효율성이 강화된 전자여권 통합 인증 메커니즘

e-Passport Integrated Authentication Mechanisms with Improved Efficiency

이 동 범* 고 웅** 곽 진**
Dongbum Lee Woong Go Jin Kwak

요 약

전자여권(e-Passport) 시스템은 새로운 형태의 출입국 관리 시스템으로서, 기존 여권보다 보안 기능이 강화되고 자동화된 출입국 관리를 할 수 있다는 장점으로 인해 전 세계적으로 도입하기 위한 연구가 활발히 진행되고 있다. 전자여권은 칩에 개인 신원 정보와 바이오정보를 저장하고, 비접촉식 무선 인식 기술을 이용하여 판독시스템과 통신을 제공하게 된다. 하지만 기존의 RFID 기술에서 발생하는 도청, 데이터 위·변조, 복제와 같은 문제점과 개인의 고유한 바이오정보 노출이라는 문제점을 내재하고 있다. 따라서 본 논문에서는 보안 취약점을 방지하는 전자여권 인증 메커니즘들에 대한 보안 취약점을 분석하고 계산량을 감소시킬 수 있는 전자여권 인증 메커니즘을 제안한다. 또한 각 인증 메커니즘의 효율성에 대하여 분석한다.

Abstract

e-Passport system is new type of emigration and immigration control system and it is a research to introduce the e-Passport Authentication Protocol with Improved Efficiency is lively proceeded over the entire world. The e-Passport's chip has a biometric information and personal identification information, Radio Frequency Identification(RFID) technology is used for communication with the Inspection System(IS). However, the feature of the RFID system may bring about various security threats such as eavesdropping, data forgeries, data alternation, cloning, biometric data-leakage. Therefore, in this paper, we analyse the e-Passport system's authentication protocol to protect vulnerability and proposed e-Passport system's authentication protocol reduce computation. Also, we compared their efficiency.

☞ keyword : e-Passport, Authentication, Key agreement protocol, Inspection system

1. 서 론

최근 활발하게 연구되고 있는 전자여권은 2001년 미국에서 발생한 9·11 테러 사태 이후 강화된 출입국 절차로써 미국애국법(US Patriot Act)에 따라 2002년에 국토안보국 (DHS : Department of Homeland Security)을 신설하여 2006년 10월 26일 이후 발급되는 27개 비자면제국가를 대상으로 전자여권 발급을 의무화하는 법률을 규정하였다. 또한 미국 주도하에 전자여권은 UN 산하 국제 민간항공기구(ICAO : International Civil Aviation Organization)에서 전자여권 개념을 확립하고, 국제 호환성을 확보하기 위한 국제 표준화 작업으로 ISO/IEC JTC1 SC 17의 기술 문서 Doc. 9303에서 요구하는 국제 표준 ISO/IEC 14443에 따라 비접촉식 스마트 기능의 IC(Integrated Circuit) 칩에 얼굴, 지문, 홍채 이미지와 같은 바이오정보[1]와 여권 소지자의 개인 정보, 그리고 전자여권 인증 메커니즘을 위해 사용하는 키들이 탑재되어 있다. 또한 IC 칩 내의 데이터 무결성을 보장하는, 즉 데이터가 변경되지 않았음을 증명하기 위해 개인

* 준 회 원 : 순천향대학교 정보보호학과 석사과정
dblee@sch.ac.kr
** 준 회 원 : 순천향대학교 정보보호학과 석사과정
wgo@sch.ac.kr
*** 종신회원 : 순천향대학교 정보보호학과 교수
jkwak@sch.ac.kr (교신저자)
[2008/11/19 투고 - 2008/11/29 심사 - 2009/03/04 심사완료]

신상정보에 대한 해쉬 연산을 표준화된 논리적 데이터 구조(LDS : Logical Data Structure)에 맞게 각각의 데이터 그룹(DG : Data Group)에 개인 신상 정보를 기록한다.

전자여권은 기존 여권을 이용한 출입국 관리 시스템의 단점을 보완하고, 여권 소지자의 편리성과 보안성을 고려한 차세대 출입국 관리 시스템이다. 그러나 전자여권을 이용한 개인 식별 기술은 전자여권 칩과 판독시스템 사이의 물리적인 접촉 없이 인식이 가능하다는 장점과 함께 도청 공격, 데이터 위·변조, 바이오정보 노출, 전자여권 복제 등의 개인 신원 정보 침해 문제를 발생 시킬 수 있다. 이러한 개인 신원 정보 침해 문제를 해결하기 위해서 ICAO에서는 많은 연구가 진행되어 왔으며, PA(Passive Authentication), BAC(Basic Access Control), AA(Active Authentication)와 같은 전자여권 인증 메커니즘들이 있다. 또한 유럽 연합(European Union)을 중심으로 EAC(Extended Access Control) 인증 메커니즘이 제안되고 있다.

본 논문에서는 전자여권 인증 메커니즘의 안전성 및 효율성에 대하여 분석하고 사용자 프라이버시를 보호하면서 전자여권 칩과 판독시스템 사이의 계산량을 감소 시킬 수 있는 효율성이 강화된 전자여권 시스템을 제안한다. 제안하는 인증 메커니즘은 도청 공격, 데이터 위·변조, 바이오정보 노출, 칩 복제, 인증서 위조에 안전하다는 장점을 가지고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 전자여권 시스템에 대해서 설명하고, 3장에서는 보안 취약점을 방지할 수 있는 전자여권 인증 메커니즘들에 대해서 기술한다. 4장에서는 제안하는 전자여권 인증 메커니즘에 대해서 구체적으로 설명하고, 5장에서는 각 방식에 대한 분석 결과를 토대로 안전성 및 효율성을 분석한다. 마지막으로 6장에서 결론을 맺는다.

2. 전자여권 시스템

전자여권 시스템은 발급기관, 검증기관, 판독시스템, 전자여권으로 구성되며 각각의 구성과 기능은 다음과 같다. (표 1)은 전자여권 시스템에서 사용하는 인증서의 종류를 설명한다[15].

(표 1) 전자여권 시스템에 사용하는 인증서의 종류

인증서 종류	설 명
CSCA 인증서	PA-PKI 최상위 인증기관의 전자서명생성키에 대한 전자서명검증키의 유효성을 증명한 인증서(Country Signing CA Certificate)
DS 인증서	PA-PKI 최상위 인증기관의 전자서명생성키로 서명한 발급기관의 인증서로 판독시스템이 PA 메커니즘의 SO_D를 검증하기 위해 사용하는 인증서(Document Signer Certificate)
CVCA 인증서	EAC-PKI 최상위 인증기관이 CVCA 링크 인증서, DV 인증서의 유효성을 증명하기 위해 해당 전자서명검증키에 EAC-PKI 최상위 인증기관의 전자서명생성키로 전자서명한 값을 포함한 인증서(Country Signing CA Certificate)
CVCA 링크 인증서	EAC-PKI 최상위 인증기관이 CVCA 인증서 유효기간 만료 이전에 새로운 CVCA 인증서를 생성한 후 예전 CVCA 인증서에 대응하는 전자서명생성키로 전자서명한 인증서(CVCA Link Certificate)
DV 인증서	판독시스템의 전자서명검증키 유효성을 증명하기 위해 검증기관의 전자서명생성키로 판독시스템의 전자서명검증키에 전자서명한 값을 포함한 인증서(Document Verifier Certificate)
IS 인증서	EAC-TA 과정에서 전자여권 IC 칩이 판독시스템이 전송한 전자서명 값을 검증하기 위해 사용하는 인증서로 검증기관의 전자서명생성키로 EAC 판독시스템의 전자서명검증키에 대해 전자서명한 인증서(Inspection System Certificate)

❖ 발급 기관

전자여권 소지자의 인증 데이터에 전자서명을 수행한 후 보안 객체(SO_D : Document Security Object)를 생성하여 전자여권 칩에 저장한다[3]. 또한 전자여권 소지자의 데이터 위·변조 검증에

필요한 전자서명키를 생성하고 CSCA / DS / CVCA / CVCA 링크 / DV 인증서의 생성·발급·관리 등 인증 업무를 수행한다.

❖ 검증 기관

전자여권 칩의 접근권한과 유효기간 제한을 위한 인증 관리 기관으로서 CVCA / CVCA 링크 / DV 인증서를 이용하여 IS 인증서를 생성한 후 판독시스템으로 전송한다.

❖ 판독시스템

출입국 대상자들의 개인 신상 정보, 인증 정보를 이용하여 전자여권 칩과 질의-응답(Challenge-Response)을 통해 출입국 심사 업무를 처리할 수 있는 시스템이다.

❖ 전자여권

(그림 1)과 같이 신원 정보면, ICAO 로고, 기계판독영역, 비접촉식 IC 칩으로 구성되며 각각의 기능은 다음과 같다.

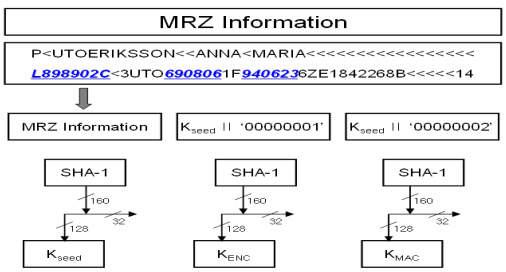
(그림 1) 전자여권 구성

- 신원정보면 : 신원정보면(Data Page)은 여권번호, 국적, 생년월일, 성별, 발급일, 여권 유효기간, 발행관청 등 육안으로 판별할 수 있는 정보
- ICAO 로고 : ICAO에서 제정한 국제 로고로서 여권에 비접촉식 스마트 기능의 IC 칩이 내장되어 있음을 의미하며, 전자여권을 발급한 나라의 여권 앞 페이지 하단에 로고를 표시하도록 권고[4]
- 기계판독영역 : 기계판독영역(MRZ : Machine Readable Zone)은 ICAO에서 표준으로 권고하고 있는 전자여권의 하단에 위치하며, OCR-B 문자를 사용하여 여권 소지자의 정보를 판독시스템이 쉽게 판독 할 수 있도록 인쇄된 영역[13]
- 비접촉식 IC 칩 : 전자여권에 내장된 비접촉식 IC 칩은 바이오정보와 여권 소지자의 개인정보 등을 데이터 그룹에 저장하고, 전자여권의 보안을 위해 사용하는 키들을 칩의 보호 메모리 영역에 탑재되어 있다. 또한 데이터가 변경되지 않았음을 증명하기 위해 개인 신상 정보에 대한 해쉬 연산(SO_D)을 표준화된 논리적 데이터 구조(LDS)에 맞게 저장[5][11]

3. 전자여권 인증 메커니즘

3.1 기본 접근 제어

기본 접근 제어(Basic Access Control)는 ICAO의 필수 요구사항이다. 전자여권 MRZ 데이터의 여권번호, 생년월일, 여권 유효기간을 이용하여 BAC 인증키를 생성하거나 전자여권 칩에 저장된 BAC 인증키를 이용하여 칩과 판독시스템 사이의 상호 인증을 수행한다. 상호 인증 수행 후, 전자여권 소지자의 개인 신상 정보를 판독시스템으로 전송하기 위해서 3DES 기반 키 분배 프로토콜을 통해 BAC 세션키로 암호화하고 MAC 값을 생성하여 칩과 판독시스템 사이의 안전한 통신 채널을 형성하여 비밀성과 무결성을 제공한다. (그림 2)는 전자여권 인증 메커니즘에서 이용하는 키를 유도하는 과정을 나타낸다[6][7][9].



(그림 2) 키유도 메커니즘

3.2 수동적 인증

수동적 인증(PA : Passive Authentication)은 ICAO의 필수 요구사항이다. 전자여권 칩의 LDS에 저장되어 있는 데이터 그룹들(DGs : Data Groups)의 해쉬값을 포함하는 보안객체(SO_D : Document Security Object)를 이용한다. SO_D는 발급기관이 전자여권 발급단계에서 기록한 전자여권 소지자 정보 및 인증정보에 발급기관의 전자서명생성키로 서명한 보안 객체이다. 이 방식은 전자여권 칩의 SO_D에 저장되어 있는 해쉬값과 판독시스템이 생성한 해쉬값을 비교하여 전자여권 데이터의 위·변조를 확인한다[12].

3.3 능동적 인증

능동적 인증(AA : Active Authentication)은 전자여권 칩에 내장된 키쌍을 이용하여 전자여권 복제를 방지하는 메커니즘이다. AA 공개키는 데이터 그룹의 DG15에 저장되어 있고, AA 비밀키는 칩의 안전한 메모리(Secure Memory)에 저장되어 판독시스템과 질의-응답(Challenge-Response) 프로토콜에 사용된다.

3.4 확장 접근 제어

확장 접근 제어(EAC : Extended Access Control)는 EU에서 제안한 인증 메커니즘이다. 여권 소지자의 전자여권 칩에 저장된 바이오 정보에 대한 접근을 통제하며 판독시스템으로 전송할 때 기본 접근 제어 메커니즘보다 강화된 통신 채널을 형성하여 칩과 판독시스템 사이의 비밀성과 무결성을 제공한다[8]. 이 메커니즘은 칩 인증(CA : Chip Authentication)과 터미널 인증(TA : Terminal Authentication)으로 구분된다.

3.4.1 칩 인증

칩 인증은 Ephemeral-Static DH 키분배 프로토콜을 이용해서 전자여권 칩의 안전한 통신과 암시적 단방향 인증(implicit unilateral authentication)을 제공한다[10][14].

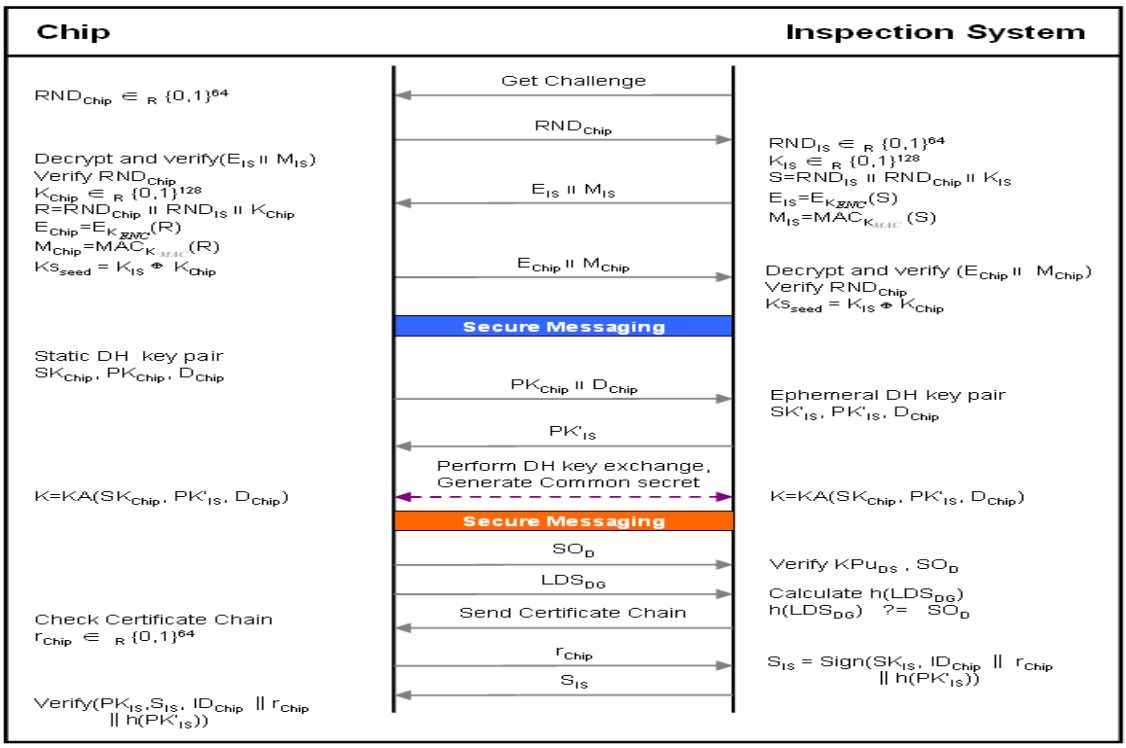
3.4.2 터미널 인증

터미널 인증은 전자여권 칩이 확장 접근 제어를 지원하는 판독시스템을 인증하기 위한 질의-응답 프로토콜로써 판독시스템의 명시적인 단방향 인증(explicit unilateral authentication)을 수행한다[2].

4. 제안하는 전자여권 인증 메커니즘

여권 소지자의 프라이버시를 보호할 수 있는 인증 메커니즘으로 수동적 인증, 기본 접근 제어, 능동적 인증, 칩 인증, 터미널 인증이 있다. 이러한 전자여권 인증 메커니즘은 질의-응답 방식을 이용해서 칩과 판독시스템 사이의 상호 인증을 수행하여 도청 공격, 데이터 위·변조, 바이오정보 노출, 칩 복제, 인증서 위조에 대한 안전성을 제공한다.

그러나 메커니즘들의 중복된 기능들로 인하여 칩과 판독시스템 사이의 계산량을 증가시키는 단점이 있다. 그러므로 본 논문에서는 사용자의 프라이버시를 안전하게 보호 할 수 있고, 전자여권 칩과 판독시스템 사이의 계산량을 감소 시킬 수 있는 인증 메커니즘에 대하여 제안한다. (그림 3)은 본 논문에서 제안하는 전자여권 인증 메커니즘을 나타낸다.



(그림 3) 제안하는 전자여권 시스템

[시스템 파라미터]

- RND_{Chip}, K_{Chip} : 칩에서 생성한 난수
- RND_{IS}, K_{IS} : 판독시스템에서 생성한 난수
- ‖ : 연접
- K_{ENC} : 키유도 메커니즘을 이용하여 생성한 암호키(BAC 인증키)
- K_{MAC} : 키유도 메커니즘을 이용하여 생성한 MAC 키(BAC 인증키)
- S, R : 칩과 판독시스템에서 생성한 난수를 연접하여 저장한 값
- E_{IS} : 판독시스템에서 S를 K_{ENC}로 암호화하고 저장한 값
- M_{IS} : 판독시스템에서 S를 K_{MAC}로 MAC를 계산한 값
- E_{Chip} : 칩에서 R을 K_{ENC}로 암호화하고 저장한 값
- M_{Chip} : 칩에서 R을 K_{MAC}로 MAC를 계산한 값
- SK_{Chip} : 칩의 보호 메모리 영역에 내장된 Static DH 비밀키(CA 비밀키)
- PK_{Chip} : 데이터 그룹의 DG14에 내장된 Static DH 공개키(CA 공개키)
- D_{Chip} : 판독시스템에서 새로운 통신을 할 때 Ephemeral DH 키쌍을 생성할 때 이용하는 칩의 도메인 파라미터
- SK'_{IS} : 판독시스템에서 생성된 Ehemeral DH 임시 비밀키
- PK'_{IS} : 판독시스템에서 생성된 Ephemeral DH 임시 공개키
- KA : 공유되는 비밀키 K를 생성하는 연산을 표기
- K : CA 세션키를 유도하기 위한 비밀키
- C_{DS} : PA-PKI 최상위 인증기관의 전자서명 생성키로 서명한 발급기관의 인증서

- KPu_{DS} : SOD가 위조되지 않았음을 판별하기 위해서 사용하는 DS 공개키
- LDS_{DG} : 칩의 LDS에 저장되어 있는 데이터 그룹
- h() : 일방향 해쉬 함수
- $h(LDS_{DG})$: 판독시스템이 칩에서 데이터를 전송받아 생성한 데이터 그룹 해쉬값
- $SO_{D_{DG}}$: SO_D에 내장된 데이터 그룹 해쉬값
- SK_{IS} : 판독시스템의 Static 인증 비밀키(TA 비밀키)
- PK_{IS} : 판독시스템의 Static 인증 공개키(TA 공개키)
- $h(PK'_{IS})$: 판독시스템에서 생성한 Ephemeral DH 공개키를 해쉬한 값
- r_{Chip} : 칩에서 생성한 난수
- ID_{Chip} : 판독시스템이 MRZ에서 읽어 들인 여권 번호

4.1 인증 과정

〔Step 1. 보안 채널(데이터 보호) 생성 과정〕

(1) 판독시스템은 칩으로 난수를 요청한다.

(2) 칩은 8byte의 난수를 생성(①)하여 판독시스템으로 전송한다.

① $RND_{Chip} \in_R \{0,1\}^{64}$

(3) 판독시스템은 8byte의 난수(②)와 16byte의 난수(③)를 생성하고, 칩에서 전송 받은 난수(RND_{Chip})와 함께 연접한 결과를 S에 저장(④)한다. 판독시스템은 안전한 통신을 제공하기 위해서 S를 키유도 메커니즘에서 생성한 BAC 인증용 암호키(K_{ENC})로 암호화(⑤)하고 그 결과를 E_{IS}로 저장한 후, MAC 키(K_{MAC})를 기초로 해서 MAC를 연산한 값을 M_{IS}에 저장(⑥)한다.

② $RND_{IS} \in_R \{0,1\}^{64}$

③ $K_{IS} \in_R \{0,1\}^{128}$

④ $S = RND_{IS} \parallel K_{IS} \parallel RND_{Chip}$

⑤ $E_{IS} = EK_{ENC}(S)$

⑥ $M_{IS} = MAC_{K_{MAC}}(S)$

(4) 판독시스템은 전송받은 데이터(RND_{Chip})가 정당한 칩으로부터 전송되어졌는지 확인하기 위해서 E_{IS}와 M_{IS}를 연접(⑦)해서 칩으로 전송한다.

⑦ $E_{IS} \parallel M_{IS}$

(5) 칩은 판독시스템에서 전송 받은 데이터($E_{IS} \parallel M_{IS}$)가 정당한 판독시스템으로부터 전송되었는지 확인하기 위하여 BAC 인증용 MAC 키(K_{MAC})로 MAC 값(M_{IS})을 검증한 후 복호화(⑧)하여 RND_{Chip}을 확인(⑨)한 후, 16byte의 난수를 생성(⑩)한다. 그 후 판독시스템에서 전송 받은 난수(RND_{IS})와 칩에서 생성한 난수(RND_{Chip}, K_{Chip})를 연접하여 R에 저장(⑪)한다. 칩은 R을 K_{ENC}로 암호화(⑫)하고, 그 결과를 E_{Chip}으로 저장한 후 K_{MAC}를 기초로 해서 MAC를 연산한 값을 M_{Chip}에 저장(⑬)한다.

⑧ Decrypt and verify($E_{IS} \parallel M_{IS}$)

⑨ Verify RND_{Chip}

⑩ $K_{Chip} \in_R \{0,1\}^{128}$

⑪ $R = RND_{Chip} \parallel RND_{IS} \parallel K_{Chip}$

⑫ $E_{Chip} = E_{K_{ENC}}(R)$

⑬ $M_{Chip} = MAC_{K_{MAC}}(R)$

(6) 칩은 BAC 인증키로 암호화 한 값(E_{Chip})과 MAC를 생성한 값(M_{Chip})을 연접(⑭)하여 판독시스템으로 전송한다.

⑭ $E_{Chip} \parallel M_{Chip}$

(7) 판독시스템은 전송 받은 E_{Chip}을 복호화 한 후 전송받은 데이터($E_{Chip} \parallel M_{Chip}$)가 정당한 칩으로부터 전송되었는지 확인하기 위하여 M_{Chip}을 연산하여 비교 후 동일하다면 정당

한 칩으로부터 전송되어졌다고 검증(⑮)하고 RND_{IS}를 확인(⑯)한다.

⑮ Decrypt and verify (E_{Chip} ‖ M_{Chip})

⑯ Verify RND_{IS}

(8) 칩과 판독시스템은 각각 K_{IS}에 K_{Chip}을 XOR 연산을 취해 키 시드 값(Ks_{seed})을 생성(⑰)한 후 3DES 기반 키분배 프로토콜을 통하여 상호 교환한 Ks_{seed}의 값으로부터 키유도 메커니즘을 이용하여 판독시스템과 칩 사이에서 안전한 메시지 교환을 위해 사용되는 BAC 암호용 세션키(KS_{ENC})와 BAC MAC용 세션키(KS_{MAC})를 유도하여 안전한 통신 채널을 구성하게 된다.

⑰ $Ks_{seed} = K_{IS} \oplus K_{Chip}$

〔Step 2. 보안 채널(바이오정보 보호) 생성 과정〕

(1) 칩은 LDS의 DG14에 저장된 Static DH 공개키와 도메인 파라미터를 연접(⑱)하여 판독시스템으로 전송한다.

⑱ PK_{Chip} ‖ D_{Chip}

(2) 판독시스템은 칩으로부터 전송받은 D_{Chip}을 이용해서 Ephemeral DH 키 쌍(SK'_{IS}, PK'_{IS})을 생성하고, 칩으로 판독시스템의 임시 공개키(PK'_{IS})를 전송하여 키분배 프로토콜을 수행한다.

(3) 칩과 판독시스템은 공유 비밀키 K를 생성한 후 키 유도 메커니즘을 이용해서 세션키를 유도(⑲)한다.

⑲ $K = KA(SK_{Chip}, PK'_{IS}, D_{Chip})$

(4) 칩은 판독시스템의 Ephemeral DH 공개키를 해쉬한 값(⑳)을 터미널 메커니즘에 이용하기 위해서 저장한다.

⑳ $(h(PK'_{IS}))$

(5) 칩 인증 메커니즘을 수행 후 전자여권 칩과 판독기간 바이오정보를 전송하기 위해서 K로부터 유도된 세션키를 이용해서 보안이 강화된 통신 채널을 형성한다.

〔Step 3. 전자여권 칩 인증 과정〕

(1) 판독시스템은 칩에 내장된 데이터의 무결성을 확인하기 위해서 칩으로부터 SO_D를 획득한 후, SO_D에 저장되어 있는 DS를 읽는다.

(2) 판독시스템은 SO_D의 전자서명이 위조되지 않았음을 확인하기 위해서 SO_D에 내장되어 있거나, 판독시스템에 저장되어 있는 C_{DS}의 KPu_{DS}를 이용해서 유효성을 검증(㉑)한다.

㉑ Verify KPu_{DS}, SO_D

(3) 전자여권 칩의 LDS에 저장되어 있는 LDS_{DG}를 읽어 해쉬값을 생성(㉒)한다.

㉒ Calculate $h(LDS_{DG})$

(4) 판독시스템은 LDS에 저장된 데이터 그룹의 해쉬값과 판독시스템이 생성한 데이터 그룹의 해쉬값이 동일한지 비교(㉓)하여 데이터가 변경되지 않았음을 증명한다.

㉓ $(SO_{D_{DG}}$?= $h(LDS_{DG}))$

〔Step 4. 판독시스템 인증 과정〕

(1) 판독시스템은 칩에 저장된 바이오정보에 접근하기 위해서 EAC 인증서 체인(CVCA 링크인증서, DV 인증서, IS 인증서)을 칩으로 전송(㉔)한다.

㉔ Send Certificate Chain
(CVCA Link, DV, IS Certificate)

(2) 칩은 인증서 서명을 검증하여 인증서 체인의 유효성 검증을 수행(㉕)한다. 만약 서명이 정당한 기관에서 발급되지 않았다고 확

인되면 검증은 실패한다. 그 후 인증서 만료일과 칩의 현재 날짜를 비교한다. 만약 만료일이 현재 날짜 이전이라면 검증은 실패한다. 칩의 보호 메모리 영역에 저장된 CVCA 공개키를 이용하여 인증서 체인을 검증한다. 인증서의 생성일과 칩의 현재날짜를 비교한 후 칩의 현재날짜가 인증서 생성일 이전이라면 현재날짜는 인증서의 생성일로 갱신한다. 칩의 보호 메모리 영역에 새로운 CVCA 공개키를 저장하고, 판독시스템의 공개키(PK_{IS})를 획득한다.

㉕ Check Certificate Chain

(3) 칩은 8byte의 난수를 생성(㉖)하여 판독시스템으로 전송한다.

㉖ $rChip \in_R \{0,1\}^{64}$

(4) 판독시스템은 여권번호(ID_{Chip})와 Ephemeral DH 공개키를 해쉬한 값($h(PK'_{IS})$)을 칩에서 전송 받은 데이터(r_{Chip})와 연접하고, 비밀키(SK_{IS})를 이용하여 서명을 생성(㉗)한 후 서명 값을 칩으로 전송한다.

㉗ $S_{IS} = Sign(SK_{IS}, ID_{Chip} \| r_{Chip} \| h(PK'_{IS}))$

(5) 칩은 판독시스템의 공개키(PK_{IS})를 이용하여 서명을 검증(㉘) 한 후, 인증된 판독시스템의 효과적인 인증 레벨에 따라 바이오정보에 접근을 허용하고, CA 메커니즘의 안전한 통신 채널을 통해 바이오정보를 전송한다.

㉘ $Verify(PK_{IS}, S_{IS}, ID_{Chip} \| r_{Chip} \| h(PK'_{IS}))$

5. 안전성 및 효율성 비교

5.1 안전성 및 효율성 분류

본 절에서는 전자여권 인증 메커니즘의 안전성 및 효율성을 분석한다. 인증 메커니즘의 안전성을 분석하기 위해서 도청 공격 방지, 데이터 위·변조 방지, 바이오정보 노출 방지, 칩 복제 방지, 인증서 위조 방지에 대한 분류 항목으로 나누고, 효율성을 분석하기 위해서 암·복호화, 난수 생성, 서명 생성, 서명 검증에 대한 분류 항목으로 전자여권 인증 메커니즘의 안전성 및 효율성을 비교·분석하였다.

(표 2) 안전성 분류 항목

분류	분류 항목	설명
안전성	도청 공격 방지	도청 공격에 대한 안전성 여부
	데이터 위·변조 방지	데이터 위·변조에 대한 안전성 여부
	바이오정보 노출 방지	바이오정보 노출에 대한 안전성 여부
	칩 복제 방지	칩 복제에 대한 안전성 여부
	인증서 위조 방지	인증서 위조에 대한 안전성 여부
효율성	암·복호화	칩과 판독시스템에서 수행하는 암·복호화 횟수
	난수생성	칩과 판독시스템에서 생성하는 난수 횟수
	서명생성	칩과 판독시스템에서 생성하는 서명 횟수
	서명검증	칩과 판독시스템에서 생성하는 서명 검증 횟수

5.2 안전성 및 효율성 분석 결과

5.2.1 BAC+PA 방식

BAC+PA 방식은 ICAO에서 요구하는 필수 적용사항이다. 칩과 판독시스템간 3DES 블록 암호화 알고리즘을 이용하여 세션키를 교환 후 데이터를 암호화하여 보안 채널이 형성한다. 이 방식은 도청 공격 방지 항목을 만족한다. 또한 전자여권 칩의 SO_D에 저장되어 있는 해쉬값과 DG의 해쉬값을 비교하여 데이터 위·변조 방지 항목에 대해서 검증이 가능하다. 반면 칩에 저장된 바이오정보 노출 방지, 칩 복제 방지, 인증서 위조 방지 항목에 대한 보안 메커니즘이 적용되지 않아 바이오 정보 노출, 전자여권 칩 복제, 인증서 위조에 대해서 취약하다.

전자여권 칩과 판독시스템은 BAC 세션키 생성

(표 3) 안전성 비교·분석

	도청 공격	데이터 위·변조	바이오정보 노출	칩 복제
BAC+PA 방식	○	○	×	×
BAC+PA+AA 방식	○	○	×	○
BAC+PA+AA+EAC 방식	○	○	○	○
제안하는 방식	○	○	○	○

- ○ : 안전 - × : 안전하지 않음

(표 4) 효율성 비교·분석

	전자여권 칩과 판독시스템 사이의 계산량							
	암호화	복호화	해쉬연산	난수생성	서명생성	서명검증	MAC생성	MAC검증
BAC+PA 방식	C : 1번 IS : 1번	C :1 번 IS :1 번	IS : 1번	C : 2번 IS : 2번	-	IS : 1번	C : 1번 IS : 1번	C : 1번 IS : 1번
BAC+PA+AA 방식	C : 1번 IS : 1번	C : 1번 IS : 1번	C : 1번 IS : 1번	C : 3번 IS : 3번	C : 1번	IS : 2번	C : 1번 IS : 1번	C : 1번 IS : 1번
BAC+PA+AA+EAC 방식	C : 2번 IS : 2번	C : 1번 IS : 1번	C : 2번 IS : 1번	C : 4번 IS : 3번	C : 1번	C : 1번 IS : 3번	C : 1번 IS : 1번	C : 1번 IS : 1번
제안하는 방식	C : 2번 IS : 2번	C : 1번 IS : 1번	C : 1번 IS : 1번	C : 3번 IS : 2번	-	C : 1번 IS : 2번	C : 1번 IS : 1번	C : 1번 IS : 1번

- C : 전자여권 칩 - IS : 판독시스템

과 칩에 내장된 데이터의 위·변조를 확인하기 위해 각각 2번의 난수 생성과 1번의 암·복호화가 필요하며 판독시스템에서는 추가적으로 1번의 해쉬연산과 서명검증 과정이 필요하다.

5.2.2 BAC+PA+AA 방식

BAC+PA+AA 방식은 AA 메커니즘에서 칩과 판독시스템 사이의 AA 키쌍을 이용한 질의-응답 방식을 수행해 칩을 검증하므로 전자여권 복제 방지 항목을 만족한다. 반면 바이오정보 노출 방지, 인증서 위조 방지 항목에 대해서 취약하다.

칩 검증 과정으로 인해 BAC+PA 방식보다 전자여권 칩은 1번의 해쉬연산, 난수 생성, 서명 생성이 추가적으로 요구되며, 판독시스템은 1번의 난수 생성, 서명 검증 과정이 필요하다.

5.2.3 BAC+PA+AA+EAC 방식

BAC+PA+AA+EAC 방식은 EAC 메커니즘에서 AA 메커니즘과 별도로 추가적으로 칩 인증 과정을 거치고, 바이오정보를 제공하기 위해서 BAC 프로토콜의 암호화 채널을 종료하고 DH 방식으로 EAC 세션키 생성 및 교환을 이용해서 전송되는 데이터를 암호화하여 BAC 프로토콜보다 강화된 통신 채널을 형성한다는 점으로 인해 도청 공격 방지, 데이터 위·변조 방지, 바이오정보 노출 방지, 전자여권 복제 방지, 인증서 위조 방지 항목에 대해서 모두 만족한다. 반면 EAC 세션키를 분배하기 위해 칩과 판독시스템 사이의 질의-응답 횟수가 증가하여 BAC+PA+AA 방식보다 칩은 1번의 암호화, 해쉬연산, 난수생성, 서명검증이 추가되고 판독시스템은 1번의 해쉬연산, 서명검증 과정이 증가한다.

5.2.4 제안하는 방식

제안하는 방식(BAC+PA+EAC)은 칩 인증 과정에서 칩의 보호 메모리 영역에 내장된 칩 인증 메커니즘의 비밀키와 DG14에 저장된 칩 인증 공개키를 이용해 칩 인증을 수행함으로써 데이터 위·변조 방지, 칩 복제 방지 항목을 만족하고 DH 방식의 EAC 세션키 생성 및 교환을 이용해 전송되는 데이터를 암호화하여 도청 공격 방지, 바이오

정보 노출 방지 항목에 대해서 만족한다. 또한 판독시스템에서 전송받은 CVCA 링크인증서, DV 인증서, IS 인증서의 유효성을 검증하여 인증서의 위조여부를 판단할 수 있어 인증서 위조 방지 항목 만족한다. 반면 BAC+PA+AA+EAC 방식과 동일한 기능을 수행하면서도 칩은 1번의 해쉬연산, 난수 생성이 감소하고, 판독시스템은 1번의 난수 생성, 서명 검증 과정이 감소한다.

제안하는 전자여권 인증 메커니즘은 앞 절에서 정의한 안전성 분류 항목을 모두 만족하는 기존의 BAC+PA+AA+EAC 방식에 비해 전자여권 칩과 판독시스템 사이의 요구되는 계산량을 감소시킬 수 있는 장점이 있다.

6. 결 론

본 논문에서는 전자여권 시스템에서 발생할 수 있는 보안 취약점들을 해결하고자 제안된 ICAO 표준 메커니즘과 EU에서 제안하는 메커니즘을 분석하고, 전자여권 칩과 판독시스템 사이의 안전한 통신을 제공하고 계산량을 감소시키는 인증 메커니즘을 제안하였다. 또한 전자여권 인증 메커니즘들의 안전성 및 효율성을 비교·분석하였다. 분석한 결과를 토대로 도청 공격, 데이터 위·변조, 바이오정보 노출, 칩 복제, 인증서 위조를 모두 방지하면서도 계산량을 감소 시킬 수 있는 방법은 PA+BAC+EAC 방식을 적용한 메커니즘이다. 전자여권 시스템 인증 메커니즘들에 대한 앞으로의 연구 방향은 기존의 여권과 달리 전자여권에서 발생할 수 있는 새로운 위협형태를 분석하여, 그에 대응하는 인증 메커니즘들에 대한 연구가 지속되어야 한다.

참 고 문 헌

[1] ICAO, ‘Biometrics deployment of Machine Readable Travel Documents’, Version 2.0, 2004.

[2] Vijayakrishnan P., Josef P., Huaxiong W., ‘An On-Line Secure E-Passport Protocol’, ISPEC 2008, Vol. 4991, pp 14-28, 2008.

[3] ICAO, ‘Development of a logical data structure - LDS for optional capacity expansion technologies’, revison 1.7, 2004.

[4] ICAO, ‘Machine Readable Travel Documents Machine Readable Passports Specifications for Electronically Enabled Passport with Biometric Identification capability’, Part 1, Volume 2, 2005.

[5] Ari J., David M., David W., ‘Security and privacy issues in e-passports’, In SecureComm 2005), pp.74-88, 2005.

[6] ICAO, ‘PKI for Machine Readable Travel Documents offering ICC Read-Only Access’, Version 1.1, 2004.

[7] Dario C., Kerstin L., Christof P., Ahma., ‘E-Passport: The Global Traceability Or How to Feel Like a UPS Package’, In: WISA 2006. LNCS, vol. 4298, pp. 391 – 404. Springer, Heidelberg, 2006.

[8] BSI, ‘Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control(EAC)’, Version 1.1, TR-03110, 2007.

[9] BSI, ‘Common Criteria Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control’, BSI-PP-0017, Version 1.0, 18th August 2005

[10] BSI, ’Common Criteria Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control’, BSI-PP-0026, Version 1.2, 19th November 2007

[11] ISO, ISO/IEC 7816 Identification cards – Integrated circuit(s) cards with contacts. Technical

report, ISO JTC 1/SC 17
[12] Gaurav S., Kc and Paul A., Karger., 'Security and privacy issues in machine readable travel documents (MRTDs)', IBM Technical Report (RC 23575), IBM T. J., Watson Research Labs, April 2005.
[13] Hoepman, J.-H., Hubbers, E., Jacobs, B., Oostdijk, M., Schreur, R.W. 'Crossing Borders: Security and Privacy Issues of the European e-Passport', IWSEC 2006, LNCS, vol. 4266, pp. 152 – 167. Springer, Heidelberg (2006)
[14] NIST, 'Recommendation for key management. Technical Report Special Publication 800-57 Draft', August 2005.
[15] 이완석, 이준호, 유연정 외, '전자여권 보호프로파일 V.0', 한국정보보호진흥원, 2008.

◐ 저 자 소 개 ◑

이 동 범(Dongbum Lee)
2008년 순천향대학교 정보보호학과 졸업(공학사)
2008~ 현재 순천향대학교 대학원 정보보호학과 석사 과정
관심분야 : 정보보안, 전자여권보안 등
E-mail : dblee@sch.ac.kr

고 웅(Woong Go)
2008년 순천향대학교 정보보호학과 졸업(공학사)
2008~ 현재 순천향대학교 대학원 정보보호학과 석사 과정
관심분야 : 정보보안, 유비쿼터스 응용시스템 보안 등
E-mail : wgo@sch.ac.kr

곽 진(Jin Kwak)
성균관대학교 학사, 석사, 박사
2006년 4월-2006년 11월 : 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월-2006년 11월 : 일본 큐슈대학교 시스템정보기술연구소 특별연구원
2006년 11월-2007년 3월 : 정보통신부 정보보호기획단 개인정보보호팀 통신 사무관
2007년 3월~현재 : 순천향대학교 정보보호학과 교수
관심분야 : 암호프로토콜, RFID 시스템 응용 보안, 개인정보보호, 정보보호제품평가, 전자여권보안 등
E-mail : jkwak@sch.ac.kr