**KECS-CR-08-37**

# Samsung Spass V1.0

## Certification Report

**Certification No. : KECS-ISIS-0120-2008**

National Intelligence Service IT Security Certification Center

<table>
<tr><th colspan="4">Establishment & Revision History</th></tr>
<tr><td>Revision Number</td><td>Date</td><td>Page</td><td>Details</td></tr>
<tr><td>00</td><td>2008. 9. 24</td><td>-</td><td>First documentation</td></tr>
</table>

This document is the certification report for

Samsung SDS SPass V1.0

Certification Committee Members

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

Yun Lee-Joong(National Security Research Institute)

Cha Sung-Duk(Korea University)

Seo Dong-Soo(Sungshin Women's University)

Ha Jae-Chul(Hosoe University)

Lee Hoon-Jae(Dongseo University)

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Information Security Agency

# Contents

1. Executive Summary ........ 4
2. Identification of the TOE ........ 6
   2.1. Physical scope of the TOE ........ 6
   2.2. Logical scope of the TOE ........ 7
3. Security Policy ........ 9
4. Assumptions and Clarification of Scope ........ 12
   4.1. Assumptions ........ 12
   4.2. Scope to Counter Threats ........ 14
5. TOE Information ........ 15
6. Guidance ........ 17
7. TOE Test ........ 18
   7.1. Developer's Test ........ 18
   7.2. Evaluator’'s Test ........ 19
8. Evaluated Configuration ........ 19
9. Result of the Evaluation ........ 21
   9.1. ST Evaluation (ASE) ........ 21
   9.2. Configuration Management Evaluation ........ 22
   9.3. Delivery and Operation Evaluation ........ 23
   9.4. Development Evaluation ........ 23
   9.5. Guidance Documents Evaluation ........ 24
   9.6. Life Cycle Support Evaluation ........ 24
   9.7. Tests Evaluation ........ 25
   9.8. Vulnerability Assessment Evaluation ........ 25
10. Recommendations ........ 26
11. Acronyms and Glossary ........ 29
12. References ........ 34

# 1. Summary

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

The evaluation of Samsung SDS SPass V1.0 has been carried out by Korea Information Security Agency and completed on August.26. 2008. This report grounds on the evaluation technical report (ETR) KISA had submitted. The evaluation has confirmed that the product had satisfied the CC Part 2 and EAL4 of the CC Part 3 which added ADV_IMP.2, ATE_DVS.2, ATE_DPT.2and AVA_VLA.4, therefore the evaluation results was decided to be “suitable”.

| | Identifier | Note |
|---|---|---|
| TOE | Samsung SDS SPass V1.0 | |
| | - Samsung SDS MULTOS SM30 R3 | Open operating system(“SM30” hereinafter) which was implemented according to the [MULTOS Specifications] |
| | - SPass LDS Application Program V1.0 | e-Passport application(“MRTD application” hereinafter) which was implemented according to the [ICAO Document] and [EAC Specification] |
| Underlying IC chip | S3CC9GC or S3CC9GW | Samsung IC chip which was certified as EAL 4+ by BSI in German |

The TOE provides all security mechanisms such as BAC and EAC required in 'e-Passport Protection Profile V1.0', and implements the AA to additionally verify the authenticity of the IC chip.

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 V1.0 is permitted use or that its quality is assured by the government of Republic of Korea.

# 2. Information for Identification

[Table 1] shows information for the TOE.

| | |
|---|---|
| Scheme | Korea evaluation and certification guidelines for IT security (16, July. 2008)<br>Korea Evaluation and Certification Scheme for IT Security (1. Dec. 2007) |
| TOE | Samsung SDS SPass V1.0 |
| Protection Profile | ePassport Protection Profile V1.0 (KECS-PP-0084-2008, 2008.1) |
| ST | Samsung SDS SPass V1.0 ST V2.21 |
| ETR | Samsung SDS SPass V1.0 ETR V1.0 (2008.8.29) |
| Evaluation results | Suitable<br>- Conformance claim: CC Part 2 and Part 3 Conformant |
| Evaluation Criteria | Common Criteria for Information Technology Security Evaluation V2.3 (16. July. 2008) |
| Evaluation Methodology | Common Methodology for Information Technology Security Evaluation V2.3(16. July. 2008) |
| Sponsor | Samsung SDS |
| Developer | Samsung SDS |
| Evaluator | IT Security Evaluation Division, CC Evaluation Lab,<br>Korea Security & Internet Agency Yoo Yun-Jung, Lee Sung-Jae, Lee Uen-Kyoung, Yu Hee-Jun |
| Certification body | IT Security Certification Center(ITSCC) of National Intelligence Service |

## 2.1. Physical scope of the TOE

The e-Passport means the passport book and the MRTD chip, and antenna embedded in the cover of the passport book. The e-Passport IC chip includes IC chip operating system, the

MRTD application, the MRTD application data, and IC chip components. The IC chip consists with CPU, cryptographic operation processor, input/output port, Memory (RAM, ROM and EEPROM), and the contactless interface etc. The TOE is defined with the SM30 which is the IC chip operating system, the MRTD application, and the MRTD application data, and the IC components are excluded from the physical scope of the TOE.

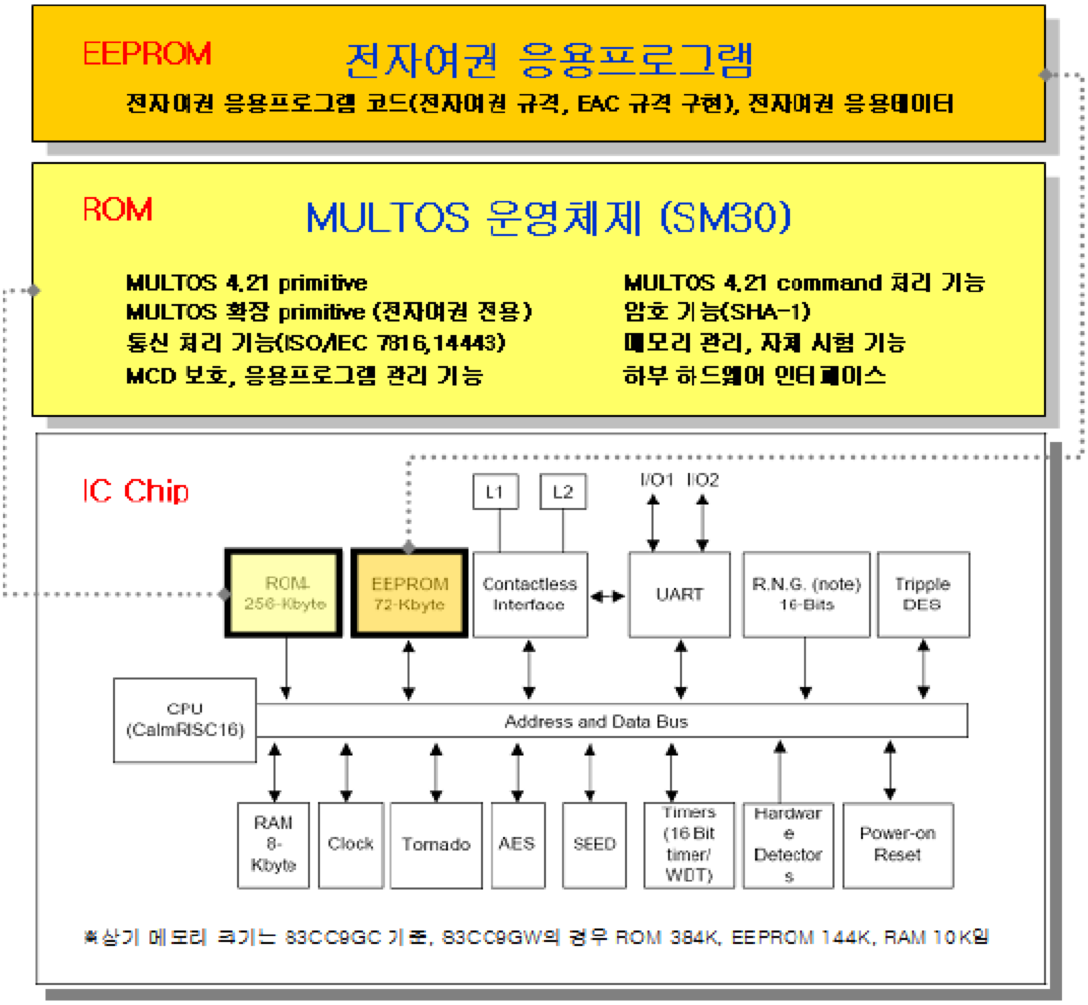

EEPROM
전자여권 응용프로그램
전자여권 응용프로그램 코드(전자여권 규격, EAC 규격 구현), 전자여권 응용데이터
ROM
MULTOS 운영체제 (SM30)
MULTOS 4.21 primitive
MULTOS 확장 primitive (전자여권 전용)
통신 처리 기능(ISO/IEC 7816,14443)
MCD 보호, 응용프로그램 관리 기능
MULTOS 4.21 command 처리 기능
암호 기능(SHA-1)
메모리 관리, 자체 시험 기능
하부 하드웨어 인터페이스
IC Chip
L1
L2
I/O1
I/O2
ROM 256-Kbyte
EEPROM 72-Kbyte
Contactless Interface
UART
R.N.G. (note) 16-Bits
Tripple DES
CPU (CalmRISC16)
Address and Data Bus
RAM 8-Kbyte
Clock
Tornado
AES
SEED
Timers (16 Bit timer/ WDT)
Hardware Detectors
Power-on Reset
※상기 메모리 크기는 83CC9GC 기준, 83CC9GW의 경우 ROM 384K, EEPROM 144K, RAM 10K임

Figure 1Physical scope of the TOE

## 2.2. Logical scope of the TOE

| IT Security Function of the TOE | Details |
|---|---|
| Cryptographic Support (CS) | • Cryptographic Key Management(CS1): Key derivation for generation of BAC authentication key, BAC session key, and EAC session key. KDF Seed distribution for BAC session key generation. KDF Seed distribution for EAC session key generation<br>• Cryptographic Operation Support(CS2): Generating SHA-1 Hash to generate session key used for BAC or EAC secure messaging |
| Data Protection (DP) | • Data Exchange Confidentiality and Integrity(DP1): Cryptographic communication using BAC session cryptographic key or EAC session cryptographic key. Confidentiality protection communication using BAC session MAC key or EAC session MAC key. Terminating messaging in case of detection of modification. Terminating personalization agent session in case of detection of data modification exchanged between the TOE and personalization agent in personalization phase.<br>• Subset residual information protection(DP2): Deleting BAC session key and EAC session key in session termination. Overwriting with '0' in case of collecting resource in temporary memory.<br>• Asymmetric Key based Data Authentication(DP3): Generation of digital signature for AA |
| Identification and Authentication (IA) | • Open Operating System Authentication Mechanism(IA1): Personalization agent authentication, MULTOS application identification and authentication<br>• e-Passport Authentication Mechanism(IA2): BAC mutual authentication, EAC-TA authentication<br>• Contactless Communication(IA3): Inspection System Identification<br>• Multiple Authentication Mechanisms(IA4): BAC mutual authentication, EAC-TA authentication, Personalization agent authentication, Applying MULTOS application authentication mechanism rule.<br>• Authentication Failure Handling(IA5): Taking response action such as session termination and function deactivation in case of authentication failure |
| Security Management (SM) | • Open Operating System Security Management(SM1): MCD activation, Open operating system access control function for application loading/deletion. Management of security attribute of open operating system access control rule<br>• e-Passport Security Management(SM2): e-Passport access control function to the personalization agent. E-Passport access control function in case of communicating with Inspection System. Management of security attribute of e-Passport access control rule. Setting EAC messaging after initializing SSC to '0' in termination of BAC messaging. Authentication of certificate chain in EAC-TA. Update such as information related to CVCA certificate, AA authentication personal key, personalization agent key, life-cycle value etc. |

| | |
|---|---|
| Platform Protection (PP) | • Failure with Preservation of Secure State(PP1): Preserving secure state by terminating session when random number exceeds allowed error in the authentication of random number generator. Terminating the session in case of abnormal behavior using Detector that the IC chip provides, and maintaining reset state until it return to scope of normal behavior. Terminating the session to preserve secure state in case of failure of integrity verification for TSF data and executable code.<br>• TSF Non-Bypassability and Area Separation(PP2): Inaccessibility to the TSF data except for designated commands. Separating secure memory area and unsecure memory area to be inaccessible to secure memory directly from external interface. Setting the blocks to control application to be executable only within the configured scope in application loading.<br>• Integrity Verification through Self-Test(PP3): Checking integrity of configured area of TSF executable code. Checking integrity of MSM activation data in every commands execution. Self-testing the open operation system by regularly testing function which verifies random of random number generator during regular operation. |

# 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. Application Program Loading

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

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

### P. Personalization Agent

The personalization agent shall issue the ePassport in the secure manner so that to confirm that the issuing subject has not been changed and shall deliver the TOE to the Operational Use phase after verifying that the data inside MRTD chip are operating normally after issuing. The Personalization agent shall deactivate the writing function before the TOE delivery to the Operational Use phase.

### P. e-Passport Access Control

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

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

# 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 EAL4+(SOF-high). 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. But, because the MRZ entropy which was determined according to the personalization agent policies considering the level of threats is applied to the TOE, the functional intensity cannot be ensured.

## 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

Samsung SDS V1.0 (the "TOE", hereinafter) implements the IT security functions according to the [ICAO document] and the [EAC specification] according to the IT security requirements required in 'e-Passport Protection Profile V1.0', and consists of MULTOS, which is IC chip open operating system and MRTD application which is loaded on MULTOS. The MULTOS open operating system executes hardware and communication, memory management, and application loading/deletion etc according to the [MULTOS specification] to provides secure run time environment for MRTD application.

S3CC9GC and S3CC9GW, the underlying IC chip, are implemented to support all contact and contactless communications, but when they are used in e-Passport the TOE is loaded, hardware controller for contact communication is deactivated to support only contactless communication in the phase of IC chip activation. SM30 is embedded upon IC chip

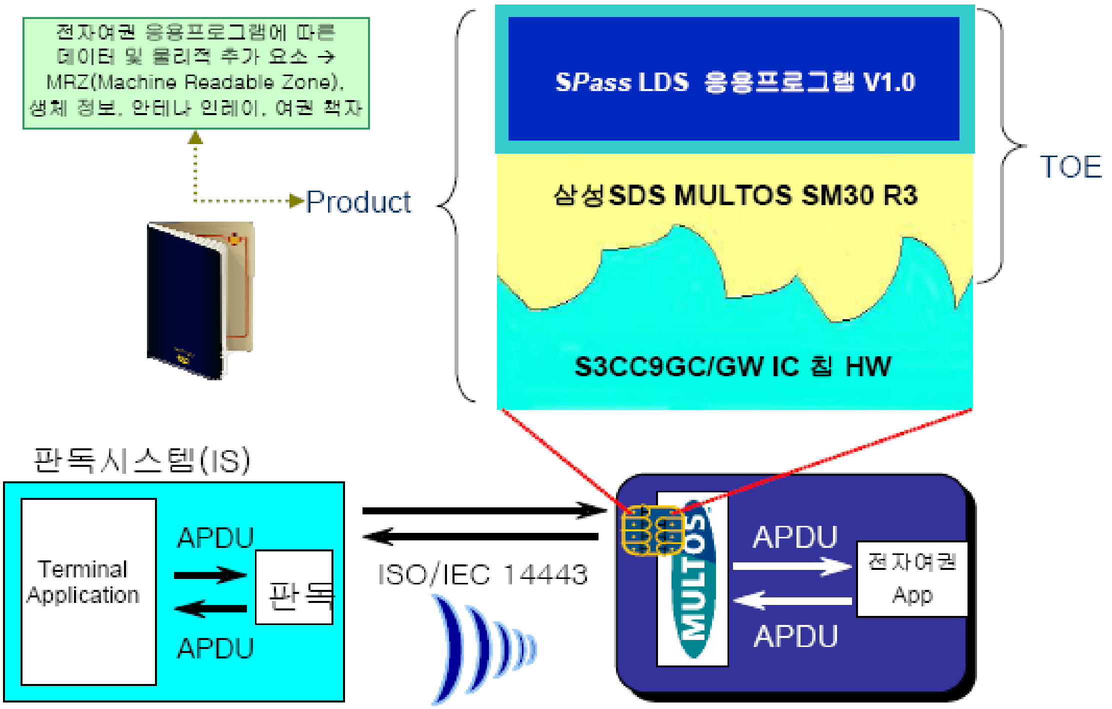

전자여권 응용프로그램에 따른
데이터 및 물리적 추가 요소 →
MRZ(Machine Readable Zone),
생체 정보, 안테나 인레이, 여권 책자
Product
SPass LDS 응용프로그램 V1.0
삼성SDS MULTOS SM30 R3
S3CC9GC/GW IC 칩 HW
TOE
판독시스템(IS)
Terminal Application
APDU
판독
APDU
ISO/IEC 14443
MULTOS
APDU
전자여권 App
APDU

Figure 2TOE Overview

TOE provides the all security mechanisms such as the BAC and EAC required in 'Protection Profile V1.0' and to implements the AA to additionally verify the authenticity of the TOE.

The IT security function the TOE provides as follows:

| | |
|---|---|
| Cryptographic Support (CS) | • Cryptographic Key Management(CS1): Key derivation for generation of BAC authentication key, BAC session key, and EAC session key. KDF Seed distribution for BAC session key generation. KDF Seed distribution for EAC session key generation<br>• Cryptographic Operation Support(CS2): Generating SHA-1 Hash to generate session key used for BAC or EAC secure messaging |
| Data Protection (DP) | • Data Exchange Confidentiality and Integrity(DP1): Cryptographic communication using BAC session cryptographic key or EAC session cryptographic key. Confidentiality protection communication using BAC session MAC key or EAC session MAC key. Terminating messaging in case of detection of modification. Terminating personalization agent session in case of detection of data modification exchanged between the TOE and personalization agent in personalization phase.<br>• Subset residual information protection(DP2): Deleting BAC session key and EAC session key in session termination. Overwriting with '0' in case of collecting resource in temporary memory.<br>• Asymmetric Key based Data Authentication(DP3): Generation of digital signature for AA |
| Identification and Authentication (IA) | • Open Operating System Authentication Mechanism(IA1): Personalization agent authentication, MULTOS application identification and authentication<br>• e-Passport Authentication Mechanism(IA2): BAC mutual authentication, EAC-TA authentication<br>• Contactless Communication(IA3): Inspection System Identification<br>• Multiple Authentication Mechanisms(IA4): BAC mutual authentication, EAC-TA authentication, Personalization agent authentication, Applying MULTOS application authentication mechanism rule.<br>• Authentication Failure Handling(IA5): Taking response action such as session termination and function deactivation in case of authentication failure |
| Security Management (SM) | • Open Operating System Security Management(SM1): MCD activation, Open operating system access control function for application loading/deletion. Management of security attribute of open operating system access control rule<br>• e-Passport Security Management(SM2): e-Passport access control function to the personalization agent. ePassport access control function in case of communicating with Inspection System. Management of security attribute of e-Passport access control rule. Setting EAC messaging after initializing SSC to '0' in termination of BAC messaging. Authentication of certificate chain in EAC-TA. Update such as information related to CVCA certificate, AA authentication personal key, personalization agent key, life-cycle value etc. |

| | |
|---|---|
| Platform Protection (PP) | • Failure with Preservation of Secure State(PP1): Preserving secure state by terminating session when random number exceeds allowed error in the authentication of random number generator. Terminating the session in case of abnormal behavior using Detector that the IC chip provides, and maintaining reset state until it return to scope of normal behavior. Terminating the session to preserve secure state in case of failure of integrity verification for TSF data and executable code.<br>• TSF Non-Bypassability and Area Separation(PP2): Inaccessibility to the TSF data except for designated commands. Separating secure memory area and unsecure memory area to be inaccessible to secure memory directly from external interface. Setting the blocks to control application to be executable only within the configured scope in application loading.<br>• Integrity Verification through Self-Test(PP3): Checking integrity of configured area of TSF executable code. Checking integrity of MSM activation data in every commands execution. Self-testing the open operation system by regularly testing function which verifies random of random number generator during regular operation. |

## 6. Guidance

The TOE provides the following guidance documents.

- Samsung SDS SPass V1.0 Administrator Guidance V1.28
- Samsung SDS SPass V1.0 User Guidance(Inspection System) V1.11
- Samsung SDS SPass V1.0 User Guidance(MULTOS Application Developer) V1.20

# 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.

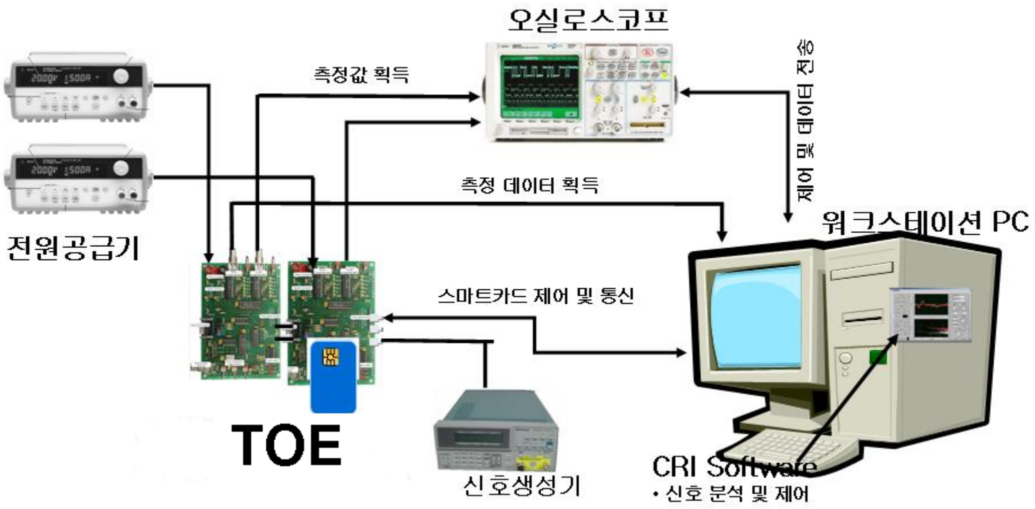
The evaluator has confirmed this consistency by performing additional tests based on the developer's test.

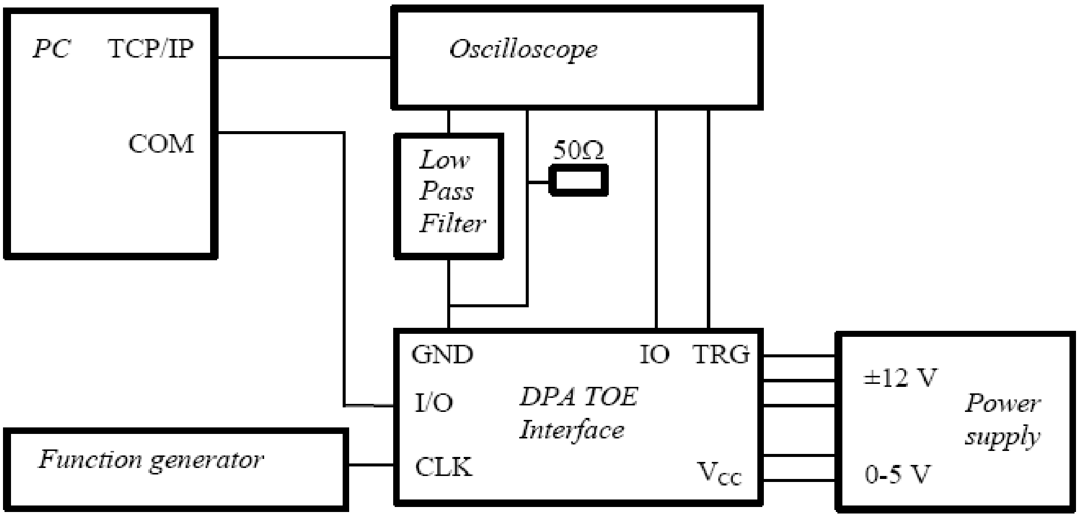
The evaluator has also confirmed that, after performing vulnerability test, no vulnerability had been exploitable in the evaluation configuration.

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:


오실로스코프
측정값 획득
제어 및 데이터 전송
측정 데이터 획득
워크스테이션 PC
전원공급기
스마트카드 제어 및 통신
TOE
신호생성기
CRI Software
• 신호 분석 및 제어


PC
TCP/IP
COM
Oscilloscope
Low Pass Filter
50Ω
GND
IO
TRG
I/O
DPA TOE Interface
CLK
Vcc
Function generator
±12 V
Power supply
0-5 V

<TOE Penetration 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 EAL4+ requirements Part 3. Refer to the ETR for more details.

## 9.1. ST Evaluation (ASE)

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

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

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

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

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

The IT security requirements specified separately identify the all TOE security requirements that specified separately without the CC references, and justify the reason of separated specification, and describe accurately and unambiguously. Therefore the verdict of ASE_SRE.1 is the Pass.

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

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

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

## 9.2. Configuration Management Evaluation

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

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

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

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

## 9.3. Delivery and Operation Evaluation

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

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

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

## 9.4. Development Evaluation

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

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

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

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

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

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

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

## 9.5. Guidance Documents Evaluation

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

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

## 9.6. Life Cycle Support Evaluation

The evaluator has confirmed that the developer's control of the development environment had been suitable to provide the confidentiality and integrity of the TOE design and implementation required for the secure operation of the TOE. Therefore, the verdict of ALC_DVS.2 is the Pass.

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

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

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

## 9.7. Tests Evaluation

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

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

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

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

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

## 9.8. Vulnerability Assessment Evaluation

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

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

The vulnerability analysis adequately describes the obvious security vulnerabilities of the TOE and the countermeasures such as the functions implemented or recommended configuration specified in the guidance documentation. The evaluator has confirmed by performing penetration testing based on the evaluator's independent vulnerability analysis that the developer's analysis had been correct. The evaluator has determined by performing vulnerability analysis that there had not been any vulnerabilities exploitable by an attacker possessing a high-level attack potential in the intended TOE environment. Therefore, the verdict of ATE_VLA.4 is the Pass.

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

## 10. Recommendations

Because the TOE security can be ensured only in the evaluated TOE operational environment, the users who operate the TOE shall comply with the followings.

① Because the TOE includes software elements which compose e-Passport, physical security technique of e-Passport shall be provided to detect attempts of a copy of e-Passport IC chip and Grandmaster chess attack, picture replacement, MRZ data modification etc.

② An immigration inspector shall have procedures to verify identity data page copied in e-Passport and e-Passport holder's identification.

③ The Open platform TOE can load the applications other than the e-Passport application, so the personalization agent shall allow loading the application after confirming that the application loaded on the e-Passport IC chip has no effect on the TOE security.

④ The Inspection System 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 Inspection System which supports the EAC 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.

⑤ 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. Also, after session ends, all information used in communication and the TOE shall be securely destroyed.

⑥ 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 normal operating and compatibility after issuing. The Personalization agent shall deactivate the writing function before the TOE delivery to the Operational Use phase.

⑦ The personalization agent shall ensure the MRZ entropy to ensure the secure BAC authentication key.

⑧ 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

⑨ 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.

# 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 |
| **TSC** | TSF Scope of Control |
| **TSF** | TOE Security Functions |
| **TSP** | TOE Security Policy |

| | |
|---|---|
| **Personalization Agent** | The agent receives the ePassport identity data from the Reception organization and generates the SOD by digital signature on the data. After recording them in the MRTD chip, the personalization agent generates TSF data and stores it in the secure memory of the MRTD chip. The agent also operates PA-PKI and/ or EAC-PKI. |
| **SOD : Security Object Document** | The SOD refers to the ePassport identity data and the ePassport authentication data recorded in the Personalization phase by the Personalization agent that is signed by the Personalization agent with the digital signature generation key. The SOD is an object implemented with signed data type of ‘RFC |

| | |
|---|---|
| | 3369 cryptographic message syntax, 2002.8’ and encoded with DER method. |
| **e-Passport Digital Signature** | Unique information which is signed with the generation key the personalization agent issued in ePassport digital signature system to check issue and entry of passport processed by digital method. |
| **e-Passport** | The passport embedded the contactless IC chip in which identity and other data of the ePassport holder stored according to the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO). |
| **User Data** | Including the ePassport identity data and the ePassport authentication data |
| **ePassport identity data** | Including personal data of the ePassport holder and biometric data of the e-Passport holder |
| **Personal data of the ePassport holder** | Visually identifiable data printed on identity information page of the of ePassport and other identity data stored in the MRTD chip in the LDS structure |
| **Biometric data of the ePassport holder(Sensitive Data)** | Fingerprint and/ or iris data of ePassport holder stored in the MRTD chip in the LDS structure |
| **MRTD Application Data** | Including user data and TSF data of the MRTD |
| **MRTD Application** | Program for loaded in the MRTD chip that is programmed by the LDS of the ICAO document and |

| | |
|---|---|
| | provides security mechanisms of BAC, PA and EAC, etc. |
| **Inspection** | Procedure in which immigration office checks identity of the ePassport holder by inspecting the MRTD chip presented by the ePassport holder, therefore verifying genuine of the MRTD chip |
| **IS : Inspection System** | As an information system that implements optical MRZ reading function and the security mechanisms (PA, BAC, EAC and AA, etc.) to support the ePassport inspection, the IS consists with a terminal that establishes the RF communication with the MRTD chip and the system that transmits commands to the MRTD chip through this terminal and processes responses for the commands. |
| **Application Protocol Data Unit**<br>**(APDU)** | A data format to exchange packaged data of Application between a Smartcard and a terminal. APDU is divided into Command APDU and Response APDU. There is a TPDU of lower layer according to a communication protocol between a card and a terminal. APDU is transmitted after transferring to appropriate TPDU which is fit to communication protocol.<br>For communication between application on IC chip and external program protocol massage unit defined in ISO/IEC 7816-4 IC (defined in ST) |
| **AA**<br>**(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**<br>**(Basic Access Control)** | The security mechanism that implements the symmetric key-based entity authentication protocol for mutual authentication of the MRTD chip and the IS and the symmetric key-based key distribution protocol to generate the session keys necessary in establishing the secure messaging for the MRTD chip and the IS |
| **BAC Mutual authentication** | The mutual authentication of the MRTD chip and the IS according to the ISO 9798-2 symmetric key-based entity authentication protocol |
| **BIS : BAC Inspection System** | The IS implemented with the BAC and the PA security mechanisms |
| **DFA**<br>**(Differential Fault Analysis)** | A method to derive a cryptographic key by generating malfunction through compelled modification such as voltage and clock and so on in process of cryptographic operation. |
| **DPA**<br>**(Differential Power Analysis)** | A method to derive a cryptographic key through statistical analysis by collecting consumed electric power in large quantities in process of cryptographic operation. |
| **EAC**<br>**(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**<br>**(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**<br>**(EAC-Terminal Authentication)** | The security mechanism that The EIS transmits values digital signature with the digital signature generation key of its own to the temporary public key used in the EAC-CA and the MRTD chip by using the IS certificate, verifies the digital signature. This security mechanism implements challenge-response authentication protocol based on digital signature through which the MRTD chip authenticates the EIS. |
| **EMA**<br>**(Electromagnetic Analysis)** | A method to derive a cryptographic key by collecting and interpreting released electromagnetic waves in process of cryptographic operation. |
| **LDS**<br>**(Logical Data Structure)** | Logical data structure defined in the ICAO document in order to store the user data in the |

| | |
|---|---|
| | MRTD chip |
| **PA**<br>**(Passive Authentication)** | The security mechanism to demonstrate that identity data recorded in the ePassport has not been forgery and corruption as the IS with the DS certificate verifies the digital signature in the SOD and hash value of user data according to read-right of the ePassport access control policy. |
| **SCP02(Secure Channel Protocol 02) Mutual Authentication** | A Symmetric Key-based Entity Authentication Protocol defined in Global Platform 2.1.1 Card Specification. |
| **SPA**<br>**(Simple Power Analysis)** | A method to derive a cryptographic key by collecting and interpreting consumed electric power in process of cryptographic operation. |

## 12. References

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

[1] Common Criteria for Information Technology Security Evaluation (July. 2008)

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

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

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

[5] Samsung SDS SPass V1.0 ST V2.21 (24. Aug. 2008)

[6] Samsung SDS SPass V1.0 ETR V1.0 (29. Aug. 2008)