Certification Report

EAL 4+ (ALC_DVS.2)
Evaluation of

TÜBİTAK BİLGEM UEKAE
KURUMSAL KART ERİŞİM CİHAZI UYGULAMA YAZILIMI (KKEC_UY) v1.41.06A
KKEC APPLICATION SOFTWARE v1.41.06A

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Date : 20.12.2011
Pages : 24
Certification Report Number :14.10.01/11-520

This page left blank on purpose.

----- o -----

TABLE OF CONTENTS:

FIGURES:

TABLES:

This page left blank on purpose.

----- o -----

CERTIFICATION REPORT

The Certification Report is drawn up to submit the Certification Committee 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 PCC Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

1. INTRODUCTION

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(refers to CCTL) 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 with respect to that standard by the Turkish Accreditation Agency (TÜRKAK), the national accreditation body in Turkey. The evaluation and tests related with the concerned product have been performed by TÜBİTAK-BİLGEM-UEKAE-OKTEM, which is a public 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 Kurumsal Kart Erişim Cihazı Uygulama Yazılımı (KKEC_UY) v1.41.06A - KKEC Application Software Version 1.41.06A whose evaluation was completed on 24.11.2011 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the Security Target document with version no 1.18 of the relevant product.

2. GLOSSARY

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AKİS	Akıllı Kart İşletim Sistemi (Smartcard Operating System)
APDU	Application Protocol Data Unit
ASGS	Akıllı Kart Tabanlı Sosyal Güvenlik Sistemi (Smartcard Based Social Security System)
CC	Common Criteria
CCID	Chip/Smart Card Interface Devices
CPU	Central Processing Unit
CTN	Cihaz Takip Numarası (Device Track Number)
DC	Direct Current
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
EDH	Ephemeral Diffie-Hellman
EKK	Elektronik Kimlik Kartı (Electronic Identity Card)
EKDS	Elektronik Kimlik Doğrulama Sistemi (Electronic Identity Verification System)
EU	Eczane Uygulaması (Pharmacy Application)
GEM	Güvenli Erişim Modülü (Security Access Module)
GSP	Güvenlik Servisleri Platformu (Security Services Platform)
HMAC	Hash Message Authentication Code
IC	Integrated Circuit
IK	Imza Kartı (Signature Card)
KDB	Kimlik Doğrulama Bildirimi (Identity Verification Assertion)
KDP	Kimlik Doğrulama Politikası (Identity Verification Policy)
KDPS	Kimlik Doğrulama Politika Sunucusu (Identity Verification Policy Server)
KDS	Kimlik Doğrulama Sunucusu (Identity Verification Server)
KKEC	Kurumsal Kart Erişim Cihazı (Institutional Smartcard Access Device)
KECÖB	Kart Erişim Cihazı Özelleştirme Birimi (Smartcard Access Device Personalization

	Unit)
KSTB	Kart Sahibinin Tek Belirleyicisi (Card Holder Unique Identifier)
MEDULA	Online Certificate Status Protocol
OCSP	Online Certificate Status Protocol
OCSPS	Online Certificate Status Protocol Server
OYA	Otomasyon Yazılımı Arabirimi (Automation Software Interface)
PGS	Performans Gözlem Sunucusu (Performance Observation Server)
PIN	Personal Identification Number
RSA	Rivest – Shamir – Adleman (RSA Algorithm)
SC	Smartcard
SGK	Sosyal Güvenlik Kurumu (Social Security Association)
SFR	Security Functional Requirement
SPS	Software Publisher Server
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TPDU	Transmission Protocol Data Unit
TSF	TOE Security Function
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (Scientific and Technologic Research Association of Turkey)
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (National Research Institute of Electronics and Cryptology)
USB	Universal Serial Bus
USB-CCID	Universal Serial Bus – Chip/Smart Card Interface Devices
USB-DFU	Universal Serial Bus – Device Firmware Upgrade

3. EXECUTIVE SUMMARY

Evaluated IT product name:

Kurumsal Kart Erişim Cihazı Uygulama Yazılımı (KKEC_UY) v1.41.06A

KKEC Application Software Version 1.41.06A

IT Product version:

v1.41.06A

Developer`s Name:

TÜBİTAK-BİLGEM-UEKAE Tasarım ve Geliştirme Müh. Birimi-2

Name of CCTL :

TÜBİTAK BİLGEM UEKAE OKTEM Common Criteria Test Laboratory

Completion date of evaluation :

24.11.2011

Common Criteria Standard version :

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3, July 2009
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 3, July 2009

Common Criteria Evaluation Method version :

- Common Methodology for Information Technology Security Evaluation v3.1 rev3, July 2009

Short summary of the Report:

1) **Assurance Package :**

EAL 4+ (ALC_DVS.2)

2) Functionality :

TOE is the application software which is loaded into the embedded flash memory of KKEC. It provides personal identity verification (PIV) and digital signature operations for smartcard based services over electronic media.

TOE SECURITY FUNCTIONS

Sign	In "*Sign*" security function; hash value of a given data is calculated and the result is encrypted (signed) by a smartcard inserted to KKEC using private key of a user's certificate. SHA-256 algorithm is used for hash calculation and 2048-bit RSA algorithm is used for data encryption.
Sign Verification	In "*Sign Verification*" security function; after verification of sign certificate, signed data is decrypted by public key of this certificate and the result is compared with calculated hash value of given data. SHA-256 algorithm is used for hash calculation and 2048-bit RSA algorithm is used for decryption.
Data Encryption using AES Algorithm	In "*Data Encryption using AES Algorithm*" security function; the data is encrypted using AES algorithm with a specified 256-bit key.
Data Decryption using AES Algorithm	In "*Data Decryption using AES Algorithm*" security function; the data is decrypted using AES algorithm with a specified 256-bit key.
Secure GEM/EKK/IK Communication	In "*Secure GEM/EKK/IK Communication*" security function; the smartcard inserted to the specified smartcard slot is set into secure operation mode. In case of failure an audit record is created. In secure communication, the data transferred between the TOE and any smartcard is in encrypted form. The encryption is done using 3DES algorithm with a specified 128-bit session key. A session key is generated by the TOE and smartcard before secure communication starts.
Remote Software Upgrade	In "*Remote Software Upgrade*" security function; remote upgrade of TOE is done securely.
EKK Authentication using KSTB	In "*EKK Authentication using KSTB*" security function; the TOE authenticates EKK using KSTB (Cardholder Unique Identifier).

EKK/IK Authentication using Asymmetric Method	In "*EKK/IK Authentication using Asymmetric Method*" security function; the TOE authenticates EKK/IK.
GEM Authentication using Symmetric Method	In "*GEM Authentication using Symmetric Method*" security function; the TOE authenticates GEM.
Validation of GEM Sign Certificate	In "*Validation of GEM Sign Certificate*" security function; the TOE validates GEM sign certificate using OCSP.
User Identification using PIN Verification Method	In "*User Identification using PIN Verification Method*" security function; PIN entered by the user is compared with PIN available within the user's EKK. The comparison is done inside the smartcard and the result is returned to the TOE.
User Identification using Fingerprint Verification Method	In "*User Identification using Fingerprint Verification Method*" security function; fingerprint data read from the fingerprint sensor is compared with the fingerprint data within the cardholder's EKK/IK. The comparison is done by TOE.
User Identification using Fingervein Verification Method	In "*User Identification using Fingervein Verification Method*" security function; fingervein data read from the fingervein device is compared with the fingervein data within the cardholder's EKK/IK. The comparison is done by the fingervein device and a score is sent to TOE. TOE decides if they match.
User Identification using Digital Photo Inspection	In "*User Identification using Digital Photo Inspection*" security function; the cardholder's digital image stored in his/her EKK/IK is displayed on the LCD screen of KKEC.
Secure GSP Communication	In "*Secure GSP Communication*" security function; secure communication session is established between the TOE and GSP.
Secure OYA Communication	In "*Secure OYA Communication*" security function; secure communication session is established between the TOE and OYA.

Secure HUBC Communication	In "*Secure HUBC Communication*" security function; secure communication session is established between the TOE and HUBC.
Fingerprint Test	In "*Fingerprint Test Method*" security function; TOE tests the operation of the fingerprint sensor and the software functions for fingerprint verification.
Fingervein Test:	In "*Fingervein Test Method*" security function; TOE tests the operation of the fingervein device connected to KKEC externally and the software functions for fingervein verification.
Review Audit Records	In "*Review Audit Records*" security function; all audit records can be displayed by TOE on the device screen with "time of origin", "location of origin" and "identity of origin" attributes in time order.

3) Summary of Threats and Organizational Security Policies (OSPs) addressed by the evaluated IT product:

Threat Agents

A threat agent to the TOE can be:

- **User:** A person who has received a KKEC in an authorized way and who wants to alter transaction data or:
  - To replace at least one of the internal TOE assets by fake ones.
  - To alter the TOE to use it in an unauthorized manner.
  - To tamper the TOE in order to obtain security relevant information.
- **Aggressor:** A person who has received a KKEC in an unauthorized way and wants to alter transaction data or:
  - To replace at least one of the internal TOE assets by fake ones.
  - To alter the TOE to use it in an unauthorized manner.
  - To tamper the TOE in order to obtain security relevant information.

Threats covered by the TOE

T_TECH	Due to technical failure of some critical components, TOE security functions may not execute as expected as in its secure state. These failures may not make the TOE stop functioning completely but may affect its security.
T_PNTR	By a threat agent, unauthorized opening of KKEC to obtain or modify security relevant data within TOE during the use stage.

Threats covered by the TOE and the environment

T_KKEC	A threat agent may use a fake KKEC to obtain a TOE service in an unauthorized way.
T_SC	A threat agent may use a fake EKK or IK to obtain a TOE service in an unauthorized way.
T_GSP	A threat agent may imitate GSP to connect to TOE or modify the data between TOE and GSP in order to obtain a service in an unauthorized way.
T_HUBC	A threat agent may use a fake HUBC to obtain PIN or biometric information of users or modify the data transferred by in order to obtain a service in an unauthorized way.
T_OCSPS	A threat agent may imitate OCSPS or modify the data sent by OCSPS in order to obtain a service in an unauthorized way.
T_SPS	A threat agent may imitate SPS or modify the software upgrade packets sent by SPS in order to modify TOE in an unauthorized way.
T_FRAUD	A threat agent may use somebody else's valid EKK or IK to obtain a TOE service in an unauthorized way.
T_MNTR	By a threat agent, unauthorized local or remote monitoring of electromagnetic radiation emitted from KKEC or directly the data transferred between KKEC and other environmental components (GSP/OYA, HUBC and EKK/IK/GEM) to discover security relevant information during the use stage.
T_REPU	A user may repudiate an operation performed by the TOE with his/her approval.

Organisational Security Policies

No Organizational Security Policy.

4) Disclaimers:

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 3, using Common Methodology for IT Products Evaluation, version 3,1, revision 3. 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.

4. IDENTIFICATION

TOE is the application software which is loaded into the embedded flash memory of KKEC. It provides personal identity verification (PIV) and digital signature operations for smartcard based services over electronic media.TOE has the following features:

- Cardholder authentication by using PIN and biometrics (either fingerprint data or fingervein data),
- Authentication of EKK/IKs and authentication of KKEC using GEM (Security Access Module, available as a SIM card):
  - Authentication of EKK/IK by using asymmetric authentication method,
  - Authentication of GEM by using symmetric authentication method,
- Symmetric and asymmetric encryption and decryption using 128-bit DES3, 256-bit AES and 2048-bit RSA algorithms,
- HMAC using 256-bit SHA algorithm,
- Digital sign and sign verification using 2048-bit RSA algorithm,
- Provable non-repudiation
- Secure communication by using TLS v1.0,

- Automatic, remote and secure upgrade

TOE is to be distributed and used with only KKEC and it will manage only smartcards with AKİS (version 1.2.1i and 1.2.1n) and UKİS (version 1.2.1) operating systems for security reasons.

5. SECURITY POLICY

The security policy of TOE is defined by the following TOE security functional requirements:

- Security Audit
- Communication
- Cryptographic support
- User Data Protection
- Identification and Authentication
- Protection of the TSF
- Trusted Path/Channels

Further details on these security policies are found in Section 6 of the ST_Lite.

6. ARCHITECTURAL INFORMATION

Operational Environment Components

a-Hardware Environment

TOE runs as the application software of KKEC. Therefore, the hardware components of KKEC compose the hardware environment of TOE.

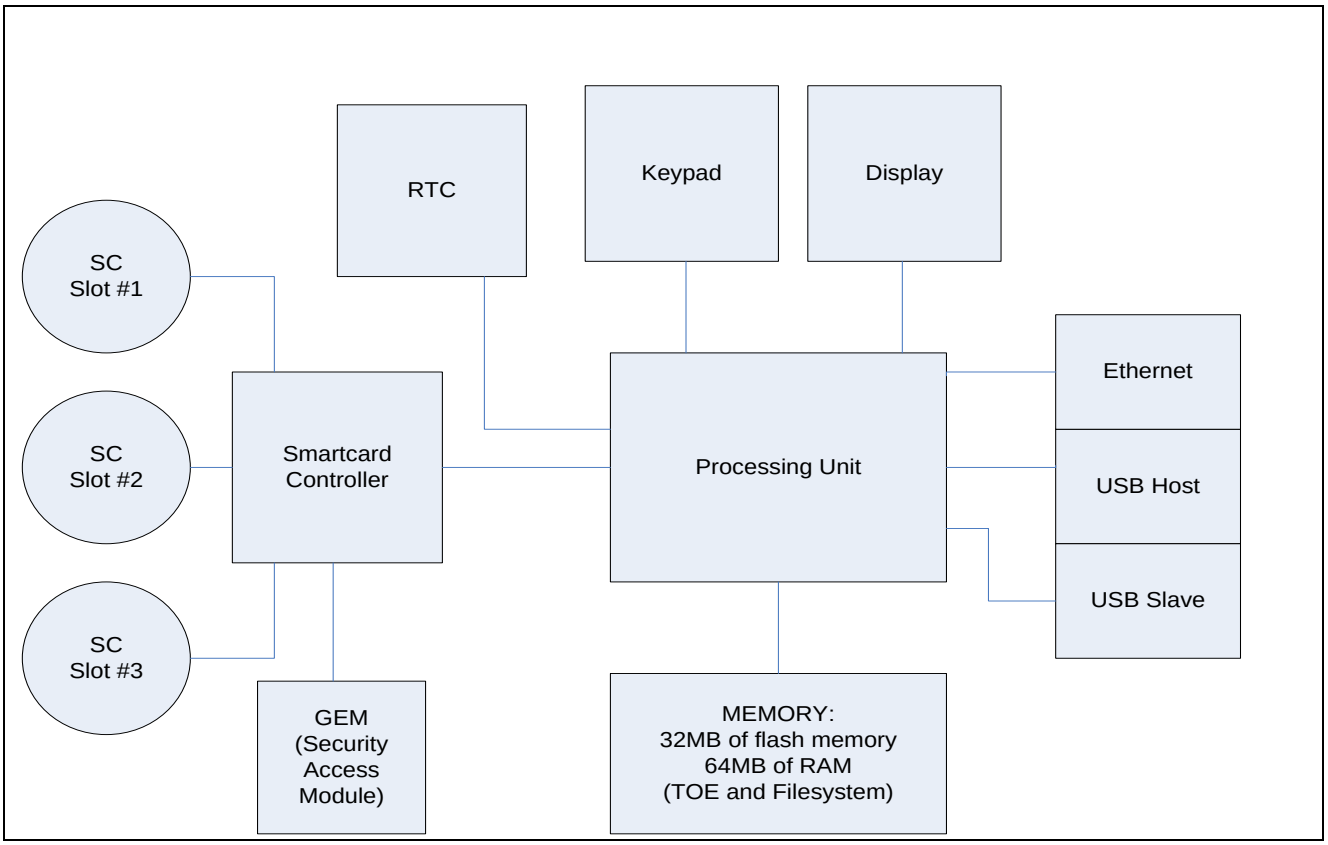

Figure 1. Hardware Environment Architecture of TOE

As shown in the block diagram in figure 1, KKEC includes:

- 200 MHz ARM920T core based processing unit,
- 32 MB of Flash Memory and 64 MB of SDRAM,
- Real Time Controller,
- 3 SC slots & 1 SIM card slot (compatible to IEC/ISO 7816),
- Security Access Module (GEM), placed into the SIM card slot
- 240x320 resolution TFT-LCD with 262K colors,
- 20-keys keypad,
- 128x128 pixels fingerprint sensor,
- USB 2.0 compliant full speed USB port for PC connection,
- 10 Mbit Ethernet port for network connection,

- USB 2.0 compliant full speed USB port for HUBC or external fingervein device connection,
- VGA port,
- +9V power supply input.

b-Software Environment

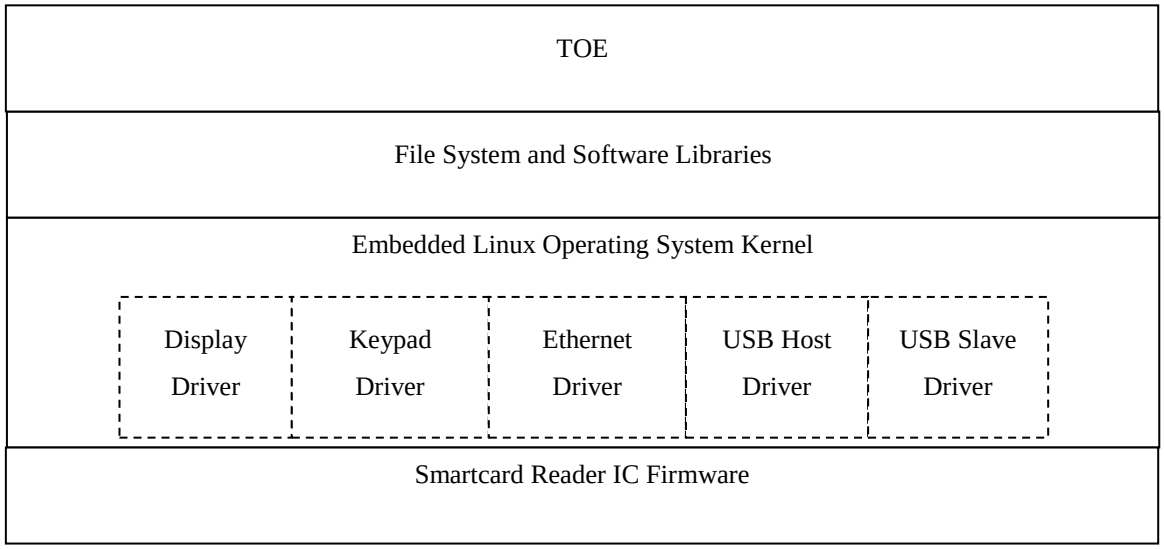

Figure 2. Software Environment Architecture of TOE

TOE operates on an embedded linux environment (Kernel version 2.6.20.4) with a file-system in jffs2 format. The compiled kernel image (version: 01.02.07) comprises the OS kernel and some of the device drivers while the file-system (version: 01.10.06) is composed of the system files, the software libraries and the rest of the device drivers required by TOE. The file system also includes the TOE (KKEC Application Software Version 1.41.06A).

TOE User Environments

There are three user environments for TOE. These are hospital environment, pharmacy environment and family doctor office/unit environment.
Further details are found in Section 1.4.1 of the ST_Lite.

7. ASSUMPTIONS AND CLARIFICATION OF SCOPE

TOE consists of the components which are defined in section 1.3.1 and 1.4.1 (Architectural information) in ST_Lite. Except these, Other components are not in the scope of Common Criteria Evaluation.

7.1 Usage Assumptions

Assumptions upon the use environment

A_USE.01	Security measures exist on the personal computer connected to KKEC to ensure protection of the PC from viruses and unwanted programs.
A_USE.02	OYA, which the TOE communicates to, is always an authorized OYA

7.2 Environmental Assumptions

Assumptions upon the development environment

A_DES.01	The designer issues and maintains a written procedure describing the security rules, and applies it in the development environment.
A_DES.02	The designer ensures protection of security relevant information involved in the design stage and during the software signature phase.

Assumptions upon the production environment

A_MAN.01	The manufacturer maintains a written procedure describing the security rules, and applies it in the production environment.
A_MAN.02	The manufacturer ensures protection of security relevant information involved in the manufacturing phase and the testing stage.
A_MAN.03	Security measures exist on the personal computer connected to KKEC to ensure protection of the PC from viruses and unwanted programs and secure transfer of the TOE relevant data over the internet.

Assumptions upon the initialization and maintenance environment

A_INIT.01	KECÖB maintains a written procedure describing the security rules, and applies it in pre-use and post-use environment.
A_INIT.02	KECÖB ensures protection of security relevant information involved in personalization, delivery, maintenance phase and end of life processes.
A_INIT.03	Security measures exist on the personal computer connected to KKEC to ensure protection of the PC from viruses and unwanted programs and secure transfer of the TOE relevant data over the internet.

A_INIT.04	EKKs are issued by an authorized association. This authorized association initializes each EKK such that symmetric and asymmetric keys are written in a securely created folder in the smartcard.

7.3 Clarification of Scope

Under normal conditions; there are no threats which TOE must counter but did not; however Operational Environment and Organizational Policies has countered. Information about threats that are countered by TOE and Operational Environmental are stated in the ST_Lite document.

8. DOCUMENTATION

KKEC Application Software Version 1.41.06A Security Target Lite

Version Number and Date: 1.0 – 07.12.2011

KKEC UY v1.41.06A Installation and Operating Guide Document

Version Number and Date: 07 – 15.11.2011

9. 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 of 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 Evaluation Technical Report (ETR) of KKEC Application Software Version 1.41.06A.

It is concluded that the TOE supports EAL 4+ (ALC_DVS.2).There are 24 assurance families which are all evaluated with the methods detailed in the ETR.

IT Product Testing is mainly realized in two parts:

1) Developer Testing :

- **TOE Test Coverage**: Developer has prepared TOE Test Document according to the TOE Functional Specification documentation.
- **TOE Test Depth:** Developer has prepared TOE Test Document according to the TOE Design documentation which include 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) Evaluator Testing :

- **Independent Testing:** Evaluator has done a total of 15 sample independent tests. 11 of them are selected from developer`s test plans. The other 4 tests are evaluator`s independent tests. All of them are related to TOE security functions.
- **Penetration Testing:** Evaluator has done 4 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. The potential vulnerabilities and the penetration tests are in the ETR and the penetration tests and their results are available in detail in the ETR document as well.

The result of AVA_VAN.3 evaluation is given below:

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

For the product KKEC Application Software Version 1.41.06A, **there are 2 residual vulnerability** (vulnerabilities can be used as evil actions by the hostile entities who have HIGH and BEYOND HIGH level attack potential), that they do not affect the evaluation result, found by CCTL(OKTEM) laboratory under the conditions defined by the evaluation evidences and developer claims.

10. EVALUATED CONFIGURATION

During the evaluation; the configuration of evaluation evidences which are composed of Software source code, Common Criteria documents, sustenance document and guides are shown below:

Evaluation Evidence: TOE – Institutional Smartcard Access Device Application Software

Kurumsal Kart Erişim Cihazı Uygulama Yazılımı (KKEC UY)

Version Number :1.41.06A

Production Date: 26.09.2011

Evaluation Evidence: KKEC UY v1.41.06A Source Code (Kaynak Kodu)

Version Number and Date: 1.0 – 26.09.2011

Evaluation Evidence: KKEC UY v1.41.06A Product Design Definition Document

(Ürün Tasarım Tanımlama Dokümanı)

Version Number and Date: 12 – 26.09.2011

Evaluation Evidence: KKEC UY v1.41.06A Functional Specification Document

(Fonksiyonel Belirtim Dokümanı)

Version Number and Date: 1.4 – 27.09.2011

Evaluation Evidence: KKEC UY v1.41.06A Security Architecture Definition Document

(Güvenlik Mimarisi Tanımlama Dokümanı)

Version Number and Date: 2.1 – 27.09.2011

Evaluation Evidence: KKEC UY v1.41.06A Delivery Document (Teslim Dokümanı)

Version Number and Date: 1.6 – 15.11.2011

Evaluation Evidence: KKEC UY v1.41.06A Configuration Management Plan Document

(Konfigürasyon Yönetim Planı Dokümanı)

Version Number and Date: 1.7 – 16.11.2011

Evaluation Evidence: KKEC UY v1.41.06A Development Environment Security

(Geliştirme Ortam Güvenliği Dokümanı)

Version Number and Date: 2.5 – 26.09.2011

Evaluation Evidence: KKEC UY v1.41.06A Development Tools Document

(Geliştirme Araçları Dokümanı)

Version Number and Date: 7.0 – 26.09.2011

Evaluation Evidence: KKEC UY v1.41.06A Life Cycle Definition Document

(Yaşam Döngüsü Tanımlama Dokümanı)

Version Number and Date: 2.2 – 16.11.2011

Evaluation Evidence: KKEC UY v1.41.06A Security Target Document

(Güvenlik Hedefi Dökümanı)

Version Number and Date: 1.18 – 24.10.2011

Evaluation Evidence: KKEC UY v1.41.06A Test Document (Test Dokümanı)

Version Number and Date: 1.11 – 27.09.2011

Evaluation Evidence: KKEC UY v1.41.06A Installation and Operating Guide Document (Kurulum ve İşletim Kılavuzu Dokümanı)

Version Number and Date: 07 – 15.11.2011

Evaluation Evidence: KKEC UY v1.41.06A The List of Changes Document

(Değişiklikler Listesi Dokümanı)

Version Number and Date: 01 – 28.09.2011

11. RESULTS OF THE EVALUATION

Table 1 below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_DVS.2.

Component ID	Component Title
ASE_INT.1	ST Introduction
ASE_CCL.1	Conformance Claims
ASE_SPD.1	Security Problem Definition
ASE_OBJ.2	Security Objectives
ASE_ECD.1	Extended Components Definition
ASE_REQ.2	Security Requirements
ASE_TSS.1	TOE Summary Specification
ADV_ARC.1	Security Architecture
ADV_FSP.4	Functional Specification
ADV_IMP.1	Implementation Representation
ADV_TDS.3	TOE Design
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.4	Configuration Management Capabilities
ALC_CMS.4	Configuration Management Scope
ALC_DEL.1	Delivery
ALC_DVS.2	Development Security
ALC_LCD.1	Life-Cycle Definition
ALC_TAT.1	Tools and Techniques
ATE_COV.2	Coverage
ATE_DPT.1	Depth
ATE_FUN.1	Functional Tests
ATE_IND.2	Independent Testing
AVA_VAN.3	Vulnerability Analysis

Table 1 - Security Assurance Requirements for the TOE

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 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 KKEC Application Software Version 1.41.06A the result of the assessment of all evaluation tasks are "Pass".

Results of the evaluation:

KKEC Application Software Version 1.41.06A product was found to fulfill the Common Criteria requirements for each of 24 assurance families and provide the assurance level EAL 4+ (ALC_DVS.2) .This result shows that TOE is resistant against the "ADVANCED-BASIC'' level attack potential and it countervails the claims of the functional and assurance requirements which are defined in ST document.

There are 2 residual vulnerability (vulnerabilities can be used as evil actions by the hostile entities who have HIGH and BEYOND HIGH level attack potential), that they do not affect the evaluation result, found by CCTL(OKTEM) laboratory under the conditions defined by the evaluation evidences and developer claims.

12. EVALUATOR COMMENTS/ RECOMMENDATIONS

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of KKEC Application Software Version 1.41.06A product, result of the evaluation, or the ETR.

13. CERTIFICATION AUTHORITY COMMENTS/ RECOMMENDATIONS

The certifier has no comments or recommendations related to the evaluation process of KKEC Application Software Version 1.41.06A product, result of the evaluation, or the ETR.

14.SECURITY TARGET

For the purpose of publishing, the security target[4] of the target of evaluation(TOE) is provided within a separate document.It is a sanitized version of the complete security target [3] used for the evaluation performed.

15. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009

[3] KKEC Application Software Version 1.41.06A Security Target
Version: 1.18 Date: 24.10.2011

[4] KKEC Application Software Version 1.41.06A Security Target Lite
Version: 1.0 Date: 07.12.2011

[5] Evaluation Technical Report (Document Code: DTR 08 TR 01), November 24, 2011

[6] PCC-03-WI-04 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 2.0

16. APPENDICES

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