KECS-CR-14-33

XSmart e-Passport V1.3 R2 on S3CT9KW/S3CT9KC/S3CT9K9 Certification Report

Certification No.: KECS-ISIS-0513-2014

2014. 6. 25

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2014.06.25	-	Certification report for XSmart e-Passport V1.3 R2 on S3CT9KW/S3CT9KC/S3CT9K9 - First documentation

This document is the certification report for XSmart e-Passport V1.3 R2 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 EAL5+ evaluation of LG CNS XSmart e-Passport V1.3 R2 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 contactless integrated circuit chip of machine readable travel documents (MRTD chip) and embedded software (IC chip operating system(COS) and the application of machine readable travel documents(MRTD application)) including Logical Data Structure (LDS) according to the ICAO documents [5]. The TOE provides Basic Access Control (BAC), Active Authentication (AA), and Extended Access Control (EAC) defined in the ICAO's Machine Readable Travel Documents, DOC 9303 Part 1 Volume 2, 6th edition, August 2006 [5], and the BSI's Advanced Security Mechanisms Machine Readable Travel Documents – Extended Access Control V1.11, February 2008 [6].

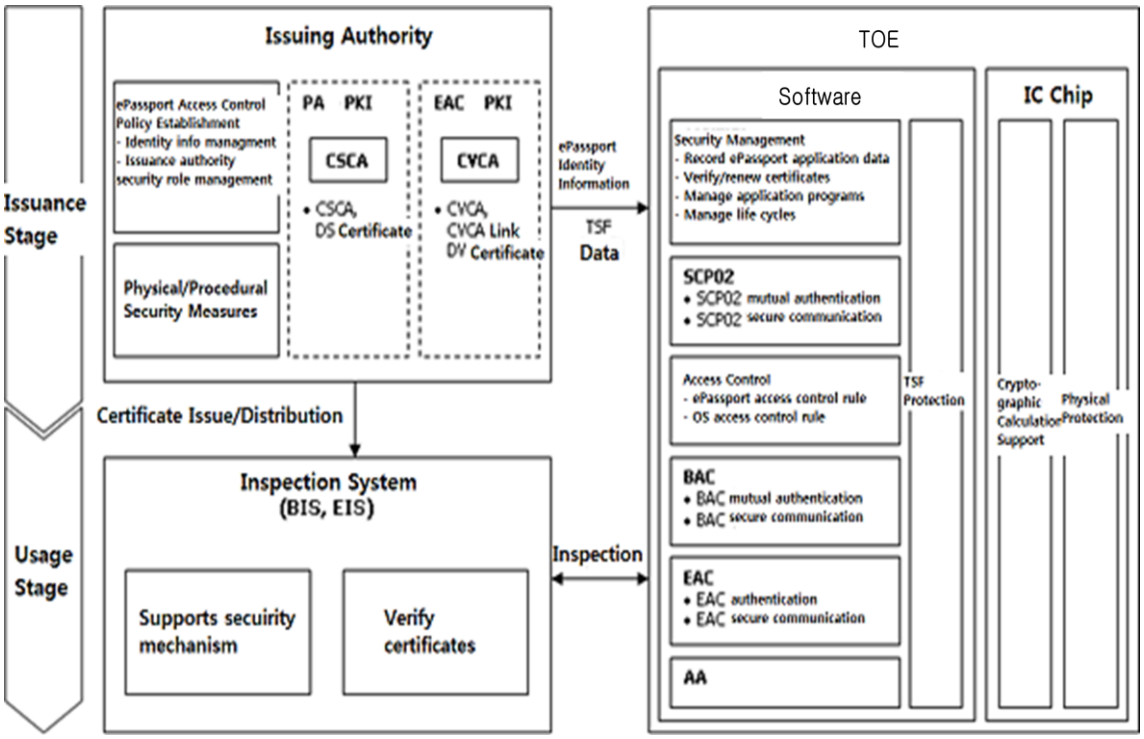
The TOE XSmart e-Passport V1.3 R2 on S3CT9KW/S3CT9KC/S3CT9K9 is composed of the following components:

- IC chip S3CT9KW/S3CT9KC/S3CT9K9 Revision 2 provided by Samsung Electronics, see ANSSI-CC-2012/70 (ANSSI-CC-2012/70-S01, surveillance report, 14 April, 2014), and
- Embedded software XSmart e-Passport V1.3 R2 provided by LG CNS.

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on June 17, 2014. This report grounds on the evaluation technical report (ETR) TTA had submitted [7] and the Security Target (ST) [8][9].

The ST is based on the certified Protection Profile (PP) ePassport Protection Profile V2.1, June 10, 2010, KECS-PP-0163a-2009 [10]. 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 ADV_IMP.2. 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 in the Personalization and Operational Use phase.



[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/ S3CT9K9 16-bit RISC	Revision 2	IC Chip Module (Note: The SW is

Type	Identifier	Release	Delivery Form
	Microcontroller for Smart Card, Revision 2 with optional secure RSA/ECC V2.2 Library including specific IC Dedicated Software		contained in ROM and EEPROM, but without passport booklet and the inlay embedded in the passport booklet.)
	Secure RSA/ECC Library	V2.2	
	TRNG Library	V2.0	
SW	XSmart e-Passport V1.3 R2	Release 2	
DOC	XSmart e-Passport V1.3 R2 on S3CT9KW/S3CT9KC/S3CT9K9 User's Guide for Management	V1.0	Softcopy

[Table 1] TOE identification

The TOE is finalized at step ③ of the Phase 2(Manufacturing) in accordance with the ePassport PP [10]. After the TOE finalization, the ePassport manufacturer (i.e., inlay and e-Cover manufacturer) embeds the TOE into the passport booklet. The inlay production including the application of the antenna is not part of the TOE.

The Personalization Agency can only access the MRTD using the securely delivered personalization key set. The personalization key set is securely delivered from the ePassport manufacturer to the Personalization Agency through PGP encryption.

The certified IC chip S3CT9KW/S3CT9KC/S3CT9K9 which is a component of the TOE provides Secure AES Symmetric Cryptography and Secure RSA-CRT Asymmetric Cryptography, they are not used by the TOE. Thus they are out of TOE scope.

For details on the MRTD chips, the IC dedicated software and the crypto libraries, see the documentation under ANSSI-CC-2012/70 [11].

[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 e-Passport V1.3 R2 on S3CT9KW/ S3CT9KC/ S3CT9K9

	(Version: Release 2) ● ROM images ■ XSMART_e-Passport_V1.3_S3CT9KW_R2.rom ■ XSMART_e-Passport_V1.3_S3CT9KC_R2.rom ■ XSMART_e-Passport_V1.3_S3CT9K9_R2.rom ● EEPROM images ■ XSMART_e-Passport_V1.3_S3CT9KW_R2.eep ■ XSMART_e-Passport_V1.3_S3CT9KC_R2.eep ■ XSMART_e-Passport_V1.3_S3CT9K9_R2.eep
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
EAL	EAL5+ (augmented by ADV_IMP.2)
Developer	LG CNS
Sponsor	LG CNS
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	June 17, 2014
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

3. Security Policy

The ST [8][9] for the TOE claims demonstrable conformance to the ePassport PP [10], and the TOE complies security policies defined in the ePassport PP [10] by security objectives and security requirements based on the ICAO document [5], EAC specification [6]. Thus the TOE provides security features BAC and EAC(EAC-CA, EAC-TA) defined in the ePassport PP [10], and AA.

Inspection procedures are as followed:

- For Inspection System supporting BAC only: BAC → PA → AA,
- For Inspection System supporting both BAC and EAC: BAC → EAC-CA →

PA → EAC-TA.

Additionally, the TOE provides security features for personalization agent to protect ePassport identity data (during personalization phase):

- Personalization agent authentication, ensures only authorized entity can access to the TOE during personalization phase
- Secure messaging, ensures transmitted data to be protected from unauthorized disclosure and modification during personalization phase.

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 Symmetric Cryptography support, Secure coprocessor for RSA and ECC Asymmetric Cryptographic Support, and a True Random Number Generator (TRNG) for AIS31-compliant Random Number Generation. For more details refer to the Security Target Lite for the IC chip [12].

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 [8][9], chapter 3.3):

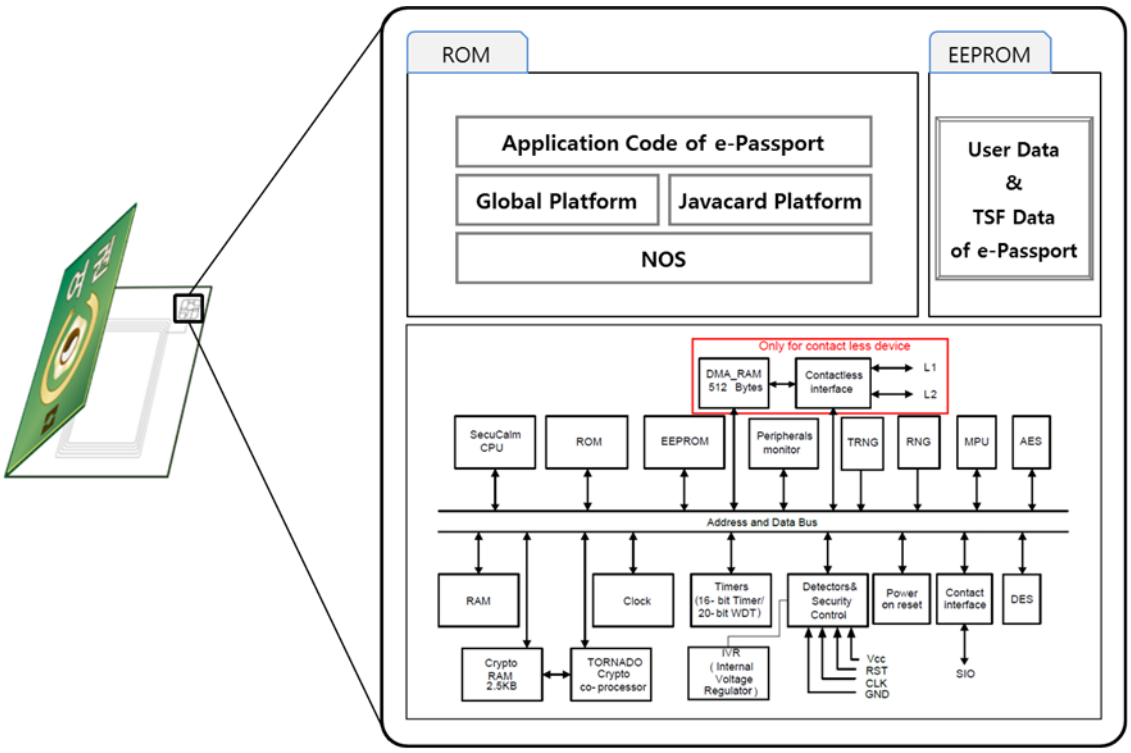
- The Inspection System verifies the Security Object of Document (SOD) after verifying validity of the certificate chain for PA in order to verify for forgery and corruption of the ePassport identity data recorded in the TOE. For this, the DS certificate and CRL shall be verified periodically. The Inspection System shall securely hold the digital signature generation key that corresponds to the IS certificate and shall provide the TOE with the CVCA link certificate, the DV certificate and the IS certificate in the EAC-TA.
- The Inspection System shall implement security mechanisms of PA, AA, BAC and EAC according to the ICAO document [5] and EAC specifications [6] on the basis of the verifying policy of the ePassport for the ePassport holder. Also, after session termination, the Inspection System shall securely destroy all information, such as the BAC session key, the EAC session key and session information, etc., used in communication with the TOE.
- The seed for BAC authentication key takes the sufficient MRZ entropy to

ensure the secure BAC authentication key.

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: ePassport Manufacturing Security, Procedures for ePassport Holder Confirmation, Interoperability for ePassport, etc. Details can be found in the ST [8][9], chapter 3.1, 3.2 and 4.3.

5. Architectural Information

[Figure 2] show the physical scope of the TOE. The TOE is the composite product which is consisting of the certified contactless MRTD chip and the embedded software (i.e., COS and MRTD application).



[Figure 2] Scope of the TOE

- MRTD application provides BAC, AA, and EAC according to the ICAO document [5] and EAC specification [6]. It also provides additional security mechanisms for personalization agent such as authentication.
- COS, which processes commands and manages files according to ISO/IEC

7816-4, 8, and 9 [19], executes MRTD application and provides functions for management of MRTD application data. It also provides additional security mechanisms for initialization agent such as authentication and initialization of the TOE. Global Platform, which is part of COS, provides installation commands for MRTD application before MRTD application is activated, and authentication commands for personalization agency after MRTD application is activated. Javacard Platform, which is part of COS, provides initialization functions right after power-on, and it is not used after MRTD application is activated.

- MRTD 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 Symmetric Cryptography support, Secure coprocessor for RSA and ECC Asymmetric Cryptographic Support, and a True Random Number Generator (TRNG) for AIS31-compliant Random Number Generation.

For the detailed description is referred to the ST [8][9].

6. Documentation

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

Identifier	Release	Date
XSmart e-Passport V1.3 R2 on S3CT9KW/S3CT9KC/ S3CT9K9 User's Guide for Management	V1.0	June 13, 2014

[Table 3] Documentation

7. TOE Testing

The developer took a testing approach based on the component of the TOE. Physically, the embedded software is not separated, but logically, it can be divided into COS and MRTD application in accordance with the ICAO documents [5] and EAC specification[6].

Tests for COS are:

- Unit Test, which tests functions implemented in COS,
- Tearing Test, which tests secure operation of the TOE under the environmental stress, and
- Chip Test, which tests features such as cryptographic operation and security register provided by IC chip.
- GP Test, which tests limited features in compliance with Global Platform such as INSTALL, GET DATA, PUT KEY commands and SCP02 authentication protocol.

Tests for MRTD application are:

- Functional and Module Test, which tests MRTD application in accordance with the ICAO Documents [5] and EAC specification [6], and
- LDS Test, which tests additional features which are not defined in the ICAO document [5] and EAC specification [6] such as initialization, personalization and inspection, life cycle state change, and residual information removal.

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

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

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

Also, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These test cases cover testing APDU commands, bypassability, observation attacks such as SEMA/CEMA, fault injection attacks, and so on. No exploitable vulnerabilities by attackers possessing moderate 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 [7].

8. Evaluated Configuration

The TOE is XSmart e-Passport V1.3 R2 on S3CT9KW/S3CT9KC/S3CT9K9. 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 e-Passport V1.3 R2

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): XSMARTEPASS130 (XSmart e-Passport V1.3)
- Command APDU (GET_DATA): 80CA9F7F
- Response APDU: 9F7F2A4250**14XX**42514080**0132**41140100626D107742524123
  - 14XX: '1420' or '140C' or '1409' (S3CT9KW / S3CT9KC / S3CT9K9 (IC chip identifier))
  - '0132': TOE Version and release number (V1.3 R2)
- Command APDU (GET_PATCH_STATUS) : 80D3E000
- Response APDU:
  53334354394B57205253412076322E3200DA08A000000003000000019E020000**022C02**9000
  - '53334354394B57205253412076322E32': RSA/ECC Library Checksum
  - '022C': RSA/ECC Library Version (V2.2)
  - '02': IC Chip Revision Number (revision 2)

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 [7] 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 [13], [14], [15] and [16]. Also the evaluation facility utilized German scheme's Evaluation Methodology for CC Assurance

Class for EAL5+ and EAL6 [18] under confirmation of the CB.
As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL5 augmented by ADV_IMP.2.

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 [15].
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. 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 [13].

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

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It provides a detailed description of the SFR-enforcing and SFR-supporting modules and enough information about the SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented; as such, the TOE design provides an explanation of the implementation representation. Therefore the verdict PASS is assigned to ADV_TDS.4.

The developer has completely described all of the TSFI in a manner such that the evaluator was able to determine whether the TSFI are completely and accurately described, and appears to implement the security functional requirements of the ST. Therefore the verdict PASS is assigned to ADV_FSP.5.

The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.

The implementation representation is sufficient to satisfy the functional requirements of the ST and is a correct realisation of the low-level design. Therefore the verdict PASS is assigned to ADV_IMP.2.

The TSF internal is well-structured such that the likelihood of flaws is reduced and that maintenance can be more readily performed without the introduction of flaws.

Therefore the verdict PASS is assigned to ADV_INT.2.
Also, the evaluator confirmed that the requirements on the embedded software, imposed by the IC chip, are fulfilled in the composite product according to the CCRA supporting document Composite Product Evaluation [13].
Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed), an implementation description (a source code level description), and TSF internals description (which describes evidence of the structure of the design and implementation of the TSF). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).
The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.2.
The developer has tested all the TSF subsystems and modules against the TOE design and the security architecture description. Therefore the verdict PASS is assigned to ATE_DPT.3.
The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.
By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.
Also, the evaluator confirmed that composite product as a whole exhibits the properties necessary to satisfy the functional requirements of its ST according to the CCRA supporting document Composite Product Evaluation [13].
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 [13].

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

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_TAT.2	ALC_TAT.2.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	ALC_CMS.5	ALC_CMS.5.1E	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.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.2	ADV_IMP.2.1E	PASS	PASS	
	ADV_INT.2	ADV_INT.2.1E	PASS	PASS	
		ADV_INT.2.2E	PASS		
ATE	ATE_COV.2	ATE_COV.2.1E	PASS	PASS	PASS
	ATE_DPT.3	ATE_DPT.3.1E	PASS	PASS	
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.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:

- The TOE must be used for e-Passport, and LDS application is installed by installation command when e-Cover is manufactured. After the installation of the MRTD application, any other applications cannot be installed.
- As the TOE can be composed with one of S3CT9KW, S3CT9KC and S3CT9K9, the personalization agent is recommended to check the product identification information right after acceptance of the TOE while referring to the user operating manual provided with the product after acquisition of TOE.
- In the initialization phase of the TOE, it is recommended that the personalization agent shall verify the checksum value of ROM code referring to user manual.
- The personalization agent is recommended to carefully manage the initial product keys, and inject the secure personalization agent authentication key while referring to the user operating manual in the product initialization stage, and perform secure communication thereafter.
- It is recommended that the personalization agent shall perform personalization in compliance with command order after establishing secure channel.
- After personalization phase is completed, the personalization agent shall deactivate the writing function for personalization.
- When operating the TOE, the personalization agent shall consider the operating environment specified in the security target.
- The personalization agent can deactivate the EAC in accordance with the policy, and shall not issue the biometric information of the e-Passport user when it is deactivated.

11. Security Target

The XSmart e-Passport V1.3 R2 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target V1.0, June 13, 2014 [8] is included in this report by reference. For the purpose of publication, it is provided as sanitized version [9] in accordance with the CCRA

supporting document ST sanitising for publication [17].

12. Acronyms and Glossary

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
API	Application Programming Interface
CC	Common Criteria
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ICAO	International Civil Aviation Organization
IS	Inspection System
BIS	BAC/SAC supporting Inspection System
EIS	EAC supporting Inspection System
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

AA (Active Authentication)	The security mechanism with which the MRTD chip demonstrates its genuine to the IS by signing random number transmitted from the IS and the IS verifies genuine of the MRTD chip through verification with the signed values
Application Protocol Data Unit(APDU)	Standard communication messaging protocol between a card accepting device and a smart card
BAC (Basic Access Control)	The security mechanism that implements the symmetric key-based entity authentication protocol for mutual authentication of the MRTD chip and the IS (BIS) and the symmetric key-based key distribution protocol to generate the session keys necessary in establishing the

	secure messaging for the MRTD chip and the IS
CSCA (Country Signing Certification Authority)	The root CA that generates and issues the CSCA certificate and the DV certificate by securely generating the digital signature key in the PA-PKI to support the PA security mechanisms
CSCA Certificate	The certificate to demonstrate validity of the digital signature verification key for the digital signature generation key of the PA-PKI root CA by signature on the digital signature verification key with digital signature generation key of the PA-PKI root CA
CVCA (Country Verifying Certification Authority)	The root CA that generates and issues the CVCA certificate, the CVCA link certificate and the DV certificate by securely generating digital signature key in the EAC-PKI to support the EAC security mechanisms
CVCA Certificate	The certificate that includes digital signature value by the EAC-PKI root CA with digital signature generation key of the EAC-PKI root CA on the digital signature verification key in order to demonstrate validity of the CVCA link certificate and the DV certificate
CVCA Link Certificate	The certificate that includes digital signature value that the EAC-PKI root CA with the digital signature generation key that corresponds to the previous CVCA certificate after generating a new CVCA certificate before expiring the valid date of the CVCA certificate
DS(Document Signer) Certificate	The certificate of the Personalization agent signed with the digital signature generation key of the PA-PKI root CA used by the IS to verify the SOD of the PA security mechanism
DV (Document Verifier)	The CA(Certification Authority) that generates and issues the IS certificate
DV Certificate	The certificate that includes digital signature value on the digital signature verification key of the IS with the digital signature generation key of the DV in order to demonstrate validity of the digital signature verification key of the IS
EAC (Extended Access	The security mechanisms consisted with the EAC-CA for

Control)	chip authentication and the EAC-TA for the IS authentication in order to enable only the EAC supporting Inspection System (EIS) to read the biometric data of the ePassport holder for access control to the biometric data of the ePassport holder stored in the MRTD chip
EAC-CA (EAC-chip Authentication)	The security mechanism to implement the Ephemeral-Static DH key distribution protocol (PKCS#3, ANSI X.42, etc.) to enable the MRTD chip authentication by the EIS through key checking for the EAC chip authentication public key and private key of the MRTD chip and temporary public key and private key of the EIS
EAC-TA (EAC-terminal Authentication)	The security mechanism that the EIS transmits values digital signature with the digital signature generation key of its own to the temporary public key used in the EAC-CA and the MRTD chip by using the IS certificate, verifies the digital signature. This security mechanism implements challenge-response authentication protocol based on digital signature through which the MRTD chip authenticates the EIS.
ePassport	The passport embedded the contactless IC chip in which identity and other data of the ePassport holder stored according to the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO)
ePassport identity data	Including personal data of the ePassport holder and biometric data of the ePassport holder
IS (Inspection System)	As an information system that implements optical MRZ reading function and the security mechanisms (PA, BAC, EAC and AA, etc.) to support the ePassport inspection, the IS consists with a terminal that establishes the RF communication with the MRTD chip and the system that transmits commands to the MRTD chip through this terminal and processes responses for the commands
IS Certificate	Certificate used by the MRTD chip to verify the digital signature transmitted by the IS in the EAC-TA. The DV

	performs a digital signature on the digital signature verification key of the EIS with the digital signature generation key
LDS (Logical Data Structure)	Logical data structure defined in the ICAO document in order to store the user data in the MRTD chip
MRTD	Machine Readable Travel Document, e.g. passport, visa or official document of identity accepted for travel purposes
MRTD Application	Program for loaded in the MRTD chip that is programmed by the LDS of the ICAO document and provides security mechanisms of BAC, PA and EAC, etc.
MRTD Chip	The contactless IC chip that includes the MRTD application and the IC chip operating system necessary in operation of the MRTD application and that supports communications protocol by ISO/IEC 14443
PA (Passive Authentication)	The security mechanism to demonstrate that identity data recorded in the ePassport has not been forgery and corruption as the IS with the DS certificate verifies the digital signature in the SOD and hash value of user data according to read-right of the ePassport access control policy
Personalization agent	The agent receives the ePassport identity data from the Reception organization and generates the SOD by digital signature on the data. After recording them in the MRTD chip, the personalization agent generates TSF data and stores it in the secure memory of the MRTD chip. The agent also operates PA-PKI and/ or EAC-PKI
SOD (Document Security Object)	The SOD refers to the ePassport identity data and the ePassport authentication data recorded in the Personalization phase by the Personalization agent that is signed by the Personalization agent with the digital signature generation key. The SOD is an object implemented with signed data type of 'RFC 3369 cryptographic message syntax, 2002.8' and encoded with DER method

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] Doc9303 “Machine Readable Travel Documents” Part1 “Machine Readable Passports” Volume 2 “Specification for Electronically Enabled Passports with Biometric Identification Capability” Sixth Edition, International Civil Aviation Organization(ICAO), August 2006

[6] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents-Extended Access Control(EAC), Version1.11, TR-03110, Bundesamtfür Sicherheitinder Informationstechnik(BSI), February 2008

[7] TTA-CCE-14-015 XSmart e-Passport V1.3 R2 on S3CT9KW/S3CT9KC/ S3CT9K9 Evaluation Technical Report V1.5, June 23, 2014

[8] XSmart e-Passport V1.3 R2 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target V1.0, June 13, 2014 (Confidential Version)

[9] XSmart e-Passport V1.3 R2 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target Public Version V1.0, June 17, 2014 (Sanitized Version)

[10] ePassport Protection Profile V2.1, June 10, 2010, KECS-PP-0163a-2009

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

[12] 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

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

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

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

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

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

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

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

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

[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