공개키 기반 구조를 이용한 EC 사용자 인증 시스템에 관한 연구

정우필
박정선

요 약

Internet상의 전자문서, 전자거래 등과 관련된 전자업무에서는 다음과 같은 중요 인증 문제를 필요로 하게 한다. 첫째, 당사자(사용자)의 신분확인 기능(신원확인). 둘째, 전자업무 내용의 정보보호 및 무결성 기능(비밀성 보장). 셋째, 전자행위에 대한 부인봉쇄(분쟁해결) 등이 그것이다. 따라서 이러한 전자업무의 중요 인증 문제와 관련하여 신뢰할 만한 제 3 자, 즉 인증기관(CA : Certificate Authority)의 확인 및 증명해주는 제도가 필요하다. 위에서 언급한 제 가지 인증 문제 중 전자업무에서의 가장 기초적인 인증 문제인 당사자(사용자)의 신분확인 기능(신원확인)에 대한 문제를 연구하고자 한다.

1. 서론

사용자 인증 기술은 이제 Internet에서 정보보호 기술로서 널리 사용되고 있다. 예전까지 사용자 인증은 주로 ID와 패스워드를 사용한 것이었으나 이것은 정보 기술이 발전함에 따라서 보안상에 많은 문제점을 보이게 되었다. 앞으로는 암호 시스템을 이용한 사용자 인증 환경이 전자 상거래에서 안전한 사용자 인증 기술로서 사용될 것이다. 현재 사용하고 있는 암호 시스템은 대칭키 암호 시스템과 공개키 암호 시스템이다. 대칭키 암호 시스템을 이용 사용자 인증 체계는 다수의 사용자에 대해 각 사용자마다 키를 관리해야 되는 어려움이 있다. 그러한 키관리 어려움을 해결하기 위하여 인증기관(Certificate Authoriry : CA)을 이용한 사용자 인증체계는 공개키 암호화 알고리즘을 사용한 공개키 기반 구조(Publick Key infrastructure : PKI) 인증기관(CA)를 사용한다.

2. 인증 기반 기술

2.1 암호 시스템

암호 시스템(Cryptographic System)은 암호화되지 않은 상태의 원문(plain text)을 암호문(cipher text)으로 만드는 암호화(encryption)와 반대로 암호문을 원문으로 변화시

명지대학교 산업공학과

키는 복호화(decryption), 그리고 이 과정 속에 사용되는 암호화 키(key, cryptographic key)와 키의 관리 등 전자적 데이터의 보호를 위한 일련의 Process들을 일컫는 말이다. 이러한 암호 시스템은 전자적 데이터와 데이터 전송에 관한 정보의 비밀성을 제공할 수 있고, 다른 보안 응용 활용에서 중요한 역할을 담당한다. 암호 시스템이 그런 중요한 역할을 담당하기 위해선 다음 세 가지 요건을 충족시켜야 한다.

- 키에 의하여 암호화 및 복호화가 효과적으로 수행되어야 한다.
- 이용하기에 용이하여야 한다.
- 암호 시스템의 알고리즘 자체보다는 암호 키에 의한 보안이 이루어져야 한다.

암호 시스템에서 사용되는 암호화 알고리즘에는 두 가지가 있다.

- 암호화와 복호화 키가 같은 대칭키 암호 시스템
- 암호화 키를 안다고 해도 복호화 키를 알 수 없는 공개키 암호 시스템

2.2 전자 서명

전자서명(Digital Signature)이란 종래의 인감도장, 혹은 사인(Sign)처럼 개인의 고유성을 주장하고 인증받기 위해 전자적 문서에 서명하는 방법을 말한다. 서명을 사용하는 이유는 문서의 실질적인 내용에 대한 보장이 필요하기 때문인데, 물론 그 내용을 변경하였을 때도 서명이 필요하다.

전자 서명에 대한 조건 및 특징은 다음과 같다.

<표 1 전자 서명의 조건 및 특징>

조건	특징
· 서명은 서명되고 있는 메시지에 의존하는 형태이어야 한다. · 위조와 부인을 방지하기 위해 송신자에게 있어서 유일한 어떤 정보를 이용해야만 한다. · 서명을 만들기가 비교적 쉬어야 한다. · 서명을 인식하고 확인하기가 쉬어야 한다. · 전자 서명을 위조하는 것이 계산적으로 실행 불가능해야 한다. · 기억 장소에 전자 서명의 복사본을 유지하는 것이 실용적이어야 한다.	· 그 서명의 저자와 날짜와 시간을 확인할 수 있다. · 서명할 때의 내용을 인증할 수 있다. · 서명은 분쟁을 해결하기 위해서, 제삼자에 의해서 확인될 수 있다.

2.3 해쉬 함수

해쉬 함수는 임의의 긴 문자열을 고정된 길이의 값으로 바꾸는 함수이다. 이때 출력 값을 해쉬 값(Hash Value), 메시지 다이제스트(Message Digest) 또는 fingerprint라 부른다. 이런 메시지 다이제스트는 다음의 속성을 가져야 한다.

· 해쉬 출력 값을 이용해 원래의 입력 값을 추정하는 것은 계산상으로 불가능해야 한다.
· 입력 값과 해당 해쉬 출력 값이 있을 때 이 해쉬 출력 값에 해당하는 또 다른 입력 값을 구하는 것은 계산상으로 불가능해야 한다.
· 같은 해쉬 출력 값을 갖는 두 개의 다른 입력 값을 발견하는 것은 계산상 불가능해야 한다.

만일 임의의 길이를 가진 한 문서에서 만든 메시지 다이제스트가 있으면, 그것을 공개키로 암호화해서 서명으로 만들면 된다. 서명을 확인하려면 서명된 문서를 받은 쪽에서 동일한 해쉬 함수를 수행해서 나온 디지털 서명을 보낸 사람의 공개키를 사용해서 해독해 보면 된다. 해독한 데이터와 문서의 메시지 다이제스트가 일치하면 서명이 맞는 것이고, 일치하지 않으면 사기이거나 전송과정에서 깨진 것이다.

3. 공개키 기반 구조

3.1 공개키 기반 구조의 필요성

전자서명 기술은 공개키 암호 시스템으로 비밀키와 공개키가 사용된다. 또한 전자서명 기술의 안전한 사용은 서명키(공개키 암호화 알고리즘의 비밀키)와 검증키(공개키 암호화 알고리즘의 공개키)의 안전한 운영에 달려있으며 서명키의 안전한 운영은 비밀키의 안전한 보관을 말하며 검증키의 안전한 운영은 공개키의 안전한 관리를 의미한다. 공개키는 공개된 정보이므로 어떻게 공개키의 위/변조 문제를 해결하는가 하는 공개키 인증 문제로 귀착된다. 이러한 공개키 인증문제를 해결하기 위해 나온 것이 공개키 기반 구조(PKI : Public Key Infrastructure)이다. 다시 말해, 전자상거래의 안전성과 신뢰성을 확보하기 위해서는 전자인증제도가 요구되며 전자인증 제도는 바로 전자서명 기술의 안전한 운영을 의미하고 다시 전자서명 기술에 사용되는 공개키 암호화 알고리즘의 비밀키의 기밀성과 공개키의 무결성을 보장해야 하며 이를 해결하고자 하는 것이 공개키 기반 구조이다. 즉, 공개키 기반 구조는 전자인증제도를 실체화하는 것이다.

3.2 공개키 기반 구조의 정의

공개키 기반 구조는 정보시스템 보안, 전자상거래, 안전한 통신 등의 여러 응용분야에서 인증서(Certificate)의 사용을 용이하도록 하는 정책, 수단, 도구 등을 수립하고 제공하는 객체들의 네트워크이다.

공개키 기반 구조는 다음의 5가지 기본 보안 서비스를 제공한다.
- 프라이버시 : 정보의 기밀성을 유지한다.
- 접근제어 : 선택된 수신자만이 정보에 접근하도록 허락한다.
- 무결성 : 정보가 전송중에 변경되지 않았음을 보장한다.
- 인증 : 정보의 원천지를 보장한다.
- 부인봉쇄 : 정보가 송신자에게 전송되었음을 보장한다.

3.3 공개키 기반 구조의 구성

공개키 기반 구조를 구성하는 최소 객체들은 인증기관, 등록기관(RA : Registration Authority), 디렉토리, 사용자이다. 다음 표는 공개키 기반 구조의 구성과 그 역할에 대한 설명이다.

<표 2 공개키 기반 구조의 구조와 역할>

구조	역할
인증기관	인증기관은 공개키 기반 구조를 구성하는 핵심 객체로 그 역할 및 기능에 따라 계층적으로 구성되며 정책승인 기관(PAA: Policy Approving Authority), 정책인증기관(PCA: Policy Certification Authority), 인증기관(CA: Certification Authority) 등 세 가지 기관을 모두 통틀어 인증기관이라고 한다.
등록기관	인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자사이에 등록기관을 두어 인증기관대신 사용자들의 인증서 신청시 그들의 신분과 소속을 확인하는 기능을 수행한다.
디렉토리	인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서취소목록등을 저장 및 검색하는 장소로 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다.
사용자	PKI내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다

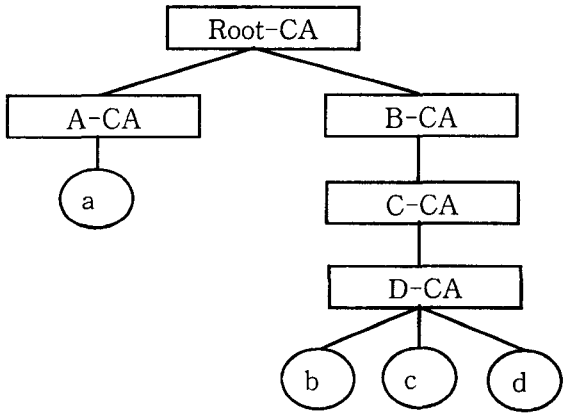
4. 인증기관(CA : Certificate Authority)

4.1 CA의 구조

인증 구조란 CA들 사이의 관계를 나타낸 것이다. 여러 가지 기술적, 경제적 이유로 인하여 세계에서 하나의 CA만이 존재한다는 것은 불가능하기 때문에 다수의 CA가 존재할 수밖에 없다. CA의 인증 구조에는 계층 구조와 네트워크 구조, 두 가지가 있다.

4.2 계층 구조

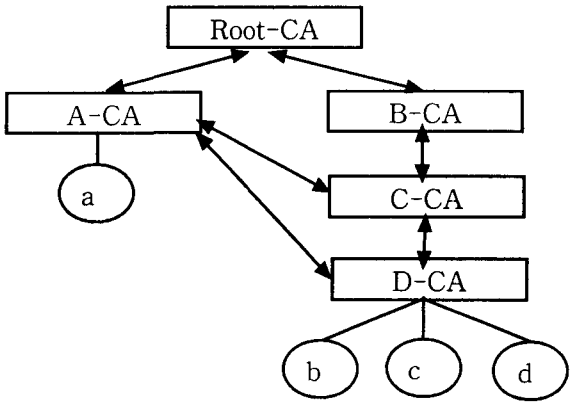
계층구조는 아래 그림과 같이 최상위의 루트 CA가 존재하고 그 아래에 하위의 CA가 계층적으로 존재하는 트리 형태로 상위 인증기관이 하위 인증기관에게 CA 인증서를 발행하며 하위인증기관은 상위 인증기관의 인증정책에 영향을 받는다.



<그림 1 계층구조>

4.3 네트워크 구조

네트워크 구조는 상위인증기관의 영향이 없이 인증기관 각각이 자신이 인증정책에 따라 독립적으로 존재하는 형태이다. 그리고 필요시에 CA간에 상호인증서를 발행하여 인증서비스를 한다. 다음 그림은 네트워크 구조를 나타내고 양방향의 화살표는 상호인증 관계를 나타낸다.



<그림 2 네트워크 구조>

4.3 각 인증구조의 장단점

계층적 인증구조와 네트워크 인증구조는 각각 서로 장.단점을 가지고 있다. 다음 표는 그 장.단점을 정리한 것이다.

실제 CA를 구축할 때에는 기본적으로 계층적 구조를 구성하면서 효율성과 다른 CA와의 통신을 위해 한 도메인내 또는 다른 도메인내의 CA 사이에 네트워크 구조를 허락한다.

5. CA의 관리 대상

5.1 X.509 인증서

인증서는 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 전자 서명하여 생성된다. 다시 말해 이것은 사용자의 공개키가 실제로 사용자의 것임을 증명한다. CA에서 인증서의 발행대상은 인증기관과 사용자, 서버 등으로 인증기관에게는 상위 인증기관이 인증기관의 적법성을 증명하기 위해 발행하고 사용자와 서버에게는 사용자의 신원, 서버 등의 적법성을 증명하기 위해 인증기관에서 발행한다. 인증서의 형식은 1988년 발표된 X.509 형식을 사용하며 현재까지 X.509 버전 3까지 공표되었다. X.509v3의 형식은 다음 그림과 같다.

<표 3 계층적 구성과 네트워크 구성의 장·단점>

인증구조	장점	단점
계층적	◎ 많은 조직의 관리 구조가 계층적이므로 자연스럽게 부합된다 ◎ 계층적 디렉토리 이름과 잘 부합된다. ◎ 인증 경로 탐색 전략이 간단하다. ◎ 도메인내의 모든 사용자는 루트의 공개키를 알고 있고 인증하고자 하는 사용자는 루트로부터 자신이 신뢰하는 인증기관까지의 인증 경로를 제공할 수 있으므로 인증서를 검증하고자 하는 다른 사용자는 루트의 공개키를 알고있으므로 그 경로를 검증할 수 있다	◎ 각 국가별 공개키 기반 구조가 구축될 경우 이것을 모두 통합하는 하나의 루트 CA가 존재한다는 것은 현실과 맞지 않다. ◎ 공개키 기반 구조가 상업적인 분야에 이용될 때는 관계는 계층적일 필요가 없다. ◎ 루트 비밀키의 노출은 끔찍한 상황을 야기하고 복구하기 위해서는 공개키 기반 구조내의 모든 사용자에게 새로운 공개키의 안전한 분배가 필요하다.
네트워크	◎ 유연성을 가지며 사업 기관의 상호 신뢰 관계를 잘 반영한다. ◎ 사용자는 자신의 인증서를 발행한 CA를 신뢰해야 하고 이것이 모든 신뢰 관계의 기본이 되는 것이 자연스럽다. ◎ 조직적으로는 멀리 떨어져 있지만 그 속의 사용자들이 높은 신뢰감으로 함께 일할 경우 CA들이 서로 직접적으로 상호 인증될 수 있다. ◎ 자신의 사용자들이 빈번히 통신하는 CA들의 직접적 상호인증을 허락함으로써 인증 경로 처리 부담을 감소한다.	◎ 인증 경로 탐색 전략이 계층적 구성에 비해 훨씬 복잡하다. ◎ 사용자는 공개키 기반 구조의 다른 사용자에게 단일 인증 경로를 제공할 수 없다. 왜냐하면 네트워크형에서의 두 사용자간의 인증경로는 여러개가 존재하기 때문이다.

version	X.509의 버전으로 0은 버전1, 1은 버전2, 2는 버전3를 의미함
serial number	발행자가 생성한 각각의 확인서에 대한 유일 식별자
signature algorithm id	발행자가 확인서를 서명하는 데에 사용한 알고리즘을 기입
issuer name	확인서를 서명하고 생성한 발행자의 ID로 X.500 명명 방식을 따름
validity period	확인서가 사용될 수 있는 시작 시간과 끝 시간을 기입하는 것으로 시간과 날짜로 표현됨
subject name	확인서를 받는 공개키의 소유주의 ID로 X.500 명명 방식을 따름
subject public key info	사용자의 공개키와 공개키에 대한 정보(알고리즘과 파라미터)를 기입
issuer unique identifier	(선택) 버전2이상에서 사용되는 것으로 발행자의 부가적인 정보를 포함함
subject unique identifier	(선택) 버전2이상에서 사용되는 것으로 객체의 부가적인 정보를 포함함
extensions	(선택) 인증 정책등 여러 가지 사항을 포함함
signature	앞의 목록들에 대한 서명값

<그림 4 X.509v3 인증서 형식>

5.2 X.509 인증서 취소목록 (CRL : Certificate Revocation List)

인증서는 인증기관에 의해 설정된 유효기간에 취소 될 수 있다. 그 이유는 다음과 같은 경우가 있다.

- 사용자가 가진 비밀 키의 노출
- 사용자의 무효화 요구
- 사용자의 가입 변경
- 사용자의 소멸
- 사용자의 잘못된 식별
- CA의 비밀키의 노출
- CA의 소멸

인증기관은 유효기간내에 효력이 상실된 인증서에 대해 CRL을 생성해서 디렉토리에 보관하며 상대편의 인증서가 의심이 갈 때 그 목록을 확인할 수 있다.
CRL 양식은 X.509v2CRL을 주로 사용하며 다음 표와 같은 형식을 따른다.

인증서는 인증된 공개키에 해당하는 비밀키가 노출된다든가 그 공개키의 소유자가 다른 도메인으로 옮기는 경우 등 여러 가지 이유로 유효기간이 만기되기 전에 그 효력이 상실될 수 있다. 인증기관은 이렇게 효력이 상실된 인증서들에 대한 목록을 생성해 공개키 기반 구조 내에서 관리한다.
인증서 취소목록은 X.509v2 형식을 따르는 추세로 다음 그림과 같다. CRL은 형식에서 볼 수 있듯이 주기적으로 생성된다. 이 주기는 인증 정책에 명시된다.

이름		설명	
signature	Algorithm Identifier	CRL을 서명할 알고리즘	
	Parameters	필요한 파라미터들	
Issuer		CRL 발행자 이름으로 X.500 명명 방식을 따름	
this date	UTCTime	갱신일에 대한 타임 스탬프	
next date	UTCTime	다음 갱신일	
revoked certificates		Serial number	취소된 인증서의 일련번호
		revocation date	인증서 취소일
		CRL entry extension(선택)	취소 이유 등 부가적인 정보를 기술함
CRL extenstion(선택)		부가적인 정보를 선택적으로 기술함	
Issuer's signature		발급자의 전자 서명	

<표 5 X.509v2 CRL 형식>

5.3 상호 인증서 쌍(cross-certification pair)

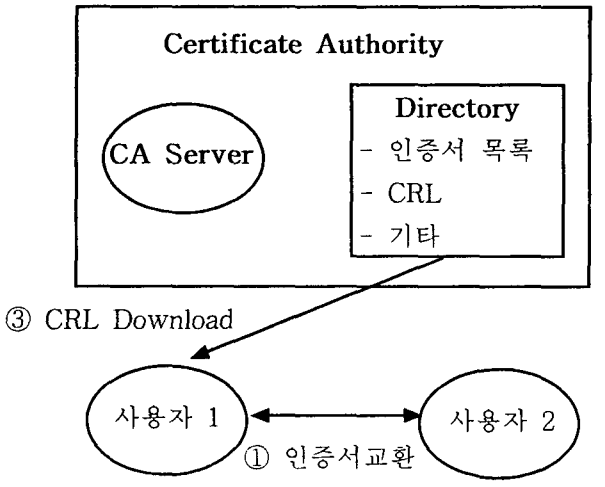
한 도메인이나 서로 다른 도메인의 인증기관들사이에 발행하는 인증서로 두가지 형태가 있다. 이것은 쌍을 이뤄 각 인증기관의 엔트리로 디렉토리에서 관리된다.

- 순방(forward) 인증서 : 인증기관에 대해 다른 인증기관에서 생성한 인증서
- 역방(reverse) 인증서 : 인증기관이 다른 인증기관에게 생성한 인증서

상호 인증서를 사용함으로써 같은 도메인내에서는 인증 경로를 단축할 수 있고 서로 다른 도메인내의 사용자들에게는 그들간의 안전한 통신 수단을 제공할 수 있다.

5.4 CA의 인증서 검증절차

인증서를 검증하기 위해서 다음 그림과 같이 송신자와 같은 CA에 소속되어 있는 경우에 수신자인 사용자 1은 송신자인 사용자 2가 소속된 CA 공개키를 이용하여 서명을 확인한다. 그리고 서명이 유효하면 다음으로 CA의 디렉토리에서 인증서 폐지목록을 다운로드 받아 폐지된 인증서가 존재하는지 여부를 확인하고 있으면 유효하지 않고 없으면 유효한 것이 된다. 그리고 사용자 2도 마찬가지 절차를 이용하여 인증서를 검증한다.



② CA 공개키를 이용하여 사용자 2의 인증서 서명 확인

④ 다운로드한 CRL에 사용자 2의 인증서와 같은 일련번호가 있는지 확인하고 있으면 무효한 것으로 판단하고 없으면 인증서는 유효함

<그림 3 인증서 검증절차>

사용자가 각각 다른 CA에 속한 경우는 CA 인증서를 통해 상대편 CA 공개키를 획득하며 점검을 한다.

계층구조일때는 인증사슬에서, 그리고 네트워크 구조일때는 상호인증서에서 상대편 CA 공개키를 획득한다. 인증사슬은 하나의 사용자 인증서와 인증경로를 구성하는 다수의 CA 인증서로 구성되며 상호인증서는 상호인증을 하고자 할 때 상대편 CA를 인증하기 위해 발행된 CA 인증서이다.

6. 결론 및 추후 연구 과제

급속하게 발전하고 있는 전자상거래의 환경을 고려할 때 서로 믿을 수 있는 전자상거래 제공자나 사용자의 확인이 절실히 필요한 때이다. 특히 전자서명법의 시행으로 인하여 앞으로 전자상거래에서 사용자 인증에 대한 관심은 더욱 고조 될것으로 생각된다. 본 논문에서는 그와 관련하여 안전한 전자상거래를 위한 여러 가지 기술 요소 가운데 가장 기초적인 문제인 사용자 인증과 그와 관련된 기반 기술에 대하여 살펴보았다. 이러한 사용자 인증 시스템은 그 자체 뿐만 아니라 다른 응용 프로그램 및 전자상거래 응용 시스템과 통합적인 사용이 중요하다. 따라서 사용자 인증 시스템 활용한 통한 전자 상거래 서비스 대한 연구가 진행되어야 할 것이며 인증 기술을 이용하여 사용자 인증 뿐만 아니라 사용자들이 주고 받는 전자적인 Data에 대한 인증도 추후 연구되어야 할 것이다.

참 고 문 헌

[1] 김철, "암호학의 이해", (주)영풍문고, 1996.12

[2] 홍승필 외 1, "정보보안 기술과 구현", 파워북, 1998.5

[3] 이덕형, "데이터보안과 공개키 기반구조(PKI)", 한국전자거래(CALS/EC)학회 proceeding, 1998.12

[4] 최진주 외 1, "전자상거래에서 인증서 검증절차 개선방안 연구", 한국전자거래(CALS/EC)학회 proceeding, 1998,12

[5] Vijay Ahuja, "Secure Commerce on the Internet", AP Professional, 1997

[6] CCITT X.500, The Directory:Overview of concepts, Models and Services, CCITT, 1992

[7] Mark Greene, Role of Certificate Authority in Internet Commerce, 1997.5

[8] The 1994 Mitre PKI Study Final Report, NIST, http://csrc.ncsl.nist.gov/pki/mitre.ps

[9] RFC 1487, X.500 Lightweight Directory Access Protocol, http://ds.internic.net/rfc/rfc1487.txt

[10] Micheal Rosing, "Implementing Elliptic Curve Cryptography", Maning, 1999