KECS-CR-09-22

ePassport Protection Profile V2.0
Certification Report

Certificate No. : KECS-PP-0163-2009

May 2009

National Intelligence Service IT Security Certification Center

This document is the certification report for ePassport Protection Profile V2.0.

Cetrification Body

IT Security Certification Center, National Intelligence Service

Evaluation Body

Korea Information Security Agency

Table of Contents

1. Summary

This report states the outcome of the [ePassport Protection Profile V2.0] evaluation. This Chapter summarizes the ePassport PP evaluation results and confirms the overall results, i.e. that the PP evaluation has been properly carried out, that Class APE of CC Part 3 V3.1 R2 and Class APE of CEM V3.1 R2 have been correctly applied.

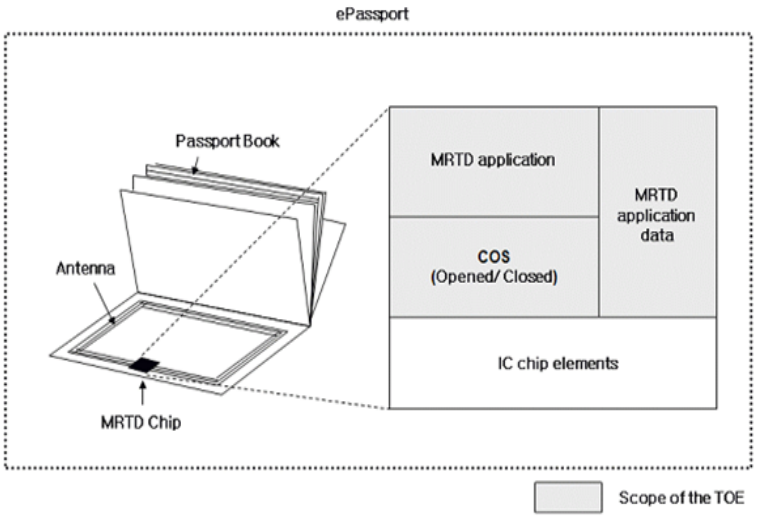
The ePassport PP evaluation was conducted by Korea Information Security Agency (KISA). It was completed on April 27, 2009 and validated by National Intelligence Service(NIS) in May, 2009. The Evaluation Technical Report (ETR) for ePassport PP was written by KISA and served as the principal basis for this Certification Report(CR).

The ePasssport PP evaluation has met all evaluator activities for a PP evaluation in both the APE CC Part 3 V3.1 R2 and CEM V3.1 R2. At the conclusion of the ePassport PP evaluation all APE CC and CEM evaluator activities were passed.

The ePassport is the electronic travel document described in Doc 9303 Part 1 Volume 2 of the International Civil Aviation Organization (ICAO), which is integrated into the contactless IC chip of machine readable travel document (MRTD chip). Passport holder's information and other data were stored on MRTD chip. IC Chip Operating System (COS) and ePassport application which provide the security mechanisms to protect the authenticity, originality, and confidentiality of the data stored on MRTD chip were loaded into the ePassport MRTD Chip.

The ePassport is composed of passport data pages, cover, MRTD chip located in cover, and antenna. COS and ePassport application are loaded and ePassport application data is stored on MRTD chip.

The Target of Evaluation (TOE) defined in the ePassport PP is the COS and ePassport application but IC Chip composed of CPU, co-processor, memory, I/O interface, and other element is out of The TOE. The security mechanisms of ePassport application address ICAO Basic Access Control(BAC) and BSI Extended Access Control V1.11(EAC). Physical scope of the TOE is depicted in Figure 1.



(Figure 1) Scope of the TOE

External IT entities interacting with the TOE from outside of th TOE boundary are organization authorized to issue MRTD and inspection system. An issuing organization, i.e. organization authorized to issue MRTD, stores user data and TSF data in MRTD to personalize MRTD for passport holder. And it establishes and operates the PKI for ePassport. Inspection system is a technical system used by an issuing organization and operated by a governmental organization. It verifies the passport presenter as the ePassport holder. While BIS is inspection system supporting BAC, EIS is inspection system supporting both BAC and EAC V1.11.

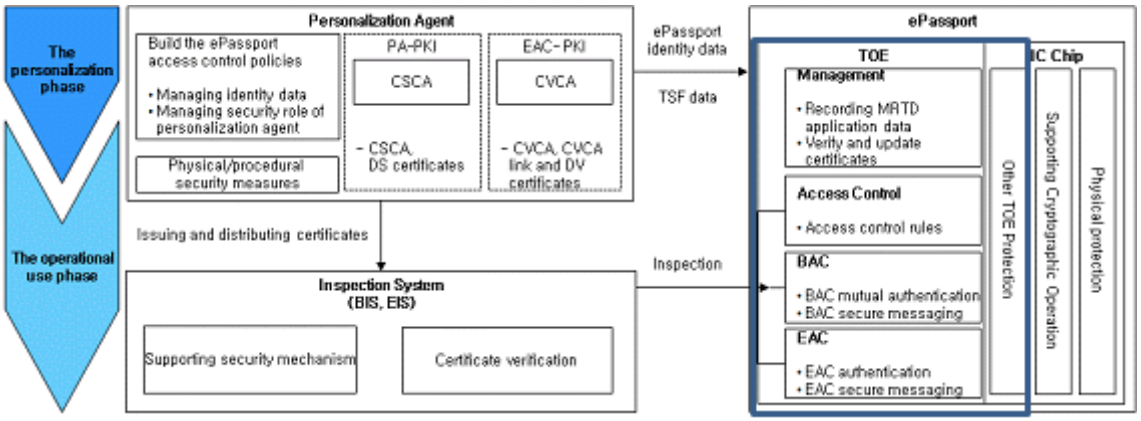
The IC chip as a platform to be used by the TOE serves cryptographic operation by its crypto processor during the TOE security mechanisms processing. And it provides protection against disclosure of user data and TSF data stored and/or processed in the TOE, against the disclosure/reconstruction of the TOE or against the disclosure of other critical operational information such as the physical attack using revers-engineering and probing.

The TOE life cycle is described in terms of the four life cycle phases: Phase 1 “Development”, Phase 2 “Manufacturing”, Phase 3 “Personalization of the MRTD”, Phase 4 “Operational Use”. The intention of the PP is to consider at least the phases 1 and parts of phase 2 as part of the evaluation and therefore to define the TOE delivery according to CC after this phase 2 or later. Since specific production steps of after phase 2 may be different according to each policy implemented by the issuing organization, these are not part of the CC evaluation under ALC.

The TOE provides BAC(Basic Access Control) and EAC(Extended Access

Control) security mechanisms to grant the access-rights to the inspection system according to the ePassport identity data. Also, the TOE provides security characteristics such as the access control, security management, other the TSF protection, etc.

[Figure 2] shows the operational environment of the TOE and logical scope.



[Figure 2] TOE Operational Environment and Logical scope

Logical scope of the TOE includes security features such as security mechanisms for the ePassport specifications(ICAO, "Machine Readable Travel Documents, Doc 9303 Part1 Volume2, 2006) and the EAC specifications(BSI, "Advanced Security Mechanisms Machine Readable Travel Documents-Extended Access Control V1.11, 2008), access control, security management, and other the TOE protection, etc.

【 ePassport Security Mechanisms】

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.

- 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.
- 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.

【 Access Control】

The TOE allows the access for the ePassport application data only to the external entities granted with access-rights according to the ePassport access control policies of issuing organization.

- The TOE provides only **the issuing organization** to writing function on the user data and TSF data in the Personalization phase.
- The TOE allows the reading user data stored on MRTD chip to BIS. But the biometric data of th user data is excluded.
- The TOE allows the reading all user data including the biometric data stored on MRTD chip to EIS.

【 Security Management】

The security management functions provide the personalization agent with the means to securely manage the ePassport user data and TSF data. Alos the TSF executes itself some security management functions such as updating the CVCA certificate and the current date and initializing the identifier for cecure messaging, etc.

【 Other TOE Protection】

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. Also, it provides handling measures so that physical phenomena occuring 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 V2.0] 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] Information for the PP Identification

Scheme	Korea evaluation and certification guidelines for IT security (16 July, 2008) Korea Evaluation and Certification Scheme for IT Security (20 March, 2009)
TOE	ePassport Protection Profile V2.0
ETR	ePassport Protection Profile ETR V1.0 (27 April, 2009)
Evaluation results	Verdict for APE Class : Pass Conformance claim : Common Criteria V3.1r2 - CC Part 2 Conformant - CC Part 3 Conformant
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1r2, CCMB, 2007. 9.
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation, Version 3.1r2, CCMB, 2007. 9.
Sponsor	Korea Information Security Agency
Developer	Korea Information Security Agency
Evaluator	IT Security Evaluation Division, CC Evaluation Lab, Korea Information Security Agency Eunkyung Lee, Ilhee Cho
Certification body	National Intelligence Service

3. Security Policies

The TOE of [ePassport Protection Profile V2.0] 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 and manage a digital signature key and to generate, issue, operate and 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 V2.0] 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' 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 V2.0] 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. 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. 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. 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. 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 V2.0] 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 behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1(1)	Management of TSF data (Certificate Verification Info.)
	FMT_MTD.1(2)	Management of TSF data (SSC Initialization)
	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_TST.1	TSF testing

5.2 Assurance Packages

Assurance requirements of [ePassport Protection Profile V2.0] consist with assurance components in CC Part 3 and evaluation assurance level is “EAL4+.”The augmented assurance components are ADV_IMP.2 and AVA_VLA.4.

6. Evaluation Results

The evaluation is performed with reference to the CC V3.1 and CEM V3.1. The verdict of [ePassport Protection Profile V2.0] 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.

The PP introduction of [ePassport Protection Profile V2.0] consistently provides information necessary in PP identification. As a result of the evaluation the verdict PASS is confirmed for the assurance component APE_INT.1 of the class APE.

The conformance claim of [ePassport Protection Profile V2.0] properly describes the PP and CC conformed. As a result of the evaluation the verdict PASS is confirmed for the assurace component APE_CCL.1 of the class APE.

The security problem definition of [ePassport Protection Profile V2.0] clearly defines the security problems which shall be addressed in the TOE and its operational environment. As a result of the evaluation the verdict PASS is confirmed for the assurance component APE_SPD.1 of the class APE.

The security objectives of [ePassport Protection Profile V2.0] adequately and completely address the security problem definition and clearly define the division of the problem between the TOE and its operational environment. As a result of the evaluation the verdict PASS is confirmed for the assurance component APE_OBJ.2 of the class APE.

[ePassport Protection Profile V2.0] doesn't include the extended components and all work units in this section are not applicable and considered to be satisfied. As a result of the evaluation the verdict PASS is confirmed for the assurance component APE_ECD.1 of the class APE.

The security requirements of [ePassport Protection Profile V2.0] are clear, unambiguous and well defined. As a result of the evaluation the verdict PASS is confirmed for the assurance component APE_REQ.2 of the class APE.

The evaluators determine the result of [ePassport Protection Profile V2.0] evaluation as of the following.

[ePassport Protection Profile V2.0] is complete, consistent and technically sound, therefore is suitable to lead to the development of the ST.

The overall verdict PASS is confirmed for the assurance components of the class APE as shown in [Table 3].

[Table 3] TOE Evaluation Results

Assurance class	Assurance Components	Evaluator Requirements	Evaluation Results		
			Evaluator Requirements	Assurance Components	Assurance class
APE	APE_INT.1	APE_INT.1.1E	Pass	Pass	Pass
	APE_CCL.1	APE_CCL.1.1E	Pass	Pass	
	APE_SPD.1	APE_SPD.1.1E	Pass	Pass	
	APE_OBJ.2	APE_OBJ.2.1E	Pass	Pass	
	APE_ECD.1	APE_ECD.1.1E	Pass	Pass	
		APE_ECD.1.2E	Pass		
	APE_REQ.2	APE_REQ.2.1E	Pass	Pass	

7. Recommendations

[ePassport Protection Profile V2.0] 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 problems, 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 V2.0] is limited to the specific operational environment of the ePassport system and the ePassport security mechanisms. Therefore, this PP includes a large number of “pplication 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

(1) Common abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
RAM	Random Access Memory
SFP	Security Function Policy
TOE	Target of Evaluation
TSF	TOE Security Functionality

(2) Terminologies

DV : Document Verifier	an organizational unit that manages inspection systems by issuing Inspection System certificates
Personalization Agent	The agent receives the ePassport identity data from the Reception organization and generates the SOD by digital signature on the data. After recording them in the MRTD chip, the personalization agent generates TSF data and stores it in the secure memory of the MRTD chip. The agent also operates PA PKI and/ or EAC PKI
SOD : Document Security Object	The SOD refers to the ePassport identity data and the ePassport authentication data recorded in the Personalization phase by the Personalization agent that is signed by the Personalization agent with the digital signature generation key. The SOD is an object implemented with signed data type of 'RFC 3369 cryptographic message syntax, 2002.8' and encoded with DER method.
IS : Inspection System	As an information system that implements optical MRZ reading function and the security mechanisms (PA, BAC, EAC and AA, etc.) to support the ePassport inspection, the IS consists with a terminal that establishes the RF communication with the MRTD chip and the system that transmits commands to the MRTD chip through this terminal and processes responses for the commands
BIS : BAC Inspection System	The IS implemented with the BAC and the PA security mechanisms

EIS : EAC Inspection System	The IS to implement the BAC, the PA and the EAC security mechanisms and the AA as an option
Probing	Attack to search data by inserting probing pin in the IC chip

9. References

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

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1r2, CCMB, 2007. 9.

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1r2, CCMB, 2007. 9.

[3] Korea evaluation and certification guidelines for IT security (16 July, 2008)

[4] Korea Evaluation and Certification Scheme for IT Security (20 March, 2009)

[5] ePassport Protection Profile ETR V1.0 (27 April, 2009)