정 보 보 호 학 회 지
제25권 제6호, 2015. 12

스마트폰 환경에서 공인인증서 사용 시 소유 및 생체인증 연동 방법

김 선 종*

요 약

본 논문에서는 국내에서 온라인 인증수단으로 많이 사용되고 있는 공인인증서의 보안성과 편의성 제고 차원에서 공인인증서의 쌍이 되는 개인키 패스워드를 지식기반이 아닌 소유 기반과 생체인증으로 확장하는 방법에 대하여 기술하고 있다.

Ⅰ. 서 론

1999년 전자서명법 제정 이후 공인인증서는 국내 금융권을 비롯해 전자정부의 주요 인증수단으로 사용되어 왔으나, 최근 액티브X 의존성, 악성코드와 악성앱에 의한 공인인증서 대량 유출, 복잡도 높은 공인인증서 패스워드 강제화 등의 이유로 부정 여론이 확산되고 있다.

특히 악성 코드 또는 스미싱을 통해 유포되는 악성앱을 통한 공인인증서 유출로 인한 피해는 심각한 수준이다.

공인인증서는 고전적으로 파일 시스템을 활용해 NPKI 폴더에 인증서 파일(signCert.der)과 개인키 파일(signPri.key)을 저장하는 방식을 사용하고 있어, 악성앱에서도 쉽게 접근할 수 있다. 물론 공인인증서는 이러한 공격을 방어하기 위해 개인키를 사용자의 패스워드로 암호화(Encrypted PKCS #8) 해 놓았다.[1-4]

한국인터넷진흥원은 암호화된 개인키에 사용된 패스워드의 복잡도가 낮아 공인인증서 파일만 유출돼도 취약할 수 있다는 지적에 따라 2014년 9월 공인인증서 패스워드 고도화 작업을 수행해 현재는 영문, 숫자, 특수문자 혼합의 패스워드를 사용하고 있다.[5]

한편 핀테크 활성화에 따라 간편 인증 기술이 급부상하고 있으며, 가장 각광받는 기술 스펙은 FIDO 동맹에서 제안한 FIDO-UAF 기술이다. FIDO-UAF 기술은 공개키 기반의 인증 기술이며 서명에 필요한 개인키를 사용하기 위한 인증수단으로 사용자의 접근이 쉬운 지문과 같은 생체 인증이나 PIN 번호 입력 등 사용자의 편의성과 보안성을 동시에 높이는 방안을 제시하고 있다.[6]

이러한 FIDO-UAF 는 최근 삼성페이에 적용되는 등 적용 사례가 점차 늘어날 것으로 기대된다.[7]

반면 공인인증의 경우 여전히 개인키 사용을 위한 인증(암호화) 수단으로 사용자가 기억하기 어렵거나 입력하기 불편한 패스워드를 입력받는 방식이어서 개선이 필요한 상황이다.

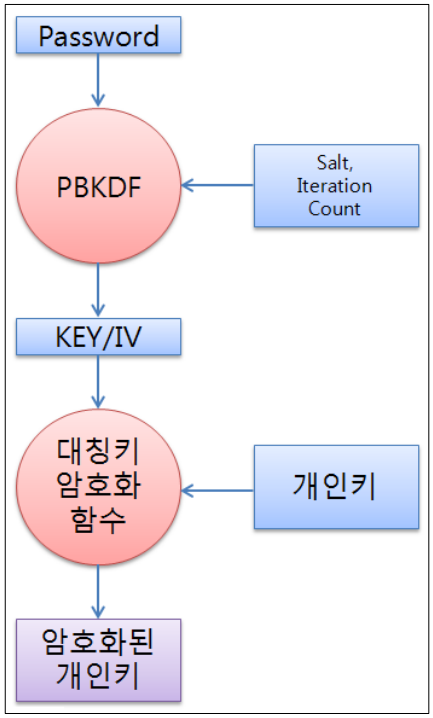
본 논문에서는 스마트폰 환경에서 공인인증서의 개인키 사용 시 생체인증과 NFC 객체를 이용한 소유기반 인증 기술을 활용해 사용자의 접근성과 편의성, 보안성을 높이는 방법을 제안한다.

Ⅱ. 현행 공인인증서의 개인키 관리 방법

현재 공인인증서와 개인키는 하드디스크, 이동식 디스크, 저장토큰, 보안토큰(HSM), 휴대폰, 웹브라우저 저장소 등 다양한 저장소에 저장할 수 있다.

범용적으로 가장 많이 사용되고 있는 저장소는 하드디스크와 이동식디스크이나, NPKI 폴더에 파일형태로 저장되어 있어 어떠한 어플리케이션이든 접근 가능해 악성코드나 악성앱에 의해 공인인증서와 개인키 파일이 유출될 수 있다. 이를 방어하기 위해서 인증서의 쌍이 되는 개인키를 PKCS #5 표준 내 PBES(Password Based Encryption Schemes)스펙을 이용해 암호화 하

* 이니텍 보안사업부문 (seonjong.kim@initech.com)



〔그림 1〕 PKCS #5 표준 내 PBES를 이용한 개인키 암호화 과정〔3〕

고 있어, 암호화에 사용된 패스워드를 모르면 공인인증서와 개인키를 가져가더라도 사용할 수 없다.[3,4]

반면 가장 안전한 저장소로 각광받고 있는 보안토큰의 경우 인증서와 개인키가 보안토큰 내 저장된 후에는 개인키가 외부로 나올 수 없도록 설계되어 있고, 개인키를 이용한 전자서명 연산은 모두 보안토큰 내에서 이루어진다. 보안토큰을 일반적으로 PIN 인증을 통해 보안토큰 내 객체를 이용할 수 있고, 정해진 횟수 이상으로 PIN 인증을 실패하면 보안토큰이 하드웨어 적으로 잠기도록 설계되어 있다. 이러한 보안성에도 불구하고 이용자가 보안토큰을 직접 구매해서 사용해야하는 부담이 있어 보급률이 높지 않은 상황이다.

Ⅲ. 소유 및 생체인증을 통한 개인키 암호화 방법

FIDO 의 경우 개인키 사용을 위해 생체 또는 PIN 인증 등을 수행하는 로컬 인증 모델을 제시하고 있다. FIDO 에서는 공개키와 개인키 쌍의 생성 및 저장, 로컬 인증, 원격 인증을 위한 전자서명 연산을 수행하는 일체화된 주체를 FIDO Authenticator 라고 한다. FIDO Authenticator 는 앞에서 언급한 보안 토큰 구조로 되어 있으며, 개인키의 안전한 저장을 위해 하드웨어 기반의 SE(Secure Element)를 사용할 것을 권장하고 있다.[6]

하지만 현실적으로 누구나 범용적으로 접근 가능한 SE 가 없는 경우가 대부분이기 때문에 본 논문에서는 로컬인증(개인키 사용을 위한 인증)과 개인키 저장을 분리한 모델을 제시하며, 로컬인증 후 개인키를 암호화하기 위한 암호키를 유도하는 방법에 초점을 둔다.

암호키가 유도되고 나면 그 키를 개인키 패스워드로 사용하기 때문에 개인키 암호화 방법은 기존 방식(PKCS#5 PEBES)을 그대로 사용해도 무방하다.

3.1. 로컬인증 모델링

개인키가 SE 아닌 일반 저장소에 저장될 경우 반드시 암호화해서 저장해야한다. 기존 공인인증서의 쌍이 되는 개인키의 경우에도 대칭키 방식으로 암호화 되어 있으므로 로컬 인증(소유 및 생체 인증 후)에는 개인키를 암/복호화 할 수 있는 키를 생성(또는 리턴)하거나, 암/복호화를 할 수 있는 객체를 제공하는 것이 바람직하다.

다음은 로컬인증을 위한 Java 인터페이스 설계의 예이다.

위 모델에서 제시한 인터페이스의 startReg 메소드는 인증 수단(예 : NFC 객체, 지문 등)을 등록하기 위해 소

```
[Model 1]
public interface LocalAuth {
    public boolean startReg();
    public boolean startAuth();
    public byte[] getCipherKey();
}

[Model 2]
public interface LoaclAuth {
    public boolean startReg();
    public boolean startAuth();
    public String getCipherAlgName();
    public byte[] encrypt(byte[] data);
    public byte[] decrypt(byte[] data);
}
```

〔그림 2〕 로컬 인증 Java 인터페이스 예

유 또는 생체 인증 센서를 실행시키는 역할을 수행하며, 등록 성공 여부를 리턴한다. startAuth 메소드는 소유 또는 생체 인증을 위한 센서를 실행시키는 역할을 하며, 인증 성공여부를 리턴한다. 인증 성공 후에는 암/복호화를 수행할 수 있는 키 또는 암/복호화 메소드를 이용할 수 있다. Model 1 에서는 getCipherKey 메소드를 통해 암/복호화를 수행할 수 있는 암호키를 리턴 받을 수 있고, Model 2 에서는 Model 1처럼 직접적으로 암호키를 외부로 리턴시키지 않고 encrypt/decrypt 메소드를 통해 암/복호화를 수행할 수 있다. getCipherAlgName 메소드는 어떤 암호 알고리즘을 통해 암/복호화를 수행하는지에 대한 정보(예 : SEED/CBC)를 리턴한다.

소유 또는 생체 기반 인증을 제공하는 벤더 입장에서는 공인인증서의 쌍이 되는 개인키를 암/복호화 하기 위해 위 모델중 하나의 인터페이스를 선택해 완전한 형태의 로컬 인증 클래스를 구현하면, 공인인증모듈을 개발하는 벤더는 해당 클래스를 이용해 공인인증서 사용 시 소유 또는 생체 기반 인증을 연동시킬 수 있다.

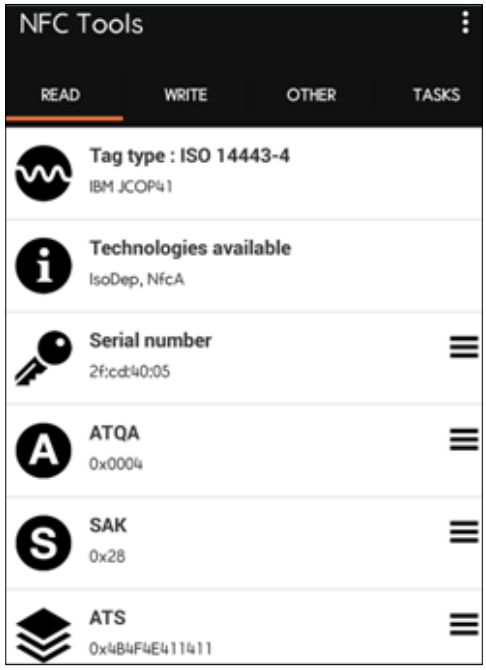
3.2. NFC 객체(소유기반 인증)를 통한 개인키 암호키 생성 과정의 예

NFC 의 경우 거의 모든 스마트폰에서 제공하고 있는 인터페이스로 소유기반 인증을 통해 개인키 암호화에 필요한 암호키 생성이 적합한 구조를 제공한다. 또한 이용자들이 통상적으로 사용하는 교통카드나, 교통카드 기능을 가진 신용/체크카드 들(이하 NFC 객체)도 NFC 통신이 가능하기 때문에 스마트폰을 통해 해당 카드들의 정보를 읽을 수 있어, 소유 기반 인증을 통한 암호키 생성이 용이하다.

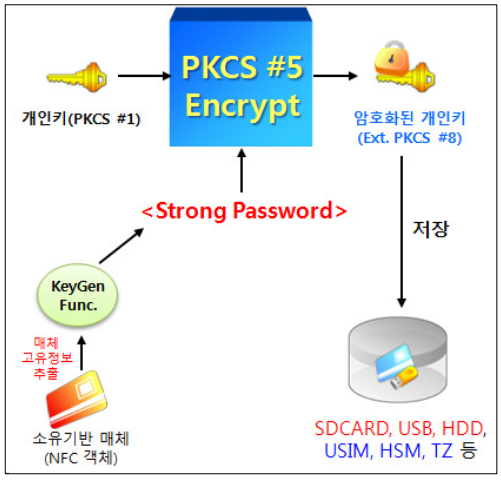
다음은 스마트폰에서 NFC 객체를 접촉했을 때 NFC 통신을 통해 얻을 수 있는 정보를 나열한 것이다.

위 그림과 같이 NFC 객체로 부터 Tag Type, Technologies Aavaiable, Serial Number, ATQA, SAK, ATS 값 등 을 얻을 수 있으며, 태그 할 때 마다 태그 된 NFC 객체의 고유정보를 리턴하기 때문에 개인키를 암호화에 사용되는 암호키 생성 시 씨드(Seed)로 참여 시킬 수 있다.

위 그림에서 KeyGenFunc 는 개인키 암호화에 사용되는 강력한 암호키(Password)를 1생성하는 역할을 수행하며, NFC 객체로부터 추출된 매체고유 정보를 입력



〔그림 3〕 NFC 객체로부터 얻을 수 있는 정보의 예



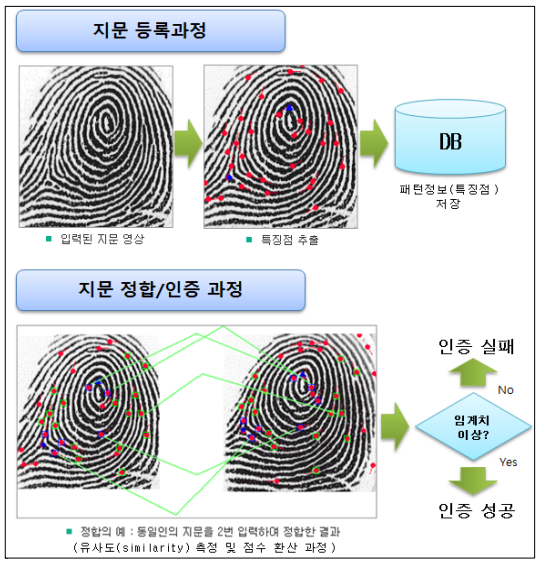
〔그림 4〕 소유기반 매체로부터 얻은 정보를 통해 암호키를 생성하고, 개인키를 암호화 하는 과정

받아, 난수 생성기의 씨드(Seed) 로 참여시킨다. 난수 생성기는 표준 보안 난수 생성 알고리즘(예 : DRBG) 사용을 권장한다.

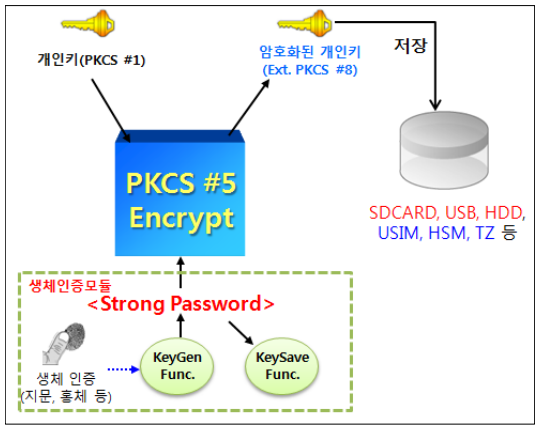
3.3. 생체인증을 통한 개인키 암호키 생성과정의 예

생체인증의 경우 지식기반 인증이나 소유기반 인증

과는 달리 인증 시 입력되는 데이터가 매번 같지 않아 입력된 생체 데이터와 등록된 생체 데이터의 유사도(similarity)를 점수로 계산하여 설정된 임계치 이상인 경우 인증 성공으로, 그렇지 않은 경우 인증 실패로 판단한다. 그렇기 때문에 입력 시 매번 달라지는 생체 데이터로는 개인키 암호화에 필요한 유일한 암호키를 생성할 수가 없다. 그러므로 생체 인증 모듈은 내부적으로 생체 인증 정보(예 : 특징점, 패턴 등)를 등록하는 과정 중 안전한 난수 생성기에 의해 암호키를 생성하여, 생체 인증 정보와 쌍으로 저장해야한다. 또한 암호키 생성 과정 중 수집된 생체 패턴 정보를 난수 생성기의 씨드(Seed) 로 참여시킬 수 있다.



〔그림 5〕 일반적인 지문 등록 및 지문 인증 과정



〔그림 6〕 생체 인증 후 생체 인증 모듈 내에서 생성된 암호키로 개인키를 암호화 하는 과정

인증과정에서 등록된 생체 패턴 정보에 부합하는 생체 입력정보가 들어왔을 경우, 쌍으로 보관되어 있던 암호키를 리턴하거나 암/복호화 메소드를 제공해야 한다.

위 그림에서 KeyGenFunc 는 개인키 암호화에 사용되는 강력한 암호키를 생성하거나, 생체인증모듈 내 저장된 암호키를 리턴하는 역할을 수행하고, KeySaveFunc 는 생체 인증 정보 등록 시 생성된 암호키를 저장하는 역할을 수행한다.

Ⅳ. 결 론

스마트폰 보급률이 높아지면서 스마트폰이 가진 여러 인터페이스(예 : NFC, 지문 인식 등)를 통해 편리한 인증 기술 구현이 가능해졌다.

본 논문에서 예제로 제안한 방법 이외에도 소유기반 인증에 있어서는 블루투스를 통한 소유 인증이 가능하며 생체 인증의 경우 안면 인식, 홍채 인식, 생체 패턴 인식 등으로 확장할 수 있다.

3.1 절에서 언급한 로컬인증 모델을 기반으로 하여 공인인증서 개인키 암호화에 사용한다면 사용자의 편의성도 높일 수 있을 뿐만 아니라, 사용자가 입력하는 복잡도가 낮은 패스워드 보다 복잡도가 높은 암호키를 개인키 암호화에 사용할 수 있으므로, 공인인증서/개인키 파일 유출 방어에도 기여하는 등 공인인증서 이용 환경 개선에 도움이 될 수 있을 것으로 기대된다.

참 고 문 헌

[1] 이호근, 고려대학교, 개인 식별을 위한 난수 정보를 이용한 공인인증서 관리 기법, 2010.12

[2] Network Working Group, RFC 5208 Public-Key Cryptography Standards(PKCS) #8: Private-Key Information Syntax Specification Version 1.2, 2008.05

[3] RSA Laboratories, PKCS #5 v2.0: Password-Based Cryptography Standard, 1999.03

[4] RSA Laboratories, PKCS #8 v1.2: Private-Key Information Syntax Standard, 1993.11

[5] 보안뉴스 김지언 기자, “공인인증서 비번 설정규칙 강화된다.”, 2014.09.19. (URL : http://www.b

oannews.com/media/view.asp?idx=43066)
[6] FIDO Alliance, FIDO UAF Architectural Overview, 2014.12
[7] 전자신문 김인순 기자, “FIDO 인증 서비스, 보안 업계 새 성장동력되나”, 2015.09.02. (URL :http://www.etnews.com/20150902000233)

〈저자소개〉

김 선 종 (Seon Jong Kim)
종신회원

2007년 2월 : 울산대학교 공과대학 컴퓨터정보통신공학부 학사 졸업
2010년 2월 : 고려대학교 정보경영공학전문대학원 정보보호 전공 석사 졸업
2004년 6월~현재 : 이니텍 보안사업부문 차장
관심분야 : 암호프로토콜, 금융정보보안, 핀테크