아이리포 지식창고

출제예감 - 01 공인인증서와 공인인증서 문제 대응방안

Certificate

양경주 정보관리기술사
(kjyang75@gmail.com)

PKI기반의 안전한 전자거래, 공인인증서

Concept	**(공인인증서 정의)** 안전한 전자거래를 위해 전자서명을 이용하여 거래자 신원확인, 전자문서 위변조 방지 등이 가능하도록 공인인증기관에서 발급한 사이버상의 인감증명서
KeyWord	**PKI, 전자서명, 비대칭/대칭 암호화, 해쉬 알고리즘, X.509**

공인인증서의 역사!

핀테크에 대한 관심이 대두되면서 인터넷 상에서 보다 편리한 이용을 위해 공인인증서가 폐지되어야 한다는 주장과 안전한 전자거래를 위해서는 공인인증서를 대체할 만한 기술이 아직 없다는 주장이 팽팽히 맞서고 있다.

또한 문재인 대통령의 대선 후보 시절 '공인인증서 폐지' 공약과 여러 매체를 통해 발표되는 '공인인증서 대체 기술 개발' 등은 공인인증서에 대한 관심과 논쟁을 뜨겁게 하고 있다.

한국에 공인인증서가 처음으로 도입된 것은 1999 년 7 월 시행된 '전자서명법'부터이다.

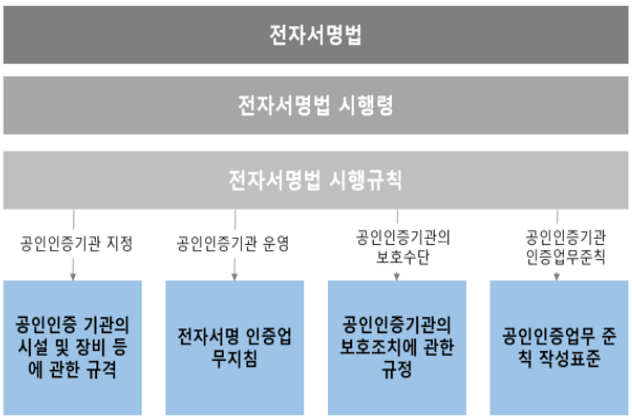
비대면 전자거래의 확산에 따라 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위해 등장한 것이 '전자서명'이며 공인전자서명이 있는 인증서가 바로 공인인증서이다. 즉, 정부는 전자상거래 당사자의 신원을 확인하고 전자문서의 위·변조 및 부인 방지**를 위해 공인인증기관이 발급하는 인증서에 기초한 전자서명에 대해 '공인전자서명'의 지위를 부여**하고 그 법적 효력을 인정하였다.

이후 '전자서명법'은 국제적 기류를 반영하여 UNCITRAL(유엔 국제 상거래법 위원회, UN Commission on International Trade Law)가 채택한 '전자서명 모델법'을 기반으로 2002 년 '전자서명법'을 개정하고 2003 년 은행의 인터넷 뱅킹이 시작되면서 전자금융거래에서 공인인증서 사용이 의무화된다.(단, 의무화 법제화는 2007 년 '전자금융거래법' 부터임)

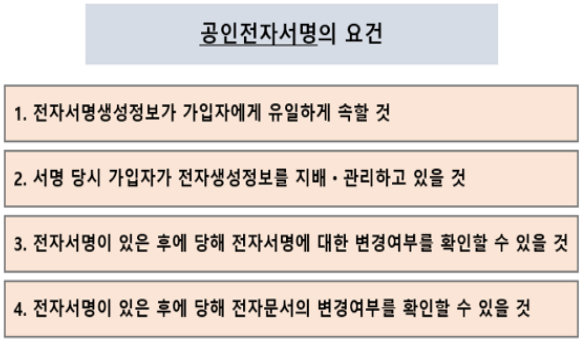
(참고. 1999 년 '전자서명법' 최초 제정 당시에는 PKI 를 근간으로 법체계를 구축했지만, UNCITRAL 의 '전자서명 모델법'의 **기술 중립성을** 수용하여 개정한 이후로는 공인인증서의 근간을 PKI 로 봐서는 안 된다. 법에서는 PKI 에 대한 직접 서술은 없으나 PKI 의 보안 우수성으로 공인인증서에서는 PKI 를 계속 사용하고 있다.)

여러 차례의 '전자서명법' 개정과 더불어 초기 증권거래, 금융거래 분야에서 주로 사용하던 공인인증서는 인터넷 주택청약, 전자민원, 연말정산 등 모든 전자거래에 사용이 확대되었다. 그러다 2014 년 **'천송이 코드' 논란으로 인해 인터넷 결제 시 공인인증서에 대한 의무화가 폐지되게 된다.**

공인인증서 폐지 찬반논란에 많은 전문가들은 공인인증서 구현 방식의 문제(Active-X, UI/UX 등)를 공인인증서 자체의 문제점으로 확대하지 말아야 한다고 피력하며 **아직까지는 인터넷 상에서 당사자 양방의 ①신원을 확인하고 송수신한 ②정보가 도중에 위·변조되는 것을 방지하고 거래 당사자의 ③거래사실 자체를 부인하는 것을 방지할 수 있는 기술로 PKI 기반의 공인인증서 만한 기술이 없다**라고 이야기 하고 있다.



[전자서명법 구조]



[공인인증서에 기초한 전자서명]

* KISA자료 재구성

Ⅰ. PKI 기반의 안전한 전자거래, 공인인증서의 개요

가. 공인인증서(Certificate)의 정의

- 안전한 전자거래를 위해 전자서명을 이용하여 거래자 신원확인, 전자문서 위변조 방지 등이 가능하도록 공인인증기관에서 발급한 사이버 상의 인감증명서

- 전자거래를 안심하고 거래할 수 있도록 공인인증기관이 특정인에게 유일하게 속한다는 사실을 확인하고 이를 증명하여 발급하는 인증서

나. 공인인증서에 포함되어야 하는 내용 (전자서명법 기반)

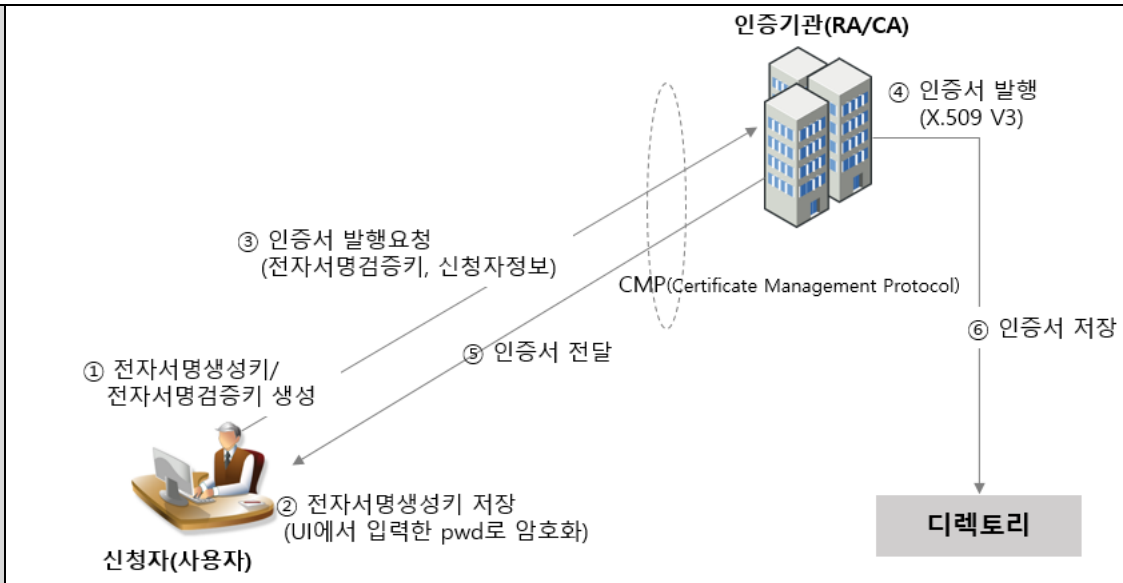
1. 가입자의 이름(법인의 경우에는 명칭을 말한다)
2. 가입자의 전자서명 검증정보
3. 가입자와 공인인증기관이 이용하는 전자서명 방식
4. 공인인증서의 일련번호
5. 공인인증서의 유효기간
6. 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보
7. 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항
8. 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격 등의 표시를 요청한 경우 이에 관한 사항
9. 공인인증서임을 나타내는 표시

- 국내 공인인증서의 경우 상호인증을 위하여 ITU-T에서 제정한 X.509 v3 규격을 이용하여 위 정보들을 저장하고 있다.

Ⅱ. 공인인증서 발급 및 거래 절차

- 공인인증서의 근간이 되는 PKI와 전자서명에 대한 상세설명은 본 내용에서 생략한다.

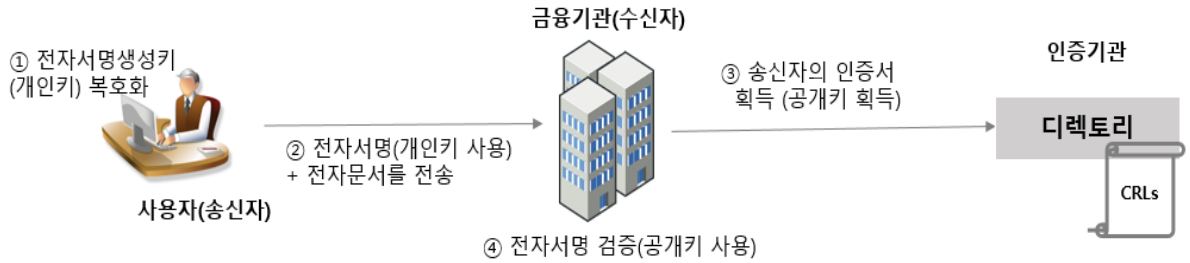
가. 공인인증서 발급 절차

<table>
<tr><td>발급
절차도</td><td colspan="3"> 
</td></tr>
<tr><td rowspan="7">발급
절차</td><td>0</td><td>대면을 통한 본인 확인</td><td>- 등록기관(RA) 방문을 통한 본인 확인</td></tr>
<tr><td>1</td><td>전자서명 생성키,
전자서명 검증키 생성</td><td>- 웹 브라우저를 통해 신청자의 전자서명을 위한 전자서명 생성키(개인키)와 전자서명 검증키(공개키)가 생성됨
- 키 길이는 안전성을 고려하여 2,048bit이상으로 생성</td></tr>
<tr><td>2</td><td>전자서명 생성키 저장</td><td>- 생성된 전자서명 생성키(개인키)는 USB, 스마트카드 등 저장매체에 저장됨
- UI에서 입력한 비밀번호로 전자서명 생성키를 암호화하여 NPKI 폴더 내의 SignPri.key 파일로 저장
(윈도우 비스타 이상부터 %UserProfile%₩AppData₩LocalLow₩NPKI₩ 에 저장)</td></tr>
<tr><td>3</td><td>인증서 발행요청</td><td>- 전자서명 검증키(공개키)와 사용자 정보를 포함하여 인증서 발행 요청을 함</td></tr>
<tr><td>4</td><td>인증서 발행</td><td>- 인증기관은 신청자의 정보를 확인하고 인증기관(CA)의 개인키로 사용자의 인증서를 발행
- 인증서 내에 신청자의 전자서명 검증키(공개키) 저장
- X.509 V3 규격에 맞춰 인증서 생성</td></tr>
<tr><td>5</td><td>인증서 전달</td><td>- 인증기관으로 발행받은 인증서를 신청자의 저장매체에 저장 (NPKI 폴더 내의 signCert.der)</td></tr>
<tr><td>6</td><td>인증서 저장</td><td>- 디렉토리에 인증서 정보를 저장하여 추후 공인인증서 검증 시 사용함</td></tr>
</table>

- 공인인증서는 국제표준인 **PKI 기술을 기반으로 발급되며** 발급된 인증서는 **NPKI(혹은 GPKI)라는 전용폴더에** 파일형태로 저장된다.
- 국내의 경우 등록기관(RA)는 금융기관이, CA 는 한국정보인증, 코스콤, 금융결제원 등이, Root CA 로 한국인터넷진흥원(KISA)이 그 역할을 담당하고 있다.
- 전자서명 생성키(개인키)에 대한 암호화 및 구문 정의 시 PKCS#5, PKCS#8 사용한다.

* PKCS(Public Key Cryptography Standard) : RSA 사에서 주관하고 있는 공개키 암호를 위한 표준

나. 공인인증서를 이용한 거래 절차

<table>
<tr><td>거래
절차도</td><td colspan="3"> 
</td></tr>
<tr><td rowspan="4">거래
절차</td><td>1</td><td>전자서명 생성키 복호화</td><td>- 저장매체에 암호화되어 있는 전자서명 생성키(개인키)를 UI에 입력한 비밀번호로 복호화</td></tr>
<tr><td>2</td><td>전자서명 + 전자문서
전송</td><td>- (전자서명)전자문서를 해쉬 알고리즘을 이용하여 해쉬값 생성, 이를 전자서명 생성키(개인키)를 이용하여 암호화
- 전자서명 시 PKCS #7 사용
- SHA256이상, RSA 2048이상
- 생성된 전자서명과 전자문서를 전송</td></tr>
<tr><td>3</td><td>송신자의 인증서 획득</td><td>- 인증기관을 통해 송신자의 인증서 정보를 획득
- 인증서 내의 전자서명 검증키(공개키)를 획득</td></tr>
<tr><td>4</td><td>전자서명 검증</td><td>- 전자서명 검증키(공개키)를 이용하여 전자서명을 복호화하고 전자문서의 해쉬 값과 비교하여 인증서 유효성 확인
- 인증서의 유효기간, 사용용도 등 검사 및 CRL 확인</td></tr>
</table>

- 공인인증서는 **본인 신분확인** 뿐만 아니라 **전자서명 기술을 활용하여 정보의 무결성**(위·변조 방지) 및 **거래에 대한 부인방지** 기능을 제공한다.

Ⅲ. 공인인증서의 문제점과 대응방안

가. 공인인증서 문제점

공인인증서는 PKI 기반의 뛰어난 보안 안정성에도 불구하고 인증서를 전용폴더(NPKI, GPKI)에 저장함으로 야기되는 인증서 및 패스워드 유출 문제, Active-X 로 인한 사용의 불편성과 보안 취약점 등 여러 가지 문제점에 대한 의견들이 거론되고 있다.

구분	문제점	설명
기술적 측면	공인인증서 전용폴더에 저장	공인인증서 구현 기술 자체는 표준을 준수하고 있으나 인증서를 웹 브라우저 각자가 정하는 인증서 위치가 아닌 전용 폴더(NPKI, GPKI)에 파일 형태로 저장하고 있음 (국제표준에 공인인증서 저장위치에 대한 기준은 없으나 전용폴더 저장에 따른 부수적인 문제점 발생)
	Active-X	전용폴더에 저장된 공인인증서를 구동시키기 위한 프로그램을 ActiveX 형태로 개발(웹 플러그인 및 exe 제공으로 해결은 되었으나 근본적 해결은 아님)

		- OS(MS Window), 브라우저(IE) 종속성 발생 - Active X를 통한 구동프로그램 설치 시 악성프로그램 다운로드 가능
	공인인증서 유출	일반매체에 파일형태로 저장된 공인인증서는 Copy&Paste가 가능 - 공인인증서 유출 자체는 문제가 되지 않으나(인증서에 저장된 공개키는 원래 공개되는 개념임) - 개인키 복호화를 위한 **비밀번호** 유출 시 인증서와 같이 저장되어 있는 개인키 복호화를 통해 악용 가능
사용자 측면	공급자 입장의 구현	- 기술자체로는 보안성이 우수하나 사용자가 인증서 및 비밀번호 분실 시 위험에 쉽게 노출 - 많은 클릭과 입력 등 불편함 (단, 인증서 설치 시 함께 설치를 강요하는 보안 프로그램의 불편함은 엄밀히 말하면 공인인증서와는 별개로 볼 수 있음)
산업적 측면	민간시장 저해	- 현재의 인증체계는 공급자의 책임전가 수단 등으로 악용되어 금융기관과 전자상거래 업체의 보안 투자를 줄이는 요인 제공 (단, 책임전가 악용 부분은 인증서 폐지 찬성자와 반대자 간의 의견이 분분함) - 정부 주도의 공인인증서 개발은 새로운 인증기술의 발전을 저해하고 있음

※ *공인인증서에 대한 문제점은 공인인증서 폐지 찬성자와 반대자 간의 의견이 분분하며 위 내용은 문제점으로 많이 거론되고 있는 내용을 정리하였음*

나. 공인인증서 문제에 대한 대응방안

이미 인터넷을 이용한 전자거래는 일상에서 떼어 놓을 수 없다. 또한, 핀테크에 대한 세계적 관심과 비즈니스 모델의 구체화 등으로 좀 더 편하고 안전하게 전자거래를 이용하고자 하는 사용자의 요구는 더 커져가고 있다.

이러한 시대적 요구에 부응하기 위해 공인인증서 문제점을 개선하고자 정부는 지속적으로 노력하고 있다.

대응방안	설명
안전한 저장매체 사용	공인인증서 저장 시 PC나 USB가 아닌 Copy가 불가능한 보안매체 사용 권고 - **보안토큰(HSM)** : 일반 USB와 달리 암호 연산 기능을 가진 칩을 내장하고 있어 해킹 방지 등 보안성 우수 - **IC 칩** : IC칩 내 안전하게 공인인증서 저장, NFC 통신으로 스마트 폰과 연동 - **스마트폰 USIM** : 스마트폰의 USIM에 인증서 저장/발급, USIM밖으로 인증서가 나갈 수 없어 인증서 및 비밀번호 유출 방지 - **SE(Secure Element)** : 스마트폰 등 디바이스 내 독립적인 H/W 저장 공간으로 보안 영역에서 안전하게 공인인증서 저장·이용 가능
HTML5 기반 공인인증서	HTML5을 이용한 OS 및 브라우저 종속성 탈피, 플러그인 없이 공인인증서 구현 - **웹 크립토 API 활용** : KISA, ETRI를 비롯해 한국 모질라 재단 등이 참여한 워킹 그룹에서 만든 표준안으로 웹 브라우저 자체에서 전자서명 기능을 구현한 API임. API를 통해 키를 발급받은 후 웹 브라우저의 Key Store에 저장하여 NPKI등 전용 폴더 불필요 (웹 크립토 API를 활용한 웹 표준 공인인증서를 시중 은행에서 사용 중에 있음)
사용성 증대	- **사용자 UX 고려** : 사용자의 UX를 고려한 UI 개선 필요

	- FIDO 접목 : 패스워드 입력없이 사용 가능한 FIDO를 접목하여 **보안성 및 사용성** 확보
사용용도 제한	전자서명이 반드시 필요한 경우와 본인확인만 필요한 경우를 구별하여 반드시 전자서명이 필요한 경우에만 공인인증서 사용하도록 제한 필요

공인인증서의 시작이 '**전자거래의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위함**'임을 기억하고 끊임없이 변화하고 발전하는 기술과 비즈니스 모델에 맞도록 기존의 기술과 제도를 개선하고 보다 안전하고 다양한 인증기술의 개발이 필요하다.

"끝"

[참고문헌]
1) KISA-전자서명 인증관리체계 운용자과정[기본], KISA
2) 공인인증서와 active x의 보완 방법(2017.03),디지에코
3) http://www.rootca.or.kr, KISA 전자서명인증관리센터 홈페이지
4) 공인인증서 규제논란의 교훈과 향후 전자상거래 정책방향 제언(2015.03), KDI