Certification Report

EAL 5+ (ALC_DVS.2 and AVA_VAN.5) Evaluation of

TÜBİTAK BİLGEM UEKAE
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-51

TABLE OF CONTENTS

Document Information

Date of Issue	***18.02.2018***
Approval Date	***19.02.2018***
Certification Report Number	***21.0.03/18-004***
Sponsor and Developer	***TÜBİTAK BİLGEM UEKAE***
Evaluation Facility	***TÜBİTAK BİLGEM TDBY OKTEM***
TOE	***AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration***
Pages	***23***

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	***18.02.2018***	***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 AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration whose evaluation was completed on 07.02.2018 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM TDBY OKTEM (as CCTL), and with the Security Target document with version no 13 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: AKIS GEZGIN_I SAC & EAC Configuration
IT Product version: v1.0.0.0
Developer's Name: TÜBİTAK BİLGEM UEKAE
Name of CCTL: TÜBİTAK BİLGEM TDBY OKTEM
Assurance Package: EAL 5+ (ALC_DVS.2 and AVA_VAN.5)
Completion date of evaluation: 07.02.2018

1.1 Brief Description

The TOE is the composition of the contactless smartcard chips SLE78CLFX3000P and SLE78CLFX4000P of Infineon M7892 B11 platform with embedded software including the electronic Machine Readable Travel Document (eMRTD) application with Extended Access Control (EAC) and Supplemental Access Control (SAC) mechanisms.

1.2 Major Security Features

The following security services are provided within the scope of the TOE:

- Protection against modification, probing, environmental stress and emanation attacks mainly by platform specification and embedded operating system support.
- Passive Authentication (PA),
- Supplemental Access Control (SAC),
- Extended Access Control (EAC),
- Cryptosystem migration (Algorithm change during certificate verification transaction).

1.3Threats

The threats are categorized into the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets protected by the TOE and the method of TOE's use in the operational environment.

Threats for the composite TOE are;

- **T.Read_Sensitive_Data**
  - An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip.
- **T.Counterfeit**
  - An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document.
- **T.Skimming**
  - An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless interface of the TOE.
- **T.Eavesdropping**
  - An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected.
- **T.Tracing**
  - An attacker tries to gather TOE tracing data (i.e., to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE.
- **T.Forgery**
  - An attacker fraudulently alters the User Data or/and TSF-data stored on the eMRTD or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS PACE by means of changed travel document holder's related reference data (like biographic or biometric data).
- **T.Abuse-Func**
  - An attacker may use functions of the TOE which shall not be used in TOE operational phase in order
    - (i) to manipulate or to disclose the User Data stored in the TOE,

(ii) to manipulate or to disclose the TSF data stored in the TOE or

(iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE

This threat addresses the misuse of the functions for the initialization and personalization in the operational phase after delivery to the travel document holder.

- **T.Information_Leakage**
  - An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected.
- **T.Phys-Tamper**
  - An attacker may perform physical probing of the travel document in order
    (i) to disclose TSF-data,
    (ii) to disclose/reconstruct the travel document's chip Embedded Software.
  - An attacker may physically modify the travel document in order to alter
    (i) its security functionality (hardware and software part, as well),
    (ii) the User Data or TSF-data stored on the travel document.
- **T.Malfunction**
  - An attacker may cause a malfunction of the travel document's hardware and Embedded Software by applying environmental stress in order to
    (i) deactivate or modify security features or functionality of the TOE' hardware
    (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software.

2. CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-51
TOE Name and Version	AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration
Security Target Title	Security Target of AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration
Security Target Version	V13
Security Target Date	29.01.2018
Assurance Level	EAL 5+ (ALC_DVS.2 and 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 Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012, version 1.3.2, 05th December 2012

Platform	Infineon Technologies, SLE78CLFX3000P and SLE78CLFX4000P
Security Target Title of the Platform Hardware	Security Target Lite M7892 B11 Recertification Including Optional Software Libraries RSA – EC – SHA2 – Toolbox Common Criteria CCv3.1 EAL6 Augmented (EAL6+) Resistance to Attackers with High Attack Potential
Security Target Version and Date of the Platform Hardware	V0.3, 13.10.2015
Protection Profile Conformance of the Platform Hardware	Security IC Platform Protection Profile, BSI-PP-0035, v1.0, June 15th 2007

2.2 Security Policy

Organizational Security Policies are;

- **P.Manufact: Manufacturing of the travel document's chip**

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely and to provide the keys for the authentication of the travel document Manufacturer.

The travel document Manufacturer writes the Pre-Personalization Data which contains at least the Personalization Agent key, the Chip Authentication public.

The eMRTD Manufacturer is an agent authorized by the Issuing State or Organization only.

- ***P*.Pre-Operational: Pre-operational handling of the travel document**
  - The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.
  - The eMRTD Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE.
  - The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e., before they are in the operational phase.

- If the travel document issuer authorises a Personalization Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalization Agent acts in accordance with the eMRTD Issuer's policy.

- **P.Card_PKI: PKI for Passive Authentication (issuing branch)**

Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed/made available to their final destination, e.g., by using directory services.

The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e., for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The eMRTD Issuer shall publish the CSCA Certificate (CCSCA).

The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the travel document Issuer by strictly secure means, see [11], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer, see [11], 5.5.1.

A Document Signer shall

(i) generate the Document Signer Key Pair,

(ii) hand over the Document Signer Public Key to the CSCA for certification,

(iii) keep the Document Signer Private Key secret and

(iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

- **P.Trustworthy_PKI: Trustworthiness of PKI**

The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.

- **P.Terminal: Abilities and trustworthiness of terminals**

The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:

The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [11].

They shall implement the terminal parts of the PACE protocol, of the Passive Authentication and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie- Hellman). The related terminals need not to use any own credentials.

They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document).

The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g., confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

- **P.Sensitive_Data: Privacy of sensitive biometric reference data**

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.

- **P.Personalization: Personalization of the travel document by issuing State or Organization only**

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

2.3 Assumptions and Clarification of Scope

Assumptions for the operational environment of the composite TOE are;

- **A.Passive_Auth: PKI for Passive Authentication**

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication, i.e., digital signature creation and verification for the logical travel document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair.

The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer:

i.generates the Document Signer Key Pair,

ii. hands over the Document Signer Public Key to the CA for certification,

iii. keeps the Document Signer Private Key secret and

iv. uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents.

The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and Organizations. It is assumed that the Document Security Object contains only the hash values of the genuine user data.

- **A.Insp_Sys: Inspection Systems for global interoperability**

The Extended Inspection System (EIS) for global interoperability

includes the Country Signing CA Public Key and implements the terminal part of PACE and/or BAC. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical eMRTD under PACE or BAC and performs the Chip Authentication v.1 to verify the MRTD and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

- **A.Auth_PKI: PKI for Inspection Systems**

The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control / Extended Access Protocol. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key

pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations sign the certificates of the Document Verifier and the Document Verifiers sign the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip.

Justification: This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

2.4 Architectural Information

TOE will be in form of a paper book or plastic card with an embedded chip and possibly an antenna. It presents visual readable data including (but not limited to) personal data of the MRTD holder:

- The biographical data on the biographical data page of the passport book/card,
- The printed data in the Machine-Readable Zone (MRZ) that identifies the MRTD and
- The printed portrait.

The TOE is the composition of the Embedded Software (ES) and the security IC. ES also includes the eMRTD Application.

The platform is certified for EAL 6+. The physical protection is mainly inherited from the platform which provides protection against modification, snooping, probing, environmental stress, logical attacks and emanation attacks. The platform is resistant against single shot power analyses attacks, applied with high attack potential.

The TOE makes use of the crypto library of the platform for RSA and ECC operations which is also certified. It provides protection against SPA, DPA and DFA attacks.

2.5 Documentation

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

Name of Document	Version Number	Date

Security Target of AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration	V13	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Admin and User Guide	V19	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration SAC & EAC Configuration Admin and User Guide	V09	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 GEZGIN_I v1.0.0.0 SAC & EAC Configuration.

It is concluded that the TOE supports EAL 5+ (ALC_DVS.2, AVA_VAN.5). There are 26 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 80 functional tests in total.

2.6.2 Evaluator Testing

- Independent Testing: Evaluator has chosen 21 developer tests to conduct by itself. Additionally, evaluator has prepared 22 independent tests. TOE has passed all 43 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, 22 penetration tests have been conducted.

2.7 Evaluated Configuration

The evaluated TOE configuration is composed of;

- the IC Embedded Software including operating system and eMRTD application (AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration),
- Secure IC (Infineon Technologies, SLE78CLFX3000P and SLE78CLFX4000P),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- Guidance documents

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

Name of Document	Version Number	Publication Date
Security Target of AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration	16	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Functional Specification Document	16	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Security Architecture Description	16	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Design Document	15	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Admin and User Guide	19	29.01.2018

Name of Document	Version Number	Publication Date
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration, SAC & EAC Configuration Admin and User Guide	09	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Development Site Security and Tools&Techniques Document	14	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Delivery and Operation Document	13	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Delivery Document	11	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Configuration Management Plan Document	14	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Life-Cycle Document	12	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Test Depth Document	12	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Test Plans and Results Document	12	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration, SAC & EAC Configuration Test Plans and Results Document	12	29.01.2018
AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration Composite Product Delivery Document	12	29.01.2018

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 5) components as specified in Part 3 of the Common Criteria, augmented with ALC_DVS.2 and AVA_VAN.5

Assurance Class	Component	Component Title
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.5	Complete semi-formal functional specification with additional error information

	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semiformal Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and automation
	ALC_CMS.5	Development tools CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.2	Sufficiency of Security Measures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.2	Compliance with implementation standards
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	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: Modular Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - sample
Vulnerability Analysis	AVA_VAN.5	Advanced Methodical Vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 5+ (ALC_DVS.2, AVA_VAN.5) 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 GEZGIN_I v1.0.0.0 SAC & EAC Configuration", 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 GEZGIN_I v1.0.0.0 SAC & EAC Configuration" 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 of AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration

Version: v13

Date of Document: 29.01.2018

A public version has been created and verified according to ST-Santizing:

Title: Security Target Lite of AKIS GEZGIN_I v1.0.0.0 SAC & EAC Configuration

Version: 01

Date of Document: 19.02.2018

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

BAC : Basic Access Control

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

ICAO : International Civil Aviation Organization

MAC : Message Authentication Code

MRTD: Machine Readable Travel Document

OKTEM : Ortak Kriterler Test Merkezi

OPE : Opretaional User Guidance

OSP : Organisational Security PolicyPP : Protection Profile

PRE : Preperative Procedures

PP : Protection Profile

SAC : Supplemental Access Control

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 GEZGIN_I v1.0.0.0 SAC & EAC Configuration EAL5+(ALC_DVS.2, AVA_VAN.5) 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] Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Basic Access control, BSI-PP-0055, version 1.10, March 25th 2009

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

[11] ICAO Doc 9303, Machine Readable Travel Documents, Part 1 – Machine Readable Travel Passports, Sixth Edition, 2006, ICAO

[12] 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