KECS-CR-19-29

KCOS e-Passport Version 5.0 - BAC and AA on S3D350A Family Certification Report

Certification No.: KECS-ISIS-0936-2019

2019. 6. 18.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2019.06.18	-	Certification report for KCOS e-Passport Version 5.0 - BAC and AA on S3D350A Family - First documentation

This document is the certification report for KCOS e-Passport Version 5.0 – BAC and AA on S3D350A Family of KOMSCO.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL4+ evaluation of KCOS e-Passport Version 5.0 - BAC and AA on S3D350A Family with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is the composite product which is consisting of the certified contactless integrated circuit chip of machine readable travel documents (IC chip) and embedded software (IC chip operating system(COS) and the application of machine readable travel documents(MRTD application)) including Logical Data Structure (LDS) in accordance with the ICAO documents [5]. The TOE provides Basic Access Control (BAC) and Active Authentication (AA) defined in the ICAO’s Doc9303 Machine Readable Travel Documents [5] and the BSI’s TR-03110 Advanced Security Mechanisms Machine Readable Travel Documents and eIDAS Token [6]. Supplemental Access Control (SAC) and Extended Access Control (EAC) are also supported by the product, but SAC and EAC are not included in the scope of this TOE and separately evaluated and certified at the same time in consideration of different level of assurance which is required by different PPs which are claimed conformance by each TOE.

The TOE is composed of the following components:

- IC chip: S3D350A/S3D300A/S3D264A/S3D232A revision 2 provided by Samsung Electronics, see ANSSI-CC-2019/01, and
- Embedded software: KCOS e-Passport Version 5.0 - BAC and AA provided by KOMSCO.

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on June 12, 2019. This report grounds on the evaluation technical report (ETR) TTA had submitted [7] and the Security Target (ST) [8][9].

The ST is based on the certified Protection Profile (PP) Machine Readable Travel Document with ICAO Application Basic Access Control Version 1.10 (“BAC PP” hereinafter) [10]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL4 augmented by ADV_FSP.5, ADV_INT.2, ADV_TDS.4,

ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, and ATE_DPT.3. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 extended.

The TOE implements the following TOE Security Features. For more details refer to the ST [8][9].

TOE Security Features	Brief Summary
SF.PAC_AUTH	Personalization Agent Authentication
SF.BAC_AUTH	BAC Authentication
SF.ACTIVE_AUTH	AA
SF.SEC_MESSAGE	Secure Messaging
SF.ACC_CONTROL	Access Control for Personalization Agent and IS, Personalization and Management
SF.RELIABILITY	TSF testing, protection against tempering and observation, preservation of secure state, residual information protection
SF.IC	IC chip security functionality

[Table 1] TOE Security Functionalities

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE is composite product consisting of the following components and related guidance documents.

	Identifier	Release	Delivery Form / Method
TOE	KCOS e-Passport Version 5.0 - BAC and AA on S3D350A Family - K5.0.01.SS.D35A.02(S3D350A) - K5.0.01.SS.D30A.02(S3D300A) - K5.0.01.SS.D26A.02(S3D264A) - K5.0.01.SS.D23A.02(S3D232A)	Rev 1	IC Chip Module (Note: The Secure Boot loader & System API Code is contained in ROM and other SW is contained in FLASH memory of the IC chip.) / By a person (HW), and PGP mail (SW)
IC Chip (HW)	S3D350A/S3D300A/S3D264A/S3D232A	Revision 2	
IC Dedicated SW	Secure RSA/ECC/SHA Library	V2.01	
	DTRNG FRO Library	V2.0	
	Secure Boot loader & System API Code	V0.7	
COS and MRTD Application	KCOS e-Passport Version 5.0 - BAC and AA - KCOS50_350A.hex-1.3 - KCOS50_300A.hex-1.3 - KCOS50_264A.hex-1.3 - KCOS50_232A.hex-1.3	Rev 1	
Document	Operational User Guidance: EPS-05-QT-OPE-BAC-1.0	V1.0	Softcopy or Hardcopy / By PGP mail or a person
	Preparative Procedures Guidance: EPS-05-QT-PRE-BAC-1.0	V1.0	

[Table 2] TOE identification

The TOE is finalized at step 3 of the Phase 2 (Manufacturing) in accordance with the PPs [10]. TOE is Composite product that should be considered in the Composite Product life cycle. Composite product integrator performs Composite product integration (FLASH code download into IC chip), preparation and shipping to the personalization for the Composite product (Composite Product Integration). After Composite Product Integration, the ePassport manufacturer (i.e., inlay and e-Cover

manufacturer) embeds the TOE into the passport booklet. Then, the Personalization Agency performs personalization and testing stage where the User Data/TSF Data is loaded into the IC's memory.

The Personalization Agency can only access the TOE using the securely delivered personalization key set (through PGP mail or directly from the SW developer to the Personalization Agency).

The certified IC chip which is a component of the TOE provides Contact interfaces and Contactless interfaces, the Contact interfaces are not used by the TOE. Thus, the Type A Contactless interface is used by the TOE. For details on the IC chips, the IC dedicated software and the crypto libraries, see the documentation under ANSSI-CC-2019/01 [11].

[Table 3] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (24 August 2017) Korea Evaluation and Certification Scheme for IT Security (12 September 2017)
TOE	KCOS e-Passport Version 5.0 – BAC and AA on S3D350A Family - K5.0.01.SS.D35A.02(S3D350A) - K5.0.01.SS.D30A.02(S3D300A) - K5.0.01.SS.D26A.02(S3D264A) - K5.0.01.SS.D23A.02(S3D232A)
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
Common Methodology	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017
EAL	EAL4+ (augmented by ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, and ATE_DPT.3)
Developer	KOMSCO
Sponsor	KOMSCO

Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	June 12, 2019
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The ST [8][9] for the TOE claims strict conformance to the BAC PP [10], and the TOE complies security policies defined in the PP [10] by security objectives and security requirements based on the ICAO document [5] and BSI specification [6]. Thus the TOE provides security features BAC and AA.

Additionally, the TOE provides security features for Personalization Agent to protect initialization data and application data (during pre-personalization and personalization phase):

- Personalization Agent authentication, ensures only authorized entity can access to the TOE during pre-personalization and personalization phase,
- Secure messaging, ensures transmitted data to be protected from unauthorized disclosure and modification during pre-personalization and personalization phase.

Furthermore, the TOE is composite product based on the certified IC chip, thus the TOE utilizes and therefore provides some security features covered by the IC chip certification such as security sensors/detectors, life time detector, dedicated hardware mechanisms against side-channel attacks, secure DES and AES symmetric cryptography support, secure TORNADO-T coprocessor for the support of RSA and ECC cryptographic operations, and a hardware Digital True Random Number Generator (DTRNG FRO) that meets PTG.2 class of BSI-AIS31 (German scheme) and some of ANSSI RGS requirements (French Scheme). For more details refer to the Security Target Lite for the IC chip [12].

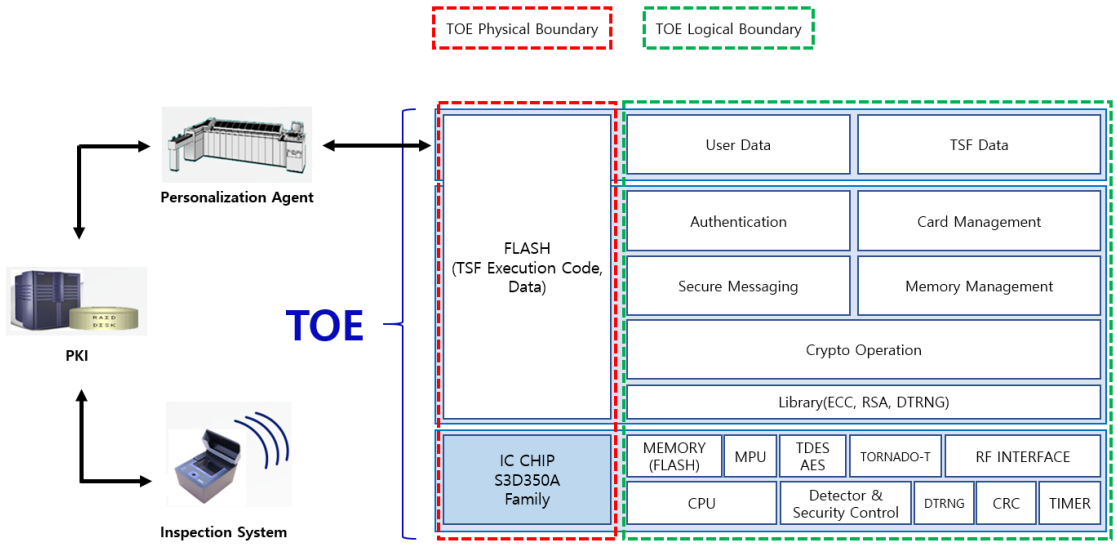
4. Assumptions and Clarification of Scope

The assumptions related to the security aspects of the operational environment in which the TOE will be used or is intended to be used are described in the ST [8][9] (for

the detailed and precise definition of the assumption refer to the ST [8][9], chapter 3.1): Furthermore, some aspects of threats and organisational security policies are not covered by the TOE itself, thus these aspects are addressed by the TOE environment: Examination of the physical part of the MRTD, MRTD holder Obligations, Issuing of the MRTD, Terminal operating, etc. Details can be found in the ST [8][9], chapter 3.2, 3.3 and 4.2.

5. Architectural Information

[Figure 1] show the physical scope of the TOE. The TOE is the composite product which is consisting of the certified contactless IC chip and the embedded software (i.e., COS and MRTD application).



[Figure 1] Scope of the TOE

- IC chip provides security features such as security sensors/detectors, MPU (Memory Protection Unit), secure DES and AES symmetric cryptography support, secure coprocessor TONADO-T for RSA and ECC cryptographic support, and a Digital True Random Number Generator (DTRNG).
- COS, which processes commands and manages files in accordance with ISO/IEC 7816-4, 8, and 9 [20], executes MRTD application and provides functions for management of application data. The COS is contained in FLASH.
- Application provides MRTD application (BAC and AA in accordance with the

ICAO document [5]). It also provides additional security mechanisms for Personalization Agent such as authentication and personalization of MRTD. The Application is contained in FLASH.

- Application Data is consisting of User Data and TSF Data. The Application Data is contained in FLASH.

For the detailed description is referred to the ST [8][9].

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
KCOS e-Passport Version 5.0 - BAC and AA on S3D350A Family Operational User Guidance V1.0(EPS-05-QT-OPE-BAC-1.0) Inspection	V1.0	May 27, 2019
KCOS e-Passport Version 5.0 - BAC and AA on S3D350A Family Preparative Procedures Guidance V1.0(EPS-05-QT-PRE-BAC-1.0)	V1.0	May 27, 2019

[Table 4] Documentation

7. TOE Testing

The TOE is composite product and the developer took a testing approach based on the components of the TOE including the platform, COS, and the MRTD application.
Tests for the TOE are:

- Standard and Security Mechanisms Test: Layer 6~7 MRTD Application Protocol & Data Test (Security and Command Test, Logical Data Structure Tests, etc.), which tests MRTD application according to Standard Test Specifications (the ICAO Technical Report RF Protocol and Application Test Standard, BSI TR-03105, etc.),
- Operational Mode Test: Additional features test which are not defined in the

ICAO document [5], BSI specification [6] such as pre-personalization, personalization and inspection, Positive and Negative Test for APDUs in each TOE life cycle(5 phases), life cycle state change, residual information removal, etc., and

- Other Test: Layer 3~4 RF Protocol Activation and Transmission Test (anti-collision test, etc.).

The developer tested all the TSF and analyzed testing results in accordance with the assurance component ATE_COV.2. This means that the developer tested all the TSFI defined for each life cycle state of the TOE, and demonstrated that the TSF behaves as described in the functional specification.

The developer tested both subsystems (including their interactions) and modules (including their interfaces), and analyzed testing results in accordance with the assurance component ATE_DPT.3.

The developer correctly performed and documented the tests in accordance with the assurance component ATE_FUN.1.

The evaluator performed all the developer's tests, and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests. The tests cover preparative procedures in accordance with the guidance. Some tests were performed by design and source code analysis to verify fulfillment of the requirements of the underlying platform to the COS and MRTD Application. The implementation of the requirements of the platform's ETR and guidance as well as of the MRTD security mechanisms was verified by the evaluators.

Also, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These test cases cover testing APDU commands, bypass, fault injection, and so on. No exploitable vulnerabilities by attackers possessing Enhanced-Basic attack potential were found from penetration testing.

The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [7].

8. Evaluated Configuration

The TOE is KCOS e-Passport Version 5.0 - BAC and AA on S3D350A Family. The TOE is composite product consisting of the following components:

- IC chip: S3D350A/S3D300A/S3D264A/S3D232A revision 2 provided by Samsung Electronics, see ANSSI-CC-2019/01, and
- Embedded software: KCOS e-Passport Version 5.0 - BAC and AA provided by KOMSCO.

The TOE is identified by the name, version and release number. The TOE identification information is provided by the command-response APDU as follows:

- Command APDU : 80FB000113
- Part of Response APDU : D35A 4250 4B53 9114 50 01 02 9000 or D30A 4250 4B53 9114 50 01 02 9000 or D26A 4250 4B53 9114 50 01 02 9000 or D23A 4250 4B53 9114 50 01 02 9000
  - D35A : IC chip identifier (S3D350A : D35A, S3D300A : D30A, S3D264A : D26A, S3D232A : D23A)
  - 4250 : IC Manufacturer (Samsung)
  - 4B53 : OS ID (KCOS e-Passport)
  - 9114 : OS Release Data (YDDD, 2019. 4. 24)
  - 50 : TOE Version (Version 5.0)
  - 01 : OS Release Level (Rev 1)
  - 02 : IC Chip Version (Revision 2)
  - 9000 : Response APDU Status Word

And the guidance documents listed in this report chapter 6, [Table 4] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [7] which references Single Evaluation Reports for each assurance requirement and Observation Reports.
The evaluation result was based on the CC [1] and CEM [2], and supporting documents for the Smartcard and similar device [13], [14], [15], [16], [17] and [18]. Also

the evaluation facility utilized German scheme's Evaluation Methodology for CC Assurance Class for EAL5+ and EAL6 [22] under confirmation of the CB.
As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL4 augmented by ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, and ATE_DPT.3.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.
The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.
The Security Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is assigned to ASE_SPD.1.
The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.
The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore the verdict PASS is assigned to ASE_ECD.1.
The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.
The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.
Also, the evaluator confirmed that the ST of the composite TOE does not contradict the ST of the IC chip in accordance with the supporting document Composite Product Evaluation [13].
Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.
The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer has used a documented model of the TOE life-cycle. Therefore the verdict PASS is assigned to ALC_LCD.1.

The developer has used well-defined development tools that yield consistent and predictable results, and implementation standards have been applied. Therefore the verdict PASS is assigned to ALC_TAT.2.

The developer has clearly identified the TOE and its associated configuration items, and the ability to modify these items is properly controlled by automated tools, thus making the CM system less susceptible to human error or negligence. Therefore the verdict PASS is assigned to ALC_CMC.4.

The configuration list includes the TOE, the parts that comprise the TOE, the TOE implementation representation, security flaws, development tools and related information, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.5.

The developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. Additionally, sufficiency of the measures as applied is intended be justified. Therefore the verdict PASS is assigned to ALC_DVS.2.

The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.

Also, the evaluator confirmed that the correct version of the embedded software is installed onto/into the correct version of the underlying IC chip, and the delivery procedures of IC chip and embedded software developers are compatible with the acceptance procedure of the composite product integrator in accordance with the supporting document Composite Product Evaluation [13].

Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the life-cycle model used by the developer, the configuration management, the security measures used throughout TOE development, the tools used by the developer throughout the life-cycle of the TOE, the handling of security flaws, and the delivery activity.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It provides a detailed description of the SFR-enforcing and SFR-supporting modules and enough information about the SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented; as such, the TOE design provides an explanation of the implementation representation. Therefore the verdict PASS is assigned to ADV_TDS.4.

The developer has completely described all of the TSFI in a manner such that the evaluator was able to determine whether the TSFI are completely and accurately described, and appears to implement the security functional requirements of the ST. Therefore the verdict PASS is assigned to ADV_FSP.5.

The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.

The implementation representation is sufficient to satisfy the functional requirements of the ST and is a correct realisation of the low-level design. Therefore the verdict PASS is assigned to ADV_IMP.1.

The TSF internal is well-structured such that the likelihood of flaws is reduced and that maintenance can be more readily performed without the introduction of flaws.

Therefore the verdict PASS is assigned to ADV_INT.2.
Also, the evaluator confirmed that the requirements on the embedded software, imposed by the IC chip, are fulfilled in the composite product in accordance with supporting documents Composite Product Evaluation [13] and ADV_ARC Evaluation [17][18].
Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed), an implementation description (a source code level description), and TSF internals description (which describes evidence of the structure of the design and implementation of the TSF). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).
The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.2.
The developer has tested all the TSF subsystems and modules against the TOE design and the security architecture description. Therefore the verdict PASS is assigned to ATE_DPT.3.
The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.
By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.
Also, the evaluator confirmed that composite product as a whole exhibits the properties necessary to satisfy the functional requirements of its ST in accordance with the supporting document Composite Product Evaluation [13].
Thus, the TOE behaves as described in the ST and as specified in the evaluation

evidence (described in the ADV class).
The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetration testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing Enhanced-Basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.3.
Also, the evaluator confirmed that there is no exploitability of flaws or weakness in the composite TOE as a whole in the intended environment in accordance with the supporting documents Composite Product Evaluation [13] and other related supporting documents [14][15][16].
Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), don't allow attackers possessing Enhanced-Basic attack potential to violate the SFRs.
The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		ASE_TSS.1.2E	PASS		
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_TAT.2	ALC_TAT.2.1E	PASS	PASS	
		ALC_TAT.2.2E	PASS		
	ALC_CMS.5	ALC_CMS.5.1E	PASS	PASS	
	ALC_CMC.4	ALC_CMC.4.1E	PASS	PASS	
	ALC_DVS.2	ALC_DVS.2.1E	PASS	PASS	
		ALC_DVS.2.2E	PASS		
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.4	ADV_TDS.4.1E	PASS	PASS	PASS
		ADV_TDS.4.2E	PASS	PASS	
	ADV_FSP.5	ADV_FSP.5.1E	PASS	PASS	
		ADV_FSP.5.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
	ADV_IMP.1	ADV_IMP.1.1E	PASS	PASS	
	ADV_INT.2	ADV_INT.2.1E	PASS	PASS	
		ADV_INT.2.2E	PASS		
ATE	ATE_COV.2	ATE_COV.2.1E	PASS	PASS	PASS
	ATE_DPT.3	ATE_DPT.3.1E	PASS	PASS	
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.3	AVA_VAN.3.1E	PASS	PASS	PASS
		AVA_VAN.3.2E	PASS		
		AVA_VAN.3.3E	PASS		
		AVA_VAN.3.4E	PASS		

[Table 5] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The documents listed in this report chapter 6, contain necessary information about the usage of the TOE and all security recommendations have to be considered. All aspects of Assumptions, Threats and Organizational Security Policies in the ST [8][9] not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.
- As the TOE supports S3D350A/S3D300A/S3D264A/S3D232A as the IC chip platform, it is recommended to refer to the user's manual provided along with the TOE and check the identification information of the TOE.
- When secure messaging is not applied during personalization phase according to the policy of the Personalization Agent, it is strongly recommended that the physical, procedural and personal security measures are in place in order to ensure confidentiality and integrity of the transmitted data during personalization phase.
- It has to be ensured that MRZ data which are used to derive BAC authentication keys provides sufficient entropy to withstand related attacks.
- The TOE supports both SAC and BAC to ensure global interoperability. Thus, the Inspection System should use SAC instead of BAC.
- The BAC mechanism cannot resist attacks with high attack potential. If nevertheless BAC has to be used, it is recommended to perform Chip Authentication before getting access to data (except EF.DG14), as this mechanism is resistant to high potential attacks.
- When accepting the TOE, it is recommended that the TOE user shall verify the integrity of the Flash code and data in accordance with the documents (Refer to chapter 6.) provided along with the TOE.

11. Security Target

KCOS e-Passport Version 5.0 – BAC and AA on S3D350A Family Security Target V1.1, May 13, 2019 [8] is included in this report by reference. For the purpose of publication,

it is provided as sanitized version [9] according to the CCRA supporting document ST sanitising for publication [19].

12. Acronyms and Glossary

APDU	Application Protocol Data Unit
CC	Common Criteria
DG	Data Group
EAL	Evaluation Assurance Level
ICAO	International Civil Aviation Organization
IS	Inspection System
BIS	BAC/SAC supporting Inspection System
EIS	EAC supporting Inspection System
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

AA (Active Authentication)	The security mechanism with which the IC chip demonstrates its genuine to the IS by signing random number transmitted from the IS and the IS verifies genuine of the IC chip through verification with the signed values
Application Protocol Data Unit (APDU)	Standard communication messaging protocol between a card accepting device and a smart card. The structure of the APDU is defined by ISO/IEC 7816-4
BAC (Basic Access Control)	The security mechanism that implements the symmetric key-based entity authentication protocol for mutual authentication of the MRTD chip and the IS (BIS) and the symmetric key-based key distribution protocol to generate the session keys necessary in establishing the

	secure messaging for the MRTD chip and the IS
DS (Document Signer) Certificate	The certificate of the Personalization agent signed with the digital signature generation key of the PA-PKI root CA used by the IS to verify the SOD of the PA security mechanism
EAC (Extended Access Control)	The security mechanisms consisted with the EAC-CA for chip authentication and the EAC-TA for the IS authentication in order to enable only the EAC supporting Inspection System (EIS) to read the biometric data of the ePassport holder for access control to the biometric data of the ePassport holder stored in the MRTD chip
EAC-CA (EAC-chip Authentication)	The security mechanism to implement the DH/ECDH key distribution protocol to enable the MRTD chip authentication by the EIS through key checking for the EAC chip authentication public key and private key of the MRTD chip and temporary public key and private key of the EIS
EAC-TA (EAC-terminal Authentication)	The security mechanism that the EIS transmits values digital signature with the digital signature generation key of its own to the temporary public key used in the EAC-CA and the MRTD chip by using the IS certificate, verifies the digital signature. This security mechanism implements challenge-response authentication protocol based on digital signature through which the MRTD chip authenticates the EIS.
ePassport	The passport embedded the contactless IC chip in which identity and other data of the ePassport holder stored in accordance with the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO)
IS (Inspection System)	As an information system that implements optical MRZ reading function and the security mechanisms (PA, BAC, SAC, EAC and AA, etc.) to support the MRTD inspection, the IS consists with a terminal that establishes the RF communication with the IC chip and

	the system that transmits commands to the IC chip through this terminal and processes responses for the commands
LDS (Logical Data Structure)	Logical data structure defined in the ICAO document in order to store the user data in the MRTD chip
MRTD	Machine Readable Travel Document, e.g. passport, visa or official document of identity accepted for travel purposes
MRTD Application	Program for loaded in the MRTD chip that is programmed by the LDS of the ICAO document and provides security mechanisms of BAC, SAC, PA and EAC, etc.
MRTD Chip	The contactless IC chip that includes the MRTD application and the IC chip operating system necessary in operation of the MRTD application and that supports communications protocol by ISO/IEC 14443
PA (Passive Authentication)	The security mechanism to demonstrate that identity data recorded in the MRTD has not been forgery and corruption as the IS with the DS certificate verifies the digital signature in the SOD and hash value of user data in accordance with read-right of the MRTD access control policy
Personalization Agent	The agent receives the ePassport identity data from the Reception organization and generates the SOD by digital signature on the data. After recording them in the IC chip, the personalization agent generates TSF data and stores it in the secure memory of the IC chip. The agent also operates PA-PKI and/ or EAC-PKI
SAC (Supplemental Access Control)	The security mechanism is supplementary to BAC. The SAC performs mutual authentication for the MRTD chip and the IS (BIS) to access control of user data of the MRTD and establishes the secure messaging for the MRTD chip and the IS
SOD (Document Security Object)	The SOD refers to the ePassport user data recorded in the Personalization phase by the Personalization agent that is signed by the Personalization agent with the

digital signature generation key

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017

[3] Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017)

[4] Korea Evaluation and Certification Scheme for IT Security (September 12, 2017)

[5] Doc9303 Machine Readable Travel Documents Seventh Edition, International Civil Aviation Organization(ICAO), 2015

[6] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Version2.20, Bundesamtfür Sicherheitinder Informationstechnik(BSI), February 2015

[7] TTA-CCE-18-004 KCOS e-Passport Version 5.0 – BAC and AA on S3D350A Family Evaluation Technical Report V1.3, June 12, 2019

[8] KCOS e-Passport Version 5.0 – BAC and AA on S3D350A Family Security Target V1.1, May 13, 2019 (Confidential Version)

[9] KCOS e-Passport Version 5.0 – BAC and AA on S3D350A Family Security Target Lite V1.0, June 10, 2019 (Sanitized Version)

[10] Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application” Basic Access Control V1.10, BSI-CC-PP-0055, March 2009

[11] Certification Report ANSSI-CC-2019/01 S3D350A/S3D300A/S3D264A/S3D232A /S3D200A/S3K350A/S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, January 18, 2019, ANSSI

[12] Security Target Lite of S3D350A/S3D300A/S3D264A/S3D232A/S3D200A /S3K350A/S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software Version 4.1, October 25, 2018

[13] Composite product evaluation for Smartcards and similar devices Version 1.5.1,

JIL, May 2018

[14] Application of Attack Potential to Smartcards Version 2.9, JIL, January, 2013

[15] The Application of CC to Integrated Circuits Version 3.0, JIL, February 2009

[16] Minimum ITSEF Requirements for Security Evaluation of Smart cards and similar devices Version 2.0, JIL, January 2017

[17] Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Version 2.0, JIL, January 2012

[18] Security Architecture requirements (ADV_ARC) for smart cards and similar devices - Appendix 1, Version 2.0, JIL, January 2012

[19] ST sanitising for publication, CCDB-2006-04-004, April 2006

[20] ISO/IEC 7816 Identification cards – Integrated circuit(s) cards with contacts

[21] ISO/IEC 14443 Identification cards – Contactless ICCs - Proximity cards

[22] Application Notes and Interpretation of the Scheme (AIS), AIS 34, Version 3, BSI, March 9, 2009