KECS-CR-09-35

KCOS e-Passport V1.0

Certification Report

Certification No : KECS-ISIS-0118-2008

Sep, 2008

National Intelligence Service IT Security Certification Center

Establishment & Revision History			
Revision Number	Date	Page	Details
00	2008. 9. 24	-	First documentation

This document is the certification report for

KCOS e-Passport V1.0

Certification Committee Members

Jang Young-Hwan(Ministry of Public Administration and Security)

Yun Lee-Joong(National Security Research Institute)

Cha Sung-Duk(Korea University)

Seo Dong-Soo(Sungshin Women's University)

Ha Jae-Chul(Hosoe University)

Lee Hoon-Jae(Dongseo University)

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Information Security Agency

Contents

Summary

This report describes the certification result drawn by the certification body on the results of the EAL4+ evaluation of KCOS e-Passport V1.0 with reference to the Common Criteria for Information Technology Security Evaluation (notified July. 16, 2008, "CC" hereinafter). It describes the evaluation result and its soundness and conformity.

The evaluation of KCOS e-Passport V1.0 has been carried out by Korea Information Security Agency and completed on August.26. 2008. This report grounds on the evaluation technical report (ETR) KISA had submitted. The evaluation has confirmed that the product had satisfied the CC Part 2 and EAL4 of the CC Part 3 which added ADV_IMP.2, ATE_DPT.2 and AVA_VLA.3, therefore the evaluation results was decided to be "suitable".

KCOS e-Passport V1.0 ("TOE" hereinafter) loaded the closed operating system, the e-Passport application and the e-Passport application data with the EAL5+ IC chip of Infineon Technology which was certified by BSI in German.

The external IT entities necessary in the TOE personalization and operation include the personalization agent and the Inspection System. The personalization agent records MRTD application data in TOE and generates and operates the ePassport PKI System necessary in security mechanism operation. The inspection system is divided into BIS, EIS etc according to security mechanisms it supports.

Following shows the operational environments which use the e-Passport in the personalization phase and operational use phase.

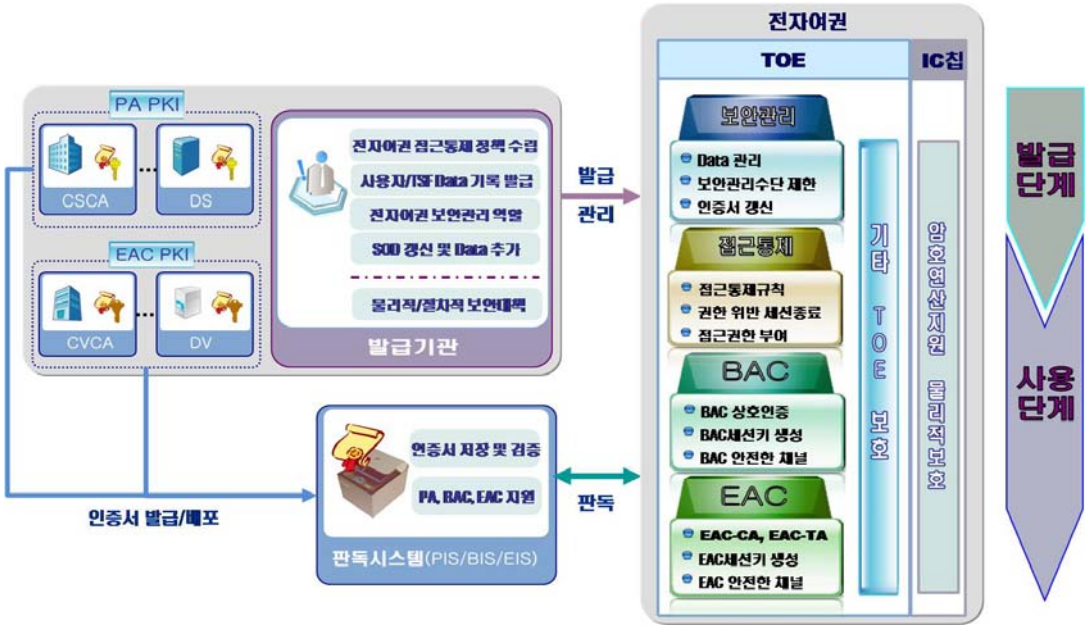

Figure 1TOE Operational Environments

A reception organization collects identity data from the ePassport holder and delivers it to the personalization agent. The personalization agent personalizes the e-Passport embedded the IC chip after recording the e-Passport identity data and the data for executing the e-Passport security mechanism in it. The e-Passport holder is identified his or her identity data by providing the e-Passport to the immigration inspector or the automated Inspection System.

The Inspection System that supports the PA verifies the digital signature by using the certificate which PA-PKI issued to certify the identity data stored in e-Passport.

The Inspection System that supports the EAC obtains the access-rights to the biometric data of the ePassport holder by providing the certificate issued by EAC-PKI to the e-Passport.

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 requirements described in ST. Therefore, the CB certified that observation and evaluation results by evaluator are accurate and reasonable.

Certification validity: Information in this certification report does not guarantee that KCOS e-Passport V1.0 is permitted use or that its quality is assured by the government of Republic of Korea.

Information for Identification

[Table 1] shows information for the TOE.

Scheme	Korea evaluation and certification guidelines for IT security (16, July. 2008) Korea Evaluation and Certification Scheme for IT Security (1. Dec. 2007)
TOE	KCOS e-Passport V1.0
Protection Profile	ePassport Protection Profile V1.0 (KECS-PP-0084-2008, 2008.1)
ST	KCOS e-Passport V1.0 ST V1.6 (2008.8.5)
ETR	KCOS e-Passport V1.0 ETR V1.0 (2008.8.26)
Evaluation results	Suitable - Conformance claim: CC Part 2 and Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V2.3 (16. July. 2008)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V2.3(16. July. 2008)
Sponsor	KCOS
Developer	KCOS
Evaluator	IT Security Evaluation Division, CC Evaluation Lab, Korea Security & Internet Agency Kwan Hyun-Jo, Lee Sung-Jae, Kim In-Sup
Certification body	IT Security Certification Center(ITSCC) of National Intelligence Service

Physical Scope of the TOE includes the MRTD application, the MRTD application data, and the IC chip operating system (COS) to support it. Following shows the physical and logical scope of the TOE.

The IC chip, the underlying platform of the TOE, is SLE66CLX800PE of Infineon, and it is the certified product of EAL5+(Certification Number: BSI-DSZ-CC-0482-2008). The IC chip consists with CPU, Memory(RAM, ROM and EEPROM), MMU(Memory Management Unit) for memory management, MED(Memory Encryption Device) for memory security, Security Logic for IC chip security, Crypto Logic for supporting the cryptographic operation, RNG, CRC calculation Logic, TIMER, and RF interface for wireless communication.

The TOE uses the cryptographic library (RSA 2048 V1.5, ECC V1.1) loaded on the IC chip to be supported by cryptographic operation of the IC chip that required for executing the e-Passport security mechanism.

The MRTD application and COS, which are the components of the TOE, are stored in the ROM of the IC chip, and the MRTD application data is stored in EEPROM.

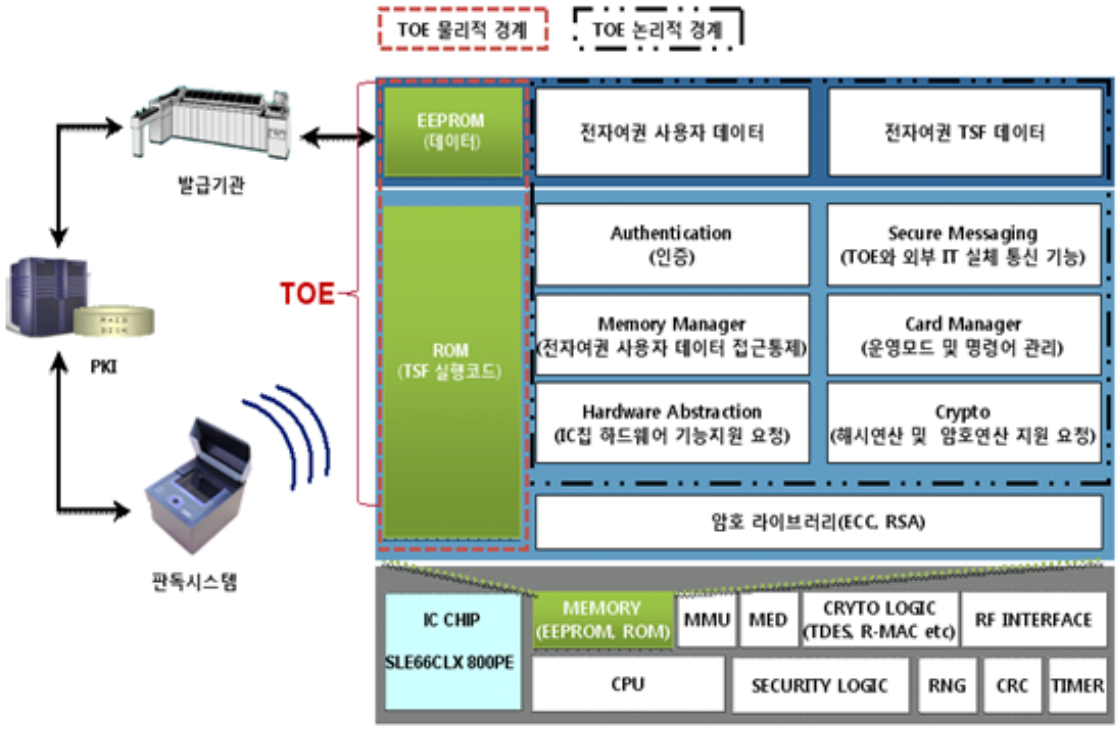

Figure 2Physical/Logical scope of the TOE

Security Policy

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

P. International Compatibility

The Personalization agent shall ensure compatibility between security mechanisms of the e-Passport and security mechanism of the Inspection System for immigration.

Application Note: The TOE shall ensure the International Compatibility by complying the ICAO document and EAC specifications.

P. Security Mechanism Application Procedures

The TOE shall ensure the order of security mechanism application according to the type of the Inspection System so that not to violate the e-Passport access control policies of the Personalization agent.

Application Note: The TOE has the different flow of work according to the types of security mechanism supported by the Inspection System. The basic flow of work complies with Standard e-Passport Inspection Procedure described in 2.1.1 and Advanced e-Passport Procedure in 2.1.2 of EAC specifications.

P. Application Program Loading

The Personalization agent shall approve application program loading after checking that application programs loaded in the MRTD chip does not affect the secure TOE.

Application Note: The loading of the MRTD application can be executed by the organizations that have equal rights to the personalization agent.

P. Personalization Agent

The personalization agent shall issue the ePassport in the secure manner so that to confirm that the issuing subject has not been changed and shall deliver the TOE to the Operational

Use phase after verifying that the data inside MRTD chip are operating normally after issuing. The Personalization agent shall deactivate the writing function before the TOE delivery to the Operational Use phase.

P. e-Passport Access Control

The Personalization agent and TOE shall build the e-Passport access control policies in order to protect the MRTD application data. Also, the TOE shall regulate the roles of user.

Application Note: The TOE shall establish the access control policy according to the ICAO document and EAC specifications as Table1 and Table 2. Also, the TOE shall subdivide the security role of the personalization agent and establish the access control policies to control the personalization management function. For this, the TOE shall use the 7 PAC authentication keys in a different way according to the roles to authenticate the PAC personalization management, allow the right of the relevant security roles according to the type of used PAC authentication keys, and control personalization management function of the personalization agent according to the allowed detailed rights. Table 3 is the PAC authentication keys.

<Table1: Passport Access Control Policies in Use-Phase>

		List of Objects	Objects									
			Personal data of the ePassport holder		Biometric data of the ePassport holder		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

<Table2: Passport Access Control Policies in Personalization Phase>

		List of Objects	Objects									
			Personal data of the ePassport holder		Biometric data of the ePassport holder		e-Passport Authentication Data		EF.CVCA		EF.COM	
List of Subjects		Security Attributes	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights
Subjects	Pesonalization Agent	Pesonalization Authorization	allow	allow	allow	allow	allow	allow	allow	allow	allow	allow

	List of Objects	Objects (e-Passport TSF data)				
		EAC chip Authentication Private Key	CVCA Certificate and Digital Signature Verification Key Current Date	BAC Authentication Key	AA Private Key	PAC Authentication Key

List of Subjects		Security Attributes	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights
Subjects	Pesonalization Agent	Pesonalization Authorization	deny	allow	deny	allow	deny	allow	deny	allow	deny	allow

<Table3: PAC Authentication Key>

Key	Details
K1	Personalization authentication key in the PAC mutual authentication
K2	TOE authentication key in the PAC mutual authentication
K3	PAC-UnBlock key for obtaining UnBlock right
K4	PAC-Keyupdata key for obtaining PAC authentication key update right
K5	PAC-LifeCycle key for obtaining operation mode modification right
K6	PAC-Patch key for obtaining executable code and data patch right
K7	CSN and ticket value cryptographic key for PAC mutual authentication

P. PKI

The Issuing State of the e-Passport shall execute certification practice to securely generate · manage a digital signature key and to generate · issue · operate · destroy certificates according to the CPS by executing the PA-PKI and EAC-PKI according to the e-Passport PKI System. Also, The Issuing State of the e-Passport shall update certificates according to the policies to manage valid date of certificates, therefore securely deliver them to the Verifying State and Inspection System. When the EAC-TA provides the TOE with CVCA link certificate, DV certificate and IS certificate after the Inspection System obtaining information from EF.CVCA stored in the TOE, the TOE shall update certificate by verifying validity of the certificates provided from the Inspection System.

P. Range of RF Communication

The RF communication distance between the MRTD chip and Inspection System shall be less than 5cm and the RF communication channel shall not be established if the page of the e-Passport attached with IC chip is not opened.

Assumptions and Scope

Assumptions

A. Certificate Verification

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

Application Note: The process of certificate distribution follows the ICAO PKD or the diplomatic channel.

A. Inspection System

The Inspection System shall execute security mechanisms of the PA, the BAC and the EAC according to the ICAO document and EAC specifications on the basis of the verifying policy of the ePassport for the ePassport holder. Also, after session ends, the BIS and the EIS shall securely destroy all information used in communication and the TOE, such as the BAC session key, the EAC session key and session information, etc.

Application Note: The TOE denies the request to access EF.SOD by the Inspection System that failed the BAC mutual authentication.

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

comparing a hash value for the personal and authentication data of the ePassport holder, it verifies the forgery and corruption for the personal and authentication data of the ePassport holder.

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

A. IC Chip

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

Application Note: The TDES and the Retail Mac for supporting the TOE security functions are provided by the Crypto-coprocessor of the IC chip, RSA and ECC cryptographic operation are provided by the cryptographic library of the IC chip, and the random number is provided by RNG of IC chip. CRC operation is provided by the CRC of the IC chip, and the hash operation is executed by TOE itself. The IC chip that the TOE is loaded is SLE66CLX800PE of Infineon, and it is certified as EAL5+(ALC_DVS.2, AVA_MSU.3, AVA_VLA.4). It provides security functions against many external attacks.

A. MRZ Entropy

The BAC authentication key seed takes the MRZ entropy to ensure the secure BAC authentication key.

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

Scope to Counter Threats

The ePassport is used by possession of individuals without physically controlled devices, therefore both logical and physical threats is occurred. The threat agent is an external entity that attempts illegal access to assets protected by the TOE, by using the physical or logical method outside the TOE. In this protection profile, the IC chip provides functions of physical protection in order to protect the TOE according to the A. IC Chip. Therefore, the physical threat of the IC chip itself by the high-level threat agent is not considered.

Therefore, the threat agent to the TOE has the moderate level of expertise, resources and motivation.

TOE Information

The logical scope of the TOE for secure assets of the TOE includes all the security functions required by e-Passport Protection Profile, such as the e-Passport security mechanism, access control and security management, and other TOE security. But the TOE is provided with the cryptographic operation necessary to the security mechanism by IC chip and IC chip cryptographic library based on the Application Note of the e-Passport Protection Profile, and also provided the SPA/DPA response mechanism that responses to the information leakage during the cryptographic operation. And the TOE provides the PAC(Personalization Access Control) security mechanism to certify the personalization agent and the AA security mechanism to verify the authenticity of the TOE.

In the access control function, the access to write ePassport user data and the TSF is allowed to the personalization agent in the phases of the personalization, and adding the data to the SOD updating and the e-Passport user data area which was not used is allowed in the operation phase.

The access to read the personal data of the ePassport applicant is allowed to the Inspection System that supports the BAC and the PA security mechanisms. Also the access to read the biometric data of the ePassport applicant is allowed to the Inspection System that supports the BAC, the PA and the EAC security mechanisms.

The security management function provides the personalization agent with the means to securely manage the e-Passport user data and e-Passport TSF data, and makes the TSF executes itself.

The other TOE security functions execute self-testing under self-testing conditions and to preserve a secure state under abnormal operation conditions detected by IC chip or upon occurrence of conditions for self-testing failure. And they ensure the separation of area and TSP non-bypassability to protect against the interruption and violation from the untrusted subject.

The e-Passport security mechanism that the TOE implemented is specified in the ICAO document and EAC specifications in detail, so the description about it is omitted and the PAC security mechanism that the TOE itself implemented for certification of the personalization agent is described.

[PAC Security Mechanism]

The PAC security mechanism is the multiple authentication mechanism that implemented to certify the personalization agent and subdivide the security role of the personalization agent for decentralizing the personalization right. The PAC security mechanism is divided into the PAC mutual authentication, PAC session key generation and PAC personalization management authentication.

The PAC mutual authentication is the function for the mutual authentication between the personalization agent and the TOE in the personalization phase, and is the implemented TDES-based entity certification protocol which modified the BAC security mechanism.

PAC session key generation is the function that generates the PAC session key(PAC session cryptographic key and PAC session MAC key) to be used for establishing the PAC secure messaging between the personalization agent and the TOE, and it is implemented by using the TDES-based key distribution protocol. This protocol is implemented by modifying the standard symmetric key-based key distribution protocol documents. The PAC session cryptographic key is generated by using the value delivered when the TOE certifies the personalization agent during the PAC mutual authentication. And the PAC session MAC is generated by using the value delivered when the personalization agent certifies the TOE during the PAC mutual authentication.

For the PAC personalization management authentication, when the personalization agent requests the TOE security function management and TSF data management, the TSF performs the PAC personalization management certification after checking the operation mode of the TOE. The right to perform the each security role is assigned to the personalization agent according to the PAC authentication key used for the PAC

personalization management authentication. The security roles includes recording of a-Passport application data, the PAC authentication key update, modification of operation mode, Unblock, executable code, and data patch etc.

In addition, in case of a series of three failures of the PAC mutual authentication and the PAC personalization management authentication, the operation mode state is changed to the Block. The session is terminated when the PAC secure messaging is failed. But, in case of a series of three failures of the authentication in a state of the Block operation mode, the operation mode is changed to the Discard and the e-Passport is discarded.

[Personalization Management Function for the Personalization Agent]

For the personalization management, the following management measures are provided to the personalization agent.

1) Function for initialization of personalization-related EEPROM area: This function provides the initialization measures of the EEPROM area for the preparation of the e-Passport personalization such as initialization of the file table, generation of the LDS file system, and re-initialization of the file table for the TOE re-personalization etc.

2) Function for modification of operation mode: When the personalization is completed, this function provides measures to modify the SecondAuth into the StartIssue state, and measures to modify the StartIssue state into the Unissued/Issued/Discard.

3) Function for executable code and data patch: When the executable code stored in the ROM needs to be modified because of the defect of the TSF executable code etc, this function provides management measures to store the TSF executable code for patch that the personalization agent reflected the modification into the EEPROM of the TOE. Also, when the IC chip manufacturer modifies the RF communication-related set point, this is used as a measure to update for the TOE.

4) Function for Unblock : If the operation mode is changed to the Block because of a series of three failures of the PAC mutual authentication, this function provides the personalization agent with the measures that revoke the Block operation mode to restore the former operation mode.

5) Function for PAC update: This function provides the personalization agent with the measures to modify the initial value of the PAC authentication key that the IC chip manufacturer delivered in the phase 1(Development) of the TOE life cycle.

6) BAC authentication key generation and storage: This provides the personalization agent with the measure of the BAC authentication key generation, and the TOE generates the BAC authentication appropriately according to the key ICAO document and then records and stores it in the EEPROM.

7) Deactivating the writing function: This provides measures that can deactivate the writing function by modifying the operation mode into the Issued before the personalization procedures are completed and delivered to the e-Passport applicant.

8) Writing TSF data and e-Passport user data: This provides measures that can record the TSF data in the TSF data area, and the e-Passport user data in the e-Passport user data area in the form of the LDS.

[TOE Self-Security Management]

The TOE initializes the security attribute of the subject when the transmitted TSF data modification is detected to maintain the TOE internal operation state, and initializes the SSC to modify the BAC secure messaging into the EAC secure messaging when the EAC session key generation is successful.

The TOE divides the TSF into the logical units, and it consists of Authentication Subsystem, Card Manager Subsystem, Secure Messaging Subsystem, Memory Manager Subsystem, Crypto Subsystem and Hardware Subsystem etc.

Authentication	BAC mutual authentication and BAC session key generation PAC mutual authentication and PAC session key generation EAC-CA and EAC session key generation EAC-TA AA authenticity verification CVCA certificate verification and update PAC authentication key update BAC authentication key generation and record e-Passport security mechanism-related key information record	SF.MUT_AUT SF.CHIP_AUTH SF.TERMINAL_AUTH SF.ACTIVE_AUTH SF.ACC_CONTROL
Card Manager (management of operation mode and commands)	Request for APDU transmission and reception handling TSF executable code patch checking Modification of operation mode Initialization of file table and security attribute Initialization of TOE personalization Initialization of TOE re-personalization TOE Block operation mode Unblock	SF.ACC_CONTROL SF.RELIABILITY
Crypto (Request for support for hash operation and cryptographic operation)	Hash operation(SHA-1, SHA-224, SHA-245) IC chip function invocation and response handling for DES, Retail MAC, random number and CRC calculation	all security functions
Hardware Abstraction (Request for IC chip function)	IC chip function invocation and response handling for detecting abnormal behavior Management of residual information	SF.RELIABLITY
Memory Manager (Access control to e-Passport user data)	Initialization of LDS file system Access control to writing and reading e-Passport user data	SF.ACC_CONTROL
Secure Messaging (Security communication between TOE and external IT entity)	PAC secure messaging BAC secure messaging EAC secure messaging	SF.SEC_MESSAGE

<TOE Subsystem>

Following shows the subdivision and summarization of the IT TSF the TOE provides.

SF.MUT_AUTH	PAC : PAC mutual authentication(TOE« personalization agent), PAC session key generation, PAC personalization management authentication(PAC-KeyUpdate authentication/PAC-LifeCycle authentication/PAC-Patch authentication/PAC-Unblock authentication) and providing personalization right to the personalization agent, authentication failure handling BAC : BAC mutual authentication(TOE« Inspection System) and providing BAC right, authentication failure handling, BAC session key generation
SF.CHIP_AUTH	EAC-CA : Support the Inspection System to authenticate the TOE by implementing the EC-D-H based key distribution protocol, EAC session key generation and SSC initialization
SF.TERMINAL_AUTH	EAC_TA : The TOE authenticates the Inspection System by implementing the ECDSA based authentication protocol, Verification of validity of the certificates the Inspection System provides, and updating CVCA certificate and current date
SF.SEC_MESSAGE	Secure Messaging using PAC session key after PAC mutual authentication Secure Messaging using BAC session key after BAC mutual authentication Secure Messaging using EAC session key after EAC mutual authentication Initialize the security attribute in case of detection of the transmitted TSF data modification
SF.ACTIVE_AUTH	AA execution : After deliver AA digital signature verification key to the Inspection System, generate and deliver the RSA digital signature with AA digital signature generation key based on random number the Inspection System provided
SF.ACC_CONTROL	TOE initialization: Starting of the TOE initialization functions such as TOE personalization initialization, re-personalization initialization, initialization of e-Passport user data EEPROM storage area in the form of LDS, initialization of temporary memory area for the TSF data allocation etc. Functions for personalization agent access control and personalization agent management: definition of the operation application rule for the object of the personalization agent in the personalization phase, and execution of the management function(access control to the personalization functions such as e-Passport application data record, key update, life cycle modification, release locking, code, and data patch etc) Inspection System access control: Definition and execution of the operation application rule for the object of the Inspection System in the operational phase.

SF.RELIABILITY	Management of residual information: Physical deletion of the authentication key and session key in the temporary memory. Response measures for vulnerability: Sensor that can detect the scope of the TOE normal behavior before executing cryptographic operation, and the Shield function that response to the physical attack etc, for the IC chip normal behavior test and the notice of the IC chip abnormal detection, the TSF initializes the RAM value and modifies the EEPROM key value into temporary value to change them inoperable. TSF self test : Checking the TSF is patched or not before each TSF execution, and executing the TSF executable code if it is patched, and it is infinite loop if the patch execution is failed. Integrity test : Providing the TSF data integrity verification measure through the CRC verification in every access to the key value stored in EEPROM during the procedures of the authentication function by user request, restoring to the previous state of EEPROM when the data is recorded in the EEPROM to prepare for the occurrence of the Anti-tearing, integrity verification for the TSF executable code stored in the ROM area in the TOE personalization initialization phase, and modifying the TOE operation mode into the Discard when the verification is failed. Separation of security function area: Because other application programs are not loaded in the e-Passport IC chip, and only the TOE is loaded solely, it has single area. And because the COS of the TOE separates the e-Passport user data area and the TSF data area and controls them, there are no interruption and violation.

Guidance

The TOE provides the following guidance documents.

•KCOS e-Passport V1.0 Administrator Guidance V1.5

•KCOS e-Passport User Installation Guidance V1.5

TOE Test

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.

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.

Evaluation Configuration

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

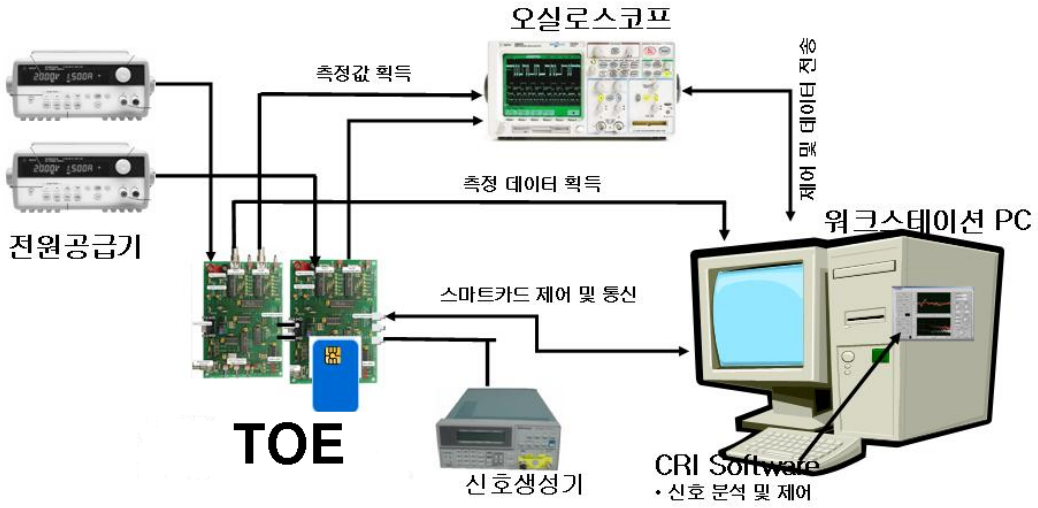

Figure 3TOE Test Environment

Evaluation Result

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 is perfect and consistent with each other, and correctly identifies the ST. Therefore the verdict of ASE_INT.1 is the Pass.

The TOE Identification describes to understand TOE Objectives and TOE functionality, and logical and internally consistent. Also, it is consistent with others of the ST. Therefore the verdict of ASE_DES.1 is the Pass.

The Security Environment defines and provides accurate and consistent security problems derived from the TOE security environment, that is assumptions, threats, and organizational security policies, and it describes completely and consistently. Therefore the verdict of ASE_ENV.1 is the Pass.

The Security objectives counter the identified threats, achieve the identified organizational security policies, and satisfy the described assumptions properly and completely. Therefore the verdict of ASE_OBJ.1 is the Pass.

The IT security requirements are described completely and consistently, and provide an appropriate basis for the development of the TOE to achieve the security objectives. Therefore the verdict of ASE_REQ.1 is the Pass.

The IT security requirements specified separately identify the all TOE security requirements that specified separately without the CC references, and justify the reason of

separated specification, and describe accurately and unambiguously. Therefore the verdict of ASE_SRE.1 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.

The ST substantiates the accepted Protection Profile accurately. Therefore the verdict of ASE_PPC.1 is the Pass.

Therefore, "KCOS e-Passport V1.0 ST V1.6" responses to the threats, describes the security functions that execute the security policies. The security functions are enough to response to the threats and execute the security policies, and the ST is internally consistent. Also, it substantiates the SFRs with security functions.

Configuration Management Evaluation

The configuration management documentation clearly identifies the TOE and its associated configuration items and confirms that the ability to modify these items is properly controlled. Therefore the verdict of ACM_CAP.4 is the Pass.

The CM documentation confirms that the developer performs configuration management at least on the TOE implementation representation and the evaluation evidence required by the assurance components in the ST. Therefore the verdict of ACM_SCP.2 is the Pass.

The CM documentation confirms that the changes to the implementation representation are controlled with the support of automated tools. Therefore the verdict of ACM_AUT.1 is the Pass.

Therefore, the evaluation of configuration management assists the consumer

in identifying the evaluated TOE, ensures that the configuration items are uniquely identified, and ensures the adequacy of the procedures that are used by the developer to control and track changes that are made to the TOE.

Delivery and Operation Evaluation

The delivery documentation describes all procedures used to maintain security and detect modification or substitution of the TOE when distributing the TOE to the user's site. Therefore, the verdict of ADO_DEL.1 is the Pass.

The evaluator has confirmed that the procedures and steps for the secure installation, generation, and start-up of the TOE had been documented and resulted in a secure configuration. Therefore, the verdict of ADO_IGS.1 is the Pass.

Therefore, the delivery and operation documentation is adequate to ensure that the TOE is installed, generated, and started in the same way the developer intended it to be and it is delivered without modification.

Development Evaluation

The functional specification adequately describes all security functions of the TOE and that the functions are sufficient to satisfy the security functional requirements of the ST. It also adequately describes the TSF interfaces. Therefore, the verdict of ADV_FSP.2 is the Pass.

The security policy model clearly and consistently describes the rules and characteristics of the security policies, and describes their correspondences to the security functions in the functional specification. Therefore, the verdict of ADV_SPM.1 is the Pass.

The low-level design describes the TSF in terms of subsystems which are main components, and describes the interface to the subsystems. Also, it correctly realizes the functional specification in terms of subsystems. Therefore, the verdict of ADV_HLD.2 is the Pass.

The high-level design describes the internal operation of the TSF in terms of internal modules and it describes the interrelationships and dependencies between the modules. It is sufficient to satisfy the functional requirements of the ST, and is a correct and effective refinement of the high-level design. Therefore, the verdict of ADV_LLD.1 is the Pass.

The implementation representation is sufficient to satisfy the functional requirements of the ST and is a correct realization of the low-level design. Therefore, the verdict of ADV_IMP.2 is the Pass.

The representation correspondence shows that the developer has correctly and completely implemented the requirements of the ST in the functional specification, high-level design, low-level design, and implementation representation. Therefore, the verdict of ADV_RCR.1 is the Pass.

Therefore, the development documentation is determined adequate to understand how the TSF provides the security functions of the TOE, as it consists of a functional specification (which describes the external interfaces of the TOE), a low-level design (which describes the architecture of the TOE in terms of internal subsystems), a high-level design (which describes the architecture of the TOE in terms of internal modules), an implementation description (a source code level description), and a representation correspondence (which maps representations of the TOE to one another in order to ensure consistency).

Guidance Documents Evaluation

The administrator guidance describes how the TOE is securely administered by the administrator. Therefore, the verdict of AGD_ADM.1 is the Pass.

The TOE does not include general user because all the authenticated general user/ limited user and authenticated administrator are the administrators that execute the security roles defined by FMT_SMR.1, and they execute functions for the management of security function and TSF data through FMT_MOF.1 and FMT_MTD.1 by role. The detailed evaluation activities of AGD_USR.1 are not applicable. Therefore, the verdict of AGD_USR.1 is the Pass.

Therefore, it gives a suitable description of how to administer the TOE.

Life Cycle Support Evaluation

The evaluator has confirmed that the developer's control of the development environment had been suitable to provide the confidentiality and integrity of the TOE design and implementation required for the secure operation of the TOE. Therefore, the verdict of ALC_DVS.1 is the Pass.

The evaluator has confirmed that the developer had used a documented life-cycle model. Therefore, the verdict of ALC_LCD.1 is the Pass.

The evaluator has confirmed that the developer had used well-defined development tools with which one can get consistent and predictable results. Therefore, the verdict of ALC_TAT.1 is the Pass.

Therefore, the life-cycle support provides an adequate description of the security procedures and tools used in the whole development process and the procedures of the development and maintenance of the TOE.

Tests Evaluation

The tests have been sufficient to establish that the TSF had been systematically tested against the functional specification. Therefore, the verdict of ATE_COV.1 is the Pass.

The evaluator has confirmed that the developer had tested the security functions of the TOE against the low-level design and high-level design. Therefore, the verdict of ATE_DPT.2 is the Pass.

The developer's test documents had been sufficient to show the security functions had behaved as specified. Therefore, the verdict of ATE_FUN.1 is the Pass.

The evaluator has determined, by independently testing a subset of the TSF, that the TOE had behaved as specified and gained confidence in the test results by performing all of the developer's tests. Therefore, the verdict of ATE_IND.2 is the Pass.

Therefore, the tests have proved that the TSF had satisfied the TOE security functional requirements specified in the ST and behaved as specified in the functional specification and design documentation.

Vulnerability Assessment Evaluation

The misuse analysis has confirmed that the guidance documentation had not been misleading, unreasonable, and conflicting, that secure procedures for all modes of operation had been addressed, and that the use of the guidance documentation had allowed insecure states of the TOE to be prevented and detected. Therefore, the verdict of AVA_MSU.2 is the Pass.

The evaluator has confirmed that the strength of TOE security function had been claimed for all probabilistic and permutation mechanism in the ST and the developer's SOF analysis had been correct. Therefore, the verdict of ATE_SOF.1 is the Pass.

The vulnerability analysis adequately describes the obvious security vulnerabilities of the TOE and the countermeasures such as the functions implemented or recommended configuration specified in the guidance documentation. The evaluator has confirmed by performing penetration testing based on the evaluator's independent vulnerability analysis that the developer's analysis had been correct. The evaluator has determined by performing vulnerability analysis that there had not been any vulnerabilities exploitable by an attacker possessing a low attack potential in the intended TOE environment. Therefore, the verdict of ATE_VLA.3 is the Pass.

Therefore, based on the developer and evaluator's vulnerability analysis and the evaluator's penetration testing, the evaluator has confirmed that there had been no flaws or vulnerabilities exploitable in the intended environment for the TOE.

Recommendations

The user that installs and operates the TOE shall comply with the followings.

Because the TOE safety can be ensured only in the evaluated TOE operational environment, the user shall comply with the following assumptions to operate the TOE.

The MRZ entropy shall be determined by the personalization policies to satisfy the SOF-High in order to ensure the BAC safety according to the assumptions.

Also, when the TOE solely uses the RSA digital signature operation, the successful attack can be possible in the procedure of the RSA cryptographic operation. But, because the TOE executes the RSA digital signature in the procedure of the AA security mechanism, and combines random values that the Inspection System and the TOE generated in the procedure of message generation targeted the RSA digital signature, the SPA attack to RSA is practically impossible. Therefore, the TOE shall execute the RSA digital signature operation only in the AA security mechanism.

Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security 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 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.
SOD : Security Object Document	The SOD refers to the ePassport identity data and the ePassport authentication data recorded in the Personalization phase by the Personalization agent that is signed by the Personalization agent with the digital signature generation key. The SOD is an object implemented with signed data type of 'RFC 3369 cryptographic message syntax, 2002.8' and

	encoded with DER method.
e-Passport Digital Signature	Unique information which is signed with the generation key the 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).
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 holder	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 holder(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.
Application Protocol Data Unit (APDU)	스마트카드와 단말간의 Application 의 package 화된 데이터를 교환하기 위한 데이터포맷으로 APDU 는 명령 APDU 와 응답 APDU 로 구분됨. 카드와 단말간의 통신 프로토콜에 따른 하위계층의 TPDU 가 존재하며 APDU 는 통신 프로토콜에 맞게 적절한 TPDU 로 전환되어 전달됨 A data format to exchange packaged data of Application between a Smartcard and a terminal. APDU is divided into command APDU and response APDU. There is TPDU of lower layer according to a communication protocol between a card and a terminal. APDU is

	transmitted after transferring to appropriate TPDU which is fit to communication protocol.
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
DFA (Differential Fault Analysis)	암호연산 과정에서 전압, 클럭 등의 강제적인 변형을 통해 오동작을 유발하고 이로부터 암호키를 유추하는 방법 A method to derive a cryptographic key by generating malfunction through compelled modification such as voltage and clock and so on in cryptographic operation.

DPA (Differential Power Analysis)	암호연산 과정에서 소모되는 전력량을 대량으로 수집하여 통계적인 분석을 통해 암호키를 유추하는 방법 A method to derive a cryptographic key through statistical analysis by collecting consumed electric power in large quantities in cryptographic operation.
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
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.
EMA (Electromagnetic Analysis)	암호연산 과정에서 방출되는 전자파를 수집하고 해석하여 암호키를 유추하는 방법 A method to derive a cryptographic key by collecting and interpreting released electromagnetic waves in cryptographic operation.
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.
SCP02(Secure Channel Protocol 02) 상호인증	Global Platform 2.1.1 Card Specification 에서 정의하고 있는 대칭키 기반 실체인증프로토콜 An symmetric Key-based Entity Authentication Protocol defined in Global Platform 2.1.1 Card Specification
SPA (Simple Power Analysis)	암호연산 과정에서 소모되는 전력량을 수집하고 해석하여 암호키를 유추하는 방법 A method to derive a cryptographic key by collecting and interpreting consumed electric power in

cryptographic operation.

Reference

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

[1] Common Criteria for Information Technology Security Evaluation (Ministry of Public Administration and Security Notice No. 2009-52, 1. Jul. 2008)

[2] Common Methodology for Information Technology Security Evaluation V2.3

[3] Korea evaluation and certification guidelines for IT security (16. Jul. 2008)

[4] Korea Evaluation and Certification Scheme for IT Security (NIS, 1. Dec. 2007)

[5] KCOS e-Passport Version 1.0 V1.0 ST V1.6 (5. Aug. 2008)

[6] KCOS e-Passport Version 1.0 V1.0 ETR V 1.0 (26. Aug. 2008)