http://dx.doi.org/10.5392/JKCA.2015.15.10.607

USB 메모리의 컨테이너ID를 이용한 PKI 기반의 개인키 파일의 안전한 관리 방안

Management Method for Private Key File of PKI using Container ID of USB memory

김선주*, 조인준**
한국정보통신기술협회*, 배재대학교 사이버보안학과**

Seon-Joo Kim(sunjoo@tta.or.kr)*, In-June Joe(injune@pcu.ac.kr)**

요약

대부분의 인터넷 사용자 및 스마트폰 보유자는 공인인증서를 발급 받았고, 공인인증서를 통해 계좌 이체, 주식거래, 쇼핑 등 다양한 업무에 활용하고 있다. 대부분은 PC나 USB 메모리와 같은 외부 저장매체에 공인인증서와 개인키를 저장한다. 특히, 공인인증기관에서는 공인인증서와 개인키 저장매체로 하드디스크보다는 보안토큰, 휴대폰, USB 메모리 등의 저장매체를 권장하고 있다. 그러나 USB메모리는 PC에 연결되는 순간 쉽게 이동/복사될 수 있고, 악성코드나 파밍 사이트 연결을 통해 쉽게 해커에게 인증서 파일과 개인키 파일이 노출될 수 있다. 더욱 큰 문제는 해커에게 복사된 인증서 파일과 개인키 파일은 아무런 제약 없이 사용자의 패스워드만 알면 정당한 사용자처럼 사용할 수 있다는 점이다. 이에 본 논문에서는 암호화된 개인키 파일의 패스워드와 USB 메모리의 HW 정보를 이용하여 USB 메모리에 개인키 파일의 안전한 관리 방안을 제안하였다. 이를 통해, 해커에 의해 암호화된 개인키 파일을 임의로 이동/복사되거나 또는 개인키 파일이 노출되더라도 암호화된 개인키를 안전하게 보호할 수 있다. 또한, 개인키 파일의 패스워드가 노출되더라도 USB 메모리의 컨테이너ID라는 추가 인증요소를 활용하여 개인키를 안전하게 보호할 수 있다. 따라서 활용도가 매우 높은 공인인증체계에서 제안시스템은 저장매체 보호 방안으로 보안성이 크게 향상될 것으로 기대한다.

■ 중심어 : | 공개키 기반 구조 | 공인인증서 | 개인키 파일 | USB 메모리 | 컨테이너 ID |

Abstract

Mosts user of internet and smart phone has certificate, and uses it when money transfer, stock trading, on-line shopping, etc. Mosts user stores certificate in a hard disk drive of PC, or the external storage medium. In particular, the certification agencies are encouraged for user to store certificate in external storage media such as USB memory rather than a hard disk drive. User think that the external storage medium is safe, but when it is connect to a PC, certificate may be copied easily, and can be exposed to hackers through malware or pharming site. Moreover, if a hacker knows the user's password, he can use user's certificate without restrictions. In this paper, we suggest secure management scheme of the private key file using a password of the encrypted private key file, and a USB Memory's hardware information. The private key file is protected safely even if the encrypted private key file is copied or exposed by a hacker. Also, if the password of the private key file is exposed, USB Memory's container ID, additional authentication factor keeps the private key file safe. Therefore, suggested scheme can improve the security of the external storage media for certificate.

■ keyword : | PKI | Certificate | Private Key File | USB Memory | Container ID |

접수일자 : 2015년 06월 15일
수정일자 : 2015년 07월 07일
심사완료일 : 2015년 07월 07일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

우리는 공인인증서를 이용하여 계좌 이체, 주식 거래, 쇼핑 등의 다양한 업무에 활용하고 있다. 이처럼 다양한 업무에 활용하는 공인인증서의 저장매체 보호방안 연구는 많지 않다. 2014년 KISA가 인터넷 사용자 및 스마트폰 보유자 1,203명을 대상으로 조사한 바에 따르면, 92.1%가 공인인증서를 발급받았고, 이중 64.9%가 USB 메모리 등의 외부 저장매체에 공인인증서를 저장하고 있다는 조사결과가 발표되었다[1]. 즉, 대부분의 사용자가 USB 메모리는 안전하다고 인식하고 있다. 그러나 USB 메모리는 PC에 연결되는 순간 공인인증서를 쉽게 복사하여 탈취가 가능하므로 안전하지 않다.

최근 들어 공인인증서의 사용자가 증가하면서 공인인증서에 대한 유출시도가 지속적으로 증가하고 있다. 금융기관 이용자 PC에서 파밍 사이트 연결을 통한 공인인증서 유출이 2014년 11월에만 7,000건이나 집계되었으며[2], 드라이브 바이 다운로드(Drive by download) 방식의 악성코드를 이용하여 공인인증서의 탈취 위협이 증가하고 있다[3].

이러한 위협에 대응하기 위한 기술로 보안토큰[4], USIM 스마트 인증 기술[5][6], OTP를 이용한 PKI기반의 개인키 관리 방안[7][8], 인증서와 개인키 유출방지를 위한 보안키 저장소[17] 등이 새롭게 제안되고 있다. 보안토큰(HSM)은 공인인증서를 보관할 수 있는 장치가 있는 물리적인 USB 메모리 장치이고, USIM 스마트 인증은 통신사에서 제공하는 USIM에 공인인증서를 저장하고 스마트폰을 통해 전자 서명하여 안전하게 보관된다. 그러나 보안토큰은 보안토큰 전용 저장매체를 소지해야 하는 불편함이 있으며, USIM 스마트 인증은 이동통신사에 매달 일정액을 지불해야 하고 통신사에서 제공하는 전용 프로그램만 사용할 수 있다. 또한 OTP를 이용한 PKI기반 개인키 관리방안은 암호화된 개인키에 대한 관리방안만 있고, 저장매체에 대한 보호방안은 제안되지 않았다.

따라서 본 논문에서는 USB 메모리의 컨테이너 정보를 활용함으로써 개인키 파일의 암호용 패스워드, 개인키 파일 및 공인인증서가 탈취되더라도 안전하게 유지할 수 있는 방안을 제안하고자 한다.

본 논문의 구성은 2장에 본 논문과 관련된 공개키 기반 구조(Public Key Infrastructure, 이하 'PKI'라 함) 개요 및 USB 메모리의 특성을 정리하고, 3장에 제안시스템을 설명하였다. 4장에서는 제안시스템의 타당성을 객관적으로 증명하기 위해 다른 인증서 보관 방법과 비교분석하였고, 5장에 결론을 맺었다.

II. 관련 연구

2.1 PKI 개요

PKI는 통신을 수행하는 주체 간에 상호 신뢰할 수 있도록 지원하는 공개키 암호시스템으로, 인터넷을 통한 전자상거래를 수행하는 이용자의 전자서명과 암호화에 의한 보안기술이다[9][10]. 이러한 PKI 인증시스템은 인증기관(CA), 등록대행기관(RA), 디렉터리 시스템(DS), 사용자(User)로 구성된다. 먼저, 인증기관(CA)은 사용자(User)의 인증서 발급요청에 따라 생성된 공개키 정보가 포함된 인증서를 발급 및 관리 시스템으로 사용자의 인증서와 인증서 폐지목록을 디렉터리 시스템(DS)에 게시한다. 사용자의 인증서 발급 요청을 수행하는 등록대행기관(RA), 인증서와 폐지된 인증서 목록이 저장된 디렉터리 시스템(DS)과 해당 인증서를 사용하는 사용자(User)가 있다. 각 구성요소 간 관계는 다음 [그림 1]과 같다.

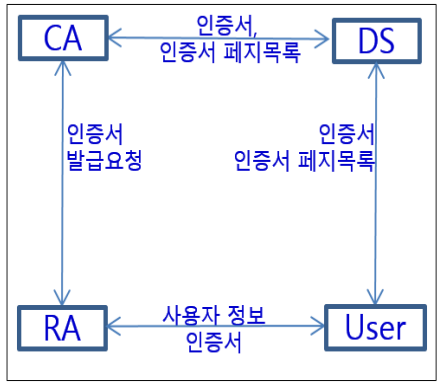

그림 1. PKI 개요

이때, 인증기관으로부터 발급된 사용자 인증서 파일 및 해당 파일의 용도는 [표 1]과 같다.

표 1. 인증서 관련 파일 및 용도

파일명	용도
signCert.der	인증서의 버전, 인증서 소유자 정보, 유효기간, 인증서 발급자 정보 등이 X.509 형식에 맞춰서 저장된 공개키 파일
signPri.key	PKCS#8 구조에 따라 암호화되어 저장한 개인키 파일
CaPubs	인증서의 유효성 검증을 위한 인증서 체인(발급기관 정보) 파일

개인키 파일은 패스워드 기반의 암호화 방식(Password Based Encryption Scheme, PBES)으로 암호화되어 저장된다[11][12]. 이때 암호화된 개인키는 사용자가 입력한 패스워드로 복호화 후 전자서명 생성·검증 및 암·복호화에 사용된다.

사용자 인증서 파일 중 인증서(signCert.der)는 사용자 접근제한이 없는 디렉터리 서버에 게시되어 쉽게 다운로드 가능하다. 또한, 인증서 체인 파일(CaPubs)는 인증서 파일을 통해 발급기관 정보를 쉽게 구할 수 있다. 그러나 개인키 파일(signPri.key)은 보안토큰, 휴대폰뿐만 아니라 많은 사용자가 PC의 하드디스크나 USB 메모리에 저장하고[18], 사용자 인증서 파일이 저장된 디렉터리는 "ProgramFiles\NPKI" 폴더로 많이 알려져 있다. 이러한 이유로 공격자(해커)는 사용자 PC에 악성코드를 설치하여 사용자 인증서를 포함하여 개인키 파일을 탈취가 가능하다.

2.2 USB 메모리 개요

USB(Universal Serial Bus, 이하 'USB'라 함)는 컴퓨터와 주변기기 사이에 데이터를 주고받을 때 사용하는 버스(Bus, 데이터가 전송되는 통로) 규격 중 하나이다. USB 메모리는 데이터를 저장, 보관할 수 있는 반도체인 플래시 메모리(Flash Memory)와 데이터 전송 규격인 USB를 결합한 것이다[13]. USB 메모리는 이스라엘의 IT업체인 M-system에서 8/16/32MB 용량의 제품을 2000년 9월에 처음 선보였다[14]. USB 메모리는 작고 가벼운 휴대성이 있고, USB 포트에 꽂기만 하면 쉽게 파일을 이동/복사/삭제가 가능하여 널리 쓰이며, 현재 많은 IT업체에서 16/32/64GB 용량의 제품을 선보이고 있다.

USB 메모리의 내부 구조는 [그림 2]와 같이 ① 플래시 메모리, ② 컨트롤러, ③ USB 커넥터로 구성된다.

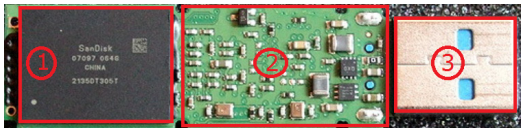

그림 2. USB 메모리 구조

먼저, ① 플래시 메모리는 데이터를 저장, 보관할 수 있는 반도체 장치이다. 데이터를 저장 및 삭제가 쉽고, 전원이 차단되어도 저장된 데이터가 보존된다. ② 컨트롤러는 플래시 메모리와 USB 커넥터 사이에서 데이터 전송을 제어한다. ③ USB 커넥터는 PC나 각종 IT 기기의 USB 포트에 연결되어 전원 공급과 데이터 전송 매체이다. 이러한 USB 메모리는 휴대하기 쉽고 부피도 작다. 하지만, 부피가 작아서 USB 메모리 분실에 따른 USB 메모리에 저장된 주요데이터의 노출 위험성이 커진다. 또한, USB 메모리를 PC에 꽂는 순간 USB 메모리에 저장된 데이터가 악성코드에 의해 쉽게 이동/복사될 수 있는 문제점이 있다.

2.3 USB 메모리 장치 인식 절차 및 파일 정보

USB 메모리의 인식 절차는 [그림 3]과 같다.

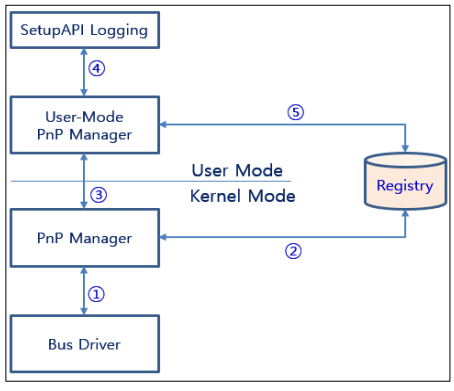

그림 3. USB 메모리 장치 인식 절차

① USB 메모리를 PC의 USB 포트에 연결하면, 버스 드라이버(Bus Driver)가 PnP 관리자(PnP Manager)에게 제조사 및 일련번호, 드라이버 정보 등이 포함된 USB 메모리의 고유 식별 정보(Device descriptor)를 보내 장치의 연결을 알린다.

② USB 메모리의 고유 식별 정보를 수신한 PnP 관리자는 Device Class ID를 생성 후 레지스트리에서 해당 장치에 맞는 드라이버를 검색한다.

③ 커널모드(Kernel Mode)의 PnP 관리자는 레지스트리에 드라이버가 있으면 해당 장치 드라이버를 로드하고, 장치 드라이버가 없으면 장치 펌웨어에 드라이버를 요청하여 사용자 모드의 PnP 관리자에게 전달한다.

④ 사용자 모드(User Mode) PnP 관리자는 전달받은 드라이버를 PC에 설치한다.

⑤ 사용자 모드의 PnP 관리자는 USB 메모리 장치의 드라이버를 설치하고, 해당 USB 메모리 장치를 저장매체로 마운트 시키고, USB 메모리 정보를 레지스트리에 기록한다. 이때, 레지스트리에 저장되는 USB 메모리 관련 정보는 다음 [표 2]와 같다.

표 2. 레지스트리에 저장되는 USB 메모리 정보

식별자	설명
장치 클래스 ID	USB 메모리 장치의 형식, 제조사명, 제품명, 버전을 이용해 만들어진 식별자
고유 인스턴스 ID	USB 메모리 장치의 시리얼 번호이며, 시리얼 번호가 포함되어 있지 않으면 OS에서 임의로 생성함
제조사ID와 제품ID	USB 메모리 제조사 및 제품 식별자
볼룸 레이블과 드라이브 문자	일반적으로 OS에서 할당하는 문자로 마운트 되지만, 지정되지 않았을 경우 해당 볼륨레이블과 함께 드라이브 문자가 표시됨
볼륨 시리얼 번호	USB 메모리 장치에 대한 볼륨 시리얼 번호
사용자명과 볼륨 GUID	다중사용자가 시스템을 사용하는 경우 USB메모리 장치를 마운트 시킨 사용자 정보와 볼륨 정보
최초연결시각	시스템에 USB 메모리 장치를 최초 연결한 시각 정보
부팅 후 최초 연결 시각	시스템 구동 후 USB 메모리 장치를 처음 연결한 시각 정보
마지막 연결 시각	USB 메모리 장치를 가장 최근에 연결한 시각 정보

레지스트리에 저장되는 USB 메모리 관련 정보 즉, 장치 클래스ID, 고유 인스턴스ID, 제조사ID와 제품ID, 볼륨 시리얼 번호 등을 활용하여 운영체제에서 사용할 수 있는 문자열 형태의 USB 컨테이너ID를 생성하여 사용한다[15]. 아래 [그림 4]는 USB 메모리 장치를 PC에 연결했을 때 생성된 USB 컨테이너ID값이다.

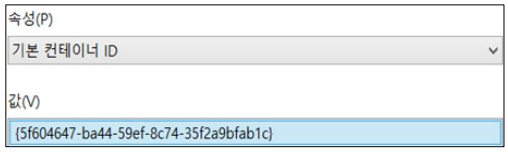

그림 4. USB 컨테이너ID값

운영체제는 USB 컨테이너ID값을 통해 유일한 USB 장치로 인식하며, USB포트에 연결된 장치를 식별하여 해당 장치의 유형(키보드, 마우스, USB 메모리 장치)에 따라 해당 장치에 맞는 기능을 수행한다.

III. 제안 방안

지금까지 PKI 인증시스템과 USB 메모리 장치의 특성을 정리하였다. 본 장에서는 제안 방안의 설계 및 동작 절차를 설명한다.

본고에서는 기존 PKI 인증시스템에 USB 메모리의 컨테이너ID 문자열을 이용하여 개인키를 포함한 공인인증서 관련 파일을 사용자가 지정한 USB 메모리에만 보관할 수 있는 방안을 제안하였다.

3.1 사용자 인증서 발급 및 USB 메모리 등록 절차

본 절에서는 PKI 인증시스템으로 부터 사용자가 인증서를 발급받을 때, 개인키가 포함된 공인인증서 관련 파일을 지정된 USB 메모리 장치에 저장하는 절차를 설명한다.

사용자 인증서 발급 및 USB 메모리 등록 절차는 [그림 5]와 같다.

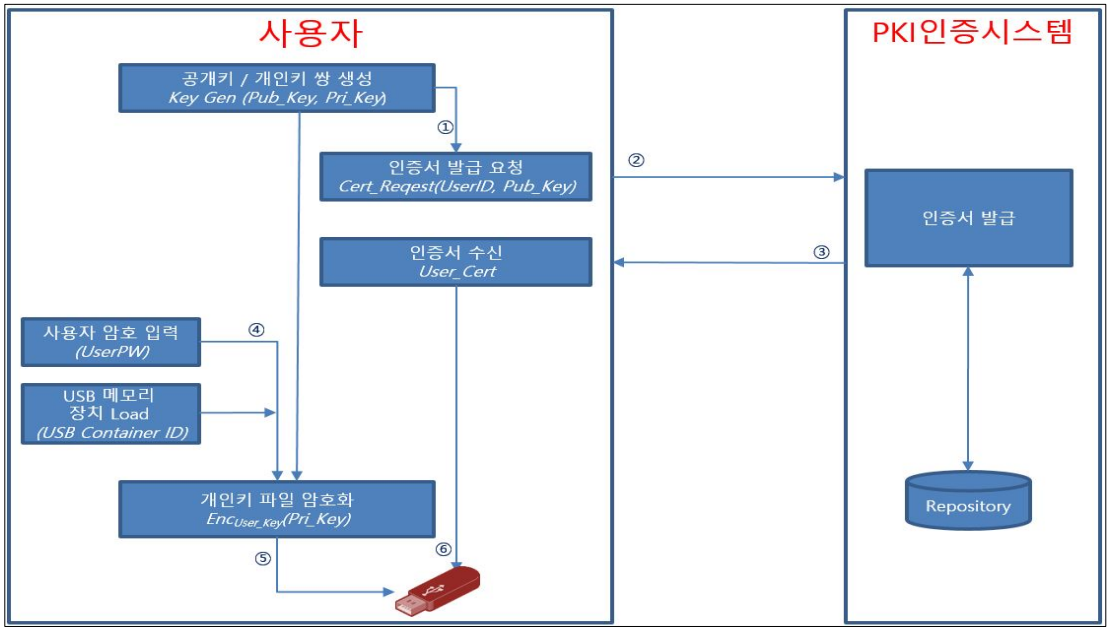

그림 5. 사용자 인증서 및 개인키 등록 절차

① 사용자 PC에서 개인키와 공개키 쌍을 생성한다.

② 생성된 공개키와 사용자 정보를 PKCS #10 인증서 요청 양식[16]에 따라 작성하여 PKI 인증시스템에 사용자의 인증서 발급을 요청한다.

③ 사용자는 PKI 인증시스템으로 부터 발급된 인증서 *(User_Cert)*를 수신한다.

④ ③번 단계가 완료되면, 사용자로부터 개인키 암호용 패스워드를 입력받고, USB 메모리의 컨테이너 ID 값과 조합하여 해시값*(User_Key)*을 생성한다.

$$User\_Key = H(UserPW \,||\, ContainerID)$$

⑤ ①에서 생성한 개인키를 ④에서 생성한 개인키 암호용 키로 암호화하여 USB 메모리에 저장한다.

$$Enc_{User\_Key}(Pri\_Key)$$

⑥ PKI 인증시스템으로 부터 수신된 인증서*(User_Cert)*를 USB 메모리에 저장한다.

3.2 USB 메모리 변경 절차

본 절에서는 사용자가 지정한 USB 메모리의 변경 절차를 설명한다.

지정된 USB 메모리 변경 절차는 [그림 6]과 같다.

① USB 메모리에서 사용자의 인증서*(User_Cert)*를 읽어온다.

② 사용자 인증서에 대한 유효성 검증을 PKI 인증시스템에 요청한다.

③ PKI 인증시스템은 사용자 인증서의 유효성을 검증하여 그 결과를 사용자에게 전송한다.

④ 사용자의 인증서가 유효한 경우, 해당 사용자의 인증서*(User_Cert)*를 변경하고자 하는 새로운 USB 메모리에 저장한다.

⑤ ④에서 사용자의 인증서가 유효한 경우, 사용자로부터 개인키 암호용 패스워드*(UserPW)*를 입력받고, 이전 USB 메모리의 컨테이너 ID 값을 해시하여 개인키 암호용 비밀키*(User_Key1)*를 생성하여 USB 메모리에 암호화되어 저장된 개인키를 복호화 한다.

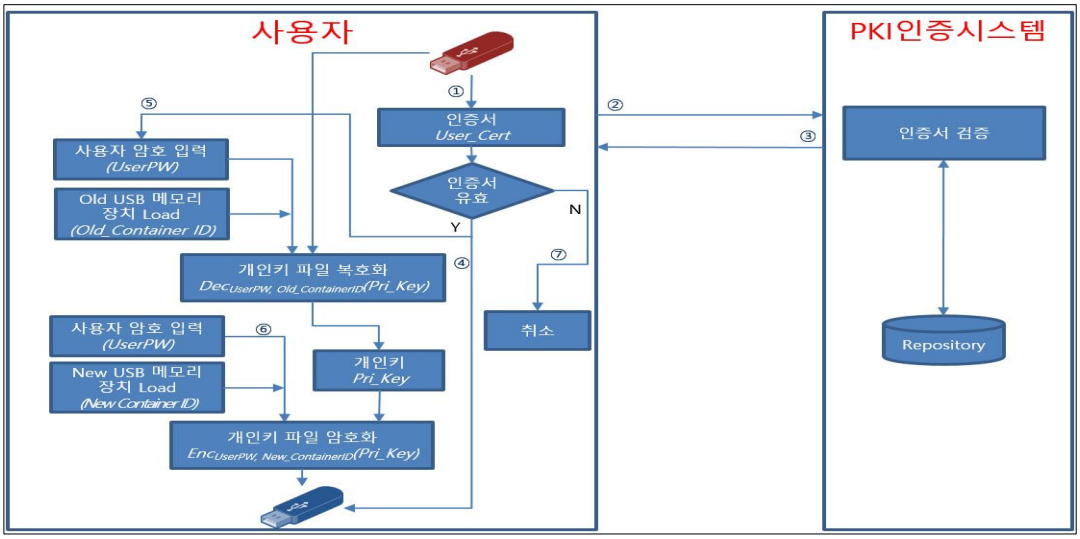

그림 6. USB 메모리 장치 변경하기

User_Key1 = H(UserPW || Old_ContainerID)

$Dec_{User\_Key1}(Pri\_Key)$

⑥ 사용자로 부터 개인키 암호용 패스워드를 다시 입력받고, 변경하고자 하는 새로운 USB 메모리의 컨테이너ID 값과 조합하여 해시값(*User_Key2*)을 생성한다.

User_Key2 = H(UserPW || New_ContainerID)

새롭게 생성된 개인키 암호용 비밀키(User_Key2)로 사용자의 개인키를 암호화하여 새로운 USB 메모리에 저장한다.

$Enc_{User\_Key2}(Pri\_Key)$

⑦ ④에서 사용자의 인증서가 유효하지 않은 경우, USB 메모리 변경절차를 취소한다.

3.3 사용자 개인키 및 인증서 사용 절차

본 절에서는 사용자가 USB 메모리에 저장된 개인키 또는 인증서의 사용 절차를 설명한다. 세부 절차는 다음 [그림 7]과 같다.

① USB 메모리로부터 사용자의 인증서(*User_Cert*)를 읽어온다.

② USB 메모리로 부터 읽어 들인 사용자 인증서에 대한 유효성 검증을 PKI 인증시스템에 요청한다.

③ PKI 인증시스템은 사용자 인증서의 유효성을 검증하여 그 결과를 사용자에게 전송한다.

④ 사용자의 인증서가 유효한 경우, 사용자의 인증서(*User_Cert*)*로부터 공개키(Pub_Key)를 추출한다.*

⑤ ④에서 사용자의 인증서가 유효한 경우, 사용자로부터 개인키 암호용 패스워드(*UserPW*)를 입력받고, USB 메모리의 컨테이너ID 값을 해시하여 개인키 암호용 비밀키(*User_Key*)를 생성한다.

User_Key = H(UserPW || ContainerID)

⑥ USB 메모리에 암호화되어 저장된 개인키를 복호화 하여 개인키(Pri_Key)를 추출한다.

$Dec_{User\_Key}(Pri\_Key)$

지금까지 제안시스템의 사용자 인증서 발급 및 USB 메모리 등록, USB 메모리 변경 및 사용자 개인키 및 인증서 사용 절차를 설명하였다.

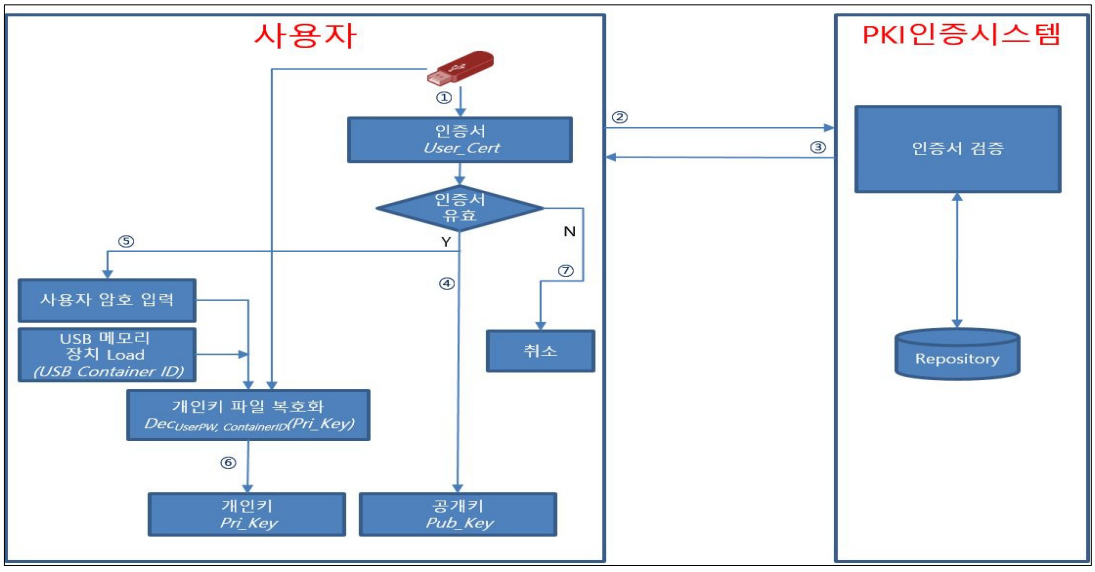

그림 7. USB 메모리에 저장된 개인키 및 공개키 로딩 절차

IV. 평가

본 장에서는 제안시스템의 객관적인 안전성 검토하기 위해 기존 PKI 인증시스템에서 안전하다고 평가받고, 활용도가 높은 방식인 USB 메모리에 개인키가 포함된 인증서를 저장하는 방식(이하, '기존방식(USB저장)'이라함)과 USIM 스마트 인증 방식, OTP 기반의 키 관리 방안 등과 제안시스템을 비교 평가하였다. 비교 결과는 다음 [표 3]와 같으며 각 차이점은 다음과 같다.

표 3. 개인키/공개키 저장 방식에 따른 비교 평가

구분 \ 방안	기존 방식 (USB저장) [9]	USIM 스마트인증 [5][6]	OTP기반 키 관리방안 [7]	제안 시스템
저장매체	일반 USB	스마트폰의 USIM	일반 USB	개인키 파일 암호화를 위해 등록된 USB
이용요금	무료	유료	무료	무료
인증요소	패스워드	패스워드 + USIM 카드암호	패스워드 + OTP	패스워드 + USB 컨테이너 ID
탈취된 데이터 재사용 방지	X	O	O	O
개인키 패스워드 노출에 따른 재사용 방지	X	X	O	O
보안성	중	상	상	상

첫째, 각각의 방식에서 사용하는 저장매체는 일반 USB 메모리 또는 스마트폰의 USIM 카드를 사용하고 있지만, 제안시스템은 일반 USB 메모리를 사용하지만, USB 메모리의 컨테이너ID 값이 동일한 장치만 사용할 수 있다는 점이 다르다. 즉, 제안시스템은 개인키 암호화를 위해 등록된 USB 메모리만 사용할 수 있는 점이 다른 방식과 다르다.

둘째, 인증요소의 차이가 있다. 기존방식(USB저장)은 개인키 암호용 패스워드, USIM 카드 패스워드, OTP 번호, 개인키 암호용 패스워드와 USB 메모리의 컨테이너ID값을 각각 사용한다.

셋째, 타 시스템과의 연동 필요성에 차이가 있다. USIM 카드 번호를 사용하기 위해서는 이동통신사와 연동이 필요하고, OTP 번호는 OTP 서버와 연동이 필요하다. 반면 제안시스템은 기존방식(USB저장)과 동일하다.

넷째, 기존 방식(USB 저장)은 USB 메모리에 저장된 개인키/인증서 파일을 임의로 이동/복사하여 바로 활용이 가능하다. 즉, 해커와 같은 공격자에 의해 탈취된 개인키/인증서가 있다면 바로 재사용이 가능하다. 그러나 USIM 스마트 인증은 이동통신사에서 제공하는 앱을

통해 USIM카드암호를 통해서만 이동/복사가 가능하고, OTP 기반 키관리 방안은 OTP서버와 연동을 통해서만 주요파일의 이동/복사가 가능하다. 또한, 제안시스템은 임의로 저장매체를 이동/복사를 하는 경우 USB 메모리의 컨테이너ID값이 달라 개인키를 사용할 수 없으며, 개인키 암호용 패스워드를 입력받아 등록된 USB 메모리를 변경하는 절차가 추가적으로 필요하다.

다섯째, PKI 인증시스템으로부터 발급받은 개인키/인증서를 개인키 암호용 패스워드만 입력 받아 저장하는 기존 방식(USB 저장), USIM 스마트인증 방식과는 다르게 OTP기반 키관리 방안은 OTP와 개인키 암호용 패스워드로 개인키를 암호화한다. 반면, 제안시스템은 컨테이너ID값과 개인키 암호용 패스워드로 개인키를 암호화한다. 이에 따라 개인키 암호용 패스워드가 외부에 노출이 되더라도 USB메모리의 컨테이너ID값을 알 수 없으므로 암호화된 개인키 파일을 복호화 하여 재사용할 수 없다. 따라서 기존 하드디스크나 USB 메모리 저장방식에 비해 제안시스템은 개인키 파일에 대해 이중으로 암호화되어 있어 보안성이 크게 향상된다.

따라서 제안시스템은 기존 방식(USB)이나 USIM 스마트인증, OTP기반 키관리방안에 비해 개인키가 포함된 인증서 파일의 재사용 방지가 되어 있어, 해당 파일이 탈취되거나 개인키 암호용 패스워드가 노출되더라도 안전하게 보호할 수 있도록 개선하였다.

V. 결론

PKI기술을 이용하는 공인인증방식은 현재까지도 안전한 보안기술이다. 그러나 파밍사이트나 악성코드를 통해 사용자의 공인인증서를 빼내가는 보안사고가 잇따라 발생하고 있어 개인키가 포함된 인증서 파일에 대한 보호대책이 필요하다. 이에 따라, 인증서 파일의 안전한 보호를 위해 키보드/메모리 해킹 방지 및 PC방화벽 사용을 강제하거나, 스마트폰을 이용한 USIM 스마트 인증 기술 활용, OTP 기반의 개인키 활용방안 등 다양한 기술들이 제안 및 활용되고 있다.

본 논문에서는 암호화된 개인키 암호용 패스워드와 USB 메모리의 컨테이너ID값을 이용하여 개인키 파일의 안전한 관리 방안을 제안하였다. 이를 통해, 해커에 의해 인증서 관련 파일이 임의로 이동/복사되더라도 개인키 파일을 복호화 할 수 없으므로 인증서 관련 파일을 안전하게 보호할 수 있게 되었다.

본 방안을 저장매체 보호 방안으로 활용함으로써 인증서 관련 파일의 보안성을 크게 향상될 것으로 기대한다. 또한 인증서를 안전하게 저장하고 보관할 수 있는 규격이 현재까지 존재하지 않아, 이에 대한 표준화 작업이 필요하다.

마지막으로 사용자 인증정보가 USB 메모리를 분실하는 경우에 인증정보가 분실되어 복구가 불가능하다. 따라서 향후 이 부분에 대한 보완 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] www.boannews.com/media/view.asp?idx= 45468

[2] www.boannews.com/media/view.asp?idx= 44245

[3] www.boannews.com/media/view.asp?idx= 45221

[4] “보안토큰(HSM) 활성화 방안”, 2007.04. 소프트포럼

[5] http://www.usimcert.com

[6] 위유경, 곽진, “USIM을 활용한 스마트워크 사용자 및 디바이스 인증 기술 연구”, 멀티미디어학회논문지, 제16권, 제3호, pp.309-317, 2013.

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

[8] 김선영, 김선주, 조인준, "이동 저장매체를 활용한 패스워드 기반 사용자 인증 강화 방안", 한국콘텐츠학회논문지, 제14권, 제11호, pp.533-540, 2014(11).

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

[10] 김미혜, 서세영, “모바일 PKI 기반한 인증구조”, 한국콘텐츠학회논문지, 제4권, 제1호, pp.67-75, 2004(3).

[11] B. Kaliski, PKCS #5, Password Based Cryptography Standard V2.1, RSA Laboratories, 2000.
[12] B. Kaliski, PKCS #8: Private-Key Information Syntax Standard V1.2, RSA Laboratories, 2008.
[13] http://it.donga.com/
[14] https://ko.wikipedia.org/
[15] MSDN, https://msdn.microsoft.com/en-us/library/windows/hardware/ff540024(v=vs.85).aspx
[16] B. Kaliski, PKCS #10: Certification Request Syntax Standard V1.7, RSA Laboratories, 2008.
[17] 박영진, 김선종, 이동훈, “인증서와 개인키 유출 방지를 위한 보안키 저장소 Secure Key Store”, 정보보호학회논문지, 제24권, 제1호, pp.31-40, 2014(2).
[18] “대국민 전자서명 이용실태 조사”, 한국인터넷진흥원.

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
- 2013년 9월 ~ 현재 : 한국정보통신기술협회 책임연구원

<관심분야> : 클라우드 컴퓨팅, SW 테스팅, 정보보호 제품 평가

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과 졸업
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1994년 : 한국전자통신연구원 선임연구원
- 1994년 1월 ~ 현재 : 배재대학교 사이버보안학과 교수

<관심분야> : 정보보호, 컴퓨터네트워크보안, 전산조직응용