic operation for secure communication between PRA-IS and TOE |
| FCS\_COP.1/TRAK | Provides authentication and integrity protection for comminication between PRA-IS and TOE |
| FCS\_COP.1/TDK | Provides the cryptographic operation for secure communication between TSM and TOE |
| FCS\_COP.1/TRMK-DEC | Provides the cryptographic operation for secure communication between PRA-IS and TOE |
| FCS\_COP.1/TRMKD-DEC | Provides the cryptographic operation for secure communication between TSM and TOE |
| FCS\_COP.1/PUB-ENC | Provides the cryptographic operation for secure communication between PRA-IS-TOE and TOE-TSM |
| FCS\_COP.1/SIGN-VER | Provides non-repuduation for TREK and TRAK sharing between PRA-IS and TOE. Provides non-repuduation for FCR parameters which are transfered to the FCR from TSM |
| FCS\_COP.1/HASHING  | Provides the cryptographic operation for secure communication between PRA-IS-TOE and TOE-TSM |
| FCS\_COP.1/EXT-DEV KENC | Provides symmetric encryption in order to establish secure communication with External Devices.  |
| FCS\_COP.1/ EXT-DEV KHMAC | Provides authentication and integrity protection for comminication with External Devices. |
| FCS\_CKM.1/ DHE-KEY | Generates private key for DHE key agreement |
| FCS\_CKM.1/ EXT-DEV KENC  | Generates keys for communication between TOE and External Devices |
| FCS\_CKM.1/ EXT-DEV KHMAC | Generates keys for communication between TOE and External Devices |
| FCS\_COP.1/ EXT-DEV KEYEXCHANGE | Provides key transport operation with External Devices |
| 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/EXT-DEV | Generates keys for communication between FCR-EFTPOS/SMART PINPAD |
| FCS\_COP.1/ EXT-DEV KEYEXCHANGE | Provides asymmetric decryption for secure exchange of the symmetric key with EFT-POS/SMART PINPAD |
| FDP\_ETC.2/TSM | Provides export of sales 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/SMART PINPAD | Provides export of amount information in sales data from the TOE to the EFT-POS/SMART PINPAD using the information flow control SFP with EFT-POS/SMART PINPAD Devices  |
| FDP\_IFC.1/TSMCOMMUNICATION | Provides information flow control policy for TSM and PRA-IS communication |
| FDP\_IFC.1/EFTPOS/SMART PINPADCOMMUNICATION | Provides information flow control policy for EFT-POS/SMART PINPAD communication |
| FDP\_IFF.1/TSMCOMMUNICATION | Provides information flow control policy rules for TSM and PRA-IS communication |
| FDP\_IFF.1/EFTPOS/SMART PINPADCOMMUNICATION | Provides information flow control policy rules for EFT-POS/SMART PINPAD communication |
| FDT\_ITC.2/TSM | Provides protection of FCR Parameters confidentiality and integrity during import from TSM |
|  FDT\_ITC.2/EFTPOS/SMART PINPAD | Provides protection of confidentiality and integrity of outcome of the operation conducted by the EFT-POS/SMART PINPAD device and AES keys (KENC and KHMAC) during import from EFT-POS/SMART PINPAD device |
|  FTP\_ITC.1/EFTPOS/SMART PINPAD | Provides protection of data (confidentiality+integrity) during communication with EFT-POS/SMART PINPAD by the help of secure channel |
|  FTP\_ITC.1/TSM | Provides protection of sales data and event data (confidentiality+integrity) during communication with PRA-IS by the help of secure channel |

#### .Rationale for Security Functional Requirements dependencies

Selected security functional requirements include related dependencies. Table 6 below provides a summary of the security functional requirements dependency analysis.

Table 6 Security Functional Requirements dependencies

|  |  |  |
| --- | --- | --- |
|  | 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 | Non-repudiation of the origin satisfied for the event and sales data send from FCR not on behalf of each user but FCR itself.Requirement satisfied but the dependency is not fulfilled because of the operational requirement. |
| FCS\_CKM.1/TRMK | FCS\_CKM.2 or FCS\_COP.1;FCS\_CKM.4 | FCS\_CKM.2; FCS\_COP.1 TRMK-DEC; FCS\_CKM.4 included |
| FCS\_CKM.1/TRKMD | FCS\_CKM.2 or FCS\_COP.1;FCS\_CKM.4 | FCS\_CKM.2; FCS\_COP.1/TRMKD-DEC;FCS\_CKM.4 included |
| FCS\_CKM.2 | [FDP\_ITC.1 or FDP\_ITC.2 orFCS\_CKM.1]; FCS\_CKM.4  | FCS\_CKM.1 (FCS\_CKM.1/TRKMD and FCS\_CKM.1/TRMK); FCS\_CKM.4 |
| 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.1/ EXT-DEV KENC  | 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 KHMAC | FCS\_CKM.2 or FCS\_COP.1;FCS\_CKM.4 | FCS\_COP.1/ EXT-DEV KHMAC and FCS\_CKM.4 included |
| FCS\_CKM.4 | FDP\_ITC.1 or FDP\_ITC.2 or FCS\_CKM.1 | FCS\_CKM.1(FCS\_CKM.1/ EXT-DEV KENC, FCS\_CKM.1/ EXT-DEV KHMAC, FCS\_CKM.1/TLS\_HMAC, FCS\_CKM.1/TLS\_AES and FCS\_COP.1/ EXT-DEV KEYEXCHANGE) included |
| FCS\_COP.1/TREK | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_CKM.1 ;FCS\_CKM.4 | FDP\_ITC.2/TSM andFCS\_CKM.4 included |
| FCS\_COP.1/TRAK | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_CKM.1 ;FCS\_CKM.4 | FDP\_ITC.2/TSM andFCS\_CKM.4 included |
| FCS\_COP.1/TDK | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_CKM.1 ;FCS\_CKM.4 | FDP\_ITC.2/TSM andFCS\_CKM.4 included |
| FCS\_COP.1/HASHING | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_CKM.1 ;FCS\_CKM.4 | No need to include any dependencies because there is no need to use any key for HASHING |
| FCS\_COP.1/TRMK-DEC | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_CKM.1 ;FCS\_CKM.4 | FCS\_CKM.1/TRMK; FCS\_CKM.4 |
| FCS\_COP.1/TRMKD-DEC | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_CKM.1 ;FCS\_CKM.4 | FCS\_CKM.1/TRMKD; FCS\_CKM.4 |
| FCS\_COP.1/PUB-ENC | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_CKM.1 ;FCS\_CKM.4 | According to PRA messaging protocol, there is no need to import key for this SFR. Key is imported during initialization.According to PRA mesaging protocol, PPRA and PTSM public key should not be deleted. Tamper system of the TOE protects keys from misuse, disclosure or modification.  |
| FCS\_COP.1/SIGN-VER | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_CKM.1 ;FCS\_CKM.4 | According to PRA messaging protocol, there is no need to import key for this SFR. Key is imported during initialization.According to PRA messaging protocol, PPRA-SIGN , PTSM-SIGN public key should not be deleted. Tamper system of the TOE protects keys from misuse, disclosure or modification.  |
| FCS\_COP.1/EXT-DEV KENC | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_CKM.1 ;FCS\_CKM.4 | FCS\_CKM.1/ EXT-DEV KENC ; FCS\_CKM.4 included  |
| FCS\_COP.1/ EXT-DEV KHMAC | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_CKM.1 ;FCS\_CKM.4 | FCS\_CKM.1/ EXT-DEV KHMAC; FCS\_CKM.4 included |
| FCS\_COP.1/ EXT-DEV KEYEXCHANGE | FDP\_ITC.1 orFDP\_ITC.2 orFCS\_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 orFDP\_IFC.1 | FDP\_ACC.1; FDP\_IFC.1/TSMCOMMUNICATION included |
| FDP\_ETC.2 /EFTPOS/SMART PINPAD | FDP\_ACC.1 orFDP\_IFC.1 | FDP\_ACC.1;FDP\_IFC.1/EFTPOS/SMART PINPADCOMMUNICATION included |
| FDP\_IFC.1/TSMCOMMUNICATION | FDP\_IFF.1 | FDP\_IFF.1/TSMCOMMUNICATION included |
| FDP\_IFC.1/EFTPOS/SMART PINPADCOMMUNICATION | FDP\_IFF.1 | FDP\_IFF.1/EFT-POS/SMART PINPAD COMMUNICATION included |
| FDP\_IFF.1/TSMCOMMUNICATION | FDP\_IFC.1;FMT\_MSA.3 | FDP\_IFC.1/TSMCOMMUNICATION; FMT\_MSA.3/USERS and SYSTEMS included |
| FDP\_IFF.1/EFT-POS/SMART PINPAD COMMUNICATION | FDP\_IFC.1;FMT\_MSA.3 | FDP\_IFC.1/EFTPOS/SMART PINPADCOMMUNICATION; FMT\_MSA.3/EFTPOS/SMART PINPAD included |
| FDP\_ITC.2/TSM | FDP\_ACC.1 orFDP\_IFC.1 ;FTP\_ITC.1 orFTP\_TRP.1 ;FPT\_TDC.1 | FDP\_IFC.1/TSMCOMMUNICATION; FTP\_ITC.1/TSM; FPT\_TDC.1/TSM included |
| FDP\_ITC.2/EFTPOS/SMART PINPAD | FDP\_ACC.1 orFDP\_IFC.1 ;FTP\_ITC.1 orFTP\_TRP.1 ;FPT\_TDC.1 | FDP\_IFC.1/EFTPOS/SMART PINPADCOMMUNICATION; FTP\_ITC.1/EFT-POS/SMART PINPAD; FPT\_TDC.1/EFT-POS/SMART PINPAD included |
| FDP\_SDI.2/MEMORY | No dependencies. | - |
| FDP\_SDI.2/DAILY and PRMTR | No dependencies. | - |
| FIA\_AFL.1/MANUFACTURER | FIA\_UAU.1 | included |
| FIA\_AFL.1/AUTHORISED | FIA\_UAU.1 | included |
| FIA\_UAU.1 | FIA\_UID.1 | included |
| 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/PRIVILEGES | FDP\_ACC.1 orFDP\_IFC.1 | FDP\_ACC.1 included |
| FMT\_MSA.1/ IP:PORT INFO | FDP\_ACC.1 orFDP\_IFC.1 | FDP\_IFC.1/TSMCOMMUNICATION included |
| FMT\_MSA.1/FILE NAME and INFO-LABEL | FDP\_ACC.1 orFDP\_IFC.1 | FDP\_IFC.1/TSMCOMMUNICATION included |
| FMT\_MSA.1/EFTPOS/SMART PINPAD SOURCE PORT INFO | FDP\_ACC.1 orFDP\_IFC.1 | FDP\_IFC.1/EFTPOS/SMART PINPADCOMMUNICATION included |
| FMT\_MSA.1/ EFT-POS/SMART PINPAD LABEL INFO | FDP\_ACC.1 orFDP\_IFC.1 | FDP\_IFC.1/EFTPOS/SMART PINPADCOMMUNICATION included |
| FMT\_MSA.3/USERS and SYSTEMS | FMT\_MSA.1 ;FMT\_SMR.1 | FMT\_MSA.1(MT\_MSA.1/PRIVILEGES,FMT\_MSA.1/IP:PORT INFO andFMT\_MSA.1/FILE NAME and INFO-LABEL) included ;FMT\_SMR.1 is hierarchical to FMT\_SMR.1 included |
| FMT\_MSA.3/EFTPOS/SMART PINPAD | FMT\_MSA.1 ;FMT\_SMR.1 | FMT\_MSA.1/ EFT-POS/SMART PINPAD LABEL INFO ) ;FMT\_SMR.2 is hierarchical to FMT\_SMR.1 included |
| FMT\_MTD.1/ FCR AUTHORİSED USER | FMT\_SMR.1 ;FMT\_SMF.1 | FMT\_SMR.2 is hierarchical to FMT\_SMR.1 ; FMT\_SMF.1 included |
| FMT\_MTD.1/ AUTHORİZED 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 | 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/TSM | No dependencies | - |
| FPT\_TDC.1/EFT-POS/SMART PINPAD | No dependencies | - |
| FPT\_TEE.1/EXT | No dependencies | - |
| FPT\_TEE.1/TIME | No dependencies | - |
| FTP\_ITC.1/TSM | No dependencies | - |
| FTP\_ITC.1/EFT-POS/SMART PINPAD | No dependencies | - |

#### 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.

#### 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 6 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.

# 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.

## Audit/Event Log Function

Audit/Event Function is going to generate the security 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, FDP\_SDI.2/DAILY and PRMTR

## 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 or SMART PINPAD. In order to install a device to TOE, first a coupling messaging takes place between TOE and EFT-POS.

This Security Function is satisfying the following SFRs;

FCS\_CKM.1/TRMK, FCS\_CKM.1/TRMKD, FCS\_CKM.2, FCS\_CKM.1/DHE-KEY, FCS\_CKM.1/EXT-DEV KENC, FCS\_CKM.1/EXT-DEV KHMAC, FCS\_CKM.4, FCS\_COP.1/TREK, FCS\_COP.1/TRAK, FCS\_COP.1/TDK, FCS\_COP.1/HASHING, FCS\_COP.1/TRMK-DEC, FCS\_COP.1/TRMKD-DEC, FCS\_COP.1/PUB-ENC, FCS\_COP.1/SIGN-VER, FCS\_COP.1/EXT-DEV KENC, FCS\_COP.1/EXT-DEV KHMAC, FCS\_COP.1/EXT-DEV KEYEXCHANGE, FDP\_ETC.2/TSM, FDP\_ETC.2/EFT POS/SMART PINPAD, FDP\_ITC.2/TSM, FDP\_ITC.2/EFTPOS/SMART PINPAD, FTP\_ITC.1/TSM, FTP\_ITC.1/EFT-POS/SMAR PINPAD

## Identification and Authentication Function

Identification and Authentication Function will support the following features;

* Enforce identification and authentication mechanism for the following users;
	+ FCR Authorised User
	+ Authorized Manufacturer User
* Enforce 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.1, FIA\_UAU.4, FIA\_UID.1, FDP\_ITC.2/TSM, FDP\_ETC.2/TSM, FCO\_NRO.2

## Access Control Function

Access Control Function will support the following features;

* Enforce an access control policy for 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

## 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

## Import/Export Function

The TOE will import FCR parameters from TSM according to the protocol defined in PRA Messaging Protocol Document [6].

The TOE will import TREK and TRAK from PRA-ISfor cryptographic operations according to the protocol defined in PRA Messaging Protocol Document [6].

The TOE will import TDK from TSMfor cryptographic operations according to the protocol defined in PRA Messaging Protocol Document [6].

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 TSM according to the protocol defined in PRA Messaging Protocol Document [6] :

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\_ETC.2/EFT-POS/SMART PINPAD, FDP\_IFF.1/ EFT-POS/SMART PINPAD COMMUNICATION, FDP\_IFC.1/ EFT-POS/SMART PINPAD COMMUNICATION, FDP\_ITC.2/ EFT-POS/SMART PINPAD, FTP\_ITC.1/TSM, FTP\_ITC.1/EFT-POS/SMART PINPAD

## 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

## 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. Function makes LRC check on the imported messages and rejects the data packets which fail at LRC check. This will provide integrity control during transmission with TSM and PRA-IS.

Data Preparation Function uses LRC calculation when communicating with EFTPOS/Smart Pinpad devices. It appends LRC to all exported messages and makes LRC check for all imported messages according to the rules defined in External Device Communication Protocol Document [7].

This Security Function is satisfying the following SFRs;

FPT\_TDC.1/TSM, FPT\_TDC.1/EFT-POS/SMART PINPAD

## 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.

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\_TEE.1/EXT, FPT\_TEE.1/TIME

## TSF Management Function

TSF Management Function provides management and initialisation functions for security attributes that are used to enforce the SFP (Administrative Access Control SFP,Information Flow Control SFP with TSM and PRA-IS and Information Flow Control SFP with EFT\_POS/SMART PINPAD Device)

Security attributes are listed below;

* Privileges for users (Subject Attributes)
* Access Control List for user access rights (Object Attributes)
* File name of sales and event data within FCR
* Information label (TAG) for PRA Messaging packets (object identifier)
* IP:Port Information of TSM (subject identifier)
* Source Port that is determined by FCR (subject identifier)
* EFT-POS/SMART PINPAD Label that is used to identify different devices(subject identifier)

TSF Management Function provides management functions in order to manage the security roles and users which also contains the policy (Administrative Access Control SFP) for maintenance mode operations and secure state operations. TOE explicitly prevents changes on the behaviour of its functions (FCR parameters) for all users however FCR Parameters can be updated by only TSM.

This Security Function is satisfying the following SFRs;

FMT\_MOF.1, FMT\_MSA.1/PRIVILEGES, FMT\_MSA.1/IP:PORT INFO, FMT\_MSA.1/FILENAME and INFO-LABEL, FMT\_MSA.1/EFTPOS/SMARTPINPAD SOURCE PORT INFO, FMT\_MSA.1/EFTPOS/SMARTPINPAD LABEL INFO, FMT\_MSA.3/USERS and SYSTEMS, FMT\_MSA.3/EFTPOS/SMART PINPAD, FMT\_MTD.1/FCR AUTHORISED USER, FMT\_MTD.1/AUTHORIZED MANUFACTURER USER, FMT\_SMF.1, FMT\_SMR.2

# 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 (TK2) Document, current version

[6] PRA Messaging Protocol (for TK2) Document, current version

[7] External Device Communication Protocol Document, current version