KECS-CR-14-53

XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 Certification Report

Certification No.: KECS-ISIS-0533-2014

2014. 9. 19

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2014.09.19	-	Certification report for XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 - First documentation

This document is the certification report for XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 of LG CNS.

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 EAL4+ evaluation of LG CNS XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 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 and embedded software (Native operating system (NOS), Global Platform, and Java Card Platform) 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 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. Additionally, the TOE provides native APIs for data group creation and access (supporting development of e-Passport in accordance with “ICAO Doc 9303” and Driving License in accordance with “ISO/IEC 18013”), and native APIs for data integrity verification of secure transaction.

The TOE XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 is composed of the following components:

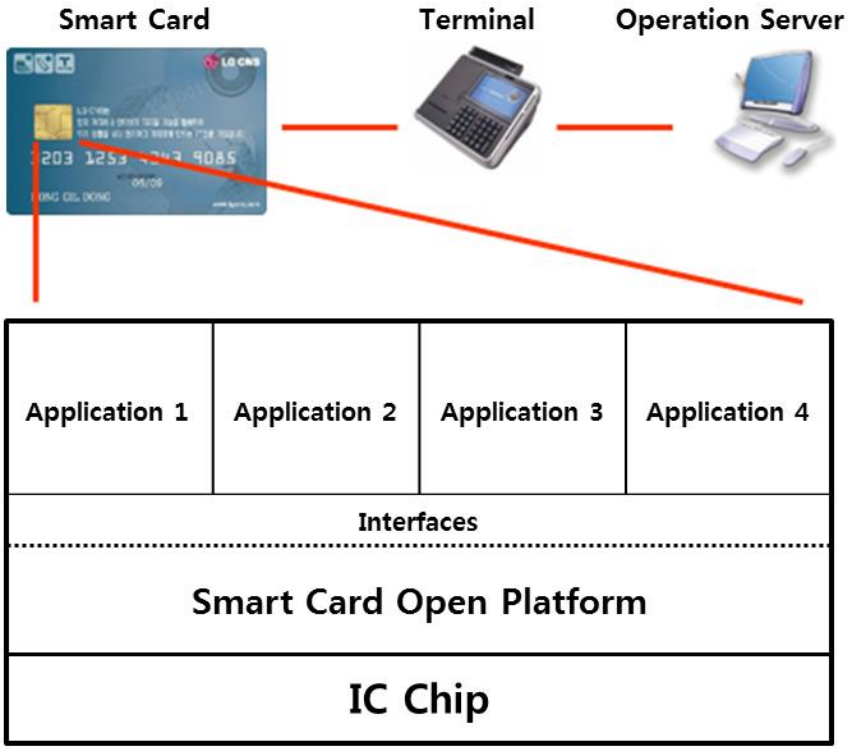
- IC chip S3CT9KW/S3CT9KC/S3CT9K9 Revision 2 provided by Samsung Electronics, see ANSSI-CC-2012/70 (ANSSI-CC-2012/70-S01, surveillance report, April 14, 2014), and
- Embedded software XSmart OpenPlatform V1.1 provided by LG CNS.

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on August 22, 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 EAL4 augmented by ATE_DPT.2 and AVA_VAN.4. 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	Samsung S3CT9KW/S3CT9KC/	Revision 2	IC Chip Module

Type	Identifier	Release	Delivery Form
	S3CT9K9 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional secure RSA/ECC V2.2 Library including specific IC Dedicated Software		(Note: The SW is contained in ROM)
	Secure RSA/ECC Library	V2.2	
	TRNG Library	V2.0	
SW	XSmart OpenPlatform V1.1	Masking Version 1	
DOC	XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 User's Guide for Management	V1.2	Softcopy

[Table 1] TOE identification

Those parts that constitute smart card open platform of the TOE are masked on the ROM area, while the other parts that constitute factory initialization of the TOE are masked on the EEPROM area.

The TOE is finalized by "IC Manufacturer" at the Manufacturing Phase (ROM masking and packaging) in accordance with the Smart Card Open Platform PP [5] and the Security Target [12]. After the TOE finalization, the "Card Manufacturer" initializes the TOE and embeds the TOE into the smart card. The card production including the application of the antenna is not part of the TOE. After the Manufacturing Phase, TOE can be issued by "Card issuer" with applications and associated personalization data.

The certified IC chip S3CT9KW/S3CT9KC/S3CT9K9 which is a component of the TOE provides Secure RSA-CRT Asymmetric Cryptography and the TOE utilizes it for a few native APIs. However, it is out of certification scope. For more details refer to the Security Target [13]. And for details on the IC chips, the IC dedicated software and the crypto libraries, see the documentation under ANSSI-CC-2012/70 [14].

[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	XSmart OpenPlatform V1.1 S3CT9KW/S3CT9KC/S3CT9K9 (Masking Version: 1) ● ROM images ■ XSMART_OPEN110_KW_m01.rom ■ XSMART_OPEN110_KC_m01.rom ■ XSMART_OPEN110_K9_m01.rom ● EEPROM images ■ XSMART_OPEN110_KW_m01.eep ■ XSMART_OPEN110_KC_m01.eep ■ XSMART_OPEN110_K9_m01.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	EAL4+ (augmented by ATE_DPT.2 and AVA_VAN.4)
Developer	LG CNS
Sponsor	LG CNS
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	August 22, 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 the TOE complies security policies defined in the PP [5] by security objectives and security requirements based on Java Card 2.2.2 [6], [7], [8] and GlobalPlatform Card Specification [9]. Thus the TOE provides security features defined in the Smart Card Open Platform PP [5] as follows.

- The TOE ensures the Java Package, Java Applet and Java Card Runtime Environment to be protected from bypassing the applet firewall policy.
- The TOE ensures that each Security Domain of GlobalPlatform to be protected from unauthorized access and modification.
- The TOE ensures the Card Manager to be protected from enforced deletion.
- The TOE ensures the unauthorized entity cannot access to the TSFI through the bypassing life cycle state of the card or the application defined in GlobalPlatform Card Specification [9].
- The TOE ensures cryptography related APIs in the scope of certification have a resistance against side channel and perturbation attacks performed by an attacker possessing Moderate attack potential.
- The TOE's Secure Channel features (e.g. SCP02) ensure transmitted data to be protected from unauthorized disclosure and modification.
- The TOE ensures safe data recovery or deletion (atomic operation) when abnormal event (e.g. tearing at installation procedure) is occurred.
- The TOE ensures the TSF data stored in the memory is protected against unauthorized modification
- The TOE ensures the installation of post-issuance application. It does not address card management issues in the broad sense, but only those security aspects of the installation procedure that are related applet execution. (referred to Java Card Protection Profile - Open Configuration, May 2012, Version 3.0)

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/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 (with SHA) 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 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 [12], chapter 3.3, and the ST

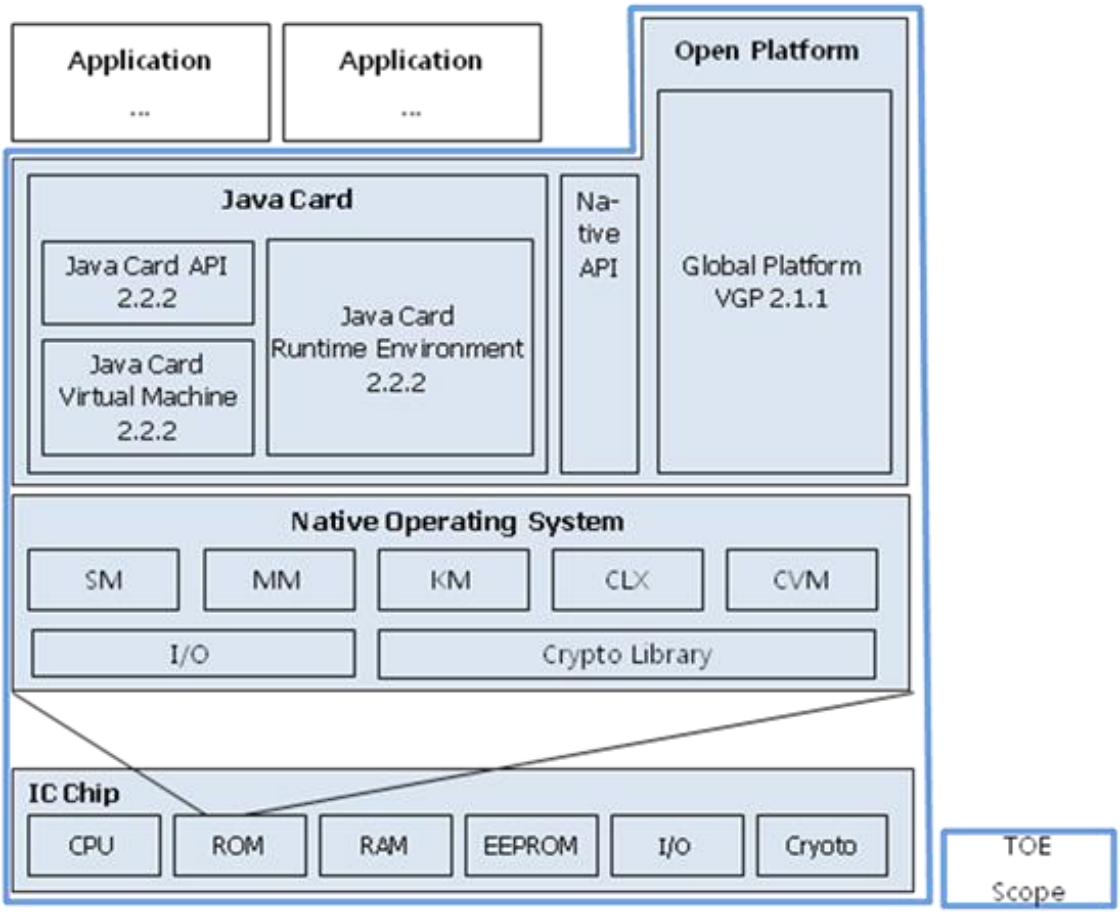
[13], chapter 4.3.):

- 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.
- During operation of the TOE, the TSF data handled in outside of the TOE is 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, bytecode verification and secure manufacturing and management, etc.. Details can be found in the ST [12], chapter 3.1, 3.2 and 4.3, and the ST [13], chapter 4.1, 4.2 and 5.3.

5. Architectural Information

[Figure 2] show 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] Scope of the TOE

- The Global Platform 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 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 and etc.. The JCVM is bytecode interpreter based on Java Card specification. The Java Card applet's methods are converted to bytecode can be performed on the JCVM. TOE can execute the applet independent from the hardware through the JCVM.
- The JCAPI is the set of classes provides for development of application in accordance with Java Card specification. The JCAPI provides primary APIs and extended API packages, and it is the upper layer JCRE, provides the interfaces for cryptographic functions and basic functions to the application.
- The 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 Native Operating System is hardware abstraction layer. It is responsible for operating system to execute the JCVM and the JCRE, and includes low level I/O function, memory management function, low level transaction and crypto functions. The TOE provides Native APIs for data group creation and access, and provides native APIs for data integrity verification of secure transaction.
- 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 Native Operating System, and they utilize certified cryptographic libraries implemented in the certified IC chip. The IC chip provides 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 cryptographic 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 [12][13].

6. Documentation

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

Identifier	Release	Date
XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/ S3CT9K9 User's Guide for Management	V1.2	August 17, 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 GlobalPlatform, Java Card, and Native Operating System.

The developer conducted 987 test cases related to the TSFI and module interface, and cryptographic functions as described below:

- Automated tools testing, which tests the security functionality and module interfaces through the scenario-based scripts using automated tools for the smartcard standards (ISO/IEC 7816 [23], ISO/IEC 14443 [24]), GlobalPlatform [9]/Visa GlobalPlatform [10], and Java Card 2.2.2 [6], [7], [8],
- Tearing testing, which tests secure operation of the TOE under the environmental stress,
- Chip testing, which tests features such as cryptographic operation and security register provided by IC chip, and
- Native API testing, which tests native APIs for data group creation and access (supporting development of e-Passport in accordance with "ICAO Doc 9303" and Driving License in accordance with "ISO/IEC 18013"), and native APIs for data integrity verification of secure transaction using in-house testing tools.

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 TSF behaves as

described in the functional specification.
The developer tested both subsystems (including their interactions) and SFR-enforcing modules (including their interfaces), and analyzed testing results in accordance with the assurance component ATE_DPT.2.
The evaluator performed all the developer's tests listed in this report chapter 7, and conducted independent testing based upon test cases devised by the evaluator.
Also, the evaluator had 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 less than 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 XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 and the TOE is composite product consisting of the following components:

- IC chips: 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)
- Embedded software: XSmart OpenPlatform 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:

- ATR (Historical Byte): XSMARTOPEN110 (XSmart OpenPlatform V1.1)
  - 3B8D8001**58534D4152544F50454E313130**29

- Command APDU (GET_DATA): 80CA9F7F
- Response APDU: 9F7F2A4250**140C**42514062**0111**410600041C710A4D42524115
  - '1420' or '140C' or '1409': S3CT9KW / S3CT9KC / S3CT9K9 (IC chip identifier)
  - '0111': TOE Version (V1.1) and Masking Version (m01)

- Command APDU (GET_DATA): 80CA005A
- Response APDU: 5A06**02**10**022C**01**02**9000
  - ‘02’: IC Chip Revision Number (revision 2)
  - ‘022C’: RSA/ECC Library Version (V2.2)
  - ‘02’: TRNG Version (2.0)

- Command APDU (GET_DATA): 80CA0056
- Response APDU: 5602**AD9B**9000
  - ‘AD9B’: ROM Code Checksum

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 [1] 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 [16], [17], [18], [19], [20] and [21].
As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL4 augmented by ATE_DPT.2 and AVA_VAN.4.

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 [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. Therefore the verdict PASS is assigned to ALC_TAT.1.
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 and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.4.
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. Therefore the verdict PASS is assigned to ALC_DVS.1.

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 [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 modules and

enough information about the SFR-supporting and 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.3.

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.4.

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.

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). 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 the SFR-enforcing modules against the TOE design and the security architecture description. Therefore the verdict

PASS is assigned to ATE_DPT.2.
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 [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 Moderate attack potential in the operational environment of the TOE.Therefore the verdict PASS is assigned to AVA_VAN.4.
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].
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 less than 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

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.1	ALC_TAT.1.1E	PASS	PASS	
	ALC_CMS.4	ALC_CMS.4.1E	PASS	PASS	
	ALC_CMC.4	ALC_CMC.4.1E	PASS	PASS	
	ALC_DVS.1	ALC_DVS.1.1E	PASS	PASS	
		ALC_DVS.1.2E	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.3	ADV_TDS.3.1E	PASS	PASS	PASS
		ADV_TDS.3.2E	PASS	PASS	
	ADV_FSP.4	ADV_FSP.4.1E	PASS	PASS	
		ADV_FSP.4.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
	ADV_IMP.1	ADV_IMP.1.1E	PASS	PASS	
ATE	ATE_COV.2	ATE_COV.2.1E	PASS	PASS	PASS
	ATE_DPT.2	ATE_DPT.2.1E	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		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.4	AVA_VAN.4.1E	PASS	PASS	PASS
		AVA_VAN.4.2E	PASS		
		AVA_VAN.4.3E	PASS		
		AVA_VAN.4.4E	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 composite product which is consisting of IC chip and smart card open platform, the TOE is finalized by “IC Manufacturer” at the Manufacturing Phase. And only the delivery procedures for the finalized TOE to card manufacturer are in the scope of the certification. Thus, the TOE user including card manufacturer shall establish the secure delivery and acceptance processes after the Manufacturing Phase.
- As the TOE can be composed with one of S3CT9KW, S3CT9KC and S3CT9K9, the TOE user is recommended to check the product identification information right after acceptance of the TOE while referring to the User’s Guide for Management provided with the product after acquisition of the TOE.
- It is recommended that the TOE user shall verify the checksum value of ROM code referring to the User’s Guide for Management.
- As the cryptographic functions out of the certification scope are not satisfied with assurance level of EAL4+, the TOE user shall not utilize them to protect important asset.
- The application provider shall verify application installed on the TOE whether there is malicious code in it or not.

- It is recommended that the TOE user shall consider security measures to manage the TSF data securely when the TSF data is processed in outside of the TOE.

11. Security Target

The XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target V1.8, September 16, 2014 [12] is included in this report by reference. For the purpose of publication, it is provided as sanitized version [13] in accordance with the CCRA supporting document ST sanitising for publication [22].

12. Acronyms and Glossary

API	Application Programming Interface
ATR	Answer To Reset
CAD	Card Acceptance Device
CC	Common Criteria
EAL	Evaluation Assurance Level
JCRE	Java Card Runtime Environment
NOS	Native Operating System
PP	Protection Profile
ST	Security Target
SAR	Security Assurance Requirement
SFR	Security Function Requirement
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
Atomic Operation	An operation that either completes in its entirety or no

	part of the operation completes at all
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
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
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
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-13-012 XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/ S3CT9K9 Evaluation Technical Report V1.3, September 16, 2014

[12] XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target V1.8, September 16, 2014 (Confidential Version)

[13] XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target Public Version V1.1, September 16, 2014 (Sanitized Version)

[14] 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 10, 2012, ANSSI

[15] 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 2.6, October 24, 2013

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

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

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

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

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

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

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

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

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