COMMON CRITERIA RECOGNITION ARRANGEMENT
FOR COMPONENTS UP TO EAL 4

Certification Report

EAL 4 + (ALC_DVS.2)
Evaluation of

TÜBİTAK BİLGEM UEKAE

ELECTRONIC IDENTITY CARD ACCESS DEVICE FIRMWARE
(KEC FIRMWARE PP)

Protection Profile

v1.0

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	04.09.2012
Version of Report	1
Author	Mustafa YILMAZ
Technical Responsible	Mariye Umay AKKAYA
Approved	Fatih ÇETİN
Date Approved	04.09.2012
Certification Report Number	14.10.01/12-311
Sponsor and Developer	TÜBİTAK BİLGEM UEKAE
Evaluation Lab	TÜBİTAK BİLGEM OKTEM
PP Name	Electronic Identity Card Access Device Firmware Protection Profile (KEC FIRMWARE PP) v1.0
Pages	17

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
v1	28.08.2012	All	Final Released

DISCLAIMER

This certification report and the PP 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 PP 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 PP 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 PP 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 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.

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 Testing Laboratory (CCTL) under CCCS' supervision.

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 CCTL 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 PP have been performed by TÜBİTAK-BİLGEM-OKTEM which is a public CCTL.

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

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Electronic Identity Card Access Device Firmware Protection Profile (KEC FIRMWARE PP) v1.0 whose evaluation was completed on 08.08.2012 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the PP document with version no 01.

The certification report, certificate of PP evaluation and PP document are posted on the PCC 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 describes the certification results by the certification body on the evaluation results applied with requirements of APE(Protection Profile Evaluation) assurance class of the Common Criteria for Information Security Evaluation in relation to Electronic Identity Card Access Device Firmware Protection Profile (KEC FIRMWARE PP) v1.0.This report describes the evaluation results and its soundness and conformity.

The evaluation on Electronic Identity Card Access Device Firmware Protection Profile (KEC FIRMWARE PP) v1.0 was conducted by TÜBİTAK-BİLGEM-OKTEM and completed on 08.08.2012.Contents of this report have been prepared on the basis of the contents of the ETR submitted by OKTEM.The evaluation was conducted by applying CEM.This PP satisfies all APE requirements of the CC,therefore the evaluation results were decided to be “suitable”.

The TOE (TOE is the product described in the PP) is the embedded application software within Electronic Identity Card Access Device (KEC - Kart Erişim Cihazı), which is the terminal device in Electronic Identity Verification System (EKDS – Elektronik Kimlik Doğrulama Sistemi). It performs smartcard based personal identity verification.
TOE can provide the following main services:

- Validation of TCKK (Türkiye Cumhuriyeti Kimlik Kartı) and validation of KEC with the help of GEM,
- Cardholder verification by using PIN and biometrics (fingerprint, fingervein, or palmvein data).

TOE provides these services for Automation Software Interface (OYA – Otomasyon Yazılımı Arabirimi), Web Client Interface (WIA – Web İstemci Arabirimi) and Security Services Platform (GSP - Güvenlik Servisleri Platformu) softwares.

TOE major security features for operational use

The TOE can provide the following security features:

- Cardholder authentication by using PIN and/or biometrics (either fingerprint data and/or fingervein data) depending either on a policy rule defined by KDPS or on verification type directly defined by the application,

- Authentication of TCKK and authentication of KEC by using GEM,
- Integrity and confidentialty of TOE,
- Data encryption and decryption using 256-bit AES and 2048-bit RSA algorithms,
- Hash Message Authentication Code (HMAC) calculation using 256-bit SHA algorithm,
- Authentications and secure communication with TCKK, GEM, GSP, externally connected pinpad and biometric devices,
- Automatically remote and secure software upgrade,
- Personal idendity verification for different security levels,
- Auditing of critical events,
- Reporting alarms to OYA/WIA/GSP,

There are 10 assumptions made in the PP regarding the development environment, production environment, initialization and maintenance environment, use environment. The PP does not include any Organizational Security Policy. There is one threat covered by TOE and there are 12 threats covered by the TOE and the operational environment. The assumptions,the threats and the organizational security policies are described in chapter 3 in PP.

The CB(Certification Body) has examined the evaluation activities, provided the guidance for the technical problems and evaluation procedures, and reviewed each OR(Observation Reports) and ETR(Evaluation Technical Report).The CB confirmed that this PP is complete, consistent and technically sound through the evaluation results. Therefore, the CB certified that observation and evaluation results by evaluator are accurate and reasonable.

2 CERTIFICATION RESULTS

2.1 PP Identification

Project Identifier	TSE-CCCS/PP-001
PP Name and Version	Electronic Identity Card Access Device Firmware Protection Profile (KEC FIRMWARE PP) v1.0
PP Document Title	Common Criteria Protection Profile for Electronic Identity Card Access Device Firmware (KEC Firmware PP)
PP Document Version	v1.0
PP Document Date	06th August 2012
Assurance Level	EAL 4+ (ALC_DVS.2)
Criteria	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
Methodology	Common Methodology for Information Technology Security Evaluation v3.1 rev3, July 2009
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package Conformant to EAL4 + (ALC_DVS.2)
Sponsor and Developer	TÜBİTAK-BİLGEM-UEKAE
Evaluation Facility	TÜBİTAK-BİLGEM-OKTEM
Certification Scheme	Turkish Standards Institution Common Criteria Certification Scheme

2.2 Security Policy

Electronic Identity Card Access Device Firmware Protection Profile (KEC FIRMWARE PP) v1.0 does not include any Organizational Security Policy.

2.3 Assumptions and Clarification of Scope

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

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 TOE 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 Authorized service personnel maintain a written procedure describing the security rules, and apply it in pre-use and post-use environment.

A_INIT.02 Authorized service personnel protect 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 TOE to ensure protection of the PC from viruses and unwanted programs and secure communication of the TOE relevant data over the internet.

Assumptions upon the use environment

A_USE.01	Security measures exist on the personal computer connected to TOE to ensure protection of the PC from viruses and unwanted programs.
A_USE.02	PIN of any GEM card is never known by any user.

Threats can be found in PP Section 3.1.

To understand clarification of scope, details can be found in PP section1.2.3, Non-TOE hardware/software/firmware part.

2.4 Architectural Information

Architectural information about TOE can be found in PP. Section 1.2.3 in PP describes Non-TOE hardware/software/firmware.This section contains Software/Firmware Environment of TOE, Hardware Environment of TOE, Smartcard Reader Classification and TOE User Environments.
Secure card access devices, that TOE can be positioned, are classified according to their security functions, configurations and specifications. Device classification table can be found in Smartcard Reader Classification Part.To understand how Class 1, Class 2 , Class 3 devices operate in the environment,details and scenario can be found in TOE User Enviroments Part.

2.5 Security Functional Requirements

This section describes the security functional requirements for the TOE as of the following.

Securityfunctional class	Security functional component	
Security Audit (FAU)	FAU_ARP.1	Security Alarms
	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAA.1	Potential Violation Analysis
	FAU_SAR.1	Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.2	Guarantees of Audit Data Availability
	FAU_STG.4	Prevention of Audit Data Loss
Communication (FCO)	FCO_NRO.2	Enforced Proof of Origin
Cryptographic Support (FCS)	FCS_CKM.1(a)	Cryptographic Key Generation (TCKK Communication)
	FCS_CKM.1/b	Cryptographic Key Generation (GEM Communication)
	FCS_CKM.1/c	Cryptographic Key Generation (Rol Certificate Holder Communication)
	FCS_CKM.1/d	Cryptographic Key Generation (GSP Communication)
	FCS_CKM.1/e	Cryptographic Key Generation (Externally Connected Trusted Device Communication)

	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/a	Cryptographic Operation (Data Encryption and Decryption)
	FCS_COP.1/b	Cryptographic Operation (Hash Computaiton)
	FCS_COP.1/c	Cryptographic Operation (Digital Signature Verification)
	FCS_COP.1/d	Cryptographic Operation (Secure Messaging with TCKK)
	FCS_COP.1/e	Cryptographic Operation (Secure Communication with GEM)
	FCS_COP.1/f	Cryptographic Operation (Secure Communication with Role Certificate Holder)
	FCS_COP.1/g	Cryptographic Operation (Secure Communication with GSP)
	FCS_COP.1/h	Cryptographic Operation (Secure Communication with External Trusted Devices)
User Data Protection (FDP)	FDP_DAU.1	Basic Data Authentication
Identification and Authentication(FIA)	FIA_AFL.1	Authentication Failure Handling
	FIA_UAU.1	Timing of Authentication

	FIA_UAU.3	Unforgeable Authentication
	FIA_UAU.4	Single Use Authentication Mechanism
	FIA_UAU.5	Multiple Authentication Mechanism
	FIA_UAU.6	Re-Authenticating
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UID.1	Timing of Identification
Protection of the TSF (FPT)	FPT_ITC.1	Inter-TSF Confidentiality During Transmission
	FPT_STM.1	Reliable Time Stamps
	FPT_TDC.1	Inter-TSF Basic TSF Data Consistency
Trusted Path/Channels (FTP)	FTP_ITC.1	Inter-TSF Trusted Channel

2.6 Security Assurance Requirements

Assurance requirements of Electronic Identity Card Access Device Firmware Protection Profile (KEC FIRMWARE PP) v1.0 consist with assurance components in CC Part 3 and evaluation assurance level is "EAL 4+".The augmented assurance component is ALC_DVS.2.

2.7 Results of the Evaluation

The evaluation is performed with reference to the CC v3.1 and CEM v3.1.The verdict of Electronic Identity Card Access Device Firmware Protection Profile (KEC FIRMWARE PP) v1.0 is the pass as it satisfies all requirements of APE(Protection Profile,Evaluation) class of CC. Therefore, the evaluation results were decided to be suitable.

Assurance Class Name	Assurance Components	Verdict
PP Introduction	APE_INT.1	PASS
Conformance Claims	APE_CCL.1	PASS
Security Problem Definition	APE_SPD.1	PASS
Security Objectives	APE_OBJ.2	PASS
Extended Components Definition	APE_ECD.1	PASS
Derived Security Requirements	APE_REQ.2	PASS

Summarizing the results of all assurance classes, the final evaluation results in PASS.

2.8 Evaluator Comments / Recommendations

There is no recommendations concerning the Electronic Identity Card Access Device Firmware Protection Profile (KEC FIRMWARE PP) v1.0.

3 PP DOCUMENT

Common Criteria Protection Profile for Electronic Identity Card Access Device Firmware

(KEC Firmware PP)

Version Number / Revision Date: 1.0 / 06th Agust 2012

4 GLOSSARY

AES	Advanced Encryption Standard
BİLGEM	Center of Research For Advanced Technologies Of Informatics and Information Security(Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi)
CC	Common Criteria
CCCS	Common Criteria Certification Scheme
CCMB	Common Criteria Management Board
CCTL	Common Criteria Test Laboratory
CEM	Common Evaluation Methodology
CPU	Central Processing Unit
CTN	Device Track Number (Cihaz Takip Numarası)
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EKDS	Electronic Identity Verification System (Elektronik Kimlik Doğrulama Sistemi)
GEM	Secure Access Module (Güvenli Erişim Modülü)
GSP	Security Services Platform (Güvenlik Servisleri Platformu)
HMAC	Hash Message Authentication Code
IC	Integrated Circuit
IT	Information Technology
KD	Identity Verification (Kimlik Doğrulama)
KDB	Identity Verification Assertion (Kimlik Doğrulama Bildirimi)
KDP	Identity Verification Policy (Kimlik Doğrulama Politikası)
KDPS	Identity Verification Policy Server (Kimlik Doğrulama Politika Sunucusu)
KDS	Identity Verification Server (Kimlik Doğrulama Sunucusu)
KEC	Elektronic Identity Card Access Device (Kart Erişim Cihazı)
KECÖB	KEC Personalization Unit (Kart Erişim Cihazı Özelleştirme Birimi)
OCSP	Online Certificate Status Protocol
OCSPS	Online Certificate Status Protocol Server
OYA	Automation Software Interface (Otomasyon Yazılımı Arabirimi)
OKTEM	Common Criteria Test Center (as CCTL)

PCC	Product Certification Center
PIN	Personal Identification Number
PP	Protection Profile
RSA	Rivest – Shamir – Adleman (RSA Algorithm)
RTC	Real Time Clock
SC	Smartcard
SFR	Security Functional Requirement
SPS	Software Publisher Server
SSL	Secure Socket Layer
ST	Security Target
TCKK	Turkish Republic Identity Card (Türkiye Cumhuriyeti Kimlik Kartı)
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TSF Interface
TÜBİTAK	Scientific and Technologic Research Association of Turkey (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu)
UEKAE	National Research Institute of Electronics and Cryptology (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü)
USB	Universal Serial Bus
WIA	Web Client Interface (Web İstemci Arabirimi)

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

[5] Electronic Identity Card Access Device Firmware Protection Profile (KEC FIRMWARE PP) v1.0 Version: 1.0 Date: 06th August 2012

[6] Evaluation Technical Report (Document Code: DTR 15 TR 01), 08.08.2012

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

[8] TSE-Product Certification Center-Information Technology-CCCS Beneficial Documents

- Secure Card Access Devices for Turkish National Identity Cards
  Part 1: Overview
- Secure Card Access Devices for Turkish National Identity Cards
  Part 2: Interfaces and their characteristics
- Secure Card Access Devices for Turkish National Identity Cards
  Part 3: Security Specifications
- Secure Card Access Devices for Turkish National Identity Cards
  Part 4: KEC Application Software Specifications

6 ANNEXES

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