https://doi.org/10.5392/JKCA.2017.17.06.032

# USIM 정보를 활용한 패스워드리스 방식의 개인키 보호 방안

## Passwordless Protection for Private Key Using USIM Information

**김선주**
한국정보통신기술협회

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

**요약**

최근 공인인증서에 대한 무용론이 제기됨에도 불구하고, 우리나라 인구의 절반(약 3,500만개)이 공인인증서를 발급받아 인터넷 뱅킹, 인터넷 쇼핑, 주식거래 등에서 본인확인용도로 사용하고 있다. 또한 공인인증서 사용자는 이동디스크나 스마트폰을 저장매체로 사용하고 있다. 이러한 저장매체는 악성코드에 의해 공인인증서 관련 파일과 사용자 패스워드가 쉽게 탈취될 수 있고 공격자는 탈취한 사용자 패스워드와 공인인증서로 언제든지 정당한 사용자로 위장할 수 있다. 이러한 공인인증서 안전성 문제로 인해 SMS를 이용한 휴대폰 소유자 인증기술, 생체인증을 통한 본인 인증 기술 등 다양한 인증기술이 제안되고 있다. 그러나 아직까지 사용자 패스워드가 필요 없고 공인인증서를 대체하는 안전한 기술이 제시되지 않고 있다.

이에 본 논문에서는 USIM 정보와 스마트폰 고유번호를 조합해서 사용자 패스워드 없이 공인인증서를 안전하게 보호할 수 있는 방안을 제안하였다. 이를 통해 공격자가 개인키 및 인증서 파일을 탈취하더라도 공인인증서를 사용할 수 없고, 사용자는 영문자/숫자/특수문자 등 조합규칙을 따르는 복잡한 패스워드를 사용하지 않아도 된다. 따라서 제안 방안을 공인인증서에 사용한다면 사용이 편리하면서도 안전한 보안 서비스를 제공할 수 있다.

■ 중심어 : | 개인키 | 인증서 | USIM | 스마트폰 고유정보 | 패스워드 리스 |

**Abstract**

Despite the opinion that certificate is useless, half of the population in Korea (approx. 35 million) get an certificate, and use it for internet banking, internet shopping, stock trading, and so on. Most users store their certificates on a usb memory or smartphone, and certificates or passwords stored on such storage media can be easily attacked and used to disguise as legitimate users. Due to these security problem of certificate, a various authentication technologies has been proposed such as smartphone owner authentication using SMS, and a personal authentication using biometric authentication. However, a safe technique is not presented yet without user password, and certificate.

In this paper, I proposed a method to secure certificate/private key without a user password using a combination of USIM card and smartphone's information. Even if a hacker gets the user password, the certificate, and the private key, he can not use the certificate. User do not need to remember complex password which is a combination of alphabetic / numeric / special characters, and use his certificate safely.

■ keyword : | Private Key | Certificate | USIM | Smartphone Information | Passwordless |

접수일자 : 2017년 04월 28일
수정일자 : 2017년 05월 08일
심사완료일 : 2017년 05월 08일
교신저자 : 김선주, e-mail : sunjoo@tta.or.kr

## I. 서 론

우리나라는 전자서명법이 제정되면서 공인인증서의 사용이 꾸준히 증가하여, 2016년 6월 현재까지 3,485만 개의 인증서가 발급되었다[1]. 공인인증서 사용실태에 따르면, 공인인증서 이용자 중 60.6% 가 5년 이상, 2~5년 미만은 21.8%로 꾸준히 사용하고 있으며, 인증서 이용자 대부분은 본인확인 서비스, 인터넷 뱅킹 서비스, 쇼핑몰 이용, 사이버 증권 등의 서비스를 사용하고 있다[2]. 또한, 사용자들은 공인인증서 저장매체로 이동식디스크(60.2%), 스마트폰(42.7%), PC HDD(41.7%)를 사용하고 있으며, 그중에서 이동식디스크 및 PC HDD는 2011년에 비해 각각 11.7%, 11.6% 감소하였고 스마트폰은 13.6%로 크게 증가했다[2].

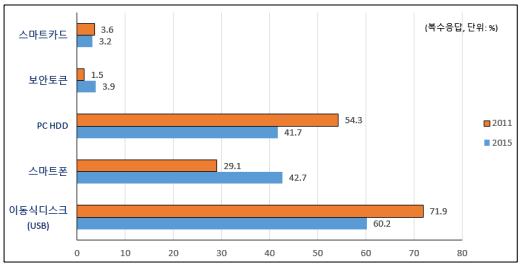


**그림 1. 공인인증서 저장매체 사용 현황**

하지만 대부분의 사람이 공인인증서를 사용하고, 스마트폰 보급률 증가에 따라 스마트폰을 공인인증서 저장매체로 활용함에 따라, 악성코드 등을 이용한 스마트폰에 저장된 공인인증서와 개인키에 대한 유출시도가 꾸준히 증가하고 있다[3][4].

이러한 위협에 대응하기 위해 OTP(One Time Password) 또는 USB 정보를 이용한 개인키 관리, 보안키 저장소 등의 방안을 통해 공인인증체계의 개인키 유출 취약점을 보완하였지만, 외부의 OTP 시스템과 연동이 필요하거나 사용자의 패스워드 입력이 반드시 요구된다[5-7]. 최근에는 사용자의 패스워드가 필요 없는 지문, 홍채 등의 생체인증을 적용한 FIDO(Fast IDentity Online)가 새롭게 제시되고 있다[8].

본 논문에서는 USIM(Universal Subscriber Identity Module, 이하 'USIM') 카드와 스마트폰 정보를 이용하여 PKI 기반의 개인키 파일을 안전하게 보호하는 방안을 제안하고자 한다.

본 논문은 2장에서는 PKI(Public Key Infrastructure, 이하 'PKI'라 함) 개요와 스마트폰 기기의 특성을 간략히 정리하였으며, 3장에서는 스마트폰 정보를 이용한 패스워드리스 방식의 개인키 파일 방안을 제시한다. 4장에서는 제안방안과 기존 방법을 비교 분석하였으며, 5장에 결론을 맺었다.

## II. 관련 연구

### 1. PKI 개요

PKI는 공개키 암호시스템을 이용하여 공개키 인증서를 안전하게 사용하고 관리하기 위한 정보보호 표준이다[9]. 그러나 최근 PKI 기반의 공인인증서에 대한 무용론이 대두되고 있으며, 이러한 원인은 공인인증서 사용을 위해 Active-X 프로그램에서 발생하는 보안취약점과 많은 종류의 Active-X 프로그램 설치 및 다양한 스마트 기기에서 사용 제한 등이라고 할 수 있다[10].

현재 우리나라의 공인인증서와 개인키 파일 목록은 다음 [표 1]과 같다.

**표 1. 공인인증서와 개인키 파일 목록**

| 파일명 | 설명 |
|---|---|
| signCert.der | 공인인증기관에서 발급하는 공개키가 포함된 X.509형식의 사용자 인증서 파일 |
| signPri.key | 공인인증기관에서 인증서 발급시 공개키와 쌍이 되는 사용자의 개인키가 저장된 파일 |
| CaPubs | 공인인증서 발급기관에 대한 정보가 저장된 파일 |

인증서 파일(signCert.der)은 공개키가 X.509 파일 포맷에 따라 소유자 정보, 유효기간, 공개키 정보 등이 저장된 파일이다. 개인키 파일(signPri.key)은 개인키 및 개인키 암호 알고리즘 등의 정보를 사용자 패스워드로 암호화하여 파일로 저장한다[11][12]. 저장된 개인키 파일은 사용자의 패스워드로 복호화 되어 전자서명 생성/검증 또는 암/복호화에 사용한다. 반면 공격자들은 키로깅, 악성코드, PC해킹 등을 통해 사용자의 인증서 및

개인키 파일과 패스워드를 몰래 빼내려는 시도가 증가하고 있다. 이러한 공격시도에 대응하기 위해 키보드 해킹 방지 프로그램, 암호화 프로그램 등의 보안프로그램 설치 및 사용을 강요하고 있는 실정으로 사용자의 편의성을 고려되지 않고 있다.

### 2. USIM 개요

USIM은 가입자 식별 정보를 구현한 IC칩으로, 주로 스마트 기기에서 가입자 확인을 위해 활용한다[8].

USIM은 사용자의 고유번호로 발급자식별자와 개인식별번호로 19자 또는 20자리를 갖는다[13][14]. 또한 스마트폰에는 제조사가 생산과정에서 부여하는 15자리의 IMEI(International Mobile Equipment Identity, 이하 'IMEI'라 함)가 있다[15]. IMEI는 제조사가 스마트폰을 공장에서 출고 시에 부여하는 식별번호로, 스마트폰의 제조사/국적/모델/스마트폰 일련번호 등의 정보가 포함되어 있으며 이동통신사에서 스마트폰을 식별하여 스마트폰의 도난을 방지하기 위해 사용한다.

**표 2. USIM 및 IMEI 구조와 형식**

| 구분 | | 자릿수 | 설명 |
|---|---|---|---|
| USIM (ICCID) | 발급자 식별자 | AA(2) | 2자리수의 USIM에 대한 산업용도 표시용이며, 전화통신용은 89 |
| | | B(1) or BBB(3) | 1~3자리수의 국가코드를 표시하는 것으로, 한국은 82 |
| | | CC(2) | 2자리수로 USIM 발급자인 이동통신사를 표시하는 코드, SKT(05), KT(30), LGT(06) |
| | 개인 식별번호 | DDDD(4) | 4자리수의 USIM 제조일자(년,월) |
| | | FFFFFF(6) or FFFFFFF(7) | 6~7자리수의 가변형 USIM 일련번호 |
| | | G(1) | 체크섬 디지트 |
| IMEI | TAC | AA(2) | IMEI 관리기관(BODY)에서 TAC의 할당된 그룹에 대한 고유코드 |
| | | BBBBBB(6) | IMEI 관리기관(BODY)에서 스마트기기를 구별하기 위해 사용하는 코드 |
| | 일련번호 | CCCCCC(6) | 스마트기기에 할당된 고유번호 |
| | 체크 디지트 | D(1) | 체크섬 디지트 |

## Ⅲ. 제안 방안

우리가 사용하는 공인인증서는 사용자의 패스워드를 입력받아 개인키를 암호화 후 PC의 HDD, USB메모리, 스마트폰 등의 저장매체에 저장하고 공인인증서 사용 시에는 사용자로부터 패스워드를 입력받아 암호화된 개인키를 복호화 하여 사용하고 있다. 이때 공격자의 공격대상이 되는 사용자의 패스워드를 보호하기 위해 보안프로그램의 설치를 강요하고, 사용자의 패스워드도 매우 복잡하게 사용하도록 강요하고 있다. 이에 본 논문에서는 기존의 공인인증시스템을 그대로 사용하면서 USIM 고유번호와 스마트폰의 고유정보를 조합하여 사용자 패스워드를 사용하지 않고 개인키 파일을 지정된 스마트폰에 안전하게 보호하는 방안을 제안하였다.

아래 절에서 사용되는 기호에 대한 표기법은 다음과 같은 의미를 갖는다.

**표 3. 표기법**

| 표기법 | 설명 |
|---|---|
| uCert | 공인인증기관에서 발급하는 공개키가 포함된 X.509 형식의 사용자 인증서 파일 |
| uPub_Key | 공개키 암호시스템에서 사용되는 사용자의 공개키 |
| uPri_Key | 공개키 암호시스템에서 사용되는 사용자의 개인키 |
| EuPri_Key | 암 · 복호용 비밀키로 암호화된 사용자의 개인키 |
| USN | USIM에 포함된 발급자식별자와 개인식별번호가 조합된 USIM의 고유번호 |
| IMEI | 스마트폰 제조사, 국적, 모델, 일련번호 등이 포함된 스마트폰의 식별번호 |
| eKey | 개인키를 암·복호화하기 위한 대칭키 기반의 비밀키 |
| EKey(M) | 메시지(M)를 Key로 대칭키 기반의 암호화를 실행함 |
| DKey(C) | 암호문(C)을 Key로 대칭키 기반의 복호화를 실행함 |
| H(M) | 메시지(M)를 일방향 해시함 |
| A \|\| B | 문자열(A)와 문자열(B)을 순차적으로 연결함 |

### 1. 사용자 인증서 발급 및 개인키 저장 절차

사용자가 PKI 인증시스템으로 부터 인증서와 개인키 파일을 발급받아 저장하는 절차는 기존과 동일하며, 세부 절차는 다음과 같다.

① 스마트폰에서 공개키(uPub_Key)와 개인키(uPri_Key) 쌍을 생성한다.

② 생성된 공개키(uPub_Key)를 PKI 인증시스템으로 전송하여 사용자의 인증서 발급을 요청한다.

③ PKI 인증시스템에서 발급된 인증서(uCert)를 수신한다.

④ USIM에서 USIM 고유번호(USN)와 스마트폰의 IMEI를 조회하여 개인키를 암·복호용 비밀키(eKey)를 생성한다.

$$eKey = H(USN \parallel IMEI)$$

⑤ ④에서 생성한 암·복호용 비밀키(eKey)로 ①에서 생성한 개인키를 암호화한다. 암호화된 개인키(EuPri_Key)를 스마트폰에 PKCS#8 형식으로 변환하여 개인키 파일(signPri.key)로 저장한다.

$$EuPri\_Key = E_{eKey}(uPri\_Key)$$

⑥ PKI 인증시스템으로부터 수신한 사용자 인증서(uCert)를 스마트폰의 저장소에 인증서 파일(signCert.der)로 저장한다.

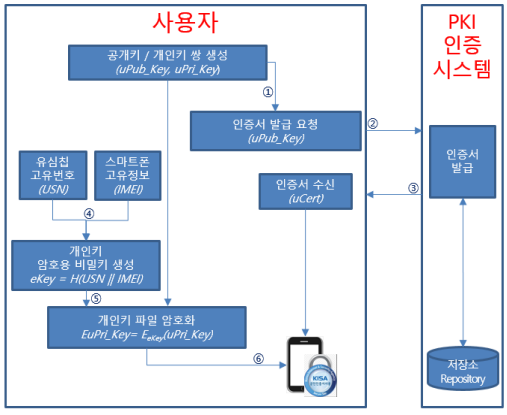


그림 2. 사용자 인증서 발급 및 개인키 저장 절차

## 2. 패스워드 리스 방식의 사용자 개인키 및 인증서 사용 절차

이 절에서는 사용자가 패스워드를 입력하지 않고, 스마트폰에 저장된 개인키 및 인증서 파일을 사용하는 절차를 설명한다.

① 스마트폰에 저장된 사용자 인증서(uCert)를 읽어온다.

② ①에서 읽어온 사용자 인증서에 대한 유효성 검증을 PKI 인증시스템에 요청한다.

③ PKI 인증시스템은 사용자 인증서의 유효성을 검증 결과를 사용자에게 전송한다.

④ 사용자 인증서가 유효한 경우에만 인증서 파일(uCert)로 부터 공개키(uPub_Key)를 추출한다.

⑤ USIM에서 USIM 고유번호(USN)와 스마트폰의 IMEI를 조회하여 개인키를 암·복호용 비밀키(eKey)를 생성한다.

$$eKey = H(USN \parallel IMEI)$$

⑥ 스마트폰의 저장소에 저장된 개인키를 ⑤에서 생성한 개인키 암·복호용 비밀키로 복호화 후 개인키(uPri_Key)를 추출한다.

$$uPri\_Key = D_{eKey}(EuPri\_Key)$$

⑦ ④와 ⑥에서 추출한 공개키와 개인키를 이용하여 어플리케이션에서 사용하면 된다.

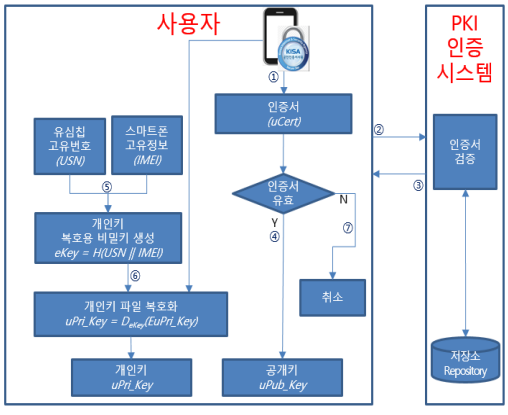


그림 3. 사용자 개인키 및 인증서 사용 절차

### 3. 스마트폰 변경 절차

사용자가 스마트폰을 교체하는 경우 USB 메모리를 이용하여 사용자의 인증서/개인키 파일을 새로운 스마트폰으로 이동하는 절차를 설명한다. 세부 절차는 다음과 같다.

① '3.2 패스워드 리스 방식의 사용자 개인키 및 인증서 사용 절차'에 따라 기존 스마트폰에서 개인키(uPri_Key)와 인증서(uCert)를 불러온다.
② USB 메모리의 정보(Container ID)를 불러온다.
③ USB 메모리 정보를 이용하여 개인키 암·복호용 비밀키를 생성한다.

$$eKey1 = H(Container\ ID)$$

④ ③에서 생성된 개인키 암·복호용 비밀키로 ①에서 불러온 개인키(uPri_Key)를 암호화하고, 스마트폰에 PKCS#8 형식으로 변환하여 인증서 파일(signCert.der)과 개인키 파일(signPri.key)을 USB 메모리에 저장한다.

$$EuPri\_Key = E_{eKey1}(uPri\_Key)$$

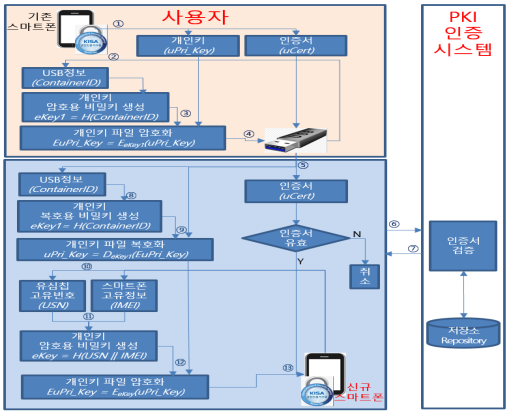


**그림 4. 스마트폰 변경 절차**

⑤ USB 메모리에서 인증서를 불러온다.
⑥ PKI 인증시스템에 사용자 인증서의 유효성을 검증 요청한다.
⑦ 사용자 인증서의 유효 여부에 따라 스마트폰 변경 절차를 취소하거나, 신규 스마트폰의 저장소에 사용자 인증서를 저장 후 아래 세부 수행절차를 수행한다.
⑧ USB 메모리의 정보(Container ID)를 불러와 개인키 복호용 비밀키를 생성한다.

$$eKey1 = H(Container\ ID)$$

⑨ USB에 암호화되어 저장된 개인키 파일(signPri.key)에서 개인키를 복호화 하여 개인키(uPri_Key)를 추출한다.

$$uPri\_Key = D_{eKey1}(uPri\_Key)$$

⑩ USIM에서 USIM 고유번호(USN)와 스마트폰의 IMEI정보를 조회한다.
⑪ ⑩에서 불러온 USIM 고유번호(USN)와 스마트폰 고유정보(IMEI)를 조합하여 개인키 암호용 비밀키(eKey)를 생성한다.

$$eKey = H(USN \parallel IMEI)$$

⑫ ⑪에서 생성한 개인키 암호용 비밀키로 ⑨에서 복호한 개인키를 암호화 하여 스마트폰에 PKCS#8 형식으로 저장된 개인키 파일(signPri.key)로 저장한다.

$$EuPri\_Key = E_{eKey}(uPri\_Key)$$

지금까지 제안 방안의 사용자 인증서 발급 및 개인키 저장 절차, 패스워드 리스 방식의 사용자 개인키 및 인증서 사용 절차, USB 메모리를 이용한 스마트폰 변경 절차를 설명하였다. 다음 장에서는 제안 방안의 안전성을 기존 인증방법과 비교 분석하였다.

## Ⅳ. 고찰 및 검증

본 장에서는 제안 방안의 안전성을 평가하기 위해 기존의 USB 저장 방안, OTP 기반 또는 USB 메모리 정보를 이용한 개인키 관리 방안과 제안 방안을 비교 평가하였다.

첫째, 제안 방안은 스마트폰을 개인키 및 인증서를 저장하는 저장매체로 활용하지만 다른 방안은 일반 USB 메모리 또는 OTP 전용장치를 사용한다. 둘째, 사용자 패스워드를 필수적인 인증요소로 활용하고 있으나, 제안 방안은 사용자 패스워드를 사용하지 않고 USIM 고유번호와 스마트폰 기기정보를 인증정보로 활용한다. 사용자로부터 패스워드를 입력받을 필요가 없음으로 인해 복잡한 패스워드 조합규칙을 강제하거나 주기적인 패스워드의 변경이 필요 없게 되었다. 셋째, 기존USB 저장 방식은 USB 플래시 드라이브에 저장된 개인키/인증서 파일을 임의로 다른 USB 플래시 드라이브에 이동/복사하여 재사용이 가능하다. 그러나 OTP방식/USB 메모리 정보를 이용한 방안 및 제안방안은 저장 매체의 정보를 인증요소로 사용하여 이동/복사를 하지 못하도록 차단하였다. 넷째, 기존 방안들은 공격자가 사용자의 패스워드를 찾아내면 언제든지 정당한 사용자로 위장이 가능하다. 그러나 제안 방안은 패스워드를 사용하지 않고, USIM 고유번호와 스마트폰의 고유정보를 조합하여 사용함으로써 공격자가 USIM 고유번호와 스마트폰의 IMEI를 동시에 알 수 없으므로 암호화된 개인키 파일을 안전하게 보호할 수 있다. 따라서 제안 방안은 패스워드를 사용하는 시스템에 비해 훨씬 높은 수준의 보안강도를 제공한다. 마지막으로, 제안방안은 지정된 스마트폰 이외의 다른 저장매체를 사용하는 경우에는 개인키 패스워드 사용 또는 다른 방안과 조합 등의 추가적인 백업/복구 방안이 마련되어야 한다.

표 4. 인증방식 비교

| | 기존 USB 저장 | OTP 방안[5] | USB ContainerID 방안[6] | 제안 방안 |
|---|---|---|---|---|
| 저장 매체 | 일반 USB 메모리 | 전용 OTP장치 | 일반 USB 메모리 | 스마트폰 |
| 인증 요소 | 개인키 패스워드 | 개인키 패스워드 + OTP장치정보 | 개인키 패스워드 + USB정보 | USIM 고유번호 + IMEI |
| 이동/복사 방지 | X | O | O | O |
| 개인키 패스워드 필요성 | O | O | O | X |
| 개인키 패스워드 노출에 따른 취약성 | O | O | O | X |
| 백업/복구 난이도 | 하 | 중 | 중 | 상 |
| 보안강도 | 하 | 중 | 중 | 상 |

## Ⅴ. 결론

공인인증서 무용론이 제기됨에도 불구하고 많은 사용자가 인터넷 뱅킹, 인터넷 쇼핑, 주식거래 등에서 공인인증서를 이용한다. 대부분의 사용자가 이동식디스크나 스마트폰에 저장하며, 특히 스마트폰의 사용률이 크게 증가하였다. 하지만, 이러한 저장매체들은 악성코드에 의해 사용자 패스워드와 공인인증서 관련 파일이 쉽게 탈취될 수 있다.

이에 본 논문에서는 USIM정보와 IMEI를 이용해서 사용자 패스워드가 필요 없으면서 공인인증서 관련 파일을 안전하게 보호할 수 있는 방안을 제안하였다. 이를 통해 공격자에게 개인키 및 인증서 파일이 탈취되더라도 공격자가 공인인증서를 사용할 수 없고, 영문자/숫자/특수문자 등 조합규칙을 따르는 복잡한 패스워드를 사용하지 않아도 된다.

따라서 제안 방안을 공인인증시스템에서 활용한다면 복잡한 사용자 패스워드를 기억하거나 주기적인 변경할 필요 없이 사용자가 소유한 스마트폰만 가지고 안전한 보안 서비스를 이용할 수 있다. 하지만 제안방안을 직접 구현하여 효율성을 검증하지 못했다는 한계가 있다. 향후에는 제안방안을 구현 후 인증 소요시간에 대한 성능측정을 통한 효율성 및 사용편이성에 대한 검증과 스마트폰 분실에 따른 백업·복구 방안에 대한 연구가 필요하다.

## 참 고 문 헌


[1] 미래창조과학부, “연도별 공인인증서 발급현황,” 2016(8).

[2] 한국인터넷진흥원, “15년도 대국민 전자서명 이용실태 조사,” 2015(12).

[3] http://www.boannews.com/media/view.asp?idx=37950&kind=3&search=title&find=%BD%BA%B8%B6%C6%AE%C6%F9+%B0%F8%C0%CE%C0%CE%C1%F5%BC%AD, 2013.10.08

[4] http://www.boannews.com/media/view.asp?idx=35172&kind=3&search=title&find=%BD%BA%B8%B6%C6%AE%C6%F9+%B0%F8%C0%CE%C0%CE%C1%F5%BC%AD, 2013.03.13.

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

[6] 김선주, 조인준, “USB 메모리의 컨테이너ID를 이용한 PKI 기반의 개인키 파일 안전한 관리방안,” 한국콘텐츠학회논문지, 제15권, 제10호, pp.607-615, 2015.

[7] 박영진, 김선종, 이동훈, “인증서와 개인키 유출방지를 위한 보안키 저장소,” 정보보호학회 논문지, 제24권, 제1호, pp.31-40, 2014.

[8] https://ko.wikipedia.org/

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

[10] http://www.zdnet.co.kr/column/column_view.asp?artice_id=20100401115240&type=det&re=

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

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

[13] 나준채, “차세대 USIM 기술,” TTA Journal No.116 pp.80-85.

[14] 인선준, “SIM, UIM과 USIM,” TTA Journal No.83 pp.89-101.

[15] https://namu.wiki/w/IMEI


## 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 수석연구원

<관심분야> : SW 테스팅, 정보보호제품 평가, Common Criteria, CC