PKI 기반의 공인인증서

홍국표 김정현 이동훈 최송화

건국대학교 컴퓨터응용과학부

PKI based Certificates

Kukpyo Hong, Junghyun Kim, Donghoon Lee, Songhwa Choi

Department of computer science

Konkuk university

요 약

정보통신 기술의 발달로 우리가 이용하는 많은 부분에서 전자문서를 이용한 전자거래가 사용되고 있다. 비대면 방식의 특성상 전자거래는 신원확인 문제가 존재한다. 본 논문에서는 이 문제에 대한 해결책인 PKI기반의 공인인증서의 개념과 구조, 활용방안 그리고 그에 따른 취약점을 살펴보고자 한다.

1. 서론

정보통신기술의 급속한 발달과 정보통신망 확산으로 인터넷 쇼핑, 뱅킹, 경매, 증권, 기업 간 전자상거래 등 온라인상에서의 전자문서를 이용한 전가거래가 증가하고 있다. 그러나 전자거래는 거래당사자와 대면거래가 아닌 온라인을 통한 거래라는 문제점을 앉고 있다. 비대면 거래에서의 문제점은 거래 상대방에 대한 신원확인 문제이다. 신분의 위조나 변조 여부 확인이 불가능하고 거래한 사실에 대한 부인방지 등의 곤란한 문제가 생긴다면 온라인 거래는 사실상 이루어지기 어렵다. 이를 해결하기 위해 인감과 동일한 효력이 있는 전자서명을 사용하여 전자문서를 송수신함으로써 온라인상의 전자거래를 안전하게 사용할 수 있게 된다.

PKI(Public Key Infrastructure)란 공개키 기반의 암호화 구조이다.

PKI기반의 인증서란 전자서명을 한 본인이 주장하는 자신의 정보에 대한 사실여부를 거래상대방이 확인할 수 있도록 제 3자가 전자적으로 발급하는 증명서이다. 다시 말하면 이는 공개키의 소유자라고 주장하는 사람이 실제 그 키의 소유자인지를 공인된 제 3자가 확인한 후 주는 인증서이다. 대체로 전자인증서에는 사용자의 이름이나 단체명, 주소, 인증기관의 서명 및 ID정보, 사용자의 공개키, 전자 ID의 유효기일, 인증서의 종류, 전자 ID의 인증서 번호 등이 포함된다. 인증기관은 신원증명이 된 자와 공개키 사이의 관련을 확인하면 전자 인증서를 발급한다. 인증기관은 인증서의 진정성(authenticity)[1]과 무결성(integrity)[2]을 확보하기 위하여 그 인증서에 디지털서명을 부가한다. 누구라도 인증기관의 공개키를 사용하여 인증기관의 디지털 서명을 확인함으로써 인증서의 진정성과 무결성을 확인할 수 있다.

본문에서는 공인인증서에 대한 자세한 사항을 소개한다.

1) 시스템의 의사표시가 누구에 의하여 이루어진 것인가를 확증할 수 있는 것을 진정성이라 한다.

2) 의사표시자의 의사가 애초에 발하여진 것과 동일한 내용으로 상대방에게 도달하였는지를 확증하는 무결성이라 한다.

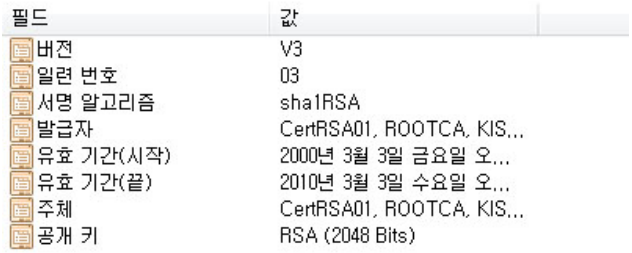
2. 인증서의 구조

공개키 인증서는 사용자의 이름이나 사용자와 연관된 어떤 특성을 사용자의 공개키와 연결하는데 사용된다. 본 장에서는 인증서의 구조에 대해 살펴보도록 하자. X.509 공개키 인증서는 세 가지 버전이 있다. 버전 2는 버전 1을 포함하며, 또한 버전 3은 버전 2를 포함한다. 공개키 인증서 버전 3은 확장옵션을 가지고 여러 가지 응용목적에 맞게 조정 하여 사용할 수 있다.

인증서는 3가지 섹션으로 구분되어 있다.

2.1 버전1 필드

버전1때부터 지금까지 사용되는 부분이다.



버전(Version) : 인증서의 버전, 즉 1이나 2, 또는 3을 나타낸다.

일련 번호(Serial Number) : 발급하는 인증기관이 인증서에 지정한 고유 일련번호이다. 인증서를 구별하기 위한 번호이다.

서명 알고리즘(Signature Algorithm) : 디지털 서명을 하기위해 사용되는 알고리즘을 식별하기 위한 항목이다. 예를 들어, RSA와 SHA-1로 표시되었다면 디지털 서명은 RSA를 사용해 암호화된 SHA-1 해시 값이다.

발급자(Issuer) : 인증서를 발행한 인증기관의 이름이다.

유효 기간(Validity) : 인증서의 효력이 유효한 기간을 나타낸다. 이 항목은 유효 기간의 시작과 종료 날짜/시간으로 구성된다.

주체(Subject) : 인증서가 발급된 대상을 나타낸다. 개인 또는 인증기관이 될 수 있다.

공개키(Public Key) : 인증서 소유자의 공개키를 보여주며 종류, 길이, 값을 나타낸다.

2.2 확장(Extension)

부정 이용 방지와 추가 정보의 기술에 이용된다.

주체 키 식별자(Subject Key Identifier) : 한 주체가 여러 키 쌍에 대해 발급받은 인증서를 가지고 있을 때, 인증서에 포함된 공개키를 구별하는데 사용한다.

기관 키 식별자(Authority Key Identifier) : 하나의 인증기관이 여러 개의 비밀키로 인증서를 발급한 경우, 서명 검증용 공개키를 식별하기 위해 사용한다.

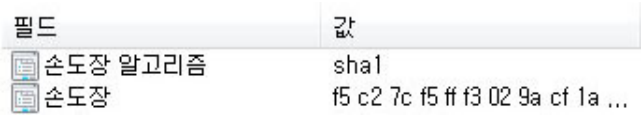
인증서 정책(Certificate policy) : 인증서 발급 정책, 인증서 사용 목적, 공표 방법 등 인증서와 관련된 일련의 규정을 의미한다.

주체/발급자 대체 이름(Subject/Issuer alternative name) : 인증서의 소유자를 나타내는 추가적인 명칭으로 이메일 및 IP 주소 등이 사용될 수 있다.

CRL 배포 지점(CRL Distribution point) : 폐기한 인증서의 목록이 저장되어있는 곳의 URL

키 사용(Key Usage) : 공개키가 어떤 용도로 쓰이고 있는지를 나타낸다.

2.3 속성



손도장(Digest) : 서명을 포함한 인증서 전체에 대한 해시 값이다.

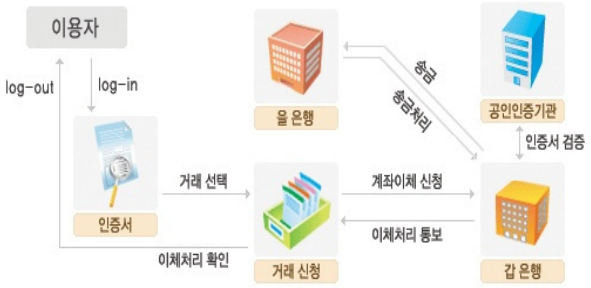
손도장 알고리즘(Digest Algorithm) : 손도장 값을 구하기 위해 사용되는 해시 알고리즘.

3. 인증서의 활용

이번 장에서는 공인인증서 활용방안에 대해 알아보도록 하겠다.

현재 공인인증서는 인터넷뱅킹, 사이버증권거래, 전자입찰조달, 전자세무처리, 전자민원 등의 각종

전자거래에서 "전자서명"을 인증해주는데 사용된다. 즉 법적효력을 가지고 전자거래의 신뢰성을 보장하는 수단으로 활용되고 있다.



[그림1] 인터넷뱅킹에서의 활용[3]

먼저 가장 많이 활용되고 있는 인터넷뱅킹의 경우, [그림1]처럼 공인인증서는 사용자의 확인절차를 통한 로그인과 거래승인 역할에 활용된다.

다음은 전자세금계산서 서비스에서의 공인인증서 활용이다.

[그림2] 전자세금계산서에서의 활용[4]

[그림2]처럼 세금계산서를 공급하는 공급자가 공인인증서를 기반으로 전자세무처리양식을 작성하여 송신을 하면 공인인증기관은 이를 검증 후 공급받는 자에게 송신하여 인증되는 방식으로 활용된다.

공인인증서를 이용한 전자 세무처리의 이런 활용은 기존의 우편발송이나 직접 전달하던 세금계산서를 전자 문서화하여 인터넷을 통해 빠르고 정확하게 전달하고 관리함으로써, 세금계산서 발행 및 전달 업무에 소요되는 시간과 비용이 대폭 절감되며 보관과 세무신고 업무도 편리하게 되었다.

현재는 인터넷뱅킹, 사이버증권거래, 카드결제, 전자세무처리, 전자민원과 같은 한정된 분야에서만 공인인증서가 쓰이고 있지만 앞으로는 인터넷을 매개로 하는 다양한 분야에서 개인 식별 수단으로 그 범위가 넓어질 것으로 예상되고 있다.

4. 인증서 관리상의 문제점

이번 장에서는 공인인증서 관리프로그램의 취약점을 알아보도록 하겠다. 현재로써는 공인인증서자체가 해킹을 당한 사례는 아직 나오고 있지 않다. 하지만 공인인증서를 관리하는 프로그램의 취약점이 발생하여 사용자의 주의를 요하고 있다. 대표적인 것이 우리나라에서 발생한 공인인증서의 관리 프로그램 문제점 중 'ActiveX 컨트롤'의 취약점이다. ActiveX 컨트롤은 웹 브라우저의 기본 기능에 각 사이트 별로 필요한 서비스 기능을 제공하기 위해 설치되는 프로그램이다. 예를 들면, 은행의 경우 공인인증서 로그인 기능을 제공해야 하는데 MS의 Internet Explorer에는 이런 기능이 없다. 따라서 은행은 공인인증 관리용 ActiveX 컨트롤을 만들어 사용자 PC에 설치하는 것이다. 자바 애플릿과 달리 ActiveX 컨트롤은 보안 수준을 각 컨트롤 별로 자체 관리하는데, 이로 인해 보안상 취약해지는 경우가 많다.

사용자 PC에 설치된 일반적인 프로그램을 공격자가 실행하고 입력 값을 조작하는 것은 공격자와 사용자 사이에 연결고리가 없기 때문에 매우 어렵다. 하지만, ActiveX 컨트롤은 HTML이라는 연결고리가 있어서 쉽게 실행할 수 있다. 공격자가 사용자에게 전자우편을 보내거나, 게시판에 글을 남겼을 때 사용자가 해당 페이지를 읽는 순간 실행된다.

다음과 같이 자바스크립트나 VB스크립트를 이용해서 ActiveX 컨트롤의 Method나 Property의 입력 값을 제어할 수 있다. 공격자의 주요 목표는 이들 Method나 Property를 조작해 사용자 PC의 로컬자원에 접근하는 것이다.

3) www.signkorea.com, 공인인증서비스 활용 참조
4) www.signkorea.com, 공인인증서비스 활용 참조

```
<script language="javascrip">
document.write('<OBJECT    ID+ Control1
CLASSID="CLSID:111111111-2222-3333-4
444-555555555555"');
document.write("heigh=0 width=0>");
document.write("</object>");
myval = Control1.Method1("argument");
</script>
```

공인인증서 관리용 프로그램 및 해킹방지 프로그램에서 발견된 취약점 유형은 다음과 같다.

1. 로컬자원에 접근할 수 있는 Method제공

가장 단순한 경우로 ActiveX 컨트롤이 readBinary와 같이 로컬자원에 접근할 수 있는 Method를 직접 제공하는 경우이다. 공격자는 다음과 같은 스크립트를 작성해 ActiveX를 실행하고, 사용자 PC의 파일을 읽을 수 있다.

```
<script language="javascript">
document.write("<OBJECT ID=Controller
CLASSID="CLSID:xxxxxxxx-xxxx-xxxx-
xxxxxxxxxxxx");
document.write(" height=0 width=0>");
document.write(</object>);
if(Controller!=null && typeof(Controller) !=
"undefined" && Controller.object != nell) {
myval                                    =
Controller.readBinary("c:₩₩boot.ini");
}
</script>
```

2. 업데이트 기능을 우회적으로 이용하는 경우

특정 ActiveX 컨트롤은 자동 업데이트 기능을 제공한다. 이때, 업데이트할 파일을 받아올 곳의 URL 등을 입력받는데 공격자는 이 값을 자신의 홈페이지 주소를 기록함으로써 우회적으로 파일쓰기가 가능하다. 컨트롤은 'UpdateURL'에 적힌 공격자 도메인에서 만든 파일을 가져와 사용자 PC에 설치할 것이며, 일단 설치가 끝나면 공격자는 사용자 PC에 대한 제어권을 얻게 된다.

```
<OBJECT classid='CLSID:xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxx' id='ctrl'>
<PARAM NAME="UpdateURL"
VALUE="http:₩₩attacker.com">
</OBJECT>
```

5. 결론

지금까지 우리는 PKI기반의 공인인증서의 전반적인 내용에 대해서 알아보았다. 현재까지의 공인인증서자체는 안전하다고 볼 수 있지만 인증서관리상의 문제점이 남아있기 때문에 사용자의 주의가 각별히 필요하다.

이러한 불안요소를 해결하고 수정하여 더욱 안전한 공인인증서를 만들게 되면 현재의 은행, 증권거래와 같은 몇몇 분야에서만 아니라 더 넓은 범위에서 이용증가를 기대해 볼 수 있다.

[참고문헌]

[1] 정보이론과 PKI, 전문석 외 6명, 도서출판 미래컴, 2003

[2] 보안을 위한 효율적인 방법 PKI, 컬리슬 아담스 외, 인포북, 2003

[3] PKI 전자서명과 인증제도, 정철현, 다산, 2003