	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No



Certification Report

EAL 2 Evaluation of

ENCORE Bilişim Sistemleri Ltd. Şti.

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)

issued by

**Turkish Standards Institution
Common Criteria Certification Scheme**

Certificate Number: 21.0.03/TSE-CCCS-48



	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

TABLE OF CONTENTS

TABLE OF CONTENTS	2
DOCUMENT INFORMATION	3
DOCUMENT CHANGE LOG	3
DISCLAIMER	4
FOREWORD	5
RECOGNITION OF THE CERTIFICATE	7
1. EXECUTIVE SUMMARY	8
1.1 TOE Overview	8
General overview of the TOE and related components	8
1.2 TOE major security features	9
1.3 Threats	9
2 CERTIFICATION RESULTS.....	11
2.1 Identification of Target of Evaluation	11
2.2 Security Policy	12
2.3 Assumptions and Clarification of Scope	14
2.4 Architectural Information.....	15
2.4.1 Logical Scope	15
2.4.2 Physical Scope.....	15
2.5 Documentation	16
2.6 IT Product Testing.....	16
2.7 Evaluated Configuration	17
2.8 Results of the Evaluation.....	18
2.9 Evaluator Comments / Recommendations	19
3 SECURITY TARGET	19
4 ACRONYMS.....	20
5 BIBLIOGRAPHY.....	21

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

DOCUMENT INFORMATION


<i>Date of Issue</i>	January 11, 2018
<i>Approval Date</i>	January 12 , 2018
<i>Certification Report Number</i>	21.0.03/18-001
<i>Sponsor and Developer</i>	ENCORE Bilişim Sistemleri Ltd. Şti.
<i>Evaluation Facility</i>	TÜBİTAK BİLGEM OKTEM
<i>TOE</i>	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)
<i>Pages</i>	21

<i>Prepared by</i>	H.Eda BİTLİSLİ ERDİVAN
<i>Reviewed by</i>	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

<i>Release</i>	<i>Date</i>	<i>Pages Affected</i>	<i>Remarks/Change Reference</i>
1.0	January 11, 2018	All	First Release

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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 Tübitak Bilgem OKTEM 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 NCR E10 New Generation FCR 2.0 whose evaluation was completed on January 11, 2018 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no 2.8 of the relevant product.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

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).


	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

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 EAL2. The current list of signatory nations and approved certification schemes can be found on:

<http://www.commoncriteriaportal.org>.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

1. EXECUTIVE SUMMARY

1.1 TOE Overview

The TOE 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 version 0.0.6) 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 ST for full functionality.

General overview of the TOE and related components

Figure 1 shows the general overview of the TOE and its related components. 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.

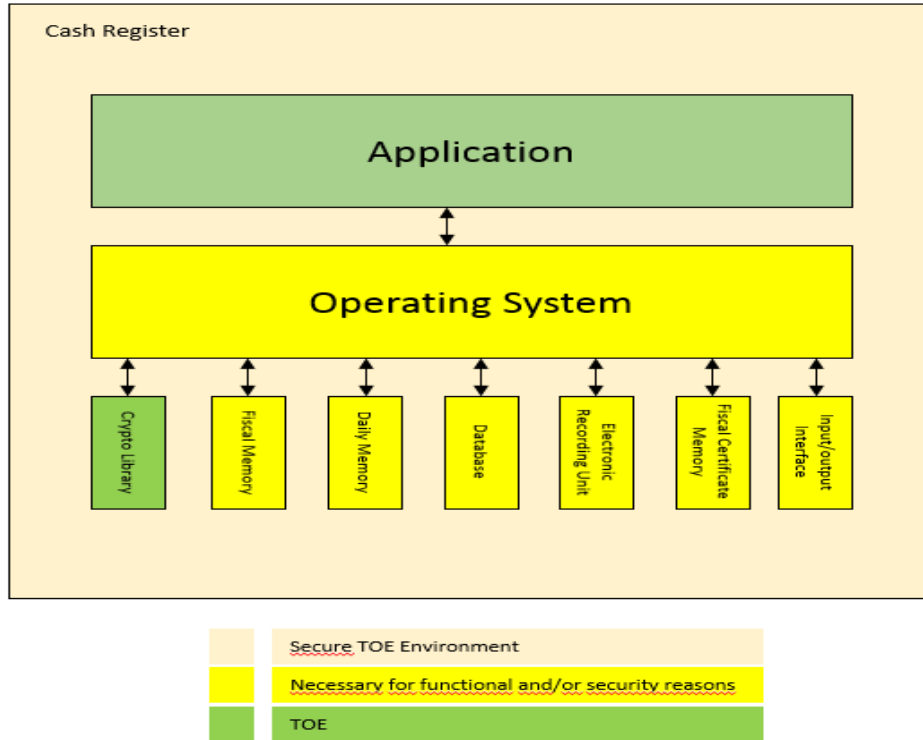



Figure 1 TOE and related components

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

1.2 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 [4] 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 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.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

- 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).

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

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 - 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

<i>Certificate Number</i>	21.0.03/TSE-CCCS-48
<i>TOE Name and Version</i>	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)
<i>Security Target Title</i>	NCR E10 New Generation FCR Security Target
<i>Security Target Version</i>	v2.8
<i>Security Target Date</i>	January 8, 2018
<i>Assurance Level</i>	EAL2
<i>Criteria</i>	<ul style="list-style-type: none"> • 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

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

<i>Methodology</i>	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
<i>Protection Profile</i>	NEW GENERATION CASH REGISTER FISCAL APPLICATION SOFTWARE 2.0 (TSE-CCCS/PP-007)
<i>Common Criteria</i>	<ul style="list-style-type: none"> • 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
<i>Sponsor and Developer</i>	ENCORE Bilişim Sistemleri Ltd. Şti.
<i>Evaluation Facility</i>	TÜBİTAK BİLGEM OKTEM
<i>Certification Scheme</i>	TSE CCCS

2.2 Security Policy


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-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.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

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.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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.

2.3 Assumptions and Clarification of Scope

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.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

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, EFT-POS Device and Main Unit A more detailed description of the implementation of these security functions is provided in “**Hata! Başvuru kaynağı bulunamadı.**” part of Security Target.

2.4.2 Physical Scope

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)

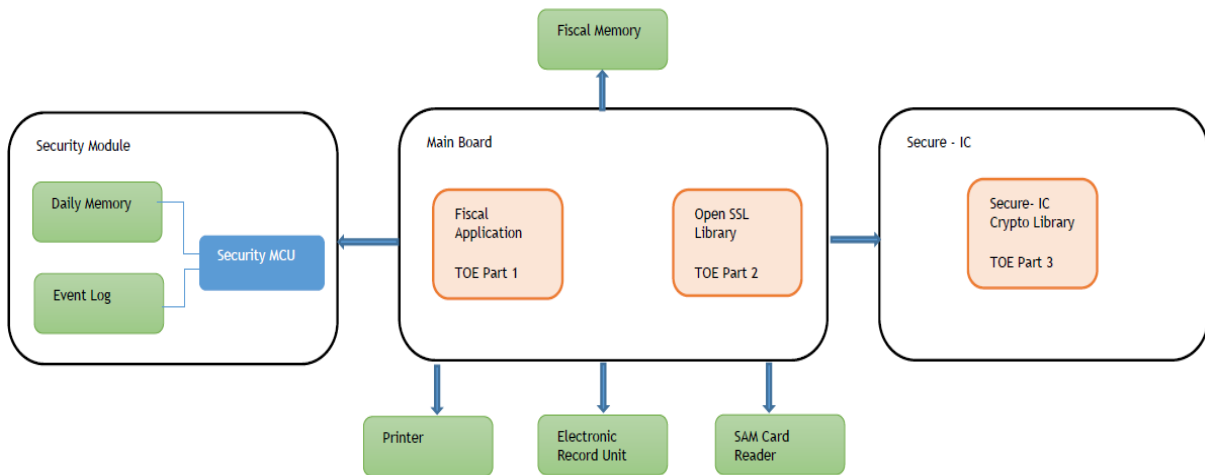



Figure 2 TOE parts

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

2.5 Documentation

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

Document Name	Version	Release Date
NCR e10 Security Target	2.8	08.01.2018
NCR e10 Operational User Guidance	1.4	20.12.2017

Table-5 Documentation

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 v3.0 of NCR E10 New Generation FCR 2.0. It is concluded that the TOE supports EAL 2.

IT Product Testing is mainly realized in two parts:

1-Developer Testing:

Developer has done total of 89 functional 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 9 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 10 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,

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

- 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

Evaluated Configuration of TOE is 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). Also TOE has been tested according to appliance which configuration listed below.

Central Processor :

MAX32550 DeepCover Secure Cortex-M3 Flash Microcontroller
ARM® Cortex® M3 Processor Core Allows for Easy
Integration into Applications

- 108MHz Core Operating Frequency Through PLL
- 1MB Dual-Bank Flash Memory with Cache
- 256KB System SRAM
- 8KB AES Self-Encrypted NVSRAM
- Security Features Facilitate System-Level Protection
- Secure Boot Loader with Public Key Authentication
- AES, DES and SHA Hardware Accelerators
- Modulo Arithmetic Hardware Accelerator (MAA)
Supporting RSA, DSA, and ECDSA
- 8-Line Secure Keypad Controller
- Hardware True Random-Number Generator
- Die Shield with Dynamic Fault Detection
- 6 External Tamper Sensors with Independent
Random Dynamic Patterns
- 256-Bit Flip-Flop-Based Battery-Backup AES Key
Storage
- Temperature and Voltage Tamper Monitor
- Real-Time Clock
- Integrated Peripherals Reduce External Component Count
- Triple-Track Magnetic Stripe Head Interface
- One ISO 7816 Smart Card Interface with Integrated
Transceiver (1.8V, 3V, and 5V)
- USB 2.0 Device with Internal Transceiver and
Dedicated PLL
- 3 SPI Ports, 2 UART Ports, and 1 I2C Controller
- 6 Timers, 4 with PWM Capability
- Up to 70 General-Purpose I/O Pins
- 2-Channel, 10-Bit ADC and 1-Channel, 8-Bit DAC
- Color/Monochrome LCD TFT Controller
- 4-Channel DMA Controller

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

- Power Management Optimizes Battery Life and Reduces Active Power Consumption
- Single 3.3V Supply Operation*
- Integrated Battery-Backup Switch
- Clock Gating Function
- Low-Current Battery-Backup Operation

Financial Memory:

- 32 Bit ARM Cortex M3 processor (48 Mhz)
- 256 MB Nand flash
- 32KB NVRAM
- Μολι Μοδ\λ\ βεσλεμεν πιλ: CR 2450 Lithium battery (10 years)

Battery which supports Tamper Mechanism:

CR2477 1Ah

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


	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

Table-6 Results of the evaluation

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “NCR E10 New Generation FCR 2.0” 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: NCR E10 New Generation FCR Security Target

Version: 2.8


Date of Document: January 8, 2018

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.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

4 ACRONYMS

AES	: Advanced Encryption Standard
CC	: Common Criteria
CCMB	: Common Criteria Management Board
DEMA	: Differential Electromagnetic Analysis
DFA	: Differential Fault Analysis
DPA	: Differential Power Analysis
EAL	: Evaluation Assurance Level (defined in CC)
EFT-POS	: Electronic Funds Transfer at Point of Sale
ERU	: Electronic Recording Unit
FCR	: Fiscal Cash Register
FCRAS	: Fiscal Cash Register Application Software
GMP	: GIB Messaging Protocol
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
ST	: Security Target
TOE	: Target of Evaluation
TSF	: TOE Security Functionality (defined in CC)
TSE	: Türk Standartları Enstitüsü
TSM	: Trusted Service Manager
VAT	: Value Added Tax
FMC	: Peripheral's control card of TOE

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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