KECS-CR-09-49

XSmart e-Passport V1.1

LG CNS

Certification Report

Certification No : KECS-ISIS-0253-2010

National Intelligence Service IT Security Certification Center

Establishment & Revision History			
Revision Number	Date	Page	Details
00	2010. 7. 22	-	First documentation

This document is the certification report for

LG CNS XSmart e-Passport V1.1

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 EAL5+ evaluation of LG CNS XSmart e-Passport V1.1 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 June. 25. 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 EAL5 of CC Part 3 which added ADV_IMP.2, therefore the evaluation results was decided to be “suitable”.

The TOE is an open operating system and a MRTD application except underlying IC chip component and it consists in the form of software. The TOE manages MRTD application data, such as MRZ area data of ePassport, personal data of ePassport holder, biometric data of ePassport holder like face and fingerprint, and cryptographic key for biometric data, authentication and secure communication etc, and authenticates a personalization agent and an inspection system to execute access control for ePassport holder data.

The underlying IC chip uses S3CC9LC of Samsung which is certified as CC EAL5+. The IC components that the TOE based on include IC chip hardware, IC chip firmware, and cryptographic operation software library for ECC operation.

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

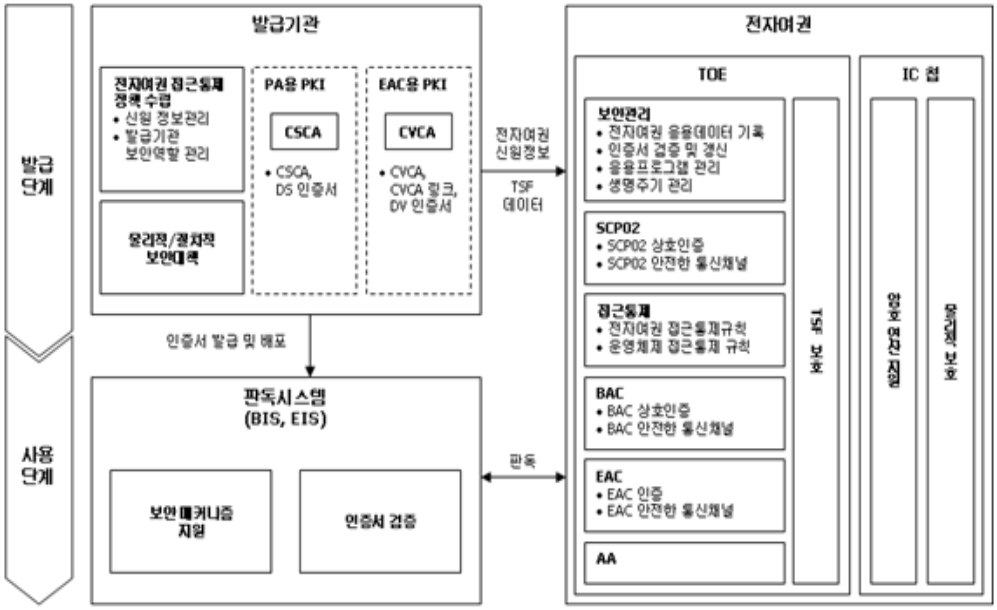

Figure 1 TOE Operation Environment

The CB(Certification Body) has examined the evaluation activities and testing procedures, provided the guidance for 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 the government of Republic of Korea permits use of XSmart e-Passport V1.1.

2. Information for Identification

Scheme	Korea evaluation and certification guidelines for IT security (01. 09. 2009) Korea Evaluation and Certification Scheme for IT Security (01. 01. 2010)
TOE	XSmart ePassport V1.1
Protection Profile	ePassport Protection Profile V2.1
ST	XSmart ePassport V1.1 ST V1.4
ETR	XSmart ePassport V1.1 ETR V1.0 (25.06.2010)
Evaluation results	Suitable - Conformance claim: CC Part 2 and Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V3.1 (01. 09. 2009)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V3.1 (01. 09. 2009)
Sponsor	LG CNS
Developer	LG CNS
Evaluator	Public Security Service Team, Public Security Division, Korea Security & Internet Agency(KISA) Hyun Jinsoo, Kim Ilgon, Han Junghoon
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 mechanisms of an e-Passport and security mechanism of an inspection system for immigration.

Application Note: The TOE shall ensure the International Compatibility by complying 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 an inspection system so that not to violate 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. The 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 EAC specification.

P. Application Program Loading

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

Application Note: The loading of a MRTD application can be executed by the organizations that have equal rights to a personalization agent. Also a MRTD application which installed by being loaded in an ePassport IC chip cannot be deleted in the Operational Use phase.

P. Personalization Agent

An personalization agent shall issue an ePassport in a 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 a MRTD chip are operating normally after issuing. A personalization agent shall deactivate the writing function before the TOE delivery to the Operational Use phase. Also a personalization agent shall establish access control policy for OS management.

Application Note: SCP02 of 'GP specification' shall be used as the security mechanism for the certification of a personalization agent.

P. e-Passport Access Control

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

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

		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	Inspection System	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	deny	allow	deny	allow	deny	allow	deny	allow	deny	allow

P. PKI

The Issuing State of an e-Passport shall execute certification practice to securely generate · manage a digital signature key and to generate · issue · operate · destroy certificate according to the CPS by establishing 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 verification countries and inspection system. When 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 internally update certificates by verifying validity of certificate.

P. Range of RF Communication

RF communication distance between a MRTD chip and an inspection system shall be less than 5cm and the 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 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: An inspection system shall periodically download the CSCA certificate from ICAO-PKD to verify the PA certificate chain of an inspection system.

A. Inspection System

An Inspection System shall execute security mechanisms of PA, BAC and EAC according to the ICAO document and the EAC specification on the basis of the verifying 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 a BAC mutual authentication.

As 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 a BAC session key, it ensures confidentiality and integrity of all transmitted data. The BIS verifies SOD by executing PA after BAC. Then, by calculating and comparing a hash value for the personal and authentication data of ePassport holders, it verifies forgery and corruption for the personal data and authentication data of ePassport holders.

As EIS supports BAC, EAC and PA security mechanisms, it obtains the read-rights for personal, authentication and biometric data of the ePassport holder. When the BAC mutual authentication and secure messaging succeed, EIS executes EAC-CA by using an EAC chip authentication public key read in the BAC to verify the genuine TOE. Then, it executes PA in order to verify a EAC chip authentication public key. When EAC-CA is succeeded, the BAC secure messaging is ended and the 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 the read-rights for biometric data of ePassport holders. Therefore, EIS is provided biometric data of ePassport holders from the TOE.

BIS or EIS can additionally implement an AA security mechanism, and through this, the digital signature that the TOE provides can be authenticated by using an AA digital signature authentication key of EF.DG15 to verify whether the TOE is copied or not.

A. IC Chip

An IC chip -an 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 normal operating conditions and provides functions of the physical protection to protect the TOE from physical attacks using a probing and reverse engineering analysis.

Application Note: To ensure the secure TOE environment, the IC chip shall be SLE66CLX800PE which is a certified product of CCRA EAL5+. The cryptographic operation supported by the IC chip may be provided in the co-processor of the IC chip or cryptographic library loaded in the IC chip.

A. MRZ Entropy

A BAC authentication key seed takes MRZ entropy to ensure a 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 shall be at least 56bit.

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 the physical or logical method outside the TOE.

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

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

5. TOE Information

An ePassport means an ePassport IC chip and an antenna embedded in a passport and cover of passport. An ePassport IC chip includes not only open OS that consists of MRTD application, executable environment, card manager, but also IC chip components such as IC chip hardware, firmware and ECC/RSA cryptographic operation library.

The TOE is defined as open OS loaded in MRTD chip and MRTD application, and IC chip components such as IC chip hardware, firmware and ECC/RSA cryptographic operation library are excluded from the TOE scope.

The TOE is loaded on S3CC9LC IC chip of Samsung and the physical scope is as followed.

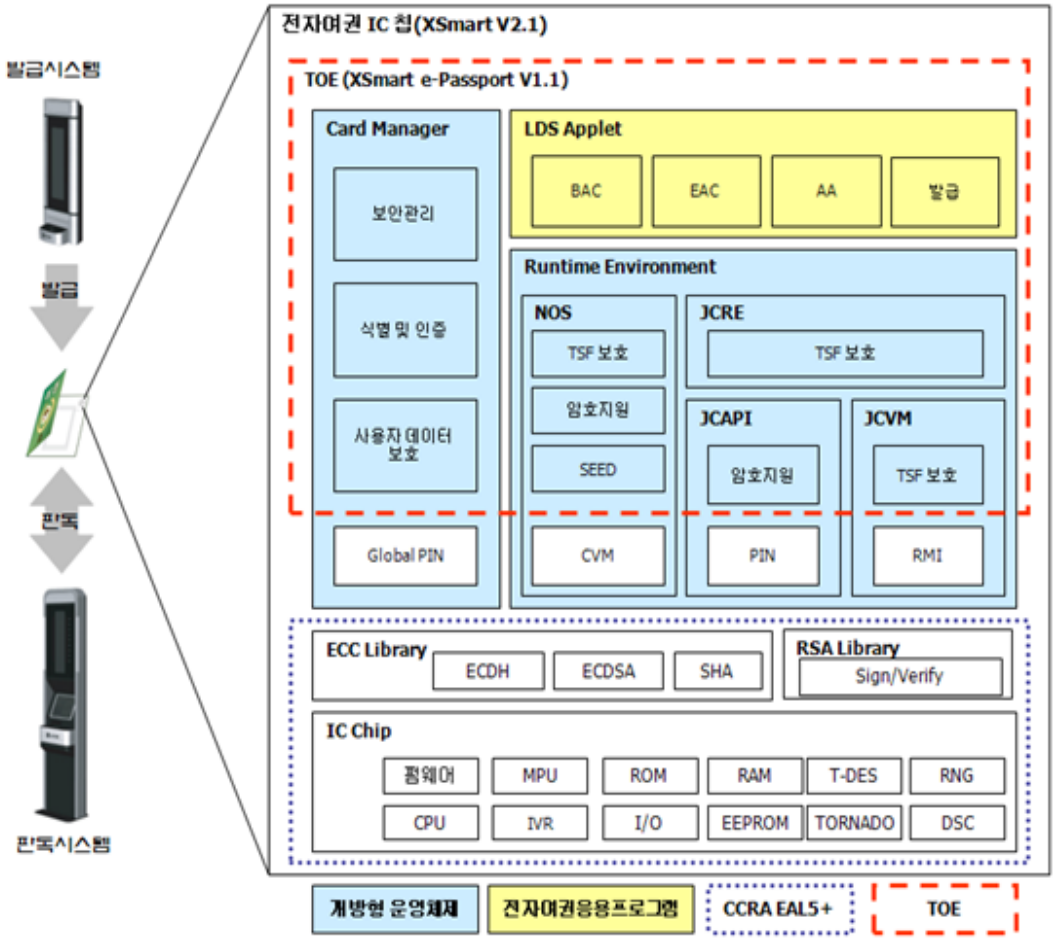

Figure 2 Physical Scope of the TOE

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

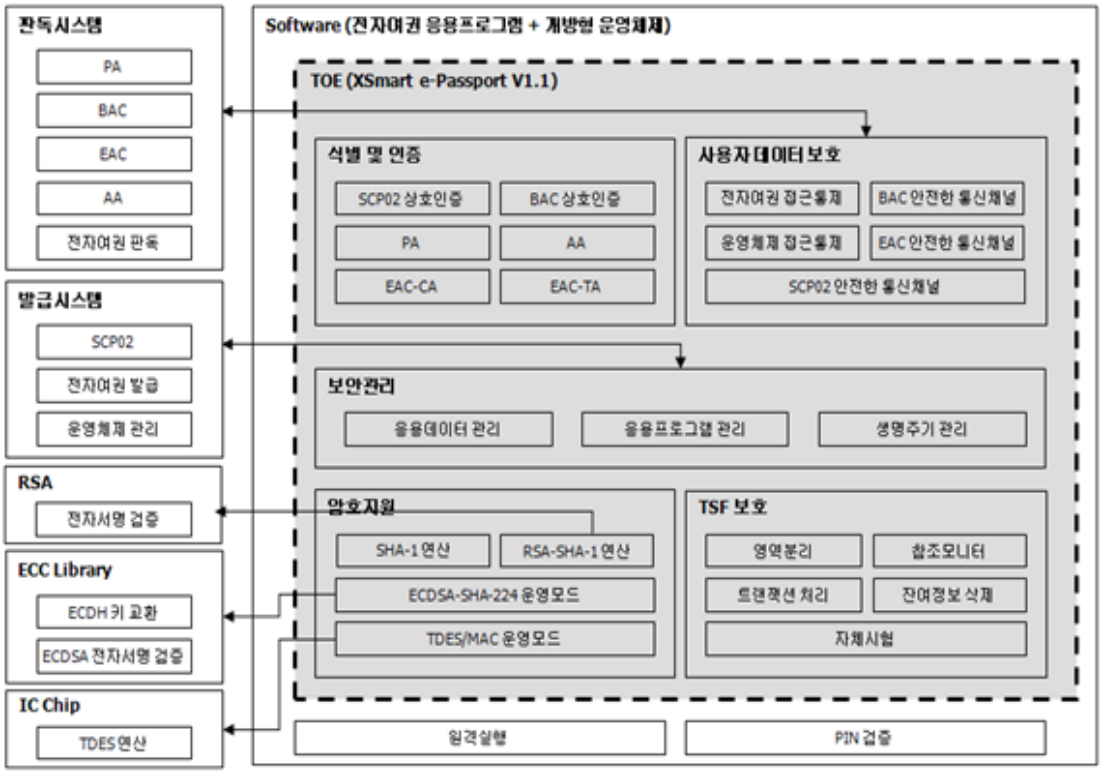

Figure 3 Logical Scope of the TOE

The TOE provides identification and authentication, user data protection, security management, TSF protection, and security function of cryptographic support.

•Identification and Authentication

The TOE provides SCP02 mutual authentication, BAC mutual authentication, EAC-CA, EAC-TA, PA and AA as the methods for identification and authentication.

<SCP02 Mutual Authentication>

SCP02(Secure Channel Protocol 02) is the security mechanism that authenticates a personalization agent that has write-right, add and update for the identity data of ePassport holder and TSF data, and it includes the SCP02 mutual authentication and secure

communication channel. The TOE and the Personalization agent generate SCP02 session key by using personalization agent authentication data and SC(Sequence Counter), and then execute mutual authentication through the method that the TOE and a personalization agent mutually verify the MAC for the mutually transmitted random number. If the SCP02 mutual authentication is failed, a session is ended, and if it is successful, the TOE establishes a secure channel by using the SCP02 session key.

< BAC Mutual Authentication >

The Inspection System that supports BAC uses a BAC authentication key generated from the optically-read MRZ, and the TOE generates the BAC authentication key from the MRZ information of DG1 or uses the stored BAC authentication key. The Inspection System and the TOE encrypt and mutually exchange the generated random number by using the BAC authentication key. The Inspection System and the TOE that support BAC perform the mutual authentication by checking the mutually exchanged random number. When the BAC mutual authentication is failed, a session shall be ended.

< EAC-CA>

An EAC-CA implements Ephemeral-static DH key distribution protocol to provide an EAC session key distribution and an IC chip authentication. The TOE transmits an EAC chip authentication public key to make an inspection system authenticates itself and performs a key distribution protocol by using a temporary public key received from the inspection system. When the EAC-CA procedure is successful, the TOE uses the EAC session key and establishes EAC secure communication channel. Even when EAC-CA is failed, the BAC secure communication channel is maintained and the inspection system can confirm the TOE is illegally copied.

< EAC-TA>

An EAC-TA implements the digital signature-based Challenge-Response authentication protocol so that the TOE authenticates the Inspection System that supports the EAC. To authenticate the inspection system, the TOE uses the IS certificate to verifies the value that the inspection system has digital-signed on a temporary public key used in EAC-CA procedure. When the TOE receives the CVCA link certificate, DV certificate, IS certificate from the Inspection System, it verifies the CVCA link certificate by using CVCA digital signature verification key in protected memory area and confirms the terms of validity of the CVCA link certificate to update the CVCA digital signature verification key and current date within the TOE if necessary. After the TOE verifies and confirms that the IS certificate is adequate, it allows read access to ePassport holder data that encoded ePassport applicant of the Inspection System and transmits through the EAC secure communication channel.

< PA>

To supports a PA security mechanism, the TOE makes the Inspection System detects forgery and corruption of ePassport user data through SOD digital signature verification by providing SOD to BIS and EIS.

< AA>

An AA (Active Authentication) implements the digital signature-based Challenge-Response authentication protocol so that the inspection system authenticates the TOE. When the TOE generates and transmits a digital signature with an AA chip authentication personal key stored in the protected memory area on the transmitted value the inspection system provided, the inspection system authenticates the TOE by verifying it with EF.DG15 AA ship authentication public key obtained from BAC secure communication channel or EAC secure communication channel. The AA is the security mechanism that provides the measure to verify illegal copy of the TOE.

•User Data Protection

The TOE provides access control and secure communication channel to protect user data.

< SCP02 Secure Communication Channel>

The TOE establishes the SCP02 secure communication channel using SCP02 session key generated during the SCP02 mutual authentication procedure to perform a secure communication with the personalization agent that has performed the SCP02 mutual authentication procedure successfully. When the TOE transmits data through the SCP02 secure communication channel, it encrypts the data by using TDES cryptographic algorithm to provide confidentiality, and verifies the MAC by using Retail MAC algorithm to provide integrity.

< BAC Secure Communication Channel>

The TOE confirms the read-access of an inspection system for ePassport applicant personal data through the BAC mutual authentication procedure, and then generates the BAC secure communication channel using the BAC session key that shared through the BAC key distribution to transmit the ePassport applicant personal data securely. When the TOE transmits the data through the BAC secure communication channel, it encrypts the data by using TDES cryptographic algorithm to provide confidentiality, and verifies the MAC by using the Retail MAC algorithm to provide integrity.

< EAC Secure Communication Channel>

The TOE generates the EAC secure communication channel using the EAC session key that shared through the EAC key distribution of the EAC-CA procedure to perform the secure communication with the Inspection System. When the TOE transmits the data through the EAC secure communication channel, it encrypts the data by using TDES cryptographic

algorithm to provide confidentiality, and verifies the MAC by using the Retail MAC algorithm to provide integrity.

< Operating System Access Control>

The TOE provides an access control function to make sure only the personalization agent that succeeded in the SCP02 mutual authentication and obtained management-right performs the application management function that loads, installs, and deletes executable file and application in open OS and write-function for personal data of a personalization agent in the ePassport personalization phase and the use phase. Also the TOE life cycle provides the access control function to make sure all operation is not executed except for the read-right for personal data of a personalization agent in the termination phase.

< ePassport Access Control>

The TOE provides the access control function to make sure only the personalization agent that succeeded in the SCP02 mutual authentication and obtained personalization-right performs write-right for the ePassport user data and TSF data in the personalization phase. Also the TOE provides the access control function for read-right of ePassport user data based on the access control of an inspection system that given by performing the security mechanism in the ePassport use phase.

•Security Management

The TOE limits the measure that manages TSF data such as MRTD application, OS user, security attribute and session key of user data, authentication key and GP registry only to authenticated personalization agent, and defines this as the security role. Also, the TSF itself performs security management functions such as CVCA certificate, update of current date, and initialization of secure communication identification information etc.

•TSF Protection

The TOE provides functions such as reference monitor, domain separation, residual information deletion, transaction processing, and self test to protect the TSF.

<Reference Monitor >

The TOE ensures that the access control function is not bypassed for all APDU command, which is the TOE external interface, and is always called to protect the TSF from interference and violation by untrusted subject.

<Domain Separation >

The TOE provides Java Card Firewall inside simulated JAVA Card machine to separate the domain like other applications etc. that untrusted subjects use, and the domain that MRTD application is executed.

<Residual Information Deletion >

The TOE provides the function that deletes residual information to make sure previous information is not available when it allocates resources to objectives or de-allocates resources from objectives, not only for information temporarily generated in temporary memory area (ex: BAC session key, EAC session key, SCP02 session key and random number etc.) but also for information generated in protected memory area (ex: BAC authentication key etc.)

<Transaction Processing >

The TOE provides the transaction function to make sure it detects failure of the TSF and initiates the TSF service as previous state if shutting off of power supply and forced TSF service termination are occurred while the TOE is working

<Self-Test >

The TOE self-tests to detect and respond to changes of transmitted TSF data, and verify integrity of stored TSF data and executable code. Also, the TOE maintains secure state not to TSF error is occurred when the self-test detects failures or detects and notifies abnormal behavior in IC chip.

. Cryptographic Support

The TOE provides hash operation, and provides random number generation, key exchange operation operating mode, encryption/decryption operation operating mode, MAC and digital signature operation operating mode by using IC chip and cryptographic operation library.

The TOE ensures that someone cannot identify cryptography related information by misusing physical phenomenon (changes of current, voltage, electromagnetism etc.) occurred in execution of cryptographic operation, and provides the measure of integrity verification for cryptographic key.

6. Guidance

The TOE provides the following guidance document.

•XSmart e-Passport V1.1 Operating Manual V1.0

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:

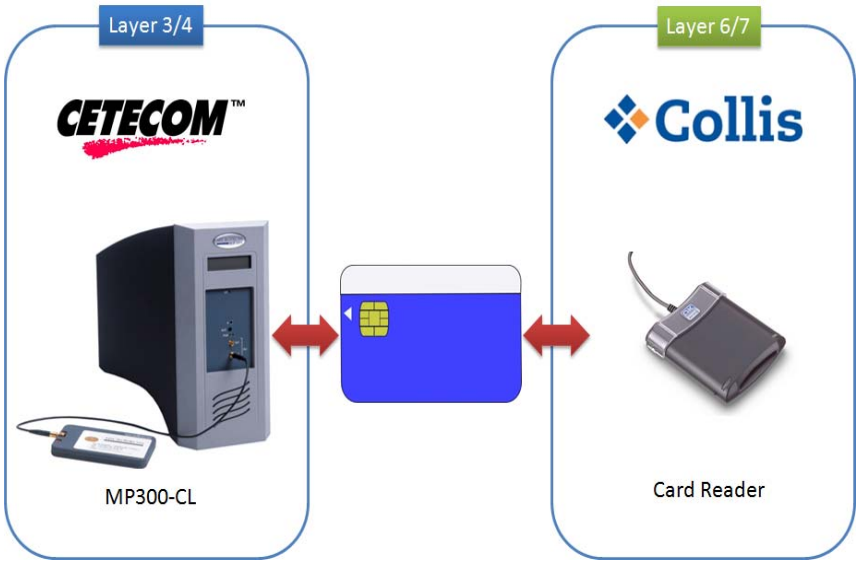

Figure 4 TOE TEST Environment

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.5 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 TSF internals is easy to implement when it is well organized, unlikely to have defects that can cause vulnerability, and easy to maintain without occurrence of defects. Therefore, the verdict of ADV_INT.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.4 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), design description and implementation representation (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 personalization document and guidance document 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, evaluation deliverables, and development tools. Therefore, the verdict of ALC_CMS.5 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 evaluator has confirmed that the developer has used development tools that follow implementation standard he/she can draw consistent and predictable results. Therefore, the verdict of ALC_TAT.2 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.3 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 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 assumption.

① When the developer loads an extra application other than the MRTD application that the TOE basically provides, the application shall be check if it would not be security threat to the smartcard OS and the MRTD application.

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	An agent receives ePassport identity data from the reception organization and generates the SOD by digital signature on the data. After recording them in a MRTD chip, a 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 Digital	A unique information which is signed with the generation key the personalization agent issued in ePassport digital signature system to

Signature	check issue and entry of passport processed by digital method.
e-Passport	A 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 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	A program for loaded in a 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 an ePassport holder by inspecting the MRTD chip presented by an 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)	A security mechanism with which a 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 signed values
BAC (Basic Access Control)	A 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	A 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	An IS implemented with the BAC and the PA security mechanisms
EAC (Extended Access	A security mechanism 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 an

Control)	ePassport holder for access control to the biometric data of the ePassport holder stored in a MRTD chip
EIS : EAC Inspection System	An IS to implement the BAC, the PA and the EAC security mechanisms and the AA as an option
EAC-CA (EAC-Chip Authentication)	A 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)	A security mechanism that EIS transmits values digital signature with a digital signature generation key of its own to a temporary public key used in EAC-CA and a MRTD chip by using an IS certificate, verifies the digital signature. This security mechanism implements challenge-response authentication protocol based on the digital signature through which a MRTD chip authenticates the EIS.
LDS (Logical Data Structure)	A logical data structure defined in the ICAO document in order to store user data in a MRTD chip
PA (Passive Authentication)	A security mechanism to demonstrate that identity data recorded in an ePassport has not been forgery and corruption as the IS with the DS certificate verifies a digital signature in SOD and a hash value of user data according to read-right of an 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 V1.1 ST V1.6 (9. June. 2010)

[6] LG CNS XSmart e-Passport V1.1 ETR V1.0 (25. June. 2010)