KECS-CR-10-59

Certification Report for KOMSCO JK11 of Korea Miniting, Security Printing & ID Card Operating Corp.

Certification No.: KECS-ISIS-0272-2010

October 2010

National Intelligence Service
IT Security Certification Center

Revision Status

#	Date of Revision	Revised Page	Description
00	Oct. 12, 2010	-	Initially prepared

This document is the Certification report on KOMSCO JK11 of the Korea Minting, Security Printing & ID Card Operating Corporation (KOMSCO).

Certification committee members:

Kim Chun-soo (National Security Research Institute)

Choi Jin-young (Korea University)

Park Chun-sik (Seoul National Women's University)

Song Jeong-hwan (Hanyang University)

Kim Seung-ju (Sungkyunkwan University)

Certification Body:

IT Security Certification Center, National Intelligence Service

Evaluation Body:

Korea Internet & Security Agency

Table of Contents

1. Summary ········ **1**

2. Identification information ········ **3**

3. Security policies ········ **5**

4. Assumptions and scope ········ **5**

4.1 Assumptions ········ 5

4.2 Threat response scope ········ 6

5. Product information ········ **7**

6. Manual ········ **9**

7. Product testing ········ **10**

7.1 Developer test ········ 10

7.2 Evaluator test ········ 10

8. Evaluation environment ········ **11**

9. Evaluation results ········ **12**

10. Recommendations ········ **6** ···· **1**

11. Definition of abbreviations and terms ········ **17**

12. References ········ **19**

1. Summary

This report describes the Certification institution's Certification results on the EAL4+ evaluation results of KOMSCO JK11 (hereinafter referred to as "TOE") based on the Common Criteria for Information Technology Security Evaluation (announced on September 1, 2009; hereinafter referred to as "CC"). This report specifies the validity and adequacy of the evaluation results.

The TOE evaluation was completed on September 15, 2010 by the Korea Internet & Security Agency (KISA). This report has been prepared on the basis of the evaluation report submitted by KISA. The product has been evaluated as "adequate" as it meets in Part 2 of CC and Part 3 of the requirements for Evaluation Assurance Level (EAL) 4 to which ATE_DPT.2 and AVA_VAN.4 are added.

TOE is a Java Card platform as an open card operating system that is used in S3CC9GC, a CC EAL4+-certified IC chip from Samsung Electronics, and S3CC9LC, a CC EAL5+-certified IC chip from Samsung Electronics.

The open card operating system that constitutes the TOE consists of JavaCard Platform V2.2.2, which provides the execution environment for applications, and Visa Global Platform V2.1.1 (hereinafter referred to as "VGP"), which offers management functions for the open card operating system, and chip OS.

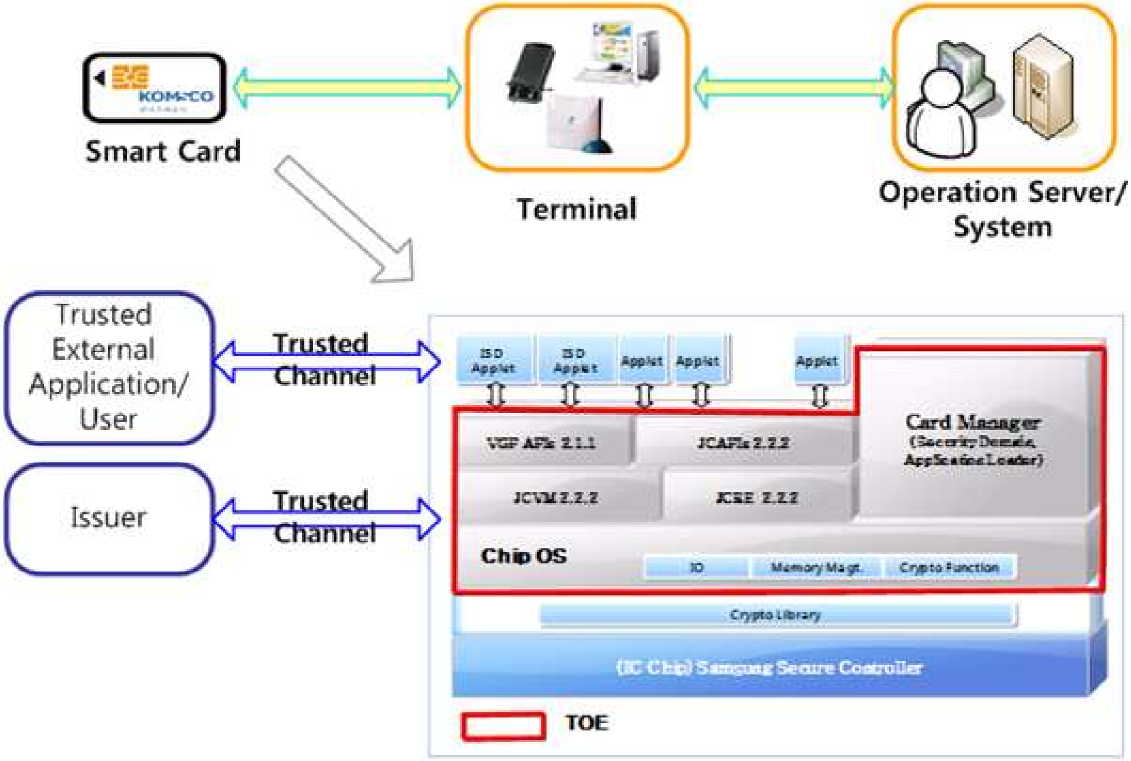
The JavaCard Platform provides cryptographic key management and cryptographic computation in addition to such functions as firewall, memory management and transaction management to ensure multiple applications coexist and interact securely with each other in a single IC chip. The components of the JavaCard Platform are JCVM 2.2.2, JCRE 2.2.2 and JCAPIs 2.2.2.

VGP provides management functions for the open card operating system, such as administrator authorization, operating system management (e.g. application loading, installation and deletion), and operating system/application lifecycle management. The components of VGP are Card Manager and VGP APIs 2.1.1.

Chip OS provides memory management for RAM and EEPROM, I/O function befitting ISO standards, low-level transaction and software-enabled cryptographic algorithm.

The sub-hardware to which the TOE is loaded is an IC chip comprised of central processing unit, cryptographic computation-dedicated processor, I/O port, memory (i.e. RAM, ROM and EEPROM) and contactless interface.

TOE can run all Java applets developed in accordance with the JavaCard v2.2.2 standard. The applets run on the TOE include: public ID card applications such as electronic resident registration card application; financial applications (e.g. cash/credit, electronic wallet, e-commerce); electronic signature applications (e.g. digital signature); and public transport card applications.



[Figure 1] TOE operational environment

The environment in which the TOE operates can be expressed as the correlation between the TOE-embedded smart card and the service system (e.g. terminal, operational server/system), as illustrated in [Figure 1].

Information needed for the service system (i.e. terminal, operational server/system) is exchanged between smart cards via the smart card terminal (contact/contactless). In other words, smart card holders and issuers generally carry out business tasks through communication with the smart card terminal. Using the issuance system and the smart card terminal, the issuers perform administrative tasks such as application installation, issuance and repair; the holders use smart card functions via the terminal. Here the smart card terminal, operational server, IC chip and TOE applications serve as the TOE operational environment.

The Certification institution has examined the evaluation activities and testing procedures of the evaluators, provided guidance on technical problems and evaluation procedures, and reviewed each unit of evaluation and the evaluation report. The institution has confirmed that the evaluation results of the product meet all the security functional requirements and assurance requirements described in the security target. Against this backdrop, the institution has authorized that the evaluators' observation and evaluation results are accurate and valid.

Scope of Certification effect: Information contained in this Certification report does not represent any approval of use or quality assurance of KOMSCO JK11 by any government agency of the Republic of Korea.

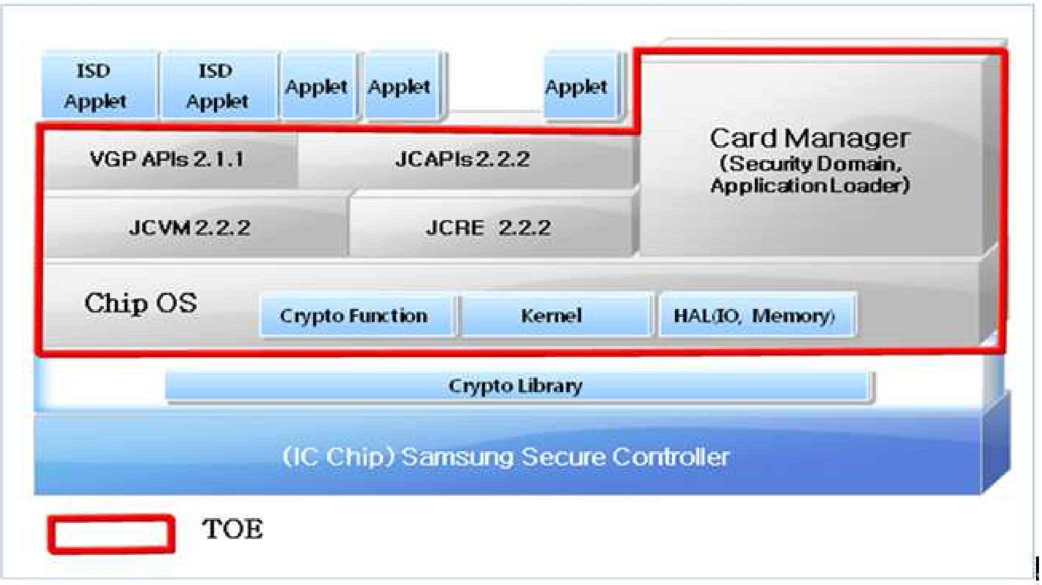
2. Identification information

[Table 1] provides information needed for the identification of the evaluated product.

[Table 1] Identification information for the evaluated product

Evaluation guidelines	Korea IT Security Evaluation and Certification Guidance (2009. 9. 1) Korea IT Security Evaluation and Certification Regulations (2010. 10. 1)
Evaluated product	KOMSCO JK11
Protection profile	Open Smart Card Platform Protection Profile V2.1(2010.6.10)
Security target	JK11 Security Target v1.3 (2010.8.6)
Evaluation report	KOMSCO JK11 V1.0 Evaluation Report V1.0 (2010.9.15)
Adequacy evaluation results	Adequate for Part 2 of Common Criteria Adequate for Part 3 of Common Criteria
Evaluation criteria	Common Criteria for Information Technology Security Evaluation V3.1 (2009. 9. 1)
Evaluation methodology	Common Evaluation Methodology for Information Technology Security Evaluation V3.1 (2009. 9. 1)
Evaluation applicant	Korea Minting, Security Printing & ID Card Operating Corporation
Developer	Korea Minting, Security Printing & IC Card Operating Corporation
Evaluator	Public Service Protection Team, Security Evaluation Headquarters, Korea Internet & Security Agency Park Hyun-mi, Yoo Hee-jun and Han Jeong-hoon (Internal experts: Lee Sung-jae, Ji Jae-deok and Hyun Jin-su)
Certification owner	National Intelligence Service IT Security Certification Center

The physical scope of the TOE is shown in [Figure 2], and the list of components included in the physical scope is provided in [Table 2].



[Figure 2] Physical scope of TOE

[Table 2] TOE components

TOE component (configuration item)	Identifier	Version	Distribution format
Open card operating system (JavaCard)	TOE name: KOMSCO JK11 TOE version: R02	-	Software (Saved in ROM)

	TOE identification:
	JK11-100C-R02(S3CC9GC)
	JK11-150C-R02(S3CC9LC)
		-	

Manual	[JK11-MA-0005] JK11 Operational User Guidance	v1.3	Documentation
	[JK11-MA-0006] JK11 Preparative Procedures	v1.2	Documentation

3. Security policies

The evaluated product is operated in a way conforming to the following security policies:

P.Open Platform

TOE should be developed as an open platform where a wide variety of applications can be loaded and used.

P.Duty Separation

The duties of responsible persons should be separated from smart card manufacturing through usage, manufacturing and managing the TOE securely depending on those duties.

4. Assumptions and scope

4.1 Assumptions

The evaluated product should be installed and run in compliance with the following assumptions:

A.Secure Channel

A secure channel is in place between the TOE and the smart card terminal as the TOE's counterparty of communication.

A.Application

Authorized procedures should be followed when installing application in the TOE. Legitimately installed applications do not contain any malicious code.

A.Underlying Hardware

The underlying hardware where the TOE operates provides cryptographic computation to support TOE security functions and is physically secure.

Application Notes: The hardware (i.e. the IC chip of a smart card) based on which the TOE operates to come up with tools to tackle physical attacks and ensure the safety of TOE includes S3CC9GC, a CC EAL4+-certified smart card IC chip from Samsung Electronics, and

S3CC9LC, a CC EAL5+-certified smart card IC chip from Samsung Electronics. Cryptographic computation supported by the IC chip is provided from the IC chip's cryptography-dedicated processor and the crypto library built in the chip, excluding the cryptographic algorithm implemented as software.

A.TOE Management

In the phases from TOE manufacturing through usage, the roles are divided into manufacturer, issuer and holder. Adequate training is provided for each role based on predetermined rules. Any repair or replacement due to TOE/smart card failure is handled in a secure manner.

A.TSF Data

TSF data sent and dealt with out of the TOE during TOE operation are securely managed.

Application Notes: TSF data processed out of the TOE are implementor key (IK) and manufacturer key (MK) used in the process of TOE initialization. They are used only during TOE initialization, so it is assumed that these keys are not leaked out to those other than the developer and the issuer (or administrator) and that they are also securely managed between the TOE and the terminal.

4.2 Threat response scope

Threat agents, in general, are IT entities and users that attempt to illegitimately access the TOE and the to-be-protected system or damage the TOE in an abnormal way. The threat agents have medium levels of expertise, resource and motivation.

5. Product information

TOE is a Java Card platform as an open card operating system that is used in S3CC9GC, a CC EAL4+-certified IC chip from Samsung Electronics, and S3CC9LC, a CC EAL5+-certified IC chip from Samsung Electronics.

The open card operating system that constitutes the TOE consists of JavaCard Platform V2.2.2, which provides the execution environment for applications, and VGP V2.1.1, which offers management functions for the open card operating system, and chip OS.

TOE's IT security functions (TSF) can be classified/summarized as below:

<table>
<tr>
<td>Security violation analysis</td>
<td>- Detects security violation events such as the check sum values of internal data, errors in resource allocation and authentication failure events and makes responses such as card function suspension and memory data deletion
- Detects violations against the check sum values of the internal major system structure (CRC32) and the check sum values of the package CAP file (SHA-1) to shut down card functions
- Security exceptions that take place during JCVM operation due to resource allocation errors or other factors are allocated to dedicated counters, suspending the functions of applets if they exceed the maximum values.
- In the event of any failure on the TOE-supported authentication protocol, the TOE is reset by force and the memory areas of relevant TSF data are deleted to prevent any reuse of resources.</td>
</tr>
<tr>
<td>Cryptographic computation</td>
<td>- Performs cryptographic computation such as cryptographic key generation/destruction, encryption, decryption, and electronic signature generation and verification (ARIC, SEED)
- Supports hash value generation and random number generation (SHA-1, SHA-256, CRC32)
<table>
<tr><th>Algorithm</th><th>Function</th></tr>
<tr><td>TDES (112, 168 bits) in ECB/CBC mode</td><td>Data encryption and decryption, data signature generation and verification
(S3CC9GC/LC: Provided by IC chip hardware)</td></tr>
<tr><td>RSA (1024, 2048 bits)</td><td>Data encryption and decryption, signature generation and verification
(S3CC9GC/LC: Provided by IC chip hardware and IC chip crypto library)</td></tr>
<tr><td>ECC (224, 256 bits)</td><td>Data signature generation and verification
(S3CC9GC: Not provided; S3CC9LC: Provided by IC chip hardware and IC chip crypto library)</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>ECDH (224, 256 bits)</td><td>Key sharing protocol
(S3CC9GC: Not provided; S3CC9LC: Provided by IC chip hardware and IC chip crypto library)</td></tr>
<tr><td>SEED (128 bits) in ECB/CBC mode</td><td>Data encryption and decryption
(S3CC9GC/LC: Provided by software)</td></tr>
<tr><td>ARIA (128, 192, 256 bits) in ECB/CBC mode</td><td>Data encryption and decryption
(S3CC9GC/LC: Provided by software)</td></tr>
<tr><td>CRC32</td><td>Integrity of TSF execution code saved in IC chip ROM</td></tr>
<tr><td>SHA-1, SHA-224/56</td><td>Hash generation for electronic signature</td></tr>
</table>
Note: The algorithms provided by the IC chip hardware support hardware accelerators for the respective algorithms and implement cryptographic functions using them.
- RSA realizes cryptographic functions with the crypto library implemented by using the modular multiplication accelerator as a hardware crypto co-processor
- ECC realizes cryptographic functions with the crypto library implemented by using the modular multiplication accelerator as an improved hardware crypto co-processor embedded in the S3CC9LC chip
</td></tr>
<tr><td>Access control</td><td>- Provides firewall access control through JCRE; prevents data from being leaked out by other applets and provides protection against hacking by isolating a single applet within the given space through the mechanism of firewall between applets</td></tr>
<tr><td>Identification and authentication</td><td>- Provides initialization authentication in the administrator mode and SCP02 authentication, DAP authentication and DM authentication in the user mode
- Initialization authentication: Confirms the administrator is authorized and initializes the TOE
- SCP02 authentication: Checks if the card issuer is an authorized one and guarantees channel safety; ensures the integrity of messages and their confidentiality through message encryption; deletes TSF data areas used upon the termination of authentication protocol and initializes the security level to ensure relevant information will not be reused
- DAP authentication: Verifies the integrity of applets and authorizes application providers using the open keys of authorized application providers for applets requiring stronger security protection
- DM authentication: When the issuer seeks to transfer the issuance authority to a second issuer, the commissioned issuer delivers information on given applets to the issuer and receives tokens for these applets before submitting them to the TOE and obtaining the issuance authority.</td></tr>
<tr><td>Security management</td><td>- Manages issues relating to security functions, security attributes, TSF data and security roles
- Compels the security policies of card issuers and provides security service through Card Manager by managing card/application lifecycles,</td></tr>
</table>

	managing security channels for protecting data transmission and data access, and managing PINs for authenticating card owners
Other TSF protection	- Performs internal tests to verify the integrity of TSF data and execution codes and provides the function of recovery to the safe state upon failure - Verifies the check sum values of patch codes and tables injected upon TOE initialization and shutting down card functions if the values are inconsistent; performs the randomness test and resets the TOE by force if any error is found when starting up the system - Verifies the check sum values of major TSF data and execution codes to suspend card functions in the event of any security violation and prevent resulting failures for recovery to the safe state upon failure; provides atomic and transaction mechanisms for Java objects within the TOE - Designs the installer as an atomic operation model to ensure that all resources allocated become free and relevant memories deleted if the installation of any applet or package is abnormally cancelled or suspended for whatever reason - Restores data to previous values and securely protects saved data through the anti-tearing mechanism when power is lost abnormally. - Encrypts major TSF data (e.g. keys, PIN) and verifies their integrity through CRC32 and hash

6. Manual

The evaluated product offers the following manuals:

- JK11 Operational User Guidance v1.3 (2010. 9. 6)
- JK11 Preparative Procedures v1.2 (2010. 8. 25)

7. Product testing

7.1 Developer test

- **Methodology**

Developers have come up with testing items considering the security functions of the product. Each testing item is described in the test document. Each of the testing items described in the test document includes the following sub-items:

- Test number/tester: Identifier of testing item and developer(s) participating in the test
- Testing purpose: Purposes of the test including to-be-tested security functions and security modules
- Testing environment: Specific testing environment for carrying out the tests
- Detailed testing procedure: Detailed procedure for testing security functions
- Expected results: Test results expected to be realized when the testing procedure is carried out
- Actual results: Test results shown when the testing procedure is actually undertaken
- Comparison between expected and actual results: Results of comparison between expected and actual results

Evaluators have examined the validity of tests such as testing environment, testing procedure, test scope analysis and detailed design test described in the test document. They have verified that the tests and test results of developers are suitable for the evaluation environment.

- **Testing environment**

The testing environment described in the test document includes the detailed environment such as configuration for testing, evaluated product, and internal/external networks. It also specifies the detailed testing environment such as testing tools needed for each testing item.

- **Testing scope analysis/detailed design test**

Detailed evaluation results are described in the ATE_COV and ATE_DPT evaluation results.

- **Test results**

The test document describes the expected and actual results of each testing item. The actual results are shown not just in the screen shots of actual product performance but also in auditing records.

7.2 Evaluator test

Evaluators have used the same evaluation environment and tools as in the developer test to install the evaluated product and test the whole of testing items provided by the developers. They have found that the actual results match the expected results in all testing items.

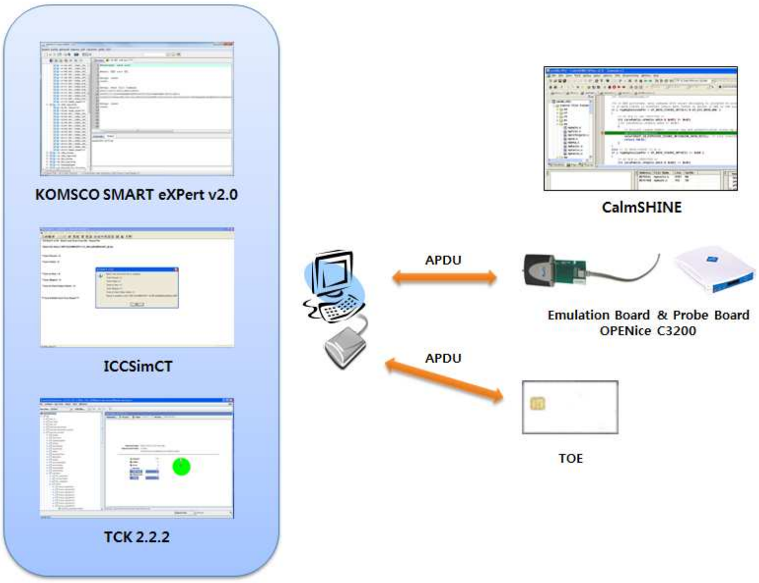
The evaluators have also devised and tested separate evaluator testing items based on the developer test and found that the actual results match the expected results.

As a result of vulnerability test, the evaluators have found that no vulnerability is available for any abuse in the evaluation environment.

The test results of the evaluators have ensured that the evaluated product works normally as described in the design document.

8. Evaluation environment

For testing purposes, the evaluators have configured the testing environment as in [Figure 3] in accordance with the environment configuration described in the security target.



[Figure 3] TOE testing environment

9. Evaluation results

The latest versions of CC and Common Evaluation Methodology have been applied to the evaluation, which has found the evaluated product to be suitable for Part 2 of CC and Part 3 of the EAL4+ Requirements. Detailed evaluation results are described in the evaluation report.

- **Security target**

Security Target Introduction accurately identifies the security target and the TOE and precisely describes the TOE at three levels of abstraction (i.e. TOE reference, TOE overview and TOE description). The three levels of description are consistent with each other, so ASE_INT.1 obtains a "pass" decision.

Conformance Claims fairly describes the conformance claims for CC that the security target conforms to, so ASE_CCL.1 obtains a "pass" decision.

Security Problem Definition clearly defines security problems that need to be dealt with in the TOE and its operational environment, so ASE_SPD.1 obtains a "pass" decision.

Security Objectives deals with the definition of security problems adequately and fully and clearly classifies security problems in the TOE and its operational environment to define security problems, so ASE_OBJ.2 obtains a "pass" decision.

As no extension components exist and evaluation activities for the work units ASE_ECD.1-1~ASE_ECD.1-13 are not applicable, ASE_ECD.1 obtains a "pass" decision.

Security requirements are clear, not vague and well-defined, ASE_REQ.2 obtains a "pass" decision.

TOE Summary Specification describes all SFRs and is consistent with other descriptive explanations of the TOE, so ASE_TSS.1 obtains a "pass" decision.

Therefore, [ST] is valid and internally consistent and is thus adequate for use as basic data for TOE evaluation.

Against this backdrop, the decision for the security target evaluation class (ASE) is "pass."

- **Development**

[ARC] is configured to prevent TSFs from being violated or bypassed and adequately specifies that TSFs providing security areas separate these areas from each other, so the ADV_ARC.1 component obtains a "pass" decision.

[FSP] accurately and fully describes TSFI (i.e. SFR-enforcing, SFR-supporting and SFR-non-interfering) by specifying purpose, method of use, input parameter, operation and error message at the same level of specification, so the ADV_FSP.4 component obtains a "pass" decision.

[IMP] is adequate for use in other evaluator analysis activities and sufficient for identifying the detailed internal operations of TSFs, so the ADV_IMP.1 component obtains a "pass" decision.

[TDS] provides overall TSF descriptions and the background for TSF descriptions, provides TOE descriptions from subsystem perspective in a way sufficient for determining the TSF boundary, and offers descriptions on the inside of TSFs from modular perspective. It also provides detailed explanations on the SFR-enforcing module and full information on the SFR-supporting and SFR-non-interfering modules to determine that SFRs have been implemented fully and accurately. The TOE design explains the expressions of implementation, so the ADV_TDS.3 component obtains a "pass" decision.

Therefore, [ARC] (TSF structural attribute explaining how not to damage or bypass TSF security execution), [FSP] (explanation on the TSF interface), [TDS] (explanation on the structure of TSF operations to perform claimed SFRs and relevant functions) and [IMP] (explanation on the level of source codes) contained in the design document are adequate to understand how TSFs satisfy SFRs and how such SFR implementation is not violated or bypassed.

Against this backdrop, the decision for the development class (ADV) is "pass."

- **Manual**

[OPE] and [PRE] explain security functionalities and interfaces that TSFs offer for each user role, provide guidance and guidelines for secure TOE use, deal with secure procedures for all operational modes, facilitate the detection and prevention of TOE insecurities, and have no room for misunderstanding or unreasonableness in place, so the AGD_OPE.1 component obtains a "pass" decision.

There is no need to apply the installation procedure as the TOE open smart card platform is already installed and distributed in operational form, but the confirmation procedure for the check sum values of ROM and EEPROM has been set as the preparative procedure to verify the integrity of the product toward the TOE after receiving the product, so the AGD_PRE.1 component obtains a "pass" decision as the procedure and phase for secure TOE preparations.

Therefore, [OPE] and [PRE] adequately describe how users can handle the TOE in a secure manner.

Against this backdrop, the decision for the manual class (AGD) is "pass."

- **Lifecycle support**

[CM] proves that developers clearly identify the TOE and its related configuration items, that the ability to modify these configuration items is adequately controlled by automated tools, and that errors from human mistakes or negligence are reduced in the configuration management system as a result, so ALC_CMC.4 obtains a "pass" decision.

[CMC] proves that the configuration list includes the TOE, TOE components, expressions of TOE implementation, security defects and evaluation report, so ALC_CMS.4 obtains a "pass" decision.

[DEL] describes all the procedures for maintaining TOE security when distributing the TOE to users, so the ALC_DEL.1 component obtains a "pass" decision.

[DVS] ensures that the security control that developers apply to the development environment to guarantee secure TOE operations are not damaged and provide confidentiality and integrity for TOE design and implementation is adequate, so the ALC_DVS.1 component obtains a "pass" decision.

It is demonstrated that developers use a documented TOE lifecycle model in [LCD], so the ALC_LCD.1 component obtains a "pass" decision.

[TAT] describes that well-defined development tools are used in TOE development and proves developers utilize well-defined development tools to produce consistent and predictable results, so the ALC_TAT.1 component obtains a "pass" decision.

Therefore, [CM], [DEL], [DVS], [LCD] and [TAT] adequately describe the lifecycle model used by developers, configuration management, security policies used throughout TOE development, and tools used and distribution activities made by developers throughout the TOE lifecycle.

Against this backdrop, the decision for the lifecycle support class (ALC) is "pass."

- **Testing**

[ATE] proves that the developers have tested TSFI and provided evidence of consistency between testing items in the test document and TSFI in the functional specification, so the ATE_COV.2 component obtains a "pass" decision.

[ATE] proves that the TSF subsystem and the SFR-enforcing module work and interact with each other as described in the TOE design and security structure description, so the ATE_DPT.2 component obtains a "pass" decision.

[ATE] proves that the developers have accurately executed and documented testing items described in the test document, so the ATE_FUN.1 component obtains a "pass" decision.

Evaluators have made independent tests on some of the TSFs and found that the TOE works as specified and have gained confidence in the test results from the developers through routine testing on the developer tests, so the ATE_IND.2 component obtains a "pass" decision.

Therefore, [ATE] demonstrates that the TSFs work as specified in the design document and in a way consistent with the TOE security functional requests described in the security target.

Against this backdrop, the decision for the testing class (ATE) is "pass."

- **Vulnerability assessment**

Evaluators have found that the potential vulnerabilities deriving from attackers with medium levels of possibility for successful attack cannot be abused in the TOE operational environment, so the AVA_VAN.4 component obtains a "pass" decision.

Therefore, the potential vulnerabilities identified during development evaluation or expected TOE operation or via other methods show that attackers cannot violate SFRs.

Against this backdrop, the decision for the vulnerability assessment class (AVA) is "pass."

10. Recommendations

Users that install and run this TOE must comply with the following recommendations:

- KOMSCO JK11 is an open JavaCard platform where user-developed applets can be loaded onto and used in the smart card. Applets and all the data used in the applets are saved in EEPROM, so it is recommended that users take additional security measures (i.e. confirmation of integrity, encryption) for important data.

- Authentication of the issuing institution should be undertaken before using the issuance commands of KOMSCO JK11; authentication protocols should be in line with the SCP02 security mechanism defined in the Global Platform V2.1.1 standard. Authentication keys for the issuing institution may be set through consultation between the TOE developer and the issuing institution, and the issuing institution may renew the keys upon issuance.

- Users of KOMSCO JK11 are divided into those in the administrator mode and the user mode. The former carries out the initialization and customizing of KOMSCO JK11, while the latter performs product personalization, application management and card issuance/disposal, so adequate user commands should be used depending on the roles of the users.

- KOMSCO JK11 provides the SEED and ARIA algorithms in software format. Application developers as users in the user mode can use SEED and ARIA functions.

11. Definition of abbreviations and terms

The following abbreviations and terms have been used in this report:

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

Smart Card Terminal
Device that contains smart card reader/recorder functions, keypad, display and security module

Authorized Issuer
Allowed user to securely operate and manage functions in accordance with TOE security policies

Authorized User
User that can run functions in accordance with security functional requirements (SFR)

Applet
Basic code that can be selected in the name of user application based on JavaCard technology for execution from outside the smart card; each applet is identified by its AID

EEPROM (Electrically Erasable Programmable Read-Only Memory)
Non-volatile memory that retains information stably for a long period of time even without power supply; modification of erasable programmable read-only memory (EPROM) where data once recorded can be electronically erased for rewriting and which can thus be useful for applications requiring program rewriting. Data are recorded and erased by electronically changing the electronic charges of devices constituting the chip. Programming can be redone while embedded in the system as electronic reading or recording are enabled

Integrated Circuit Chip
Important semiconductor to undertake smart card functions; processor including four functional units such as mask ROM, EEPROM, RAM and I/O ports

JCAPI
(JavaCard Application Programming Interface)

Interface for functions defined in the Java framework and the extended Java package used to configure JavaCard applications; JavaCard Application Programming Interface is the subset of the Java programming language

Package

Name of the Java programming language including classes and interfaces that defines user library and applets; package is divided into export and CAP files

RAM
(Random Access Memory)

Repository that maintains operating system, applications and currently used data to ensure fast access of computer processor; enables faster reading and writing than any other computer storages such as hard disk, floppy disk and CD-ROM. Data saved in RAM, however, are retained only while the computer is on and disappear when the computer is turned off. When the computer is on again, the operating system and other files in the hard disk are loaded again to RAM

ROM
(Read-Only Memory)

A sort of semiconductor memory whose content can be read but cannot be modified, as opposed to RAM which is both readable and writable; used mainly for embedding basic operational system functions and language interpreter in the computer as saved content remains intact even if the computer's power goes out

APDU

Standard communication message protocol between the card terminal and the smart card defined by ISO 7816

SCP02

Combination of secure communication protocol and security service defined in Global Platform Card Specification V2.1.1 and used to authenticate the issuance institution

CVM
(Cardholder Verification Method)

Method for checking the card issuer

DAP

Mechanism used by the security domain to verify the authentication of load file data block

DM
(Delegated Management)

Modification of pre-authorized card content carried out by the authorized application provider

12. References

The Certification institution has prepared this Certification report using the following documents:

[1] Common Criteria for Information Technology Security Evaluation (2009. 9)

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

[3] Korea IT Security Evaluation and Certification Guidance (2009. 9. 1)

[4] Korea IT Security Evaluation and Certification Regulations (2010. 10. 1)

[5] JK11 Security Target v1.3 (2010. 8. 6)

[6] KOMSCO JK11 Evaluation Report V1.0 (2010. 9. 15)