KECS-CR-25-33

KOMSCO JK62 V1.1

Certification Report

Certification No.: KECS-ISIS-1370-2025

2025. 9. 30.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2025.09.30	-	Certification report for KOMSCO JK62 V1.1 - First documentation

This document is the certification report for KOMSCO JK62 V1.1 of KOMSCO.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Testing Certification (KTC)

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 JK62 V1.1 with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1][22]. 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 Technology AG and embedded software (IC chip operating system(COS), Java Card APIs (JCAPIs), Java Card Runtime Environment (JCRE), Java Card Virtual Machine (JCVM), and Card Manager) in accordance with the Java Card Platform (Open Configuration) specifications version 3.0.4 [5][6][7] and the GlobalPlatform Card Specification 2.3.1 [8]. 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.

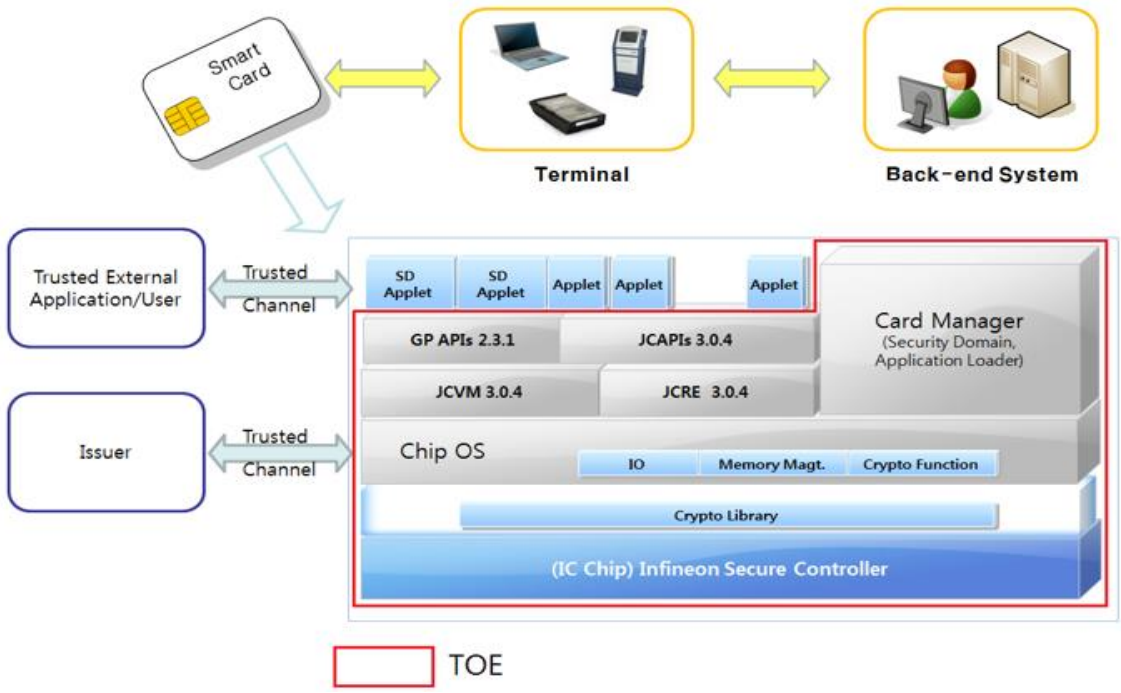
The TOE KOMSCO JK62 V1.1 is composed of the following components:

- IC chip: Infineon Security Controller IFX_CCI_000005h in the design step H13 with optional RSA2048 v2.09.002, EC v2.09.002 and HSL v03.12.8812 libraries and with specific ID dedicated software (firmware) (BSI-DSZ-CC-1110-V7-2024), and
- Embedded software: KOMSCO JK62 COS V1.1 provided by Korea Minting, Security Printing & ID Card Operating Corp.(KOMSCO).

The evaluation of the TOE has been carried out by Korea Testing Certification (KTC) and completed on September 30, 2025. This report grounds on the evaluation technical report (ETR) KTC had submitted [9] and the Security Target (ST) [10][11].

The ST is based on the certified Protection Profile (PP) Smart Card Open Platform Protection Profile V2.2, 20 December 2010, KECS-PP-0097b-2008 [13]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC:2022 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:2022 Part 3 conformant. The Security Functional Requirements (SFRs) are based upon the functional components in CC:2022 Part 2. The TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC:2022 Part 2 conformance.

[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
TOE	KOMSCO JK62 V1.1 (JK62-160C070D-R3/ JK62-160F070D-R3)	V1.0	COB / Hand Delivery
HW	Infineon SLC52GDL448(A2) (IFX_CCI_000005h)	HW Version: H13 FW Version:	COB / Hand Delivery

Type	Identifier	Release	Delivery Form
		80.100.17.3	
Embedded SW	KOMSCO JK62 COS V1.1 (RSA2048 v2.09.002, EC v2.09.002, HSL v03.12.8812 library included) (JK62-160C070D-R3.hex/ JK62-160F070D-R3.hex)	V1.1	Flash code / Infineon Developer Center Upload
DOC	[JK62-MA-0001] Preparative procedures	v2.3	Softcopy or Hardcopy/PGP email or Hand Delivery
	[JK62-MA-0002] Operational user guidance	v2.3	

[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) and shipping to End User. Then the TOE is issued by End User (e.g, 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 2048 bits to 4096 bits, the TOE only supports RSA with key length 2048 bits. Also, the certified IC chip provides Hybrid Random Number Generator (HRNG) and True Random Number Generator (TRNG), the TOE uses both. For details on the chips, the IC dedicated software and the crypto libraries, see the documentation under BSI-DSZ-CC-1110-V7-2024 [14].

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

Scheme	Korea IT Security Evaluation and Certification Guidelines (Ministry of Science and ICT Guidance No. 2022-61) Korea IT Security Evaluation and Certification Regulation (Ministry of Science and ICT·ITSCC, May 17, 2021)
TOE	KOMSCO JK62 V1.1 - Flash image: JK62-160C070D-R3.hex/JK62-160F070D-R3.hex
Common Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-

	2022-11-005, November 2022 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2024-002 Version 1.1, July 2024
EAL	EAL5+ (augmented by ALC_DVS.2 and AVA_VAN.5)
Developer	KOMSCO
Sponsor	KOMSCO
Evaluation Facility	Korea Testing Certification (KTC)
Completion Date of Evaluation	September 30, 2025
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

3. Security Policy

The ST [10][11] for the TOE claims demonstrable conformance to the Smart Card Open Platform PP [13], and complies security policies defined in the Smart Card Open Platform PP [13] by security objectives and security requirements based on the Java Card Platform (Open Configuration) specifications version 3.0.4 [5][6][7] and the GlobalPlatform Card Specification 2.3.1 [8]. Thus the TOE provides security features defined in the Smart Card Open Platform PP [13] 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 chip, 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, HRNG, 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 [15].

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 [10][11], chapter 3.4):

- 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 [10][11], 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] Architecture of the TOE

- The Card Manager controls the TOE and applets Life Cycles, and provides Key and applet management functions of TOE with administrator authority in the TOE user mode. The TOE manages applets through applet's load, install and delete functions and life cycle management function of Card Manager. The TOE enforces the security policy of 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 during java applet running, the selected applet management, the communication with CAD and the security of applet. And the JCRE performs running 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 hacking. And it prevents unauthorized access about field or method of an instance of a class, as well as length or the contents of an array. Applet Firewall is considered the primary security feature.
- 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 Javacard Specification 3.0.4 appropriately designed for the smart card system and the Java language subset.

The Javacard applet's methods are converted to byte code can be performed on the JCVM. The process that converts it into machine code that can be understood by the hardware referred to as interpreting. TOE can run the applet independent from the hardware through JCVM.

- The JCAPIs are the set of classes provided for development of application according to Java Specification. JCAPI provides primary APIs and extended APIs packages according to JCAPIs 3.0.4. JCAPIs provide the interface for cryptographic functions and basic functions of application. TOE performs cryptographic computation such as cryptographic key generation/destruction, encryption, decryption, and electronic signature generation and verification. It also supports hash value generation and random number generation. The TOE provides these functions for applications through the interface of JCAPI 3.0.4
- The GP APIs are Javacard Interfaces of Global Platform function. 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 serves as a Hardware Abstraction Layer, implementing low-level ISO-compliant I/O functions, memory management functions for RAM and FLASH memory, low-level transaction functions, and cryptographic functions. It operates as the underlying system to run both the Java Card Virtual Machine (JCVM) and the Java Card Runtime Environment (JCRE). The TOE (Target of Evaluation) has two modes: Administrator Mode and User Mode. In Administrator Mode, the initialization authentication is provided by the Chip Operating System, which verifies the identity of an authorized administrator and performs TOE initialization. In User Mode, the TOE supports SCP02, SCP03, DAP, and DM authentications. The Cryptographic Library is compiled and built together with the TOE. It is a library certified at CC EAL6+ assurance level, developed by the smart card chip vendor along with the IC chip.

  The supported cryptographic functions include:

  - RSA, ECC

  These cryptographic algorithms are implemented using a cryptographic library built on the hardware crypto co-processor, specifically a modular multiplication accelerator. These functions are implemented within the Chip Operating System's Crypto Functions, and are made available via JCAPIs. TDES and AES are implemented using both the hardware accelerator and software. RSA

and ECC are supported through cryptographic functions that rely on the crypto co-processor via the certified cryptographic library.CRC is supported natively by the IC chip hardware. Additionally, software-based implementations of cryptographic algorithms such as SEED, ARIA, and SHA are also supported.

- The IC chip is the Infineon SLC52GDL448(A2), and it is equipped with the KOMSCO JK62 COS V1.1. The following summarizes the functions supported by the IC chip are utilized in the composite TOE.

The functions supported by IC chip		TOE usage
Security Related Features	・TDES (scope : 112, 168 bits) (provided in SLC52 IC hardware)	Use (112, 168 bits)
	・AES (scope : 128, 192, 256 bits) (provided in SLC52 IC hardware))	Use (128, 192, 256 bits)
	・RSA (scope : 2048 ~ 4096 bits) (provided in RSA2048 v2.09.002 Cryptographic library)	Use (2048 bits)
	・ECC (scpoe : 192 ~ 521 bits) (provided in EC v2.09.002 Cryptographic library)	Use (192 ~ 521 bits)
	・Hash (scope : SHA 224 ~ 512 bits) (provided in software)	Use (224 ~ 512 bits)
	・CRC	Use
	・HRNG(Hybrid Random Number Generator) ・TRNG(True Random Number Generator)	Use
	・Filters & Sensors	Use
	・Memory management (MMU, MED)	Use
	・Timer & WDT	Use
	・Control (ICO, ITP/PEC 등)	Use
Communication Features	・ISO7816 Contact Interface	Use
	・ISO14443 TypeA/TypeB RF Interface	Use
	・NRG Interface	Use

[Table 3] Supported algorithms and their usages

For the detailed description is referred to the ST [10][11].

6. Documentation

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

Identifier	Release	Date
[JK62-MA-0001] Preparative procedures	v2.3	June 4, 2025
[JK62-MA-0002] Operational user guidance	v2.3	June 4, 2025

[Table 4] 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 JavaCard Platform 3.0.4 [5][6][7], and the GlobalPlatform 2.3.1 [8], respectively.

The developer conducted 1,560 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, 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 all the modules (including their interfaces), and analyzed testing results according to 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, malicious application, 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 [9].

8. Evaluated Configuration

The TOE is KOMSCO JK62 V1.1 which is composite product consisting of the following components:

- IC chips: Infineon Security Controller IFX_CCI_000005h in the design step H13 with optional RSA2048 v2.09.002, EC v2.09.002 and HSL v03.12.8812 libraries and with specific ID dedicated software (firmware) (BSI-DSZ-CC-1110-V7-2024), and
- Embedded software: KOMSCO JK62 COS V1.1.

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 160C 4A4B 4245 **6203** XX XX XX XX XX XX XX XX 00 00 90 00

  - 8100 160F 4A4B 4245 **6203** XX XX XX XX XX XX XX XX 00 00 90 00
  - IC fabricator: 0x8100 (Infineon)
  - IC type: 0x160C (SLC52GDL448) / 0x160F (SLC52GDL448A2)
  - OS identifier: 0x4A4B (JK)
  - OS release date: 0x4245 (202Y, DDD: Start on Jan. 1st)
  - TOE version: 0x6203 (JK62 R3)
- Command APDU: D088000900
- Response APDU: **070D 80100173 209002 20A3**
  - IC Version: 0x070D (H13)
  - Firmware Version: 0x80100173 (80.100.17.3)
  - Crypto Library Version: 0x2070033420 (v2.09.002)
- Command APDU: D088000C00
- Response APDU:

  - CD **16** 33 8802 **0013000F** 0000 **070D** XXXX XXXXXX XX XXXX XXXX 6B6F **80100173** 82030301 92032103 0A 01 **000005** 1102141F0B060000000000000000000000000000000000000000000009000

  - Platform Identifier: 0x16
  - IC Type:

0x0013000C (SLC52GDL448) / 0x0013000F (SLC52GDL448A2)

- IC Design Step (Chip version): 0x070D (H13)
- IC Firmware Version: 0x80100173 (80.100.170.3)
- Infineon CC product number: 0x000005 (IFX_CCI_000005h)

And the guidance documents listed in this report chapter 6, [Table 4] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [9] which references Work Package Reports for each assurance requirement and Observation Reports.
The evaluation result was based on the CC [1][22] and CEM [2][22], and CCRA supporting documents for the Smartcard and similar device [16][17][18][19][20][21].
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 describe show the ST and the TOE conform to the CC and how the STs are to claim conformance with the PP or PP-Configuration. 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 assignedto ASE_OBJ.2.
The Extended Components do not exist. 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.
The consistency of composite product ST and its related base component ST has been confirmed. Therefore, the verdict PASS is assigned to ASE_COMP.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 [16].
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.
The correct version of the dependent component was installed on the correct version of the base component. The delivery procedures of the base and dependent component developers are compatible with the composite product integrator’s acceptance procedures. Therefore, the verdict PASS is assigned to ALC_COMP.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 [16].
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 can not 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.
The requirements for the dependent component imposed by the base component have been confirmed to be met in the composite product. Therefore, the verdict PASS is assigned to ADV_COMP.1.
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 [16].
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 can not 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 theTOE 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.

The composite product as a whole was confirmed to exhibit the necessary attributes to satisfy the functional requirements of the composite ST. Therefore, the verdict PASS is assigned to ATE_COMP.1

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 [16].

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.

The composite TOE as a whole was confirmed to be free of exploitable flaws or vulnerabilities within its intended environment. Therefore, the verdict PASS is assigned to AVA_COMP.1.

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 [16][17][18][19].

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 processing 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		
	ASE_COMP.1	ASE_COMP.1.1E	PASS	PASS	
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_TAT.2	ALC_TAT.2.1E	PASS	PASS	
		ALC_TAT.2.2E	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	
	ALC_COMP.1	ALC_COMP.1.1E	PASS	PASS	
		ALC_COMP.1.2E	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	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		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		
	ADV_COMP.1	ADV_COMP.1.1E	PASS	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		
	ATE_COMP.1	ATE_COMP.1.1E	PASS	PASS	
		ATE_COMP.1.2E	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		
	AVA_COMP.1	AVA_COMP.1.1E	PASS	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 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 (COB) to card manufacturer. 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 IFX_CCI_0x000005h as a secure IC chip platform, it is recommended to refer to the user 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 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 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 JK62 Security Target v2.5, September 5, 2025 [10] is included in this report by reference. For the purpose of publication, it is provided as sanitized version [11] according to the CCRA supporting document ST sanitising for publication [12].

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
JCAPI	Java Card Application Programming Interface
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	The name is given to a Javacard technology-based user application. An applet is the basic piece of code that can be selected for execution from outside the card. Each applet on the card is uniquely identified by its AID.
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
FLASH Memory	Flash memory is an electronic non-volatile computer storage medium that can be electrically erased and reprogrammed
GlobalPlatform Registry	A container of information related to Card Content management
IC Chip (Integrated Circuit Chip)	A semiconductor for Smartcard functions, and it has FLASH, RAM and I/O port
Issuer Security Domain	On-card entity providing support for the control, security, and communication requirements of the Card Issuer
JCAPI	The interface for functions defined java framework and extended java package. JCAPI is a subset of the Java™ programming language
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	The central on-card administrator that owns the

(OPEN)	GlobalPlatform Registry
Package	A package is a namespace within the Java programming language that may contain classes and interfaces
SCP02/03	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, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, November 2022
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components
Part 4: Framework for the specification of evaluation methods and activities
Part 5: Pre-defined packages of security requirements

[2] Common Methodology for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-006, November 2022

[3] Korea IT Security Evaluation and Certification Guidelines (Ministry of Science and ICT Guidance No. 2022-61)

[4] Korea IT Security Evaluation and Certification Regulation (Ministry of Science and ICT·ITSCC, May 17, 2021)

[5] Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.4., September 2011, Oracle

[6] Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.4., September 2011, Oracle

[7] Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.4., September 2011, Oracle

[8] GlobalPlatform Card Specification 2.3.1, GPC_SPE_034, March 2018

[9] CC2024-00004 KOMSCO JK62 V1.1 Evaluation Technical Report V3.0, September 30, 2025

[10] KOMSCO JK62 Security Target v2.5, September 5, 2025 (Confidential Version)

[11] KOMSCO JK62 Security Target Lite v2.1, September 5, 2025 (Sanitized Version)

[12] ST sanitizing for publication, CCDB-2006-04-004, April 2006

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

[14] Certification Report BSI-DSZ-CC-1110-V7-2024 - Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h,000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13, 30 September 13, 2024

[15] Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13, Revision 5.1, 11 September, 2024

[16] Composite product evaluation for Smartcards and similar devices v1.6, April 2024

[17] Application of Attack Potential to Smartcards Version 3.2.1, Feb. 2024

[18] Security Architecture requirements(ADV_ARC) for smart cards and similar devices extended to Secure Sub-Systems in Soc, Version 2.1, July. 2021

[19] Security Architecture requirements(ADV_ARC) for smart cards and similar devices – Appendix 1, Version 4, 2024.4

[20] Application of CC to Integrated Circuits, Version 4.0, 2024. 4

[21] Guidance for smartcard evaluation v3.0, 2024.4

[22] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2024-002 Version 1.1, July 2024