KECS-CR-11-27

XSmart e-Passport V1.2

LG CNS

Certification Report

Certification No : KECS-ISIS-0319-2011

National Intelligence Service IT Security Certification Center

Establishment & Revision History			
Revision Number	Date	Page	Details
V1.0	2011. 06. 23	34	First documentation

This document is the certification report for

LG CNS XSmart e-Passport V1.2

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Internet & 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 V1.2 with reference to Common Criteria for Information Technology Security Evaluation (notified July. 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 Internet & Security Agency and completed on May 18, 2011. 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 a chip 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 S3CT9KW of Samsung which is certified as CC EAL5+. The IC components that the TOE is based on include IC chip hardware, IC chip firmware, and cryptographic operation software library for RSA/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.

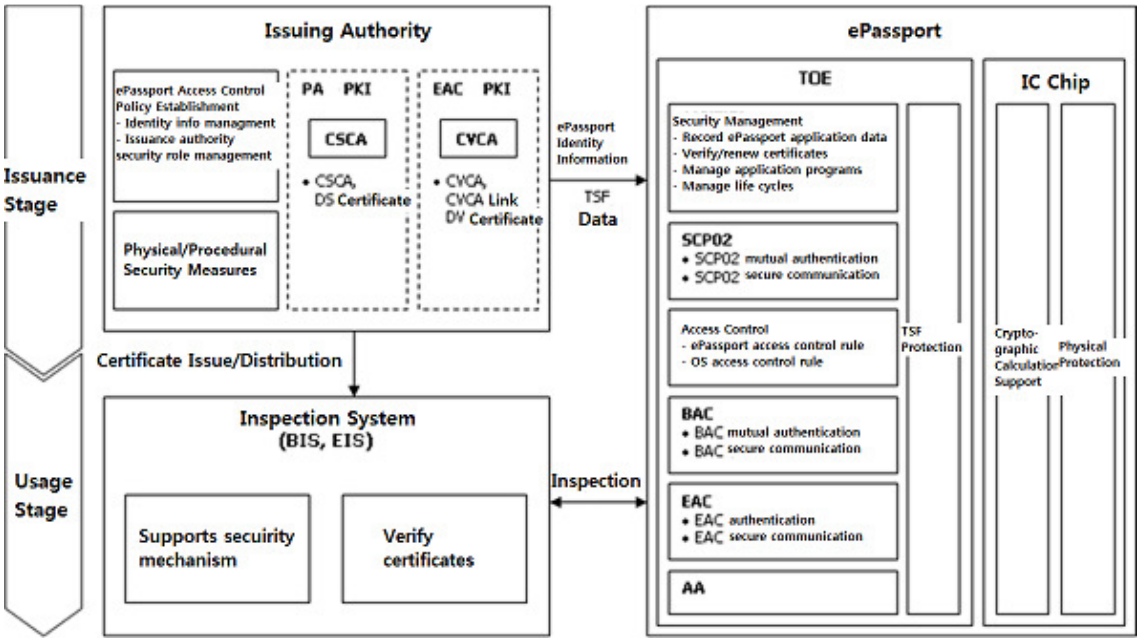

Figure 1 TOE Operation Environment

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 V1.2.

2. Information for Identification

Scheme	Korea Evaluation and Certification Guidelines for IT security (Sep. 1, 2009) Korea Evaluation and Certification Scheme for IT Security (Jan. 01, 2010)
TOE	XSmart ePassport V1.2
Protection Profile	ePassport Protection Profile V2.1
ST	XSmart ePassport V1.2 ST V1.5
ETR	XSmart ePassport V1.2 ETR V1.0 (May 18, 2011)
Evaluation results	Suitable - Conformance claim: CC Part 2 and Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V3.1 (July 01, 2009)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V3.1 (July 01, 2009)
Sponsor	LG CNS
Developer	LG CNS
Evaluator	IT Security Evaluation Team, Public Information Security Division, Korea Internet & Security Agency(KISA) Jae-Deok Ji, In-Sup Kim
Certification body	IT Security Certification Center(ITSCC)

3. Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

P.INTERNATIONAL_COMPATIBILITY

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

Application Notes: The international compatibility shall be ensured according to 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 ePassport access control policies of the Personalization agent.

Application Notes: The operation flow of the TOE differs according to the type of security mechanisms supported by the Inspection System. The basic operation flow depends on 2.1.1 Standard ePassport Inspection Procedure and 2.1.2 Advanced ePassport Procedure of the EAC specifications.

P.APPLICATION_PROGRAM_INSTALL

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

Application notes: The application program installing can only be done by organizations holding the same authority as the Personalization agent. Also, ePassport application program installed in the IC chips cannot be deleted in the utilized procedure.

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. Also, the personalization agent should establish the access control policy about the operation system management.

Application Notes: SCP02 security mechanism of 'GP standard' as the security mechanism is used for the personalization agent authentication

P.EPASSPORT_ACCESS_CONTROL

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

Application Notes: The TOE shall build access control policies as of the following according to the ICAO document and EAC specifications.

		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 the ePassport shall execute certification practice to securely generate · manage a digital signature key and to generate · issue · operate · destroy certificates according to the CPS by implementing the PA-PKI and EAC-PKI according to the ePassport PKI System.

Also, The Issuing State of the ePassport 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 internally update certificates by verifying validity of the certificates.

P.RANGE_RF_COMMUNICATION

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

4. Assumptions and Scope

4.1. Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used in order to limit the scope of security consideration.

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 identity 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 Notes: The Inspection System should connect to ICAO-PKD periodically, and download CSCA certificates to verify the certificate for PA of the inspection system.

A. Inspection System

The Inspection System shall implement 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 Notes: 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 inspection system.

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. BIS or EIS could implement AA security mechanism additionally, verify the digital signature provided by TOE using the AA digital signature verification key of EF.DG15, and verify the probability of 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's 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 Notes: The IC chip is authorized item S3CT9KW of CCRA EAL5+ to ensure the security of TOE. The cryptographic operation supported by the IC chip may be provided in the co-processor of the IC chip or cryptographic libraries loaded in the IC chip.

A. MRZ Entropy

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

Application Notes: In order to resistant to the moderate-level threat agent, the entropy for the passport number, date of birth, data of expiry or valid until date and check digit used as BAC authentication key seed among the MRZ in the current technological level shall be at

least 56bit. The ST author may change MRZ entropy according to the level of the threat agent.

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 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 S3CT9KW IC chip of Samsung and the physical scope is as followed.

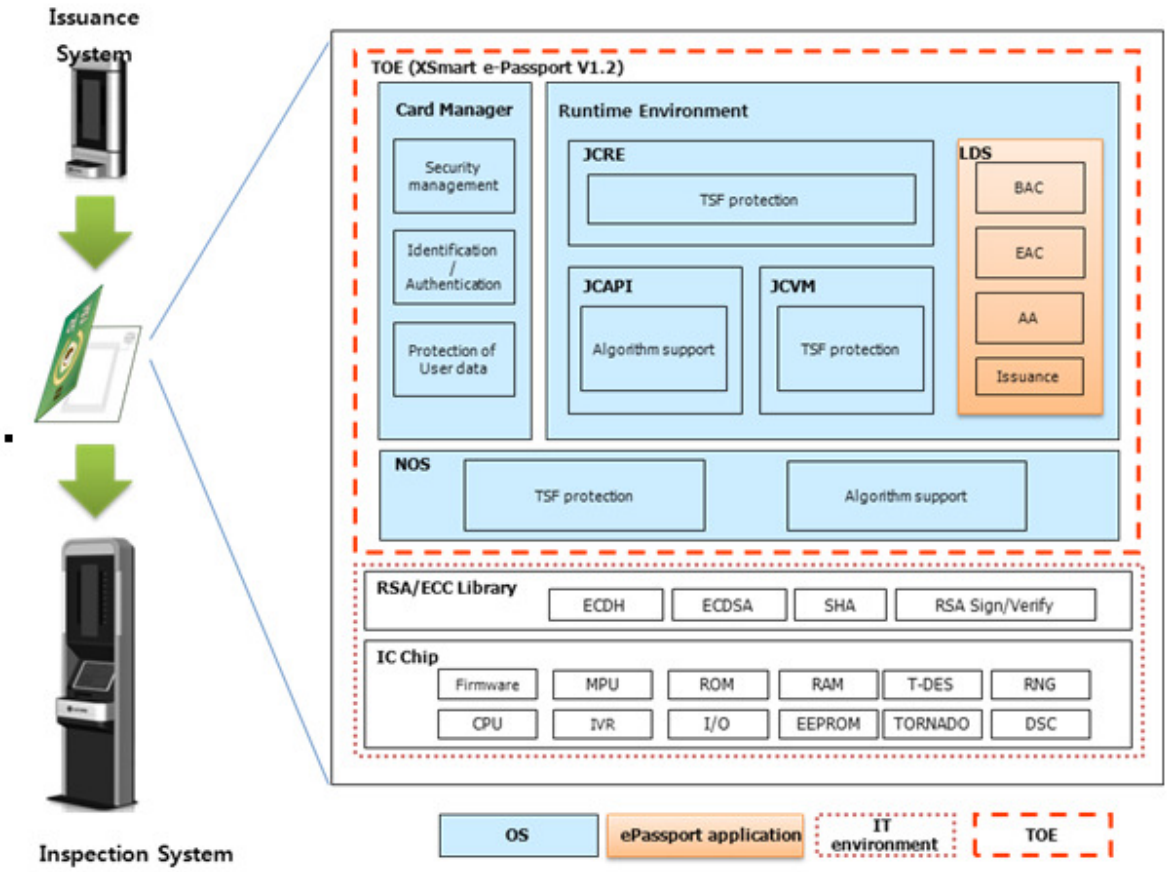

Figure 2 Physical Scope of the TOE

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

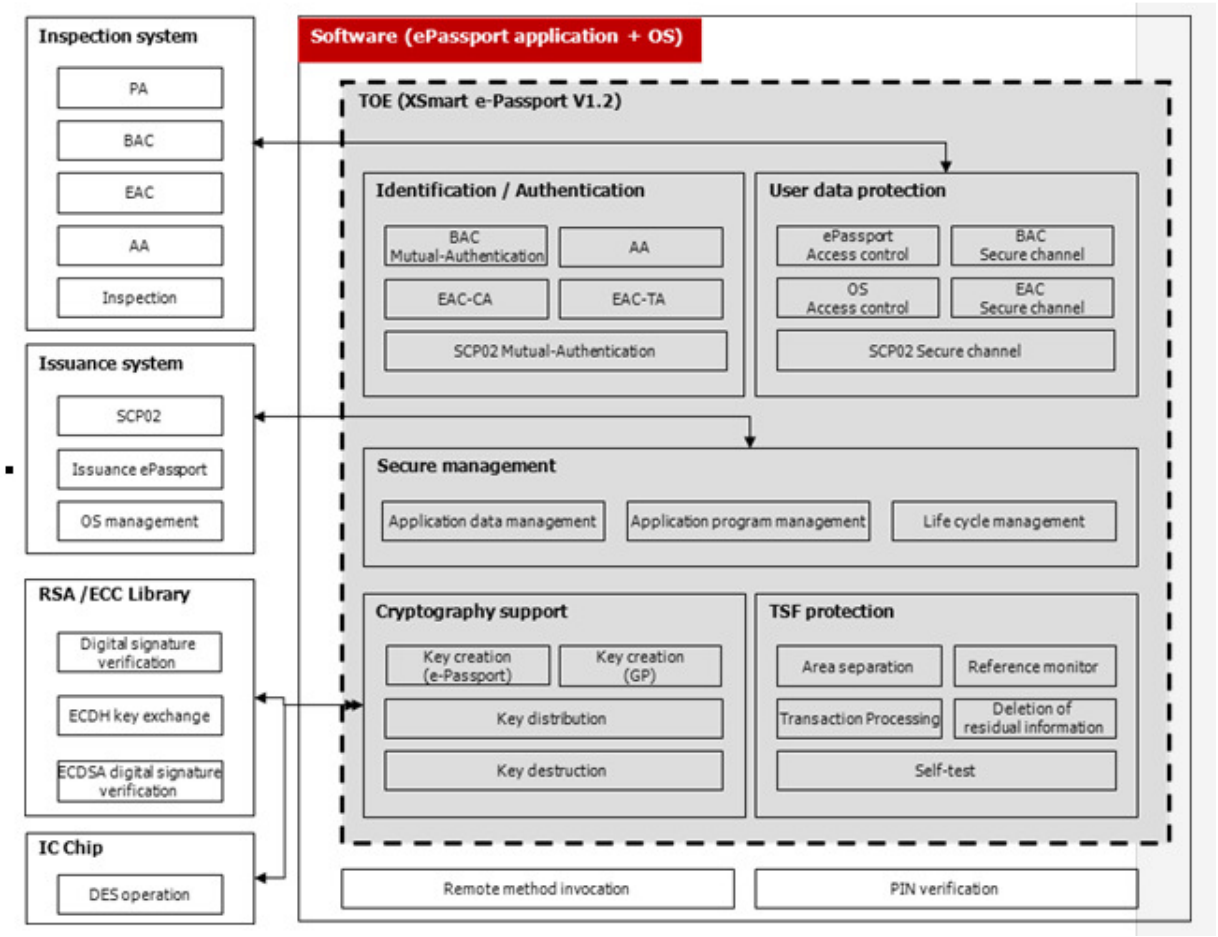

Figure 3 Logical Scope of the TOE

TOE provides security functions such as identification and authentication, user data protection, security management, TSF protection, and cryptography support.

•Identification and Authentication

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

<SCP02 Mutual Authentication>

SCP02 (Secure Channel Protocol 02) is the security mechanism for authenticating Personalization agent with write, add, and renew rights for ePassport applicant identity

information and TSF data in TOE, and includes SCP02 mutual authentication and secure messaging. TOE and Personalization agent use Personalization agent authentication information and SC (Sequence Counter) to generate SCP02 session key, and then mutually verify the MAC value for the exchanged random numbers to perform mutual authentication. If the SCP02 mutual authentication fails, the session is terminated, and if it succeeds, TOE forms a secure messaging using SCP02 session key.

< BAC Mutual Authentication >

The inspection system supporting BAC uses BAC authentication key generated from the optically read MRZ and TOE either generates BAC authentication key from MRZ information of DG1 or uses stored BAC authentication key to each encrypt the generated random number values and exchange. The inspection system supporting BAC and the TOE perform mutual authentication by confirming the exchanged random number value. If the BAC mutual authentication fails, the session is terminated.

< EAC-CA>

EAC-CA implements the Ephemeral-static DH key distribution protocol to provide EAC session key distribution and chip authentication. TOE sends EAC chip authentication public key so that it can be authenticated by the inspection system, and uses the temporary public key received from the inspection system to perform key distribution protocol. If the EAC-CA succeeds, TOE forms EAC secure messaging using EAC session key. Even if EAC-CA fails, BAC secure messaging is maintained, and the inspection system can confirm that TOE has been pirated.

< EAC-TA>

EAC-TA implements the digital-signature-based Challenge-Response authentication protocol so that TOE can authenticate the inspection systems supporting EAC. The value which the

inspection system digitally signed on the temporary public key used in EAC-CA process is verified by TOE with IS certificate to authenticate the inspection system. When TOE receives CVCA link certificate, DV certificate, and IS certificate from the inspection system supporting EAC, it uses the CVCA digital signature verification key in protected memory area to verify CVCA link certificate, and checks the expiry date of CVCA link certificate and renews the CVCA digital signature verification key and the current date within TOE when necessary. Once TOE confirms that the certificate is appropriate by verifying IS certificate, it permits read access by the inspection system to the ePassport applicant bio information and sends through EAC secure messaging.

< AA>

AA (Active Authentication) implements the digital-signature-based Challenge-Response authentication protocol so that the inspection system can authenticate TOE. Once TOE generate the digital signature with AA chip authentication private key in protected memory area on top of the received value provided by the inspection system, the inspection system verifies with the EF.DG15 AA chip authentication public key acquired through BAC secure messaging or EAC secure messaging to authenticate TOE. AA is a security mechanism providing a method to verify the authenticity of TOE.

•User Data Protection

TOE provides access control and secure messaging for user data protection.

< SCP02 Secure Communication Channel>

TOE establishes SCP02 secure messaging using the SCP02 session key generated in the SCP02 mutual authentication process to perform secure communication with the Personalization agent which performed the SCP02 mutual authentication successfully. When sending data through this channel, data is encrypted using TDES encryption algorithm

to provide confidentiality and MAC Verification using Retail MAC algorithm provides integrity.

< BAC Secure Communication Channel>

TOE confirms the reading rights of inspection system for ePassport applicant Basic Information through BAC mutual authentication, and then generates BAC secure messaging using the BAC session key shared through BAC key distribution to transfer ePassport applicant basic information securely. When sending data through this channel, data is encrypted using TDES encryption algorithm to provide confidentiality and MAC Verification using Retail MAC algorithm provides integrity.

< EAC Secure Communication Channel>

TOE generates EAC secure messaging using EAC session key shared through EAC key distribution of EAC-CA process to perform secure communication with the inspection system. When sending data through this channel, data is encrypted using TDES encryption algorithm to provide confidentiality and MAC Verification using Retail MAC algorithm provides integrity.

< Operating System Access Control>

TOE provides access control function which permits only the Personalization agent that acquired management rights by succeeding in SCP02 mutual authentication to have the application program management function to load/install/delete executable code and application program to the OS at the ePassport issuance Phase and usage Phase and the write rights to the basic information of the Personalization agent. Also, the access control function which prohibits performance of all operations except reading the Personalization agent basic information at the termination Phase of TOE life cycle is provided.

< ePassport Access Control>

TOE provides access control function which permits only the Personalization agent that acquired management rights by succeeding in SCP02 mutual authentication to perform the write functions for ePassport user data and TSF data. Also, access control function provided for ePassport user data reading rights based on the access rights of inspection system granted through performance of security mechanisms at the ePassport usage Phase.

•Security Management

TOE limits the method of managing the security properties of user and user data of the ePassport application program and OS and the TSF data such as session key, authentication key and GP registry to the authorized Personalization agent and defines this as the security role. Also, several security management functions such as CVCA certificate and current date renewal and secure messaging identification information initialization are performed by TSF itself.

•TSF Protection

TOE provides functions such as reference monitor, area separation, deletion of residual information, transaction processing, and self-test for TSF protection.

<Reference Monitor >

TOE guarantees that for all APDU commands which are the external interface of TOE, the access control will not be bypassed but invoked every time to protect TSF from interference and invasion by an unauthorized subject.

<Domain Separation >

TOE provides Javacard Firewall within Javacard virtual machine to separate the area use such as other application programs and the area where ePassport application program executes. After LDS application is installed in TOE, all functions such as additional installation, deletion, and retrieval of other applet are prohibited. Therefore, the domain is separated from other unauthorized subjects because only ePassport area exists in TOE.

< Deletion of Residual Information >

TOE provides the function to delete residual information when allocating resources to the object or retrieving resources back from the object so that previous information is not employed for not only temporarily generated information in the temporary memory area such as BAC session key, EAC session key, SCP02 session key, and random number, but also the information generated in the protected memory are such as BAC authentication key.

<Transaction Processing >

TOE provides transaction function to detect TSF malfunctioning when a power-supply shut-off or enforced termination of TSF service during operation occurs, and resume TSF service from the state before the malfunctioning.

<Self-Test >

TOE performs TSF data change detection and measure functions, and performs self-test to verify the integrity of stored TSF data and executable code. Also, when a failure from self-test or an abnormal operation status from the IC chip is detected, it maintains secure state so that malfunctioning of TSF does not occur.

. Cryptographic Support

TOE provides hash calculation, and provides random number generation, key exchange calculation operation mode, encryption/decryption calculation operation mode, and MAC and digital signature calculation operation mode using the IC chip and cryptographic calculation library. TOE guarantees that encryption-related information cannot be found by abusing physical phenomenon (current, voltage, electromagnetic change, etc.) occurring during performance of cryptographic calculation, and provides a method to verify integrity for the encryption key.

6. Guidance

The TOE provides the following guidance document.

•XSmart e-Passport V1.2 Operating Manual V1.3

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:

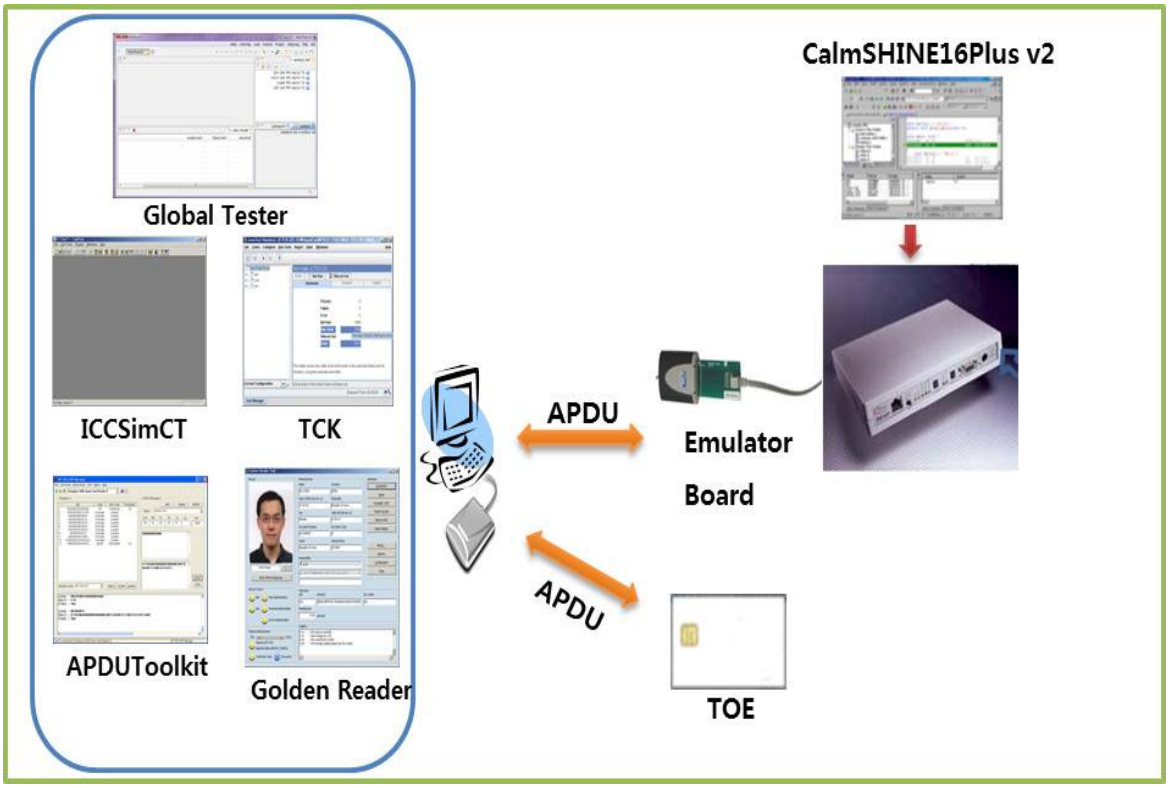

Figure 4 TOE TEST Environment

9. Result of the Evaluation

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 EAL5+ 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 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 i the s 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 TOE does not allow to load extra applications after a MRTD application is installed, because it is only used for an electronic passport.

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 Signature	A 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	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 Authenticati on)	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 Authenticati on	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 Control)	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 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 (July 1, 2009)

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

[3] Korea Evaluation and Certification Guidelines for IT Security (Sep. 1, 2009)

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

[5] LG CNS XSmart e-Passport V1.2 ST V1.5 (May 6, 2011)

[6] LG CNS XSmart e-Passport V1.2 ETR V1.0 (May 18, 2011)