KECS-CR-10-10

Samsung SDS Spass V2.0

Certification Report

Certification No. : KECS-ISIS-0271-2010

October, 2010

National Intelligence Service IT Security Certification Center

Establishment & Revision History			
Revision Number	Date	Page	Details
00	2010. 10. 12	-	First documentation

This document is the certification report for

Samsung SDS SPass V2.0

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Internet & Security Agency

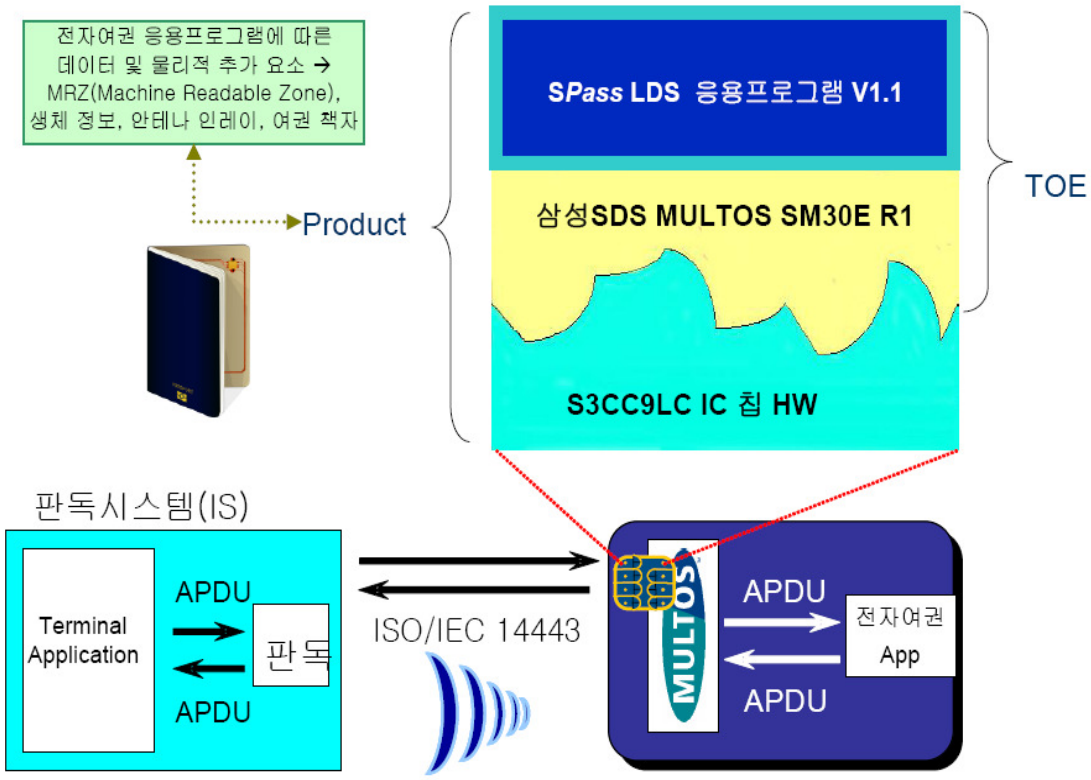
Contents

1. Summary

This report describes the certification result drawn by the certification body on the results of the EAL5+ evaluation of Samsung SDS SPass V2.0 with reference to the Common Criteria for Information Technology Security Evaluation (notified on 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 Internet & Security Agency (KISA) and completed on August 31, 2010. 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 EAL5 of the CC Part 3 which added ADV_IMP.2, ATE_DVS.2, and AVA_VAN.5, therefore the evaluation results was decided to be "suitable".

The TOE, as described in [Figure 1], is software that implemented by open IC chip OS, SM30X that implemented e-Passport Primitive and LDS MRTD application.



[Figure 1] The TOE Overview

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 Samsung SDS SPass V2.0 received permission from the government of Republic of Korea to be used.

2. Information for Identification

[Table 1] shows information for the TOE.

Scheme	Korea evaluation and certification guidelines for IT security (2009. 9. 1) Korea Evaluation and Certification Scheme for IT Security (2010. 1 .1)
TOE	Samsung SDS SPass V2.0
Protection Profile	ePassport Protection Profile V2.1 (KECS-PP-0163a-2009, 2010.6.10)
ST	Samsung SDS SPass V2.0 ST V1.0 (2010. 7. 30)
ETR	Samsung SDS SPass V2.0 ETR, V1.0 (2010. 8.31)
Evaluation results	Suitable - Conformance claim: CC Part 2 and Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V3.1 (2009. 9. 1)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V3.1 (2009. 9. 1)
Sponsor	Samsung SDS
Developer	Samsung SDS
Evaluator	IT Security Evaluation Division, CC Evaluation Lab, Korea Security & Internet Agency Sungjae Lee, Hyunjo Kwan, Junghoon Han
Certification body	IT Security Certification Center(ITSCC) of National Intelligence Service

3. Security Policies

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. 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 Issuing Policy

The TOE deactivates the EAC when the personalization agent does not store biometric information in e-Passport according to the issuing policy. The TOE shall provide a method for deactivation when secure communication channel is not necessary because security of transmitted data is ensured by blocking issuing environment from the outside.

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 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	BIS	BAC Authorization	allow	deny	deny	deny	allow	deny	deny	deny	allow	deny
	EIS	BAC Authorization	allow	deny	deny	deny	allow	deny	allow	deny	allow	deny
		EAC Authorization	allow	deny	allow	deny	allow	deny	allow	deny	allow	deny
	Pesonalization Agent	Pesonalization Authorization	allow	allow	allow	allow	allow	allow	allow	allow	allow	allow

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 security mechanism 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 provided from the Inspection System by verifying validity of the certificates.

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.

P. Application Program Loading

The MCD Personalization agent shall issue a certificate to a provider of MRTD application to ensure that application loaded in MRTD chip does not affect security of the TOE and load only application programs of registered users.

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

P. Application Program Certification

The MCD Personalization agent shall correspond to security attributes and load, execute and delete application programs of provider who has a certificate issued by the MCD Personalization agent.

4. Assumptions and Scope

4.1. Assumptions

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

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. In this case, the BIS additionally executes the AA when it supports the AA security mechanism as an option to explicitly detect the forgery of the TOE through the verification for the digital signature the TOE generated.

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. In this case, when the EIS supports the AA security mechanism as an option, the AA is executed before the EAC-TA, after the EAC-CA and the PA to explicitly detect the forgery of 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: To ensure the secure TOE environment, the IC chip shall be a certified product of over CCRA EAL5+ (level of vulnerability analysis that has immunity against high attack success potential). 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 Note: In order to resistant to the high-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 80bit.

4.2. 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.

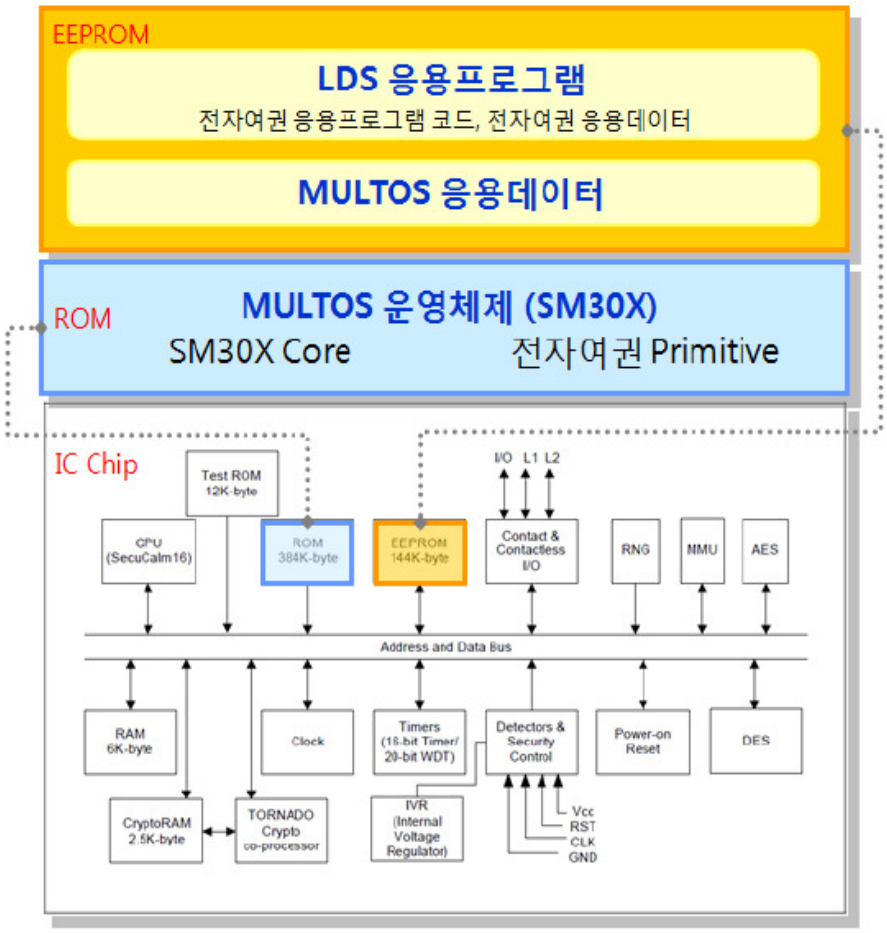
In this certificate report, the IC chip provides functions of physical protection in order to protect the TOE according to the A. IC Chip. Therefore, the physical threat of the IC chip itself by the high-level threat agent is not considered. Nevertheless, the fact that the high-level attack through the logical method has high potential cannot be disregarded.

Therefore, the threat agent to the TOE has the high level of expertise, resources and motivation, and there is high possibility that the attacker finds the exploitable vulnerabilities.

5. TOE Information

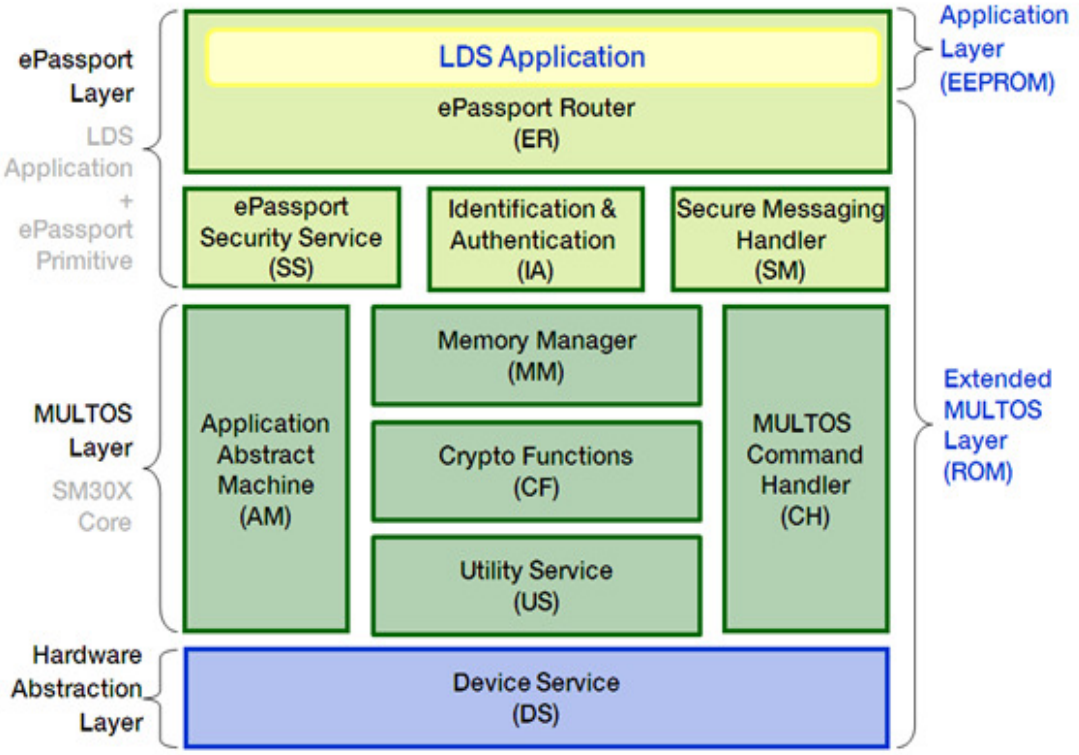
The TOE is a packaged form of a wafer manufactured by loading the TOE on S3CC9LC, contact/contactless IC chip of Samsung Electronics Co. The TOE consists of SM30E compliant with the MULTOS specification and MRTD application compliant with e-Passport specification and EAC specification.

SM30E is masked(masking) in ROM area of Smartcard underlying IC chip. And the MRTD application that contains MRTD application data necessary to operate ePassport is an application over OS and it is loaded on EEPROM. The underlying IC chip loads and packages SM30E and the MRTD application constructing SPass11. SPass11 is completed as a e-Passport product of Samsung SDS by combining with antenna inlay and e-Cover, and mutually works with an Inspection System according to the ISO/IEC 14443 contactless communication. [Figure 2] shows the physical scope of the TOE.



[Figure 2] Physical Scope of the TOE

The TOE consists of 10 subsystem units of TSF to have logical separation as described in [Figure 3].



[Figure 3] Logical Scope of the TOE

The TOE provides security functions as follows:

[MULTOS related Security Function]

- MCD certification, MCD personalization agent certification
- MULTOS access control for loading/execution/deletion of MULTOS application program
- Security attribute management of subject/object for scope of MULTOS access control
- Access control of invalidated instruction

[e-Passport related Security Function]

- e-Passport security mechanisms (BAC, EAC, AA etc.)
- Certification mechanism of personalization agent

- Access control of instruction according to access control and operation mode of e-Passport
- e-Passport security management (management of e-Passport life-cycle and security attribute of access control, writing of TSF data etc.)
- Secure communication channel of issuing phase
- Security of residual information in temporal memory area

[Common Security Function]

- Self-test of random number verification in start-up
- Verification of executable code and data integrity
- Encryption-related interface for cryptographic operation service call of IC chip

6. Guidance

The TOE provides the following guidance documents.

- Samsung SDS SPass V2.0 User Operation Guidance V1.00
- Samsung SDS SPass V2.0 Procedure Guidance V1.00
- Samsung SDS SPass V2.0 Issuing Guidance V1.00

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.

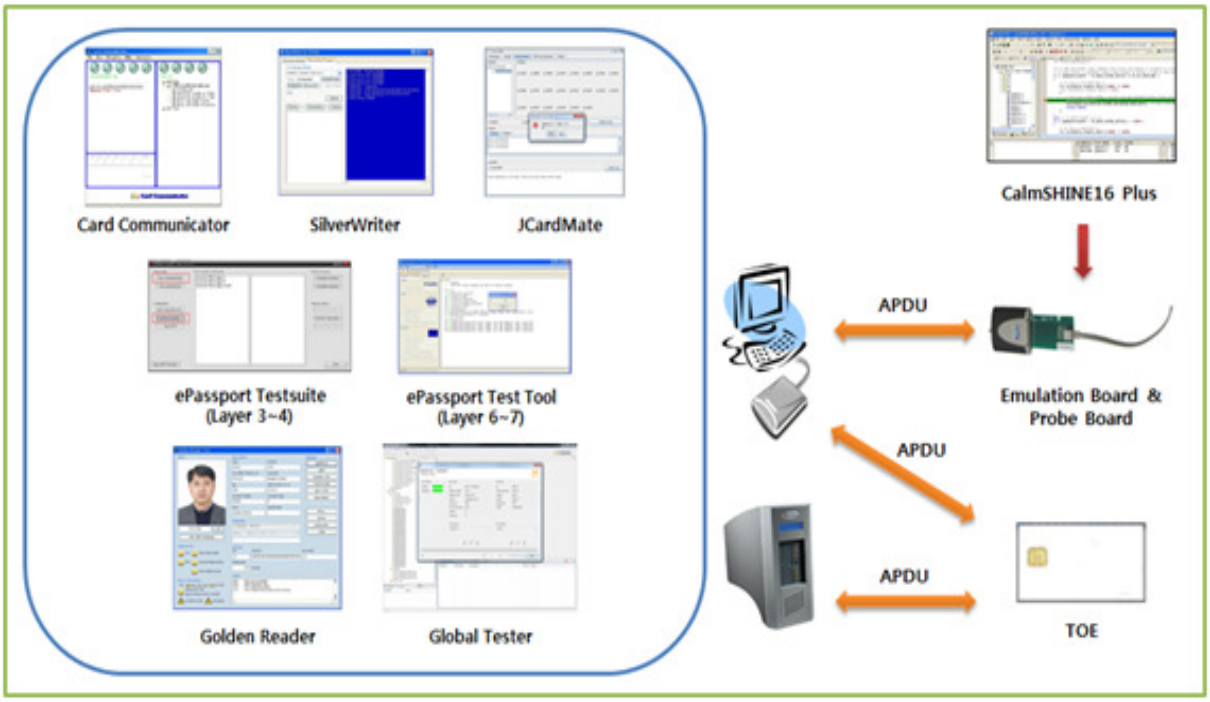
The evaluator has confirmed this consistency by performing additional tests based on the developer's test.

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 4]:



[Figure 4] Evaluator's Test Environment

9. 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 EAL5+ requirements Part 3. Refer to the ETR for more details.

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

9.2. Life Cycle Support Evaluation

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

The developer 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.

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

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.2 is the Pass.

Therefore, life-cycle 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.

9.3. Guidance Documents Evaluation

The guidance document describes procedures and phases to prepare the TOE securely and consequently the TOE is securely configured. Therefore, the verdict of AGD_PRE.1 is the Pass.

The guidance document describes 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.

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

9.4. Development Evaluation

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 specifies with semi-standardized description of the SFR-enforcing module and provides 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.

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) with semi-standardized description, and involves all additional residual error messages. Therefore, the verdict of ADV_FSP.5 is the Pass.

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 TSF internals identifies standards to measure well-organized functions, and based on the fact, demonstrates that overall TSF has well-organized internal designs. Therefore, the verdict of ADV_INT.2 is the Pass.

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

Therefore, the security architecture document, functional specification, TOE design description and implementation representation are adequate to give understanding about how the TSF satisfies the SFRs, and how these SFRs implementation are not damaged or bypassed.

9.5. 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 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.

9.6. Vulnerability Assessment Evaluation

The evaluator confirmed that potential vulnerabilities cannot be misused by attackers with high attack potential in the operational environment. Therefore, the verdict of AVA_VAN.5 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

Because the TOE security can be ensured only in the evaluated TOE operational environment, the TOE shall be operated by complying with the followings.

① The TOE provides the function that can deactivate EAC when DG3 and DG4 are involved in e-Passport according to the policy of personalization agent, but certification of the TOE is available when it is operated with the deactivated EAC function because it was evaluated with the deactivated EAC function.

② The physical, procedural and personal security policy shall be established when secure messaging is not used in e-Passport issuing phase according to issuing policy of personalization agent. In other words, confidentiality and integrity of all data transmitted in issuing phase shall be ensured by physically blocking external network and RF communication.

11. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

Personalization Agent	The agent receives the ePassport identity data from the Reception organization and generates the SOD by digital signature on the data. After recording them in the MRTD chip, the personalization agent generates TSF data and stores it in the secure memory of the MRTD chip. The agent also operates PA-PKI and/ or EAC-PKI.
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.
AA **(Active Authentication)**	The security mechanism with which the MRTD chip demonstrates its genuine to the IS by signing random number transmitted from the IS and the IS verifies genuine of the MRTD chip through verification with the signed values
BAC **(Basic Access Control)**	The security mechanism that implements the symmetric key-based entity authentication protocol for mutual authentication of the MRTD chip and the IS and the symmetric key-based key distribution protocol to generate the session keys necessary in establishing the secure messaging for the MRTD chip and the IS
BAC Mutual authentication	The mutual authentication of the MRTD chip and the IS according to the ISO 9798-2 symmetric key-based entity authentication protocol
BIS : BAC Inspection System	The IS implemented with the BAC and the PA security mechanisms

EAC **(Extended 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.
LDS **(Logical Data Structure)**	Logical data structure defined in the ICAO document in order to store the user data in the MRTD chip

PA **(Passive Authentication)**	The security mechanism to demonstrate that identity data recorded in the ePassport has not been forgery and corruption as the IS with the DS certificate verifies the digital signature in the SOD and hash value of user data according to read-right of the ePassport access control policy.

12. References

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

[1] Common Criteria for Information Technology Security Evaluation (September 1, 2009)

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

[3] Korea evaluation and certification guidelines for IT security (September 1, 2009)

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

[5] Samsung SDS SPass V2.0 ST V1.00 (July 30, 2010)

[6] Samsung SDS SPass V2.0 ETR V1.0 (August 31. 2010)