KECS-CR-08-01

ePassport Protection Profile V1.0 Certification Report

Certification No. : KECS-PP-0084-2008

Jan, 2008

National Intelligence Service
IT Security Certification Center

This document is the certification report for ePassport Protection Profile V1.0.

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Information Security Agency

Table of Contents

1. Summary

This report describes the certification results by the certification body on the evaluation results applied with requirements of APE(Protection Profile Evaluation) Class of Common Criteria for Information Security Evaluation (‘CC’ hereinafter) in relation to [ePassport Protection Profile V1.0]. This report describes the evaluation result and its soundness and confirmity.

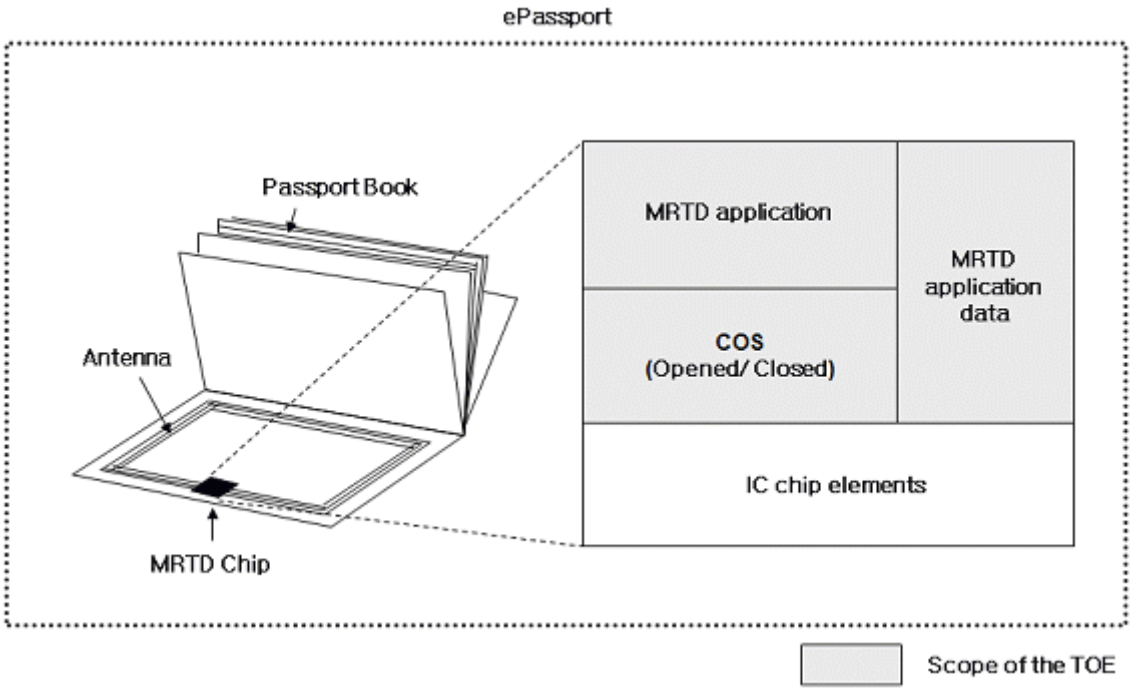
The evaluation on [ePassport Protection Profile V1.0] was conducted by Korea Information Security Agency and completed on December 17, 2007. Contents of this report have been prepared on the basis of the contents of the ETR submitted by Korea Information Security Agency. The evaluation was conducted by applying CEM. This PP satisfies all APE requirements of the CC, therefore the evaluation results was decided to be ‘suitable’.

The TOE described in [ePassport Protection Profile V1.0] is the IC chip operating system (COS), the MRTD application and the MRTD application data with the exception of hardware elements of the MRTD chip.

The ePassport is 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). The contactless IC chip used in the ePassport is referred to as the MRTD chip. The MRTD chip is loaded with the MRTD application and the IC chip operating system(COS) to support IT and information security technology for electronic storage, processing and handling of the ePassport identity data.

The MRTD application satisfies the ICAO’s Machine Readable Travel Documents, DOC 9303 Part 1 Volume 2[1] (ICAO document) and the BSI’s Advanced Security Mechanisms Machine Readable Travel Documents – Extended Access Control V1.1 2007.08 [2] (EAC specification).

Physical scope of the TOE is as follows:

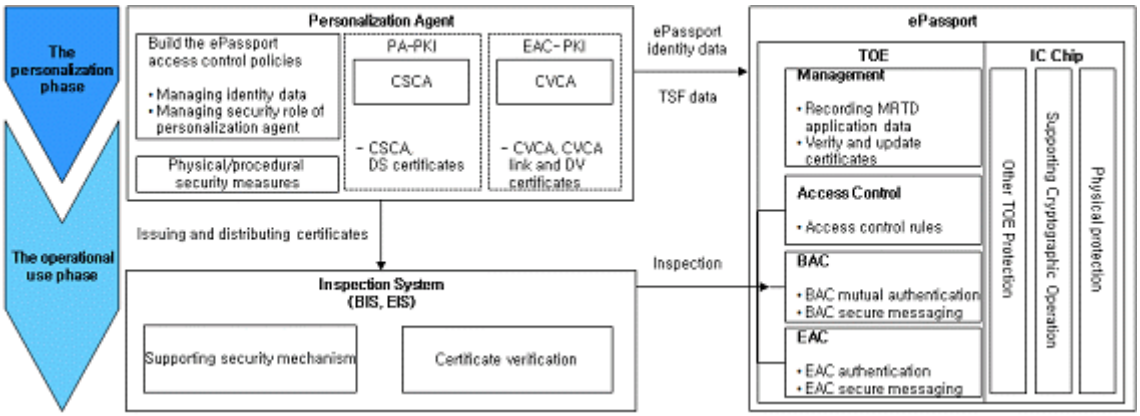


(Figure 1) Scope of the TOE

Logical scope of the TOE to protect assets include IT security functions, such as security mechanisms for the ICAO document and the EAC specifications, access control, security management and other the TOE protection, etc.

Security mechanisms of the ePassport include the PA (Passive Authentication), the BAC (Basic Access Control), the AA (Active Authentication) and the EAC (Extended Access Control), etc. However, in logical scope of the TOE, the AA is excluded as it can be substituted with the EAC.

Operational environments and logical scope of the TOE are as follows:



(Figure 2) TOE Operational Environment

IT security functions of security mechanisms provided by the TOE are as follows:

The PA of the TOE is implemented only with the function to transmit the SOD in case the Inspection System requests the SOD to verify forgery and corruption of the user data, such as the ePassport identity data, etc. Also, the BAC and the EAC of the TOE are to implement the mutual authentication protocol in order to provide Inspection System with access right to ePassport identity data and to implement the key distribution protocol necessary in establishing the secure messaging.

The access control function allows the personalization agent the access to write the TSF and user data in the phases of the Personalization. In the phases of the Operational Use, it allows SOD update and to add data in the unused user data domain.
The access to read the personal data of the ePassport holder is allowed to the Inspection System that supports the BAC and the PA security mechanisms. Also, the access to read the biometric data of the ePassport holder is allowed to the Inspection System that supports the BAC, the PA and the EAC security mechanisms.

The security management functions provide the personalization agent with the means to securely manage the MRTD application data or enable the TSF execute itself

Other TOE security functions are used to execute self-testing under self-testing conditions and to preserve a secure state under abnormal operation conditions detected by IC chip or upon occurrence of conditions for self-testing failure.

The TOE ensures domain separation and non-bypassability of the TSP in order for protection against interference and tampering by untrusted subjects. Also, it provides handling measures so that physical phenomena occurring in the course of cryptographic operation cannot be exploited by threat agent.

The CB(Certification Body) has examined the evaluation activities, provided the guidance for the technical problems and evaluation procedures, and reviewed each WPR(Work Package Report), OR(Observation Report) and ETR(Evaluation Technical Report). The CB confirmed that this PP is complete, consistent and technically sound through the evaluation results. Therefore, the CB certified that observation and evaluation results by evaluator are accurate and reasonable.

Certification validity: Information in this certification report does not guarantee that [ePassport Protection Profile V1.0] is permitted use or that its quality is assured by the government of Republic of Korea.

2. Information for Identification

[Table 1] shows information for the PP identification.

[Table 1] Shows Information for the PP Identification.

Scheme	Korea evaluation and certification guidelines for IT security (Notification No.2007-31 by the MIC, 22 Aug. 2007) Korea Evaluation and Certification Scheme for IT Security(NIS, 1 Dec. 2007)
TOE	ePassport Protection Profile V1.0
ETR	ePassport Protection Profile ETR V1.0 (Dec. 17, 2007)
Evaluation results	Suitable - Conformance claim: CC Part 2 and Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (Ministry of Information & Communication Public Notice No. 2005-25)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation v2.3
Sponsor	Korea Information Security Agency
Developer	Korea Information Security Agency
Evaluator	IT Security Evaluation Division, CC Evaluation Lab, Korea Information Security Agency Hyeonjo Kwon, Jinsu Hyeon, Seongjae Lee
Certification body	National Intelligence Service

3. Security Policies

The TOE of [ePassport Protection Profile V1.0] shall comply with the following Organizational Security Policies.

P. International Compatibility	The Personalization agent shall ensure compatibility between security mechanisms of the ePassport and security mechanism of the Inspection System for immigration.
P. Security Mechanism Application Procedures	The TOE shall ensure the order of security mechanism application according to the type of the Inspection System so that not to violate the ePassport access control policies of the Personalization agent.
P. Application Program Loading	The Personalization agent shall approve application program loading after checking that application programs loaded in the MRTD chip does not affect the secure TOE.
P. Personalization Agent	The personalization agent shall issue the ePassport in the secure manner so that to confirm that the issuing subject has not been changed and shall deliver the TOE to the Operational Use phase after verifying that the data inside MRTD chip are operating normally after issuing. The Personalization agent shall deactivate the writing function before the TOE delivery to the Operational Use phase.
P. ePassport Access Control	The Personalization agent and TOE shall build the ePassport access control policies in order to protect the MRTD application data. Also, the TOE shall regulate the roles of user.
P. PKI	The Issuing State of the ePassport shall execute certification practice to securely generate · manage a digital signature key and to generate · issue · operate · destroy certificates according to the CPS by implementing the PA-PKI and EAC-PKI according to the ePassport PKI System. Also, The Issuing State of the ePassport shall update certificates according to the policies to manage valid date of certificates, therefore securely deliver them to the Verifying State and Inspection System. When the EAC-TA provides the TOE with CVCA link certificate, DV certificate and IS certificate after the Inspection System obtaining information from EF.CVCA stored in the TOE, the TOE shall internally update certificates by verifying validity of the certificates.
P. Range of RF Communication	The RF communication distance between the MRTD chip and Inspection System shall be less than 5cm and the RF communication channel shall not be established if the page of the ePassport attached with IC chip is not opened.

4. Assumptions and Scope

4.1 Assumptions

The TOE of [ePassport Protection Profile V1.0] shall be installed and operated with the following assumptions in consideration.

A. Certificate Verification The Inspection System, such as the BIS and the EIS, verifies the SOD after verifying validity of the certificate chain for the PA (CSCA certificate → DS certificate) 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 EIS 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.

A. Inspection System The Inspection System shall implement security mechanisms of the PA, the BAC and the EAC according to the ICAO document and EAC specifications on the basis of the verifying policy of the ePassport for the ePassport holder. Also, after session ends, the BIS and the EIS shall securely destroy all information used in communication and the TOE, such as the BAC session key, the EAC session key and session information, etc.

A. IC Chip The IC chip, the underlying platform of the TOE, provides the random number generation and cryptographic operation to support security functions of the TOE. It also detects the TOE's malfunction outside the normal operating conditions and provides functions of the physical protection to protect the TOE from physical attacks using the probing and reverse engineering analysis.

A. MRZ Entropy The BAC authentication key seed takes the MRZ entropy to ensure the secure BAC authentication key.

4.2 Scope to Counter Threats

[ePassport Protection Profile V1.0] defines security threats possible to be caused on the protected assets of the TOE by external threat agent as the phase of the TOE operational environment and security mechanisms. The ePassport is used by possession of individuals without physically controlled devices, therefore both logical and physical threats is occurred. The threat agent is an external entity that attempts illegal access to assets protected by the TOE, by using the physical or logical method outside the TOE.

In this protection profile, the IC chip provides functions of physical protection in order to protect the TOE according to the A. IC Chip. Therefore, the physical threat of the IC chip itself by the high-level threat agent is not considered. Therefore, the threat agent to the TOE has the moderate level of expertise, resources and motivation.

This PP provides methods to counter the following threats caused by threat agent that has the moderate level expertise, resources and motivation. Also, all security objectives and security requirements are described so that to provide measures to counter the identified security threats.

<Threats to the TOE in the Personalization phase>

T. Application Program Interference	The threat agent may attempt access to the user and TSF data by exploiting other application programs loaded in the MRTD chip and may deactivate or bypass security functions of the TOE.
T. TSF Data Modification	The threat agent may modify the transmitted TSF data when the Personalization agent records TSF data or attempt access to the stored TSF data by using the external interface through the Inspection System.

<BAC-related Threats in the Operational Use phase>

T. Eavesdropping	In order to find out the personal data of the ePassport holder, the threat agent may eavesdrop the transmitted data by using the terminal capable of the RF communication.
T. Forgery and Corruption of Personal Data	In order to forge and corrupt the personal data of the ePassport holder stored in the MRTD chip, the threat agent may attempt access to read the user data by using the unauthorized Inspection System.
T. BAC Authentication Key Disclose	In order to find out the personal data of the ePassport holder, the threat agent may obtain the read-rights of the BAC authentication key located inside the TOE and disclose the related information.
T. BAC Replay Attack	The threat agent may bypass the BAC mutual authentication by replay after intercepting data transmitted by the TOE and the Inspection System in the initial phase of the BAC mutual authentication.

<EAC-related Threats in the Operational Use phase>

T. Damage to Biometric Data	The threat agent may disclose, forge and corrupt the biometric data of the ePassport holder by using terminal capable of the unauthorized RF communication, etc.
T. EAC-CA Bypass	The threat agent may bypass the authentication of the Inspection System so that to go through EAC-CA by using the threat agent generated EAC chip authentication public key.
T. IS Certificate Forgery	In order to obtain the access-rights the biometric data of the ePassport holder, the threat agent may attempt to bypass the EAC-TA by forging the CVCA link certificate, DV certificate and IS certificate and requesting verification of the certificates to the TOE

<BAC and EAC-related Threats in the Operational Use phase>

T. Session Data Reuse	In order to find out the transmitted data through the secure messaging, the threat agent may derive session keys from a number of cryptographic communication texts collected by using the terminal capable of wide-ranging RF communication
T. Skimming	The threat agent may read information stored in the IC chip by communicating with the MRTD Chip through the unauthorized RF communication terminal without the ePassport holder realizing it.

<Threats related to IC Chip Support>

T. Malfunction	In order to bypass security functions or to damage the TOE executable code and TSF data stored in the TOE, threat agent may occur malfunction of the TOE in the environmental stress outside the normal operating conditions.

<Other Threats in the Operational Use phase

T. ePassport Reproduction	The threat agent may masquerade as the ePassport holder by reproduction the MRTD application data stored in the TOE and forgery identity information page of the ePassport
T. Leakage to Cryptographic Key Information	By using electric power and wave analysis devices, the threat agent may obtain key information used in cryptographic technique applied to the ePassport security mechanism by analyzing information of electric power and wave emitted in the course of the TOE operation.
T. Residual Information	The threat agent may disclose to critical information by using residual information remaining while the TSF data, such as BAC authentication key, BAC session key, EAC session key, DV certificate and IS certificate, etc., are recorded and used in temporary memory.

5. PP Information

5.1 Security Functional Requirements

The TOE of [ePassport Protection Profile V1.0] defines security functional requirements as of the following.

[Table 2] Security Functional Requirements

Security functional class	Security functional component	
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation (Key Derivation Mechanism)
	FCS_CKM.2(1)	Cryptographic key distribution (KDF Seed Distribution for BAC session key generation)
	FCS_CKM.2(2)	Cryptographic key distribution (KDF Seed Distribution for EAC session key generation)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (Symmetric Key Cryptographic Operation)
	FCS_COP.1(2)	Cryptographic operation (MAC)
	FCS_COP.1(3)	Cryptographic operation (Hash Function)
	FCS_COP.1(4)	Cryptographic operation (Digital signature Verification for Certificates Verification)
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_RIP.1	Subset residual information protection
	FDP_UCT.1	Basic data exchange confidentiality
	FDP_UIT.1	Data exchange integrity
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_UAU.1(1)	Timing of authentication(BAC Mutual Authentication)
	FIA_UAU.1(2)	Timing of authentication(EAC-TA)
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1(1)	Management of TSF data (Certificate Verification Info.)
	FMT_MTD.1(2)	Management of TSF data (SSC Initialisation)
	FMT_MTD.3	Secure TSF data

	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Privacy (FPR)	FPR_UNO.1	Unobservability
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_TST.1	TSF testing

5.2 Assurance Packages

Assurance requirements of [ePassport Protection Profile V1.0] consist with assurance components in CC Part 3 and evaluation assurance level is “EAL4+.” The augmented assurance components are ADV_IMP.2, ATE_DPT.2 and AVA_VLA.3.

5.3 Strength of Function(SOF)

In [ePassport Protection Profile V1.0], ‘SOF–high’ was claimed in relation to FCS_CKM.1, FCS_COP.1(1), FCS_COP.1(2), FIA_UAU.4 and FMT_MTD.3 security functional requirements.

6. Evaluation Results

The evaluation is performed with reference to the CC V2.3 and CEM V2.3. The verdict of [ePassport Protection Profile V1.0] is the pass as it satisfies all requirements of APE(Protection Profile Evaluation) Class of CC. Therefore, the evaluation results were decided to be suitable. Refer to the ETR for more details.

• **Protection Profile Evaluation (APE)**
Evaluators conducted evaluation by applying work units of each component included in APE of CEM. Accordingly, the evaluation results of [ePassport Protection Profile V1.0] are as follows.

The PP introduction of [ePassport Protection Profile V1.0] consistently provides information necessary in PP identification, therefore the verdict of APE_INT.1 is the Pass.

The TOE description of [ePassport Protection Profile V1.0] describes the objectives and functionality of the TOE sufficiently to be understandable and is coherent, internally consistent, and consistent with all other parts of the PP. Therefore, the verdict of APE_DES.1 is the Pass.

The TOE security environment of [ePassport Protection Profile V1.0] provides a clear and consistent definition of the security problems that are induced in the TOE and its environment in terms of assumptions, threats, and OSP(organizational security policy)s. Therefore, the verdict of APE_ENV.1 is the Pass.

The security objectives of [ePassport Protection Profile] counter the identified threats, achieve the identified OSPs, and are consistent with the identified assumptions. Therefore, the verdict of APE_OBJ.1 is the Pass.

The IT security requirements of [ePassport Protection Profile V1.0] completely satisfy all the TOE security objectives and IT security requirements applied with the CC operation do not conflict with each other. Therefore, the verdict of APE_REQ.1 is the Pass.

The explicitly stated IT security requirements of [ePassport Protection Profile V1.0] are only applicable if the PP contains IT security requirements that are explicitly stated without reference to either CC Part 2 or CC Part 3. If this is not the case, all work units in this section are not applicable, and considered to be satisfied. Therefore, the verdict of APE_SRE.1 is the Pass.

[ePassport Protection Profile V1.0] is complete, consistent and technically sound, therefore is suitable to lead to the development of the ST.

Therefore, the final verdict on the APE is the **Pass**.

<Summary of the evaluation results>

Assurance Components	Evaluation Results
APE_INT.1 PP Introduction	Pass
APE_DES.1 TOE Description	Pass
APE_ENV.1 Security environment	Pass
APE_OBJ.1 Security objectives	Pass
APE_REQ.1 IT security requirements	Pass
APE_SRE.1 Explicitly stated IT security requirements	Pass

7. Recommendations

[ePassport Protection Profile V1.0] includes the minimum requirements of the ICAO document and the EAC specifications. In relation to security problems possible to occur according to the TOE implementation model, the ST author shall define additional security environments, security objectives and security requirements.

.

① The AA (active authentication) is optional in the EAC specifications. Therefore, the AA security mechanism is not included in this PP. So, the ST author can add the AA security mechanism according to the Issuing policy of the ePassport. In case of adding AA security mechanism, the ST author shall additionally define security environments, security objectives and security requirements.

② The TOE life cycle and Personalization agent authentication mechanism, etc. may differ according to the Issuing policy of the ePassport. Therefore, the Personalization agent authentication mechanism is not included in this PP. When the personalization agent authentication mechanism is determined by the personalization agent in accordance with the issuing policy of the ePassport, the ST author may add or modify TOE description, security environments, security objectives and security requirements by considering these details.

③ [ePassport Protection Profile V1.0] is limited to the specific operational environment of the ePassport system and the ePassport security mechanisms. Therefore, this PP includes a large number of “application notes” unlike other general PP. The ST author may demand the CB for interpretations in case policies of the personalization agent conflict with the contents of this PP.

8. acronyms

The following acronyms have been used in this report.

AA	Active Authentication
BAC	Basic Access Control
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
CB	Certification Body
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IS	Inspection System
MRTD	Machine Readable Travel Documents
OR	Observation Report
PP	Protection Profile
PA	Passive Authentication
TOE	Target of Evaluation
WPR	Work Package Report

9. References

The CB has used the following documents to produce this certification report.

[1] Common Criteria for Information Technology Security Evaluation (Ministry of Information & Communication Public Notice No. 2005-25)

[2] Common Methodology for Information Technology Security Evaluation V2.3

[3] Korea evaluation and certification guidelines for IT security (Notification No.2007-31 by the MIC, 22 Aug. 2007)

[4] Korea Evaluation and Certification Scheme for IT Security(NIS, 1 Dec. 2007)

[5] ePassport Protection Profile ETR V1.0(Dec. 17, 2007)