Certification Report

EAL 4+ (AVA_VAN.5) Evaluation of

TÜBİTAK BİLGEM UEKAE
UKİS v2.2.8H

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-34

TABLE OF CONTENTS

Document Information

Date of Issue	***15.06.2016***
Version of Report	***1.0***
Author	***Zümrüt MÜFTÜOĞLU***
Technical Responsible	***İbrahim Halil KIRMIZI***
Approved	***Mariye Umay AKKAYA***
Date Approved	***14.06.2016***
Certification Report Number	***21.0.03/16-003***
Sponsor and Developer	***TÜBİTAK BİLGEM UEKAE***
Evaluation Lab	***TÜBİTAK BİLGEM OKTEM***
TOE Name	***UKIS 2.2.8H***
Pages	***18***

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
V1.0	***13.06.2016***	***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 4 , using Common Methodology for IT Products Evaluation, version 3.1 , revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the 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 (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 is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by TÜBİTAK BİLGEM 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 UKİS v2.2.8H whose evaluation was completed on 01.06.2016 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no 16 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the STCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).The certification report, certificate of product *evaluation and security target document are posted on the STCD 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 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: UKİS
IT Product version: v2.2.8H
Developer's Name: TÜBİTAK BİLGEM UEKAE
Name of CCTL: TÜBİTAK BİLGEM OKTEM
Assurance Package: EAL 4+ (AVA_VAN.5)
Completion date of evaluation: 01.06.2016 (DTR 32 TR 06)

UKİS v2.2.8H contact based smartcard is a composite product consisting of embedded operating system and the security IC. The TOE consists of

- AKİS v2.2.8I embedded operating system,
- IC dedicated software (test and support software including libraries),
- security IC,
- guidance documentation,
- activation data.

1.1 Major Properties of the TOE

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,
- 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.

- The following cryptographic services:
  -SHA-256 Operation,
  -AES Operation 2 ,
  -CMAC Operation,
  -TDES Operation3,
  -signature generation PKCS#1 v1.5,
  -signature generation PKCS#1 v2.1,
  -signature generation ISO/IEC 9796-2 Scheme 1,
  -signature verification ISO/IEC 9796-2 Scheme 14 ,
  -asymmetric decryption PKCS#1 v1.5,

-asymmetric decryption PKCS#1 v2.1,
-asymmetric encryption/decryption RAW RSA ,
-random number generation.

- 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.

1.2 Usage of the TOE

The TOE is designed and developed to be as a platform for smart card applications. It supports the life cycle requirements of the smart card applications and provides security services to the smart card applications.

AKİSv2.2.8Isupports two different configurations to the application owner:

- Chip configuration,
- SAM configuration.

Chip configuration is developed to act as user card application like eIDs. The SAM configuration is developed to act on behalf of the terminal as a secure access module.
In chip configuration, two secure messaging types are performed. The first one is mutual authentication between card (chip) and the terminal by certificate exchange. In this method, both the terminal and the card possess a public key certificate and the corresponding private key. They share their trusted public keys with each other by certificate exchange procedure. Next, they agree on secure messaging keys by key agreement procedure. Finally secure messaging starts. This secure messaging starts in each mutual authentication automatically. In the second method, a random data is generated by the terminal and sent to TOE confidentially. Next, using this random data, card and the terminal agree on the secure messaging keys by key agreement procedure. Finally, TOE starts secure messaging. Public key cryptography is used in each step of the key agreement process to ensure confidentiality. No certificate is needed in this method.
In SAM configuration, only the second method is performed.
The other difference between the two configurations is in the terminal authentication method. Chip configuration provides terminal authentication by internal and external authentication with certificate exchange. But in SAM configuration, it is provided by PIN authentication. By this way, “authenticated terminal" means PIN authenticated terminal for SAM configuration.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-34
TOE/PP Name and Version	UKİS v2.2.8H
Security Target Title	UKİS v2.2.8H Security Target
Security Target / PP Document Version	16
Security Target Document Date	31.05.2016
Assurance Level	EAL4+ (AVA_VAN.5)
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 Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	-
Common Criteria Conformance	• 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,extended • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012,conformant
Sponsor and Developer	TÜBİTAK BİLGEM UEKAE eID Applications Unit
Evaluation Facility	TÜBİTAK BİLGEM OKTEM
Certification Scheme	TSE-CCCS

2.2 Security Policy

Organizational security policies of the composite TOE is given in Table 1.

#	Policy Name	Definition
1.	P.Identification_and_Authentication	The TOE should support • chip authentication, • terminal authentication, • PIN verification, • role holder authentication and any combination of this.

2.	P.PKI	There will be terminal authentication CA, chip authentication CA, Role CA all of which certificates are signed by Root CA. terminal certificates, chip certificates and role certificates will be signed by according CA.
3.	P.Access_Control	Role attribute, PIN knowledge attribute, device authentication attribute of the user will be used as a security attribute to determine the access control behavior and security management privileges during operational phase.
4.	P.PreOperational_Security_Management	The TOE should support • activation agent, • initialization agent, • personalization agent functions and roles
5.	P.Operational_Security_Management	The TOE should support • any management function and role defined by the application.

6.	P.Cryptographic_Operations	The TOE should support following cryptographic functions: • RSA key pair generation, • hash calculation , • eSign operations; • PKCS #1 v2.1, • PKCS #1 v1.5, • ISO/IEC 9796-2 Scheme 1, • asymmetric decryption; • PKCS #1 v2.1 OAEP, • PKCS #1 v1.5, • Raw RSA, • asymmetric encryption; • Raw RSA, • TDES calculation, • AES operation, • CMAC operation.

Table 1. Organizational security policies of the composite TOE

2.3 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- There must be Terminal Authentication CA, Chip Authentication CA, Role CA all of which certificates are signed by Root CA. Terminal Certificates, Chip Certificates and Role Certificates must be signed by the corresponding CA.
- Application shall correctly define the access rules of the application data.
- Key creation and storage outside of the TOE shall be handled securely.

- PIN Creation and usage by Card Holder shall be handled securely.
- The personnel who have privileges (EOS developer, Activation Agent, Initialization Agent and Personalization Agent) shall have necessary security clearances and shall act responsibly.
- The parties that the TOE communicates (sends or receives data; and/or receives or gives services) shall act responsibly.
- Physical environment of initialization and personalization phases shall be secure.

Details can be found in the Security Target [3] , chapter 5.2.

2.4 Architectural Information

TOE consists of the Communication Subsystem, Cryptographic Support Subsystem, Command Subsystem, Security Subsystem, Memory and File system:

Communication Subsystem:

Communication subsystem manages the communication between UKİS v2.2.8H and the external world. Two layered communication takes place between the outer world and the UKİS v2.2.8H, for the transmission purposes T=1 protocol is implemented, for the application purposes APDU packets are used.

Cryptographic Support Subsystem:

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

Command Subsystem

Command subsystem processes the commands received from communication subsystem. It performs the commands via help of the Security Subsystem, Memory and File System Subsystem.

Security Subsystem

Access control conditions, lifecycle management and cryptographic 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.

System Subsystem

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

Memory and File system

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

Details can be found in the Security Target [3] , chapter 1.5.1.

2.5 Documentation

The evaluated documentation as outlined in the following table is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Type	Identifier	Release	Date
SW	UKİS	V2.2.8H	01.06.2016
DOC	Security Target	16	31.05.2016
DOC	User Guidance	17	30.05.2016

Table 2 Documentation

2.6. IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc are mapped to the assurance families 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 UKİS 2.2.8H.

It is concluded that the TOE supports EAL 4+ (AVA_VAN.5). There are 29 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 56 sample independent tests. 31 of them are selected from developer`s test plans. The other 25 tests are evaluator`s independent tests. All of them are related to TOE security functions.
- Penetration Testing: Evaluator has done 35 penetration tests to find out if TOE`s

vulnerabilities can be used for malicious purposes. The potential vulnerabilities and the penetration tests are in "TOE Security Functions Penetration Tests Scope" which is in Annex-D of the ETR and the penetration tests and their results are available in detail in the ETR document as well.

2.7 Evaluated Configuration

This certification covers the following configurations of the TOE as outlined in the Security Target [3]:

UKİS v2.2.8H contact based smartcard is a composite product consisting of Embedded Operating System and the Security IC.
The TOE consists of:

- UKİS v2.2.8H Embedded Operating System,
- IC Dedicated Software (Test and Support Software including Libraries),
- Security IC,
- Guidance Documentation,
- Activation Data.

2.8 Results of the Evaluation

The following table 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.

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security Architecture
	ADV_FSP.4	Functional Specification
	ADV_IMP.1	Implementation Representation
	ADV_TDS.3	TOE Design
	ADV_COMP.1	Composite Design Compliance
	AGD_OPE.1	Operational User Guidance

Guidance documents	AGD_PRE.1	Preparative Procedures
Life-cycle support	ALC_CMC.4	CM Capabilities
	ALC_CMS.4	CM Scope
	ALC_DEL.1	Delivery
	ALC_DVS.1	Development Security
	ALC_LCD.1	Life-Cycle Definition
	ALC_TAT.1	Tools and Techniques
	ALC_COMP.1	Integration of composition parts and consistency of delivery procedures
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
	ASE_COMP.1	Consistency of composite product Security Target
	ATE_COV.2	Coverage
	ATE_DPT.1	Depth

Tests	ATE_FUN.1	Functional tests
	ATE_IND.2	Independent testing
	ATE_COMP.1	Composite functional testing
Vulnerability assessment	AVA_VAN.5	Vulnerability Analysis

Table 3 Security Assurance Requirements of 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 “UKİS v2.2.8H” the results of the assessment of all evaluation tasks are “Pass”.
As a result,UKİS v2.2.8H product was found to fulfill the Common Criteria requirements for each of 29 assurance families and provide the assurance level EAL 4+ (AVA_VAN.5) .This result shows that TOE is resistant against the “HIGH “level attack potential and it countervails the claims of the functional and assurance requirements which are defined in ST document.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of UKİS v2.2.8H product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The ST associated with this Certification Report is identified by the following nomenclature:
Title : UKİS v2.2.8H Security Target
Version No: 16
Date of Document: 31.05.2016

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

4 GLOSSARY

ADV : Assurance of Development
AGD : Assurance of Guidance Documents
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 (Informatics and Information Research Center)
CC : Common Criteria (Ortak Kriterler)
CCCS : Common Criteria Certification Scheme (TSE)
CCRA : Common Criteria Recognition Arrangement
CCTL : Common Criteria Test Laboratory (OKTEM)
CEM :Common Evaluation Methodology
CMC : Configuration Management Capability
CMS : Configuration Management Scope
DEL : Delivery
EAL : Evaluation Assurance Level
GR : Observation Report - Gözlem Raporu
OKTEM : Ortak Kriterler Test Merkezi
OPE : Opretaional User Guidance
OSP : Organisational Security Policy
PP : Protection Profile
PRE : Preperative Procedures
SAR : Security Assurance Requirements
SFR : Security Functional Requirements
ST : Security Target
STCD :Software Test and Certification Department
TOE : Target of Evaluation
TSF : TOE Secrity Functionality
TSFI : TSF Interface
UEKAE: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (National Research Institute of Electronics and Cryptology))

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] UKİS v2.2.8H Security Target Version: 12 Date: 25.11.2015

[4] Evaluation Technical Report (Document Code: DTR 32 TR 06), June 02, 2016

[5] Composite product evaluation for Smart Cards and similar devices v1.0 rev 1 Sep 2007 (CCDB-2007-09-001)

[6] ETR for composite evaluation according to M7892 B11(Version:5),March 20,2015

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

[8] CC Supporting Document Guidance, Mandatory Technical Document, Application of Attack Potential to Smartcards, Version 2.7 Revision 1, March 2009, CCDB-2009-03-001

[9] CC Supporting Document Guidance, Mandatory Technical Document, Application of CC to Integrated Circuits, Version 3.0 Revision 1, March 2009, CCDB-2009-03-002

[10] ISO 7816-3 Information Technology – Identification Cards – Integrated Circuits with Contacts Part 3: Electronic Signals and Transmission Protocols - T=1 Protocol

6 ANNEXES

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