Certification Report

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

TÜBİTAK BİLGEM UEKAE

AKIS GEZGIN_N v2.0 SAC & EAC Configuration

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-92

TABLE OF CONTENTS

TABLE OF CONTENTS 2
DOCUMENT INFORMATION 3
DOCUMENT CHANGE LOG 3
DISCLAIMER 3
FOREWORD 4
RECOGNITION OF THE CERTIFICATE 5
1 EXECUTIVE SUMMARY 6
2 CERTIFICATION RESULTS 12
2.1 IDENTIFICATION OF TARGET OF EVALUATION 12
2.2 SECURITY POLICY 13
2.3 ASSUMPTIONS AND CLARIFICATION OF SCOPE 16
2.4 ARCHITECTURAL INFORMATION 17
2.5 DOCUMENTATION 18
2.6 IT PRODUCT TESTING 18
2.7 EVALUATED CONFIGURATION 18
2.8 RESULTS OF THE EVALUATION 19
2.9 EVALUATOR COMMENTS / RECOMMENDATIONS 21
3 SECURITY TARGET 21
4 GLOSSARY 21
5 BIBLIOGRAPHY 23
6 ANNEXES 24

Document Information

Date of Issue	28.02.2024
Approval Date	29.02.2024
Certification Report Number	21.0.03/24-002
Sponsor and Developer	TÜBİTAK BİLGEM UEKAE
Evaluation Facility	TÜBİTAK BİLGEM TDD OKTEM
TOE Name	AKIS GEZGIN_N v2.0 SAC&EAC Configuration
Pages	24

Prepared by *(Common Criteria Inspection Expert)*	Merve Hatice KARATAŞ
Prepared by *(Common Criteria Candidate Inspection Expert)*	Almıla Beyza KARAKAPICI
Prepared by *(Common Criteria Candidate Inspection Expert)*	Yavuz AVCI
Reviewed by *(Reviewer)*	Mehmet Kürşad ÜNAL

The experts whose names and signatures are shown as above prepared and reviewed this report.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	28.02.2024	All	Initial 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 5, using Common Methodology for IT Products Evaluation, version 3.1, revision 5. 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 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 (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 = Common Criteria Testing Laboratory) 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 TDD OKTEM, which is a public/commercial CCTL.

A Common Criteria Certificate given to a product/PP means that such product/PP meets the security requirements defined in its security target/PP document that has been approved by the CCCS. The Security Target/PP 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_N v2.0 SAC&EAC Configuration whose evaluation was completed on January 18th, 2024 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM TDD OKTEM (as CCTL), and with the Security Target with version no 11 of the relevant product.

The certification report, certificate of product/PP evaluation and security target/PP 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 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 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:

https://www.commoncriteriaportal.org

1. EXECUTIVE SUMMARY

Developer of the IT product: TÜBİTAK BİLGEM UEKAE
Evaluated IT product: AKIS GEZGIN_N SAC&EAC Configuration
IT Product Version: v2.0
Name of IT Security Evaluation Facility: TÜBİTAK BİLGEM TDD OKTEM
Completion date of evaluation: 18.01.2024
Assurance Package: EAL 5+ (ALC_DVS.2, AVA_VAN.5)

1.1. Brief Description

The TOE is the composition of contactless smartcard IC which is P71D352P of NXP N7121 P71D321 platform, platform crypto library, and the Embedded Operating System (EOS) supporting the electronic Machine Readable Travel Document (eMRTD) application, ISO-compliant Driving Licence (IDL) application, and e-Sign application.

1.2. Major Security Features

The TOE provides the following security services:

- Protection against modification, probing, environmental stress and emanation attacks mainly by platform specification and embedded operating system support as detailed in § 8,
- Passive Authentication (PA),
- Supplemental Access Control (SAC),
- Extended Access Control (EAC),
- The following cryptographic operations for e-Sign:
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Operations,
  - Signature generation with RSASSA-PKCS1-v1_5 and RSASSA-PSS,
  - Signature generation with ECDSA.

The hardware platform including the crypto library is certified for EAL 6 augmented and resistant to physical attacks. For details, please see the platform ST.

1.3. Threats

The threats 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. Note, that the sensitive biometric reference

data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ/SAI data and the portrait are visually readable on the physical part of the travel document as well.

- **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. This violates the authenticity of the travel document's chip used for authentication of a traveler by possession of a travel document. The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them on another appropriate chip to imitate this genuine travel document's chip.
- **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.Tracing:**
  - **(i)** 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.
  - **(ii)** An attacker might also be listening to an existing communication between the MRD's chip and an e-Signature terminal to capture the value(s) of PIN(s) used to authenticate for the use of asymmetric private keys to perform e-Signature generation operations.
- **T.Forgery:** An attacker fraudulently alters the User Data or/and TSF-data stored on the eMRD or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS PACE by means of changed MRD holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.
- **T.Abuse-Func:** An attacker may use functions of the TOE which shall not be used in TOE operational phase in order to:
  - **(i)** manipulate or to disclose the User Data stored in the TOE,
  - **(ii)** manipulate or to disclose the TSF data stored in the TOE or
  - **(iii)** 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 MRD 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 to:
  - **(i)** disclose TSF-data,
  - **(ii)** 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.

- **T. Unauthorised_Access_Sign_Key:** An attacker may improperly use the asymmetric private keys used for e-Signature generation or may capture the value(s) of PIN(s) needed to authenticate for e-Signature generation using asymmetric private keys that he or she is not authorized to. In addition, the software used for the generation of e-Signatures may, intentionally or inadvertently, direct TOE holders to sign additional documents without his or her knowledge or approval.

- **T. Unauthorised_Management_Sign_Objects:** An attacker may illegitimately use the security management services of the TOE for PINs and asymmetric private keys used for e-Signature generation.

1.4. Organizational Security Policies (OSPs)

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)**

  1. The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.
  2. 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.

3. 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.
4. 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)**
  1. 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).
  2. 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. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer.
  3. A Document Signer shall
     a. generate the Document Signer Key Pair
     b. hand over the Document Signer Public Key to the CSCA for certification
     c. keep the Document Signer Private Key secret and
     d. 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)**
  1. The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:
  2. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders.

3. 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.
4. 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).
5. 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.

- **P. Access_Control_Sign_Objects**

  Knowledge of PINs should be used as security attributes to determine the access control behavior and security management privileges during "operational-use" phase for PINs and asymmetric private keys used for e-Signature generation.

- **P. Signature_Generation**

  The TOE shall support following e-Signature generation algorithms:

  - RSASSA-PKCS1-v1_5,
  - RSASSA-PSS,
  - ECDSA

2. CERTIFICATION RESULTS

2.1. Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-92
TOE Name and Version	AKIS GEZGIN_N v2.0 SAC&EAC Configuration
Security Target Title	Security Target of AKIS GEZGIN_N v2.0 SAC&EAC Configuration
Security Target Version	11
Security Target Date	16.01.2024
Assurance Level	EAL 5+ (ALC_DVS.2, AVA_VAN.5)
Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
Protection Profile Conformance	None
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

	• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, conformant • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, conformant
Platform	NXP N7121 P71D321, NXP Technologies
Security Target Title of the Platform Hardware	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4), Security Target Lite
Security Target Version and Date of the Platform Hardware	Version 2.6, *June 13th* 2022
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
Sponsor and Developer	TÜBİTAK BİLGEM UEKAE
Evaluation Facility	TÜBİTAK BİLGEM TDD OKTEM
Certification Scheme	TSE CCCS

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)**

5. The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.
6. 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.
7. 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.
8. 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)**

4. 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).
5. 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. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer.
6. A Document Signer shall
   a. generate the Document Signer Key Pair
   b. hand over the Document Signer Public Key to the CSCA for certification
   c. keep the Document Signer Private Key secret and
   d. 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)**
  6. The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:
  7. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders.
  8. 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.
  9. 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).
  10. 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.

- **P. Access_Control_Sign_Objects**

  Knowledge of PINs should be used as security attributes to determine the access control behavior and security management privileges during "operational-use" phase for PINs and asymmetric private keys used for e-Signature generation.

- **P. Signature_Generation**

  The TOE shall support following e-Signature generation algorithms:

  - RSASSA-PKCS1-v1_5,
  - RSASSA-PSS,
  - ECDSA

2.3. Assumptions and Clarification of Scope

Assumptions for the operational environment of the 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 (i) includes the Country Signing CA Public Key and (ii) 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.

- **A.Sign_Keys (Cryptographic quality of asymmetric keys used for e-Signature generation)**

  The asymmetric private keys used for e-Signature generation must provide sufficiently high cryptographic strength. High quality random numbers must be used for the generation of these key pairs.

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.

For further information see ST.

2.5. Documentation

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

Name of Document	Version Number	Date
Security Target Lite of AKIS GEZGIN_N v2.0 SAC&EAC Configuration	V1	16.02.2024
AKIS GEZGIN_N v2.0 Yönetici ve Kullanıcı Kılavuzu	V7	16.01.2024
AKIS GEZGIN_N v2.0 Kişiselleştirme Kılavuzu	V5	13.12.2023
AKIS GEZGIN_N v2.0 SAC & EAC Configuration Teslim ve İşletim Dokümanı	V2	14.08.2023

2.6. IT Product Testing

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 432 functional tests in total.

2.6.2 Evaluator Testing

- **Independent Testing:** Evaluator has chosen 33 developer tests to conduct by itself. Additionally, evaluator has prepared 23 independent tests. TOE has passed all 56 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, 24 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_N v2.0 SAC&EAC Configuration),
- Secure IC (NXP Technologies, N7121 P71D321),

- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- Guidance documents
- Activation data

2.8. Results of the Evaluation

The table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 5 (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	Result
ADV: Development	ADV_ARC.1	Security Architecture Description	PASS
	ADV_FSP.5	Complete semi-formal functional specification with additional error information	PASS
	ADV_IMP.1	Implementation representation of the TSF	PASS
	ADV_INT.2	Well-structured internals	PASS
	ADV_TDS.4	Semiformal Modular Design	PASS
	ADV_COMP.1	Design Compliance with the Platform Certification Report, Guidance and ETR_COMP	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance	PASS
	AGD_PRE.1	Preparative Procedures	PASS
ALC: Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and automation	PASS
	ALC_CMS.5	Development tools CM coverage	PASS
	ALC_DEL.1	Delivery Procedures	PASS
	ALC_DVS.2	Sufficiency of security measures	PASS
	ALC_LCD.1	Developer defined life-cycle model	PASS
	ALC_TAT.2	Compliance with implementation standards	PASS

	ALC_COMP.1	Integration of the Application into the Underlying Platform and Consistency Check for Delivery And Acceptance Procedures	PASS
ASE: Security Target Evaluation	ASE_CCL.1	Conformance Claims	PASS
	ASE_ECD.1	Extended Components Definition	PASS
	ASE_INT.1	ST Introduction	PASS
	ASE_OBJ.2	Security Objectives	PASS
	ASE_REQ.2	Derived Security Requirements	PASS
	ASE_SPD.1	Security Problem Definition	PASS
	ASE_TSS.1	TOE Summary Specification	PASS
	ASE_COMP.1	Consistency of Security Target Objectives	PASS
ATE: Tests	ATE_COV.2	Analysis of Coverage	PASS
	ATE_DPT.3	Testing: Modular Design	PASS
	ATE_FUN.1	Functional Testing	PASS
	ATE_IND.2	Independent Testing - Sample	PASS
	ATE_COMP.1	Composite Functional Testing	PASS
AVA: Vulnerability Analysis	AVA_VAN.5	Advanced Methodical Vulnerability Analysis	PASS
	AVA_COMP.1	Composite Product Vulnerability Assessment	PASS

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_N v2.0 SAC&EAC Configuration", the results of the assessment of all evaluation tasks are "Pass".

2.9. Evaluator Comments / Recommendations

It is recommended that all guidance outlined in the Guidance Documents be followed and all assumptions are fulfilled in order to the secure usage of the TOE.

3. SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:

Title: Security Target of AKIS GEZGIN_N v2.0 SAC&EAC Configuration

Version: 11

Date of Document: 16.01.2024

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

Title: Security Target Lite of AKIS GEZGIN_N v2.0 SAC&EAC Configuration

Version: 01

Date of Document: 16.02.2024

4. GLOSSARY

AA : Active Authentication

ADV : Assurance of Development

AES : Advanced Encryption Standard

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

BAC : Basic Access Control

BAP : Basic Access Protection

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 : Operational User Guidance

OSP : Organizational Security Policy

PP : Protection Profile

PRE : Preparative Procedures

PP : Protection Profile

SAC : Supplemental Access Control

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

TDD: Test ve Değerlendirme Direktörlüğü

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

TÜBİTAK : 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 5, April 2017

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017

[3] Composite Product Evaluation for Smart Cards and Similar Devices, v1.5.1, May 2018

[4] Application of Attack Potential to Smartcards, v3.2, November 2022

[5] DTR 97 TR 01 AKIS GEZGIN_N v2.0 SAC&EAC Configuration EAL 4+ (ALC_DVS.2, AVA_VAN.5) Evaluation Technical Report, Rev1.0, 18 January 2024

[6] 1136-V3_ETR-COMP_220825_v2, ETR for Composite Evaluation V2: N7121 B1, NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) B1, v2, 25 August 2022

[7] Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Extended Access Control, BSI-PP-0056-V2-2012, version 1.3.2, 5 December 2012

[8] Security IC Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, version 1.0, 19 February 2014

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

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

[11] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) Security Target Lite, NXP Semiconductors, rev. 2.6, 13 June 2022

[12] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, BSI-DSZ-CC-1136-V3-2022, v3, 2022

[13] Assurance Continuity Maintenance Report, NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, BSI-DSZ-CC-1136-V3-2022-MA-01, v3, 2022

[14] NXP Secure Smart Card Controller N7121 Information on Guidance and Operation, rev.3.2, 28 May 2019

[15] SmartMX3 Family N7121 Wafer and Delivery Specification, rev. 3.3, 3 November 2021

[16] N7121 Crypto Library Information on Guidance and Operation, rev.3.4, 4 May 2022

[17] N7121 Crypto Library Errata sheet, rev.1.0, 2 February 2023

[18] N7121 Crypto Library ECC over GF(p) Library, rev.2.3, 4 May 2022

6. ANNEXES

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