Certification Report

EAL 2 Evaluation of

PANAROMA BİLİŞİM TEKNOLOJİLERİ SANAYİ VE TİC. A.Ş. PFAS v1.1

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.01/TSE-CCCS-25

TABLE OF CONTENTS

Document Information

Date of Issue	***12.04.2015***
Version of Report	***v1.0***
Author	***Zümrüt MÜFTÜOĞLU***
Technical Responsible	***Zümrüt MÜFTÜOĞLU***
Approved	***Mariye Umay AKKAYA***
Date Approved	***13.04.2015***
Certification Report Number	***21.0.01/15-030***
Sponsor and Developer	***PANAROMA Bilişim Teknolojileri Sanayi ve Tic. A.Ş.***
Evaluation Lab	***TÜBİTAK BİLGEM OKTEM***
TOE	***PFAS v1.1***
Pages	***16***

Document Change Log

Release	*Date*	*Pages Affected*	*Remarks/Change Reference*
V1.0	***12.04.2015***	***all***	***Final released***

DISCLAIMER

This certification report and the IT product defined 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 STCD 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) 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 TÜBTAK BİLGEM OKTEM,which is a public/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 PFAS v1.1 whose evaluation was completed on 09.04.2015 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no 1.16 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the STCD 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

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: PFAS

IT Product version: v1.1

Developer's Name: Panaroma

Name of CCTL: TÜBİTAK BİLGEM OKTEM

Assurance Package: EAL 2

Completion date of evaluation: 12.04.2015 (DTR 40 TR 01)

1.1 Brief Description

The TOE addressed by this Security Target (ST) is an application software which is the main items of a Fiscal Cash Register (FCR). TOE is used to process the transaction amount of purchases which can be viewed by both seller and buyer. Since transaction amount is used to determine tax revenues; secure processing, storing and transmission of this data is very important.
The FCR is mandatory for first-and second-class traders and is not mandatory for sellers who sell the goods back to their previous seller as completely the same as the purchased good.
In addition to TOE, which is the main item of FCR, FCR may consist of several other hardware and software components.

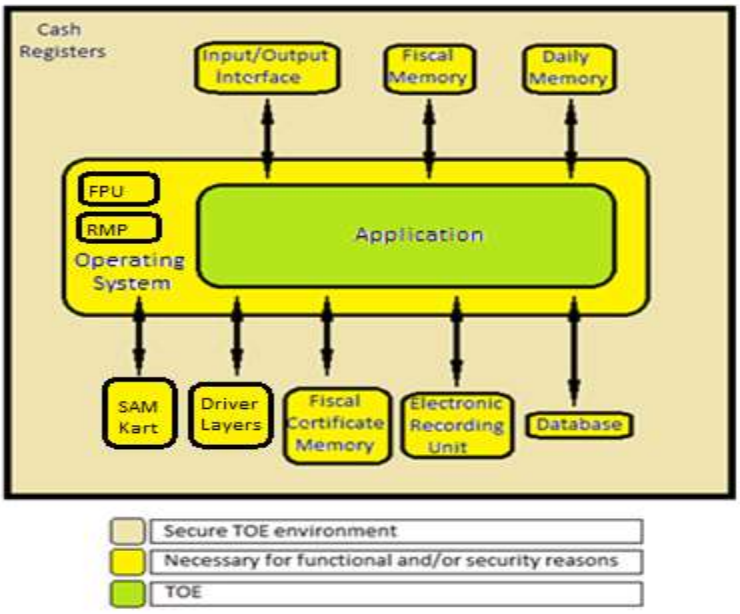

Figure 1 TOE and Related Components

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

the FCR for functionality and security. Connections between the TOE and its environment are also subject to evaluation since these connections are made over the interfaces of the TOE.

1.2 TOE Security Functions

The TOE provides following security features;

i. TOE supports access control.

ii. TOE supports secure communication between main processor and fiscal memory.

However, for the cases where the main processor and the fiscal memory are included within the same electronic seal secure communication is not mandatory. TOE is able to detect disconnection between main processor and fiscal memory and enter into the maintenance mode.

iii. TOE supports usage of ITU X509 v3 formatted certificate and its protected private key for authentication and secure communication with PRA- IS and TSM.

iv. TOE supports secure communication between FCR-PRA-IS and FCR–TSM.

v. TOE ensures the integrity of event data, sales data, authentication data, characterization data and FCR parameters.

vi. TOE records important events defined in PRA Messaging Protocol Document [6] and send urgent event data immediately to PRA-IS in a secure way.

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

1.3 Threats

T.AccessControl
Adverse action: Authenticated users could try to use functions which are not allowed.
(e.g. FCR Users gaining access to FCR Authorised User management functions)
Threat agent: An attacker who has basic attack potential, has physical and logical access to FCR.
Asset: Event data, sales data, time information.

T.Authentication
Adverse action: Unauthorized users could try to use FCR functions.
Threat agent: An attacker who has basic attack potential, has logical and physical access to the FCR
Asset: Sales data, event data, time information

T.MDData - Manipulation and disclosure of data
Adverse action: This threat deals with four types of data: event data, sales data, characterization data and FCR parameters.

- An attacker could try to manipulate the event data to hide its actions and 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.

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.

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

Adverse action: An attacker could try to eavesdrop event data, sales data and characterization data transmitted between the TOE and the PRA-IS and also between the TOE and the distributed memory units (Fiscal memory, Database, Daily memory, ERU).
Threat agent: An attacker who has basic attack potential, physical and logical access to the FCR.
Asset: Characterization data, sales data, and event data.

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

Adverse action: An attacker could try to imitate PRA-IS to receive information from FCR and to imitate TSM to set parameters to FCR via the communication channel.
Threat agent: An attacker who has basic attack potential and logical access to the FCR.
Asset : Sales data, and event data, FCR parameters.

T.Counterfeit - FCR counterfeiting

Adverse action: An attacker could try to imitate FCR by using sensitive(session keys) data while communicating with PRA-IS and TSM to cover information about tax fraud.
Threat agent: An attacker who has basic attack potential, has physical and logical access to the FCR.
Asset: Sensitive data (session keys).

T.Malfunction - Cause malfunction in FCR

Adverse action: An attacker may try to use FCR out of its normal operational conditions to cause malfunction without the knowledge of TOE.
Threat agent: An attacker who has basic attack potential, has physical access to the FCR.
Asset: Sales data, event data.

T.ChangingTime

Adverse action: An attacker may try to change time to invalidate the information about logged events and reports in FCR.
Threat agent: An attacker who has basic attack potential, has physical and logical access to the FCR.
Asset: Time Information.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	*21.0.01/TSE-CCCS-25*
TOE/PP Name and Version	*PFAS v1.1*
Security Target Document Title	*PFAS Security Target*
Security Target Document Version	*V1.16*
Security Target Document Date	*12.04.2015*
Assurance Level	*EAL 2*
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 Fiscal Application Software Protection Profile TSE-CCCS/PP-006, version 1.8, 18 December 2014*
Common Criteria Conformance	*•Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012, conformant* *•Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012, conformant*
Sponsor and Developer	*Panaroma Bilişim Teknolojileri San. Ve Tic. A.Ş.*
Evaluation Facility	*TÜBİTAK BİLGEM OKTEM*
Certification Scheme	*TSE-CCCS*

2.2 Security Policy

Organizational Security Policies are;

P.Certificate

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

P.Comm_EXT - Communication between TOE and External Device

It has to be assured that communication between TOE and external devices is used to encrypted using AES algorithm with 256 bits according to PRA Messaging Protocol Document[6].

P.InformationLeakage - Information leakage from FCR

It has to be assured that TOE's environment provides a secure mechanism which prevents attacker to obtain sensitive information (secret key) when FCR performs encryption 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. Moreover, it has to be assured that fiscal memory doesn't accept transactions with negative amounts which results in a decrease of total tax value. Also it has to be assured that environment of TOE provides a mechanism that sales data in daily memory which is not reflected to the fiscal memory cannot be deleted and modified in an uncontrolled way. In addition to this, it has to be assured that sales data in ERU cannot be deleted and modified.

P.PhysicalTamper

It has to be assured that TOE environment and TOE provide a tamper respondent system which is formed by electromechanical seals. It has to be assured that physical tampering protection system protects the keys (asymmetric key, symmetric key), the certificates, event data, characterization data, FCR parameters and sales data in FCR. It has to be assured that TOE logs this type of events and enters into the maintenance mode when physical tampering protection system detect unauthorised access. On the other hand it has to be assured that authorised access such as maintenance work or service works are logged.

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

P.PKI - Public key infrastructure

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

P.UpdateControl

TOE is allowed to be updated by only TSM or Authorised Manufacturer User to avoid possible threats during this operation, FCR shall verify the signature of the new version of TOE to ensure that the TOE to be updated is signed by the correct organisation. Thus, the TOE to be updated is ensured to be the correct certified version because only the certified versions will be signed. In addition, FCR shall check version of TOE to ensure that it is the latest version.

2.3 Assumptions and Clarification of Scope

Assumptions for the operational environment of the composite TOE are;

A.TrustedManufacturer

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

A.Control

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

A.Initialisation

It is assumed that environment of TOE provides secure initialization steps. Initialization step is consist of secure boot of operating system, and integrity check for TSF data. Moreover, it is assumed that environment of TOE provides secure installation of certificate to the FCR in initialization phase. Before certificate installation it is assumed that asymmetric key pair generated in a manner which maintains security posture.

A.TrustedUser

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

A.Activation

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

A.AuthorizedService

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

A.Ext_Key

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

2.4 Architectural Information

As the TOE is software, the subsystems described here are actual software modules implemented as libraries or independent objects those are linked together producing a single binary.

Each subsystem is in charge of very specific and specialized tasks in the context of the TOE and work together with the rest of the modules to produce the desired TOE complex behavior.

TOE has following subsystems:

- Communications Interface
- User Interface
- SSL Library

- Authentication and Access Control
- Logger
- Operative functions
- Maintenance functions
- ERU Database Controller
- Fiscal Database Controller
- Daily Database Controller
- Scheduler
- SW Update Manager
- Self-Test
- Fiscal Configuration Manager
- Firewall Manager
- PSAM Card Client
- Secure IC Client

The TOE must run over an operating system (A customized Linux OS running kernel v3.2.0) providing;

-Device Drivers

Network Ethernet
Network PSTN or GPRS
Serial port RS232 (to internal or external devices)
USB Port (for peripherals)
Printer
PSAM Card (to store sensitive data)
Secure IC (to control security sensitive devices and data)
User Console (Keyboard and Displays)
Physical media (SD cards, NAND Flash)
File systems
Buzzer

-Software Libraries (abstracting devices, of functions)

-Network connectivity (controlled by a Firewall (IPTables Firewall v1.4.15))

-File system (abstracting several device media)

2.5 Documentation

Name of Document	Version Number	Publication Date
PFAS v1.1 Security Target	1.16	12.04.2015
PFAS v1.1 Security Architecture	1.6	31.03.2015
PFAS v1.1 Configuration	1.20	12.04.2015

Management Plan		
PFAS v1.1 Teslim Prosedürleri	1.5	12.04.2015
PFAS v1.1 Functional Specification	1.8	29.03.2015
PFAS v1.1 TOE Design	1.9	29.03.2015
PFAS v1.1 Test Documentation	1.7	31.03.2015
PFAS v1.1 Kurulum Prosedürü	1.5	31.03.2015
Olivetti PBT 900 Elektronik Yazar Kasa Türkçe Tanıtma ve Kullanım Kılavuzu	1.6	12.04.2015

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 (ETR) of PFAS v1.1

It is concluded that the TOE supports EAL 2. There are 19 assurance families which are all evaluated with the methods detailed in the ETR.
IT Product Testing is mainly described in two parts:

2.6.1 Developer Testing:

•TOE Test Coverage: Developer has prepared TOE System Test Document according to the TOE Functional Specification documentation.
•TOE Test Depth: Developer has prepared TOE System Test Document according to the TOE Design documentation which includes TSF subsystems and its interactions.
•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.

2.6.2 Evaluator Testing:

•Independent Testing: Evaluator has done a total of 19 sample independent tests. 7 of them are selected from developer`s test plans. The other 12 tests are evaluator`s independent tests. All of them are related to TOE security functions.
•Penetration Testing: Evaluator has done 10 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. The potential vulnerabilities and the penetration tests are in "TOE Security Functions Penetration Tests Scope" and the penetration tests and their results are available in detail in the ETR document as well.

2.7 Evaluated Configuration

During the evaluation; the configuration of evaluation evidences which are composed of Common Criteria documents, sustenance documents and guides are shown below;

Name of Document	Version Number	Publication Date
PFAS v1.1 Security Target	1.16	12.04.2015
PFAS v1.1 Security Architecture	1.6	31.03.2015
PFAS v1.1 Configuration Management Plan	1.20	12.04.2015
PFAS v1.1 Delivery Procedures	1.5	12.04.2015
PFAS v1.1 Functional Specification	1.8	29.03.2015
PFAS v1.1 TOE Design	1.9	29.03.2015
PFAS v1.1 Test Documentation	1.7	31.03.2015
Olivetti PBT 900 E-P-G User Manual	1.6	12.04.2015

Table 2 – Documentation

2.8 Results of the Evaluation

Table 3 below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 2 (EAL 2) components as specified in Part 3 of the Common Criteria;

Assurance Class	Component	Component Title
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage

Life-Cycle Support	ALC_DEL.1	Delivery Procedures
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
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing
Vulnerability Analysis	AVA_VAN.2	Vulnerability analysis

Table 3 – Security Assurance Requirements of TOE

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE "PFAS v.1." the results of the assessment of all evaluation tasks are "**Pass**".

The result of AVA_VAN.2 evaluation is given below:

It is determined that TOE, in its operational environment, is resistant to an attacker possessing **"Basic"** attack potential.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of "PFAS v1.1" 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: PFAS v1.1 Security Target

Version: v1.16

Date of Document: 12.04.2015

4 GLOSSARY

ADV : Assurance of Development

AGD : Assurance of Guidance Documents

ALC : Assurance of Life Cycle

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCRA : Common Criteria Recognition Arrangement

CCTL : Common Criteria Test Laboratory (OKTEM)

CEM :Common Evaluation Methodology

CMC : Configuration Management Capability

CMS : Configuration Management Scope

DEL : Delivery

EAL : Evaluation Assurance Level

FCR: Fiscal Cash Register

OR : Observation Report

OKTEM : Ortak Kriterler Test Merkezi

OPE : Opretaional User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

PRA: Presidency of Revenue Administration

PRE : Preperative Procedures

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

STCD :Software Test and Certification Department

TOE : Target of Evaluation

TSF : TOE Security Functionality

TSFI : TSF Interface

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] CC Supporting Document Guidance, Mandatory Technical Document Composife Product Evaluation for Smart Cards and Similar Devices,April,2012,CCDB-2012-04-001

[4] YTBD-01-01-TL-01 Certification Report Preparation Instructions, Rel.Date: July,30,2013

[5] PRA Messaging Protocol, v2.02

[6] Technical Guidance (TK1), version 2.0

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections