NCR E10 New Generation FCR

Security Target

Document Attributes

File name:	Security Target NCR E10.pdf
Status:	Published
Release Date:	16.10.2017
Version:	2.7
Sensitivity:	Restricted
Author:	Funda ÇETİNTAŞ
Approved by	Okan TUNÇER

Revision Table

Revision No	Revision Date	Explanation	Made by
0.1	22.11.2013	First Draft	Saadet Gökçe Ekiz
0.2	25.11.2013	TSF Updated	Saadet Gökçe Ekiz
0.3	19.04.2014	TSF Explanations and rational updated	Saadet Gökçe Ekiz
0.4	10.06.2014	Minor updates on SFRs	Saadet Gökçe Ekiz
0.5	17.11.2014	Updated according to updated Protection Profile	Saadet Gökçe Ekiz
0.6	02.01.2015	Updated according to Protection Profile v1.8	Saadet Gökçe Ekiz
0.7	06.01.2015	Updated according to labratory observation	Funda Çetintaş
0.8	07.01.2015	Updated according to labratory second observation	Funda Çetintaş
0.9	08.01.2015	7.3.1 Check	Funda Çetintaş
0.9.1	09.01.2015	Final draft	Funda Çetintaş
1.0	5.2.2015	Updated per new authorization rules	Funda Çetintaş
1.1	6.3.2015	Updated according to observations	Funda Çetintaş
2.0	03.06.2015	Updated according to updated PP 2.0 version	Funda Çetintaş
2.1	13.09.2015	Minor changes	Funda Çetintaş
2.2	12.10.2015	Minor changes	Funda Çetintaş
2.3	24.11.2015	TOE parts definition updated	Funda Çetintaş
2.4	27.11.2015	Minor Change	Funda Çetintaş
2.5	01.02.2016	Open SSL v, FIA class reorg.	Funda Çetintaş
2.6	19.09.2017	TSE review updates	Ufuk Öz
2.7	16.10.2017	Review updates	Ufuk Öz

Table of Contents

LIST OF FIGURES

LİST OF TABLES

1. INTRODUCTION

1.1. ST Reference

ST Title	NCR E10 New Generation FCR Security Target
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 4)
Version Number	2.7
Status	Released

1.2. TOE Reference

TOE Identification	NCR E10 New Generation FCR 2.0 (FCR Application Version 2.0, OpenSSL Version 1.0.2d Secure-IC firmware and hardware crypto library Version 0.0.6)
CC Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 4)
PP Conformance	COMMON CRITERIA PROTECTION PROFILE for NEW GENERATION CASH REGISTER FISCAL APPLICATION SOFTWARE (NGCRFAS PP), version 2.0, 06 May 2015
Assurance Level Evaluation	Assurance Level 2

1.3. TOE Overview

The TOE addressed by this Security Target (ST) is a NCR E10 New Generation FCR 2.0 application and crypto library (includes OpenSSL (version 1.0.2d) library, Secure IC firmware and hardware crypto library) which are the main items of a Fiscal Cash Register (FCR). TOE is used to process the transaction amount of purchases which can be viewed by both seller and buyer. Since transaction amount is used to determine tax revenues; secure processing, storing and transmission of this data is very important.

The FCR is mandatory for first-and second-class traders and is not mandatory for sellers who sell the goods back to their previous seller as completely the same as the purchased good.

In addition to TOE, which is the main item of FCR, FCR may consist of several other hardware and software components as described in Section 1.3.2 for full functionality. TOE and related components are given in Figure 1. Usage and major security features of TOE are described in section 1.3.3.

1.3.1. General overview of the TOE and related components

Figure 1 shows the general overview of the TOE and its related components as regarded in this ST. The green part of Figure 1 is the TOE. Yellow parts given as Input/output interface, fiscal memory, daily memory, database, ERU, fiscal certificate memory are TOE's environmental components which are crucial parts of the FCR 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.

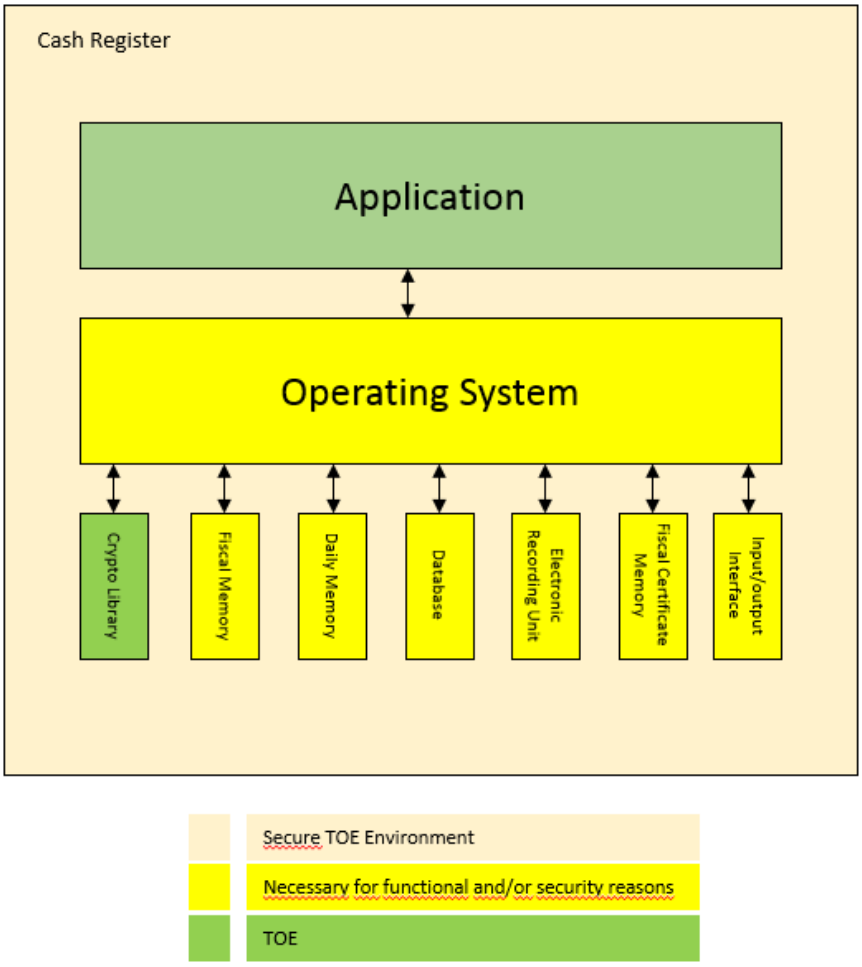

Figure 1 TOE and related components

1.3.2. Required Non-TOE Hardware/Software

Software and hardware environment of the TOE are described below.

1.3.2.1. Software environment of TOE

Application runs on 32-bit GNU/Linux Angstrom operating system version 2.6.39 angstrom armv5tejl 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 necessary for security and functionality of the FCR:

- Application (FCR) runs on an operating system which supports following features
  - at least 32-bit data processing capacity
  - multi-processing
  - IPv4 and IPv6
  - NTP (Network Time Protocol)
- Database which is used to store sales data, has the following features;
  I. Database has data recording, organizing, querying, reporting features
  II. Database stores sales records for main product groups (food, clothing, electronics, glassware etc.) and sub-product groups (milk, cigarette, fruit, trousers etc.) in order to track detailed statistics
  III. Database has an indexing mechanism

1.3.2.2. Hardware Environment of TOE

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

- **Fiscal memory**

i. Fiscal memory has following features;
   a. Fiscal memory has the capacity to store at least 10 years (3650 days) of data,
   b. Fiscal memory keeps data at least 5 years after the capacity specified in (a) has been reached,
   c. Fiscal memory has to be fixed within FCR in a way that it cannot be removed without damaging the chassis.
   d. Fiscal memory is protected by mesh cover,
   e. Fiscal memory has the ability to be protected against magnetic and electronic threats, When the connection between fiscal memory and main processor is broken, FCR enters in maintenance mode,
   f. The data stored in the fiscal memory is not be lost in case of power off,
   g. Fiscal memory accepts only positive amounts from the application and the peripherals,
   h. FCR checks "Z" reports from fiscal memory during device start-up. In case where there are days for which Z report was not generated, FCR will be able to run in normal mode only after it generates Z report for the missing days. Seasonal firms can take cumulative Z report by specifying date and time range.

ii. Fiscal Memory includes following data;
   a. Fiscal symbol, company code, identification number of the device,
   b. Cumulative sum of the total sales amount and Value Added Tax (VAT) amounts of all sales receipts, starting from the device activation time (i.e. first use),
   c. Date and number of daily "Z" reports with total sales and VAT per day,
   d. The number of receipts per day.

- **Daily memory** has following features;

i. Receipt total and total VAT amount for each receipt are to be stored in the daily memory instantly. This data can be transmitted to PRA - IS, instantly or daily depending on demand.
ii. Data in the daily memory which is not already transmitted to fiscal memory, cannot be modified in an uncontrolled way.
iii. Data transmitted from daily memory to fiscal memory is to be kept in daily memory for at least 10 days.
iv. Z reports, taken at the end of the day; and X reports, taken within the current day are produced by using the data in the daily memory.
v. Following values are stored in the daily memory
   a. total VAT amount per day,
   b. total daily sales values per day grouped by payment type
   c. payment type (Cash, credit card etc.)
   d. number of receipts.

- FCR supports X.509 formatted digital certificate generated by Authorized Certificate Authority. This **Public Key Infrastructure (PKI)** compatible digital certificate is called **fiscal certificate** and is used for authentication and secure communication between PRA-IS and FCR through Trusted Service Manager (TSM). For physical security, FCR is protected by electronic and mechanic systems called **electronic seal**. FCR uses **cryptographic library** for secure communication with PRA-IS and TSM
- **Electronic Record Unit(ERU)** is used to keep second copy of the receipt and has following features;

i. ERU stores information about receipts and FCR reports (Except ERU Reports) in a retrievable form.
ii. ERU is included in the sealed part of the FCR. ERU has 140 million row capacity.
iii. Data stored in ERU cannot be modified
iv. ERU also has features specified in "*Fiscal Cash Register General Communique Serial Number: 67*", part A" which is about Law No: 3100 except item (ii) above.

- FCR devices has ETHERNET interface for communication with PRA-IS (for data transfer) and TSM system (for parameter management and software update). External ETHERNET may be accepted as internal in case the data is encrypted in fiscal unit.
- Incoming and outgoing data traffic for FCR passes over a **firewall**.
- FCR has a **printer** to print sales receipt.
- FCR supports the use of **EFT-POS/SMART PINPAD**.
- FCR needs some input/output devices for functionalities listed below;

i. FCR has separate displays for **cashier and buyer**
ii. FCR has a **keyboard unit**
iii. FCR has **internal battery** to keep time information, to protect event data and fiscal memory.

1.3.3. TOE major security features for operational use

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

1.3.3.1. TOE functional features

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

i. TOE stores sales data in fiscal memory.
ii. TOE stores total receipt and total VAT amount for each receipt in daily memory.
iii. TOE is able to generate reports (X report, Z report etc.).
iv. TOE is able to transmit Z reports, receipt information, sale statistics and other information determined by PRA to PRA-IS in PRA Messaging Protocol format.
v. TOE 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.
vi. TOE is able to be used by users in secure state mode or maintenance mode. Roles and modes of operation are described in 3.1.2 and 3.1.3 respectively.

1.3.3.2. TOE major security features

The TOE provides following security features;

i. TOE supports access control.
ii. TOE has ability to detect disconnection between main processor and fiscal memory and enter into the maintenance mode.
iii. TOE supports usage of ITU X509 v3 formatted certificate and its protected private key for authenticating against PRA-IS and establishing a secure communication with PRA-IS and TSM.
iv. TOE supports secure communication between FCR, PRA-IS and FCR TSM.
v. TOE supports secure communication with EFT-POS /SMART PINPAD
vi. TOE ensures the integrity of event data, sales data, authentication data, characterization data and FCR parameters.
vii. TOE records important events defined in PRA Messaging Protocol Document [6] and send urgent event data to PRA-IS in a secure way.
viii. TOE detects physical attacks to FCR and enters into the maintenance mode in such cases.

1.3.4. TOE Type

TOE is a set of embedded software application and hardware and software crypto library within FCR.

The parts of TOE are

- Secure-IC firmware and hardware crypto engine. (Module with its own micro controller, MAXIM MAX32550)
- Fiscal Application (Main software processes fiscal and other security related operations)
- Crypto Library (library used for cryptographic operations includes OpenSSL library)

1.3.5. Non-TOE hardware/software/firmware

Fiscal Cash Register Component diagram is given in Figure 2 and printer contains TOE and necessary environment for operating TOE. Other EFT POS Device, Keyboard, Sales Software, Cashier display, Scale, Customer display and barcode reader are although parts of Fiscal Cash register, they are not part of Target of evaluation.

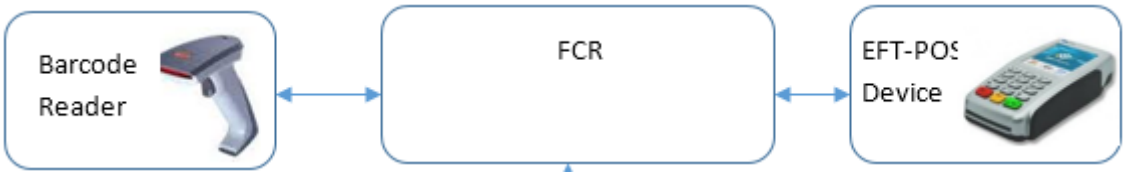

Figure 2 Fiscal Cash Register Component Diagram

1.4. TOE Description

The target of evaluation (TOE) is the NCR E10 New Generation FCR Application software version 2.0.

1.4.1. TOE Boundaries

1.4.1.1. TOE Physical Boundaries

TOE is implemented in Print station shown in Figure 3 and Figure 4 in a plastic case protected by tampering switches. TOE is a firmware and cryptographic library stored in a non-volatile memory. The components of main board are depicted in basic architecture model given in Figure 3 TOE communicates with EFT POS device by RS 232 (POS) interface, with TSM and PRA-IS by Ethernet interface. TOE uses Daily memory, Fiscal Memory, Electronic journal, SD Card for storing Fiscal and security related data and TOE uses Smart Card for Private and public key related cryptographic operations. In addition, TOE uses Secure IC to generate random number, verify digital signatures, encrypt data and store keys. TOE uses Printer for printing receipt, Z reports and other necessary fiscal outputs.

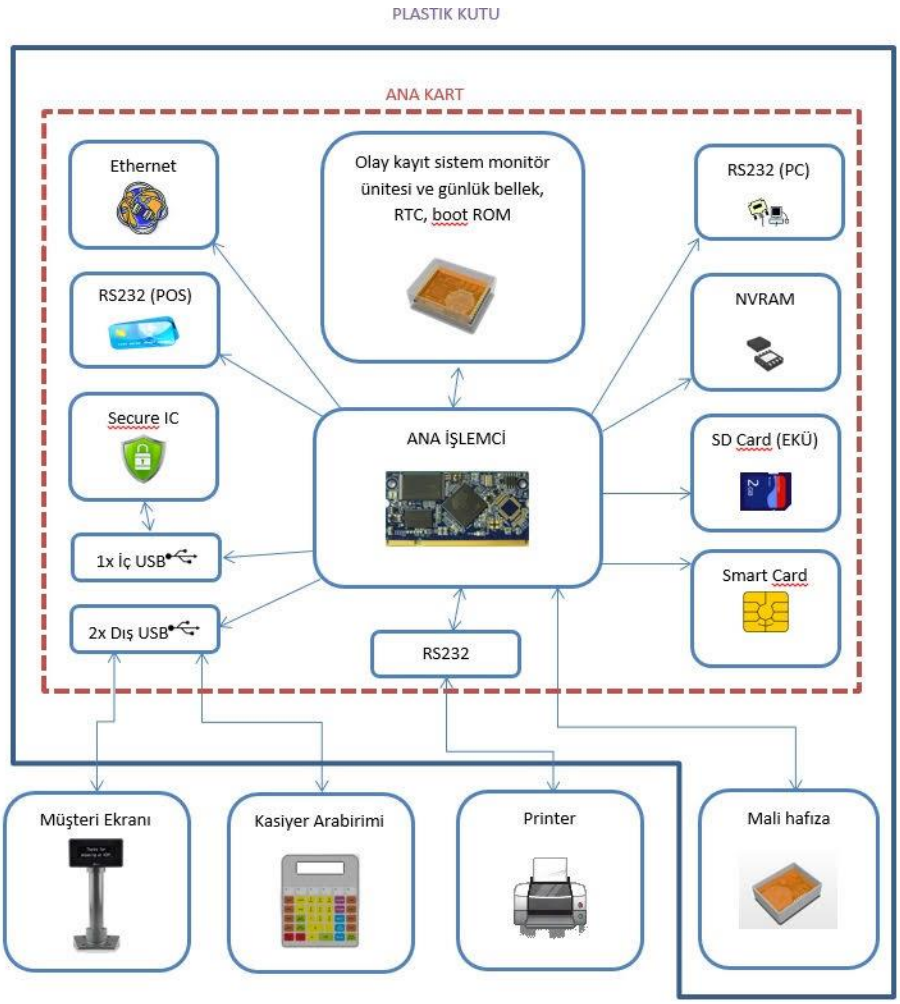

Figure 3 NGFCR Basic Architecture Model

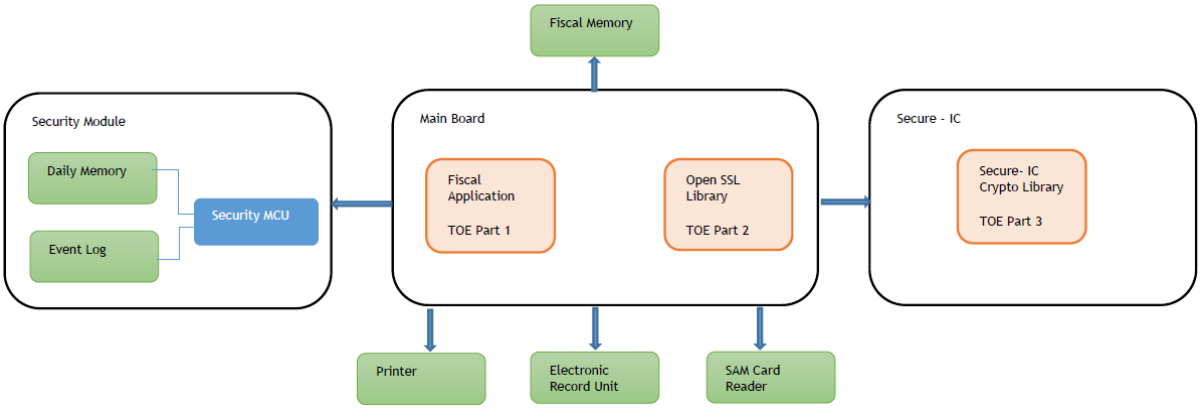

Figure 4 TOE parts

1.4.1.2. TOE Logical Boundaries

The logical boundaries of the TOE include those security functions implemented exclusively by the TOE. These security functions includes accurate fiscal operation, generation security related and fiscal log information and storing in dedicated memories (daily memory, fiscal memory and Electronic Recording Unit), access control for sales data, event data, time information and authentication data, authentication for FCR Authorised User, Authorised Manufacturer User, communication security function (Secure Transfer) with TSM, PRA-IS, EFT-POS Device and Main Unit A more detailed description of the implementation of these security functions is provided in Section 7 “TOE SUMMARY SPECIFICATION”

1.4.2. TOE Guidance Documents

The TOE guidance documentation delivered is listed in Table 6 Assurance Measure- AGD Guidance Documents.

2. CONFORMANCE CLAIMS

2.1. CC Conformance Claims

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

As follows

- Part 2 conformant,
- Part 3 conformant.

The

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

has to be taken into account.

2.2. PP Conformance Claims

This security target claims demonstrable conformance to the protection profile “Common criteria protection profile for new generation cash register fiscal application software (NGCRFAS PP), version 2.0, 06 May 2015.

2.3. Package Claim

The current Security Target is conformant to the following security requirements package:

- Assurance package EAL2 conformant to CC, part 3.

2.4. Conformance Rationale

Since this security target (ST) claims demonstrable conformance with the protection profile (PP) referenced in 2.2 PP Conformance Claims. TOE type is a set of software application run by microprocessor depicted in Figure 1 and it is consistent with the TOE type explained in PP document in chapter 1.2.4 and depicted in Figure 1 in PP document.

Security problem definition, security objectives and security requirements contained in this ST are consistent with those in the PP.

3. SECURITY PROBLEM DEFINITION

3.1. Introduction

3.1.1. External Entities

PRA-IS

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

Trusted Service 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 behaviour and functionality. Attacker tries to breach confidentiality, integrity and availability on the FCR.

PRA On-site Auditor

PRA On-site Auditor is an employee of PRA who performs audits onsite to control the existence of expected FCR functionalities by using the rights of FCR Authorised 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 critical level (urgent, high, warning, information). List of events can be found in PRA messaging protocol document [6].

Storage unit

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

Input interface

Input interfaces provide necessary input data from input devices to the TOE. Input devices for FCR may be keyboard, barcode reader, QR code (matrix barcode) reader, order tracking device or global positioning devices.

External Device

External device is the device which is used to communicate with FCR by using secure channel according to External Device Communication Protocol Document [7]

Output interface

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

3.1.2. Roles

FCR 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.

Authorised Manufacturer User

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

Unauthenticated User

Unauthenticated user operates sales functions, print receipts and simple non fiscal reports.

3.1.3. Modes of FCR

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

- FCR Authorised User;
    - to configure FCR,
    - to take fiscal reports

Secure State Mode is also allows;

- Unauthenticated Users;
    - to do fiscal sales,
    - to get FCR reports (except fiscal reports).

Maintenance Mode

Maintenance Mode is the mode that allow only Authorised Manufacturer User;

- to fix FCR in case of any technical problem,
- to change 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,
- Mesh cover monitoring check fails,
- A disconnection between fiscal memory and main processor occurs,
- Electronic seal is opened, or forced by unauthorised persons
- NCR E10 Application integrity error occurs,
- Event log data and sales data integrity error occurs,
- The state of unable to write to fiscal memory, daily memory and ERU
- First initialisation phase successfully passed

3.1.4. Assets

Sensitive data

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

Sensitive data consists of symmetric keys (TREK, TRAK, TRMK and SSL session keys).

- *TREK is used to provide confidentiality of data transfer to PRA-IS,*
- *TRAK is used to integrity control of data transferred to the PRA-IS,*
- *TRMK is used for key transportation from PRA-IS to TOE,*
- *SSL session keys are used for secure communication with the TSM.*

Event data

Event data is used to obtain information about important events contained in audit storage. The integrity of this asset is crucial while stored in FCR and both integrity and confidentiality of this asset 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 for 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 Users and Authorised Manufacturer User to gain access to FCR functionalities. Both integrity and confidentiality of this asset has to be protected.

Application Note 1: TOE does not use Authentication Data (password) to authenticate Authorised Manufacturer User. A challenge-response application is implemented in TOE and a secondary system which is run in manufacturer premises is used to create a response to authenticate authorised manufacturer user.

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 certificates (P_{PRA} and $PPRA_{-SIGN}$) P_{PRA} and $P_{PRA-SIGN}$ certificates are used for encryption and sign verification process during key transportation between TOE and PRA-IS.

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
- Critical level of event data sent to the PRA-IS
- Maximum number of days that FCR will work without communicating with PRA-IS

3.2. Threats

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

T.AccessControl

Adverse action: Authenticated users could try to use functions which are not allowed. (e.g. FCR Authorised Users gaining access to Authorised Manufacturer User functions)

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

Asset: Event data, sales data, time information.

T. Authentication

Adverse action: Unauthenticated users could try to use FCR functions.

Threat agent: An attacker, who has basic attack potential, has logical and physical access to the FCR except doing fiscal sales and taking reports which are not fiscal.

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 unauthorised access to the FCR, failure reports, and deletion of logs. An attacker also could try to disclose important events while transmitted between PRA-IS and FCR.
- An attacker could try to manipulate or delete the sales data generated by TOE which may result in tax fraud. In addition, an attacker also could try to disclose sales data while transmitted between PRA-IS and FCR. Manipulation and deletion of sales data may be caused by magnetic and electronic reasons.
- An attacker could try to manipulate the characterization data to cover information about tax fraud; to masquerade the user identity.
- An attacker could try to manipulate the FCR parameters to use FCR in undesired condition.
- An attacker also could try to disclose and modify authentication data in FCR

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 and ERU).

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

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

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

Adverse action: An attacker could try to imitate TSM to set parameters to FCR via the communication channel.

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

FCR.

Asset: FCR parameters.

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 and has physical and logical access to the FCR.

Asset: Sensitive data (session keys).

T. Server counterfeiting

Adverse action: An attacker could try to imitate PRA-IS by changing server certificates (P_{PRA} and $P_{PRA-SIGN}$) in FCR. In this way, the attacker could try to receive information from 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.

3.3. Organizational Security Policies

This section describes organizational security policies that must be satisfied.

P.Certificate

It has to be assured that certificate which is installed at initialization step is compatible with ITU X.509 v3 format. FCR contains

- FCR certificate,
- Certification Authority root and sub-root (subordinate) certificate that are used for verification of all certificates that are produced by Certification Authority,
- P_{PRA} certificate that is used for key transport process between FCR and PRA-IS,
- $P_{PRA-SIGN}$ certificate that is used by TOE for signature verification
- Update Control 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 (P_{PRA} $P_{PRA\text{-}SIGN}$, Certification Authority root and sub-root certificates, Update Control certificate, FCR certificates if handled as soft) 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 encrypt 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; i.e by side channel attacks like SPA (Simple power analysis), SEMA (Simple Electromagnetic Analysis), DPA (Differential power analysis), DEMA (Differential electromagnetic analysis).

P.SecureEnvironment

It has to be assured that environment of TOE senses disconnection between fiscal memory and main processor. Then TOE enters into the maintenance mode and logs urgent event.

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.

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 assured that physical tampering protection system (mesh cover) protects fiscal memory.

P.PKI - Public key infrastructure

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

P.UpdateControl

TOE is allowed to be updated by 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 in latest version.

3.4. Assumptions

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

A.TrustedManufacturer

It is assumed that manufacturing is done by trusted manufacturers. They process manufacturing step in a manner which maintains IT security.

A.Control

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

A.Initialisation

It is assumed that environment of TOE provides secure initialization steps. Initialization step consists of secure boot of operating systems, and integrity check for TSF data. Moreover, if certificate is handled as soft (not in the smartcard) it is assumed that environment of TOE provides secure installation of it the FCR in initialization phase. Before certificate installation it is assumed that asymmetric key pair generated in a manner which maintains security posture.

A.TrustedUser

User is assumed to be trusted. It is assumed that for each sale a sales receipt is provided to the buyer.

A.Activation

It is assumed that environment of TOE provides secure activation steps at the beginning of the TOE operation phase and after each maintenance process.

A.AuthorisedService

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

A.Ext_Key

It is assumed that External Device (EFT-POS/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.

4. SECURITY OBJECTIVES

This chapter describes security objectives for the TOE and its operational environment.

4.1. Security Objectives for the TOE

This part describes security objectives provided by the TOE.

O.AccessControl

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

O.Event

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

O.Integrity

TOE must provide integrity for sales data and event data, characterization data, authentication data, sensitive data, 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.

4.2. 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 its 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 should be disabled or removed.

OE.StrongAlgorithm

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

OE.UpgradeSoftware

FCR software Updates should be get pass verdict from Common Criteria maintenance or reevaluation procedures (according to update type) before installed to the FCR. This will be validated by the 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.Ext_Pairing

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

OE.SecureEnvironment

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

Tampering protection system shall protect fiscal memory with mesh cover.

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

4.3. Security Objective Rationale

Table 2 provides security problem definition covered by security objectives. Threats and OSPs are addressed by security objectives for the TOE and its operational environment. Assumptions are addressed by only security objectives for the operational environment.

Table 2 Security Objective Rationale

	Threats									OSPs								Assumptions							
	T.AccessControl	T. Authentication	T.MDData	T.Eavesdropping	T.Server Counterfeiting	T.Skimming	T.Counterfeit	T.Malfunction	T.ChangingTime	P.Certificate	P.Certificates 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				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 2 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 if user authenticated to the FCR or not; 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 parameters during transferring 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.Server Counterfeiting is addressed by O.Integrity to ensure the integrity of server certificates (P_{PRA}, $P_{PRA\text{-}SIGN}$); O.Event to log physical tamper; OE. SecureStorage to provide secure environment for server certificates.

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

T.Counterfeit is addressed by O.Integrity to ensure the integrity of sensitive data; O.Event to log physical tamper; OE.SecureStorage to provide secure environment for sensitive data.

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

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

P.Certificate is fulfilled by OE.KeyGeneration.

P.CertificateInstallation is fulfilled OE.Transportation and OE.SecureStorage.

P.SecureEnvironment is fulfilled by OE.SecureEnvironment, O.Event and 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 by OE.Ext_Pairing.

5. EXTENDED COMPONENTS DEFINITION

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

6. SECURITY REQUIREMENTS

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

The following notations are used:

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

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

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

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

6.1. Security Functional Requirements for the TOE

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

6.1.1. Class FAU Security Audit

6.1.1.1. FAU_GEN Security audit data generation

FAU_GEN.1 Audit data generation

Hierarchical to:

Dependencies: FPT_STM.1 Reliable time stamps: is fulfilled by FPT_STM.1

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, and the outcome (success or failure) of the event; and

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

6.1.1.2. FAU_SAR Security audit review

FAU_SAR.1 Audit review

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

6.1.1.3. FAU_STG Security audit event storage

FAU_STG.1 Protected audit trail storage

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

FAU_STG.4 Prevention of audit data loss

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

6.1.2. Class FCO Communication

6.1.2.1. FCO_NRO Non-repudiation of origin

FCO_NRO.2 Enforced proof of origin

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

6.1.3. Class FCS Cryptographic Support

6.1.3.1. FCS_CKM Cryptographic key management

FCS_CKM.1/ TRMK Cryptographic key generation

Hierarchical to:	-
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RNG] and specified cryptographic key sizes [256 bits] that meet the following: [NIST SP800-22B].

FCS_CKM.1/TLS_AES Cryptographic key generation

Hierarchical to:	-
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [PRF] and specified cryptographic key sizes [AES:128 bits and AES:256 bits] that meet the following: [RFC 5246].

FCS_CKM.1/TLS_HMAC Cryptographic key generation

Hierarchical to:	-
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [PRF] and specified cryptographic key sizes [256 bit] that meet the following: [RFC 5246].

FCS_CKM.1/ DHE-KEY Cryptographic key generation

Hierarchical to:	-
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RNG] and specified cryptographic key sizes [2048 bits] that meet the following: [none].

FCS_CKM.1/ EXT-DEV K_{HMAC} Cryptographic key generation

Hierarchical to:	-
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [PRF] and specified cryptographic key sizes [256 bits] that meet the following: [RFC 5246].

FCS_CKM.1/ EXT-DEV K_{ENC} Cryptographic key generation

Hierarchical to:	-
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [PRF] and specified cryptographic key sizes [AES:256 bits] that meet the following: [RFC 5246].

FCS_CKM.2 Cryptographic key distribution

Hierarchical to:	-
Dependencies:	[[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_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.4 Cryptographic key destruction

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwriting values by 0] 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
TRMK	After key transport from PRA-IS to TOE for TREK and TRAK

K_{ENC}	➢ Conditions specified in External Device Communication Protocol Document [7] occur ➢ The usage number that is specified External Device Communication Protocol Document [7] is exceeded
K_{HMAC}	➢ Conditions specified in External Device Communication Protocol Document [7] occur ➢ The number that is specified External Device Communication Protocol Document[7] is exceeded
DHE-KEY	After key agreement between TOE and External Device
AES KEY	Deletion after use of AES key for TSM communication
Certificates	Certificates are not necessary to delete because no confidentiality needs for the public keys

6.1.3.2. FCS_COP Cryptographic operation

FCS_COP.1/TREK Cryptographic operation

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [encryption] 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: -
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/ TRMK-DEC Cryptographic operation

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [decryption] 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/PUB-ENC Cryptographic operation

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [encryption] 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: -
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/ENC-DEC Cryptographic operation

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [encryption, decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [AES:128 bits and AES:256 bits] that meet the following: [NIST SP800-38A].

FCS_COP.1/INT-AUTH Cryptographic operation

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [authentication and integrity protection] in accordance with a specified cryptographic algorithm [HMAC-SHA256] and cryptographic key sizes [256 bits] that meet the following: [FIPS 198-1 and NIST FIPS PUB 180-2].

FCS_COP.1/HASHING Cryptographic operation

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [hashing] in accordance with a specified cryptographic algorithm [SHA2] and cryptographic key sizes [none] that meet the following: [NIST FIPS PUB 180-2].

Application Note 3: No need to include any dependencies because there is no need to use any key for HASHING

FCS_COP.1/EXT-DEV KEYEXCHANGE Cryptographic operation

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [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 K_{ENC} Cryptographic operation

Hierarchical to: -
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [encryption 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 K_{HMAC} Cryptographic operation

Hierarchical to:	-
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform [encryption and decryption for integrity protection] in accordance with a specified cryptographic algorithm [HMAC-SHA256] and cryptographic key sizes [256 bits] that meet the following: [FIPS 198-1 and NIST FIPS PUB 180-2].

6.1.4. Class FDP User Data Protection

6.1.4.1. FDP_ACC Access control policy

FDP_ACC.1 Subset access control

Hierarchical to:	-
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 Authorised Manufacturer User Objects: Sales and event data, exchange rates, time information. Operations: Secure state mode and maintenance mode actions]

6.1.4.2. FDP_ACF Access control functions

FDP_ACF.1 Security attribute based access control

Hierarchical to:	-
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the [Administrative Access Control SFP] to objects based on the following: [Subjects: FCR Authorised User and Authorised Manufacturer User Subject Attributes: 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.
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 privileges].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].

6.1.4.3. FDP_ETC Export from the TOE

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

Hierarchical to:	-
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 4: *User data (sales data, event data and TRMK) are exported from FCR to the PRA-IS via TSM.*

FDP_ETC.2/EFT-POS/SMART PINPAD Export of user data with security attributes

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1	The TSF shall enforce the [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]].

6.1.4.4. FDP_IFC Information flow control policy

FDP_IFC.1/TSMCOMMUNICATION Subset information flow control

Hierarchical to:	-
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1	The TSF shall enforce the [Information Flow Control SFP with TSM and PRA- IS] on [subjects (TSM and PRA-IS) and objects (sales data ,event data reports, FCR

parameters) , TREK, TRAK and TRMK as specified in PRA Messaging Protocol Document [6]]

FDP_IFC.1/EFT-POS/SMART PINPADCOMMUNICATION Subset information flow control

Hierarchical to:	-
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1	The TSF shall enforce the [Information Flow Control SFP with EFT-POS/SMART PINPAD Device] on [subjects (EFT-POS/SMART PINPAD) and objects (amount information in sales data, slip data request, EOD requests, loyalty card operation commands, bank selection command, other banking operational commands, EFT-POS/SMART PINPAD status commands, etc) as specified in External Device Communication Protocol Document [7]]

6.1.4.5. FDP_IFF Information flow control functions

FDP_IFF.1/TSMCOMMUNICATION Simple security attributes

Hierarchical to:	-
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1	The TSF shall enforce the [Information Flow Control SFP with TSM and PRA-IS] based on the following types of subject and information security attributes: [TOE has ability to send reports related to sales data and event data 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 PRA Messaging Protocol Document [6]; TOE has ability to receive FCR parameters from TSM by using subject identifier (IP/Port information) and object identifier (information label) according to PRA Messaging Protocol Document [6]].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [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 PINPADCOMMUNICATION Simple security attributes

Hierarchical to:	-
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1	The TSF shall enforce the [Information Flow Control SFP 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.1.3	The TSF shall enforce the [none].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [none].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.4.6. FDP_ITC Import from the outside of the TOE

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

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1	The TSF shall enforce the [Information Flow Control SFP 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 5: FCR parameters are imported from TSM to TOE. TREK and TRAK are imported from PRA-IS to TOE

FDP_ITC.2/EFT-POS/SMART PINPAD Import of user data with security attributes

Hierarchical to:	-
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1	The TSF shall enforce the [Information Flow Control SFP 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]].

6.1.4.7. FDP_SDI Stored data integrity

FDP_SDI.2/MEMORY Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring
Dependencies: -
FDP_SDI.2.1 The TSF shall monitor ~~user data~~ **sales data stored in fiscal memory and ERU, event data and characterization data** stored in containers controlled by the TSF for [integrity errors] ~~on all objects, based on the following attributes: [assignment: user data attributes]~~.
FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [Generate an audit event and then enter maintenance mode]

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

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring
Dependencies: -
FDP_SDI.2.1 The TSF shall monitor ~~user data~~ **sales data stored in 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 print Z report automatically]

6.1.5. Class FIA Identification and Authentication

6.1.5.1. FIA_AFL Authentication failures

FIA_AFL.1/MANUFACTURER Authentication failure handling

Hierarchical to: -
Dependencies: FIA_UAU.1 Timing of authentication
FIA_AFL.1.1 The TSF shall detect when [***three***] unsuccessful authentication attempts occur related to [Authorised Manufacturer User authentication].
FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [warn the user and make user wait for a new authentication attempt for 15 minutes].

FIA_AFL.1/AUTHORISED Authentication failure handling

Hierarchical to: -
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [***ten***] 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 [warn the user and make user wait for a new authentication attempt for 15 minutes].

6.1.5.2. FIA_UAU User authentication

FIA_UAU.1 Timing of authentication

Hierarchical to: -

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 behalf of 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: -

Dependencies: -

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [the authentication mechanism employed to authenticate Authorised Manufacturer User].

6.1.5.3. FIA_UID User Identification

FIA_UID.1 Timing of identification

Hierarchical to: -

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.

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.

6.1.6. Class FMT Security Management

6.1.6.1. FMT_MOF Management of security functions behaviour

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: -

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 **nobody.**

Application Note 6*: No authorised user makes the changes on the behaviour of the functions. The TSF itself makes the behavioural changes according to the FCR parameters received from TSM.*

Application Note 7*: Ability to Modification of behaviour shall be used according to PRA directives. Normal operation functions includes all FCR parameters that are sent to FCR by TSM.*

6.1.6.2. FMT_MSA Management of security attributes

FMT_MSA.1/PRIVILEGES Management of security attributes

Hierarchical to:	-
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:	-
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 [Authorised Manufacturer User].

FMT_MSA.1/FILE NAME and INFO-LABEL Management of security attributes

Hierarchical to:	-
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/EFT-POS/SMART PINPAD SOURCE PORT INFO Management of security attributes

Hierarchical to:	-

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/SMART PINPAD Devices] to restrict the ability to [***modify***] the security attributes [Source Port] to [none].

FMT_MSA.1/EFT-POS/SMART PINPAD LABEL INFO Management of security attributes

Hierarchical to:	-
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/SMART PINPAD Device] to restrict the ability to [***modify***] the security attributes [EFT-POS/SMART PINPAD Label] to [none].

FMT_MSA.3/USERS and SYSTEMS Static attribute initialisation

Hierarchical to:	-
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [Administrative Access Control SFP, 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/EFT-POS/SMART PINPAD Static attribute initialisation

Hierarchical to:	-
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [Information Flow Control SFP with EFT-POS/SMART PINPAD Device] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

6.1.6.3. FMT_MTD Management of TSF data

FMT_MTD.1/FCR AUTHORISED USER Management of TSF data

Hierarchical to:	-
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [***modify***] the [FCR Authorised User's authentication data] to [FCR Authorised Manufacturer User] and ***[create, modify***, ***delete***] the [FCR Authorised User's authentication data] to [FCR Authorised User]

FMT_MTD.1/AUTHORISED MANUFACTURER USER Management of TSF data

Hierarchical to: -
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1 The TSF shall restrict the ability to [***create***] the [Authorised Manufacturer User's authentication data] to ~~[assignment: the authorised identified roles]~~ **[nobody].**

Application Note 8*: No authorised identified roles make the changes on Authorized Manufacturer User's authentication data but TSM creates it.*

6.1.6.4. FMT_SMF Specification of Management Functions

FMT_SMF.1 Specification of Management Functions

Hierarchical to: -
Dependencies: -
FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [Authorised Manufacturer User modifies IP: Port Information, FCR Authorised User add and delete other FCR Authorised User, FCR Authorised User modifies FCR Authorised User's authentication data, Authorised Manufacturer User changes to default FCR Authorised User's User Identity and FCR Authorised User's authentication data]

6.1.6.5. FMT_SMR Security management roles

FMT_SMR.2 Restrictions on security roles

Hierarchical to: FMT_SMR.1 Security roles
Dependencies: FIA_UID.1 Timing of identification
FMT_SMR.2.1 The TSF shall maintain the roles: [FCR Authorised User, Authorised 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 [Authorised Manufacturer User shall take action in maintenance works and FCR authorised user take action in secure state works] are satisfied.

6.1.7. Class FPT Protection of the TSF

6.1.7.1. FPT_FLS Fail secure

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: -
Dependencies: -

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

6.1.7.2. FPT_PHP TSF physical protection

FPT_PHP.2 Notification of physical attack

Hierarchical to: FPT_PHP.1 Passive detection of physical attack
Dependencies: FMT_MOF.1 Management of security functions behaviour
FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
FPT_PHP.2.3 For [the devices/elements for which active detection is required in Technical Guidance Document [5]], and elements and notify [all user] when physical tampering with the TSF's devices or TSF's elements has occurred.

6.1.7.3. FPT_RCV Trusted recovery

FPT_RCV.1 Manual recovery

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

FPT_RCV.4 Function recovery

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

6.1.7.4. FPT_STM Time stamps

FPT_STM.1 Reliable time stamps

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

6.1.7.5. FPT_TDC Inter-TSF TSF data consistency

FPT_TDC.1/TSM Inter-TSF basic TSF data consistency

Hierarchical to: -
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: -

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.

6.1.7.6. FPT_TEE Testing of external entities

FPT_TEE.1/EXT Testing of external entities

Hierarchical to: -

Dependencies: -

FPT_TEE.1.1 The TSF shall run a suite of tests [***during initial start-up and during fiscal transactions***] to check the fulfilment 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 8: External entities are ERU, Fiscal Memory, Daily Memory, Mesh Cover and Electronic Seal.

FPT_TEE.1/TIME Testing of external entities

Hierarchical to: -

Dependencies: -

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

FPT_TEE.1.2 If the test fails, the TSF shall [overwrite time information received from trusted server, generate an audit event according to Technical Guidance Document [5]]

6.1.8. Class FTP Trusted Patch/Channels

6.1.8.1. FTP_ITC Inter-TSF trusted channel

FTP_ITC.1/TSM Inter-TSF trusted channel

Hierarchical to: -

Dependencies: -

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and

provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [sending user data (sales, event data and TRMK) to PRA-IS; receiving user data (TREK and TRAK) from PRA-IS and receiving user data (FCR parameters and exchange rates) from TSM].

FTP_ITC.1/EFT-POS/SMART PINPAD Inter-TSF trusted channel

Hierarchical to: -

Dependencies: -

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [sending amount information to EFT-POS/SMART PINPAD and receiving outcome of the operation from EFT-POS/SMART PINPAD].

6.2. Security Assurance Requirements for the TOE

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

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

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

Table 4 Coverage of security objectives by SFRs for TOE

		O.AccessControl	O.Event	O.Integrity	O.Authentication	O.Function	O.Transfer
FAU_GEN.1	Audit data generation		X				
FAU_SAR.1	Audit review	X					
FAU_STG.1	Protected audit trail storage			X			
FAU_STG.4	Prevention of audit data loss			X			

		O.AccessControl	O.Event	O.Integrity	O.Authentication	O.Function	O.Transfer
FCO_NRO.2	Enforced proof of origin						X
FCS_CKM.1/TRMK	Cryptographic key generation						X
FCS_CKM.2	Cryptographic key distribution						X
FCS_CKM.1/TLS_AES	Cryptographic key generation						X
FCS_CKM.1/TLS_HMAC	Cryptographic key generation						X
FCS_CKM.1/ DHE-KEY	Cryptographic key generation						X
FCS_CKM.1/ EXT-DEV K_{ENC}	Cryptographic key generation						X
FCS_CKM.1/ EXT-DEV K_{hmac}	Cryptographic key generation						X
FCS_CKM.4	Cryptographic key destruction						X
FCS_COP.1/TREK	Cryptographic operation						X
FCS_COP.1/TRAK	Cryptographic operation						X
FCS_COP.1/ENC-DEC	Cryptographic operation						X
FCS_COP.1/INT-AUTH	Cryptographic operation						X
FCS_COP.1/HASHING	Cryptographic operation				X		
FCS_COP.1/TRMK-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 K_{ENC}	Cryptographic operation						X
FCS_COP.1/EXT-DEV K_{HMAC}	Cryptographic operation						X
FCS_COP.1/EXT-DEV KEYEXCHANGE	Cryptographic operation						X
FDP_ACC.1	Subset access control	X					
FDP_ACF.1	Security attribute based access control	X					

		O.AccessControl	O.Event	O.Integrity	O.Authentication	O.Function	O.Transfer
FDP_ETC.2/TSM	Export of user data with security attributes						X
FDP_ETC.2/EFT-POS/SMART PINPAD	Export of user data with security attributes						X
FDP_IFC.1/TSMCOMMUNICATION	Subset information flow control						X
FDP_IFC.1/EFT-POS/SMART PINPADCOMMUNICATION	Subset information flow control						X
FDP_IFF.1/TSMCOMMUNICATION	Simple security attributes						X
FDP_IFF.1/EFT-POS/SMART PINPADCOMMUNICATION	Simple security attributes						X
FDP_ITC.2/TSM	Import of user data with security attributes						X
FDP_ITC.2/EFT-POS/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	

		O.AccessControl	O.Event	O.Integrity	O.Authentication	O.Function	O.Transfer
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/EFT-POS/SMART PINPADSOURCE 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/EFT-POS/SMART PINPAD	Static attribute initialisation						X
FMT_MTD.1/FCR AUTHORISED USER	Management of TSF data	X			X		
FMT_MTD.1/FCR AUTHORISED 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	

		O.AccessControl	O.Event	O.Integrity	O.Authentication	O.Function	O.Transfer
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

6.3.2. Rationale for SFR's Dependencies

Selected security functional requirements include related dependencies. Table 5 below provides a summary of the security functional requirements dependency analysis.

Table 5 Security Functional Requirements dependencies

Component	Dependencies	Included / not included
FAU_GEN.1	FPT_STM.1	included
FAU_SAR.1	FAU_GEN.1	included
FAU_STG.1	FAU_GEN.1	included
FAU_STG.4	FAU_STG.1	included
FCO_NRO.2	FIA_UID.1	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.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]; FCS_CKM.4	FCS_CKM.1/TRMK; FCS_CKM.4
FCS_CKM.1/TLS_AES	FCS_CKM.2 or FCS_COP.1; FCS_CKM.4	FCS_COP.1/ENC-DEC and FCS_CKM.4 included
FCS_CKM.1/TLS_HMAC	FCS_CKM.2 or FCS_COP.1; FCS_CKM.4	FCS_COP.1/INT-AUTH and FCS_CKM.4 included
FCS_CKM.1/EXT-DEV K_{ENC}	FCS_CKM.2 or FCS_COP.1; FCS_CKM.4	FCS_COP.1/EXT-DEV K_{ENC} FCS_CKM.4 included
FCS_CKM.1/EXT-DEV K_{HMAC}	FCS_CKM.2 or FCS_COP.1; FCS_CKM.4	FCS_COP.1/EXT-DEV K_{HMAC} 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 K_{ENC}, FCS_CKM.1/ EXT-DEV K_{HMAC}, FCS_CKM.1/TLS_HMAC, FCS_CKM.1/TLS_AES, FCS_CKM.1/TRMK, FCS_CKM.1/DHE-KEY) included
FCS_COP.1/TRAK	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ;FCS_CKM.4	FDP_ITC.2/TSM and FCS_CKM.4 included
FCS_COP.1/TREK	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ;FCS_CKM.4	FDP_ITC.2/TSM and FCS_CKM.4 included
FCS_COP.1/TRMK-DEC	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 ;FCS_CKM.4	FCS_CKM.1/TRMK; FCS_CKM.4
FCS_COP.1/PUB-ENC	FDP_ITC.1 or FDP_ITC.2 or FCS_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, P_{PRA} and P_{TSM} 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 or FDP_ITC.2 or FCS_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, $P_{PRA-SIGN}$ public key should not be deleted. Tamper system of the TOE protects keys from misuse, disclosure or modification.
FCS_COP.1/ENC-DEC	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1; FCS_CKM.4	FCS_CKM.1/TLS_AES and FCS_CKM.4 included
FCS_COP.1/INT-AUTH	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1; FCS_CKM.4	FCS_CKM.1/TLS_HMAC and FCS_CKM.4 included
FCS_COP.1/HASHING	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1; FCS_CKM.4	No need to include any dependencies because there is no need to use any key for HASHING
FCS_COP.1/DHE-KEY	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1; FCS_CKM.4	FCS_COP.1/ EXT-DEV KEYEXCHANGE and FCS_CKM.4 included.
FCS_COP.1/EXT-DEV K_{ENC}	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1; FCS_CKM.4	FCS_CKM.1/ EXT-DEV K_{ENC}, FCS_CKM.4 included
FCS_COP.1/EXT-DEV K_{HMAC}	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1; FCS_CKM.4	FCS_CKM.1/ EXT-DEV K_{HMAC}, FCS_CKM.4 included
FCS_COP.1/ EXT-DEV KEYEXCHANGE	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1; FCS_CKM.4	FCS_CKM.1/ DHE-KEY and FCS_CKM.4 included
FDP_ACC.1	FDP_ACF.1	included
FDP_ACF.1	FDP_ACC.1; FMT_MSA.3	FDP_ACC.1; FMT_MSA.3/USERS and SYSTEMS included
FDP_ETC.2/TSM	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1; FDP_IFC.1/TSMCOMMUNICATION included
FDP_ETC.2/EFT-POS/SMART PINPAD	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1; FDP_IFC.1/EFT-POS/SMART PINPADCOMMUNICATION included
FDP_IFC.1/TSMCOMMUNICATION	FDP_IFF.1	FDP_IFF.1/TSMCOMMUNICATION included

FDP_IFC.1/EFT-POS/SMART PINPADCOMMUNICATION	FDP_IFF.1	FDP_IFF.1/EFT-POS/SMART PINPADCOMMUNICATION 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 PINPADCOMMUNICATION	FDP_IFC.1; FMT_MSA.3	FDP_IFC.1/EFT-POS/SMART PINPAD COMMUNICATION; FMT_MSA.3/EFT-POS/SMART PINPAD included
FDP_ITC.2/TSM	FDP_ACC.1 or FDP_IFC.1 ; FTP_ITC.1 or FTP_TRP.1 ; FPT_TDC.1	FDP_IFC.1/TSMCOMMUNICATION; FTP_ITC.1; FPT_TDC.1 included
FDP_ITC.2/EFT-POS/SMART PINPAD	FDP_ACC.1 or FDP_IFC.1 ; FTP_ITC.1 or FTP_TRP.1 ; FPT_TDC.1	FDP_IFC.1/EFT-POS/SMART PINPAD COMMUNICATION; FTP_ITC.1/EFT-POS/SMART PINPAD; FPT_TDC.1/ EFT-POS/SMART PINPAD included
FDP_SDI.2	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 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	FDP_ACC.1 included; FMT_SMR.2 is hierarchical to FMT_SMR.1 FMT_SMF.1 included
FMT_MSA.1/ IP:PORT_INFO	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	FDP_IFC.1/TSMCOMMUNICATION included; FMT_SMR.2 is hierarchical to FMT_SMR.1 FMT_SMF.1 included

FMT_MSA.1/FILE NAME and INFO-LABEL	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	FDP_IFC.1/TSMCOMMUNICATION included; FMT_SMR.2 is hierarchical to FMT_SMR.1 FMT_SMF.1 included
FMT_MSA.1/EFT-POS/SMART PINPAD SOURCE PORT INFO	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	FDP_IFC.1/EFT-POS/SMART PINPADCOMMUNICATION included; FMT_SMR.2 is hierarchical to FMT_SMR.1 FMT_SMF.1 included
FMT_MSA.1/ EFT-POS/SMART PINPAD LABEL INFO	FDP_ACC.1 or FDP_IFC.1; FMT_SMR.1; FMT_SMF.1	FDP_IFC.1/EFT-POS/SMART PINPADCOMMUNICATION included; FMT_SMR.2 is hierarchical to FMT_SMR.1 FMT_SMF.1 included
FMT_MSA.3/USERS and SYSTEMS	FMT_MSA.1; FMT_SMR.1	FMT_MSA.1 (FMT_MSA.1/PRIVILEGES, FMT_MSA.1/IP:PORT_INFO, FMT_MSA.1/FILE NAME and INFO-LABEL) ; FMT_SMR.2 is hierarchical to FMT_SMR.1 included
FMT_MSA.3/EFT-POS/SMART PINPAD	FMT_MSA.1 ; FMT_SMR.1	FMT_MSA.1(FMT_MSA.1/ EFT-POS/SMART PINPAD LABEL INFO) ; FMT_SMR.2 is hierarchical to FMT_SMR.1 included
FMT_MTD.1/FCR AUTHORISED USER	FMT_SMR.1 ; FMT_SMF.1	FMT_SMR.2 is hierarchical to FMT_SMR.1 ; FMT_SMF.1 included
FMT_MTD.1/AUTHORISED 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	-

6.3.3. Security Assurance Requirements Rationale

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

6.3.4. Security Requirements – Internal Consistency

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 section 6.3.2 Rationale for SFR's Dependencies for the security functional requirements 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 dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are internally consistent, because 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 – an opportunity having been shown not to arise in sections 6.3.2 Rationale for SFR's Dependencies and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements

7. TOE SUMMARY SPECIFICATION

7.1. TOE Security Functions

TOE Security functions are determined parallel to TOE security objectives. TOE security functions are nominated as below.

7.1.1. Access Control

TOE controls user (FCR Authorised User, Authorised Manufacturer User) access to functions and data. Following security function policies is applied by TOE.

Administrative Access Control Security Function Policy

Subjects		Sales data	Event data	Exchange rates	Authentication Data (FCR Auth. User)	Time information
Secure State Mode	**FCR Authorised User**	Read /Write	N/A	Read/Write	Write	Read
	Authorised Manufacturer User	N/A	N/A	N/A	N/A	N/A
	Unauthenticated User	Read /Write	N/A	Read	N/A	Read
Maintenance Mode	**FCR Authorised User**	N/A	N/A	N/A	N/A	N/A
	Authorised Manufacturer User	Read	Read	Read/Write	Change to Default Value	Read/Write
	Unauthenticated User	N/A	N/A	N/A	N/A	N/A

Access Rules for assets:

- Only FCR Authorised User can modify User Identity. FCR Authorised User can create and delete FCR Authorised User.
- Authorised Manufacturer User can change FCR Authorised User Identity and password values to default.
- Any user cannot modify Privileges.
- TSM or PRA–IS cannot modify User Identity, Privileges, secure state and maintenance mode access rights.
- Authorised Manufacturer User can modify IP: Port Information,
- Authorised Manufacturer users are allowed to do their actions in only maintenance mode, FCR Authorised User is allowed to their actions in only secure state mode.

- FCR Authorised User's password can be modified by FCR Authorised Users and set to default password value by Authorised Manufacturer Users.
- No authorised identified roles make the changes on Authorised Manufacturer User's authentication data (challenge code) but manufacturer trusted server creates it.
- TOE allows only authorised users and systems to read relevant records.

7.1.2. Accuracy

TOE ensures that processing of inputs to derive sales data and event data is accurate. TOE security functionality cannot be changed by any user. Only parameters are sent from TSM by acceptance of PRA is used for functionality change. Sales data and event data is processed only if FCR is used by authorised user. Authentication attempts are restricted to 3 try.

If TOE enters in maintenance mode, it can be switched to the secure state manually. If any situation except following, it can be switched to the secure state automatically.

- FCR Certificate check fails,
- Mesh cover monitoring check fails,
- A disconnection between fiscal memory and main processor occurs,
- Electronic seal is opened, or forced by unauthorised persons
- NCR E10 Application integrity error occurs,
- Event log data and sales data integrity error occurs,
- The state of unable to write to fiscal memory, daily memory and ERU
- First initialisation phase fails.

TOE has the testing capability of external entities during the initial start-up and fiscal transaction. TOE has the capability of time synchronisation with trusted server (TSM). During Z report delivery or parameter download, TOE synchronizes its time information by using NTP with trusted server. If any test fails, the TOE generates an audit event according to PRA Messaging Protocol Document [6].

TOE detects anomaly when Authorized Manufacturer User updates time information, TOE controls whether new time information is earlier than last fiscal memory record's.

7.1.3. Secure Transfer

TOE communicates external systems TSM, PRA-IS and External (EFT-POS/SMART PINPAD) Device securely. For secure communication with these entities TOE uses well known cryptographic algorithms such as TLS, AES and RSA. TOE uses TLS and AES algorithms for communication with TSM and PRA-IS and TOE uses DHE for AES key agreement with external Device (EFT-POS/SMART PINPAD) and also it uses AES to communicate securely with External Device (EFT-POS/SMART PINPAD). TOE generates AES, DHE keys by using Pseudo Random Functions of cryptographic libraries.

When a physical tampering attack occurs FCR hardware controls detects unauthorised case openings and TOE generates an audit log for that kind of physical tampering by using environment hardware measures/controls and delete TREK, TRAK and TRMK Keys.

TSM Communication:

TOE initiates traffic to TSM and uses SSL authentication to authenticate TSM and then TOE generates AES session key by using cryptographic library for encryption and integrity control. After usage of AES key it is deleted by library a new key is created for the next session during the next communication with TSM. Certificate private key is not necessary to delete, because it is stored in smart card and it is not exported.

The asymmetric keys used in communication with TSM cannot be changed by any user types for an identified FCR and default security attribute (keys) values cannot be changed.

Information Flow Control Security Function Policy for TSM Rules:

- TOE uses IP/Port information and file name to communicate TSM
- TSM has ability to send parameters of new generation cash register fiscal application software functions to FCR according to PRA messaging protocol document [6]. TOE uses IP/Port information and information label to communicate TSM
- Information flow is granted only if secure communication with SSL CA is established. After secure communication settlement FCR parameters and exchange rates can be received from TSM.
- Only Authorised Manufacturer User can change TSM IP and port information any other security related functionality cannot be changed by any user.

PRA-IS Communication:

TOE communicates to PRA-IS over TSM. TOE does not communicate PRA-IS directly. TOE authenticates PRA-IS by using Digital certificates of PRA-IS. While sending sales and event data to PRA-IS TOE will provide its identity and time information. TOE has capability of authenticate PRA-IS by using PRA-IS certificate provided the same certification authority of TOE.

TOE provides confidentiality and integrity for transferring sales data, event data to the PRA-IS by using GMP protocol. All data transfer uses encryption and integrity controls. TOE provides integrity for characterization data transferred to the PRA-IS.

TOE initiates traffic to PRA-IS and uses authentication methods defined in GMP protocol to authenticate PRA-IS. TOE generates TRMK by using random number generator. TOE encrypts TRMK by using PRA-IS public key then sends encrypted TRMK to PRA-IS. PR-IS generates TREK and TRAK keys and encrypt both keys then sends back to TOE. After receiving and controlling integrity of keys, if there is no error. TOE uses these keys for secure communication with PRA-IS and deletes TRMK.

TOE uses AES crypto system for encryption of packets to send to PRA-IS.

Information Flow Control Security Function Policy for PRA-IS Rules:

- PRA-IS has ability to receive reports related to sales data, event data reports. TOE uses IP/Port information of TSM and file name to communicate PRA-IS

- After secure communication settlement sales and event data can be sent to PRA-IS and FCR parameters and exchange rates can be downloaded from TSM.

TOE communicates PRA-IS with Secure IC as follows:

- TOE make produce random number Secure IC, then encrypt this TRMK with PRA-IS public key and send encrypted TRMK to PRA-IS.
- RPA-IS produce TREK and TRAK keys and encrypt these keys with TRMK, then sends them back to TOE over TSM.
- TOE passes these encrypted keys to Secure IC to make it decrypt and store

External Device (EFT-POS/SMART PINPAD) Device Communication:

EFT-POS/SMART PINPAD Device communication is done by using AES cryptosystem. All fiscal data is encrypted between EFT-POS Device and TOE. For AES key exchange, TOE uses DHE key exchange methods detailed in GMP3 document [7].

The EFT-POS/SMART PINPAD pairing process can only be done under supervision of Authorised Manufacturer user and default security attribute (source port, label) values can only be changed by authorised manufacturer users.

Information Flow Control SFP with EFT_POS/SMART PINPAD Device Rules:

- Amount information in sales data can be sent to EFT-POS/SMART PINPAD Device.
- Outcome of EFT-POS/SMART PINPAD operation can be received from EFT-POS/SMART PINPAD.
- EFT-POS/SMART PINPAD Label and source port info cannot be modified by any user.
- Initial configuration can only be done by Authorised Manufacturer User.

7.1.4. Authentication

TOE authenticates FRC Authorised User by controlling username and password match. TOE does not store FCR Authorised User's password (authentication data) in the form of clear text. If FCR Authorised User enters wrong password ten times, TOE does not accept its authentication attempt and it warns the user make user wait for a new authentication attempt for 15 minutes. FCR Authorised User's password can be modified by only FCR Authorised Users.

TOE authenticates Authorised Manufacturer User by challenge response authentication mechanism. TOE generates a randomized challenge code to Authorised Manufacturer user for authentication. Authorised Manufacturer User uses this code information to generate the response code by using a mobile application, call center or web service of manufacturer. If user enters the required response code then TOE authenticates authorised manufacturer user. TOE uses last logon time information for inhibition of reuse of authentication data (response code).

If Authorised Manufacturer User enters wrong response code three times, TOE does not accept its authentication attempt and it warns the user and make user wait for a new authentication attempt for 15 minutes.

TOE allow to do fiscal sales prior to any user identification and authentication.

FCR authenticates PRA-IS by using Digital certificates by TLS 1.2. TOE has capability of authenticate TSM by using TSM certificate provided the same certification authority with its environment. While communication with TSM and PRA-IS TOE generates Hash outputs of and Smartcard is used for signing.

7.1.5. Integrity

TOE provides integrity for sales data and event data while storing these data by using CRC and for the daily memory stored data integrity is controlled by using hashing algorithms.

TOE protects stored audit records from unauthorised deletion and modification. For that purpose TOE does not give any deletion and modification capability to any user role. FCR has hardware and software tampering detection measures. When unauthorised case opening attempt occurs, hardware and software measures can detect this kind of attack even the FCR powered off. If physical tampering occurs TOE notifies FCR Authorised User.

TOE has limited capacity for audit records. When limit is reached TOE overwrite the oldest stored audit records.

TOE monitors integrity of sales data, event data, authentication data, characterization data and FCR parameters. TOE uses CRC check and Hash controls for detection of integrity errors even if it is erroneous or misuse of TOE. TOE protects all records from unauthorised modification by using integrity checking mechanisms

If any integrity error occurs in sales data stored in fiscal memory and ERU, event data, authentication data and characterization data, TOE generates an audit event then TOE enters maintenance mode.

If any integrity error occurs in sales data stored in daily memory and FCR Parameters TOE generates an audit event and prints Z report automatically.

During the communication of TSM and PRA-IS, TOE uses checksum for checking integrity of messages.

7.1.6. Event recording

TOE records important events stated as in PRA Messaging Protocol document [6] and start-up shutdown actions with reliable time stamps. All events contains following information date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

For reliable time information TOE uses Trusted Server to synchronise its time with TSM meanwhile every Z report sending actions.

7.2. Assurance Measure

To satisfy the security assurance requirements, suitable assurance measures are employed by the developer of the TOE. The documents describe the measures and include further information supporting the verification of the conformance of these measures against the claimed assurance requirements.

The following table includes a mapping between the assurance requirements and the documents including the relevant information for the correspondent requirement.

Table 6 Assurance Measure

Assurance Class	Family	Document Reference
ADV Development	ADV_ARC.1	Security architecture description: NCR e10 Güvenlik Mimarisi
	ADV_FSP.2	Security-enforcing functional specification: NCR e10 Fonksiyonel Spesifikasyon
	ADV_TDS.1	Basic design: NCR e10 Tasarım Tanımlama
AGD Guidance Documents	AGD_OPE.1	Operational user guidance: NCR e10 Kullanıcı Kılavuzu
	AGD_PRE.1	Preparative procedures: NCR e10 Kurulum Prosedürü
ALC Life Cycle Support	ALC_CMC.2	Use of a CM system: NCR e10 Konfigürasyon Yönetimi
	ALC_CMS.2	Parts of the TOE CM coverage: CM Item List
	ALC_DEL.1	Delivery procedures: NCR e10 İlklendirme Prosedürü
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives

	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE Tests	ATE_COV.1	Evidence of coverage: NCR e10 Test Kurgusu
	ATE_FUN.1	Functional testing: NCR e10 Test Kurgusu Test Results/Records
	ATE_IND.2	Independent testing - sample: TOE hardware and software sample
AVA Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis: TOE hardware and software sample

7.3. TOE Summary Specification Rational

7.3.1. Security Functions Rational

Table 7 Security Functions Rationale

		Access Control	Event Recording	Integrity	Authentication	Accuracy	Secure 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

		Access Control	Event Recording	Integrity	Authentication	Accuracy	Secure Transfer
FCS_CKM.2	Cryptographic key distribution						X
FCS_CKM.1/TLS_AES	Cryptographic key generation						X
FCS_CKM.1/TLS_HMAC	Cryptographic key generation						X
FCS_CKM.1/ DHE-KEY	Cryptographic key generation						X
FCS_CKM.1/ EXT-DEV K_{ENC}	Cryptographic key generation						X
FCS_CKM.1/ EXT-DEV K_{hmac}	Cryptographic key generation						X
FCS_CKM.4	Cryptographic key destruction						X
FCS_COP.1/TREK	Cryptographic operation						X
FCS_COP.1/TRAK	Cryptographic operation						X
FCS_COP.1/ENC-DEC	Cryptographic operation						X
FCS_COP.1/INT-AUTH	Cryptographic operation						X
FCS_COP.1/HASHING	Cryptographic operation				X		
FCS_COP.1/TRMK-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 K_{ENC}	Cryptographic operation						X
FCS_COP.1/EXT-DEV K_{HMAC}	Cryptographic operation						X
FCS_COP.1/EXT-DEV KEYEXCHANGE	Cryptographic operation						X

		Access Control	Event Recording	Integrity	Authentication	Accuracy	Secure Transfer
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/EFT-POS/SMART PINPAD	Export of user data with security attributes						X
FDP_IFC.1/TSMCOMMUNICATION	Subset information flow control						X
FDP_IFC.1/EFT-POS/SMART PINPADCOMMUNICATION	Subset information flow control						X
FDP_IFF.1/TSMCOMMUNICATION	Simple security attributes						X
FDP_IFF.1/EFT-POS/SMART PINPADCOMMUNICATION	Simple security attributes						X
FDP_ITC.2/TSM	Import of user data with security attributes						X
FDP_ITC.2/EFT-POS/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		

		Access Control	Event Recording	Integrity	Authentication	Accuracy	Secure Transfer
FIA_UAU.4	Single-use authentication mechanisms				X		
FIA_UID.1	Timing of identification				X		
FMT_MOF.1	Management of security functions behaviour	X				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/EFT-POS/SMART PINPADSOURCE 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/EFT-POS/SMART PINPAD	Static attribute initialisation						X
FMT_MTD.1/FCR AUTHORISED USER	Management of TSF data	X			X		
FMT_MTD.1/AUTHORISED 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	

		Access Control	Event Recording	Integrity	Authentication	Accuracy	Secure Transfer
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

7.3.2. Assurance Measures Rational

The assurance measures of the developer as referred in section 7.2 are suitable and sufficient to meet the CC assurance level EAL2 as claimed in section 6.2. In particular, the deliverables listed in chapter 7.2 are suitable and sufficient to document that the assurance requirements are met.

8. 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

GPS : Global Positioning System

IT : Information Technology

ITU : International Telecommunication 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

SFR : Security Functional Requirements

SHA : Secure Hash Algorithm

SPA : Simple Power Analysis

SSL - CA : Secure Sockets Layer - Client Authentication

TOE : Target of Evaluation

TLS 1.2 : Transport Layer Security version 1.2

TSF : TOE Security Functionality (defined in CC)

TSE : Turkish Standards Institute

TSM : Trusted Service Manager

VAT : Value Added Tax

9. BIBLIOGRAPHY

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

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

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

New Generation Cash Register Directives

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

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

[7] External Device Communication Protocol Document, current version