KECS-CR-09-49

LG CNS XSmart OpenPlatform V1.0

Certification Report

National Intelligence Service IT Security Certification Center

Establishment & Revision History			
Revision Number	Date	Page	Details
00	2009. 9. 8	-	First documentation

This document is the certification report for

LG CNS XSmart OpenPlatform V1.0

Certification Committee Members

Choi Jin-Young(Korea University)

Kim Seung-Joo(SungKyunKwan University)

Ryu Jae-Chul(Choong Nam University)

Lee Kang-Soo(Hannam University)

Yoon Lee-JoongDirector(National Security Research Institute)

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Information Security Agency

Contents

1. Summary

This report describes the certification result drawn by the certification body on the results of the EAL4+ evaluation of LG CNS XSmart OpenPlatform 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 LG CNS XSmart OpenPlatform 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 the CC Part 3, therefore the evaluation results was decided to be “suitable”.

The TOE is the product that implements open operating system developed by LG CNS into SLE66CLX800PE/m1581-e13 which is CC EAL5+ IC chip components of Infineon Technologies.

The TOE intends to protect the TOE itself, the TOE data, and important user data from unauthorized access and disclosure, and provides functions of smart cart platform related to application management, separation of executable areas between applications, life cycle management of smart card and application, and user identification and authentication etc.

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

2. Information for Identification

Scheme	Korea evaluation and certification guidelines for IT security (Ministry of Public Administration and Security Notice No. 2008-27, 16. July. 2008) Korea Evaluation and Certification Scheme for IT Security (20. March. 2008)
TOE	XSmart OpenPlatform V1.0
Protection Profile	OpenPlatform Protection Profile V2.0 (KECS-PP-0097-2008, 2008.1)
ST	XSmart OpenPlatform V1.0 ST V1.5
ETR	XSmart OpenPlatform V1.0 ETR V1.0 (2008.8.29)
Evaluation results	Suitable - Conformance claim: CC Part 2 and Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (Ministry of Public Administration and Security Notice No. 2008-26, 16. July. 2008)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation, CCMB-2007-09-004, V3.1(July. 2008)
Sponsor	LG CNS
Developer	LG CNS
Evaluator	IT Security Evaluation Division, CC Evaluation Lab, Korea Security & Internet Agency Hyun Jun-Soo, Ji Jae-Duk
Certification body	IT Security Certification Center(ITSCC) of National Intelligence Service

3. Security Policies

The TOE 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 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. Underlying Hardware

The underlying hardware in which the TOE is operated provides cryptographic operation to support security function and it is physically secure.

Application Note: To ensure the TOE security, IC chip is SLE66CLX800PE/M1581-e13 and SLE66CLX360PE/M1587-e13, which are certified products of CC EAL5+(SOF-high). Cryptographic operation supported by IC chip is provided by Crypto-coprocessor of the IC chip and cryptographic library which is loaded on IC chip.

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.

Application Note: The developer does not directly manage/use the TOE, and take a role in using the TOE independently of the TOE life-cycle through the development of application.

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.

Application Note: The TSF data which is leaked out of the TOE and addressed is AS.GP_Registry, and this assumes that it is securely managed between terminal and external system, in addition to between the TOE and terminal.

4.2. Scope to Counter Threats

Threat agents are generally IT entity or users that illegally accesses and abnormally damage the TOE and the assets of the internal networks. Threat agents hold basic level of professional knowledge, resources and motives.

5. TOE Information

Overall, the TOE consists of SS.NOS subsystem which communicates with underlying of Chip and SS.GPCM which handles GlobalPlatform, SS.JCVM, SS.JCLL, SS.JCRE, and SS.JCGC related to JAVA Card, and each system consists of as follows

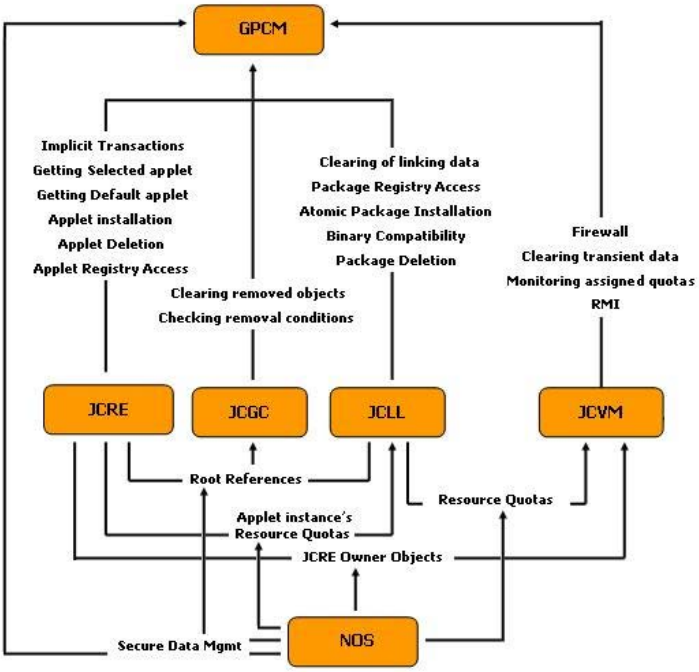

Figure 1 TOE Subsystem

The major functions of the TOE subsystem are as follows:

TOE Subsystem	Major Function
SS.NOS	The Native Operating System (NOS) provides memory management functions with separate interface to RAM and EEPROM, I/O drivers compliant with ISO standards, a low level transaction mechanism, and secure and highly efficient implementation of cryptographic functions. It uses the dedicated software, which provides interface with the integrated circuit.
SS.JCVM	The Java Card Virtual Machine (JCVM) is in charge of interpreting the bytecode of the applets according to [JCVM], and of creating, accessing and deleting class instances and arrays from the heap. It provides the entry points for launching the execution of a Java Card method from the card manager, e.g. the Applet process method when a SELECT command is received.

SS.JCLL	The Java Card Loader and Linker (JCLL) is responsible for the management of the Java Card Packages that are currently installed on the card. It provides the following services to the OPEN and the JCVM: Querying information about the currently installed packages; Accessing the bytecode of the installed packages; Managing static fields; Loading, linking or deleting a package.
SS.JCRE	The Java Card Runtime Environment (JCRE) is responsible for a collection of transversal services required by both the Java Card Virtual Machine and the applet instances. Firstly, it provides access to the native implementation of the Applet Registry. Secondly, it provides some resources that are shared by all the applet instances, such as the unique instances of the runtime exceptions that the JCVM throws, the AID objects identifying both applet instances and Java Card packages, etc. Finally, it manages the implicit transaction that is opened when a new applet instance is installed. All these services are detailed in [JCRE].
SS.JCGC	The Java Card Garbage Collector (JCGC) is responsible for the deletion of Java Card packages and applets, and for the garbage collection of inaccessible Java Card objects. The root references defining which references are accessible are provided by the other systems of the Java Card layer (JCRE, JCLL and JCVM).
SS.GPCM	Card management functions include APDU command dispatching, secure communication channels with the terminal, installation and deletion of Executable Files and applet instances, access to the information contained in the GlobalPlatform registry, enforcement of the card and applications life cycles and management of a global Cardholder Verification Method.

The design document subdivides the subsystems and describes them as Module and detailed Functionality as follows:

Sub System	Module	Functionality
SS.GPCM	M.Card Data Manager	F.Access to CPLC Data [S]
		F.Modification of the ATR Historical Bytes [S]
		F.Modification ISD's AID
		F.Initialization of the ISK(D) [S]
	M.APDUD is patcher	F.GlobalPlatform's APDU Interpreter [S]
		F.Manage a logical communication channel [S]
		F.Selects Application instance [S]
	M.LifeCycle Manager	F.Retrieving Card State [S]
		F.Management of life cycles [S]
	M.Application Installer	F.Card Content Management [S]
		F.Checking whether in Applet install or not
	M.Applet Instance Manager	F.Access to the Applet Registry [S]
		F.Querying Applet AID (s) [S]
		F.Querying Applet Privileges [S]
		F.Querying and Updating Applet State [S]
		F.Handling the Default Selected Applet [S]
	M.Load File Manager	F.Accessing the Package Registry [S]
		F.Querying Package States [S]

	M.APDU Command Processor	F.APDU Command Processing [S]
	M.Secure Messaging Manager	F.Processing of Secure Message [S]
	M.KeyRepository	F.Updating the Key Repository [S]
		F.Browsing the Key Repository [S]
		F.Getting Key Information [S]
	M.Data Store	F.Retrieving proprietary data [S]
		F.Updating proprietary data [S]
	M.GlobalPlatform API	F.Secure Channel class [S]
		F.CVM class [S]
		F.GP System class [S]
		F.Provider Security Domain class [S]
		F.OPSystem class [S]
SS.JCGC	M.Applet Deletion Manager	F.Deletion of Applets and Packages [S]
		F.Garbage Collector Initialization [S]
	M.Object Garbage Collector	F.Garbage Collection [S]
		F.Garbage Collection Request
SS.JCLL	M.CAP File Manager	F.Reading Package's Classes [S]
		F.Reading Package's Methods [S]
	M.Package Registry	F.Global AID Access [S]
		F.Package Deletion [S]
		F.Package Enumeration
		F.Package Loading [S]
		F.Package Lookup [S]
		F.Package Quotas [S]
		F.Package Status [S]
		F.Reference Enumeration [S]
	M.Static Field Manager	F.Access to Static Fields
SS.JCRE	M.AID Manager	F.Accessing AID byte array
		F.AID Creation [S]
		F.AID Deletion [S]
		F.Comparing AID bytes
		F.Current AID Access
	M.Applet Registry	F.Access to Applet Attributes [S]
		F.Applet Deletion [S]
		F.Applet Enumeration [S]
		F.Applet Installation [S]
		F.Applet lookup [S]
		F.JCRE Management [S]
		F.JCRE Reference Enumeration [S]
		F.Management of the applet's life cycle [S]
	M.Applet Selection Manager	F.Managing the Currently Selected Applet [S]
		F.Managing the Default Selected Applet
		F.Selection in Progress
	M.JCRE Exception Manager	F.Getting an Exception's Status Word
		F.Throwing JCRE Owned Exceptions
	M.Unified Transaction Manager	F.Transaction Management [S]
		F.Transaction Status [S]
	M.JavaCard API	F.Java lang

		F.Javacard Framework [S]
		F.Javacard Framework Service [S]
		F.Javacard Security [S]
		F.Javacardx Crypto [S]
		F.Java RMI
		F.Java IO
SS.JCVM	M.Array Manager	F.Access to Array Positions
		F.Array Creation [S]
		F.Checking Byte Array Access Rules [S]
	M.Byte Code Interpreter	F.Current frame access [S]
		F.Interface for Native Methods
		F.Method Interpretation [S]
		F.Operand stack initialization[S]
		F.Operands stack access [S]
	M.Class Instance Manager	F.Access to Instance Fields
		F.Class Instance Creation [S]
		F.Class Instance Deletion [S]
		F.Current Object Access
		F.Direct Access to Class Instance's Data
		F.Enumeration of References [S]
		F.Transient Data Reset [S]
	M.Remote Method Dispatcher	F.Export Flag Assignment [S]
		F.Remote Method Invocation [S]
		F.Service Selection [S]
SS.NOS	M.Boot Manager	F.TOE Initialization [S]
	M.Card holder Verification Manager	F.CVM Block And Unblock [S]
		F.CVM Create And Delete [S]
		F.CVM Initialize [S]
		F.CVM Instance Attributes [S]
	M.Cryptographic Library	F.Cryptographic Library Initialize [S]
		F.Encrypt And Decrypt [S]
		F.Message Digest [S]
		F.Random Data Generation [S]
		F.Signature Generation And Verification [S]
		F.Support Key Agreement Algorithms [S]
	M.IO Manager	F.Check Current State
		F.Managing ATR Historical Bytes
		F.Muting Card [S]
		F.Receiving And Sending Data
	M.Key Manager	F.Key Content Manager [S]
		F.KM Initialize [S]
	M.Memory Manager	F.Handle Management [S]
		F.High Level Transaction [S]
		F.Memory Allocation [S]
		F.Memory Deletion [S]
		F.Memory Reading [S]
		F.Memory Writing [S]
		F.MM Initialization [S]

		F.Object Enumeration [S]
	M.Security Manager	F.Card State Management [S]
		F.CPLC Data Initialization [S]
		F.Error Handling
		F.Module State Management [S]
		F.Read Write CPLC Data [S]
		F.SM Initialization [S]

5.1. TOE Scope

5.1.1. Physical Scope of the TOE

The TOE physically consists of CC EAL5+ IC chip hardware portion of Infineon Technology and JAVA based open smart card platform, software portion which consists of GlobalPlatform, and the TOE guidance. Among these, the IC chip which is hardware portion, is not included in scope of the TOE, and considered as the TOE operational environment.

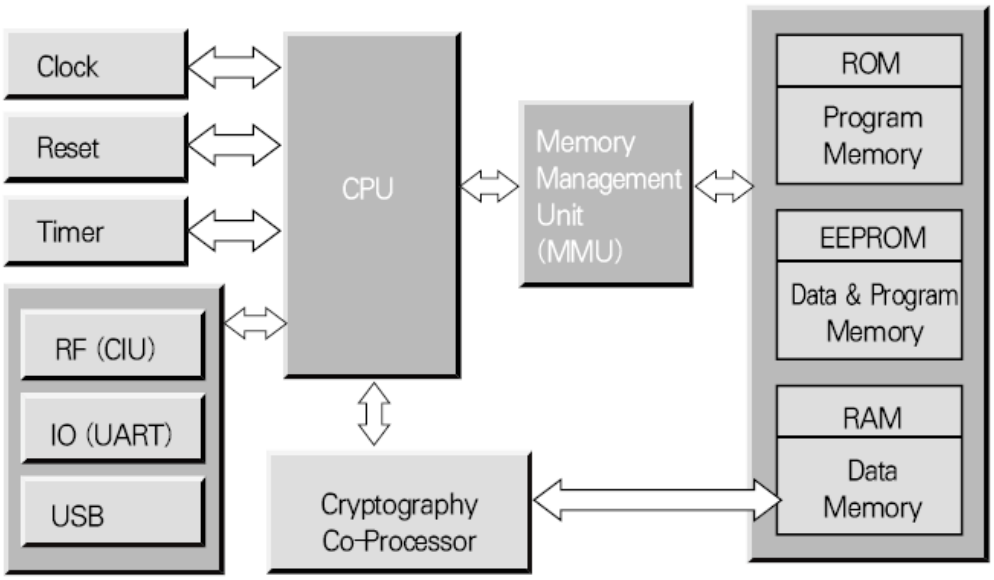

Figure 2 Physical Scope of IC Chip

Hardware is IT environment of the TOE that includes IC ship hardware and firmware and is not included in scope of the TOE. IC chip hardware include micro processor which performs executable code of the TOE; RAM, ROM, EEPROM memory which the TOE, TOE user data, and TSF data are stored in; cryptographic operation processor of DDC and ACE which support cryptographic operation of the TOE etc.

IC chip memory is protected through encryption, and IC chip hardware provides security measures against physical attack through shield, sensor, filter etc. IC chip provides security measures against attacks of SPA, DPA, EMA, DFA etc. Firmware, included in IC chip, provides management and test functions for IC chip hardware.

Software consists of Java Card-based open smart card platform and GlobalPlatform. Software exists by being masked in IC chip ROM area and works by using EEPROM, RAM memory during execution.

Application, which is loaded in the TOE, is not included in scope of the TOE, and it is stored in EEPROM to be executed. Also, user data, which is generated by application, is stored in EEPROM and RAM to be managed.

The TOE guidance describes operation, management and/or usage of the TOE and it is stored in CD-ROM in the form of PDF file with the TOE to be provided.

5.1.2. Logical Scope of the TOE

The TOE logically consists of Card Manager which performs management function, Runtime Environment which provides run time environment of application, Operating System which supports access to resource of hardware, and asset.

Card Manager is a component which performs function of smart card manager, mandates security policy of card publisher, and provides functions such as life cycle management of card and application, logical channel management with terminal, security channel

management with card manager, transmission of APDU commands to currently active applet, PIN management for card owner authentication which is shared between every applications.

● Administration Command Control

It only processes card management commands specified in [VGP] and returns proper error massages for commands which do not follow the types defined in specification. Also, it controls whether each card management commands can be processed according to state of card.

● Card Content Management

It loads, installs, and deletes application.

● Life Cycle Management

It controls life cycle of card defined in GlobalPlatform and application installed in card.

● Open Platform Environment (OPEN)

It selects, activates application and delivers received commands. Also, it initializes required internal data structure to implement card management service.

● Host Authentication (SCP02)

It is the method which authenticates host through security channel to provide authentication function of card manager. This function ensures integrity of messages which are exchanged through security channel. This function ensures confidentiality by encrypting

messages for secret information. This function deletes used session key and initiates configured security level when security channel ended.

Runtime Environment interprets bytecode which is executable code of application, and provides each application with its own separated executable areas. It supports functions related to loading, installation, deletion of application, and supports transaction, PIN management function of application own, cryptographic function, communication function, and Remote Method Invocation etc.

- Resource Quotas

It manages limitation of resource usage allowed to application.

- Java Card Firewall

It controls sharing of Java object between each application, or operational environment and application.

- Remote Access Control

It controls access of remote terminal through RMI to Java object

- Clearing Sensitive Information

It keeps residual information not being existed in allocation and return of resource

- Automic Transactions

It supports serial activities related to allocation and modification of EEPROM to only allow success of every activity or return to former situation prior to execution.

Operating System supports management function for underlying hardware resources. It provides allocation and revoke of memory like RAM and EEPROM, access to I/O devices, low level of transaction management, low level of cryptographic operation using cryptographic co-processor etc.

● CVM

It provides management for security attributes Global PIN which all applications in platform are sharing and PIN authentication function. This function supports management function for Owner PIN that application defined on its own.

● Encryption Function

It supports generation and verification of digital signature, encryption and decode, generation of hash value, and generation of random number for data.

● Encryption Algorithm

It supports RSA of 1024 bit key and TDES algorithm by using function which is provided from IC chip and library included in IC chip.

Excepted functions of the TOE

Among the functions XSmart V1.0 provides, TDES algorithm, ECDH key exchange algorithm, ECDSA digital signature generation and authentication algorithm, RSA CRT digital signature algorithm, SEED algorithm, AES algorithm, and SHA-224 algorithm, which are provided from IC chip components, are not included in the TOE.

Among the algorithms, TDES algorithm provided from DDC, which is IC chip hardware, is not included in the TOE. Retail MAC and Full Triple DES MAC algorithms use TDES algorithm, so

they also are not included in the TOE. Modulo operation, which is used for cryptographic algorithm using asymmetric key, is provided from ACE module of IC chip so not included in the TOE.

ECDH key exchange algorithm and ECDSA digital signature generation and authentication algorithm provided from ECC library also are not included in scope of the TOE. RSA algorithm also is not included in scope of the TOE. Algorithms IC provided from IC chip components are as follows:

[Algorithms of IC chip component]

Component	Algorithm
IC chip Hardware	TDES operation in DDC module Modulo operation in ACE module
ECC Library	ECDH key exchange ECDSA digital signature generation and verification

RSA CRT 2048 digital signature algorithm, SEED algorithm, ASE algorithm only completed 1st order level of function authentication, so they are excepted from the TOE.

SHA-224 algorithm is not provided from Javacard 2.2.1 API, so it is excepted from the TOE.

6. Guidance

The TOE provides the following guidance documents.

• XSmart OpenPlatform V1.0 Guidance V1.1

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 a 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 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:

8.1. Developer's Test Environment Configuration

The developer's test environment is as follows:

8.2. Evaluator's Test Environment Configuration

The evaluator configured the test environment for the independent testing

as consistent with that specified in the ST as the following figure:

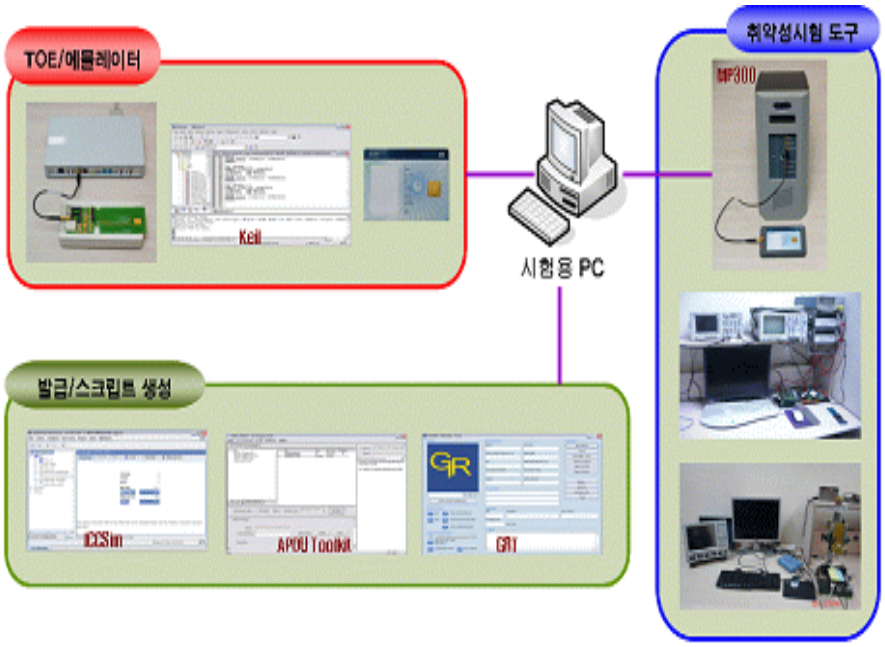

Figure 3 Evaluator's Test Environment

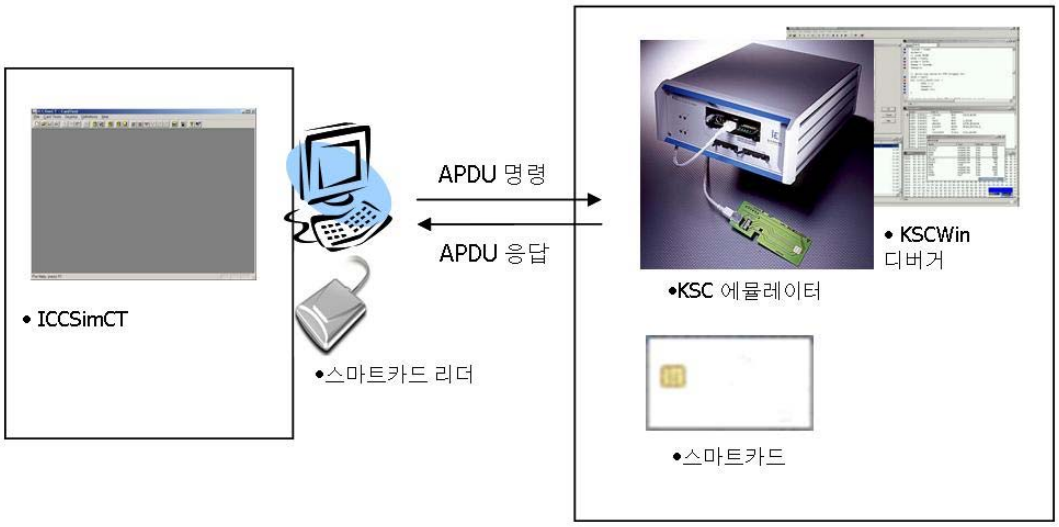

Figure 4Evaluator's Penetration Test Environment

9. Evaluation Result

The TOE conforms to the CC Part 2 and Part 3

And satisfies the EAL4 requirements

9.1. ST Evaluation (ASE)

The ST introduction correctly identifies the ST and the TOE, and accurately describes the TOE in a narrative way on three levels of abstraction level (TOE reference, TOE overview, TOE description), and these three 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 Protection Profile follows. Therefore the verdict of APE_CCL.1 is the Pass.

The Definition of Security Problem accurately defines security problems should be included in the TOE and the TOE operational environment. Therefore the verdict of ASE_SPD.1 is the Pass.

The Security Objectives adequately and completely address the security problem definition, and define security problems by clearly classifying security 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 APE_REQ.2 is the Pass.

The TOE summary specification addresses all security functional requirements, and it is consistent with other description of the TOE. Therefore, the verdict of ASE_TSS.1 is the Pass.

Therefore, the ST is appropriate and internally consistent, and suitable for use as the basis for the TOE evaluation.

9.2. Development Evaluation (ADV)

[ARC] 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.

[FSP] specifies the objective, way of using, input parameter, operation, and error message to the TSFI (SFR-enforcing, SFR-supporting, and SFR-non-interfering) with equal detail level, and accurately and completely describes the TSFI. Therefore, the verdict of ADV_FSP.4 is the Pass.

[IMP] is adequate to be used for other evaluator's analysis, and is sufficient to understand the detailed internal workings. Therefore, the verdict of ADV_IMP.1 is the Pass.

[TDS, LLD, IMP] provides background for TSF description and overall TSF description. And it provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary and a description of the internal TSF in terms of module.

Also, it also provides detailed description of the SFR-enforcing module and sufficient information about the SFR-supporting, and SFR-non-interfering modules to determine that the SFRs are completely and accurately implemented. Hence the TOE design describes the implementation representation. Therefore, the verdict of ADV_TDS.3 is the Pass.

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 TSFIs (TSF interfaces) to the extent that a reader can understand how the TSF satisfies the TSP.

Therefore, [ARC](the TSF architecture attribute which describes how to the TSF security enforcement is not compromised or bypassed), [FSP](TSF interface description), [TDS, LLD, IMP](architecture description about how the TSF behaves to execute the functions related to the claimed SFR), and [IMP](description of source code level), which are included in the development documentation, are adequate to give understanding about how the TSF satisfies the SFRs, and how these SFRs implementation are not damaged or bypassed.

9.3. Guidance Documents Evaluation (AGD)

[AGD] describes the security functionality and interface provided by the TSF by each user role, provides the guidance and guideline to use the TOE securely, addresses secure procedures for all operation modes, and makes the detection and prevention of the unsecure state of the TOE easy, and does not includes misleading or unreasonable guidance. Therefore, the verdict of AGD_OPE.1 is the Pass.

[AGD] documents the procedures and steps to prepare the TOE securely, and as a result, the TOE is structured securely. Therefore, the verdict of AGD_PRE.1 is the Pass.

Therefore, [AGD] give a suitable description of how the user can administrates the TOE in a secure way.

9.4. Life Cycle Support Evaluation (CM)

[CM] ensures that the developer clearly identifies the TOE and its associated configuration items, and that the ability to modify these items is properly controlled, and that as a result, the errors caused by the personnel's mistake or negligence in the configuration management system decrease. Therefore, the verdict of ALC_CMC.4 is the Pass.

[CM] ensures that the configuration list includes the TOE, the TOE elements, the TOE implementation representation, security flaws, and evaluation deliverables. Therefore, the verdict of ALC_CMS.4 is the Pass.

[DEL] describes all the procedures for the TOE security maintenance when the TOE is distributed to the user. Therefore, the verdict of ADO_DEL.1 is the Pass.

[ALC] ensures 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.1 is the Pass.

The evaluator has confirmed that the developer uses the TOE life-cycle model documented in the [ALC]. 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, [CM], [DEL], and [ALC], as a procedure to determine if the security procedures used while the developer implements and maintains the TOE are appropriate, properly describes the life-cycle model the developer used, configuration management, security policies used in the overall TOE development, tools and delivery activities the developer used in the overall TOE life-cycle.

9.5. Tests Evaluation (ATE)

[FUN] confirms that the TSFIs have been tested, and provides the evidence that can demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification. Therefore, the verdict of ATE_COV.2 is the Pass.

[DPT] confirms that the TSF subsystem and SFR-enforcing module behave and interact as described in the TOE design and security architecture description. Therefore, the verdict of ATE_DPT.2 is the Pass.

[FUN] confirms that the developer to demonstrate that the tests in the test documentation are performed and documented correctly. 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, [FUN] and [DPT] have confirmed that the TSF behaves as specified in design documentation and satisfied the TOE security functional requirements specified in the ST.

9.6. Vulnerability Assessment Evaluation (AVA)

The evaluator has confirmed that potential vulnerabilities cannot be misused by the attacker with strengthened-basic attack potential. Therefore, the verdict of AVA_VAN.4 is the Pass.

Therefore, the evaluator has confirmed potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods, could allow attackers to violate the SFRs.

10. Recommendations

The user that installs and operates the TOE shall comply with the followings.

In case of loading the application which is loaded in the OpenPlatform, the application shall be checked whether it threats security of the smartcard operation system and other applications.

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

Object

An entity within the TOE that contains or receives information and upon which subjects perform operations.

Attack Potential

The level of efforts for success of an attack, expressed in terms of an attacker's expertise, resources and motivation.

Iteration

The use of the same component to express two or more distinct requirements.

Security Target (ST)

An implementation-dependent statement of security needs for a specific identified TOE.

Protection profile (PP)

An implementation-independent statement of security needs for a TOE type.

Human User

See ‘external entity’

User

Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Selection

The specification of one or more items from a list in a component.

Smart Card Terminal

Device mounted with smart card reader/ recorder function as well as keypad, display and security module, etc.

Identity

A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Element

An indivisible security requirement.

Role

A predefined set of rules establishing the allowed interactions between a user and the TOE.

Operation (on a component of the CC)

Modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection.

Operation (on an object)

A specific type of action performed by a subject on an object.

External IT Entity

Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Threat Agent

An unauthorized external entity that brings assets under such threats as illegal access, modification or deletion.

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.

Assets

Entities that the owner of the TOE presumably places value upon.

Refinement

The addition of details to a component.

Organizational security policy (OSP)

A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.

Dependency

A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.

Subject

An active entity in the TOE that performs operations on objects.

Augmentation

The addition of one or more requirement(s) to a package.

Component

The smallest selectable set of elements on which requirements may be based.

Class

A grouping of CC families that share a common focus.

Target of evaluation (TOE)

A set of software, firmware and/or hardware possibly accompanied by guidance.

Evaluation assurance level (EAL)

An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

Family

A grouping of components that share a similar goal but may differ in emphasis or rigor.

Assignment

The specification of an identified parameter in a component (of the CC) or requirement.

EEPROM (Electrically Erasable Programmable Read-Only Memory)

This is non-volatile memory 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.

TOE Security Functionality (TSF)

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

TSF data

Data created by and for the TOE that might affect the operation of the TOE.

12. References

[1]Common Criteria for Information Technology Security Evaluation (Ministry of Public Administration and Security Notice No. 2008-26, 16.July. 2008)

[2]Common Criteria Part 1: Introduction and general model, CCMB-2007-09-001, Version 3.1, 2008. 7.

[3]Common Criteria Part 2: Security functional components, CCMB-2007-09-002, Version 3.1, 2008. 7.

[4]Common Criteria Part 2: Security assurance components, CCMB-2007-09-003, Version 3.1, 2008. 7.

[5]Common Methodology for Information Technology Security Evaluation, CCMB-2007-09-004, Version 3.1, 2008. 7