

KECS-CR-15-105

XSmart e-Passport V1.4 EAC with SAC on M7892 Certification Report

Certification No.: KECS-ISIS-0677-2015

2015. 12. 15



IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2015.12.15	-	Certification report for XSmart e-Passport V1.4 EAC with SAC on M7892 - First documentation

This document is the certification report for XSmart e-Passport V1.4
EAC with SAC on M7892 of LG CNS.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

Table of Contents

1. Executive Summary	5
2. Identification	7
3. Security Policy	9
4. Assumptions and Clarification of Scope	9
5. Architectural Information	11
6. Documentation	12
7. TOE Testing	12
8. Evaluated Configuration	13
9. Results of the Evaluation	14
9.1 Security Target Evaluation (ASE).....	15
9.2 Life Cycle Support Evaluation (ALC)	15
9.3 Guidance Documents Evaluation (AGD).....	16
9.4 Development Evaluation (ADV)	17
9.5 Test Evaluation (ATE)	18
9.6 Vulnerability Assessment (AVA)	19
9.7 Evaluation Result Summary	19
10. Recommendations	20
11. Security Target	21
12. Acronyms and Glossary	21
13. Bibliography	25

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 V1.4 EAC with SAC on M7892 with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is the composite product which is consisting of the certified 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) in accordance with the ICAO documents [5]. The TOE provides Supplemental Access Control (SAC) and Extended Access Control (EAC) defined in the ICAO’s Machine Readable Travel Documents, the BSI’s Advanced Security Mechanisms Machine Readable Travel Documents – Extended Access Control V1.11, February 2008 [6] and the ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010 [7].

The TOE XSmart e-Passport V1.4 EAC with SAC on M7892 is composed of the following components:

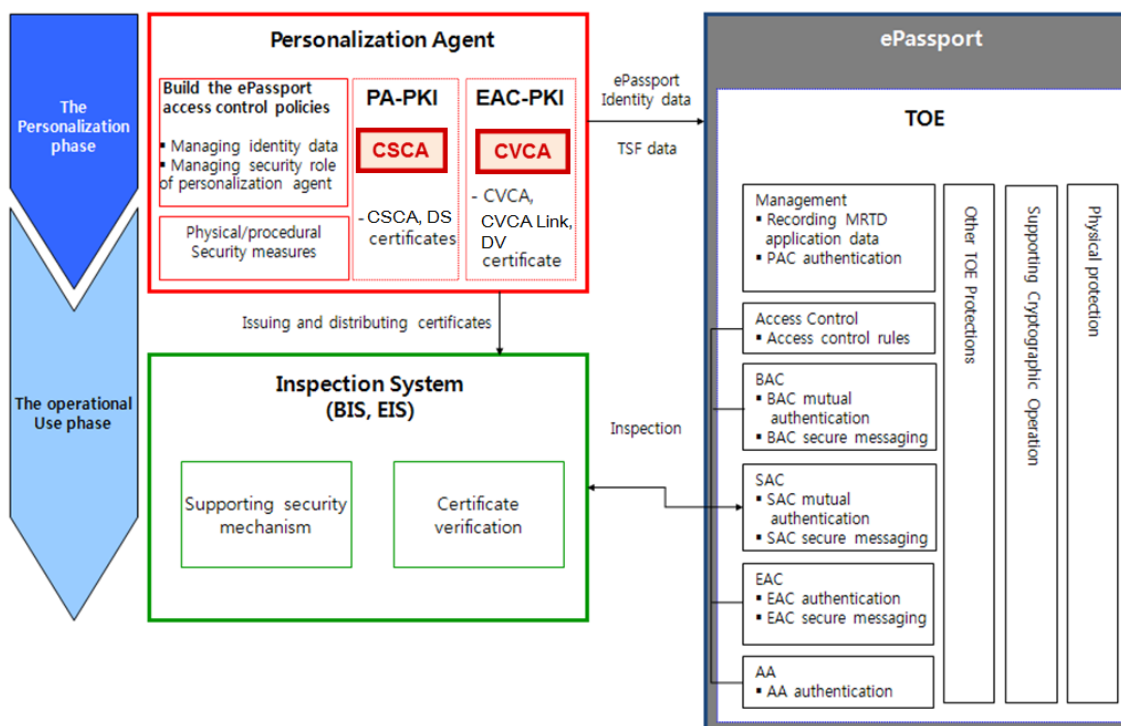
- IC chip, Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013,SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) provided by Infineon, see BIS-DSZ-CC-0782-V2-2015, and
- Embedded software, XSmart e-Passport V1.4 provided by LG CNS.

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on December 10, 2015. This report grounds on the evaluation technical report (ETR) TTA had submitted [6] and the Security Target (ST) [9][10].

The ST is based on the certified Protection Profile (PP) “ICAO Application”, Extended Access Control with PACE (EAC PP) Version 1.3.2, December 05, 2012, BSI-CC-PP-0056-V2-2012(“EAC PP” hereinafter) [11]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL5 augmented by ALC_DVS.2 and AVA_VAN.5. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components

in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] shows the operational environment of the TOE in the Personalization and Operational Use phase.



[Figure 1] Operational environment of the TOE

In this certification, although BAC (Basic Access Control) and AA (Active Authentication) exist inside of physical scope of the TOE, these mechanisms are certified separately. The TOE implements the following TOE Security Features. For more details refer to the ST [9][10].

TOE Security Features	Brief Summary of Issue
SF_READ_ACC	Data access control
SF_AUTH	Authentication
SF_SM	Data secure messaging
SF_WIRTE_MGT	Card write management
SF_EAC_TA	Extended access control

TOE Security Features	Brief Summary of Issue
SF_CRYPTO	Cryptographic operation
SF_PROTECTION	Countermeasure by IC chip

[Table 1] TOE Security Functionalities

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

2. Identification

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

Type	Identifier	Release	Delivery Form
HW/SW	Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013,SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)	B11	IC Chip Module (Note: The SW is contained in FLASH memory, but without passport booklet and the inlay embedded in the passport booklet.)
	RSA Library	v1.02.013	
	EC Library	v1.02.013	
	SHA-2 Library	V1.01	
SW	XSmart e-Passport V1.4	V1.4	
DOC	Operational User Guidance : XSmart e-Passport V1.4_AGD(EAC with SAC)_V1.4	V1.4	Softcopy or Hardcopy

[Table 2] TOE identification

The TOE is finalized at step 3 of the Phase 2 (Manufacturing) in accordance with the EAC PP [11]. After the TOE finalization, the MRTD 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 and the Guidance documents are securely delivered (through PGP or directly from the SW developer to the Personalization Agency).

For details on the MRTD chips, the IC dedicated software and the crypto libraries, see the documentation under BSI-DSZ-CC-0782-V2-2015 [10].

[Table 3] 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 V1.4 EAC with SAC on M7892 <ul style="list-style-type: none"> ● e-Passport_V14_CLFX2400P.hex (implemented on 78CLFX2400P) ● e-Passport_V14_CLFX3000P.hex (implemented on 78CLFX3000P) ● e-Passport_V14_CLFX4000P.hex (implemented on 78CLFX4000P)
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
EAL	EAL5+ (augmented by ALC_DVS.2 and AVA_VAN.5)
Developer	LG CNS
Sponsor	LG CNS
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	December 10, 2015
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The ST [9][10] for the TOE claims demonstrable conformance to the EAC PP [11], and the TOE complies security policies defined in the EAC PP [11] by security objectives and security requirements based on the ICAO document [5], EAC specification [6] and SAC specification [7]. Thus the TOE provides security features EAC and SAC defined in the EAC PP [11].

Inspection procedures are as followed:

- For Inspection System supporting SAC only, or both SAC and BAC: (recommended) SAC → EAC-CA → PA → AA → EAC-TA,
- For Inspection System supporting BAC only, or BAC required by MRTD policy: BAC → EAC-CA → PA → AA → EAC-TA.

Additionally, the TOE provides security features for Personalization Agent to protect initialization data and MRTD identity data (during pre-personalization and personalization phase):

- Personalization agent authentication, ensures only authorized entity can access to the TOE during pre-personalization and personalization phase,
- Secure messaging, ensures transmitted data to be protected from unauthorized disclosure and modification during pre-personalization and 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 filters, sensors, PFD (Post Failure Detection), REGMA (Mask Register File), CAMA (Cache Mask), MED (Memory Encryption/Decryption Unit), UmSLC (User Mode Security Life Control), co-processors of asymmetric algorithms (RSA/EC) and symmetric algorithms (3DES/AES), and a True Random Number Generator (TRNG), that meet the class PTG.2 of the AIS31. For more details refer to the Security Target Lite for the IC chip [13].

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 [9][10], chapter 3.2):

- The Extended Inspection System (EIS) for global interoperability (i) includes

the Country Signing CA Public Key and (ii) implements the terminal part of PACE and/or BAC. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

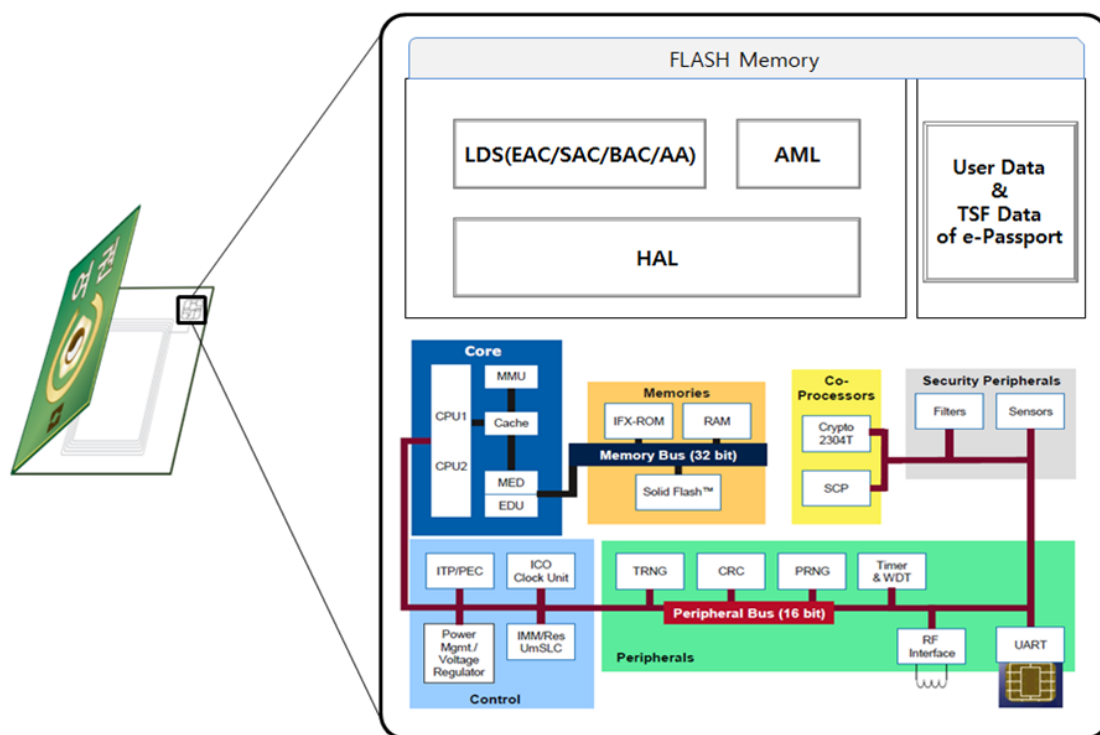
- The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip.
- The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations. It is assumed that the Personalization Agent ensures that the Document Security Object contains only the hash values of genuine user data in accordance with [5].

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: MRTD Manufacturing Security, Procedures for MRTD Holder Confirmation, Interoperability for MRTD, etc. Details can be found in the ST [9][10], chapter 3.3 and 3.4.

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 Data is consisting of User Data such as MRTD identity data and TSF Data such as SAC session Key. The Application Data is contained in FLASH.
- COS, which processes commands and manages files in accordance with ISO/IEC 7816-4, 8, and 9 [22], executes MRTD application and provides functions for management of application data. MRTD application provides EAC

and SAC in accordance with EAC Specification [6] and SAC specification [7]. It also provides additional security mechanisms for personalization agent such as authentication and personalization of MRTD. The COS and the MRTD Application are contained in FLASH memory.

- MRTD chip provides security features such as filters, sensors, PFD (Post Failure Detection), REGMA (Mask Register File), CAMA (Cache Mask), MED (Memory Encryption/Decryption Unit), UmSLC (User Mode Security Life Control), co-processors of asymmetric algorithms (RSA/EC) and symmetric algorithms (3DES/AES), and a True Random Number Generator (TRNG).

For the detailed description is referred to the ST [9][10].

6. Documentation

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

Identifier	Release	Date
XSmart e-Passport V1.4 EAC with SAC on M7892 Operational User Guidance : XSmart e-Passport V1.4_AGD(EAC with SAC)_V1.4	V1.4	August 7, 2015

[Table 4] Documentation

7. TOE Testing

The TOE is composite product and the developer took a testing approach based on the logical components of the TOE including the platform, COS, and the MRTD application.

Tests for the TOE are:

- MRTD conformance test: Layer 6~7 MRTD Application Protocol & Data Test (Security and Command Test, Logical Data Structure Tests, etc.), which tests MRTD application in accordance with Standard Test Specifications (the ICAO Technical Report RF Protocol and Application Test Standard),
- Subsystem and module test: Additional test of features provided by subsystem and module which are not defined in the ICAO document [5], and

- Other test: Tests for secure operation of the TOE such as initialization, residual information removal, anti-Tearing and etc.

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 modules (including their interfaces), and analyzed testing results in accordance with the assurance component ATE_DPT.3.

The evaluator performed all the developer's tests, and 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 MRTD Application. The implementation of the requirements of the platform's ETR and guidance as well as of the MRTD security mechanisms was verified by the evaluators.

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

The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [8].

8. Evaluated Configuration

The TOE is XSmart e-Passport V1.4 EAC with SAC on M7892. The TOE is composite product consisting of the following components:

- IC chip: Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) (BSI-DSZ-CC-0782-V2-2015)
- Embedded software : XSmart e-Passport V1.4

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

9.1 Security Target Evaluation (ASE)

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

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

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

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

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

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

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

Also, the evaluator confirmed that the ST of the composite TOE does not contradict the ST of the IC chip in accordance with the CCRA supporting document Composite Product Evaluation [14].

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

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

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

The developer has used well-defined development tools (e.g. programming languages or computer-aided design (CAD) systems) that yield consistent and predictable results, and implementation standards have been applied. Therefore the verdict PASS is assigned to ALC_TAT.2.

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

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

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

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

Also, the evaluator confirmed that the correct version of the embedded software is installed onto/into the correct version of the underlying IC chip, and the delivery procedures of IC chip and embedded software developers are compatible with the acceptance procedure of the composite product integrator in accordance with the CCRA supporting document Composite Product Evaluation [14].

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

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been

documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

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

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

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

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

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

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

The implementation representation is sufficient to satisfy the functional requirements of the ST and is a correct realisation of the low-level design. Therefore the verdict PASS is assigned to ADV_IMP.1.

The TSF internal is well-structured such that the likelihood of flaws is reduced and that maintenance can be more readily performed without the introduction of flaws. Therefore the verdict PASS is assigned to ADV_INT.2.

Also, the evaluator confirmed that the requirements on the embedded software,

imposed by the IC chip, are fulfilled in the composite product in accordance with the CCRA supporting document Composite Product Evaluation [14].

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

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.2.

The developer has tested all the TSF subsystems and modules against the TOE design and the security architecture description. Therefore the verdict PASS is assigned to ATE_DPT.3.

The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.

Also, the evaluator confirmed that composite product as a whole exhibits the properties necessary to satisfy the functional requirements of its ST in accordance with the CCRA supporting document Composite Product Evaluation [14].

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

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

Also, the evaluator confirmed that there is no exploitability of flaws or weakness in the composite TOE as a whole in the intended environment in accordance with the CCRA supporting document Composite Product Evaluation [14].

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

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
ASE_TSS.1.2E		PASS			
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_TAT.2	ALC_TAT.2.1E	PASS	PASS	
		ALC_TAT.2.2E	PASS		
	ALC_CMS.5	ALC_CMS.5.1E	PASS	PASS	
ALC_CMC.4	ALC_CMC.4.1E	PASS	PASS		

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

[Table 5] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational

environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- As the TOE is composite product which is consisting of IC chip, COS and MRTD application, the TOE is finalized by “IC Manufacturer” at the Manufacturing Phase in EAC PP [11]. And only the procedure of delivering the finalized TOE to card manufacturer is in the scope of this evaluation. Thus, the TOE user including card manufacturer shall establish the secure delivery and acquisition process after the Manufacturing Phase.
- As the TOE can be composed with one of SLE78CLFX2400P, SLE78CLFX3000P and SLE78CLFX4000P, the TOE user 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 the TOE.
- When secure messaging is not applied during personalization phase in accordance with the policy of the Personalization Agent, it is strongly recommended that the physical, procedural and personal security measures are in place in order to ensure confidentiality and integrity of the transmitted data during personalization phase.
- The TOE supports both SAC and BAC to ensure global interoperability. Thus, it is recommended that the inspection system uses SAC instead of BAC in order to provide more secure authentication mechanism.

11. Security Target

The XSmart e-Passport V1.4 EAC with SAC on M7892 Security Target V1.5, August 7, 2015 [9] is included in this report by reference. For the purpose of publication, it is provided as sanitized version [10] in accordance with the CCRA supporting document ST sanitising for publication [20].

12. Acronyms and Glossary

APDU	Application Protocol Data Unit
CC	Common Criteria

DG	Data Group
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) DV Certificate	The CA(Certification Authority) that generates and issues the IS 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 Control)	The security mechanisms consisted with the EAC-CA for 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

EAC-TA (EAC-terminal Authentication)	<p>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</p> <p>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.</p>
ePassport	<p>The passport embedded the contactless IC chip in which identity and other data of the ePassport holder stored in accordance with the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO)</p>
ePassport identity data	<p>Including personal data of the ePassport holder and biometric data of the ePassport holder</p>
IS (Inspection System)	<p>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</p>
IS Certificate	<p>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</p>
LDS (Logical Data Structure)	<p>Logical data structure defined in the ICAO document in order to store the user data in the MRTD chip</p>
MRTD	<p>Machine Readable Travel Document, e.g. passport, visa or official document of identity accepted for travel purposes</p>
MRTD Application	<p>Program for loaded in the MRTD chip that is</p>

MRTD Chip	programmed by the LDS of the ICAO document and provides security mechanisms of BAC, PA and EAC, etc. 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 in accordance with 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
SAC (Supplemental Access Control)	The security mechanism is supplementary to BAC. The SAC performs mutual authentication for the MRTD chip and the IS (BIS) to access control of personal data of the ePassport holder and establishes the secure messaging for the MRTD chip and the IS
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, Bundesamt für Sicherheit in der Informationstechnik(BSI), February 2008
- [7] ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010
- [8] TTA-CCE-14-020 XSmart e-Passport V1.4 EAC with SAC on M7892 Evaluation Technical Report V1.3, December 14, 2015
- [9] XSmart e-Passport V1.4 EAC with SAC on M7892 Security Target V1.5, August 7, 2015 (Confidential Version)
- [10] XSmart e-Passport V1.4 EAC with SAC on M7892 Security Target Lite V1.5, August 7, 2015 (Sanitized Version)
- [11] Common Criteria Protection Profile, Machine Readable Travel Document with “ICAO Application” Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012(Version 1.3.2, December 5, 2012)
- [12] BSI-DSZ-CC-0782-V2-2015 for Infineon Security Controller M7892 B11 with optional RSA2028/4096 v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware), November 3, 2015
- [13] Security Target Lite M7892 B11 Recertification including optional Software Libraries RSA - EC - SHA-2 - Toolbox, Version 0.3, October 13, 2015
- [14] Composite product evaluation for Smartcards and similar devices Version 1.2, CCDB-2012-04-01, April 2012
- [15] Application of Attack Potential to Smartcards Version 2.9, CCDB-2013-05-002,

May 2013

- [16] The Application of CC to Integrated Circuits Version 3.0 Revision 1, CCDB-2009-03-002, March 2009
- [17] Requirements to perform Integrated Circuit Evaluations, Version 1.1, CCDB-2013-05-001, May 2013
- [18] Security Architecture requirements (ADV_ARC) for smart cards and similar devices Version 2.1, CCDB-2014-04-001, April 2014.
- [19] Security Architecture requirements (ADV_ARC) for smart cards and similar devices Version 2.0 – Appendix 1, CCDB-2012-04-004, April 2012.
- [20] ST sanitising for publication, CCDB-2006-04-004, April 2006
- [21] ISO/IEC 7816 Identification cards – Integrated circuit(s) cards with contacts
- [22] ISO/IEC 14443 Identification cards – Contactless ICCs - Proximity cards
- [23] Application Notes and Interpretation of the Scheme (AIS), AIS 34, Version 3, BSI, March 9, 2009