情 報 保 護 學 會 誌
第 17 券 第 5 號, 2007. 10

전자여권에 사용된 융합보안 기술

전은경,* 이용준*

요 약

본 논문에서는 전자여권이 무엇이고, 그것에 사용된 개인 확인을 위한 바이오 인식 기술과 전자여권 내 삽입된 개인 정보를 보호하기 위한 보안 기술은 무엇이 있으며, 우리나라 전자여권에는 어떠한 보안 기술이 삽입되었는지를 간단히 살펴본다.

Ⅰ. 서 론

현재 전자여권은 미국을 중심으로 도입이 시작, 전 세계 36개국에서 발행되고 있으며 우리나라도 올해 시범사업을 시작으로 내년부터 비자 면제국 가입을 위한 기본 조건으로 전자여권 전환 작업이 시작될 예정이다.

전자여권의 도입과 함께 지문 정보 저장에 대한 프라이버시 문제 및 전자여권 내 정보 보호의 문제 등이 대두되고 있는데, 이에 대해 전자여권에서는 어떠한 보안 장치 들이 있으며, 이러한 정보를 보호하기 위하여 정부에서는 어떠한 노력을 하고 있는지를 정리한다.

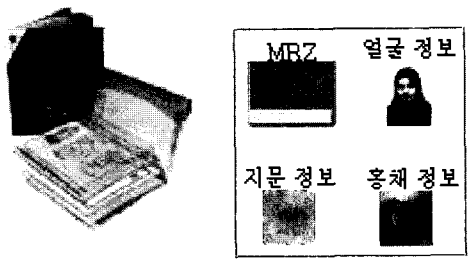
Ⅱ. 전자여권 개요

전자여권은 여권 내 데이터 페이지 정보, 개인을 확인할 수 있는 바이오 정보와 데이터를 보호할 수 있는 보안요소를 저장한 비접촉 IC칩을 내장하고 있는 여권이다.[1]

2.1. 전자여권 저장 정보

개인의 정보는 모두 국제 항공기구인 ICAO에서 정의한 국제 규격에 맞추어 저장되며, 데이터 페이지에 보이는 여권번호, 영문성명, 성별, 주민 번호 등 개인 정보와, 얼굴 사진 정보는 필수 입력사항으로, 그리고 지문정보와 홍채정보 등 바이오 정보는 선택 입력 사항으로 저장될 수 있다.

또한 전 세계 모든 국가에서 동일하게 정보를 판독해야 하는 만큼, 상호호환성 확보를 위해 얼굴, 지문, 홍채 정보들은 각 업체별로 다른 알고리즘이 반영된 Template 형태가 아닌 이미지 원형으로 저장되어야 하며, 판독 속도 개선을 위해 얼굴, 홍채는 JPEG 혹은 JPEG200 포맷으로, 지문은 WSQ 포맷으로 압축 저장하도록 하고 있다.



〔그림 1〕 전자여권 내 삽입되는 정보는 개인의 기본 정보가 담긴 MRZ* 와 얼굴사진이 필수로 삽입되고, 지문과 홍채 등 바이오 정보는 선택기재 사항이다.

우리나라의 경우, 데이터 페이지에 보이는 여권번호, 영문성명, 성별, 주민 번호 등 개인 정보와, 얼굴 사진 정보 그리고 지문정보를 삽입하여 발급하는 것으로 결정되었다. 지문 정보를 삽입함으로써 일란성 쌍둥이가 서로 다른 사람의 여권을 사용하는 등의 위명, 차명 여권의 발급과 사용을 불

* LG CNS 책임연구원 (ekjun@lgcns.com, bigman@lgcns.com)

가하게 하여 여권의 신뢰성을 강화하게 되었다.

2.2. 전자여권 판독

전자여권은 전 세계 어디에서나 통용되어 사용되는 신분증이다.

일반적으로 해외 출입국시 각국 출입국 사무소에서 신원을 확인하기 위한 용도로 활용될 뿐 아니라, 해외 호텔, 항공사 등에서 개인 확인용 신분증으로 사용되고, 국내에서도 학생들이 TOEIC, TOFEL 등 국제 시험을 보기 위한 신분증으로 사용될 수 있다.

개인의 신분증이 본인을 확인하기 위한 정보를 오픈하는 것은 당연한 사항이나, 사용 용도에 맞게 개인의 정보가 제한되어 오픈될 필요가 있으며, 특히 개인의 민감한 데이터인 바이오 정보는 여권 발행국에서 허용된 국가의 정보기관만이 판독 할 수 있도록 제한되어야 한다.

Ⅲ. 전자여권내 사용된 보안기술

3.1. 전자여권 정보 보호 방안

전자여권이 비접촉식 통신을 통하여 데이터를 전송하는 만큼, 허가받지 않은 자의 Chip내 데이터 접근이 가능할 수 있으며, 이를 제한하기 위하여 전자여권의 표준에서는 BAC (Basic Access Control), EAC (Extended Access Control)와 같은 방식의 접근제한 방식을 두고 있다.

BAC 방식은 전자여권 내부에 물리적으로 표시된 88자리의 MRZ 정보를 알고 있는 사람만 Chip 내부 정보에 접근할 수 있도록 하는 것으로, 여권을 소지자로부터 물리적으로 건내 받지 않은 상태에서는 정보를 읽지 못하도록 하는 것이다. 또한 MRZ 정보로 상대를 확인한 후에는 여권과 판독기 간에 DES 알고리즘을 사용한 암호화된 채널을 생성하여 판독 내용을 도청할 할 수 없도록 한다.

EAC 방식은 전자여권 내 삽입된 개인의 지문, 홍채 등의 바이오 정보에 접근하기 위해서 추가적인 접근 통제를 하는 것으로, 국가마다 방식을 지정하도록 되어 있다. 유럽과 우리나라의 경우에는 BAC 보안채널 생성 이후 Diffle-Hellman 알고리즘을 사용한 Key Agreement를 통하여 보다 한 단계 더 강력한 보안채널을 생성한 후, 각 여권 발행국 CVCA (Country Verifying CA)가 발급한 인증서가 주입된 판독기(타국가의 출입국 사무소를 포함한)임이 판명된 경우에만 지문 정보를 제공하도록 되어 있다.

허나, BAC, EAC가 모두 필수 사항이 아닌 선택사항이므로, 각 국가에서 판단하여 사용할 수 있으며, 미국의 경우 BAC 방식이 아닌 차폐막을 사용하여 허가받지 않은 여권 정보의 접근을 막고 있다.

3.2. 전자여권 위변조 방지 방안

전자여권에 대한 위조가능성에 대해서 여러 가지 언론 기사가 나오고 있으나, 대부분의 경우, 여권의 기능이 구현 수준에 대해서는 언급된 바가 없다. ICAO에서 규정한 전자여권의 위변조 방지 방안은 PA (수동인증 : Passive Authentication)과 AA (능동인증 : Active Authentication)이 있으며, EAC 기능에도 CA (칩 인증 : Chip Authentication) 기능이 포함되어 위변조 여부를 확인하고 있다.

PA기능은 전자여권에 저장된 데이터에 대한 진위 검증 작업으로 여권 내에 전자여권에 삽입된 개인정보에 대한 모든 해쉬 및 디지털 서명을 포함한 문서보안객체를 저장하고 판독 시에 ICAO PKD에 등록된 인증서를 내려 받아, 이를 비교하게 하는 방법이다. 이를 통하여 개인이 임의적으로 여권의 데이터를 변조하게 되면 이를 판별해 낼 수 있다.

AA 기능은 전자여권 내 칩이 대체되지 않았음을 보증하는 방식으로, 능동인증을 위한 RSA 혹은 ECDSA알고리즘을 활용하여 생성된 키쌍이 전자여권 내에 저장되어 판독기에서 칩의 보안 영역에 저장된 개인키의 정보를 확인함으로써 칩이 복제되지 않았음을 보증한다.

CA 기능은 칩이 복제되지 않았음을 증명하는 것은 AA와 비슷한 기능이나, EAC에서 사용되는 보안채널을 만드는데 활용된다는 부분이 다르다.

Ⅳ. 전자여권 보안성 강화를 위한 추가 사항

4.1. 보안성 평가 (CC)

민간업체가 개발한 정보보호제품의 보안기능을 검증하여 국가차원에서 안전성과 신뢰성을 보증하는 제도로써 세계 각 업체들이 개발한 전자여권

제품이 CC 인증을 획득함으로써 그 보안성을 국제적으로 인정받을 수 있다.

전자여권에 대한 보호 프로파일 (PP : Protection Profile)은 독일 BSI에서 작성한 Machine Readable Travel Document with "ICAO Application", Basic Access Control (BSI-PP- 0017)과 Machine Readable Travel Document with "ICAO Application", Extended Access Control (BSI-PP-0026)이 있으며, 우리나라 국가정보원에서도 최근 '전자여권 보호 프로파일(PP)' 초안을 만들고 최종안 마련을 위해 관련 기업 및 기관을 대상으로 의견 수렴에 들어갔다.

CC 평가를 통과하게 될 경우, 일반적으로 전자여권의 위협이라 판단되는 도청, 위변조, 정보누출, 비인가된 판독 등에 대해서 전자여권에서 어떻게 대처하고 있는지에 대한 보안성을 인정받을 수 있다.

V. 바이오 정보 보호 기술

지금까지 전자여권 내 개인 정보에 대한 보호 기술을 소개하였다. ICAO에서는 전자여권 내에 담겨진 개인의 정보를 어떠한 방식으로 보호해야 하는지에 대한 논의가 주로 되고 있다. 허나, 여권에 담겨지기 위해 채취되는 개인의 바이오 정보들 역시 보호되어져야 하며, 이는 각 국가별로 문제를 해결하고 있다.

아래 설명되는 내용은 우리나라 외교통상부에서 진행하는 신여권 프로젝트에서 바이오정보를 보호하기 위해 적용하는 기술이다.

5.1. 바이오정보 관리 및 보안 표준(K-X9.84)

바이오정보 관리 및 보안 표준(K-X9.84)은 정보통신망 환경에서 동작하는 바이오인식 시스템의 각 모듈 간 또는 바이오인식 사용자 인증을 위해 전송되는 각 개인의 고유한 바이오정보의 보안성과 안전성을 확보하기 위해 제정되었다.

기본적인 바이오정보 객체인 Biometric Object는 바이오정보 헤더 블록과 바이오정보 데이터 블록으로 구성된다. 바이오정보 헤더 블록은 바이오인식 시스템이 바이오정보 데이터 블록을 인식하고 처리하기 위해 필요한 기본적인 속성과 바이오인식을 제공하는 업체를 명기하기 위한 속성을 포함하고 있다.

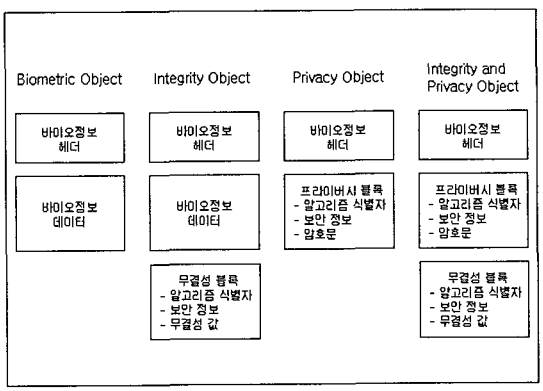
무결성을 제공하는 Integrity Object는 바이오정보 헤더 블록, 바이오정보 데이터 블록, 무결성 블록으로 구성된다. 무결성 블록은 알고리즘 식별자와 보안 정보, 그리고 무결성 값으로 구성된다. 무결성은 전자서명 또는 MAC(Message Authentication Code) 알고리즘으로 구현한다.

프라이버시를 제공하는 Privacy Object는 바이오정보 헤더 블록과 프라이버시 블록으로 구성된다. 바이오정보 데이터 블록은 없으며 프라이버시 블록은 알고리즘 식별자와 보안 정보 그리고 암호화된 바이오정보 데이터 블록으로 구성되어 있다. 암호화는 대칭키 방식 또는 암호봉투 방식으로 수행한다.

무결성과 프라이버시를 제공하는 Integrity And Privacy Object는 바이오정보 헤더 블록, 프라이버시 블록, 무결성 블록으로 구성된다. 프라이버시 블록과 무결성 블록은 위에 제시한 블록을 사용하게 되며 무결성과 프라이버시를 동시에 제공하게 된다.

전자여권에서는 사진, 지문의 등록에서 중앙DB의 저장하는 구간의 통신 및 저장에서 Integrity And Privacy Object로 제공함으로써 바이오정보의 보호를 강화시켰다.

[그림 1]은 X9.84가 제정한 Biometric Object, Integrity Object, Privacy Object, Integrity and Privacy Object의 블록을 나타내었다.

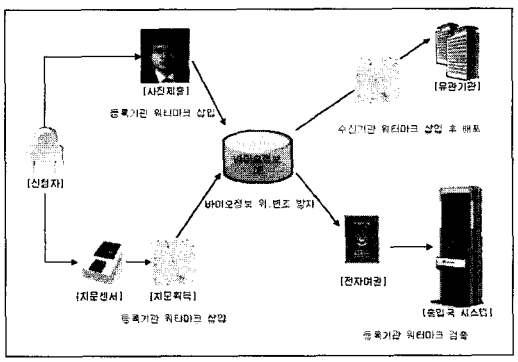


〔그림 1〕 X9.84 바이오정보 객체의 종류

5.2. 바이오정보 워터마킹 기법

바이오정보는 개인의 가장 민감한 정보 중에 하나이며 사용자 인증을 위하여 저장된 바이오정보

가 타인에게 도용된다면 기존의 패스워드나 공인 인증서와 달리 재발급이 불가능하여 심각한 문제를 발생시킬 수 있다. 이러한 문제를 해결하기 위하여 워터마킹 기법을 사용할 수 있다. 이는 바이오정보에 부가정보를 삽입함으로써 해당 바이오정보에 대한 소유자 인증 및 바이오 정보의 위변조를 검출할 수 있다. 즉, 바이오정보가 타인에게 도용되었을 경우 워터마킹 기법에 의해 인증 및 위변조 여부를 판단하여 바이오인식 시스템이 인증을 요구한 바이오정보에 대하여 거부할 수 있다.



〔그림 2〕 바이오정보 워터마킹 기법

[그림 2]는 전자여권 시스템에서 바이오정보 워터마킹 기술을 도입하여 프라이버시를 보호하는 과정을 나타내었다.

바이오정보 등록기관은 사진 또는 지문 등을 등록받는 시점에서 등록시점에 대하여 해당기관의 고유키로 워터마크 삽입을 하여 DB에 전송한다. 워터마크가 삽입된 바이오정보가 위변조 여부는 워터마크 추출을 통해 확인할 수 있다. 또한 타 기관과의 바이오정보를 상호연동하는 경우 수신기관의 키로 워터마킹을 수행함으로써 소유기관 및 무결성을 보장하도록 하였다.

Ⅵ. 결 론

대한민국 전자여권은 IC카드의 주요 보안 기능인 상호 인증 기술을 통하여 BAC, EAC 기능을 구현함으로써 칩내 정보를 보호하고, PA, AA 기능으로 위변조여부를 판독하는데 사용되고 있으며, CC 인증을 통하여 적합한 보안 요소들을 검증 받고 있다.

또한 전자여권의 신뢰성을 높이기 위하여 사용되는 개인의 바이오정보 또한 채취 및 등록 과정에서 보안성과 안정성을 확보할 수 있는 보안 표준을 준수하고, 워터마킹을 사용한 프라이버시 보호 과정을 충분히 반영하고 있다.

참고문헌

[1] *ICAO Doc 9303 Machine Readable Passport Part 1 Machine Readable Passports Volume 1 Passports with Machine Readable Data Stored in Optical Character Recognition Format* pp. II-3, 2006

[2] *바이오정보 관리 및 보안 표준(K-X9.84) TTAS. AS-X9.84* 2003년

[3] 생체정보 인증 및 위변조 검출 알고리듬, 전자공학회 학회지, 2006년.

〈著者紹介〉

전 은 경 (Eun Kyung Jun)
정회원
1997년 : 이화여자 대학교 통계학과 졸업
1996년 ~현재 : LG CNS 기술연구부문
관심분야 : IC카드, 바이오 인식, 정보보호

이 용 준 (Yong-Joon Lee)
정회원
1999년 : 강남대학교 전자계산학과 졸업
2001년 : 숭실대학교 컴퓨터학과 석사
2005년 : 숭실대학교 컴퓨터학과 박사
2006년~현재 : LG CNS 기술연구부문 책임연구원
관심분야 : 바이오정보 보호, 바이오 인식, PKII