KECS-CR-21-70

XSmart e-Passport V1.5 BAC with AA on M7892 Certification Report

Certification No.: KECS-ISIS-1140-2021

2021. 12. 23.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2021.12.23	-	Certification report for XSmart e-Passport V1.5 BAC with AA on M7892 - First documentation

This document is the certification report for XSmart e-Passport V1.5 BAC with AA on M7892 of LG CNS.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Testing Certification (KTC)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL4+ evaluation of XSmart e-Passport V1.5 BAC with AA on M7892 with reference to the Common Criteria for Information Technology Security Evaluation ("CC" hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is the composite product which is consisting of the certified integrated circuit chip (IC chip) provided by Infineon Technologies AG and the embedded software (IC chip operating system (COS), the application of machine readable travel documents(MRTD application)) including Logical Data Structure(LDS) in accordance with the ICAO Documents [5]. The TOE provides Basic Access Control (BAC) and Active Authentication (AA) defined in the ICAO's Doc9303 Machine Readable Travel Documents [5]. Password Authenticated Connection Establishment (PACE) and Extended Access Control (EAC) are also supported by the product, but PACE and EAC are not included in the scope of this TOE and separately evaluated at the same time in consideration of different level of assurance which is required by different PPs which are claimed conformance by each TOE.

The TOE XSmart e-Passport V1.5 BAC with AA on M7892 is composed of the following components:

- IC chip : Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware), see BSI-DSZ-CC-0782-V5-2020, and
- Embedded software : e-Passport_V15 provided by LG CNS.

The evaluation of the TOE has been carried out by Korea Testing Certification (KTC) and completed on 10 December 2021. This report grounds on the evaluation technical report (ETR) KTC had submitted [7] and the Security Target (ST) [8][9].

The ST is based on the certified Protection Profile (PP) Machine Readable Travel Document using ICAO Application and Basic Access Control Version 1.10 ("BAC-PP-0055" hereinafter) [6]. 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 ALC_DVS.2 and ATE_DPT.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.

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	TOE Format /Delivery Method
Composite TOE	XSmart e-Passport V1.5 BAC with AA on M7892	V1.5	IC chip (module type) /By manual (Note: The IC Dedicated SW is contained in ROM and IC optional SW, COS and Application is contained in FLASH memory of the IC Chip.)
TOE component: IC + IC Dedicated SW	Infineon Security Controller M7892 B11 - SLE78CLFX2400P - SLE78CLFX3000P - SLE78CLFX4000P	B11	IC+SW
	Firmware	V78.015.14.1	
TOE component:	RSA4096	v2.07.003	Library (SW)
	Base	v2.07.003	

Type	Identifier	Release	TOE Format /Delivery Method
IC Optional SW	Toolbox	v2.07.003	
TOE Component: COS + Application	e-Passport_V15 - e-Passport_V15_CLFX2400P.hex - e-Passport_V15_CLFX3000P.hex - e-Passport_V15_CLFX4000P.hex	V1.5	Hexa code image (SW)
Guidance Document	XSMART e-Passport V1.5_AGD(BAC with AA)_V1.3.docx	V1.3	Softcopy /PGP email

[Table 1] TOE identification

TOE is Composite product that should be considered in the Composite Product life cycle. Composite product integrator performs Composite product integration (FLASH code downloads into IC chip), preparation and shipping to the personalization for the Composite product (Composite Product Integration). Then the TOE is issued by Card Issuer with applications and associated personalization data after the initialization step. For details on the chips, the IC dedicated software and the crypto libraries, see the documentation under BSI-DSZ-CC-0782-V5-2020 [10].

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

Scheme	Korea Evaluation and Certification Guidelines for IT Security (14 August 2017) Korea Evaluation and Certification Scheme for IT Security (17 May 2021)
TOE	XSmart e-Passport V1.5 BAC with AA on M7892
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL4+ (augmented by ALC_DVS.2 and ATE_DPT.2)
Developer	LG CNS
Sponsor	LG CNS

Evaluation Facility	Korea Testing Certification (KTC)
Completion Date of Evaluation	10 December 2021
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

3. Security Policy

The ST [8][9] for the TOE claims strict conformance to the BAC PP [6] by security objectives and security requirements based on the ICAO documents [5]. Thus, the TOE provides security features defined in the BAC PP [6].
Additionally, the TOE provides security features as follows:

- 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.

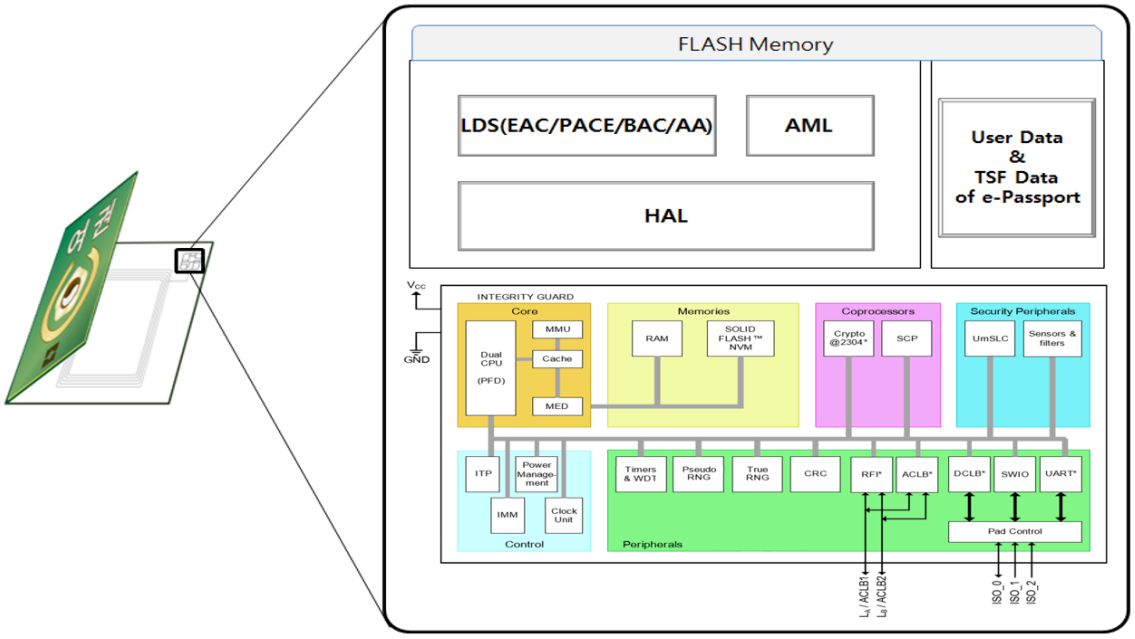
Furthermore, the TOE is composite product based on the certified IC chip, the TOE utilizes and therefore provides some security features covered by the IC chip certification such as security sensors, protection against physical proving, malfunctions, physical manipulations and abuse of functionality, against leakage of information of 3DES, RSA and TRNG. Therefore, the TOE maintains the integrity and the confidentiality of data stored in the memory or of security functionalities provided by the TOE. For more details refer to the Security Target Lite for the IC chip [11].

4. Assumptions and Clarification of Scope

The assumptions are described in the ST [8][9] in terms of 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 3.2).

5. Architectural Information

[Figure 1] 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 1] Architecture of the TOE

- MRTD application includes LDS (BAC and AA) and application data which is consisting of User Data and TSF Data of e-Passport.
- AML (Application Middle Layer) supports functions of MRTD application such as cryptographic key management and logics for transactions and cryptographic operations linked to HAL (Hardware Abstraction Layer).
- HAL (Hardware Abstraction Layer) implements hardware-dependent parts and provides IC chip initialization, hardware resource management, cryptographic algorithm implementation based on the cryptographic libraries, and security settings on the chip.
- IC chip provides security features such as security sensors/detectors, and supports cryptography.

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 V1.5_AGD(BAC with AA)_V1.3.docx	V1.3	29 September 2021

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

- The automated tools for testing, whether the smartcard specifications (ISO/IEC 7816, ISO/IEC 14443, ICAO BAC, and AA) are satisfied, are used to conduct the security function tests and module interface tests through the scenario-based scripts.
- The developer used an in-house testing tool for some special tests including crypto test, tear test, card initializations test and security audit test.
- The developer conducted additional special tests including memory range checking test, cryptographic key deletion test, and forcing card reset test.

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

The developer tested both subsystems (including their interactions) and SFR-enforcing modules (including their interfaces) and analyzed testing results in accordance with the assurance component ATE_DPT.2.

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

The evaluator performed all the developer’s tests listed in this report chapter 7 and had conducted independent testing based upon test cases devised by the evaluator. The

TOE and test configuration are identical to the developer's tests. The tests cover preparative procedures in accordance with the guidance. Some tests were performed by design and source code analysis to verify fulfillment of the requirements of the underlying platform to the COS and Application. The implementation of the requirements of the platform's ETR and guidance was verified by the evaluators.
Also, the evaluator had conducted vulnerability analysis and 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 SEMA, fault injection attacks and so on. No exploitable vulnerabilities by attackers possessing Enhanced-Basic 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 V1.5 BAC with AA on M7892 composed of the following components:

- IC chips: Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware) (BSI-DSZ-CC-0782-V5-2020)
- Embedded software: e-Passport_V15

The TOE is identified by the name, version and release number:

- IC fabricator: 0x8100 (Infineon)
- IC type: 0x0001 (SLE78CLFX4000P)
- OS release date: 0x1285 (YDDD, 2021.10.12)
- OS release level: 0x0150 (V1.5)

And the guidance document is 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 Single Evaluation 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 [12][13][14][15][16][17].
As result of the evaluation, the verdict PASS is assigned to all assurance components of EAL4 augmented by ALC_DVS.2 and ATE_DPT.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 in accordance with the CCRA supporting document Composite Product Evaluation [12].

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 that yield consistent and predictable results, and implementation standards have been applied. 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. 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 [12].
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' sufficiency 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 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. Also, the evaluator confirmed that the requirements in accordance with the CCRA supporting document ADV_ARC Evaluation [16][17].

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 in accordance with the CCRA supporting document Composite Product Evaluation [12].

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), and 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 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 in accordance with the CCRA supporting document Composite Product Evaluation [12].

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 Enhanced-Basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.3.
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 [12].
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		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_TAT.1	ALC_TAT.1.1E	PASS	PASS	
		ALC_TAT.1.2E	PASS	PASS	
	ALC_CMS.4	ALC_CMS.4.1E	PASS	PASS	
	ALC_CMC.4	ALC_CMC.4.1E	PASS	PASS	
	ALC_DVS.2	ALC_DVS.2.1E	PASS	PASS	
		ALC_DVS.2.2E	PASS		
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.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		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.3	AVA_VAN.3.1E	PASS	PASS	PASS
		AVA_VAN.3.2E	PASS		
		AVA_VAN.3.3E	PASS		
		AVA_VAN.3.4E	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 is a product used only for ePassport purposes, and the ePassport application program initializes with the HAL_INS_INITIALIZE_CARD command after successful authentication with the HAL_INS_EXTERNAL_AUTHENTICATE command. Initialization is performed only once for the first time.
- Since the TOE is classified into SLE78CLFX4000P, SLE78CLFX3000P, and SLE78CLFX2400P according to the size of the underlying platform (IC chip) flash memory, it is recommended to check the identification information of the product by referring to the guidance document provided with the product before initializing the ePassport application program.
- After initialization of the ePassport application program, it is recommended to verify the checksum value of the hexa code image by referring to the user operational guidance document provided with the product.
- The Personalization Agent should pay attention to the management of the initial product key, and it is recommended to inject a secure personalization agent authentication key by referring to the guidance document during the product initialization process so that secure communication can be performed afterwards.
- It is recommended that the Personalization agent create a secure channel by following the command usage sequence and issue ePassport user data.
- The Personalization Agent shall distribute the ePassport whose status is changed to PERSONALIZED to the user after the ePassport issuance is completed.
- The Personalization Agent shall consider the operating environment specified in the ST when operating the product.

11. Security Target

The XSmart e-Passport V1.5 BAC with AA on M7892 Security Target V1.4, 9 December 2021 [10] is included in this report by reference. For the purpose of publication, it is provided as sanitized version [11] according to the CCRA supporting document ST sanitising for publication [20].

12. Acronyms and Glossary

AA	Active Authentication
APDU	Application Protocol Data Unit
BAC	Basic Access Control
CC	Common Criteria
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ICAO	International Civil Aviation Organization
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

Active Authentication	Security mechanism defined in ICAO Doc 9303 option by which means the travel document's chip proves and the inspection system verifies the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State of Organisation.
Basic Access Control (BAC)	Security mechanism defined in ICAO Doc 9303 by which means the travel document's chip proves and the inspection system protects their communication by means of secure

	messaging with Document Basic Access Keys (see there).
ePassport application	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [EAC].
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
Initialization	Process of writing Initialization Data to the TOE.
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are for instance used for traceability and for IC identification as travel document's material (IC identification data).
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organisation
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology. The capacity expansion technology used is the travel document's chip.
Machine readable travel document (MRTD)	Official document issued by a State or Organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data

	collected during the “Enrolment”.
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i)establishing the identity of the travel document holder for the biographic data in the travel document, (ii)enrolling the biometric reference data of the travel document holder, (iii)writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in EAC PP, (iv)writing the document details data, (v)writing the initial TSF data, (vi)signing the Document Security Object defined in ICAO Doc 9303.
Personalisation Data	A set of data including followings: (i)individual-related data (biographic and biometric data) of the travel document holder, (ii)dedicated document details data and (iii)dedicated initial TSF data (including the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing.
Pre-Personalisation	Process of writing Pre-Personalisation Data to the TOE including the creation of the travel document application.
Travel document	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.

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 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
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 5, CCMB-2017-04-004, April 2017

[3] Korea Evaluation and Certification Guidelines for IT Security (24 August 2017)

[4] Korea Evaluation and Certification Scheme for IT Security (17 May 2021)

[5] Doc9303 Machine Readable Travel Documents Seventh Edition, International Civil Aviation Organization (ICAO), 2015

[6] Protection Profile - Machine Readable Travel Document with ICAO Application and Basic Access Control, BSI-CC-PP-0055, Version 1.10, 25th March 2009

[7] CC2020-00001 XSmart e-Passport V1.5 BAC with AA on M7892 Evaluation Technical Report V3.0, 10 December 2021

[8] XSmart e-Passport V1.5 BAC with AA on M7892 Security Target V1.4, 9 December 2021 (Confidential Version)

[9] XSmart e-Passport V1.5 BAC with AA on M7892 Security Target Lite V1.0, 30 November 2021 (Sanitized Version)

[10] Certification Report BSI-DSZ-CC-0782-V5-2020 - Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware), 26 November 2020

[11] Security Target Lite M7892 B11 Version 4.1, 21 October 2020

[12] Composite product evaluation for Smartcards and similar devices v1.5.1, May 2018

[13] Application of Attack Potential to Smartcards Version 3.1, JIL, June 2020

[14] The Application of CC to Integrated Circuits Version 3.0, JIL, February 2009

[15] Minimum ITSEF Requirements for Security Evaluation of Smart cards and similar devices Version 2.0, JIL, January 2017

[16] Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Version 2.0, JIL, January 2012

[17] Security Architecture requirements (ADV_ARC) for smart cards and similar devices - Appendix 1, Version 2.0, JIL, January 2012

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