KECS-CR-13-37

KOMSCO JK21 V1.0 on S3CT9KA/KC/KW

Certification Report

Certification No.: KECS-ISIS-0468-2013

2013. 11. 8

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2013.11.08	-	Certification report for KOMSCO JK21 V1.0 on S3CT9KA/KC/KW - First documentation

This document is the certification report for KOMSCO JK21 V1.0 on S3CT9KA/KC/KW of KOMSCO.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Internet & Security Agency (KISA)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL5+ evaluation of KOMSCO JK21 V1.0 on S3CT9KA/KC/KW with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is the composite product which is consisting of the certified contact/contactless integrated circuit chip, and embedded software(IC chip operating system(COS), Java Card Virtual Machine (JCVM), Java Card Runtime Environment (JCRE), Java Card API (JCAPI), Card Manager & VGP API) in accordance with the Java Card 2.2.2 [6], [7], [8], the Global Platform Card Specification [9], and the Visa Global Platform Card Specification [10]. The TOE provides Java Card Platforms for multiple applications by allowing them to be loaded and deleted, cryptographic services to be used by applications installed on the Java Card Platform.

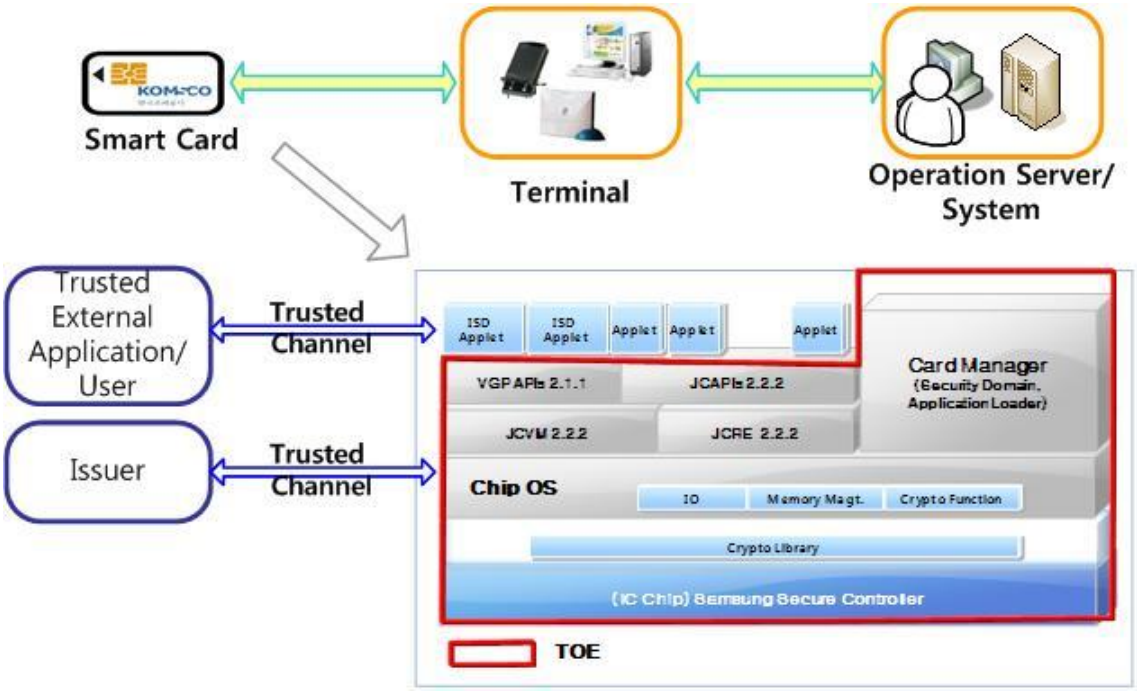
The TOE KOMSCO JK21 V1.0 on S3CT9KA/KC/KW is composed of the following components:

- IC chip S3CT9KA Revision 0 and S3CT9KC/S3CT9KW Revision 2 provided by Samsung Electronics, see BSI-DSZ-CC-0719 and ANSSI-CC-2012/70 respectively, and
- Embedded software KOMSCO JK21 V1.0 provided by Korea Minting, Security Printing & ID Card Operating Corp. (KOMSCO).

The evaluation of the TOE has been carried out by Korea Internet & Security Agency (KISA) and completed on October 31, 2013. This report grounds on the evaluation technical report (ETR) KISA had submitted [11] and the Security Target (ST) [12][13].

The ST is based on the certified Protection Profile (PP) Smart Card Open Platform Protection Profile V2.2, December 20, 2010, KECS-PP-0097a-2008 [5]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL5 augmented by ALC_DVS.2 and AVA_VAN.5. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] shows the operational environment of the TOE.



[Figure 1] Operational environment of the TOE

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE is composite product consisting of the following components and related guidance documents.

Type	Identifier	Release	Delivery Form
S3CT9KA (HW/SW)	Samsung S3CT9KA/S3CT9K7/S3CT9K3 16-bit RISC Microcontroller for Smart Card, Revision 0 with optional Secure RSA/ECC Library Version	Revision 0	IC Card (Note: The SW is contained in ROM and EEPROM.)

Type	Identifier	Release	Delivery Form
	1.0 including specific IC Dedicated Software		
	Secure RSA/ECC Library	V1.0	
	TRNG Library	V1.0	
S3CT9KC /S3CT9KW (HW/SW)	Samsung S3CT9KW/S3CT9KC/ S3CT9K9 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional secure RSA/ECC V2.2 Library including specific IC Dedicated Software	Revision 2	
	Secure RSA/ECC Library	V2.2	
	TRNG Library	V2.0	
SW	KOMSCO JK21 V1.0	Revision 1	
DOC	[JK21-MA-0005] Operational user guidance	V1.4	Softcopy Hardcopy
	[JK21-MA-0006] Preparative procedures	V1.4	

[Table 1] TOE identification

The TOE is finalized at step ⑦ of the Initialization and Issuance Phase in accordance with the Smart Card Open Platform PP [5]. The TOE can be issued by issuer after it is initialized at step ⑥ of the Manufacturing Phase or step ⑦ of the Initialization and Issuance Phase using initialization data generated by the developer.
The certified IC chip S3CT9KA which is a component of the TOE provides Deterministic Random Number Generator, it is not used by the TOE. Thus it is out of TOE scope.
For details on the chips, the IC dedicated software and the crypto libraries, see the documentation under BSI-DSZ-CC-0719 (for S3CT9KA) [14] and ANSSI-CC-2012/70 (for S3CT9KC/S3CT9KW) [15].

[Table 2] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 8, 2013) Korea Evaluation and Certification Scheme for IT Security (November 1, 2012)
TOE	KOMSCO JK21 V1.0 on S3CT9KA/KC/KW (ROM Code/EEPROM Code Revision 1) ● ROM images: JK21-140A00-R1.rom, JK21-140C02-R1.rom, JK21-142002-R1.rom ● EEPROM images: JK21-140A00-R1.eep, JK21-140C02-R1.eep, JK21-142002-R1.eep
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
EAL	EAL5+ (augmented by ALC_DVS.2 and AVA_VAN.5)
Developer	KOMSCO
Sponsor	KOMSCO
Evaluation Facility	Korea Internet & Security Agency (KISA)
Completion Date of Evaluation	October 31, 2013
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

3. Security Policy

The ST [12][13] for the TOE claims demonstrable conformance to the Smart Card Open Platform PP [10], and the TOE complies security policies defined in the Smart Card Open Platform PP [5] by security objectives and security requirements based on the Java Card 2.2.2 [6], [7], [8]. Thus the TOE provides security features defined in the Smart Card Open Platform PP [5] as follows.

- The TOE ensures the runtime environment of the Java Card System implementing logical channels. This includes the firewall policy and the requirements related to the Java Card API.

- The TOE ensures the installation of post-issuance applications. It does not address card management issues in the broad sense, but only those security aspects of the installation procedure that are related to applet execution.
- The TOE ensures erasure of installed applets from the card.
- The TOE ensures the remote method invocation feature, which provides a new protocol of communication between the terminal and the applets.
- The TOE ensures the object deletion capability. This provides a safe memory recovering mechanism.
- The TOE ensures security policies for controlling access to card content management operations and for expressing card issuer security concerns through Card Manager. Also, this contains the security requirements to fulfill GP and VGP specific objectives.
- The TOE ensures smart card platform, that is, operating system and chip that the Java Card System is implemented upon.

Furthermore, the TOE is composite product based on the certified IC chips, the TOE utilizes and therefore provides some security features covered by the IC chip certifications such as Security sensors/detectors, Active Shields against physical attacks, Synthesizable glue logic, Dedicated hardware mechanisms against side-channel attacks, Secure DES and AES Symmetric Cryptography support, Secure coprocessor for RSA and ECC Asymmetric Cryptographic Support, and a True Random Number Generator (TRNG) for AIS31-compliant Random Number Generation. For more details refer to the Security Target Lite for the IC chips [16][17].

4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the ST [13], chapter 3.4):

- There shall be a secure channel between the TOE and the IFD.
- The application program must follow approved procedure when installed into the TOE. If the application program is installed adequately, it shall not contain malicious code.
- In the steps from manufacturing to using the TOE, there are roles of

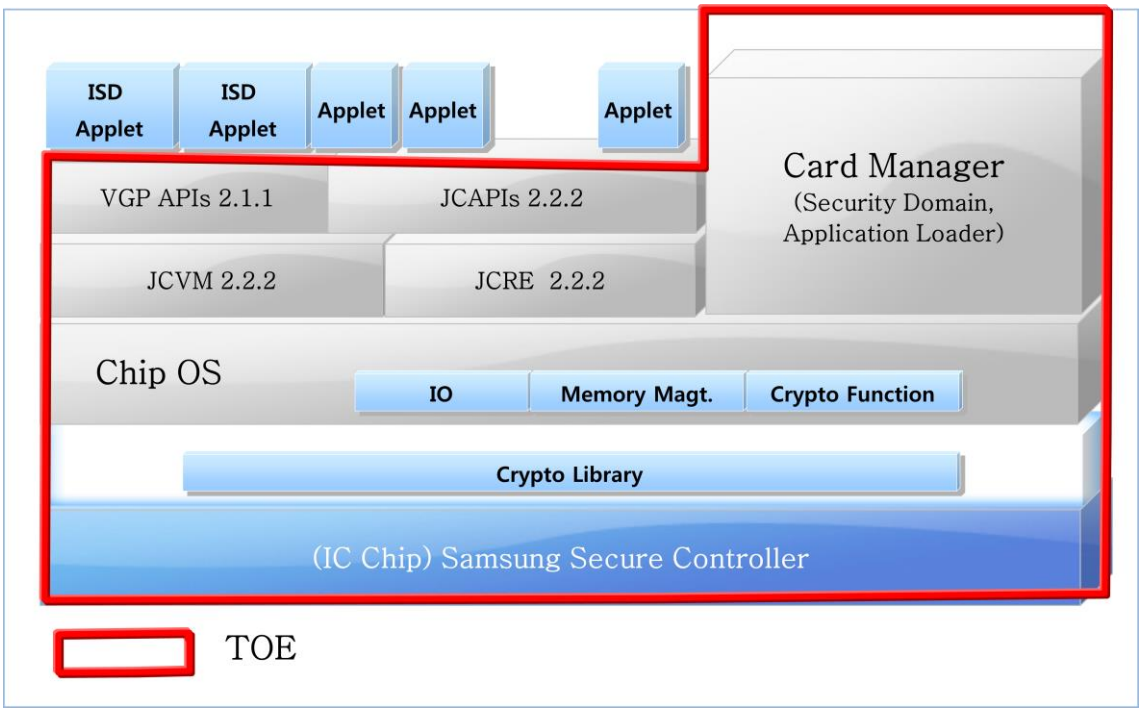
manufacturers, issuers and holders and training to each role shall be conducted in accordance with defined provisions. And the TOE is handled in a secure manner when repaired or replaced due to breakdown of the TOE or the smartcard.

- TSF data that are exposed to be processed in the course of TOE operation are managed securely.

Furthermore, some aspects of threats and organisational security policies are not covered by the TOE itself, thus these aspects are addressed by the TOE environment: TOE user training, and Secure data handling procedures etc. Details can be found in the ST [13], chapter 3.2, 3.3 and 4.2.

5. Architectural Information

[Figure 2] show the physical scope of the TOE. The TOE is the composite product which is consisting of the certified contact/contactless chip and the embedded software.



[Figure 2] Scope of the TOE

- The Card Manager controls the life cycle of the TOE and applets, and provides Key and applet management functions of TOE with administrator authority in the TOE user mode. The TOE manages applets through applet load, installation, and deletion functions and life cycle management function of Card Manager. The TOE enforces the security policy for the card issuer, and provides the security services as the secure channel management during data transaction and data access, and PIN management for Card holder authentication.
- The JCRE is responsible for the resource management for the java applet running, the selected applet management, the communication with CAD and the security of the applet. And the JCRE performs running of applets using JCVM. The JCRE includes the frameworks related to the APDU routing, ISO communication protocol, JCVM and the classes for handling. The TOE provides the firewall access control through JCRE. By isolating a single applet within the given space through the mechanism of firewall between applets, it prevents data from being leaked out by other applets and provides protection against attacks.
- The JCVM executes the CAP file as entity of the applet. It performs byte-code execution, memory allocation management, object management, security features, etc. The JCVM is byte code interpreter based on Java Card Specification. The Java Card applet's methods are converted to byte code can be performed on the JCVM. TOE can run the applet independent from the hardware through JCVM.
- JCAPI is the set of classes provided for development of application in accordance with Java Specification. JCAPI provides primary APIs and extended APIs packages, and it is the upper layer of JCRE, provides the interface for cryptographic functions and basic functions to application.
- Visa Global Platform API is Java Card Interfaces for Global Platform functions. It provides access to the OPEN, services for the application such as cardholder verification, personalization, security services and Card Content Management service such as card locking, application life cycle state update.
- The Chip Operating System is hardware abstraction layer. It is responsible for operating system to run JCVM and JCRE, and include low level I/O function, memory management function, low level transaction and crypto functions. The TOE provides the administrator mode and user mode. The TOE provides initialization authentication, SCP02 authentication in the administrator mode

and DAP authentication and DM authentication in the user mode.

- Cryptographic Library belongs to the TOE hardware, and it has been certified along with the IC chips. The primary crypto functions are implemented in the Chip Operating System, and they utilize certified cryptographic libraries implemented in the certified IC chips. The IC chips provide security features such as Security sensors/detectors, Active Shields against physical attacks, Synthesizable glue logic, Dedicated hardware mechanisms against side-channel attacks, Secure DES and AES Symmetric Cryptography support, Secure coprocessor for RSA and ECC Asymmetric Cryptographic Support, and a True Random Number Generator (TRNG) for AIS31-compliant Random Number Generation.

For the detailed description is referred to the ST [13].

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
[JK21-MA-0005] Operational user guidance	V1.4	Oct 17, 2013
[JK21-MA-0006] Preparative procedure	V1.4	Oct 21, 2013

[Table 3] Documentation

7. TOE Testing

The developer took a testing approach based on the component of the TOE and the respective specification of each component. Physically, the embedded software is not separated, but logically, it can be divided into Java card system in accordance with the Java Card 2.2.2 [6], [7], [8], card manager in accordance with Visa Global Platform Card Specification [10].

The developer conducted 2,461 tests related to the TSFI and module interface, and cryptographic functions as described below:

- The automated tools for testing whether the smartcard specifications (ISO 7816, ISO 14443) and VGP, Java Card specifications are satisfied are used to conduct the security function test and module interface test through the scenario-based script.
- The developer used an in-house testing tool for some special tests including crypto test, tear test, patch test, random number analyser test, card initialization test, delegated management test, and security audit test
- And the developer conducted additional special tests including fault attack protection mechanisms test, valid/invalid input range checking test, data object security test, Java Card native code access test, etc

The developer tested all the TSF and analyzed testing results according to the assurance component ATE_COV.2. This means that the developer tested all the TSFI defined for each life cycle state of the TOE, and demonstrated that the TSF behaves as described in the functional specification.

The developer tested both subsystems (including their interactions) and all the modules (including their interfaces), and analyzed testing results according to the assurance component ATE_DPT.3.

The evaluator performed all the developer's tests listed in this report chapter 7.1, and conducted independent testing based upon test cases devised by the evaluator.

Also, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These test cases cover testing APDU commands, perturbation attacks, observation attacks such as SPA/DPA and SEMA/DEMA, fault injection attacks, and so on. No exploitable vulnerabilities by attackers possessing high attack potential were found from penetration testing.

The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [11].

8. Evaluated Configuration

The TOE is KOMSCO JK21 V1.0 on S3CT9KA/KC/KW. The TOE is composed of the following components:

- IC chips: S3CT9KA/S3CT9K7/S3CT9K3 16-bit RISC Microcontroller for Smart Card, Revision 0 with optional Secure RSA/ECC Library Version 1.0 including

specific IC Dedicated Software (BSI-DSZ-CC-0719) and S3CT9KW/S3CT9KC/S3CT9K9 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional secure RSA/ECC V2.2 Library including specific IC Dedicated Software (ANSSI-CC-2012/70), and

- Embedded software: KOMSCO JK21 V1.0 (Revision 1)

The TOE is identified by the name, version and release version. The TOE identification information is provided by the command-response APDU following:

- Command APDU: D088000020
- Response APDU

Item	S3CT9KA	S3CT9KC	S3CT9KW	Remarks
IC fabricator	0x4250	0x4250	0x4250	Samsung Electronics
IC type	0x140A	0x140C	0x1420	chip name
IC version	0x00	0x02	0x02	chip version
OS identifier	0x4A4B	0x4A4B	0x4A4B	JK
OS release date	*[YDDD(2bytes)]*	*[YDDD(2bytes)]*	*[YDDD(2bytes)]*	*variable*
OS release level	0x2101	0x2101	0x2101	21, R1
IC fabrication date	*[YDDD(2bytes)]*	*[YDDD(2bytes)]*	*[YDDD(2bytes)]*	*variable*
IC serial number	*[number(4bytes)]*	*[number(4bytes)]*	*[number(4bytes)]*	*variable*
IC batch identifier	*[identifier(2bytes)]*	*[identifier(2bytes)]*	*[identifier(2bytes)]*	*variable*
Patch version	0x0000	0x0000	0x0000	Patch version

[Table 4] Evaluated Configuration

And the guidance documents listed in this report chapter 6, [Table 3] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [11] which references Work Packages Reports for each assurance requirement and Observation Reports.

The evaluation result was based on the CC [1] and CEM [2], and CCRA supporting documents for the Smartcard and similar device [18], [19], [20] and [21]. Also the evaluation facility utilized German scheme's Evaluation Methodology for CC Assurance Class for EAL5+ and EAL6 [23] under confirmation of the CB.

As a result of the evaluation, the verdict PASS is assigned to all assurance

components of EAL5 augmented by ALC_DVS.2 and AVA_VAN.5.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Also, the evaluator confirmed that the ST of the composite TOE does not contradict the ST of the IC chip according to the CCRA supporting document Composite Product Evaluation [18].

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer has used a documented model of the TOE life-cycle. Therefore the verdict PASS is assigned to ALC_LCD.1.

The developer has used well-defined development tools that yield consistent and predictable results, and implementation standards have been applied. Therefore the verdict PASS is assigned to ALC_TAT.2.

The developer has clearly identified the TOE and its associated configuration items, and the ability to modify these items is properly controlled by automated tools, thus making the CM system less susceptible to human error or negligence. Therefore the verdict PASS is assigned to ALC_CMC.4.

The configuration list includes the TOE, the parts that comprise the TOE, the TOE implementation representation, security flaws, development tools and related information, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.5.

The developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. Additionally, sufficiency of the measures as applied is intended be justified. Therefore the verdict PASS is assigned to ALC_DVS.2.

The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.

Also, the evaluator confirmed that the correct version of the embedded software is installed onto/into the correct version of the underlying IC chip, and the delivery procedures of IC chip and embedded software developers are compatible with the acceptance procedure of the composite product integrator according to the CCRA supporting document Composite Product Evaluation [18].

Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the life-cycle model used by the developer, the configuration management, the security measures used throughout TOE development, the tools used by the developer throughout the life-cycle of the TOE, the handling of security flaws, and the delivery activity.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is

assigned to AGD_PRE.1.
The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.
Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.
The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It provides a detailed description of the SFR-enforcing and SFR-supporting modules and enough information about the SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented; as such, the TOE design provides an explanation of the implementation representation. Therefore the verdict PASS is assigned to ADV_TDS.4.
The developer has completely described all of the TSFI in a manner such that the evaluator was able to determine whether the TSFI are completely and accurately described, and appears to implement the security functional requirements of the ST. Therefore the verdict PASS is assigned to ADV_FSP.5.
The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.
The implementation representation is sufficient to satisfy the functional requirements of the ST and is a correct realisation of the low-level design. Therefore the verdict PASS is assigned to ADV_IMP.1.
The TSF internal is well-structured such that the likelihood of flaws is reduced and that maintenance can be more readily performed without the introduction of flaws. Therefore the verdict PASS is assigned to ADV_INT.2.
Also, the evaluator confirmed that the requirements on the embedded software, imposed by the IC chip, are fulfilled in the composite product according to the CCRA

supporting document Composite Product Evaluation [18].
Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed), an implementation description (a source code level description), and TSF internals description (which describes evidence of the structure of the design and implementation of the TSF). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).
The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.2.
The developer has tested all the TSF subsystems and modules against the TOE design and the security architecture description. Therefore the verdict PASS is assigned to ATE_DPT.3.
The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.
By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.
Also, the evaluator confirmed that composite product as a whole exhibits the properties necessary to satisfy the functional requirements of its ST according to the CCRA supporting document Composite Product Evaluation [18].
Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).
The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing High attack potential in the operational environment of the TOE.Therefore the verdict PASS is assigned to AVA_VAN.5.

Also, the evaluator confirmed that there is no exploitability of flaws or weakness in the composite TOE as a whole in the intended environment according to the CCRA supporting document Composite Product Evaluation [18].

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), don't allow attackers possessing High attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_TAT.2	ALC_TAT.2.1E	PASS	PASS	
	ALC_CMS.5	ALC_CMS.5.1E	PASS	PASS	
	ALC_CMC.4	ALC_CMC.4.1E	PASS	PASS	
	ALC_DVS.2	ALC_DVS.2.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		ALC_DVS.2.2E	PASS		
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.4	ADV_TDS.4.1E	PASS	PASS	PASS
		ADV_TDS.4.2E	PASS	PASS	
	ADV_FSP.5	ADV_FSP.5.1E	PASS	PASS	
		ADV_FSP.5.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
	ADV_IMP.1	ADV_IMP.1.1E	PASS	PASS	
	ADV_INT.2	ADV_INT.2.1E	PASS	PASS	
		ADV_INT.2.2E	PASS		
ATE	ATE_COV.2	ATE_COV.2.1E	PASS	PASS	PASS
	ATE_DPT.3	ATE_DPT.3.1E	PASS	PASS	
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.5	AVA_VAN.5.1E	PASS	PASS	PASS
		AVA_VAN.5.2E	PASS		
		AVA_VAN.5.3E	PASS		
		AVA_VAN.5.4E	PASS		

[Table 5] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by

complying with the followings:

- As the memory capacity of the TOE varies depending on the IC chips, the issuing organization is recommended to refer to the user's manual provided along with the TOE and check the identification information of the TOE after acceptance of the TOE.
- The issuing organization is recommended to refer to the user's manual, provided along with the TOE during the initialization stage and verify the integrity of the ROM and EEPROM after acceptance of the TOE.
- The issuing organization must pay attention to managing the initial keys of the TOE, and is recommended to refer to the user's manual during the initialization process and insert a safe Card Issuer Key for safe communication.
- When developing applications for the TOE, the application developer is recommended to store Error Detection Codes like CRC for important data writing operations to apply a mechanism that can verify integrity, and apply the mechanism for calculating the Error Detection Codes stored for reading operations, comparing them with stored values and checking integrity.
- The issuing organization is recommended to comply with the command usage sequence, create safe channels and install applications.
- When installing applications, it is recommended to use the DAP (Data Authentication Pattern) function to assure the integrity of applications and verify the suppliers of applications.
- When developing applications, it is recommended to apply the mechanism for encrypting important data before saving it, and decoding it when reading it from the memory to protect the confidentiality of important data.
- The issuing organization is recommended to carefully verify the robustness and correctness of applications loaded in the TOE.
- The issuing organization is recommended to operate the TOE in accordance with operation environment specified in Security Target.

11. Security Target

The KOMSCO JK21 V1.0 on S3CT9KA/KC/KW Security Target v1.8, July 9, 2013 [12] is included in this report by reference. For the purpose of publication, it is provided as sanitized version [13] according to the CCRA supporting document ST sanitising for publication [22].

12. Acronyms and Glossary

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
API	Application Programming Interface
CC	Common Criteria
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
GP	Global Platform
JCAPI	Java Card API
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VGP	Visa Global Platform

Application Protocol Data Unit(APDU)	Standard communication messaging protocol between a card accepting device and a smart card
Application (Applet)	The name is given to a Java Card technology-based user application. An application is the basic piece of code that can be selected for execution from outside the card
Cardholder	The end user of a card
Card Manager	Generic term for the 3 card management entities of a GlobalPlatform card i.e. the OPEN, Issuer Security Domain and the Cardholder Verification Method Services provider
Global Platform (GP)	Global Platform, GP is an organization that has been established by leading companies from the payments and communications industries, the government sector

	and the vendor community, and is the first to promote a global infrastructure for smart card implementation across multiple industries. Its goal is to reduce barriers hindering the growth of cross-industry, multiple Application smart cards. The smart card issuers will continue to have the freedom to choose from a variety of cards, terminals and back-end systems.
JCRE	The Java Card runtime environment consists of the Java Card virtual machine, the Java Card API (JCAPI), and its associated native methods. This notion concerns all those dynamic features that are specific to the execution of a Java program in a smart card, like applet lifetime, applet isolation and object sharing, transient objects, the transaction mechanism, and so on.
JCVM	The embedded interpreter of bytecodes. The JCVM is the component that enforces separation between applications (firewall) and enables secure data sharing.
Logical channel	A logical link to an application on the card. A new feature of the Java Card System, version 2.2.2, that enables the opening of up to four simultaneous sessions with the card, one per logical channel. Commands issued to a specific logical channel are forwarded to the active applet on that logical channel.

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-004, September 2012

[3] Korea Evaluation and Certification Guidelines for IT Security (August 8, 2013)

[4] Korea Evaluation and Certification Scheme for IT Security (November 1, 2012)

[5] Smart Card Open Platform Protection Profile V2.2, December 20, 2010, KECS-PP-0097a-2008

[6] Java Card Platform, version 2.2.2 Runtime Environment (Java Card RE) Specification. March 2006. Published by Sun Microsystems, Inc.

[7] Java Card Platform, version 2.2.2 Virtual Machine (Java Card VM) Specification. Beta release, October 2005. Published by Sun Microsystems, Inc.

[8] Java Card Platform, version 2.2.2 Application Programming Interface, March 2006. Published by Sun Microsystems, Inc.

[9] GlobalPlatform Card Specification, Version 2.1.1, March 2003

[10] Visa GlobalPlatform 2.1.1 Card Implementation Requirements, Version 2.0, July 2007

[11] CC-2011-002 KOMSCO JK21 V1.0 on S3CT9KA/KC/KW Evaluation Technical Report V1.2, Nov 5, 2013

[12] KOMSCO JK21 V1.0 on S3CT9KA/KC/KW Security Target v1.8, July 9, 2013 (Confidential Version)

[13] KOMSCO JK21 V1.0 on S3CT9KA/KC/KW Security Target Lite v1.1, Oct 21, 2013 (Sanitized Version)

[14] Certification Report BSI-DSZ-CC-0719-2011 for Samsung S3CT9KA / S3CT9K7 / S3CT9K3 16-bit RISC Microcontroller for Smart Card, Revision 0 with optional Secure RSA/ECC Library Version 1.0 including specific IC Dedicated Software, May 19, 2011, BSI

[15] Certification Report ANSSI-CC-2012/70 – Samsung S3CT9KW/S3CT9KC/ S3CT9K9 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional secure RSA/ECC V2.2 Library including specific IC Dedicated Software, October 12, 2012, ANSSI

[16] Security Target Lite of Samsung S3CT9KA/S3CT9K7/S3CT9K3 16-bit RISC Microcontroller for Smart Card with optional secure RSA and ECC Library including specific IC Dedicated Software Version 1.0, April 20, 2011

[17] Security Target Lite of Samsung S3CT9KW/S3CT9KC/S3CT9K9 16-bit RISC Microcontroller for Smart Card with optional secure RSA and ECC Library including specific IC Dedicated Software Version 2.2, September 26, 2012

[18] Composite product evaluation for Smartcards and similar devices Version 1.2, CCDB-2012-04-01, April 2012

[19] Application of Attack Potential to Smartcard Version 2.8, CCDB-2012-04-002,

April 2012

[20] The Application of CC to Integrated Circuits Version 3.0 Revision 1, CCDB-2009-03-002, March 2009

[21] Requirements to perform Integrated Circuit Evaluations, Version 1.0 Revision 1, CCDB-2009-03-001, September 2009

[22] ST sanitising for publication, CCDB-2006-04-004, April 2006

[23] Application Notes and Interpretation of the Scheme (AIS), AIS 34, Version 3, BSI, March 9, 2009

[24] ISO/IEC 7816 Identification cards – Integrated circuit(s) cards with contacts

[25] ISO/IEC 14443 Identification cards – Contactless ICCs - Proximity cards