Certification Report

EAL 4+ (ALC_DVS.2)
Evaluation of

TÜBİTAK BİLGEM UEKAE

AKİS v1.4i PASAPORT

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	07.03.2014
Version of Report	1.0
Author	Murat ADSIZ
Technical Responsible	Mustafa YILMAZ
Approved	Mariye Umay AKKAYA
Date Approved	07.03.2014
Certification Report Number	21.0.01/14-001
Sponsor and Developer	TÜBİTAK BILGEM UEKAE
Evaluation Lab	TÜBİTAK BILGEM OKTEM
TOE/ PP Name*	Akis v1.4i Pasaport
Pages	14

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
v1.0	07.03.2014	All	First 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 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.

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 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 (CCCS) 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 product have been performed by TÜBİTAK BILGEM 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 Akis v1.4i Pasaport whose evaluation was completed on 07.03.2014 and whose evaluation technical report was drawn up by TÜBİTAK BILGEM OKTEM (as CCTL), and with the Security Target document with version no v7 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the STCD Certified Products List at http://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: Akis
IT Product version: v1.4i
Developer`s Name: TÜBİTAK BILGEM UEKAE
Name of CCTL : TÜBİTAK BILGEM OKTEM
Assurance Package : EAL 4+ (ALC_DVS.2)
Completion date of evaluation : 07.03.2014

AKiS-Pasaport v1.4i is a smart card which is designed to be used as Machine Readable Travel Document (MRTD). The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel document (AKiS-Pasaport) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303'.

The usage and security features are as defined in the MRTD with ICAO Application, Basic Access Control protection profile:

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this ST contains

(i) visual (eye readable) biographical data and portrait of the holder,

(ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and

(iii) data elements on the MRTD's chip according to LDS for contactless machine reading.

The authentication of the traveler is based on

(i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and

(ii) optional biometrics using the reference data stored in the MRTD.

The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

There are 5 assumptions made in the ST regarding the development environment, production environment, initialization and maintenance environment, use environment. The ST defines one Organizational Security Policy. There is 8 threat covered by TOE and the operational environment. The assumptions, the threats and the organizational security policies are described in chapter 3 of ST in detail.

The results documented in the Evaluation Technical Report (ETR) for this product provide sufficient evidence that it meets the EAL 4 augmented with ALC_DVS.2 assurance requirements for the evaluated security functionality. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. CCCS declares that the Akis v1.4i Pasaport evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the CCCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Project Identifier	*TSE-CCCS-019*
TOE Name and Version	*Akis v1.4i Pasaport*
Security Target Document Title	Akis v1.4i Pasaport Security Target
Security Target Document Version	*7*
Security Target Document Date	*24.06.2013*
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, Revision 3, July 2009
Protection Profile Conformance	BSI-CC-PP-0055, Version 1.10, 25th March 2009
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009, conformant • Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1, Revision 3, July 2009, conformant.
Sponsor and Developer	TÜBİTAK BILGEM UEKAE
Evaluation Facility	TÜBİTAK BILGEM OKTEM
Certification Scheme	Turkish Standards Institution Common Criteria Certification Scheme

2.2 Security Policy

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Manufacturing of the MRTD's chip
The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

Personalization of the MRTD by issuing State or Organization only
The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by an agent authorized by the issuing State or Organization only.

Personal data protection policy
The biographical data and their summary printed in the MRZ and stored on the MRTD's chip
are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys.

2.3 Assumptions and Clarification of Scope

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

MRTD manufacturing
It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

MRTD delivery
Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:
- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

Personalization of the MRTD's chip
The Personalization Agent ensures the correctness of

(i) the logical MRTD with respect to the MRTD holder,

(ii) the Document Basic Access Keys,

(iii) the Chip Authentication Public Key if stored on the MRTD’s chip, and

(iv) the Document Signer Public Key Certificate (if stored on the MRTD’s chip). The Personalization Agent signs the Document Security Object.

The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

Inspection Systems for global interoperability
The Inspection System is used by the border control officer of the receiving State

(i) examining an MRTD presented by the traveler and verifying its authenticity and

(ii) verifying the traveler as MRTD holder.

The Basic Inspection System for global interoperability

(i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and

(ii) implements the terminal part of the Basic Access Control.

The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

Cryptographic quality of Basic Access Control Keys
The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the ‘ICAO Doc 9303’ , the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

2.4 Architectural Information

Operating system components are shown in the figure bellow;

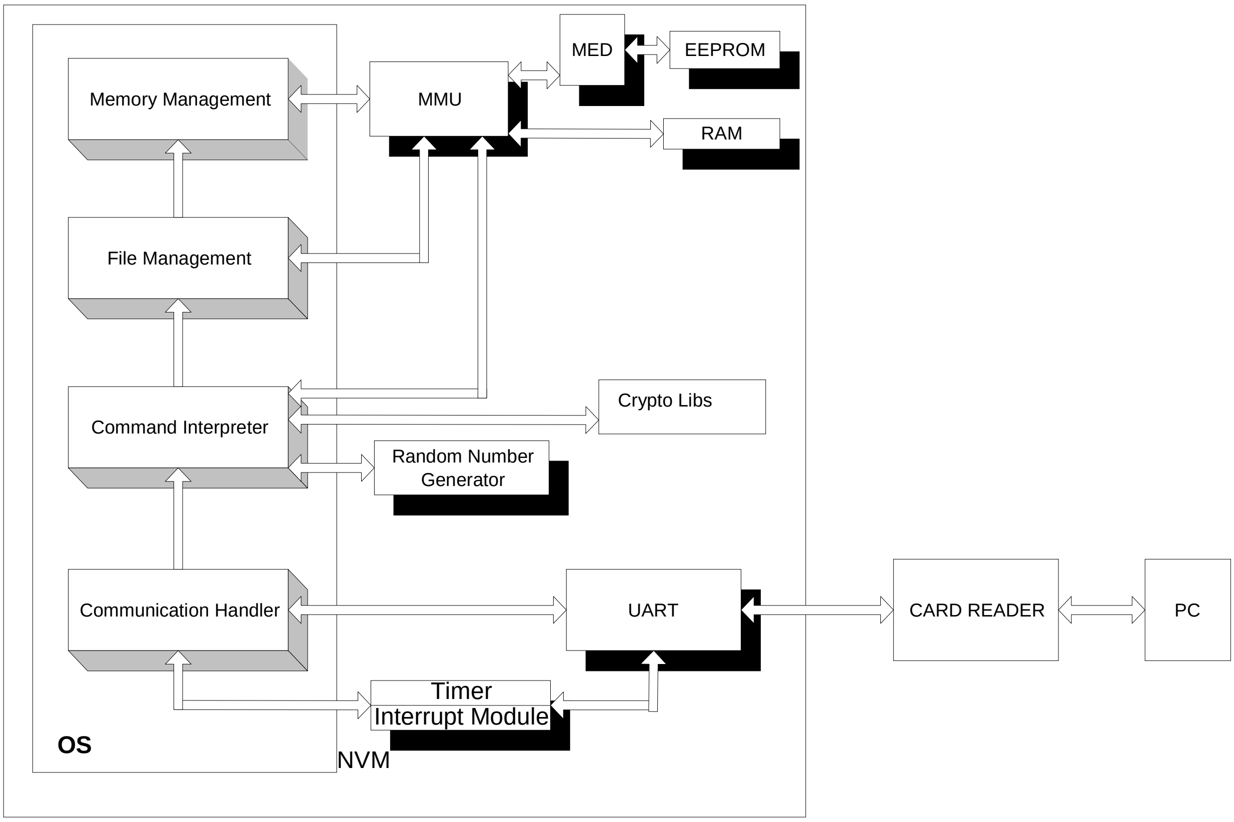

Figure AKiS v1.4i Operating System components and environment

Message is received by UART which is managed by communication handler in TOE. The message comes in TPDU format which is mentioned above. Incoming TPDU packet is analysed and block type decision is made by the communication handler. TPDU may include 3 different types of blocks, named R, S and I block. R and S blocks are used to control the transmission protocol (ISO 7816-3). I block carries the command which is transmitted to the command interpreter and executed in TOE. When command execution is finished, communication handler sends the answer to the reader via UART. If the command is related with the file system, command interpreter calls the file manager. File manager is responsible for the operations in the file field which is in the EEPROM. Memory manager is used to open new file, close file, delete page and attach new page.

2.5 Documentation

Akis v1.4i Pasaport Security Target v7

Akis v1.4i Pasaport Kullanıcı Kılavuzu v2

Akis v1.4i Pasaport Teslim ve İşletim Dökümanı v1

2.6 IT Product Testing

Developer tests effort: Description and tests results, the developer scheduling, description and test results are documented in Akis v1.4i Pasaport Test Document. The approach defined in these documents for TSFIs and depth testing is adequate to check whether the TOE behaves as described in the design documentation. The approach is oriented to test the interfaces and subsystems as they are detailed in Software Functional Specification Document, Design Document. The setup and procedures for the test cases allows demonstrating that the behavior of each subsystem is checked.

Evaluator tests effort:

Repeating Developer Tests:

- The evaluator has repeated the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report.
- The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included.

Independent Test Strategy:

- The main objective of the test performed by the evaluator is to check that the security functional requirements are implemented as expected, that the subsystems defined behave as expected, and that the TSFIs definitions are consistent with the TOE.
- The evaluator has chosen a subset of tests and an appropriate strategy for the TOE delivered by the developer. The evaluator has also considered the information coming from the security functional requirements in the security target.
- The evaluator has designed a set of tests following a suitable strategy for the TOE type.
- The evaluator has carried out tests with parameters of the TSFIs and subsystems that could have special importance in the maintenance of the TOE security. The evaluator has designed his TSFIs and subsystems independent test cases including all the security requirements defined in ST.
- All the test cases have been performed using the external interfaces that allow testing appropriately both the SFRs defined in ST and the subsystems.
- The evaluator has executed for TOE, all the tests cases defined in the independent test plan and the results obtained have been documented and referenced in this ETR.

2.7 Evaluated Configuration

The TOE configuration used in the penetration testing is consistent with the evaluated configuration according to security target

The evaluator has defined the test cases taking into account the security requirements defined in ST and the external interfaces defined in Software Functional Specifications.

The TOE configuration comprises

- the circuitry of the MRTD’s chip (the integrated circuit, IC): IFX SLE78CLFX1600PM

  the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (AKiS-Pasaport v1.4i OS),
- the MRTD application

2.8 Results of the Evaluation

All evaluator actions are satisfied for the evaluation level of EAL 4+ (ALC_DVS.2) as defined by the Common Criteria and the Common Methodology. The overall verdict for the evaluation is **PASS**. The results are supported by evidence in the ETR. There is no residual vulnerability for this product. TOE is resistant against to “ENHANCED BASIC” level attack potential attackers.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of Akis v1.4i Pasaport product, result of the evaluation, or the ETR.

3 *SECURITY* TARGET

The ST associated with this Certification Report is identified by the fallowing nomenclature:

Title : Akis v1.4i Pasaport Security Target

Version : 7

Date : 24.06.2013

4 GLOSSARY

CB: Certification Body (TSE)

CC: Common Criteria

CCTL: Common Criteria Test Laboratory (TÜBİTAK BILGEM OKTEM)

CCCS: Common Criteria Certification Scheme (Turkish CC Scheme)

CCMB: Common Criteria Management Board

CCRA: Common Criteria Recognition Arrangement

EAL: Evaluation Assurance Level

ETR: CCTL Akis v1.4i Pasaport ETR (03.09.2013)

IT: Information Technology

STCD: Software Test and Certification department (of TSE)

ST: Security Target (Akis v1.4i Pasaport Security Target v7)

TOE: Target of Evaluation (Akis v1.4i Pasaport)

TSE: Turkish Standards Institution

TSFI: TOE Security Functionality Interface

UEKAE: National Research Institude of Electronics and Cryptology of Turkey

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 3, July 2009

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 3, July 2009

[5] Composit Product Evaluation for Smartcards and Similiar Devices v1.0 rev1, Ekim 2007

[6] YTBD-01-01-TL-01 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 1.0

6 ANNEXES

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