KECS-CR-09-49

SK e-Pass V1.0

Certification Report

Certification No: KECS-ISIS-0254-2010

National Intelligence Service IT Security Certification Center

Establishment & Revision History			
Revision Number	Date	Page	Details
00	2010. 07. 22	-	First documentation

This document is the certification report for

SK C&C SK e-Pass V1.0

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Information Security Agency

Contents

1. Summary

This report describes the certification result drawn by the certification body on the results of the EAL4+ evaluation of SK e-Pass V1.0 with reference to Common Criteria for Information Technology Security Evaluation (notified September. 1, 2009, "CC" hereinafter). It describes the evaluation result and its soundness and conformity.

The evaluation of the TOE has been carried out by Korea Information Security Agency and completed on 30. June. 2010. This report grounds on the evaluation technical report (ETR) KISA had submitted. The evaluation has confirmed that the product had satisfied CC Part 2 and EAL4 of CC Part 3 which added ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4, therefore the evaluation results was decided to be “suitable”.

The TOE consists of JAVA card based-smartcard OS (‘SK COS’ hereinafter) and MRTD application installed and operated in the SK COS, and it is installed on S3CC9LC (EAL5+, BSI-DSZ-CC-0624-2010-MA-01, 2010.3.16) IC chip of Samsung Electronics to be operated.

The TOE composes an ePassport by combining IC chip hardware and an antenna, and an IC chip and an antenna are excluded from the TOE scope. Following shows the operational environment where the TOE drives.

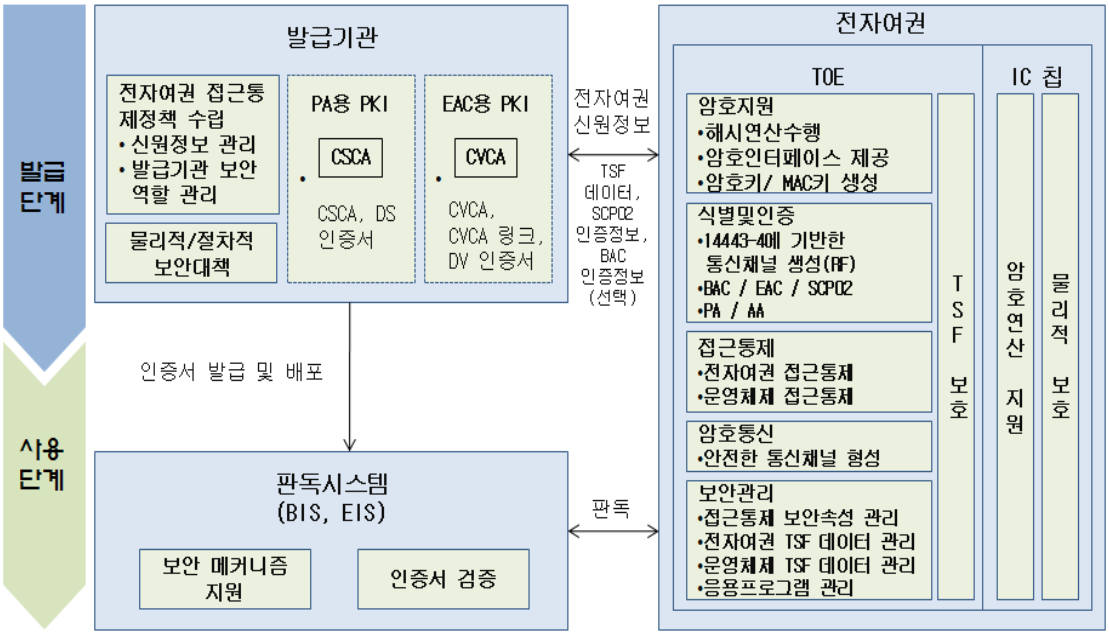

Figure 1 TOE Operation Environment

The CB(Certification Body) has examined the evaluation activities and testing procedures, provided the guidance for the technical problems and evaluation procedures, and reviewed each WPR(Work Package Report), and ETR(Evaluation Technical Report). The CB confirmed that the evaluation results ensure that the TOE satisfies all security functional requirement and assurance requirement described in ST. Therefore, the CB certified that observation and evaluation results by evaluators are accurate and reasonable.

Certification validity: Information in this certification report does not guarantee that the government of Republic of Korea permits use of the SK e-Pass V1.0.

2. Information for Identification

Scheme	Korea evaluation and certification guidelines for IT security (1. 9. 2009) Korea Evaluation and Certification Scheme for IT Security (1. 1. 2010)
TOE	SK e-Pass V1.0
Protection Profile	ePassport Protection Profile V2.1
ST	SK e-Pass V1.0 ST V1.6
ETR	SK e-Pass V1.0 ETR V1.0 (2010.6.30)
Evaluation results	Suitable - Conformance Claim: CC Part 2 and Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V3.1 (1. 9. 2009)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V3.1 (1. 9. 2009)
Sponsor	SK C&C
Developer	SK C&C
Evaluator	Public Security Service Team, Public Security Division, Korea Security & Internet Agency(KISA) La Eunjoo, Ji Jaeduck
Certification body	IT Security Certification Center(ITSCC)

3. Security Policies

The TOE is operated by complying with the following Security Policies.

P. International Compatibility

A personalization agent shall ensure compatibility between security mechanism of an ePassport and security mechanism of an inspection system for immigration.

Application Note: The TOE shall ensure international compatibility by complying the ICAO document and the EAC specification.

P. Security Mechanism Application Procedures

The TOE shall ensure an order of security mechanism application according to the type of an inspection system so that not to violate the e-Passport access control policies of a personalization agent.

Application Note: The TOE has a different flow of work according to the types of security mechanism supported by an inspection system. A basic flow of work complies Standard e-Passport Inspection Procedure described in 2.1.1 and Advanced e-Passport Procedure in 2.1.2 of the EAC specification.

P. Application Program Loading

A personalization agent shall approve a loading of an application program after checking that the application program loaded in the MRTD chip does not affect the secure TOE.

Application Note: The TOE does not allow loading other application programs except for a MRTD application.

P. Personalization Agent

A personalization agent shall issue an ePassport in the secure manner so that it confirm that a subject of issuance has not been changed, and shall deliver the TOE to the operational use

phase after verifying that the data inside a MRTD chip are operating normally after issuance. The personalization agent shall deactivate the write-function before the TOE delivery to the operational use phase.

P. e-Passport Access Control

A Personalization agent and the TOE shall build an e-Passport access control policy in order to protect MRTD application data. Also, the TOE shall regulate the user roles. A personalization agent has personalization authorization when it succeeded in personalization agent authentication in the issuance phase, and has management authorization when it succeeded in personalization agent authentication in the operational use phase.

Application Note: The TOE shall establish an access control policy according to the ICAO document and the EAC specification as followings.

		List of Objects	Objects									
			Personal data of the ePassport applicant		Biometric data of the ePassport applicant		e-Passport Authentication Data		EF.CVCA		EF.COM	
List of Subjects			Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights
Subjects	BIS	BAC Authorization	allow	deny	deny	deny	allow	deny	allow	deny	allow	deny
	EIS	BAC Authorization	allow	deny	deny	deny	allow	deny	allow	deny	allow	deny
		EAC Authorization	allow	deny	allow	deny	allow	deny	allow	deny	allow	deny
	Pesonalization Agent	Pesonalization Authorization	allow	allow	allow	allow	allow	allow	allow	allow	allow	allow
		Management Authorizatio	deny	deny	deny	deny	deny	deny	deny	deny	deny	deny

		n										

P. PKI

ePassport issuing countries shall execute certification practice to securely generate · manage a digital signature key and to generate · issue · operate · destroy certificates according to CPS by establishing PA-PKI and EAC-PKI according to e-Passport PKI System. Also, ePassport issuing countries update a certificate according to the management policy for validity of certificate; therefore they securely deliver a certificate to verifying countries and an inspection system. When EAC-TA provides the TOE with CVCA link certificate, DV certificate and IS certificate after an inspection system obtaining information from EF.CVCA stored in the TOE, the TOE shall internally update certificate by verifying validity of the certificate.

P. Range of RF Communication

RF communication distance between a MRTD chip and an inspection system shall be less than 5cm and RF communication channel shall not be established if the page of an ePassport attached with IC chip is not opened.

4. Assumptions and Scope

4.1. Assumptions

The TOE shall be installed and operated with the following assumptions in consideration.

A. Certificate Verification

An inspection system, such as BIS and EIS, verifies SOD after verifying validity of a certificate chain for PA (CSCA certificate → DS certificate) in order to verify forgery and corruption of ePassport personal data recorded in the TOE. For this, DS certificate and CRL shall be verified periodically. EIS shall securely hold a digital signature generation key that corresponds to IS certificate and shall provide the TOE with CVCA link certificate, DV certificate and IS certificate in EAC-TA.

Application Note: BIS shall periodically verify CSCA certificate according to ICAO PKD or a diplomatic channel of ePassport issuing countries. EIS shall periodically verify a CVCA certificate and a CVCA link certificate according to a diplomatic channel of ePassport issuing countries.

A. Inspection System

An inspection system shall execute security mechanisms of PA, BAC and EAC according to ICAO document and EAC specification on the basis of the verification policy of an ePassport for an ePassport holder. Also, after session ends, BIS and EIS shall securely destroy all information used in communication and the TOE, such as a BAC session key, a EAC session key and session information, etc.

Application Note: The TOE denies the request to access EF.SOD by an inspection system that failed in BAC mutual authentication.

As BIS supports BAC and PA security mechanism, it obtains read-rights for personal data and authentication data of an ePassport holder if BAC mutual authentication using a BAC authentication key succeeds. Then, by establishing BAC secure messaging with a BAC session key, it ensures confidentiality and integrity of all transmitted data. BIS verifies SOD by executing PA after BAC. Then, by calculating and comparing a hash value for personal

data and authentication data of an ePassport holder, it verifies forgery and corruption for personal data and authentication data of an ePassport holder.

As EIS supports the BAC, EAC and PA security mechanism, it obtains read-rights for personal data, authentication data and biometric data of an ePassport holder. When BAC mutual authentication and secure messaging succeed, EIS executes EAC-CA by using an EAC chip authentication public key read in BAC to verify the genuine TOE. Then, it executes PA in order to verify an EAC chip authentication public key. When EAC-CA is succeeded, BAC secure messaging is ended and EAC secure messaging with an EAC session key is started, and EAC-TA that the TOE authenticates an inspection system is executed. When EAC-TA is succeeded, EIS obtains read-rights for biometric data of an ePassport holder. Therefore, EIS is provided biometric data of an ePassport holder from the TOE.

An inspection system can implement an AA security mechanism other than security mechanisms like PA, BAC, EAC etc. When an inspection system provides an AA security mechanism, it can verify authenticity of the TOE through an AA security mechanism.

A. IC Chip

An IC chip, which is an underlying platform of the TOE, provides a random number generation and a cryptographic operation to support security functions of the TOE. It also detects a TOE malfunction outside normal operating conditions and provides functions of physical protection to protect the TOE from physical attacks using a probing and a reverse engineering analysis.

Application Note: S3CC9LC of Samsung Electronics -an IC chip the TOE is loaded- is the certified product of CCRA EAL5+, and it supports cryptographic functions as RNG(random number generator) and hardware DES/TDES and provides RSA cryptographic library(version 3.7s) and ECC cryptographic library(version 2.4s). Also, An IC chip provides a function that can protect the TOE physically.

A. MRZ Entropy

A BAC authentication key seed takes MRZ entropy to ensure security of BAC authentication key.

Application Note: In order to resistant to a moderate-level threat agent, an entropy for passport number, date of birth, expiration date or validity, and check digit used as a BAC authentication key seed among MRZ shall be at least 56bit to the current technological level.

4.2. Scope to Counter Threats

An ePassport is used by possession of individuals without physically controlled devices, therefore both logical and physical threats is occurred.

A threat agent is an external entity that attempts illegal access to assets protected by the TOE, by using a physical or logical method outside the TOE.

In this certification report, an IC chip provides a function of physical protection in order to protect the TOE according to A. IC Chip. Therefore, a physical threat of an IC chip itself by a high level threat agent is not considered. Nevertheless, strong possibility of high level attack through logical method can be ignored.

Therefore, a threat agent to the TOE has high level of expertise, resource and motivation, and there is a high possibility to find a vulnerability which attackers are likely to exploit.

5. TOE Information

An ePassport is embedded with a contactless IC chip that identity of a passport applicant and other data are stored according to the international standard that ICAO and ISO specified. A MRTD Chip is a contactless IC chip used in an ePassport. A MRTD Chip contains COS and MRTD Chip Application that support IT technology and information security technology for electronic storage and processing of ePassport identity data

SK COS was developed based on JAVA Card Specification (Java Card 2.2.2(Java Card 2.2.2 Virtual Machine Specification, Java Card 2.2.2 Runtime Environment Specification, Java Card 2.2.2 Application Programming Interfaces), Global Platform Specification (GlobalPlatform Card Specification 2.1.1) and Visa Global Platform Specification (Visa GlobalPlatform 2.1.1 Card Implementation Requirements - Configuration 2).

A MRTD application satisfies ICAO ePassport Specification (ICAO Machine Readable Travel Documents, Doc 9303 Part 1 Volume 2) and BSI EAC Specification (BSI, Advanced Security Mechanisms Machine Readable Travel Documents-Extended Access Control V1.11(2008.2))

The TOE is loaded on S3CC9LC IC chip of Samsung Electronics and following [Figure2] shows the physical scope of the TOE.

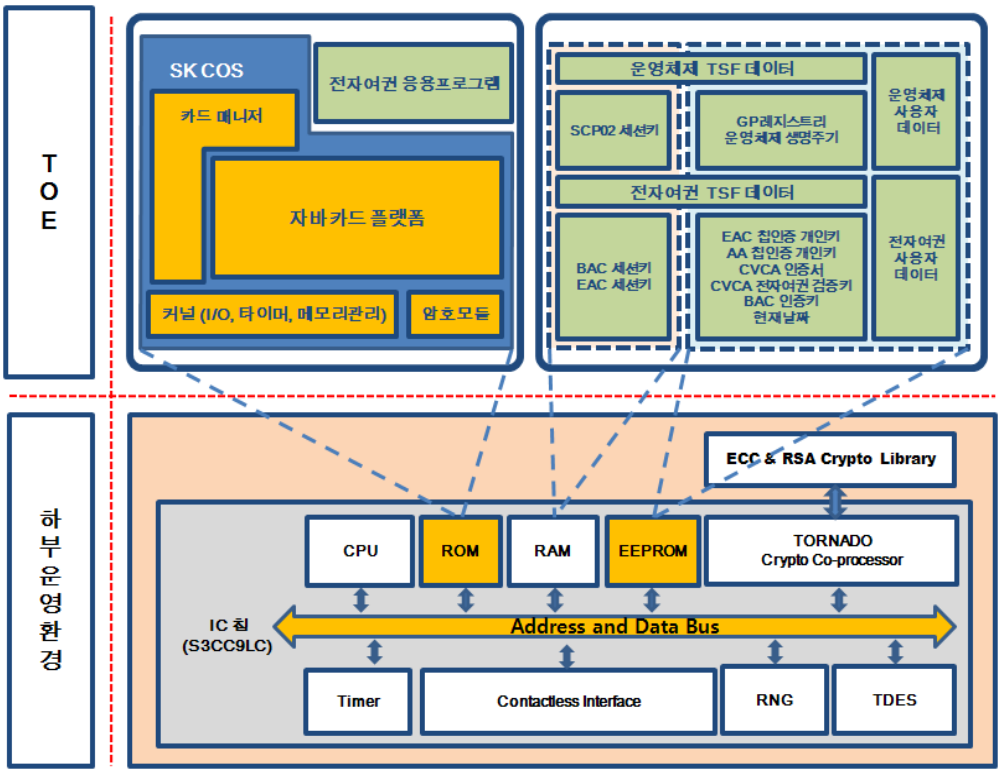

Figure 2 Physical Scope of the TOE

Following [Figure3] shows the logical scope of the TOE.

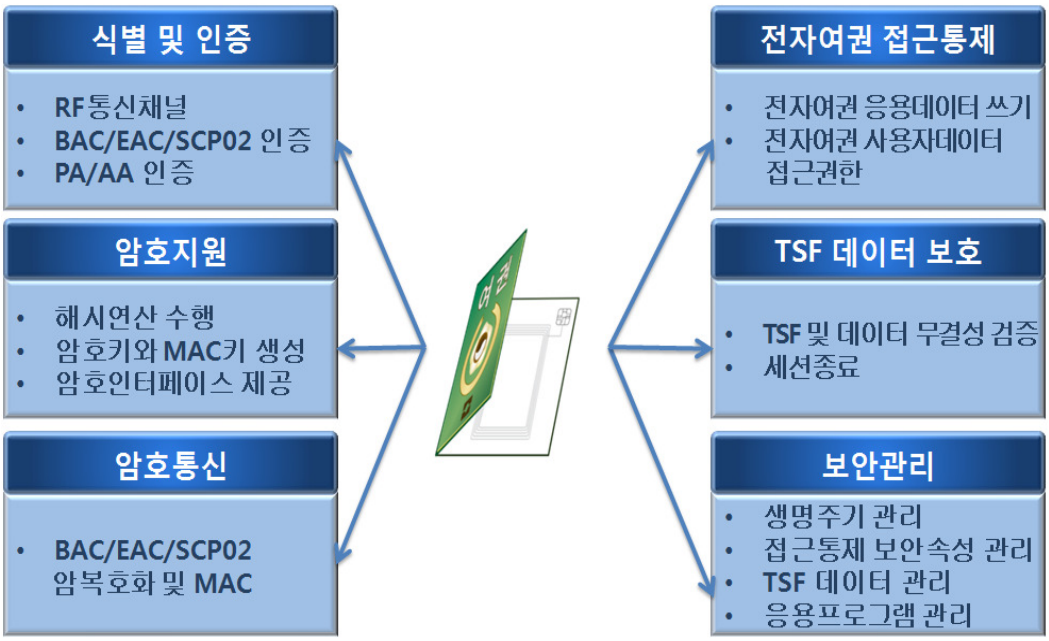

Figure 3 Logical Scope of the TOE

A MRTD application provides following functions.

• Cryptographic support

- Operating hash operation: Operate SHA-1, SHA-224, SHA-256 hash operations

- Providing cryptographic interface: Provide interface for TDES, RSA, ECC and random number generator supported in an IC chip to a MRTD application

- Generating cryptographic key and MAC key: Generate a cryptographic key and a MAC key for BAC authentication, EAC authentication and SCP02 authentication.

• Identification and Authentication

- RF Communication Channel: Generate communication channel based on ISO/IEC 14443-4 that can be performed instead of user before identifying user

- BAC Authentication: Authenticate user to make sure that only the inspection system authenticated in use phase through BAC mutual authentication can access to personal data of ePassport applicant

- EAC Authentication: Authenticate user to make sure that only the inspection system authenticated in use phase through EAC mutual authentication can access to biometric data of ePassport applicant

- SCP02 Authentication: Authenticate personalization agent to make sure that only the personalization agent authenticated in issuance phase and use phase can access to ePassport application data and OS application data

- PA Authentication: Inspection system which has DS certificate verifies digital signature signed in SOD and verifies hash value of ePassport user data to confirm that ePassport identity data stored in an ePassport have not been forged and corrupted after it issued.

- AA Authentication: The TOE generates a digital signature on random number that inspection system delivered with an AA personal key and inspection system checks if the TOE was not forged by verifying a digital signature with an AA public key.

• **ePassport Access Control**

- Access Control for ePassport application data:

Only the personalization agents that gained SCP02 authentication have write-right to ePassport application data

※ ePassport Application Data: Consists of ePassport user data and ePassport TSF data

Only the Inspection Systems that gained BAC and EAC authorization have access right to ePassport user data after issuing.

• **Cryptographic Communication**

- Cryptographic Communication to protect confidentiality and integrity

The TOE protects confidentiality and integrity of communication by using a cryptographic key and a MAC key after SCP02 authentication and BAC and EAC authentication.

• **Security Management**

- OS Life Cycle Management:

The TOE changes OS life cycle to operational use phase when issuance of an ePassport is finished.

The TOE changes OS life cycle to discard phase when it failed in SCP02 mutual authentication 255 times.

- Access Control Security Attribute Management:

The TOE enforces ePassport access control policy to initialize security attribute of a subject in detecting changes of TSF data being transmitted

- TSF Data Management: Information management of certificate verification, SSC initialization, GP registry, BAC authentication key, SCP02 authentication key management

- Application Management:

Deleting MRTD application is not allowed

Loading other applications is not allowed

• **TSF Protection**

- Self Test :

The TOE verifies confidentiality for TSF data and TSF

The TOE ends a session and deletes a session key when it failed in verifying confidentiality

6. Guidance

The TOE provides the following guidance documents.

• SK e-Pass *V*1.0 Issuance Guideline V1.1

• SK e-Pass *V*1.0 Operating Manual V1.1

7. TOE Test

7.1. Developer's Test

[Test method]

The developer derived test cases regarding the security functions of the product, which are described in the tests. Each test case includes the following information:

- Test no. and conductor: Identifier of each test case and its conductor

- Test purpose: Includes the security functions and modules to be tested

- Test configuration: Details about the test configuration

- Test procedure detail: Detailed procedures for testing each security function

- Expected result: Result expected from testing

- Actual result: Result obtained by performing testing

- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator has assessed the appropriateness of the developer's test configuration, test procedures, analysis of coverage, and detail of testing and verified that the test and its results had been suitable for the evaluation configuration.

[Test configuration]

The test configuration described in the tests includes details such as network configuration, evaluated product, server, test PC, or test tools required for each test case.

[Analysis of coverage / testing: basic design]

Details are given in the ATE_COV and ATE_DPT evaluation results.

[Test result]

Tests describe expected and actual test results of each test case. The actual result can be checked on the screen of the product and also by audit log.

7.2. Evaluator''s Test

The evaluator has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results.

The evaluator has confirmed this consistency by performing additional tests based on the developer's test.

The evaluator has also confirmed that, after performing vulnerability test, no vulnerability had been exploitable in the evaluation configuration.

The evaluator's test result has ensured that the product had normally operated as described in the design documents.

8. Evaluation Configuration

The evaluator configured the test environment as consistent with that specified in the ST as the following figure:

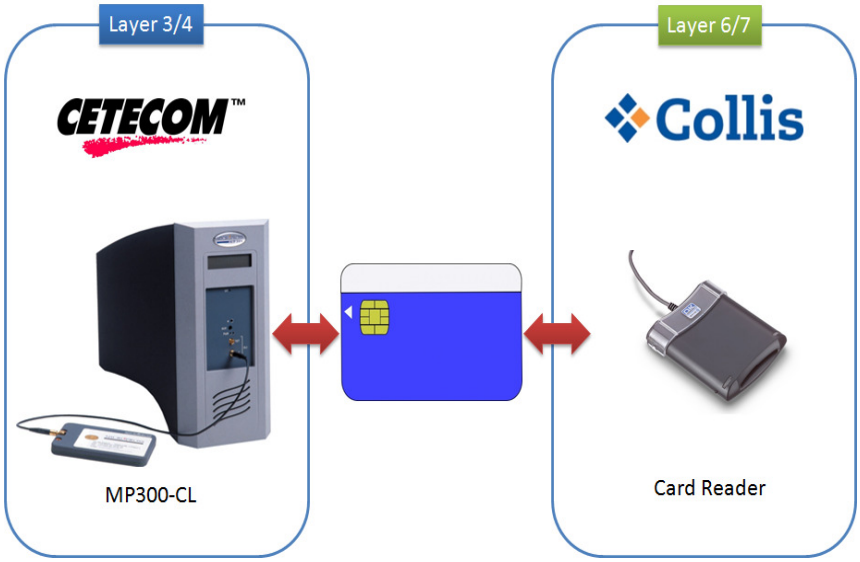

Figure 4 TOE TEST Environment

9. Evaluation Configuration

The evaluation is performed with reference to the CC and CEM. The evaluation decided the TOE conforms to the CC Part 2 and satisfies the EAL4+ requirements Part 3. refer to the ETR for more details.

•ST Evaluation (ASE)

The ST introduction correctly identifies the ST and the TOE, and describes the TOE in three steps of abstraction level (TOE reference, TOE introduction, TOE description), and these three steps of descriptions are consistent with each other. Therefore the verdict of ASE_INT.1 is the Pass.

The Conformance Claim properly describes the conformance claim for the Common Criteria the ST follows. Therefore the verdict of ASE_CCL.1 is the Pass.

The definition of security problem accurately defines security problems that should be included in the TOE and the TOE operational environment. Therefore the verdict of ASE_SPD.1 is the Pass.

The security objectives properly and completely cover the definition of security problems, and define security problems by clearly classifying them of the TOE and the TOE operational environmental. Therefore the verdict of ASE_OBJ.2 is the Pass.

The extended component does not exist and ASE_ECD.1-1 ~ ASE_ECD.1-13 work units evaluation activities are not applicable. Therefore the verdict of ASE_ECD.1 is the Pass.

The security requirements are clear, not ambiguous, and well defined. Therefore, the verdict of ASE_REQ.2 is the Pass.

The TOE summary specification defines the security functions and assurance measures accurately and consistently, and satisfies all described security functional requirements. Therefore the verdict of ASE_TSS.1 is the Pass.

Therefore, ST is appropriate and internally consistent, and suitable to be used as basic material for the TOE evaluation.

•Development Evaluation

The security architecture document is structured to ensure that TSF cannot be compromised or bypassed, and appropriately describes that the TSF which provides the security domain separates these domains from each other. Therefore, the verdict of ADV_ARC.1 is the Pass.

The functional specification specifies the objective, way of using, input parameter, operation, and error message to the TSFI(SFR-enforcing, SFR-supporting, and SFR-non-interfering) at equal detail level, and accurately and completely describes the TSFI in semi-standardized way. Therefore, the verdict of ADV_FSP.4 is the Pass.

The implementation representation is adequate to be used for other evaluators' analysis, and is sufficient to understand the detailed internal workings. Therefore, the verdict of ADV_IMP.2 is the Pass.

The TOE design description provides environment and overall TSF description to describe TSF, provides sufficient TOE description with respect to subsystem to determine the TSF boundary, and provides description about the TSF internals with respect to module. Also, it also provides detailed description of the SFR-enforcing module and sufficient information about the SFR-supporting, and SFR-non-interfering modules to determine that the SFRs are completely and accurately implemented. Hence the TOE design provides the description about the implementation representation. Therefore, the verdict of ADV_TDS.3 is the Pass.

Therefore, the security architecture document (the TSF architecture attribute which describes how to the TSF security enforcement is not compromised or bypassed), functional specification (TSF interface description), TOE design description (architecture description about how the TSF behaves to execute the functions related to the claimed SFR), and implementation representation (description of source code level), which are included in the development documentation, are adequate to give understanding about how the TSF satisfies the SFRs, and how these SFRs implementation are not damaged or bypassed.

•Guidance Documents Evaluation

The personalization document and guidance document describe the security functionality and interface provided by the TSF by each user role, provide the guidance and guideline to use the TOE securely, address secure procedures for all operation modes, and make sure the unsecure state of the TOE easily detected and prevented, and they are not misleading or unreasonable. Therefore, the verdict of AGD_OPE.1 is the Pass.

The TOE includes installation procedure of ePassport applet in the development phase and additional procedure is not necessary, so AGD_OPE.1 is not applicable. Therefore, the verdict of AGD_PRE.1 is the Pass.

Therefore, the issuance guidelines and operating manual give suitable description of how the users can operate the TOE in a secure way.

•Life Cycle Support Evaluation

The configuration management document verifies that the developer clearly identifies the TOE and its associated configuration items, that the ability to modify these items is properly controlled by automated tool, and that as a result, the errors caused by someone's mistake

or negligence in the configuration management system decrease. Therefore, the verdict of ALC_CMC.4 is the Pass.

The configuration management document verifies that the configuration list includes the TOE, the TOE elements, the TOE implementation representation, security flaws, and evaluation deliverables. Therefore, the verdict of ALC_CMS.4 is the Pass.

The distribution procedure document describes all the procedures for the TOE security maintenance when the TOE is distributed to users. Therefore, the verdict of ADO_DEL.1 is the Pass.

The development security document ensures that security control that developer applies to the development environment is suitable to provide the confidentiality and integrity of the TOE design and implementation in order to make sure the secure operation of the TOE is not compromised. Therefore, the verdict of ALC_DVS.1 is the Pass.

The evaluator has confirmed that the developer uses the TOE life-cycle model documented in the life-cycle document. Therefore, the verdict of ALC_LCD.1 is the Pass.

The development tool documentation describes that the developer uses well-defined development tools in TOE development and confirmed that the developer used the well-defined development tools that can draw consistent and predictable results. Therefore, the verdict of ALC_TAT.1 is the Pass.

Therefore, life-cycle associated document is a procedure to determine if the security procedures developer used while implementing and maintaining the TOE are appropriate, and it properly describes the life-cycle model the developer used, configuration management, security measures used in the overall TOE development, tools and distribution activities the developer used throughout TOE life-cycle.

- **Tests Evaluation**

The test document confirms that the developer tested the TSFIs and provided the evidence that can demonstrate the correspondence between the tests items in the test document and the TSFIs in the functional specification. Therefore, the verdict of ATE_COV.2 is the Pass.

The test document confirms that the TSF subsystem and SFR-enforcing module behave and interact as described in the TOE design and security architecture description. Therefore, the verdict of ATE_DPT.2 is the Pass.

The test document confirms that the developer correctly performs and documents the test items described in the test document. Therefore, the verdict of ATE_FUN.1 is the Pass.

The evaluator performed independent test for subsets of the TSF to verify that the TOE behaves as specified, and he/she gained confidence for the test the developer performed through the complete test. Therefore, the verdict of ATE_IND.2 is the Pass.

Therefore, the test document confirmed that the TSF behaves as specified in a design documentation and satisfies the TOE security functional requirements specified in the ST.

- **Vulnerability Assessment Evaluation**

The evaluator confirmed that potential vulnerabilities cannot be misused by attackers with moderate attack potential in the operational environment. Therefore, the verdict of AVA_VAN.4 is the Pass.

Therefore, the evaluator confirmed that attackers cannot violate the SFRs by misusing the potential vulnerabilities that identified during the development evaluation and anticipated TOE operation or by other methods.

10. Recommendations

The security of the TOE can be ensured only in the evaluated TOE operational environment, so it shall be operated by complying with the following assumptions.

① To use personalization command of SK e-Pass V1.0, authentication of personalization agent shall be preceded, and an authentication protocol shall comply SCP02 security mechanism defined in Global Platform 2.1.1 standard. An authentication key of personalization agent can be installed through arrangement between a TOE development company and a personalization agent and the key can be updated into a new key in personalization agent while issuing.

② The MRTD application of SK e-Pass V1.0 does not need to be installed separately because it was already generated in TOE development phase and can Select through the Select command after a RF communication session is set.

③ The Public Data file of SK e-Pass V1.0 shall conform a data format defined in ePassport standard of ICAO 9303 and EAC V1.11, and the Private Data file shall conform a data format defined in 5.3.2 Private Data file.

④ To perform Inspection period communication with SK e-Pass V1.0, it is recommended that distance between SK e-Pass V1.0 and Inspection System is less than 5cm and the page of the e-Passport attached with IC chip is opened. If the RF communication is disconnected, retry it by contacting again.

⑤ The BAC security mechanism shall be necessarily performed to inspect SK e-Pass V1.0 and the EAC security mechanism is used to control access right for fingerprints and irises information. It can be changed according to an operational policy of a personalization agent and an operational environment of an inspection system.

⑥ When biometric information of fingerprints and irises are stored in SK e-Pass V1.0, EAC security mechanism (EAC-CA and EAC-TA) shall be necessarily performed to access biometric information DG3 and DG4 file, and access right to biometric information file in

CVCA, DV, and IS certificate is required. (But, ECDH-based Secure Messaging shall be installed through EAC-CA to perform EAC-TA)

⑦ When distance between SK e-Pass V1.0 and Inspection System is more than 5cm during inspection, or RF communication between SK e-Pass V1.0 and Inspection System is disconnected by shutoff of power supply, An inspection shall be retried according to the procedure defined in this inspection guide.

⑧ When errors of SK e-Pass V1.0 Chip and an antenna disconnection are occurred during inspection, a mechanical inspection of SK e-Pass V1.0 can be impossible and identify an ePassport holder's identity according to operational policy of authentication agency.

11. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
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 MRTD chip, the personalization agent generates TSF data and stores it in the secure memory of the MRTD chip. The agent also operates PA-PKI and/ or EAC-PKI.
e-Passport	The unique information which is signed with the generation key the

Digital Signature	personalization agent issued in ePassport digital signature system to check issue and entry of passport processed by digital method.
e-Passport	The passport embedded the contactless IC chip in which identity and other data of the ePassport holder stored according to the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO).
e-Passport User Data	Including the ePassport identity data and the ePassport authentication data
ePassport Identity Data	Including personal data of the ePassport holder and biometric data of the e-Passport holder
Personal Data of the ePassport applicant	Visually identifiable data printed on identity information page of the of ePassport and other identity data stored in the MRTD chip in the LDS structure
Biometric Data of the ePassport Applicant(Sensitive Data)	Fingerprint and/ or iris data of ePassport holder stored in the MRTD chip in the LDS structure
MRTD Application Data	Including user data and TSF data of the MRTD
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, PA and

	EAC, etc.
Inspection	Procedure in which immigration office checks identity of the ePassport holder by inspecting the MRTD chip presented by the ePassport holder, therefore verifying genuine of the MRTD chip
IS : Inspection System	As an information system that implements optical MRZ reading function and the security mechanisms (PA, BAC, EAC and AA, etc.) to support the ePassport inspection, the IS consists with a terminal that establishes the RF communication with the MRTD chip and the system that transmits commands to the MRTD chip through this terminal and processes responses for the commands.
AA (Active Authentication)	The security mechanism with which the MRTD chip demonstrates its genuine to the IS by signing random number transmitted from the IS and the IS verifies genuine of the MRTD chip through verification with the signed values
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 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
BAC Mutual Authentication	The mutual authentication of the MRTD chip and the IS according to the ISO 9798-2 symmetric key-based entity authentication protocol
BIS : BAC Inspection System	The IS implemented with the BAC and the PA security mechanisms
EAC (Extended	The security mechanisms consisted with the EAC-CA for chip authentication and the EAC-TA for the IS authentication in order to

Access Control)	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
EIS : EAC Inspection System	The IS to implement the BAC, the PA and the EAC security mechanisms and the AA as an option
EAC-CA (EAC-Chip Authentication)	The security mechanism to implement the Ephemeral-Static DH key distribution protocol (PKCS#3, ANSI X.42, etc.) 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.
LDS (Logical Data Structure)	Logical data structure defined in the ICAO document in order to store the user data in the MRTD chip
PA (Passive Authentication)	The security mechanism to demonstrate that identity data recorded in the ePassport 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 according to read-right of the ePassport access control policy.

12. References

The CB has used the following documents to produce this certification report.

[1] Common Criteria for Information Technology Security Evaluation (1. Sep. 2009)

[2] Common Methodology for Information Technology Security Evaluation V3.1

[3] Korea evaluation and certification guidelines for IT Security (1. Sep. 2009)

[4] Korea Evaluation and Certification Scheme for IT Security (1. Jan. 2010)

[5] LG CNS XSmart e-Passport V1.0 ST V1.6 (18. June. 2010)

[6] LG CNS XSmart e-Passport V1.0 ETR V1.0 (30. June. 2010)