Certification Report

EAL 2 Evaluation of

POS Perkende Otomasyon Sistemleri San. Ve Tic. A.Ş. Toshiba 4610-2nf Fiscal Microcode v.90 Build EB

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-42

TABLE OF CONTENTS

DOCUMENT INFORMATION

Date of Issue	July 8, 2017
Approval Date	July 8, 2017
Certification Report Number	21.0.03/17-005
Sponsor and Developer	POS Perkende Otomasyon Sistemleri San. Ve Tic. A.Ş.
Evaluation Facility	TÜBİTAK BİLGEM
TOE	Toshiba 4610-2nf Fiscal Microcode v.90 Build EB
Pages	22

Prepared by	Cem ERDİVAN
Reviewed by	İbrahim Halil KIRMIZI

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.

DOCUMENT CHANGE LOG

Release	Date	Pages Affected	Remarks/Change Reference
1.0	July 8, 2017	All	First Release

DISCLAIMER

This certification report and the IT product in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1,revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by Beam Technology Testing Facility, which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Toshiba 4610-2nf Fiscal Microcode v.90 Build EB whose evaluation was completed on June 23, 2017 and whose evaluation technical report was drawn up by TÜBİTAK OKTEM (as CCTL), and with the Security Target document with version no 0.D of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

1.1 TOE Overview

The TOE is an application software and crypto coprocessor. Application Software is the main item of a Fiscal Cash Register (FCR). TOE is used to process transaction amount of purchases to be viewed by both seller and buyer. This transaction amount is used to determine tax revenues. Therefore, secure processing, storing and transmitting of this data is very important. The FCR is mandatory for first-and second-class traders. FCR is not mandatory for sellers who sell the goods back to its previous seller completely the same as the purchased good. FCR may consist of different parts. The TOE being the main item of an FCR, there are also several additional components necessary to get a fully functional FCR.

General overview of the TOE and related components

Figure 1 shows the general overview of the TOE and 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 environments which are crucial parts of the FCR for functionality and security. Connections between the TOE and its environment are also subject of the evaluation since they are interfaces of the TOE.
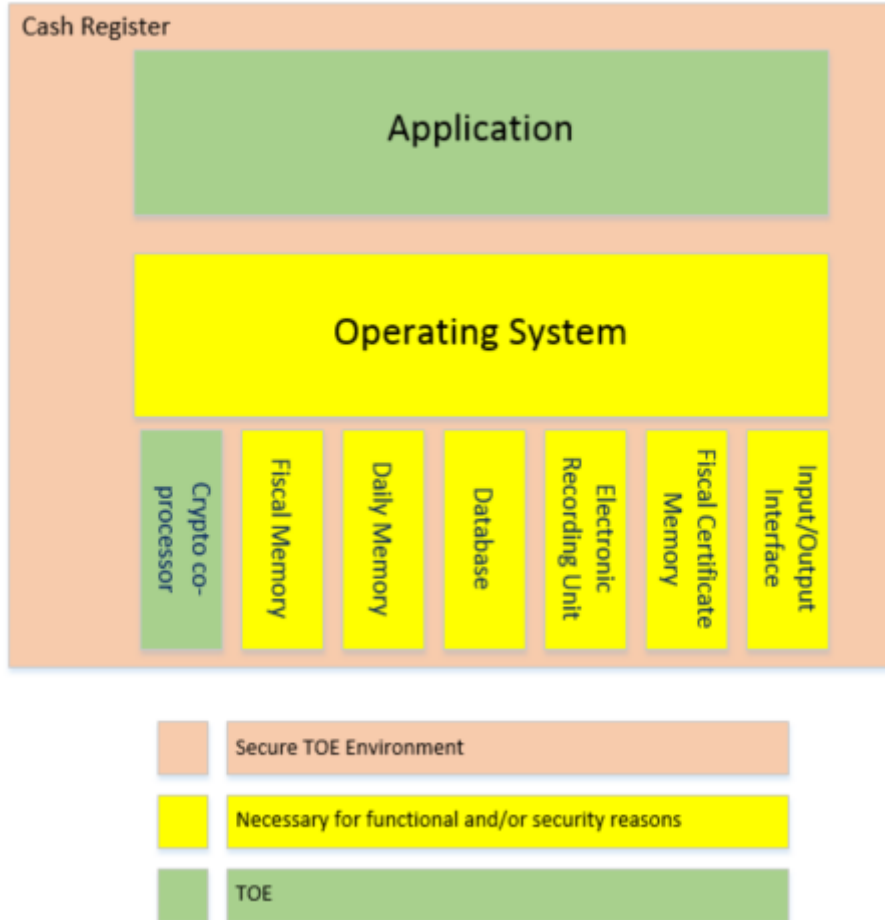

Figure 1- TOE and related components

1.2 Threats

Threats	Definition
T.AccessControl	• Adverse action: Authenticated users could try to use functions which are not allowed. (e.g. FCR Authorised User gaining access to FCR 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 except doing fiscal sales and taking reports which are not fiscal. • Threat agent: An attacker who has basic attack potential, has logical and physical access to the FCR. • Asset: Sales data, event data, time information.

T.MDData	• Adverse action: This threat deals with five types of data: event data, sales data, characterization data, authentication data and FCR parameters.
	    o 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.
	    o 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 located in FCR may be caused by magnetic and electronic reasons.
	    o An attacker could try to manipulate the characterization data to cover information about tax fraud; to masquerade the user identity.
	    o An attacker could try to manipulate the FCR parameters to use FCR in undesired condition.
	    o An attacker also could try to disclose and modify authentication data in FCR to gain access to functions which are not allowed to his/her.
	
	• Threat agent: An attacker who has basic attack potential, has physical and logical access to the FCR.
	
	• Asset: Event data, sales data, characterization data, FCR parameters and authentication data.

T.Eavesdrop	• 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	• 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	• 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.
T. Server counterfeiting	• Adverse action: An attacker could try to imitate PRA-IS by changing server certificates (PPRA and PPRA-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	• 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.

Table 1: Threats

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-42
TOE Name and Version	Toshiba 4610-2nf Fiscal Microcode v.90 Build EB
Security Target Title	Toshiba 4610-2nf Fiscal Microcode v.90 Build EB Security Target
Security Target Version	v0.D
Security Target Date	July 25, 2017
Assurance Level	EAL2
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	NEW GENERATION CASH REGISTER FISCAL APPLICATON SOFTWARE 2.0 (TSE-CCCS/PP-007)
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, extended • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, conformant
Sponsor and Developer	POS Perkende Otomasyon Sistemleri San. Ve Tic. A.Ş.
Evaluation Facility	TÜBİTAK BİLGEM
Certification Scheme	TSE CCCS

2.2 Security Policy

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

1. TOE supports storing sales data in fiscal memory.
2. TOE supports storing for each receipt the total receipt amount and total VAT amount in daily memory.
3. TOE supports generating reports (X report, Z report etc.).

4. TOE supports transmitting Z reports, receipt information, sale statistics and other information determined by PRA to PRA-IS in PRA Messaging Protocol format.
5. TOE stores records of important events as stated in PRA Messaging Protocol document and transmits to PRA-IS in PRA Messaging Protocol [6] format in a secure way.
6. TOE supports using by authorized user or authorized manufacturer user and using in secure state mode or maintenance mode.

The security policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

1. TOE supports access control.
2. TOE is able to detect disconnection between main processor and fiscal memory and should enter into the maintenance mode.
3. 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.
4. TOE supports secure communication between FCR, PRA-IS and FCR TSM.
5. TOE supports secure communication with EFT-POS/ SMART PINPAD
6. TOE ensures the integrity of event data, sales data, authentication data, characterization data and FCR parameters.
7. TOE records important events given in PRA Messaging Protocol document and send urgent event data to PRA-IS in a secure way.
8. TOE detects physical attacks to FCR and enters into the maintenance mode in such cases.

2.3 Assumptions and Clarification of Scope

Policy	Definition
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) certificates 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 - UpdateControl certificate that is used to verify the signature of the TOE.

Table 2: Organizational Security Policies

Assumption	Definition
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 to the FCR in initialization phase. Before certificate installation it is assumed that asymmetric key pair generated in a manner which maintains security posture.
A.TrustedUser	User is assumed to be trusted. It is assumed that for each sale a sales receipt is provided to the buyer.
A.Activation	It is assumed that environment of TOE provides secure activation steps at the beginning of the TOE operation phase and after each maintenance process.
A.AuthorisedService	It is assumed that repairing is done by trusted authorised services. The repairing step is processed in a manner which maintains legal limits.
A.Ext_Key	It is assumed that External Device (EFT-POS/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.

Table 3: Assumptions

2.4 Architectural Information

2.4.1 Logical Scope

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 and EFT-POS Device.

2.4.2 Physical Scope

TOE is microcode running on Montoya Fiscal Processor in Printer hardware following Figure 2 shows high level hardware diagram for the printer:
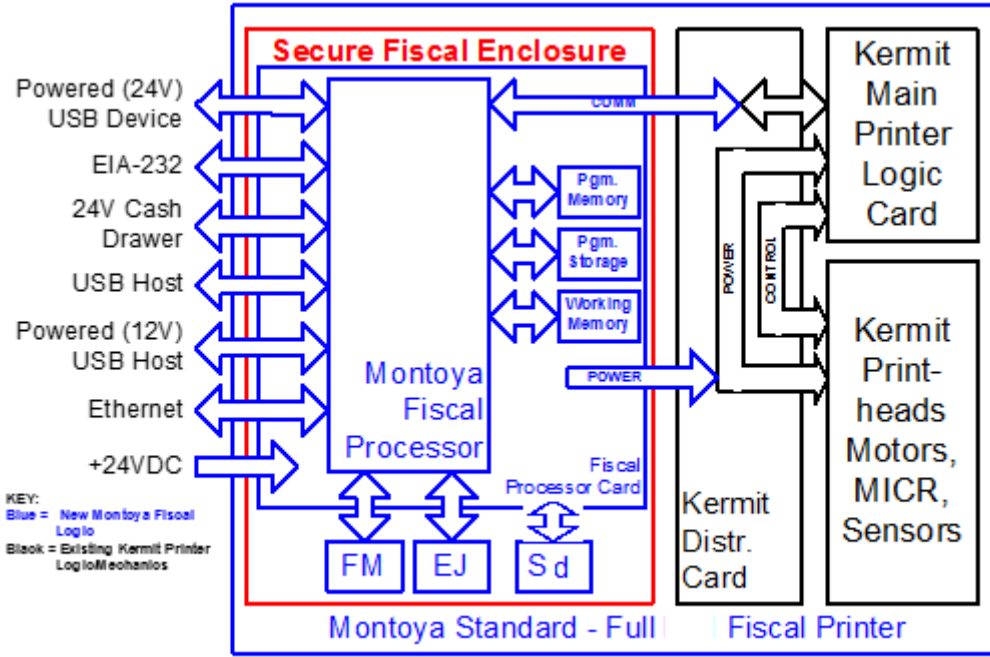
Figure-2 4610-2nf– Montoya Standard High Level Logic Card Block Diagram-1

2.4.3 Software environment of TOE

Application runs at the top of an operating system's kernel, file-system as in a typical software environment. This structure is shown in Table 4.

File System
Operating System Kernel

Table 4 Typical software environment of TOE

In addition to TOE, following software components are necessary for security and functionality of the FCR:
- FCR 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;
  - Database has data recording, organizing, querying, reporting features
  - 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
  - Database has indexing mechanism

2.4.4 Hardware Environment of TOE

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

- Fiscal memory

    o Fiscal memory has following features;
      1. Fiscal memory has the capacity to store at least 10 years (3650 days) of data,
      2. Fiscal memory keeps data at least 5 years after the capacity specified in (a) has been reached,
      3. Fiscal memory is to be fixed in FCR in a way that it cannot be removed without damaging the chassis.
      4. Fiscal memory is protected with mesh cover,
      5. Fiscal memory has the ability to protect against magnetic and electronic threats, When the Fiscal memory and main processor interconnection is interrupted, FCR will begin to run in maintenance mode,
      6. The data stored in the fiscal memory shouldn't be lost in case of power off,
      7. Fiscal Memory accepts only positive amounts from the application and the peripherals,
      8. FCR checks "Z" reports from fiscal memory during device start-up. In case there are days for which Z report was not generated, FCR will be able to run in normal mode only after it generates Z reports for the missing days. Seasonal firms can take cumulative Z report by specifying date and time range.

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

- Daily memory

    o Daily memory has following features;
      1. 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.
      2. Data in the daily memory which is not already transmitted to fiscal memory, cannot be modified in an uncontrolled way.
      3. Data transmitted from daily memory to fiscal memory is to be kept in daily memory for at least 10 days.
      4. Z reports, taken at the end of the day; and X reports, taken within the current day are produced by using the data in the daily memory.

    o Following values are stored in the daily memory
      1. total VAT amount per day,
      2. total daily sales values per day grouped by payment type
      3. payment type (Cash, credit card etc.)
      4. 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;

  1. ERU stores information about receipts and FCR reports (except ERU reports) in a retrievable form.
  2. ERU has at least 1.2 million row capacity. ERU may be included in the sealed part of the FCR. In this case ERU must have at least 40 million row capacity
  3. Data stored in ERU cannot be modified
  4. ERU also 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 device 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 EFTPOS/SMART PINPAD.
- FCR needs some input/output devices for functionalities listed below;
  1. FCR has separate displays for cashier and buyer
  2. FCR has a keyboard unit
  3. FCR has money drawer for keeping cash
  4. FCR has internal battery to keep time information, to protect event data and fiscal memory.
  5. FCR has serial I/O port for barcode reader.

2.5 Documentation

These documents listed below are provided to customer by the developer alongside the TOE:

Document Name	Version	Release Date
Toshiba 4610-2nf Fiscal Microcode v.90 Build EB Security Target	v0.D	July 25, 2017
Toshiba 4610-2nf Fiscal Microcode v.90 Guidance Document	v1.0	December 10, 2015

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report v1.0 of Toshiba 4610-2nf Fiscal Microcode v.90 Build EB. It is concluded that the TOE supports EAL 2.

IT Product Testing is mainly realized in two parts:

1-Developer Testing: (67 Tests)

- **TOE Test Coverage:** Developer has prepared TOE Test Document according to the TOE Functional Specification documentation.
- **TOE Functional Testing:** Developer has made functional tests according to the test documentation. Test plans, test scenarios, expected test results and actual test results are in the test documentation.

2- Evaluator Testing:

Independent Testing: The evaluator conducted testing using 10 of developer tests found in the developer's test plan and procedures. Additionally, the evaluator conducted 17 independent tests prepared by the evaluators themselves. All off these tests have ensured that TOE is capable of demonstrating the functional requirements stated in security document. TOE has successfully passed all tests.

Penetration Testing: Evaluator has done 9 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. During devising the tests, a flaw hypothesis was prepared considering:
- SFRs in security target,
- Architectural elements in architecture document,
- Guidance documents,
- Internet search for publicly known vulnerabilities of TOE and tools used to create TOE etc.

TOE has successfully passed all tests.

2.7 Evaluated Configuration

Processor:

- ARM926EJ-S™ Processor Core with 16KB Data Cache and 32KB Instruction Cache
- 384MHz Core Operating Frequency via PLL
- 192MHz Multilayer AHB Bus Matrix

Memory:

- 384KB System SRAM
- 4KB Instruction TCM, 4KB Data TCM
- 24KB AES User-Encryptable NV SRAM
- Dual External Memory Controller (LPDDR400, SDRAM, SRAM, NOR Flash, NAND Flash)
- 2KB User-Programmable OTP
- NAND Flash Controller with Hardware ECC

I/O and Peripherals:

- USB 2.0 Host/Device with Internal Transceivers
- Three UART Ports/One I2C Port
- Five SPI Ports with I2S Functionality

- Two ISO 7816 Smart Card Interfaces
- SD/SDHC/SDIO Interface
- 10/100Mbps Ethernet MAC Controller
- Thermal Printer Interface
- Three Timers with PWM Capability
- Up to 160 General-Purpose I/O Pins
- 3-Channel, 10-Bit ADC
- LCD Controller Supporting STN and TFT Displays
- Monochrome LCD Controller
- 16-Channel DMA Controller
- Advanced Interrupt Controller

Power Management:

- Flexible Clock Prescalers
- Clock Gating Function
- Low-Current Battery-Backup Operation
- Configurable Low-Power Modes

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL2 and the security target evaluation) is summarized in the following table:

Assurance Class	Component ID	Component Title	Verdict
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.2	Security-enforcing functional specification	PASS
	ADV_TDS.1	Basic design	PASS
AGD: Guidance documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system	PASS
	ALC_CMS.2	Parts of the TOE CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims	PASS
	ASE_ECD.1	Extended components definition	PASS
	ASE_INT.1	ST introduction	PASS
	ASE_OBJ.2	Security objectives	PASS
	ASE_REQ.2	Security requirements	PASS
	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS
ATE: Tests	ATE_COV.1	Evidence of coverage	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS

AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of "Toshiba 4610-2nf Fiscal Microcode v.90 Build EB" product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The security target associated with this Certification Report is identified by the following terminology:
Title: Toshiba 4610-2nf Fiscal Microcode v.90 Build EB Security Target
Version: 0.D
Date of Document: July 25, 2017

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

4 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	: Organizational Security Policy
PP	: Protection Profile
PKI	: Public Key Infrastructure
PRA	: Presidency of Revenue Administration
PRA-IS	: Presidency of Revenue Administration Information Systems
SAR	: Security Assurance Requirements
SEMA	: Simple Electromagnetic Analysis
SFR	: Security Functional Requirements
SHA	: Secure Hash Algorithm
SPA	: Simple Power Analysis
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

.

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012

[3] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel. Date: February 8, 2016

[4] ETR v2.0 of Toshiba 4610-2nf Fiscal Microcode v.90 Build EB, Rel. Date: July 28, 2017

[5] Toshiba 4610-2nf Fiscal Microcode v.90 Build EB Security Target, Version 0.D, Rel. Date: July 25, 2017