Certification Report

EAL 4+ (AVA_VAN.5,ALC_DVS.2) Evaluation of

TÜBİTAK BİLGEM UEKAE

AKiS v2.5.2N

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-59

TABLE OF CONTENTS

Document Information

Date of Issue	***03.06.2019***
Approval Date	***06.06.2019***
Certification Report Number	***21.0.03/19-005***
Sponsor and Developer	***TÜBİTAK BİLGEM UEKAE***
Evaluation Facility	***TÜBİTAK BİLGEM TDBY OKTEM***
TOE	***AKiS v2.5.2N***
Pages	***19***

Prepared by	***Zümrüt MÜFTÜOĞLU***
Reviewed by	***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

Release	*Date*	*Pages Affected*	*Remarks/Change Reference*
1.0	***06.06.2019***	***All***	***First Release***

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced.

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 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 (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 Evaluation Facility (CCTL = Common Criteria Testing Laboratory) 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 BİLGEM TDBY 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 AKİS v2.5.2N whose evaluation was completed on 21.03.2019 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM TDBY OKTEM (as CCTL), and with the Security Target document with version no 24 of the relevant product.

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).

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

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: AKİS v2.5.2N
IT Product version: v2.5.N
Developer's Name: TÜBİTAK BİLGEM UEKAE
Name of CCTL: TÜBİTAK BİLGEM TDBY OKTEM
Assurance Package: EAL 4+ (AVA_VAN.5, ALC_DVS.2)
Completion date of evaluation: 21.03.2019

1.1 Brief Description

AKiS v2.5.2N contact based smartcard is a composite product consisting of Embedded Operating System, platform crypto library (platform library) and the platform security IC (platform IC). The crypto library is evaluated as a composite product consisting of crypto library and security IC NXP Technologies, SmartMX3 P71D320P.

1.2 Major Security Features

The TOE provides the following services to the application:

- Protection against modification, probing, environmental stress and emanation attacks mainly by platform specification and Embedded Operating System support as detailed in Section 8
- Access control to services and data by using role attribute, PIN-knowledge attribute, activation agent authentication status, personalization agent authentication status, initialization agent authentication status and device authentication status.
- The following identification and authentication services:
- activation agent identification & authentication by asymmetric cryptographic verification,
- initialization and personalization agent identification & authentication by symmetric decryption,
- terminal and chip identification & authentication by certificate authentication,
- role identification & authentication by certificate authentication,
- user identification & authentication by PIN verification.

- Security management, for services and data by supporting activation agent, initialization agent and personalization agent roles, and any other roles defined by the application.
- Secure messaging services between TOE and the terminal.
- The following cryptographic services:
- SHA Operation,
- AES Operation,
- MAC, Retail-MAC and CMAC Operation,
- TDES Operation,
- signature generation PKCS#1 v1.5,
- signature generation PKCS#1 v2.1,
- signature generation ISO/IEC 9796-2 Scheme 1,
- signature generation ECDSA,
- signature verification ISO/IEC 9796-2 Scheme 1 ,
- asymmetric decryption PKCS#1 v1.5,
- asymmetric decryption PKCS#1 v2.1,
- asymmetric encryption/decryption RAW RSA ,
- RSA key pair generation,
- ECC key pair generation,
- random number generation.

1.3Threats

The threats are categorized into Hardware related , Terminal and communication related, Card cloning and forgery related.

Hardware Related Threats are;

- **T.Phys-Tamper**

  An attacker may perform physical probing of the TOE in order
  - to disclose user data or
  - to disclose/reconstruct the TOE's Embedded Operating System or
  - to disclose other critical information about the operation of the TOE.

  An attacker may physically modify the TOE in order to alter
  - its security functionality (hardware and software part, as well),

- the user data or the TSF-data stored on the TOE.

- **T.Information_Leakage**

  An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

- **T.Malfunction**

  An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to

  - deactivate or modify security features or functionality of the TOE's hardware or to
  - circumvent, deactivate or modify security functions of the TOE's Embedded Operating System.

- **T.Abuse-Func**

  An attacker may use functions of the TOE which may not be used after the delivery of the TOE in order manipulate User Data,

  - to manipulate or to disclose the TSF-data stored in the TOE or
  - to manipulate or to disclose the TSF-data stored in the TOE or
  - to manipulate (explore, bypass, deactivate or modify) security functionality of the TOE.

Terminal and communication related threats and card cloning and forgery related threats are because of composite TOE specific functionality.

Terminal and communication related threats are;

- **T.Session_Hijacking**

  An attacker may wait until the identification and authentication process is completed and session is established between the TOE and the terminal. After the session is established, attacker may take out the TOE or the terminal from the communication channel and takes over. That way attacker bypasses the identification and authentication process and accesses to services illegitimately.

- **T.Skimming**

  The terminal which obtains smart card's interactions with the world by controlling all I/O's can observe user identification data, so this terminal must be trusted not to capture the user's identification data. Concerning a variety of fake-terminal attacks become possible, in these cases the user must be able to differentiate between "real devices" that are manufactured by a trusted party and between "fake devices" that are manufactured by the attackers. The user cannot identify that the terminal has hidden

features, for example the message they sign was not altered by a malicious terminal. The security has nothing to do with the smart card/ terminal exchange; it is the back-end processing system that monitors the card.

- **T.Eavesdropping (Eavesdropping to the communication between TOE and inspection system)**
  An attacker may monitor the communication between the TOE and the terminal/card reader to get unauthorized access to the user data and/or TSF Data.
- **T.Man_in_The_Middle**
  An attacker may alter the communication between the TOE and the terminal. An attacker listens and alters the connection between the TOE and the terminal in order to access the services that he or she is unauthorized to access.

Card cloning and forgery related threats are ;

- **T.Counterfeit**
  An attacker produces an unauthorized copy or reproduction of a genuine TOE to be used as part of a counterfeit operation. He or she may generate a new data set or extract completely or partially the data from a genuine TOE and copy them on another functionally appropriate chip to imitate this genuine TOE. This violates the genuineness of the TOE being used either for authentication of a Card presenter as the Card holder.
- **T.Unauthorised_Access**
  An attacker may access to data that he or she is not authorized to.
- **T.Unauthorised_Management**
  An attacker may illegitimately use the security management services of the TOE.

2. CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-59
TOE Name and Version	AKIS v.2.5.2N
Security Target Title	AKIS v.2.5.2N
Security Target Version	V24
Security Target Date	04.03.2019
Assurance Level	EAL 4+ (AVA_VAN.5,ALC_DVS.2)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	None

Platform	
Security Target Title, Version and Date of the Platform Hardware	NXP Secure Smart Card Controller N7021 VA Security Target Lite, Rev. 1.1, 2017-05-31 Crypto Library Cobalt on N7021 VA Security Target Lite, Rev. 1.1, 5 July 2017
Protection Profile Conformance of the Platform Hardware	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014

2.2 Security Policy

Organizational Security Policies are;

- **P.Identification_and_Authentication**

  The TOE shall support

  •chip authentication,

  •terminal authentication,

  •PIN verification,

  •role holder authentication

  and any combination of this.

  In addition, TOE shall calculate the cryptographic checksum value of the Embedded Operating System HEX code in the flash memory code area and return it upon request, and each instantiation of the TOE shall include a unique identification.

- **P.PKI**

  There will be Certificate Authorities (CA's) for terminal authentication, chip authentication, and role authentication and the certificates for these CA's will be signed by Root CA. Terminal certificates, chip certificates, and role certificates will be signed by the corresponding CA.

- **P.Access_Control**

  Role attribute, PIN knowledge attribute, device authentication attribute of the user shall be used as a security attribute to determine the access control behavior and security management privileges during operational phase.

No memory separation is required in the operational phase (the TOE is a single application EOS), the access control is rather file permission based. However, memory separation is required in between the memory areas of IC dedicated software and the EOS which is supported by the platform.

Another security feature related to access control and not derived from the threats is access to Special Function Registers and hardware resources. Access control policy for the access to the SFRs and hardware resources by System Mode and the EOS code (executing in User Mode) shall be applied such that EOS gains access to resources via the NXP System Mode.

- **P.PreOperational_Security_Management**

  The TOE shall support
  - activation agent,
  - initialization agent,
  - personalization agent

  functions and roles.

  Personalization software shall handle the user data considering their integrity as stated in the Guidance Documents.

- **P.Operational_Security_Management**

  The TOE shall support any management function and role defined by the application.

  Software accessing the TOE in the operational phase shall check the integrity of the user data stored in the TOE in each read operation as described in the Guidance Documents.

- **P.Cryptographic_Operations**

  The TOE shall support following cryptographic functions:
  - RSA key pair generation,
  - ECC key pair generation,
  - hash calculation,
  - eSign operations,
  - PKCS #1 v2.1 PSS,
  - PKCS #1 v1.5,
  - ISO/IEC 9796-2 Scheme 1,
  - ECDSA

- asymmetric decryption,
- PKCS #1 v2.1 OAEP,
- PKCS #1 v1.5,
- Raw RSA
- asymmetric encryption,
- Raw RSA
- TDES operation,
- AES operation,
- MAC, Retail-MAC and CMAC operation,
- Destruction of the keys used

- **P.Process-TOE**

  An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification. This also results in a unique activation cryptogram for each TOE.

2.3 Assumptions and Clarification of Scope

Assumptions for the operational environment of the composite TOE are;

- **A.Secure_Application**

  It is assumed that the application correctly defines the access rules of the application data.
- **A.Key_and_Certificate_Security**

  It is assumed that all keys and certificates are produced, stored and used securely outside of TOE.
- **A.PIN_Handling**

  It is assumed that PINS belonging to the application are handled securely by PIN owner.
- **A.Personnel_Security**

  It is assumed that personnel who hold privileges over the TOE acts responsively and according to the application requirements.
- **A.Trusted_Parties**

  It is assumed that the authenticated parties that the TOE communicates act responsively.

- **A.Pre-Operational_Environment**

  It is assumed that the Physical environments of initialization and personalization phases are secure.

2.4 Architectural Information

TOE consists of the communication subsystem, command subsystem, cryptographic support subsystem, security subsystem, memory and file subsystem and system subsystem.

Communication Subsystem

Communication subsystem manages the communication between AKiS v2.5.2N and the external world. Two layered communication takes place between the outer world and AKiS v2.5.2N, for the transmission purposes T=1 protocol is implemented, for the application purposes APDU packets are used.

Command Subsystem

Command subsystem processes the commands received from communication subsystem. It performs the commands via help of the security subsystem, memory and file subsystem.

Cryptographic Support Subsystem

All cryptographic functions like encryption, decryption, signature generation, signature verification, random number generation, hash calculation are performed within this subsystem.

Security Subsystem

Access control conditions and lifecycle management operations are performed within this subsystem. Whenever a security control is to be done via command subsystem, it asks to the security subsystem if the action is allowed or not.

Memory and File Subsystem

Memory and file subsystem manages the non-volatile memory of the security IC. Memory and file subsystem gives services to both of the command subsystem and the security subsystem.

System Subsystem

System subsystem includes the functions related to the whole system such as security controls of the system.

2.5 Documentation

Documents below are provided to the customer by the developer alongside the TOE;

Name of Document	Version Number	Date
AKIS v.2.5.2N Security Target	V16	29.01.2018
AKİS v2.5.2N User Guide	V19	29.01.2018

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report (ETR) of AKIS v.2.5.2N.

It is concluded that the TOE supports EAL 4+ (AVA_VAN.5, ALC_DVS.2). There are 29 assurance families which are all evaluated with the methods detailed in the ETR.

IT Product Testing is mainly described in two parts:

2.6.1 Developer Testing

Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE Design documentation which includes TSF subsystems and its interactions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 74 functional tests in total.

2.6.2 Evaluator Testing

- Independent Testing: Evaluator has chosen 42 developer tests to conduct by itself. Additionally, evaluator has prepared 32 independent tests. TOE has passed all functional tests to demonstrate that its security functions work as it is defined in the ST.
- Penetration Testing: TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 30 penetration tests have been conducted.

2.7 Evaluated Configuration

The evaluated TOE configuration is composed of;

- the IC Embedded Software including operating system (AKIS v2.5.2N),
- Secure IC (NXP Technologies, SmartMX3 P71D320P),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software, IC Dedicated Crypto library
- Guidance documents

During the evaluation; following documents of the developer were used;

2.8 Results of the Evaluation

Table 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 AVA_VAN.5, ALC_DVS.2

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4+ (AVA_VAN.5, ALC_DVS.2) assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE “AKIS v2.5.2N”, the results of the assessment of all evaluation tasks are “Pass”.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of "AKIS v2.5.2N" 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: Security Target Lite of AKIS v.2.5.2N

Revision: v01

Date of Document: 27.05.2019

4. GLOSSARY

AA : Active Authentication

ADV : Assurance of Development

AES : Advanced Encryption Standard

AGD : Assurance of Guidance Documents

AKIS : Akıllı Kart İşletim Sistemi

ALC : Assurance of Life Cycle

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCRA : Common Criteria Recognition Arrangement

CCTL : Common Criteria Test Laboratory

CEM :Common Evaluation Methodology

CMC : Configuration Management Capability

CMS : Configuration Management Scope

DEL : Delivery

DES : Data Encryption Standard

DF : Dedicated File

DVS : Development Security

EAC : Extended Access Control

EAL : Evaluation Assurance Level

EF : Elementary File

MAC : Message Authentication Code

OKTEM : Ortak Kriterler Test Merkezi

OPE : Opretaional User Guidance

OSP : Organisational Security PolicyPP : Protection Profile

PRE : Preperative Procedures

PP : Protection Profile

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

TUBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

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] Composite product evaluation for Smart Cards and similar devices, v1.2, April 2012

[4] Application of Attack Potential to Smartcards, v2.9, May 2013

[5] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel.Date: February 8th 2016

[6] DTR 54 TR 02 AKIS v2.5.2N EAL4+(ALC_DVS.2) Evaluation Technical Report Rev2.0

[7] 0782-v2_ETR-COMP_151021_v7 Evaluation Technical Report for Composite Evaluation (ETR COMP), v7, October 21st 2015

[8] BSI-DSZ-CC-0782-V2-2015-RA-01 Assurance Continuity Reassessment Report, April 7th 2017

[9] Security IC Protection Profile, BSI-PP-0035, version 1.0, June 15th 2007

[10] Technical Guideline TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents, Part 3: Common Specifications, Version 2.10, March 10th 2012

6. ANNEXES

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