KECS-CR-10-36

Smart Card Open Platform Protection Profile V2.1 Certification Report

Certificate No. : KECS-PP-0097-2010

June, 2010

National Intelligence Service IT Security Certification Center

This document is the certification report for Smart Card Open Platform Protection Profile V2.1.

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Internet & Security Agency

Table of Contents

1. Summary

This report states the outcome of the [Smart Card Open Platform Protection Profile V2.1] evaluation. This Chapter summarizes the Smart Card Open Platform PP evaluation results and confirms the overall results, i.e. that the PP evaluation has been properly carried out, that Class APE of CC Part 3 V3.1 R3 and Class APE of CEM V3.1 R3 have been correctly applied.

The Smart Card Open Platform PP evaluation was conducted by Korea Internet & Security Agency (KISA). It was completed on May 2, 2010 and validated by National Intelligence Service(NIS) in June, 2010. The Evaluation Technical Report (ETR) for Smart Card Open Platform PP was written by KISA and served as the principal basis for this Certification Report(CR).

The Smart Card Open Platform PP evaluation has met all evaluator activities for a PP evaluation in both the APE CC Part 3 V3.1 R3 and CEM V3.1 R3. At the conclusion of the Smart Card Open Platform PP evaluation all APE CC and CEM evaluator activities were passed.

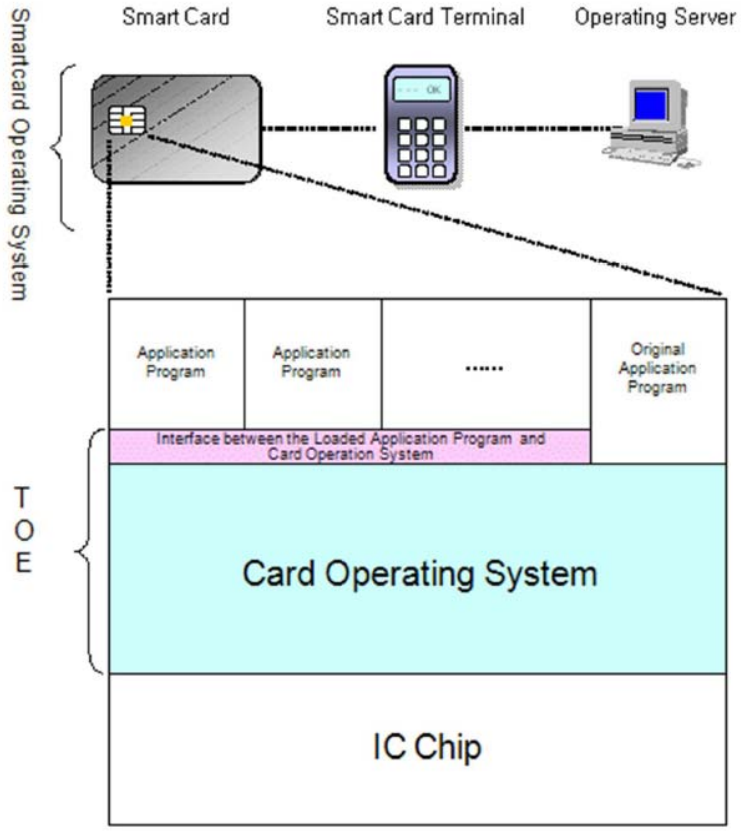
The TOE is the Smart Card operating system, and interface between loaded application program and operating system except for IC chip which is hardware part of Smart Card and loaded application program.

In general, Smart Card is a device built in with central processing unit (CPU) and memory that is capable of information processing and storage. Supporting multiple functions, Smart Card mainly consists with the hardware element of IC chip, card operating system for resource and data management, interface between the loaded application program and card operating system, and application program to provide specific functions. IC chip, the hardware part of Smart Card, generally consists with central processing unit (CPU), coprocessor, input/ output port, RAM, ROM and EEPROM.

The Smart Card Operating System is designed for operation with the Smart Card terminal through bi-directional serial interface. The tasks include input/output data transmission, instruction execution management, file management, cryptographic function, etc.

[Figure 1] shows the environment in which Smart Card is actually operated and the scope of the TOE and hierarchy of Smart Card that provides multiple functions. The TOE is an open platform that includes the Smart Card operating system, execution environment and the management program, etc. with the

exception of IC chip and the loaded application program. The IC chip, the software for the IC chip and the firmware are IT environment in which the TOE is operated.



[Figure1] TOE Configuration

Smart card holder and issuer generally execute operations through communication with Smart Card terminal. Issuer executes management operations of loading, deleting and modifying application by using Smart Card terminal. The holder uses Smart Card functions by using terminal. Here, Smart Card terminal and the operating server becomes the IT environment for the TOE operation.

The TOE can be loaded with the application program. However, security requirements for this will not be discussed in this Protection Profile. In case the Smart Card developed by conforming this Protection Profile includes the application, the developer must describe in the security target specifications that security of the Smart Card operating platform is not damaged and must include, when applicable, security requirements for the application program.

Major assets to be protected by the TOE in this Protection Profile are the data managed in the card. The TOE data are largely divided into 2 types, such as

the user data and the TSF data necessary in the TOE operation. Also, documents created in the course of the TOE production are additional assets to be protected as they affect the integrity and the confidentiality of the TOE.

【 Security Violation Analysis 】

TOE detects security violation events security violation in relation to checksum value of internal data or incidents, such as the resource allocation error or the authentication failure, etc and takes actions such as the card function disablement and memory data deletion, etc

【 Cryptographic Function 】

TOE executes cryptographic key generation/destruction. Also, it ensures that cryptographic-related information cannot be found out by exploiting physical state (changes of the electrical current, voltage and the electromagnetic, etc) that occurred in cryptographic operation.

【 Access Control 】

The TOE provides access control rules to ensure that only the authorized user can access data.

【 Identification and Authentication 】

TOE ensures that it identifies and authenticates the identity of user and provides action in case of the authentication failure.

【 Security Management 】

TOE manages security capability, security attribute, TSF data and security role etc.

【 Other TSF Security 】

TOE conducts self-test to verify the integrity of TSF data and executable code, provides capability to recover to secure state when the failure occurred.

TOE can require additional hardware, software or firmware for operation. This protection profile was developed to reflect TOE that implemented in various types and required for TOE execution when ST author accept this protection profile, but shall describe all non-TOE hardware, software or firmware.

The CB(Certification Body) has examined the evaluation activities, provided the guidance for the technical problems and evaluation procedures, and reviewed each WPR(Work Package Report), OR(Observation Report) and ETR(Evaluation Technical Report). The CB confirmed that this PP is complete, consistent and technically sound through the evaluation results. 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 [Smart Card Open Platform Protection Profile V2.1] is permitted for use within the government of Republic of Korea, or that its quality is assured.

2. Information for Identification

[Table 1] shows information for the PP identification.

[Table 1] Information for the PP Identification

Scheme	Korea evaluation and certification guidelines for IT security (16 July, 2008) Korea Evaluation and Certification Scheme for IT Security (20 March, 2009)
TOE	Smart Card Open Platform Protection Profile V2.1
ETR	Smart Card Open Platform Protection Profile V2.1 ETR V1.0 (2 May, 2010)
Evaluation Results	Verdict for APE Class : Pass Conformance claim : Common Criteria V3.1r3 - CC Part 2 Conformant - CC Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1r3, CCMB, 2009. 7.
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation, Version 3.1r3, CCMB, 2009. 7.
Sponsor	Korea Internet & Security Agency
Developer	Korea Internet & Security Agency & Sungkyunkwan University
Evaluation Body	IT Security Evaluation Division, Korea Internet & Security Agency
Certification Body	National Intelligence Service

3. Security Policies

The TOE of [Smart Card Open Platform Protection Profile V2.1] shall comply with the following Organizational Security Policies.

P. Open_Platform	The TOE must be developed as open platform that can be loaded with a variety of application programs.
P. Role_Division	The role is divided per each responsible person from the stage of the Smart Card manufacturing to the stage of use. The TOE must be manufactured and managed with secure method according to the role.

4. Assumptions and Scope

4.1 Assumptions

The TOE of [Smart Card Open Platform Protection Profile V2.1] shall be installed and operated with the following assumptions in consideration.

A.Trusted_Path	There is trusted path between the TOE and the Smart Card terminal, the communication target of the TOE.
A.Application_Program	When installing the application program in the TOE, the approved procedures must be followed. Also, the legitimately installed the application program does not contain malicious code.
A.Underlying_Hardware	The underlying hardware in which the TOE is operated provides cryptographic function to support security function and it is physically secure.
A. TOE_Management	The stage from the TOE manufacturing to use is divided of the roles, such as the manufacturer, the issuer and the holder. Appropriate training is necessary according to the regulations prescribed per each role. Also, repair and replacement due to defect of the TOE or the Smart Card are processed with secure method.

A. TSF_Data	The TSF data exported to the outside of the TOE, therefore handled in the course of the TOE operation are securely managed.

4.2 Scope to Counter Threats

[Smart Card Open Platform Protection Profile V2.1] defines security threats possible to be caused on the protected assets of the TOE by threat agents. Threat agents are generally IT entity or users that illegally accesses and abnormally damage TOE and security target system. Threat agents hold medium level of professional knowledge, resources and motives.

T. Logical_Attack	The threat agent may change or disclose the user data or the TSF data by exploiting logical interface.
T. Issuance_Misuse	The threat agents may exploit the TOE in the process issuing the Smart Card that includes the TOE.
T. Illegal_Terminal _Use	The threat agent may change and disclose the user data or the TSF data by using unauthorized the Smart Card terminal.
T. Illegal Program	The threat agent may change and disclose the user data or the TSF data by illegally installing the application program that includes malicious code in the TOE.
T. Unintentional_Failure	The threat agent may exploit disclosure of and damage to the user data and the TSF data caused by suspension of the power supply during the card use or incomplete ending of the TSF service due to impact, etc.
T. Continuous_ Authentication_Attempt	The threat agent may access the TOE by continuously attempting authorization.
T. Intentional_Triggering _of_Failures	The threat agent may change and disclose the user data or the TSF data by incompletely ending the TSF service with attack using physical stress to the Smart Card.
T. Residual_Information	In case the TOE reuses resources, the threat agent may illegally access information as information of the object is not properly removed.
T. Information Disclosure	The threat agent may exploit the information disclosed from the TOE during normal use of the TOE.

5. PP Information

5.1 Security Functional Requirements

The TOE of [Smart Card Open Platform Protection Profile V2.1] defines security functional requirements as of the following.

[Table 2] Security Functional Requirements

Security Functional Classes	Security Functional Components	
Security Audit	FAU_ARP.1	Security Alarms
	FAU_SAA.1	Potential violation analysis
Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
	FDP_RIP.1	Subset residual information protection
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.6	Re-authenticating
	FIA_UID.1	Timing of identification
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
Privacy	FPR_UNO.1	Unobservability
TSF Protection	FPT_FLS.1	Failure with preservation of secure state
	FPT_RCV.3	Automated recovery without undue loss
	FPT_RCV.4	Function recovery
	FPT_TST.1	TSF testing

5.2 Assurance Packages

Assurance requirements of [Smart Card Open Platform Protection Profile V2.1] consist with assurance components in CC Part 3 and evaluation assurance level is “EAL4+.”The augmented assurance components are ATE_DPT.2 and AVA_VAN.4.

6. Evaluation Results

The evaluation is performed with reference to the CC V3.1 and CEM V3.1. The verdict of [Smart Card Open Platform Protection Profile V2.1] is the pass as it satisfies all requirements of APE(Protection Profile, Evaluation) Class of CC. Therefore, the evaluation results were decided to be suitable. Refer to the ETR for more details.

The PP introduction of [Smart Card Open Platform Protection Profile V2.1] consistently provides information necessary in PP identification. As a result of the evaluation the verdict PASS is confirmed for the assurance component APE_INT.1 of the class APE.

The conformance claim of [Smart Card Open Platform Protection Profile V2.1] properly describes the PP and CC conformed. As a result of the evaluation the verdict PASS is confirmed for the assurace component APE_CCL.1 of the class APE.

The security problem definition of [Smart Card Open Platform Protection Profile V2.1] clearly defines the security problems which shall be addressed in the TOE and its operational environment. As a result of the evaluation the verdict PASS is confirmed for the assurance component APE_SPD.1 of the class APE.

The security objectives of [Smart Card Open Platform Protection Profile V2.1] adequately and completely address the security problem definition and clearly define the division of the problem between the TOE and its operational environment. As a result of the evaluation the verdict PASS is confirmed for the assurance component APE_OBJ.2 of the class APE.

[Smart Card Open Platform Protection Profile V2.1] doesn't include the extended components and all work units in this section are not applicable and considered to be satisfied. As a result of the evaluation the verdict PASS is confirmed for the assurance component APE_ECD.1 of the class APE.

The security requirements of [Smart Card Open Platform Protection Profile V2.1] are clear, unambiguous and well defined. As a result of the evaluation the verdict PASS is confirmed for the assurance component APE_REQ.2 of the class APE.

The evaluators determine the result of [Smart Card Open Platform Protection Profile V2.1] evaluation as of the following.

[Smart Card Open Platform Protection Profile V2.1] is complete, consistent and technically sound, therefore is suitable to lead to the development of the ST.

The overall verdict PASS is confirmed for the assurance components of the class APE as shown in [Table 3].

[Table 3] TOE Evaluation Results

Assurance class	Assurance Components	Evaluator Requirements	Evaluation Results		
			Evaluator Requirements	Assurance Components	Assurance class
APE	APE_INT.1	APE_INT.1.1E	Pass	Pass	Pass
	APE_CCL.1	APE_CCL.1.1E	Pass	Pass	
	APE_SPD.1	APE_SPD.1.1E	Pass	Pass	
	APE_OBJ.2	APE_OBJ.2.1E	Pass	Pass	
	APE_ECD.1	APE_ECD.1.1E	Pass	Pass	
		APE_ECD.1.2E	Pass		
	APE_REQ.2	APE_REQ.2.1E	Pass	Pass	

7. Recommendations

[Smart Card Open Platform Protection Profile V2.1] includes the minimum security requirements and does not make definition on implementation model of the TOE. In relation to security problems possible to occur according to the TOE implementation model, the developer shall define additional security problems, security objectives and security requirements.

8. Acronyms

(1) Common abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
RAM	Random Access Memory
SFP	Security Function Policy
TOE	Target of Evaluation
TSF	TOE Security Functionality

(2) Terminologies

- Smart Card Terminal : Device mounted with Smart Cardreader/ recorder function as well as keypad, display and security module, etc.

- Authorized Issuer : Authorized user that securely operates and manages functions according to TOE security policies

- Authentication Data : Information used to verify the claimed identity of a user.

- EEPROM (Electrically Erasable Programmable Read-Only Memory) : This is non-volatilememory device that stably remembers memory over a long period of time without requiring power. As a modified version of EPROM (Electrically Programmable Read-only Memory), EEPROM can electrically erase and re-record data. Therefore, this can be conveniently used in application that requires to re-record program. Data are recorded and erased by electrically changing the electric charge of elements that consists a chip. As electric reading or recording is possible, reprogramming is possible while loaded inside system.

- IC Chip (Integrated Circuit Chip) : As an important semiconductor to process the functions of Smart Card, IC chip is a processing device that includes the four functional units of mask ROM, EEPROM, RAM and I/O port.

- RAM (Random Access Memory) : RAM is a storage that maintains operating system application program and the currently used data in order to enable quick access by computer processor. RAM if capable of reading and writing faster than any other computer storage devices, such as hard disk,floppy disk and CD-ROM, etc. However, data stored in RAM are maintained only during the computer is in operation. Data in RAM disappear when computer is turned off. When computer is turned on again, operating system or other files in hard disk are loaded in RAM again.
- ROM (Read-Only Memory) : As a semiconductor memory device, ROM can read, but cannot change contents. This is compared with RAM, which is capable of both reading and writing. Since contents of data are maintained even when computer is turned off, ROM is generally used to load the basic operating system function or language interpreter in computer.

9. References

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

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1r3, CCMB, 2009. 7.

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1r3, CCMB, 2009. 7.

[3] Korea Evaluation and Certification Guidelines for IT Security (16 July, 2008)

[4] Korea Evaluation and Certification Scheme for IT Security (20 March, 2009)

[5] Smart Card Open Platform Protection Profile V2.1 ETR V1.0 (2 May, 2010)