



Certification Report

EAL 4+ (ALC_DVS.2) Evaluation of

TÜBİTAK BİLGEM UEKAE

**AKIS GEZGIN_I v1.0.0.0 BAC Configuration with Active
Authentication**

issued by

**Turkish Standards Institution
Common Criteria Certification Scheme**



	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

TABLE OF CONTENTS

DOCUMENT INFORMATION	3
DOCUMENT CHANGE LOG	3
DISCLAIMER	4
FOREWORD	4
RECOGNITION OF THE CERTIFICATE	5
1. EXECUTIVE SUMMARY	6
1.1 BRIEF DESCRIPTION	6
1.2 MAJOR SECURITY FEATURES	6
1.3 THREATS	7
2. CERTIFICATION RESULTS	9
2.1 IDENTIFICATION OF TARGET OF EVALUATION	9
2.2 SECURITY POLICY	10
2.3 ASSUMPTIONS AND CLARIFICATION OF SCOPE	10
2.4 ARCHITECTURAL INFORMATION	12
2.5 DOCUMENTATION	13
2.6 IT PRODUCT TESTING	13
2.7 EVALUATED CONFIGURATION	14
2.8 RESULTS OF THE EVALUATION	16
2.9 EVALUATOR COMMENTS / RECOMMENDATIONS	17
3. SECURITY TARGET	18
4. GLOSSARY	19
5. BIBLIOGRAPHY	21
6. ANNEXES	21

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

Document Information


<i>Date of Issue</i>	<i>18.02.2018</i>
<i>Approval Date</i>	<i>20.02.2018</i>
<i>Certification Report Number</i>	<i>21.0.03/18-002</i>
<i>Sponsor and Developer</i>	<i>TÜBİTAK BİLGEM UEKAE</i>
<i>Evaluation Facility</i>	<i>TÜBİTAK BİLGEM TDBY OKTEM</i>
<i>TOE</i>	<i>AKIS GEZGIN_I v1.0.0.0 BAC Configuration with Active Authentication</i>
<i>Pages</i>	<i>21</i>

<i>Prepared by</i>	<i>İbrahim Halil KIRMIZI</i>
<i>Reviewed by</i>	<i>Zümrüt MÜFTÜOĞLU</i>

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.

Document Change Log

<i>Release</i>	<i>Date</i>	<i>Pages Affected</i>	<i>Remarks/Change Reference</i>
<i>1.0</i>	<i>20.02.2018</i>	<i>All</i>	<i>First Release</i>

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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 ITCB 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.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

This certification report is associated with the Common Criteria Certificate issued by the CCCS for AKIS GEZGIN_I v1.0.0.0 BAC Configuration with Active Authentication whose evaluation was completed on 05.02.2018 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM TDBY OKTEM (as CCTL), and with the Security Target document with version no 16 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>

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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 BAC Configuration with Active Authentication

IT Product version: v1.0.0.0

Developer's Name: TÜBİTAK BİLGEM UEKAE

Name of CCTL: TÜBİTAK BİLGEM TDBY OKTEM

Assurance Package: EAL 4+ (ALC_DVS.2)

Completion date of evaluation: 05.02.2018


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 electronic Machine Readable Travel Document (eMRTD) Application.

1.2 Major Security Features

The TOE provides the following security services:

- Protection against modification, probing, environmental stress and emanation attacks,
- Passive Authentication (PA),
- Active Authentication (AA),
- Basic Access Control (BAC),
- SHA-1, SHA-2/224, SHA-2/256, SHA-2/384, SHA-2/512 Operations,
- True Random Number Generation,
- DES3 Encryption and Decryption,
- Retail MAC (DES3),
- Signature generation with ISO 9796-2 Scheme 1,
- Signature generation with ECDSA

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

1.3 Threats

The threats are categorized into Hardware related threats and Terminal, Communication and Application related threats.

Hardware Related Threats are;

- **T.Phys-Tamper (Physical Tampering)**

An attacker may perform physical probing of the MRTD's chip in order to;

- disclose TSF Data or
- disclose/reconstruct the MRTD's chip Embedded Software.

An attacker may physically modify the MRTD's chip in order to

- modify security features or functions of the MRTD's chip,
- modify security functions of the MRTD's chip Embedded Software,
- modify User Data or (iv) to modify TSF data

- **T.Information Leakage (Information Leakage from the MRTD's chip)**

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 (Malfunction due to Environmental Stress)**

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 functions of the TOE or
- circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

- **T.Abuse-Func (Abuse of Functionality)**


An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order to

- manipulate User Data,
- manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or
- disclose or to manipulate TSF Data.

- **T.Counterfeit (Production of unauthorized copies or reproductions of genuine MRTD's chips)**

An attacker produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as the chip of a counterfeit MRTD. The attacker may either

- generate a new data set from scratch or

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

- extract completely or partially the data from a genuine MRTD's chip and then copy them on another chip to imitate the genuine MRTD's chip.

Terminal, Communication and Application related threats are;

- **T.Chip_ID (Identification of MRTD's chip)**

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface.

- **T.Skimming (Skimming the logical MRTD)**


An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE.

- **T.Eavesdropping (Eavesdropping to the communication between TOE and inspection system)**

An attacker is listening to an existing communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.

- **T.Forgery (Forgery of data on MRTD's chip)**


An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

2. CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-49
TOE Name and Version	AKIS GEZGIN_I BAC Configuration with Active Authentication
Security Target Title	AKIS GEZGIN_I v1.0.0.0 BAC Configuration with Active Authentication
Security Target Version	V16
Security Target Date	29.01.2018
Assurance Level	EAL 4+ (ALC_DVS.2)
Criteria	<ul style="list-style-type: none"> • 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”, Basic Access Control, BSI-CC-PP-0055, version 1.10, March 25 th 2009

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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+)
Security Target Version and Date of the Platform Hardware	V0.3, 13.10.2013
Protection Profile Conformance of the Platform Hardware	Security IC Platform Protection Profile, BSI-PP-0035, v1.0, June 15 th 2007

2.2 Security Policy

Organizational Security Policies are;

- **P.Manufact (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.

- **P.Personalization (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.


- **P.Personal_Data (Personal Data protection policy)**

The biographical data and their summary printed in the MRZ and stored on MRTD's chip, the printed portrait and the digitized portrait, the biometric reference data of finger(s), the biometric reference data of iris image(s) and data according to LDS stored on the MRTD's chip are personal data of the MRTD holder.

2.3 Assumptions and Clarification of Scope

Assumptions for the operational environment of the composite TOE are;

- **A.MRTD_Manufact (MRTD manufacturing on steps 4 to 6)**

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
		Yayın Tarihi	30/07/2015	
	CCCS CERTIFICATION REPORT	Revizyon Tarihi	29/04/2016	No

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 the manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

- **A.MRTD_Delivery (Delivery of the MRTD during steps 4 to 6)**

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.

- **A.Pers_Agent (Personalization of the MRTD's chip)**

The Personalization Agent ensures the correctness of;

- the logical MRTD with respect to the MRTD holder,
- the Document Basic Access Keys,
- the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and
- the Document Signer Public Key Certificate (if stored on the MRTD's chip).


The Personalization Agent signs the Document Security Object.

- **A.Insp_Sys (Inspection Systems for global interoperability)**

The Inspection System is used by the border control officer of the receiving State for eMRTD examining an MRTD presented by the user and verifying its authenticity and verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and implements the terminal part of the Basic Access Control. The Basic Inspection System reads the logical MRTD under BAC and performs the Passive Authentication to verify the logical MRTD.

- **A.BAC-Keys (Cryptographic quality of BAC Keys)**

The Document BAC 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 BAC 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

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

- **A.Pers_Agent_AA (Personalization of the MRTD's chip including Active Authentication)**

The Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by mechanisms mentioned in A.Pers_Agent.

- **A.Insp_Sys_AA (Inspection Systems for global interoperability with Active Authentication)**

The Inspection System may also implement the terminal part of the Active Authentication Protocol if it wants to ensure the TOE is not cloned.

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.

TOE is composed of the IC dedicated software, the IC embedded software and the IC platform that the embedded software runs on.

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.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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 BAC Configuration with Active Authentication	V16	29.01.2018
AKIS GEZGIN_I v1.0.0.0 BAC Configuration with Active Authentication Admin and User Guide	V19	29.01.2018
AKIS GEZGIN_I v1.0.0.0 BAC Configuration with Active Authentication 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 BAC Configuration with Active Authentication.

It is concluded that the TOE supports EAL 4+ (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 80 functional tests in total.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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 BAC Configuration with Active Authentication),
- 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 BAC Configuration with Active Authentication	16	29.01.2018
AKIS GEZGIN_I v1.0.0.0 BAC Configuration with Active Authentication Functional Specification Document	16	29.01.2018
AKIS GEZGIN_I v1.0.0.0 BAC Configuration with Active Authentication Security Architecture Description	16	29.01.2018
AKIS GEZGIN_I v1.0.0.0 BAC Configuration with Active Authentication Design Document	15	29.01.2018
AKIS GEZGIN_I v1.0.0.0 BAC Configuration with Active Authentication Admin and User Guide	19	29.01.2018



**BİLİŞİM TEKNOLOJİLERİ
TEST VE BELGELENDİRME
DAİRESİ BAŞKANLIĞI /
INFORMATION TECHNOLOGIES TEST AND
CERTIFICATION DEPARTMENT**

Doküman No

BTBD-03-01-FR-01

CCCS CERTIFICATION REPORT

Yayın Tarihi

30/07/2015


Revizyon Tarihi

29/04/2016

No

05


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

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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 ALC_DVS.2

Assurance Class	Component	Component Title
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic 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.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.2	Sufficiency of Security Measures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-Defined Development Tools
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.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing


	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT		Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT		Yayın Tarihi	30/07/2015	
			Revizyon Tarihi	29/04/2016	No

	ATE_IND.2	Independent Testing
Vulnerability Analysis	AVA_VAN.3	Focused Vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4+ (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 GEZGIN_I v1.0.0.0 BAC Configuration with Active Authentication”, 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 BAC Configuration with Active Authentication” product, result of the evaluation, or the ETR.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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 BAC Configuration with Active Authentication

Version: v16


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 BAC Configuration with Active Authentication

Version: 01

Date of Document: 19.02.2018

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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 Secirity Functionality

TSFI : TSF Interface

TUBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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 BAC Configuration with Active Authentication 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] 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