http://dx.doi.org/10.5392/JKCA.2016.16.08.090

스마트폰 고유정보를 이용한 안전한 개인키 관리 방안

Secure Management Method for Private Key using Smartphon's Information

김선주
한국정보통신기술협회

Seon-Joo Kim(sunjoo@tta.or.kr)

요약

우리나라는 스마트폰 보급률이 83%로 성인인구 4,000만명 중 3,390만 명이 사용하고 있으며, 이러한 사용자 대부분이 공인인증서에 대한 안전성 문제가 지속적으로 제기됨에도 불구하고 공인인증서를 사용하고 있다. 이러한 안전성의 문제로 인해 SMS를 이용한 휴대폰 소유자 인증기술, 생체인증을 통한 본인 인증기술 등 다양한 인증기술들이 제안되고 있다. 그러나 아직까지도 공인인증서를 대체할 만한 안전하고 믿을 만한 인증체계가 제시되지 않고 있다. 또한 사용자가 제일 많은 공인인증서와 개인키에 대한 탈취 시도가 지속적으로 발생하고 있다. 이러한 이유로 인해 보안전문가들은 공인인증서와 개인키를 USB 플래시 드라이브, 보안토큰, 스마트폰에 저장하도록 권고한다. 하지만 보안전문가가 추천하는 외부 저장매체 중 스마트폰은 앱을 통해 악성코드가 쉽게 전파되고, 악성코드에 의한 인증서나 개인키 파일을 외부로 유출이 가능하다. 해커가 유출한 인증서와 개인키 파일과 함께 개인키 암호용 패스워드만 알아내면 언제든지 정당한 사용자로 위장할 수 있다. 이에 본 논문에서는 스마트폰의 고유정보와 사용자 패스워드를 조합하여 스마트폰에 저장된 개인키 파일의 안전한 관리 방안을 제안한다. 제안 방안을 활용하게 되면 스마트폰에 저장된 개인키와 인증서 파일이 공격자에게 탈취되더라도 스마트폰의 고유 정보를 획득할 수 없으므로 암호화된 개인키의 재사용이 불가능하다. 따라서 제안 방안을 공인인증 체계에 활용한다면 스마트폰 사용자에게 현재보다 훨씬 향상된 보안 서비스를 제공할 수 있을 것으로 예상한다.

■ 중심어 : | 공개키 기반 구조 | 공인인증서 | 개인키 파일 | 스마트폰 고유정보 | 단말기 국제 고유 식별번호 |

Abstract

The 3390 million people, around 83% of the adult population in Korea use smartphone. Although the safety problem of the certificate has been occurred continuously, most of these users use the certificate. These safety issues as a solution to 'The owner of a mobile phone using SMS authentication technology', 'Biometric authentication', etc are being proposed. but, a secure and reliable authentication scheme has not been proposed for replace the certificate yet. and there are many attacks to steal the certificate and private key. For these reasons, security experts recommend to store the certificate and private key on usb flash drive, security tokens, smartphone. but smartphones are easily infected malware, an attacker can steal certificate and private key by malicious code. If an attacker snatchs the certificate, the private key file, and the password for the private key password, he can always act as valid user. In this paper, we proposed a safe way to keep the private key on smartphone using smartphone's unique information and user password. If an attacker knows the user password, the certificate and the private key, he can not know the smart phone's unique information, so it is impossible to use the encrypted private key. Therefore smartphone user use IT service safely.

■ keyword : | PKI | Certificate | Private Key File | Smartphone Unique Information | IMEI |

접수일자 : 2016년 05월 09일
수정일자 : 2016년 05월 30일
심사완료일 : 2016년 05월 30일
교신저자 : 김선주, e-mail : sunjoo@tta.or.kr

I. 서 론

2015년 3월 기준으로 우리나라의 스마트폰 보급률은 [표 1]과 같이 UAE, 싱가포르, 사우디아라비아에 이어 4위를 차지하며, 성인인구 40,879,472명 중 33,929,961명 사용한다[1][2].

표 1. 국가별 스마트폰 보급률 (2015년 3월 기준)

국가	UAE	싱가포르	사우디아라비아	대한민국	스웨덴
보급률 (%)	90.8	87.7	86.1	83.0	82.8

스마트폰 사용자 대부분은 지정된 공인인증서 발급기관에서 공인인증서를 발급받아 사용하고 있으며, [그림 1]과 같이 사용자의 64.9%는 USB 플래시 드라이브 등의 외부 저장매체에 공인인증서와 개인키를 저장하고 있다[3].

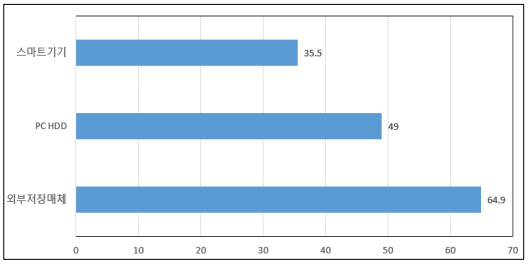

그림 1. 저장매체 사용 현황(2014년 11월 기준)

하지만 공인인증서의 사용자가 증가함에 따라 공인인증서와 개인키에 대한 유출시도가 꾸준히 증가하고 있다[4]. 또한 USB 플래시 드라이브 등의 외부 저장매체를 PC에 연결하는 순간 데이터를 이동/복사할 수 있으며, 공격자가 개인키 파일에 대한 패스워드만 알면 정당한 사용자로 위장할 수 있다. 이러한 위협에 대응하기 위해 SMS를 이용한 휴대폰명의 인증기술, 생체인증을 통한 본인 인증 기술, 보안토큰, OTP 등의 안전한 개인키 관리 방안 등의 방안이 새롭게 제시되고 있다[5][6]. 하지만, 보안토큰은 전용 저장매체를 소지해야 하는 불편함이 있으며, OTP 등의 개인키 관리방안은 암호화된 개인키에 대한 관리방안만 제시되고 저장매체에 대한 보호방안이 없다.

본 논문에서는 스마트폰의 고유번호인 IMEI (International Mobile Equipment Identity)를 이용하여 공인인증서 파일과 개인키 파일을 안전하게 유지할 수 있는 방안을 제안하고자 한다.

본 논문의 구성은 2장에 공개키 기반 구조(Public Key Infrastructure, 이하 'PKI'라 함)와 IMEI를 살펴보고, 3장에서는 스마트폰을 이용한 공인인증서 및 개인키 파일의 안전한 관리 방안을 제안한다. 4장에서는 제안방안과 기존 방법과 비교 분석하였으며, 5장에 결론을 맺었다.

II. 제안 동기 및 관련 기술

1. PKI 개요

PKI는 공개키 암호시스템을 안전하게 사용하고 관리하기 위한 정보보호 표준 방식으로, 인증서 기반의 상호인증을 제공한다[7]. PKI 인증시스템은 인증서를 발급 및 관리하는 인증기관(CA)과 사용자 인증서 및 인증서 폐지목록을 저장/게시하는 디렉터리 시스템(DS), 인증서 사용자(User)로 구성된다. 우리나라에서는 전자서명법에 따라 공인인증기관에서 공인인증서와 개인키를 발급하고 있다. 이때 발급되는 공인인증서와 개인키 파일 목록은 다음 [표 2]과 같다.

표 2. 공인인증서와 개인키 파일 목록

파일명	설명
signCert.der	X.509 인증서 형식으로 저장된 공개키 파일
signPri.key	PKCS#8 형식으로 저장된 개인키 파일
CaPubs	인증서 발급기관에 대한 체인정보가 저장된 파일

개인키 파일(signPri.key)은 개인키, 개인키 암호 알고리즘 등의 정보를 사용자가 입력한 패스워드 기반의 암호화 방식(Password Based Encryption Scheme, PBES)으로 암호화하여 PKCS(Public-Key Cryptography Standards) #8 구조체에 맞추어 저장한다[8][9]. 이때

암호화되어 저장된 개인키 파일은 전자서명 생성/검증 또는 암/복호화 시에 사용자로부터 패스워드를 입력받아 복호화 후 사용한다. 이에 따라 공격자들은 사용자의 개인키 파일과 패스워드를 알아내기 위한 다양한 시도를 한다.

2. IMEI 개요

스마트폰에는 제조사에서 부여하는 IMEI가 있으며, IMEI는 이동통신사에서 도난당한 스마트폰이나 등록되지 않은 단말기의 사용을 방지하기 위해 사용한다. 이러한 IMEI는 단말기 출고 시 제조사가 부여하는 고유 식별번호로, 이동통신사에서 단말기 제조사/국적/모델/단말기 일련번호 등의 정보가 포함된다[10]. 또한 동일한 모델이더라도 단말기별로 고유한 일련번호를 할당하므로 IMEI로 단말기를 식별할 수 있다.

표 3. IMEI 구조와 형식[10]

구분	자릿수	설명
TAC (Type Allocation Code)	AA(2)	IMEI 인증기관 고유번호
	BBBBCC(6)	승인번호 (Allocation code)
일련번호	DDDDDD(6)	단말기 고유번호
체크 디지트	E(1)	EIR 등록 검증용 번호

다음 그림은 스마트폰(삼성전자 갤럭시 S4 미니)에서 디바이스 정보 보기를 통해 확인한 IMEI이다.

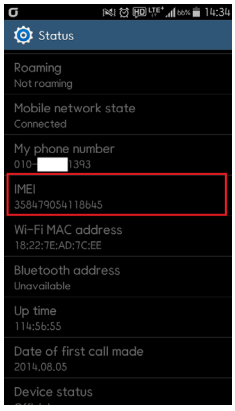

그림 2. 삼성 갤럭시 S4 미니 IMEI 정보

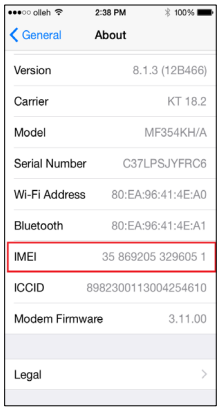

그림 3. 아이폰 5S IMEI 정보

III. 제안 방안

본 논문에서는 기존의 공인인증시스템을 그대로 사용하면서 스마트폰 단말기의 IMEI를 이용하여 공인인증서 및 개인키 파일을 지정된 스마트폰에만 안전하게 보관할 수 있는 방안을 제안하였다.

아래 절에서 사용하는 기호에 대한 표기법은 다음과 같은 의미를 갖는다.

표 4. 표기법

표기법	설명
Pub_Key	사용자 공개키
Pri_Key	사용자 개인키
ID	사용자 ID
PW	사용자 Password
IMEI	스마트폰 단말기의 IMEI 정보
Container ID	USB 플래시 드라이브에 대한 고유한 식별 정보 [12][13]
eKey	사용자의 개인키를 암복호화하기 위한 비밀키
User_Cert	사용자의 인증서
Key_Gen(A, B)	사용자의 공개키(A)와 개인키(B)쌍을 생성
$E_{Key}(M)$	메시지(M)를 Key로 암호화
$D_{Key}(M)$	메시지(M)를 Key로 복호화
H(M)	메시지(M)를 일방향 해시
A || B	문자열(A)와 문자열(B)를 순차적으로 연결

1. 사용자 인증서 발급 및 저장 절차

사용자가 PKI 인증시스템으로부터 공인인증서와 개인키 파일을 발급받는 전체적인 절차는 기존의 방식과 동일하다. 다음 [그림 4]는 사용자 인증서 발급 후 스마트폰에 저장하는 절차이며, 각 단계별 세부절차는 다음과 같다.

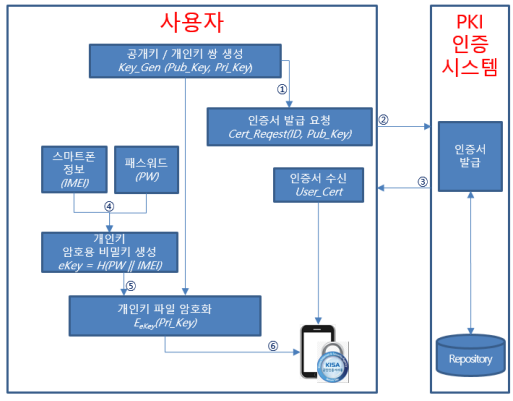

그림 4. 사용자 인증서 발급 및 저장 절차

① 스마트폰에서 공개키(Pub_Key)/개인키(Pri_Key) 쌍을 생성한다.
② 생성된 공개키를 PKCS#10 인증서 요청양식[11]에 따라 작성 후 PKI 인증시스템에 인증서 발급을 요청한다.
③ 사용자는 PKI 인증시스템으로 부터 발급된 인증서(User_Cert)를 수신한다.
④ 개인키 암호용 비밀키(eKey = H(PW || IMEI))는 사용자로부터 입력받은 패스워드(PW)와 스마트폰의 IMEI를 조합하여 일방향 해시하여 생성한다.
⑤ ①에서 생성한 개인키를 ④에서 생성한 개인키 암호용 비밀키(eKey)로 암호화(E_{eKey}(Pri_Key))하여 스마트폰에 PKCS#8 형식의 개인키 파일(signPri.key)로 저장한다.
⑥ ③에서 수신된 인증서(User_Cert)를 스마트폰에 인증서(signCert.der)파일로 저장한다.

2. 사용자 인증서 및 개인키 사용 절차

이 절에서는 사용자가 스마트폰에 저장된 개인키와 및 인증서 파일을 사용하는 절차를 설명한다. 세부 절차는 다음 [그림 5]와 같다.

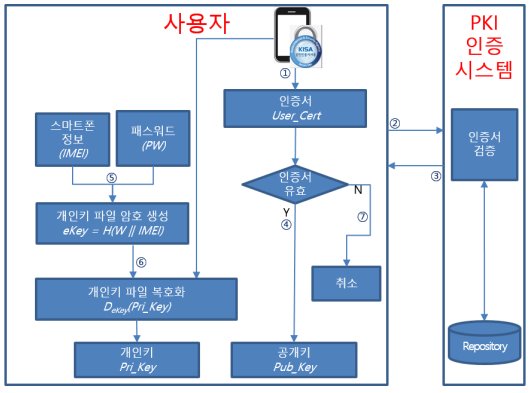

그림 5. 사용자 인증서 및 개인키 사용 절차

① 스마트폰으로 부터 사용자의 인증서(User_Cert)를 불러온다.
② 스마트폰으로 부터 불러온 사용자 인증서의 유효성 검증을 PKI 인증시스템에 요청한다.
③ PKI 인증시스템은 사용자 인증서의 유효성을 검증 후 그 결과를 사용자에게 전송한다.
④ 사용자 인증서가 유효한 경우에만 인증서 파일(User_Cert)로 부터 공개키(Pub_Key)를 추출한다.
⑤ 개인키 복호용 비밀키(eKey = H(PW || IMEI))는 사용자로부터 입력받은 패스워드(PW)와 스마트폰의 IMEI를 조합하여 일방향 해시하여 생성한다.
⑥ 스마트폰에 암호화되어 저장된 개인키 파일을 복호화 (D_{eKey}(Pri_Key))하여 원래의 개인키(Pri_Key)를 추출한다.
⑦ ④에서 추출한 공개키(Pub_Key)와 ⑥에서 복호한 개인키(Pri_Key)를 이용해 일반 응용프로그램에서 전자서명 생성/검증 등에 활용한다.

3. 스마트폰으로 복구 절차

이 절에서는 사용자가 스마트폰을 교체 또는 분실에 대비하여 USB 플래시 드라이브에 백업했던 개인키 및 인증서 파일을 새로운 스마트폰에 복구하는 절차를 설명한다. 세부 절차는 다음 [그림 6]와 같다.

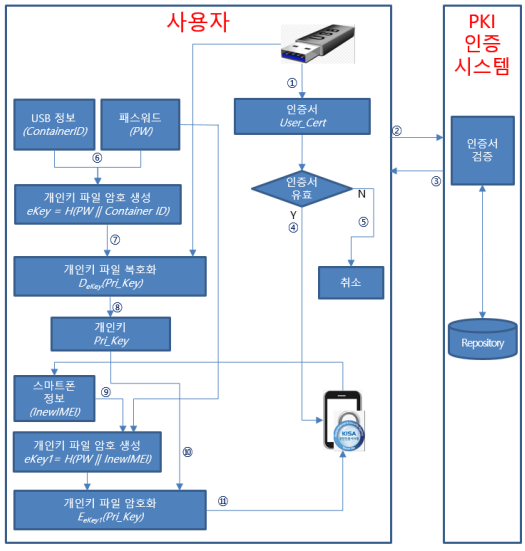

그림 6. 스마트폰으로의 복구 절차

① USB 플래시 드라이브에서 사용자의 인증서(User_Cert)를 불러온다.

② USB 플래시 드라이브에서 불러온 인증서의 유효성 검증을 PKI 인증시스템에 요청한다.
③ PKI 인증시스템은 사용자 인증서의 유효성을 검증 결과를 사용자에게 전송한다.
④ 인증서가 유효한 경우에만 인증서 파일(User_Cert)을 스마트폰에 저장한다.
⑤ 인증서가 유효하지 않은 경우 스마트폰 변경절차를 취소한다.
⑥ 사용자로부터 패스워드(PW)를 입력받고 USB 플래시 드라이브의 Container ID를 로드한다.
⑦ 개인키 복호용 비밀키(eKey = H(PW || Container ID))는 사용자로부터 입력받은 패스워드(PW)와 USB 플래시 드라이브의 Container ID를 조합하여 일방향 해시하여 생성한다.
⑧ 스마트폰에 암호화되어 저장된 개인키를 복호화(D_{eKey}(Pri_Key))하여 개인키(Pri_Key)를 추출한다.
⑨ ⑧에서 추출한 개인키를 암호화하기 위해 개인키 암호용 비밀키(eKey1 = H(PW || newIMEI))를 ⑥에서 입력받은 사용자 패스워드(PW)와 새로운 스마트폰의 IMEI(newIMEI)를 조합하여 일방향 해시알고리즘으로 생성한다.
⑩ ⑧에서 복호된 개인키를 ⑨에서 생성한 개인키 암호용 비밀키로 암호화(E_{eKey1}(Pri_Key)) 후 스마트폰에 PKCS#8 형식의 개인키 파일(signPri.key)로 저장한다.

4. USB 플래시 드라이브로의 백업 절차

이절에서는 사용자가 스마트폰 분실 등에 대비하여 자신의 공인인증서와 개인키를 USB 플래시 메모리에 백업하는 절차를 설명한다. 세부 절차는 다음 [그림 7]과 같다.

① 스마트폰에서 사용자의 인증서(User_Cert)를 불러온다.
② 스마트폰에서 불러온 인증서의 유효성 검증을 PKI 인증시스템에 요청한다.
③ PKI 인증시스템은 사용자 인증서의 유효성을 검증 결과를 사용자에게 전송한다.
④ 인증서가 유효한 경우에만 인증서 파일(User_Cert)을 USB 플래시 드라이브에 저장한다.
⑤ 인증서가 유효하지 않은 경우 백업절차를 취소한다.
⑥ 스마트폰의 IMEI를 조회 후 사용자로 부터 패스워드(PW)를 입력받는다.
⑦ 개인키 복호용 비밀키(eKey = H(PW || IMEI))는 사용자로부터 입력받은 패스워드(PW)와 스마트폰의 IMEI를 조합하여 일방향 해시하여 생성한다.
⑧ 스마트폰에 암호화되어 저장된 개인키를 ⑦에서 생성한 비밀키(eKey)로 복호화(D_{eKey}(Pri_Key))하여 개인키(Pri_Key)를 추출한다.
⑨ 개인키 암호용 비밀키(eKey1 = H(PW || Container ID))는 사용자로부터 입력받은 패스워드(PW)와 USB 플래시 드라이브의 Container ID를 조합하여 일방향 해시하여 생성한다.
⑩ ⑨에서 생성한 비밀키로 ⑧에서 복호한 개인키 암호화(E_{eKey1}(Pri_Key))하여 USB 플래시 드라이브에 PKCS#8 형식의 개인키 파일(signPri.key)로 저장한다.

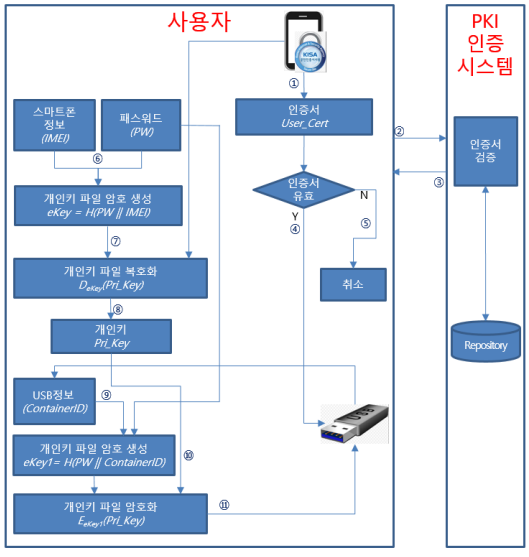

그림 7. USB 플래시 드라이브로의 백업 절차

지금까지 제안 방안의 사용자 인증서 발급 및 저장, 스마트폰에 저장된 인증서/개인키 파일의 사용, 스마트폰 변경 및 USB 플래시 드라이브에 백업 절차를 설명

하였다. 다음 장에서는 제안 방안의 안전성을 기존 인증방법과 비교 분석하였다.

IV. 고찰 및 검증

본 장에서는 제안 방안의 안전성을 평가하기 위해 기존의 USB 저장 방안 및 보안토큰(HSM)을 이용하는 방안, OTP 기반의 키관리 방안을 활용한 방안과 제안 방안을 비교 평가하였다.

표 5. 인증방식 비교

	기존 USB 저장	HSM 방안	OTP 방안	제안 방안
저장 매체	일반 USB 플래시 드라이브	전용 장치	전용 OTP장치	스마트폰
인증 요소	개인키 패스워드	개인키 패스워드 + 전용 HW장치	개인키 패스워드 + OTP장치정보	개인키 패스워드 + 스마트폰 고유정보
재사용 방지	X	O	O	O
개인키 패스워드 노출에 따른 취약성	O	X	X	X
보안강도	중	상	상	상

[표 5]에서 보는 바와 같이 제안방안은 스마트폰을 개인키 및 인증서를 저장하는 저장매체로 활용한다, 또한, 기존의 USB 저장 방식을 비롯한 다른 방안도 개인키 암호용 패스워드를 공통적으로 사용하지만, 저장매체에 따라 전용 HW 장치/OTP장치정보/스마트폰의 주요 기기정보 등을 조합하여 인증요소로 사용한다. 그리고 기존 PKI 기반 USB 저장 방식은 USB 플래시 드라이브에 저장된 개인키/인증서 파일을 임의로 다른 USB 플래시 드라이브에 이동/복사하여 재사용이 가능하다. 그러나 제안 방안을 비롯한 보안토큰(HSM)을 이용하는 방식, OTP 기반의 키관리 방안 등은 하드웨어 정보를 사용하여 추가 인증요소로 사용하므로 재사용 방지 기능을 제공한다. 또한, 기존 PKI기반 USB 저장 방식은 개인키 암호용 패스워드를 공격자가 알아내면 어디서든지 암호화된 개인키를 복호하여 정당한 사용자로 위장하여 사용할 수 있다. 그러나 제안방안은 개인키 암호용 패스워드와 스마트폰의 고유정보를 조합하여 개인키를 암호화하여 저장하므로 공격자가 개인키 암호용 패스워드를 알아내더라도 스마트폰의 IMEI를 알 수 없으므로 암호화된 개인키 파일을 복호화가 불가능하여 암호화된 개인키 파일을 안전하게 보호할 수 있다. 따라서 제안방안은 기존 USB 플래시 드라이브에 저장하던 방식에 비해서 전용 HW 장치/OTP장치 정보와 동일한 수준의 보안강도를 제공한다.

V. 결론

최근까지도 공인인증서의 안전성 문제는 지속적으로 제기되지만 대부분의 사용자가 공인인증서를 사용하고 있다. 이때 대부분 사용자들은 보안토큰이 아닌 일반 USB 플래시 드라이브, 하드디스크 드라이브 또는 스마트폰에 저장하고 있다. 그러나 이러한 저장매체에 저장된 파일은 악성코드에 의해 쉽게 탈취 가능하고, 추가적으로 패스워드까지 해커에게 노출될 경우 해커는 아무런 제한 없이 사용할 수 있다.

이에 본 논문에서는 패스워드와 스마트폰의 IMEI를 조합하여 개인키 파일의 안전한 관리 방안을 제안 하였다. 즉, 정당한 스마트폰 사용자만 개인키 파일을 복호화가 가능하지만, 다른 저장매체에서는 스마트폰의 IMEI를 알 수 없어서 개인키 파일을 복호할 수 없다. 특히 제안 방안은 스마트폰과 일반 USB 플래시 드라이브만 있으면 되며, 스마트폰 OS의 SDK(Software Development Kit)에서 제공하는 간단한 API(예. getDeviceId)를 이용해 쉽게 구현이 가능하다. 또한 기존 공인인증체계의 스마트폰 관련 모듈을 간단히 수정하면 되어 개발비용이 적게 드는 장점이 있다. 또한 기존 공인인증체계에서는 파일의 안전한 관리를 위해 암호화하는 방안 이외에는 연구된 사례가 미비했지만, 스마트폰의 IMEI를 이용하여 개인키 파일의 안전한 관리 방안을 통해 제안했다는 점에서 학문적 의의가 매우 크다.

향후 제안방안을 구현하여 성능 검증, 스마트폰 분실 시 개인키/인증서 파일의 안전한 복구 방안에 대한 지속적인 연구가 필요하다.

참 고 문 헌

[1] "2015년 상반기 모바일 트랜드," KT경제경영연구소 DIGIECO, 2015.7.6.

[2] http://rcps.egovgo.kr:8081/jsp/stat/ppl_stat_jf.jsp

[3] http://www.boannews.com/media/view.asp?idx=45468

[4] http://www.boannews.com/media/view.asp?idx=44245

[5] 소프트포럼, "보안토큰(HSM) 활성화 방안," 2007(4).

[6] 김선주, 조인준, "OTP를 이용한 PKI 기반의 개인키 파일의 안전한 관리방안," 한국콘텐츠학회논문지, 제14권, 제12호, pp.565-573, 2014.

[7] http://word.tta.or.kr

[8] B. Kaliski, PKCS #8: Private-Key Information Syntax Standard V1.2, RSA Laboratories, 2008.

[9] B. Kaliski, PKCS #5, Password Based Cryptography Standard V2.1, RSA Laboratories, 2000.

[10] TTAE.3G-22.016, "IMT2000 3GPP - 국제이동통신장비식별(IMEI)," TTA, 2000.07.13.

[11] B. Kaliski, PKCS #10: Certification Request Syntax Standard V1.7, RSA Laboratories, 2008.

[12] 김선주, 조인준, "USB 메모리의 컨테이너ID를 이용한 PKI 기반의 개인키 파일의 안전한 관리방안," 한국콘텐츠학회논문지, 제15권, 제10호, pp.607-615, 2015.

[13] https://msdn.microsoft.com/en-us/library/windows/hardware/ff540024(v=vs.85).aspx

저 자 소 개

김 선 주(Seon-Joo Kim) 정회원

- 1998년 2월 : 배재대학교 컴퓨터공학과 졸업
- 2001년 2월 : 배재대학교 컴퓨터공학과 석사
- 2013년 2월 : 배재대학교 컴퓨터공학과 박사
- 2001년 1월 ~ 2003년 9월 : ㈜케이사인 선임연구원
- 2003년 9월 ~ 현재 : 한국정보통신기술협회 책임연구원

<관심분야> : 클라우드 컴퓨팅, SW 테스팅, 정보보호 제품 평가