KECS-CR-15-07

KOMSCO JK31 V1.0 on M7892

Certification Report

Certification No.: KECS-ISIS-0579-2015

2015. 1. 22

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2015.01.22	-	Certification report for KOMSCO JK31 V1.0 on M7892 - First documentation

This document is the certification report for KOMSCO JK31 V1.0 on M7892 of KOMSCO.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

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 JK31 V1.0 on M7892 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 integrated circuit chip (IC chip) provided by Infineon Technologies AG and embedded software (IC chip operating system(COS), Java Card APIs (JCAPIs), Java Card Runtime Environment (JCRE), Java Card Virtual Machine (JCVM), Card Manager, and Visa Global Platform APIs (VGPAPIs)) in accordance with the Java Card Platform (Open Configuration) specifications version 2.2.2 [6][7][8], the GlobalPlatform Card Specification 2.1.1 [9], and the Visa GlobalPlatform Card Specification version 2.1.1 [10]. The TOE provides Java Card Platforms with Open Configuration for multiple applications by allowing them to be loaded and deleted, cryptographic services to be used by applications installed on the Java Card Platform.

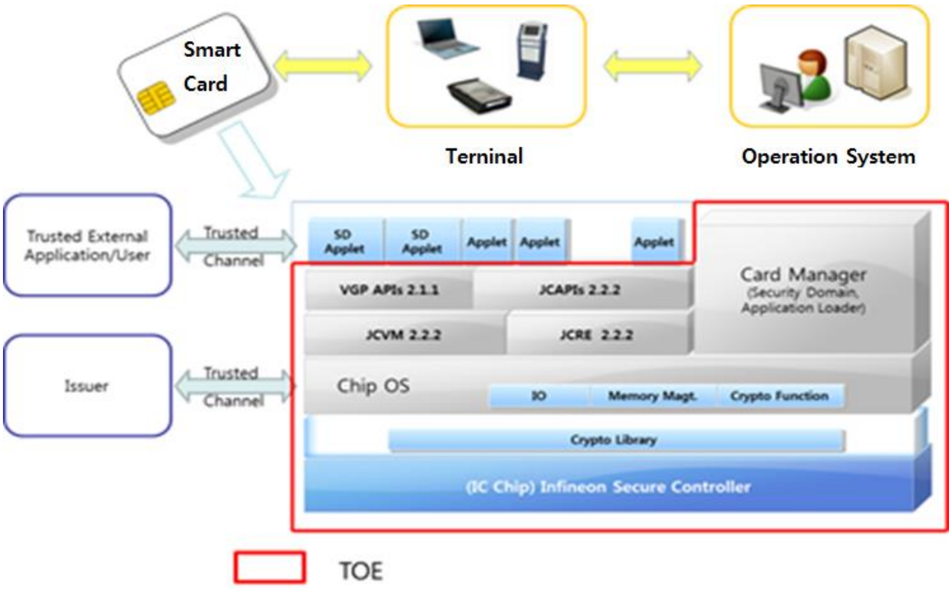
The TOE KOMSCO JK31 V1.0 on M7892 is composed of the following components:

- IC chip Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware), see BSI-DSZ-CC-0782-2012 and BSI-DSZ-CC-0782-2012-MA-01, and
- Embedded software KOMSCO JK31 V1.0 provided by Korea Minting, Security Printing & ID Card Operating CorP. (KOMSCO).

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on December 31, 2014. This report grounds on the evaluation technical report (ETR) TTA 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
HW/SW	Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, ECv1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)	B11	IC Chip Module (Note: The SW is contained in FLASH memory)

Type	Identifier	Release	Delivery Form
	RSA/EC Library	V1.02.013	
	SHA-2 Library	V1.01	
SW	KOMSCO JK31 V1.0	V1.0	
DOC	[JK31-MA-0001] Preparative procedures	V1.2	Softcopy
	[JK31-MA-0002] Operational User guidance	V1.2	

[Table 1] TOE identification

TOE is Composite product that should be considered in the Composite Product life cycle. Composite product integrator performs Composite product integration (FLASH code download into the IC chip), preparation and shipping to the personalization for the Composite product (Composite Product Integration). Then the TOE is issued by Card Issuer with applications and associated personalization data after the initialization step.

Though the certified IC chip which is a component of the TOE supports RSA with key length from 1024 bits to 4096 bits, the TOE only supports RSA with key length from 1024 bits to 2048 bits. Also, the certified IC chip provides True Random Number Generator (TRNG), the TOE uses it. For details on the chips, the IC dedicated software and the crypto libraries, see the documentation under BSI-DSZ-CC-0782-2012 [14] and BSI-DSZ-CC-0782-2012-MA-01 [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 JK31 V1.0 on M7892 – JK31-7805010B-R1 for SLE78CLFX4000PM – JK31-7859010B-R1 for SLE78CAFX4000PM
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	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	December 31, 2014
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 [5], and complies security policies defined in the Smart Card Open Platform PP [5] by security objectives and security requirements based on the Java Card Platform (Open Configuration) specifications version 2.2.2 [6][7][8], the GlobalPlatform Card Specification 2.1.1 [9], and the Visa GlobalPlatform Card Specification version 2.1.1 [10]. Thus the TOE provides security features defined in the Smart Card Open Platform PP [5] as follows:

- Loading, installation, deletion, integrity checking of application,
- Secure operation of application instances through Java Card Platform ,
- Securely clearing and destroying of sensitive information (such as keys, PIN), that is, the TOE shall ensure that no residual information is available and protect sensitive information that is no longer used,
- Safe data recovery or deletion (atomic transactions) when abnormal event (e.g. tearing at installation procedure) is occurred.

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 certification such as security sensors, protection against physical proving, malfunctions, physical manipulations and abuse of functionality, against leakage of information of

AES, Triple-DES, RSA, EC, and TRNG for AIS31-compliant Random Number Generation. Therefore, the TOE maintains the integrity and the confidentiality of data stored in the memory or of security functionalities provided by the TOE. For more details refer to the Security Target Lite for the IC chip [16][26].

4. Assumptions and Clarification of Scope

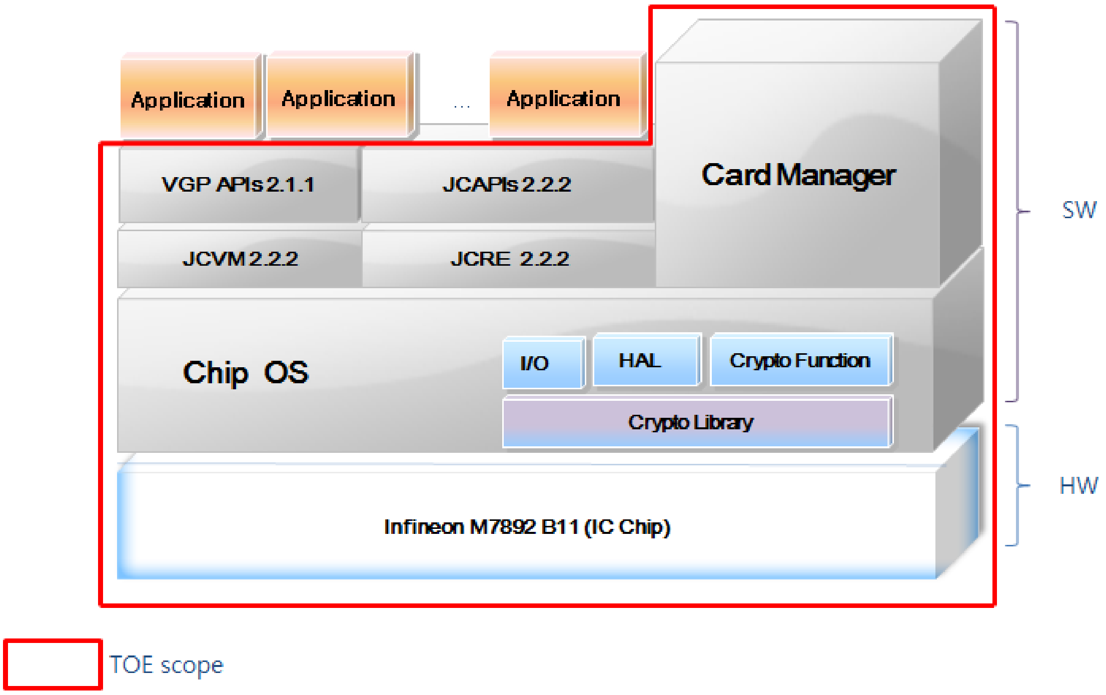
The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the ST [12][13], chapter 3.3):

- There shall be a secure channel between the application installed in the TOE and the CAD (Card Acceptance Devices).
- The application which is installed in the manner of approved procedure (e.g. bytecode verification before loading and installation) shall not include malicious code.
- At all of phases from the manufacturing to the use of the TOE, the training is provided to each role (such as manufacturer, issuer and cardholder) according to related regulations. And the TOE is handled in the secure manner when repairing and replacing due to the breakdown.
- The TSF data that is exposed to outside of the TOE is managed securely.
- Security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use). This means that the Phases after TOE Delivery are assumed to be protected appropriately.

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, secure channels, trustworthy applications, secure TSF data management, etc. Details can be found in the ST [12][13], chapter 3.2, 3.3 and 4.2.

5. Architectural Information

[Figure 2] shows the physical scope of the TOE. The TOE is the composite product which is consisting of the certified IC chip and the embedded software.



[Figure 2] Physical 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. 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 verification.
- 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 execution of applets using the 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 the 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 bytecode execution, memory allocation management, object management, security features, etc. The JCVM is the bytecode interpreter based on Java Card Specification. The Java Card applet's methods are converted to bytecode that can be performed on the JCVM. The TOE can execute the applet independent from the hardware through the JCVM.
- The JCAPIs are the set of classes provided for development of application in accordance with Java Card specification. The JCAPIs placed in an upper layer than the JCRE provide primary APIs and extended API packages, e.g., the interfaces for cryptographic functions and basic functions to the application.
- The VGPAPIs are defined by Java Card interfaces for Global Platform functions. They provide access to the OPEN (Global Platform Environment), 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 (COS) is responsible for the operating system to execute the JCVM and the JCRE, and includes low level I/O functions, memory management functions, low level transaction and crypto functions. Cryptographic Library belongs to the TOE hardware and has been certified together with the IC chip at CC EAL 6+. The primary crypto functions are implemented in the COS and support TDES, AES, RSA, ECC, SHA, and TRNG. The certified symmetric crypto processor serves TDES and AES algorithms. RSA and ECC algorithms are offered by the certified cryptographic co-processor and cryptographic libraries for all common public key algorithms. The symmetric ciphers ARIA and SEED (which have been adopted by most of the security systems in the Republic of Korea) are implemented in software using native APIs. A true random number generator (TRNG) is able to supply the CPU with true random numbers in order to fulfill the quality defined in the AIS31-compliant random number generation.

For the detailed description is referred to the ST [12][13].

6. Documentation

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

Identifier	Release	Date
[JK31-MA-0001] Preparative procedures	V1.2	December 18, 2014
[JK31-MA-0002] Operational User guidance	V1.2	December 18, 2014

[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 Platform and card manager in accordance with the Java Card Platform 2.2.2 [6][7][8], the GlobalPlatform 2.1.1 [9] and the Visa GlobalPlatform 2.1.1 [10], respectively.

The developer conducted 2,370 test cases related to the TSFIs and module interfaces, and cryptographic functions as described below:

- The automated tools for testing, whether the smartcard specifications (ISO/IEC 7816, ISO/IEC 14443) and GP/VGP, Java Card specifications are satisfied, are used to conduct the security function tests and module interface tests through the scenario-based scripts.
- The developer used an in-house testing tool for some special tests including crypto test, tear test, card initializations test, delegated management test, and security audit test.
- The developer conducted additional special tests including fault attack protection mechanisms test, memory range checking test, secure object (key, PIN) integrity checking test, cryptographic key deletion test, and forcing card reset test.

The developer tested all the TSF and analyzed testing results in accordance with 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 TSFI behaves as described in the functional specification.

The developer tested both subsystems (including their interactions) and modules (including their interfaces), and analyzed testing results in accordance with the assurance component ATE_DPT.3.

The developer correctly performed and documented the tests in accordance with the assurance component ATE_FUN.1.

The evaluator performed all the developer's tests listed in this report chapter 7, and had conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests. The tests cover preparative procedures in accordance with the guidance. Some tests were performed by design and source code analysis to verify fulfillment of the requirements of the underlying platform to the COS and Application. The implementation of the requirements of the platform's ETR and guidance was verified by the evaluators.

Also, the evaluator conducted vulnerability analysis and penetration testing based upon test cases devised by the evaluator resulting from the independent, methodical 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 JK31 V1.0 on M7892 which is composite product consisting of the following components:

- IC chips : Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, ECv1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) (BSI-DSZ-CC-0782-2012 and BSI-DSZ-CC-0782-2012-MA-01)
- Embedded software : KOMSCO JK31 V1.0

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

- Command APDU : D088000000
- Response APDU: 8100 7805 4A4B 4328 3101 xxxxxxxx 9000 or 8100 7859 4A4B 4328 3101 xxxxxxxx 9000
  - IC fabricator : 0x8100 (Infineon)

- IC type : 0x7805 (SLE78CLFX4000PM) or 0x7859 (SLE78CAFX4000PM)
- OS identifier : 0x4A4B (JK)
- OS release date : 0x4328 (YDDD)
- TOE version : 0x3101 (JK31 V1.0)
- 9000 : Response APDU Status Word

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 Package 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 [17][18][19][20][21][22].

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 in accordance with the CCRA supporting document Composite Product Evaluation [17].

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 (e.g. programming languages or computer-aided design (CAD) systems) 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 in accordance with the CCRA supporting document Composite Product Evaluation [17].

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. Also, the evaluator confirmed that the requirements in accordance with the CCRA supporting document ADV_ARC Evaluation [21], [22].

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 in accordance with the CCRA supporting document Composite Product Evaluation [17].

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 in accordance with the CCRA supporting document Composite Product Evaluation [17].

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 in accordance with the CCRA supporting document Composite Product Evaluation [17][18][19][20].

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	Assurance	Evaluator	Verdict

Class	Component	Action Elements	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	
		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	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		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 4] 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 TOE is the composite product consisting of IC chip and smart card open platform, the TOE is generated by downloading the card open platform software on the IC chip hardware at the Manufacturing Phase. The scope of this evaluation is limited to delivering the TOE to card issuer. The delivery between card manufacturer, card issuer, final user (card holder) falls outside the scope of this evaluation. Thus, the TOE user including card manufacturer and card issuer shall establish the secure delivery and acquisition process after the Manufacturing Phase.
- In the Initialization and Issuance Phase (initialization, issue, and loading application) and the Use Phase (loading application), if secure communication is not used, the TOE user shall establish physical, procedural, and personnel security measures which can guarantee the reliability for transmission.
- As the TOE supports SLE78CLFX4000PM and SLE78CAFX4000PM as a secure IC chip platform, it is recommended to refer to the user’s manual provided along with the TOE and check the identification information of the TOE.

- When accepting the TOE, it is recommended that the TOE user shall verify the integrity of the Flash code and data according the user’s manual provided along with the TOE.
- As the non-TSF cryptographic functions cannot satisfy the requirement for resistance to high attack potential for vulnerability analysis of AVA_VAN.5, the TOE user shall not use them to protect important asset except for the use only for compatibility with the VGP/GP specifications.
- The application provider shall carefully verify that any malicious code is inserted in applications loaded in the TOE.
- It is recommended that the TOE user shall establish security measures to manage the TSF data securely when the TSF data (key, PIN, and so on) is processed in outside of operational environment of the TOE.

11. Security Target

The KOMSCO JK31 V1.0 on M7892 Security Target V1.2, December 19, 2014 [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 [23].

12. Acronyms and Glossary

APDU	Application Protocol Data Unit
API	Application Programming Interface
CAD	Card Acceptance Device
CC	Common Criteria
DAP	Data Authentication Pattern
EAL	Evaluation Assurance Level
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
TSFI	TSF Interface

Applet Firewall	The mechanism that prevents unauthorized accesses to objects in contexts other than currently active context
Application Provider	Entity that owns an application and is responsible for the application's behavior
Bytecode	Machine-independent code generated by the compiler and executed by the Java virtual machine
CAD	The device where the card is inserted, and which is used to communicate with the card
CAP file	The CAP file is produced by the Converter and is the standard file format for the binary compatibility of the Java Card platform
Card Issuer	Entity that owns the card and is ultimately responsible for the behavior of the 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
Cardholder	The end user of a card
Cardholder Verification Method(CVM)	A method to ensure that the person presenting the card is the person to whom the card was issued
Context	A context is an object-space partition associated to a package. Applets within the same Java technology-based package belong to the same context
DAP Verification	The Mechanism used by Security Domain to verify that the Load File Data Block is authenticated
Delegated Management	Pre-authorized Card Content changes performed by an approved Application Provider
GlobalPlatform Registry	A container of information related to Card Content management
Issuer Security Domain	On-card entity providing support for the control, security, and communication requirements of the Card Issuer

JCRE	The runtime environment under which Java programs in a smart card are executed
JCVM	The embedded interpreter of bytecodes
Life Cycle State	A specific state within the Life Cycle of the card or of Card Content
Load File	A file transferred to a GlobalPlatform card that contains a Load File Data Block and possibly one or more DAP Blocks
Open Platform Environment (OPEN)	The central on-card administrator that owns the GlobalPlatform Registry
Package	A package is a namespace within the Java programming language that may contain classes and interfaces
SCP02	A secure communication protocol and set of security services

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] Runtime Environment Specification, Java Card Platform, Version 2.2.2, March 2006

[7] Virtual Machine Specification, Java Card Platform, Version 2.2.2, March 2006

[8] Application Programming Interface, Java Card Platform, Version 2.2.2, March 2006

[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] TTA-CCE-14-008 KOMSCO JK31 V1.0 on M7892 Evaluation Technical Report V1.3, January 12, 2015

[12] KOMSCO JK31 V1.0 on M7892 Security Target V1.2, December 19, 2014 (Confidential Version)

[13] KOMSCO JK31 V1.0 on M7892 Security Target Public Version V1.0, January 14, 2015 (Sanitized Version)

[14] Certification Report BSI-DSZ-CC-0782-2012 – Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, ECv1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)

[15] Assurance Continuity Maintenance Report BSI-DSZ-CC-0782-2012-MA-01 - Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware), 5 September 2013

[16] Security Target Lite M7892 B11 Version 1.1, August 28, 2012

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

[18] Application of Attack Potential to Smartcard Version 2.9, CCDB-2013-05-002, May 2013

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

[20] Requirements to perform Integrated Circuit Evaluations, Version 1.1, CCDB-2013-05-001, May 2013

[21] Security Architecture requirements (ADV_ARC) for smart cards and similar devices Version 2.1, CCDB-2014-04-001, April 2014.

[22] Security Architecture requirements (ADV_ARC) for smart cards and similar devices Version 2.0 – Appendix 1, CCDB-2012-04-004, April 2012.

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

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

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

[26] Maintenance Security Target Lite M7892 B11 Version 1.4, August 26, 2013