전자서명을 통한 인증기술과 공개키 기반구조에 대한 고찰

황재훈, 박춘석, 정연식, 송홍엽
연세대학교 공과대학 전기전자공학전공

Authentication by Digital Signature and Public-Key Infrastructure

Jae-Hoon Whang, Choon-Seok Park, Yeonsik-Jung, Hong-Yeop Song

Dept. of Electrical and Electronic Engineering, Yonsei University

요약

전자서명과 인증의 정의 및 필요성과 개략적인 기술적 요소 등을 정리하고, 정보보호시스템의 보안에 대한 신뢰도를 향상시킬 수 있는 방향을 제안한다. 공개키의 인증문제를 해결하기 위해 발전된 공개키 기반구조, 즉 PKI에 대해서 살펴봄으로써 인증에 대한 심층적 고찰을 수행한다.

1. 개요

오늘날 인터넷과 같은 새로운 정보통신 매체를 이용한 다양한 정보기술의 발전으로 정보통신시스템 사용자들은 많은 혜택을 누리는 동시에 시스템 구현상의 오류 또는 사용자 실수, 해커 등 예기치 못한 수많은 외부의 위협으로부터 자신의 중요한 정보를 안전하게 지키지 못해 중요정보의 누출, 파괴, 위, 변조로 인한 금전적 또는 정신적 피해를 입는 경우가 많다.

또한 정보통신 기술의 급속한 발달과 정보통신망 확산으로 종이문서가 전자 문서로 급군 지휘채널 상에서의 작전 명령 지시 및 실시간 정보 요구, 전자상거래, 전자자금 이체 등 전자문서를 이용하는 전자적 거래 행위가 증가 추세에 있다. 이러한 전자문서 이용으로 기업이나 정부의 생산성이 향상되고 군 작전이 신속 정확하게 수행되며 국민 개인의 생활편익이 증진되게 되었다.

그러나 전자문서를 이용한 정보전달은 비접촉, 비 대면으로 이루어지기 때문에 전달 당사자간에 상대방의 신원확인이 어렵고 타인으로 위장하여 전자문서 등을 부정하게 사용할 위험이 있다. 또한 전자문서는 유통되는 과정에서 위, 변조가 용이하고, 문서작성 사실을 입증하기 곤란하다.

이같이 전자문서 및 전자거래가 가지는 문제점을 해소하기 위하여 다음과 같은 방안이 있다. 정보전달 상대방의 신원을 확인하고 전자문서의 위, 변조 및 부인을 방지하기 위하여 전자서명 기술 활용하며, 신뢰할 수 있는 제 3자(인증기관)가 정보전달 당사자의 전자서명을 인증해 주는 전자서명 인증 제도를 도입하는 것이 그것이다. 또한 전송 내용의 비밀을 유지하기 위하여 암호를 사용하는 방안이 있다.

특히 공개키와 비밀키 쌍을 이용하는 공개키 암호 방식(Public Key Cryptosystem)은 향후 전자상거래의 성공을 위해서 필수 불가결한 요소로 인식되고 있다. 공개키 암호 방식을 이용할 경우, 본인의 공개키를 악용하는 것을 방지하기 위하여 그 공개키가 본인의 것임을 확인하는 인증(Certification) 기능이 필요하다.

따라서 본고에서는 전자서명과 인증의 정의 및 필요성과 개략적인 기술적 요소 등을 연구하는 것으로 정보보호시스템의 보안에 대한 신뢰도를 향상시킬 수 있는 방향을 찾아보도록 하겠다. 특히 공개키의 인증 문제를 해결하기 위해 발전된 공개키 기반구조, 즉 PKI에 대해서 살펴봄으로써 인증에 대한 심층적 고찰을 해보도록 하겠다.

2. 전자서명

2.1. 전자서명의 개념 및 필요성

2.1.1. 전자서명의 개념

일반적으로 전자서명은 크게 두 가지 의미로 나뉘어 진다. 첫 번째는「Electronic Signature」를 의미하는 것이며, 두 번째는「Digital Signature」를 말하는 것이다.

전자의 가장 일반적인 예는 전자펜을 이용한 그래픽 기반의 서명 방식이다. 전자서명된 문서를 수신한 수신자는 시각적으로 전자서명의 진위를 확인한 후 전자문서의 접수여부를 결정하게 된다.

후자는 공개키 암호기술에 기반을 두는 방식으로서 사용자는 자신만이 알고있는 전자서명생성키를 이용하여 수학적인 연산을 통하여 자신만의 고유한 전자서명 값을 계산한 후, 그 결과를 수신자에게 송신한다. 수신자는 송신자가 제공하는 전자서명검증키를 사용하여 전자서명 값의 진위 여부를 수학적인 연산으로 확인할 수 있으며, 올바른 결과 값이 나오는 경우에만 전자문서를 접수한다.

최근 선진 각국에서 시행 또는 제정 중에 있는 전자서명법은 일반적으로 후자의 개념을 법적으로 인정하고 있다.

2.1.2. 전자서명의 필요성

컴퓨터 네트워크를 통한 비 대면 방식의 전자적 거래는 기존 거래 방식에서 시간적 · 공간적 제약의 문제점을 해결해줌으로써 새로운 거래 문화로서 자리잡아 가고 있다. 이러한 전자적 거래는 많은 장점을 가지고 있음에도 불구하고, 보안 요구사항이 먼저 해결되어야만 전자적 거래의 활성화를 기대할 수 있을 것이다. 대표적인 보안 선결 요구사항은 다음과 같다.

가. 무결성(Integrity) : 메사지가 변조나 수정이 될 수 없게 하는 것을 말한다.

나. 비밀성(Confidentiality) : 적법한 수신자를 제외한 제3자는 볼 수 없도록 하는 기능을 말한다.

다. 부인방지(Non-repudiation) : 부인방지는 메시지를 송 · 수신하는 경우 해당자가 송 · 수신에 대한 행위를 부인 못하도록 하는 기능을 말한다.

전자서명은 상기의 보안 요구사항 중 인증, 무결성, 부인방지에 대한 보안 기능을 제공해 주며, 이것은 결국 비 대면 방식의 전자적 거래 환경 구축 시 전자서명 기술이 필요하다는 것을 의미한다.

2.1.3 전자서명의 요구사항

전자서명 알고리즘은 안전·신뢰성 보장을 위해 기본적인 요구사항을 만족해야만 한다. 전자서명 알고리즘은 전자서명검증키로부터 전자서명생성키가 계산되는 것이 실행 불가능해야 하며, 전자서명은 메시지 내용, 서명자의 전자서명생성키, 그리고 사용자 정보에 의존되어 생성되어야만 한다. 전자서명의 요구사항들은 다음과 같다.

가. 위조 불가(Unforgeable) : 합법적인 서명자만이 전자서명을 생성할 수 있어야 한다.

나. 서명자 인증(User authentication) : 서명자를 불특정 다수가 검증할 수 있어야 한다.

다. 부인 방지(Non-repudiation) : 서명자는 서명한 후에 서명한 사실을 부인할 수 없어야 한다.

라. 변경 불가(Unalterable) : 서명한 문서의 내용을 변경할 수 없어야 한다.

마. 재사용불가(Not reusable) : 전자서명을 다른 전자문서의 서명으로 사용할 수 없어야 한다.

2.2. 전자 서명 구현 방법

2.2.1. 대칭키 암호시스템을 이용한 전자서명

대칭키 암호시스템은 고속의 암호화 및 복호화가 가능하지만 암호화와 복호화에 사용되는 키가 동일하기 때문에 통신 대상간에 안전한 키의 공유가 필요하다는 단점이 있다. 대칭키 암호시스템을 이용한 전자서명은 다음과 같다.

우선 각 사용자는 동일한 대칭키 암호시스템을 사용하고, 모든 사용자들이 믿을 수 있는 중재자(arbitrator)가 존재한다. 사용자 A는 사전에 중재자와 비밀키 KA를 공유한다. 중재자는 B와 KB의 비밀키를 공유한다. 서명의 과정은 다음과 같다.

㉮ 사용자 A는 사용자 B에게 전송할 정보를 KA로 암호화하여 중재자에게 전송한다.

㉯ 중재자는 정보를 KA로 복호화한다.

㉰ 중재자는 복호화 한 정보와 자신이 그 정보를 사용자 A에게 받았다는 내용을 함께 KB로 암호화하여 사용자 B에게 전송한다.

㉱ 사용자 B는 수신한 내용을 KB로 복호화한다.

중재자는 각각의 사용자들과 비밀키를 하나씩 공유하여 모든 사용자들의 비밀키를 알고 있고, 모든 정보를 복호화하기 때문에 모든 사용자들이 믿을 수 있어야 한다. 중재자는 사용자 A만이 알고 있는 KA로 암호화된 문서를 수신하여 사용자 B만이 알고 있는 KB로 암호화하기 때문에 중재자의 인증으로 사용자 B는 송신자(A)의 인증이 가능하고, 암호화가 이루어졌기 때문에 서명의 위조나 재사용, 서명 후의 변경 등은 불가능하다. 중재자는 모든 사용자들이 믿는 존재이기 때문에 서명자가 서명 이후 자신의 서명을 부인할 수 없다. 그러므로 위의 방법은 전자서명의 요구사항을 만족한다. 하지만 중재자가 모든 서명 문서의 전송에 관여하여 암호화와 복호화를 수행하기 때문에 계산량이 너무 많고, 모든 사용자들이 믿을 수 있는 중재자를 실제 구현하는 것은 매우 어렵다. 따라서 대칭키를 이용하는 전자서명은 현실적으로 타당

성이 없다.

2.2.2. 공개키 암호시스템을 이용한 전자서명

공개키 암호 시스템은 두 개의 키는 하나를 공개하고 하나는 비밀로 간직한다. 또한 공개키를 공개해도 그 공개키에 대응하는 비밀키를 알아내는 것은 계산상 불가능하다. 공개키 암호 시스템을 이용한 전자서명을 아래과 같다.

사용자 A의 공개키를 PA, 비밀키를 SA로 표시하면, A가 B에게 전송할 경우 A는 메시지의 암호를 SA를 이용해서 하고, 이를 받은 B는 PA를 이용하여 메시지를 복호화한다.

사용자 A의 공개키 PA에 대응되는 유일한 비밀키 SA는 사용자 A만이 알고 있다는 가정이므로 이와 같은 방법은 전자서명의 요구사항을 모두 만족시킨다. 공개키 암호시스템을 이용한 전자서명은 대칭키 암호시스템을 이용한 전자서명에 비해 사용자의 비밀키를 공개키로 인증할 수 있으므로 중재자가 필요하지 않고 훨씬 간단하게 구성된다.

2.2.3. 해쉬 알고리즘을 이용한 전자서명

해쉬 알고리즘은 임의의 길이의 정보를 입력으로 하여 고정된 길이의 출력 값을 내는 것으로서 출력 값(해쉬 값)들이 난수적 특성을 갖는다. 전자서명에 사용되는 해쉬 알고리즘은 주어진 출력 값에 대하여 입력 값을 계산하기 어려워야 하고, 같은 출력 값을 갖는 입력 쌍을 찾기가 어려워야 한다. 해쉬 알고리즘을 이용한 전자서명은 다음과 같다.

㉮ 사용자 A는 전송할 정보를 해쉬알고리즘에 넣어 해쉬값 h를 얻는다.

㉯ A는 자신의 비밀키 SA를 이용, h에 전자서명을 하여 전자서명 값을 구한다.

㉰ A는 전송할 정보 M과 함께 계산된 전자서명 값을 전송한다.

㉱ 사용자 B는 받은 전자서명 값을 PA로 복호하고, 이 값을 M을 해쉬 알고리즘에 넣어 얻은 해쉬값과 비교하여 같으면 옳은 서명이라고 판정한다.

해쉬 알고리즘을 이용한 전자서명은 공개키 암호시스템을 이용한 전자서명보다 더 복잡해 보이지만 해쉬 알고리즘의 계산 효율이 좋고, 전자서명 값을 계산할 때 전체 정보에 대한 계산이 아닌 상대적으로 작은 해쉬값 h에 대한 계산을 하기 때문에 전체적인 계산 속도는 공개키 암호시스템을 이용한 전자서명보다 월등히 앞선다.

2.3. 전자 서명의 응용

2.3.1. 신분인증

신분인증을 위한 전자서명은 서명자가 자신의 비밀키를 가지고 있는지의 여부를 확인자가 서명자의 공개키를 이용하여 증명하는 것이다. 신분인증 방식은 정보의 해쉬값 h를 사용하는 대신 신분을 확인하는 확인자가 임의의 난수를 선택하면, 그 난수에 대하여 올바른 전자서명을 생성하는지의 여부를 확인한다.

사용자 B가 사용자 A에게 신분인증을 요구할 경우 신분인증은 다음과 같이 이루어진다.

㉮ B는 사전에 약속된 크기의 임의의 난수 r을 생성하여 r 값을 직접 알 수 없도록 계산하여 R을 생성하여 이를 A에게 전송한다.

㉯ A는 비밀키 SA를 이용하여 R에 대한 전자서명 값을 계산하고 이를 B에게 전송한다.

㉰ B는 전송받은 서명 값과 자신이 선택한 R, 사용자 A의 공개키 PA를 이용하여 서명

이 옳은지 검증한다.

신분인증 프로토콜의 경우 다른 사용자의 신분 인증 과정의 정보를 도용하여 재사용할 경우가 있으므로 서명의 생성 과정에 현재 시간 정보를 이용하여 재사용을 방지하고 있다.

2.3.2. 부인 방지 서명

어떠한 서명에 대해서 서명 후에 자신의 서명이 아니라고 부인할 경우 이것의 진위여부를 가릴 필요가 있게 된다. 이를 위해 제안된 부인 방지 서명은 서명에 대한 부인을 막는 것으로 서명자의 도움 없이는 서명의 검증을 수행할 수 없다.

예를 들어 소프트웨어 공급회사나 각종 제조업체들이 자사의 제품을 보증하는 전자서명을 발행할 경우 서명자의 도움이 있어야만 발행된 서명을 확인할 수 있게 하여, 그 회사의 제품을 직접 구매한 고객만이 해당 업체와의 대화를 통해 자신이 구입한 제품이 진품임을 확인할 수 있게 하고, 구입한 제품에 하자가 있을 경우라도 판매회사가 이를 부인할 수 없게 하여 서명자의 서명이 남용되는 것을 막을 수 있고, 발행된 서명의 안전성에 대한 위협도 방지할 수 있다.

2.3.3. 다중 서명

일반적인 전자서명은 한 사용자가 어떤 정보에 대하여 전자적으로 서명한다. 그러나 일반적인 실무 환경에서는 어떤 하나의 정보에 대하여 여러 사람의 서명이 필요한 경우가 대부분이다. 이럴 경우 각각의 사용자가 동일한 정보에 대하여 일반적인 전자서명을 생성할 수도 있으나, 이는 서명의 크기가 서명자의 수에 따라 증가하며 확인 과정의 계산량이 많기 때문에 정보에 덧붙여지는 서명의 크기는 동일하게 유지하면서 여러 사용자의 서명을 확인할 수 있는 방법들이 개발되었다. (n, k) 서명 방식은 다중 서명의 응용으로써 n명 중 k명의 서명이 있는 경우 서명의 유효성을 인정한다.

2.3.4. 제한 서명

기존의 전자서명에서 비밀키를 가지고 있는 사용자는 서명을 무한히 많이 생성할 수 있다. 그러나 제한 서명은 서명을 생성할 수 있는 능력을 k회로 제한한다. 따라서 서명자는 k개의 서명을 생성하기 위하여 k개의 비밀키를 사용한다. 각각의 비밀키는 한번의 서명만을 만들고, 사용된 후에는 공개되어 더 이상 사용할 수 없도록 한다.

제한 서명을 이용할 경우 매번 다른 비밀키를 사용하여 신분 확인을 받게 되며, 사용 횟수 또한 제한을 받게 된다. 제한 서명은 서명을 한번만 사용할 수 있으므로 비밀 정보를 대리인에게 주어 대리인으로 하여금 서명을 하게 할 수도 있다.

2.3.5 은닉 서명

은닉 서명은 정보의 내용을 상대방에게 알려주지 않으면서 서명을 얻는 것으로 전자화폐나 거래 내용을 은닉해야 하는 곳에 활용할 수 있으며, 추적 불가능성 및 개인의 프라이버시를 제공할 수 있다. 은닉 서명의 기본적인 요구사항은 서명하는 정보의 내용은 서명자에게 노출되지 않아야 하고, 서명과 서명 대상 정보가 노출된 이후라도 그 정보와 서명을 받은 사람과의 관계가 추적 불가능해야 한다. 또한 은닉 서명은 서명을 받고자 메시지를 제공하는 제공자의 신원과 메시지를 서명자가 연결시킬 수 없도록 하는 익명성을 보장한다.

2.3.6. 기타 특수 서명

· Group Signature - 신분을 노출하지 않고 그룹 소속원임을 입증하는 방식

· Nominative Signature - 지정된 수신자만이 검증할 수 있는 방식

· Fail-Stop Signature - 강력한 공격자에 의한 서명의 위조를 서명자가 증명가능

· One-time Signature - 단일메세지에 대해서만 서명하는 방식

2.4. 전자서명 알고리즘

2.4.1. RSA 알고리즘

RSA 전자서명은 Rivest, Shamir, Adleman이 1978년 제안한 것으로 RSA 공개키 암호 시스템을 이용한 전자서명 방식이다.

가. 키생성

· 소수 p, q(p와 q의 크기는 거의 동일해야 한다.)를 선택하고, $\lambda(n) = lcm(p-1, q-1)$을 구한다(여기서 $n=p*q$, lcm은 최소공배수).

· $\lambda(n)$과 서로소인 수 e를 선택한다.

· $d \equiv e^{-1}(\bmod \lambda(n))$를 계산한다.

* n과 d는 공개키(전자서명 검증키) , d, p, q는 비밀키(전자서명 생성키)가 된다.

나. 서명

이제 내가 평문 m을 서명해서 보낸다고 하자.

· 서명은 $s \equiv h(m)^d(\bmod n)$이 된다.

다. 서명검증

m과 s를 같이 전송하면, 받은 사람은 서명의 검증은 다음과 같이 한다.

· m을 가지고 $h(m)$ 계산, s를 이용 $s^e(\bmod n)$를 계산하여, $h(m) \equiv s^e(\bmod n)$일 경우에 유효한 서명으로 간주한다.

RSA 서명 방식은 공개된 n에서 p나 q를 찾는 소인수 분해 문제가 어렵다는 안전성 근거를 가지고 있다. 현재까지 알려진 소인수분해 알고리즘 중 가장 빠른 것은

number field sieve이고, 이것은 $O(e^{(1.923+o(1))(\ln n)^{1/3}(\ln \ln n)^{3/2}})$의 시간이 걸린다.

이 방식은 현재 가장 널리 사용되고 있는데, IBM, Microsoft, Digital, Apple, General Electric, Unisys 등 유수의 기업들이 사용하고 있다.

2.4.2. DSS(Digital Signature Standard)

DSS는 NIST(National Institution of Standard and Technology)가 1991년 8월에 정부용 전자서명 알고리즘으로 DSA(Digital Signature Algorithm)를 발표한 후, 이를 미국내 전자서명 표준안으로 제안한 전자서명 알고리즘이다. DSS방식의 안전성은 이산대수 문제의 어려움에 근거한다.

가. 키생성

· 소수 p, q ($q \mid p-1$)를 선택. p는 $0 \le t \le 8$에 대해서 $2^{511+64t} < p < 2^{512+64t}$사이의 값이다.

· 이 소수의 승법군 Z_p^*에서 위수가 q가 되도록 g를 정한다. 여기서 $2^{159} < q < 2^{160}$이다. 여기서 $g \equiv h^{(p-1)/q}(\bmod p)$이고 h는 $1<h<p-1$인 정수로 $h^{(p-1)/q}(\bmod p) > 1$을 만족한다.

· 비밀키 x를 $0<x<q$ 결정한다(즉 , $x \in Z_q$).

· $y \equiv g^x(\bmod p)$를 계산

* 공개키는 p, q, g, y. 비밀키는 x가 된다.

나. 서명

· 우선 난수 k를 $0 < k < q$ 에서 결정한다.

· $r \equiv g^k(\bmod p)(\bmod q)$와

$s \equiv k^{-1}(h(m)+x*r) \pmod q$를 계산

· 이 (r, s)가 서명이 된다

다. 서명검증

이 r과 s를 메시지 m과 함께 보내면,

· $u_1 \equiv h(m)*s^{-1} \pmod q$와

$u_2 \equiv r*s^{-1} \pmod q$를 계산

· $u \equiv (g^{u_1} r^{u_2} \pmod p) \pmod q$가 받은 r과 같으면 서명이 유효한 것으로 간주한다.

2.4.3. KCDSA 알고리즘

KCDSA(Korea Certification-based DSA)는 우리나라의 주요 암호학자들이 주축이 되어 1996년 에 개발하였으며, 이후 지속적인 수정 작업을 거쳐 1998년 10월 TTA에서 단체 표준으로 제정되었다.

가. 키생성

· 소수 p, q를 선택한다(단, $q|p-1$이다). 여기서 $|p| = 512+256i \quad i=0,1,\ldots,6$

$|q| = 128+32j, \quad j=0,1,\ldots 4$이다.

· 위수가 q인 Z_p의 원소 g를 선택한다.

· $x \in Z_q^*$인 x를 선택하고, $y \equiv g^{1/x} \pmod p$를 계산한다. 여기서 $1/x \equiv x^{-1} \pmod q$이다.

· $z = h(CertData)$. CertData는 최소한 서명자의 식별자와 공개키 y와 p,q,g를 포함해야 한다.

* 공개키는 y, p, q, g 비밀키는 x가 된다.

나. 서명

· $k \in Z_q^*$를 임의로 선택하고,

$w \equiv g^k \pmod p$를 계산, $r = h(w)$를 구한다.

· $e \equiv r \oplus h(z \| m) \pmod q$를 계산($\oplus$는 비트의 XOR 연산임)하고, $s \equiv x(k-e) \pmod q$를 구한다.

· $\{r||s\}$가 서명이 된다.

다. 서명검증

$\{m||r||s\}$를 받으면 다음과 같이 검증한다.

· 인증서에서 CertData를 빼내

$z = h(CertData)$를 계산하고, $0 < r < 2^{|q|}$, $0 < s < q$임을 확인한다.

· $e \equiv r \oplus h(z \| m) \pmod q$와

$w \equiv y^s g^e \pmod p$를 계산하여 $r = h(w)$ 일때만 서명이 유효하다고 간주한다.

2.4.4. ElGamal 전자서명 방식(1985년 제안)

가. 키생성

· 소수 p를 선택, Z_p^*에서의 원시근 g를 구한다.

· 비밀키 x를 1 ~ (p-1)사이의 값에서 결정).

· $y \equiv g^x \pmod p$를 계산

* y, g, p는 공개키, x는 비밀키가 된다.

나. 서명

· 우선 난수 $k \in Z_{p-1}^*$를 결정한다.

· $r \equiv g^k \pmod p$와

$s \equiv k^{-1}(h(m)-x*r) \pmod{p-1}$를계산

· 이 (r, s)가 서명이 된다.

다. 서명검증

· 받은 사람은 m을 가지고 $h(m)$을 구하고, $y^r r^s$를 구해서, $g^{h(m)} \equiv y^r r^s \pmod p$이면 서명을 유효한 것으로 간주한다.

2.4.5. Schnorr 전자서명 방식(1989년 제안)

가. 키생성

· 소수 p,q를 선택하고, Z_p^*에서의 위수가 q가 되는 g를 구한다.

· $x \in Z_p$를 정해 $v \equiv g^{-x} \pmod p$를 계산한다.

* v, g, p, q는 공개키, x는 비밀키가 된다.

나. 서명

· 우선 난수 k를 $0 < k < q$ 에서 결정한다.

· $s \equiv g^k \pmod p$와 $e = h(s, m)$를 계산.

· $y \equiv k + xe \pmod q$를 계산

· 이 (s, y)가 서명이 된다.

다. 서명검증

· $e = h(s, m)$를 계산.

· $s \equiv g^y v^e \pmod p$이면 서명은 유효하다..

2.4.6. ESIGN 전자서명 방식(1991년)

- 후지오까, 오까모도, 미야구찌가 제안

가. 키생성

· 보내는 이는 소수 p,q를 선택($p>q$, p와 q의 크기는 거의 같음)하고, $n = p^2 q$를 계산한다.

· 정수 k(k>3)의 값을 정한다.

* k,n은 공개키, p,q는 비밀키가 된다.

나. 서명

· $x \in Z^*_{pq}$인 x를 선택. 즉 $0 \le x \le pq - 1$.

· $w = \lceil \frac{h(m) - (x^k (\bmod n))}{pq} \rceil$를 계산,

$y \equiv \frac{w}{(kx^{k-1})} (\bmod p)$를 구한다.

· $s = x + y * pq$가 서명이 된다.

다. 서명검증

· $u \equiv s^k (\bmod n)$, $z = h(m)$를 계산한다.

· $z \le u \le z + 2^{\lceil \frac{2}{3}|n| \rceil}$ 이면 서명은 유효하다.

2.4.7. Fiat-Shamir 전자서명 방식(1987년)

가. 키생성

· 소수 p, q 를 선택. $n=pq$를 계산한다.

· 양의 정수 k를 선택하고 서로 다른 임의의 정수들 $s_1, s_2, \ldots, s_k \in Z^*_n$을 선택한다.

· $v_j \equiv s_j^{-2} (\bmod n)$, 와 $y \equiv g^x (\bmod p)$를 계산

공개키는 k-tuple $(v_1, v_2, \ldots, v_k)$와 n, 비밀키는 k-tuple $(s_1, s_2, \ldots, s_k)$, p, q.

나. 서명

· 난수 r를 $1 \le r \le n-1$ 에서 결정한다.

· $u \equiv r^2 (\bmod n)$을 계산한다.

· $e = (e_1, e_2, \ldots, e_k) = h(m \| u)$를 계산한다. 여기서 $e_i \in \{0,1\}$

· $s \equiv r \cdot \prod_{j=1}^{k} s_j^{e_j} (\bmod n)$를 계산한다.

이 (e, s)가 메시지에 대한 서명이 된다.

다. 서명검증

· 공개키 $h(m \| s^2 \cdot \prod_{i=1}^{k} v_i^{e_i} (\bmod n))$을 v_i를 가지고 계산하여 이 값이 e와 같으면 서명이 유효한 것으로 간주한다.

2.4.8. 여러 전자서명 방식 비교

서명	안정성 근거	단점	장점	비고
RSA	소인수분해문제	법승산횟수가 많다. 전처리가 불가능	가장 많이 사용, 안정성이 널리 검토됨	
ElGamal	이산대수문제	서명크기가 크고, 난수의 기밀성 필요	전처리 가능	
DSS	이산대수문제	검증의 연산수가 많고 난수의 기밀성 필요	전처리 가능	NIST에서 표준으로 제안
Schnorr	소인수분해문제	검증의 연산수가 많고 난수의 기밀성 필요	전처리 가능, 서명크기 작음	
ESIGN	소인수분해문제		전처리 가능, 서명생성, 검증시간 우수	일본에서 표준화 추진
KCDSA	이산대수문제	난수의 기밀성 필요	전처리 가능, 서명크기 작음	국내 표준안으로 제안

[표 1] 전자서명 방식 비교

3. 공개키 기반구조(PKI)

3.1. 인증(Certification)의 정의 및 기능

인증이라 함은 어떤 사실을 증명하거나 확인하기 위해 사용되는 기능으로, 최근 자주 언급되고 있는 인증은 일반적으로 크게 두가지 의미로 나뉘어 사용되고 있다. 첫번째는 사용자 인증이나 메시지 인증을 의미하는 [인증(Authentication)] 이고, 두 번째는 공개

키 암호방식에서 공개키의 무결성의 보장을 의미하는 [인증(Certification)] 이다. 물론 일각에서는 Certification을 보증이라고 정의하여 Authentication과 구별을 하기도 하지만 일반적으로 혼용되고 있는 상태이다. 그러나 여기서 언급하고자하는 인증서비스는 Certification을 의미하는 것이며, 이것은 Authentication과는 구분된다.

인증서비스의 필요성은 공개키 암호 알고리즘의 사용에서부터 비롯된다. 현재 전자거래의 안전성을 정량화 시킬 수 있는 방법으로 공개키 암호 방식의 전자서명 기술이 가장 우수하다고 알려져 있으며, 이것의 실제 적용을 위해서는 인증 서비스가 필요하게 된다. 인증기관은 전자서명을 이용하고 자 하는 사용자들에 의해 인증서 발급 서비스를 제공해 줌으로써 이윤을 창출하거나, 기업내 안전한 정보 통신망 구축을 담당하는 하나의 조직을 일컫는 것이며, 인증 서비스란 인증기관이 제공해주는 인증서 발급, 인증서 관리 등 일련의 서비스를 통칭하는 것이라고 말할 수 있다.

전자상거래에 적용되는 인증 기능은 일반적으로 다음과 같이 구분할 수 있다.

가. 사용자 인증: 상대방의 본인성을 확인하는 기능

나. 내용 인증(전자 공증): 거래 내용, 일시 등을 확인하는 기능

다. 신용 인증: 거래 상대의 신용 능력을 확인하는 기능

3.2. 용어 설명

본 장에서는 우선 PKI에 관련되는 용어를 정리하도록 한다.

가. 인증기관(CA: Certification Authority)

인증 정책에 따라 인증서를 생성하거나 취소하는 객체(entity)로 모든 인증기관들은 자신의 키쌍을 생성하고 선택적으로 사용자의 키를 생성할 수 있다.

나. 인증서(certificate)

인증 기관의 비밀키로 암호화되어 위조할 수 없는 사용자의 유일한 이름, 사용자의 공개키 및 기타 정보로 이루어진 문서로 인증서를 발행한 CA의 인증 정책도 포함한다. X<<Y>>는 인증 기관 X가 사용자 또는 하위 인증 기관 Y에게 발행한 인증서를 의미한다.

다. 인증정책(certification policy)

인증정책은 CA가 작동하는 메커니즘과 사용되는 암호 알고리즘과 서명 알고리즘, 최소 키 크기, 인증서 유효의 최대 길이, 인증서 취소 목록 갱신의 최대 기간, 인증서를 발행하기 위해 사용자의 신분을 확인하는 메커니즘등을 기술한다. 정책은 객체 식별자(OID: Object Identifier)로 명명되고 정책의 OID는 그 정책하에 발행된 모든 인증서내(extension 영역)에 포함된다.

라. 보안 정책(security policy)

보안 서비스 및 기능의 제공을 관리하는 보안 기관에 의한 규칙들이다.

마. 도메인(domain)

공통적인 보안 정책을 구현하거나 밀접하게 관련있는 명명공간(namespace)내에 사용자들에 대해 인증서를 발행해주는 CA들이 논리적으로 그룹화되어 있는 것을 도메인이라 한다.

바. 고유 이름(Distinguished Name)

PKI내의 객체들을 유일하게 구별하는 이름으로 보통 X.500 명명 방식을 따른다.

사. 상호인증서(cross-certificate)

한 CA가 다른 CA를 신뢰하여 그 CA에 인증서를 발행할 때 그 인증서를 상호인증서라 한다. 한 CA를 신뢰하는 모든 객체는 그 CA가 상호 인증한 CA에 의해서 발행된 모든 인증서를 신뢰한다.

아. 인증 경로(certification path)

경로상의 최종 객체에 대한 공개키를 얻기 위한 인증서들의 정렬된 순서로 A→B는 A로부터 B로의 인증 경로를 나타낸다. A→B는 A의 인증서로 시작되어 B의 인증서로 끝나는 고리의 형태인 CAA<<A>> CAB<<B>>로 구성된다.

자. 디렉토리(directory)

객체에 대한 정보 저장소로 사용자들로 하여금 그 정보에 접근할 수 있는 서비스를 제공한다.

차. 신뢰(trust)

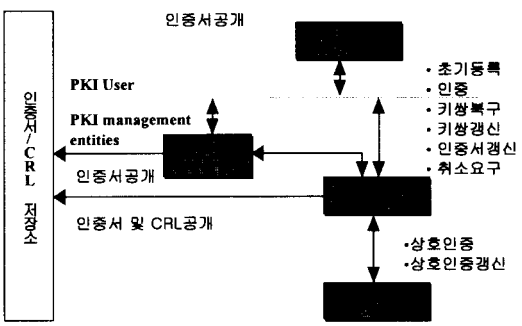
일반적으로 한 실체는 다른 실체가 자신의 기대한 바와 같이 행동을 하리라고 가정할 수 있을 때 실체는 다른 실체를 신뢰한다고 말할 수 있다. 이러한 신뢰는 일부 특정 기능에만 적용될 수 있다. 인증 프레임워크에서 이 신뢰의 주요 역할은 인증하려는 실체와 인증 기관간의 관계를 기술하는 것으로 인증하려는 실체는 인증 기관이 유효하고 신뢰할만한 인증서를 생성한다고 확신할 수 있어야 한다.

3.3. 공개키 기반구조(PKI)의 당위성

공개키 암호기술은 보안이 필요한 응용 분야에 널리 사용된다. 공개키 암호 기술에서는 비밀키와 공개키를 이용한다. 비밀키는 그 소유자만이 알고 있고 공개키는 공개된다. 공개키를 공개하는 문제는 비밀키를 소유자만이 알도록 하는 것보다 얼핏 보기에 매우 단순한 것 같지만 실제 구현시 공개키를 공개하는 데에 사용되는 메커니즘(공개키 디렉토리, 게시판 등)이 자체적으로 안전하지 않아 누구나 쉽게 접근하여 정보를 변경할 수 있으므로 공개키의 위·변조 문제를 야기시킨다.

이렇게 공개된 공개키가 위·변조되지 않았음을 보장하는 문제 즉, 공개키의 무결성을 보장하기 위해 등장한 것이 공개키 기반구조(PKI:Public Key Infrastructure)이다. 공개키 기반구조에서는 공개키를 공개하는 대신 공개키와 그 공개키의 소유자를 연결하여 주는 인증서(certificate)를 공개한다. 인증서는 신뢰할 수 있는 제 3자(인증기관)의 서명문이므로 신뢰 객체가 아닌 사람은 그 문서의 내용을 변경할 수 없도록 한다.

즉, Public Key Infrastructure(PKI)는 전자서명과 암호화 기술이 필요로 되는 전자적 거래를 안전하게 보장하는 솔루션으로 Key와 certificate의 관리를 통해 조직에게 신뢰성있는 네트워크 환경을 제공한다.



[그림 1] 공개키기반구조의 구성

여기서는 공개키 기반구조의 정의 및 응용분야와 함께 이를 구성하는 모델 적용 절차 등을 살펴보도록 한다.

3.3.1. PKI의 정의

공개키 기반구조에 대한 정의는 다음과 같이 여러 가지로 생각할 수 있다.

가. 사용자의 공개키를 인증해주는 인증기관들의 네트워크

나. 모르는 사람과의 비밀 통신을 가능하게 하는 암호학적 키와 인증서의 배달 시스템

다. 공개키의 인증서를 이용해 공개키들을 자동적으로 관리해주는 기반구조

라. 공개키 인증서를 발행하고 그에 대한 접근을 제공하는 인증서 관리 기반 구조

이를 통합하여 정리하면 정보시스템 보안, 전자 상거래, 안전한 통신등의 여러 응용분야에서 인증서(certificate)의 사용을 용이하도록 하는 정책, 수단, 도구등을 수립하고 제공하는 객체들의 네트워크이다.

3.3.2. PKI가 제공하는 서비스

PKI는 다음의 5가지 기본 보안 서비스를 제공한다.

가. 프라이버시 : 정보의 기밀성을 유지한다.

나. 접근 제어 : 선택된 수신자만이 정보에 접근하도록 허락한다.

다. 무결성 : 정보가 전송중에 변경되지 않았음을 보장한다.

라. 인증 : 정보의 원천지를 보장한다.

마. 부인 봉쇄 : 정보가 송신자에 의해 전송되었음을 보장한다.

3.4. PKI 모델

3.4.1. PKI 구성 요소

PKI를 구성하는 최소 객체들은 등록기관(RA:Registration Authority), 인증기관, 디렉토리, 사용자이다.

1) 인증기관

공개키 기반구조를 구성하는 가장 핵심 객체로 그 역할 및 기능에 따라 계층적으로 구성되며 여러 명칭으로 불리운다. 아래 세 기관 모두를 통틀어 인증기관이라 한다.

가. 정책승인기관(PAA: Policy Approving Authority)

PKI 전반에 사용되는 정책을 생성하고 PKI구축의 루트 CA로의 역할을 하며 다음을 수행한다.

- PKI 전반에 사용되는 정책과 절차를 생성하여 수립한다.

- 하위 기관들의 정책 준수 상태 및 적정성을 감사한다.

- PKI내 외에서의 상호 인증을 위한 정책을 수립하고 그를 승인한다.

- 하위 기관의 공개키를 인증하고 인증서, 인증서취소목록등을 관리한다.

나. 정책인증기관(PCA: Policy Certification Authority)

PAA 아래 계층으로 자신의 도메인내의 사용자와 인증기관(CA)이 따라야 할 정책을 수립하고 인증기관의 공개키를 인증하고 인증서, 인증서취소목록등을 관리한다.

다. 인증기관(CA: Certification Authority)

PCA 아래 계층으로 다음과 같은 기능을 수행한다.

- 사용자의 공개키 인증서를 발행하고 또

필요에 따라 취소한다.

- 사용자에게 자신의 공개키와 상위 기관의 공개키를 전달한다.

- 등록기관의 요청에 의해 인증서를 발행하고 되돌린다.

- 상호 인증서를 발행한다.

- 최소한의 정책 책임을 진다.

- 인증서와 그 소유자 정보를 관리하는 데이터베이스를 관리한다.

- 인증서, 인증서 취소목록, 감사 파일을 보관한다.

2) 등록기관(RA)

인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자사이에 등록기관을 두어 인증기관대신 사용자들의 인증서 신청시, 그들의 신분과 소속을 확인하는 기능을 수행한다. 사용자들의 신분을 확인한 후, 등록기관은 인증서 요청에 서명을 한 후 인증기관에게 제출한다. 인증기관은 등록기관의 서명을 확인한 후 사용자의 인증서를 발행한 후 등록기관에게 되돌리거나 사용자에게 직접 전달한다. RA는 조직 등록기관(ORA: Organizational Registration Authority)라고도 불리운다.

3) 디렉토리

인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서 취소 목록등을 저장 및 검색하는 장소로 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버(인증기관)는 DAP (Directory Access Protocol)나 LDAP(Lightweight DAP)를 이용하여 X.500 디렉토리 서비스를 제공한다. 인증서와 상호 인증서 쌍은 유효기간이 경과된 후에도 서명 검증의 응용을 위해 일정기간동안 디렉토리에 저장된다.

4) 사용자

PKI내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다. 다음의 기능을 수행한다.

- 자신의 비밀키/공개키 쌍을 생성할 수 있어야 한다.

- 공개키 인증서를 요청하고 획득할 수 있어야 한다.

- 전자 서명을 생성 및 검증할 수 있어야 한다.

- 특정 사용자에 대한 인증서를 획득하고 그 상태를 결정할 수 있어야 한다.

- 인증 경로를 해석할 수 있어야 한다.

- 디렉토리를 이용하여 자신의 인증서를 다른 사용자에게 제공할 수 있어야 한다.

- 인증서 취소 목록을 해석할 수 있어야 한다.

- 비밀키가 분실 또는 손상되거나 자신의 정보가 변했을 때(예: 조직의 탈퇴) 인증서 취소를 요청할 수 있어야 한다.

3.4.2. PKI의 관리 대상

PKI에서 관리해야 할 대상은 크게 인증서와 인증서 취소목록, 상호 인증서쌍이 있다.

1) 인증서

인증서는 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 전자서명하여 생성된다. 다시 말해 이것은 사용자의 공개키가 실제로 사용자의 것임을 증명한다. PKI에서 인증서의 발행대상은 인증기관과 사용자, 서버 등으로 인증기관에게는 상위 인증기관이 인증기관의 적법성을 증명하기 위해 발행하고 사용자와 서버에게는 사용

자의 신원, 서버 등의 적법성을 증명하기 위해 인증기관에서 발행한다. 인증서의 형식은 1988년에 ITU-T가 X.509 초기 버전을 공표하고 1993년에 버전 2를 공표했으며 1995년 이후로는 ISO/IEC 9594-8의 문서와 동일시되어 공동 개발되어왔다. 현재에는 X.509 버전 3까지 공표되었고 인증서의 extensions 영역에 대한 개정이 진행되고 있다. X.509v3의 형식은 [표 2]와 같다.

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 날짜(UTCT 형식)로 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

[표 2] X.509v3 인증서 형식

2) 상호인증서쌍(cross-certification pair)

한 도메인이나 서로 다른 도메인의 인증기관들사이에 발행하는 인증서로 두가지 형태가 있다. 이것은 쌍을 이뤄 각 인증기관(X)의 엔트리로 디렉토리에서 관리된다.

가. 순방(forward) 인증서 : 인증기관 X에 대해 다른 인증기관에서 생성한 인증서

나. 역방(reverse) 인증서 : 인증기관 X가 다른 인증기관에게 생성한 인증서

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

3) 인증서 취소 목록(CRL: Certificate Revocation List)

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 PKI내에서 관리한다. 인증서 취소목록은 X.509v2 형식을 따르는 추세로 아래 그림과 같다. CRL은 형식에서 볼 수 있듯이 주기적으로 생성된다. 이 주기는 인증 정책에 명시된다.

3.5. PKI 구성 형태

PKI에서 신뢰는 인증 경로를 통해 전달된다. 전자 서명을 검증할 때를 생각해 보자. 전자서명의 검증자는 자신이 신뢰하는 인증기관의 공개키만을 알고 있으므로 그 인증기관의 공개키를 이용하여 인증 경로를 검증함으로써 서명자의 공개키를 획득한다. 이렇게 획득한 공개키는 무결성이 보장된다. 검증자는 무결성이 보장된 공개키를 이용하여 서명을 검증할 수 있는 것이다. 이러한 신뢰가 인증 경로를 통해 어떻게 전달되는 지에 따라 PKI는 다음 두가지 형태로 구성될 수 있다.

이름		설명
signature	Algorithm identifier	CRL을 설명할 알고리즘
	parameter	필요한 파라미터들
issuer		CRL 발행자 이름으로 X.500 명명방식을 따름
this update	UTC time	갱신일에 대한 타임스탬프
next update	UTC time	다음 갱신일
revoked certificates		
CRL extension(선택)		부가적인 정보를 선택적으로 기술함
Issure's signature		

Serial number	취소된 인증서의 일련번호
revocation date	인증서 취소일
CRL entry extwnsion(선택)	취소이유등 부가적인 정보를 기술함

[표 3] X.509 v2 CRL 형식

1) 계층적 구성

인증기관들이 하위 CA에게 인증서를 발행하는 "루트" CA(PAA)아래에 계층적으로 배열되어 있는 구성으로 인증기관들은 자신의 아래 CA들에게 인증서들을 발행한다. 계층적으로 구성된 PKI에서 루트 CA의 공개키는 모든 사람에게 알려져 있어 사용자들의 인증서는 루트 CA로에서 자신이 신뢰하는 인증기관까지의 인증 경로를 검증함으로써 검증된다.

2) 네트워크 구성

인증기관이 각각의 도메인을 형성하여 독립적으로 존재하는 구성으로 CA들이 서로를 상호 인증하여 서로에게 인증서를 발행한다. 네트워크로 구성된 PKI의 사용자는 자신의 인증서를 발행한(즉, 자신이 신뢰하는) 인증기관의 공개키만를 알고 있다. 네트워크로 구성되었을 경우에는 인증 경로가 여러개 존재할 수 있으므로 이중 짧은 경로를 찾는 것이 중요 관건이다.

PKI의 두가지 구성은 서로 장·단점을 가지고 있다. 아래표는 그 장·단점을 비교한 것이다.

실제 PKI 구축시에는 기본적으로는 계층적 구조를

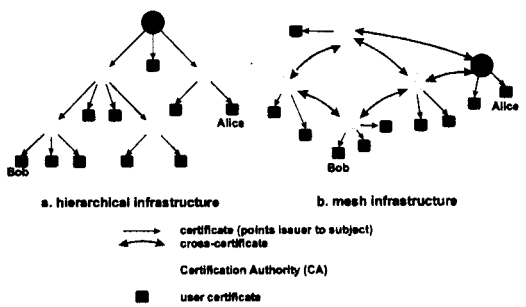
	장점	단점
계층적 구조 (Hierarchy)	• 정부와 같은 관리 조직에 적합함 • 인증 경로 탐색이 용이함 • 모든 사용자가 루트 CA의 공개키를 알고 있으므로 인증서 검토가 용이함	• 범세계적인 PKI를 위한 루트 CA의 존재는 비현실적임 • 루트 CA에 집중되는 오버헤드 문제 • 사업적 관계에는 부적절함 • 루트 CA의 비밀키 노출시 복구가 어려움
네트워크 구조 (Mesh)	• 유연하며 실질적인 사업 관계에 적합함 • 지리적으로는 멀지만 거래가 빈번한 사용자들의 CA간에 상호 인증이 직접 이루어지므로 인증 경로 처리절차가 단순함 • 루트 CA의 비밀키 노출시 그 피해가 국소적임	• 인증 경로 탐색이 복잡함 • 상호 인증서의 CRL 관리가 어려움

[표 4] PKI의 두 가지 구성 비교

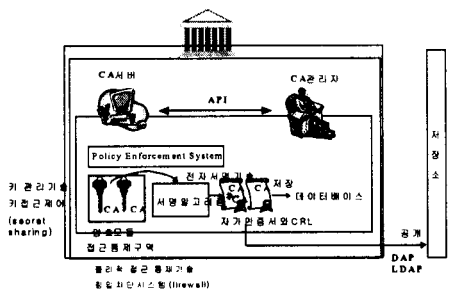
구성하면서 효율성과 다른 PKI와의 통신을 위해 한 도메인내 또는 다른 도메인내의 인증기관들사이에 네트워크 구조를 형성하는 것이 효율적이다.

3.6 PKI 동작 절차

3.6.1. (최상위) CA 구축

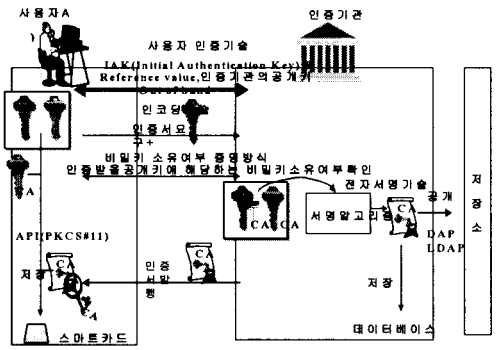


[그림 2] 계층적 구성과 네트워크 구성



[그림 3] CA 구축

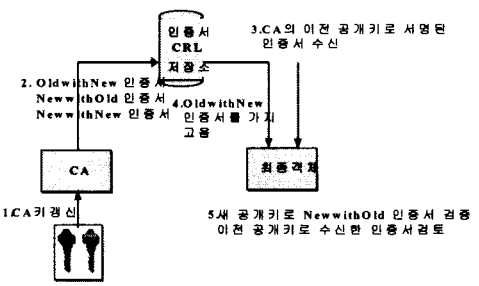
3. 6. 2 초기 등록 및 인증서 발행



[그림 4] 초기 등록 및 인증서 발행

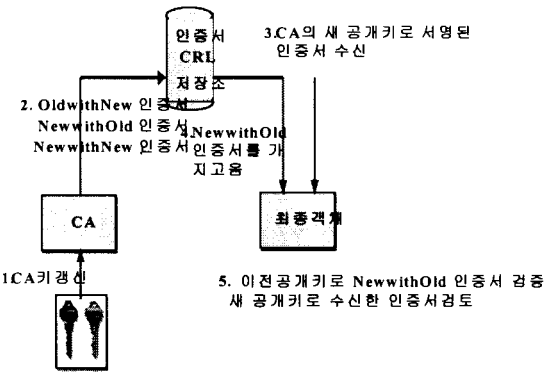
3. 6. 3 인증서 활용

가. 최종 객체는 새로운 공개키를 가지고 있는 데 CA의 이전 공개키로 서명된 인증서를 수신하는 경우



[그림 5] 가.의 경우

나. 최종 객체는 이전 공개키를 가지고 있는 데 CA의 새 공개키로서 인증서를 수신하는 경우



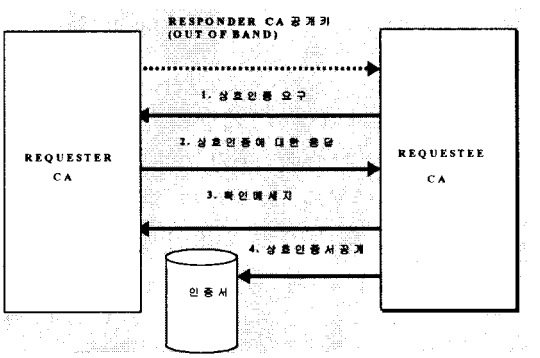
[그림 6] 나.의 경우

3.6.4. 상호 인증 단계

가. requester CA : 상호인증을 통해 생성되는 상호인증서의 주체 CA

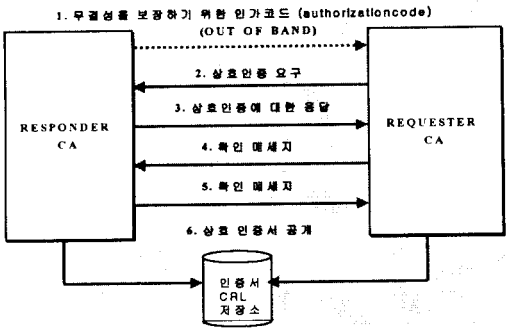
나. responder CA : 상호인증을 통해 생성되는 상호인증서의 발행자 CA

다. 일방향 상호인증



[그림 7] 일방향 상호인증

라. 양방향 상호인증



[그림 8] 양방향 상호인증

4. 결 론

전자서명과 인증은 정보통신의 발달함에 따라 중요한 역할을 하고 있다.

공개키를 기반의 전자서명과 인증은 전자적 거래 환경에서 효율적인 보안 서비스를 제공하는 것이라고 할 수 있다. 그러나 다양한 전자서명 방식이 오히려 역기능이 되어 네트워크의 장애로 발전될 수 있으며, 위 변조 및 부인방지를 위한 다양한 기술과 알고리즘에 대한 연구가 더욱 절실하다고 할 수 있다.

또한 획일적이면서 계층적인 PKI 구조로는 효율적인 인증이 불가능하므로 응용되는 서비스의 다양성과 확장성에 따라 융통성 있는 PKI 구조가 필요하다고 할 수 있겠다. 즉 미국의 FPKI 처럼 각 공통분별 네트워크 PKI를 구축하고 이들을 루트 CA에서 상호 연동하고 인증하는 방식의 계층적 PKI와 네트워크 PKI의 결합구조가 급속히 발전하는 전자거래 환경에 바람직하다고 할 수 있어 이에 대한 추가적인 연구가 필요함을 알 수 있다.

5. References

[1] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, New York, 2nd edition, 1996.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 1997.

[3] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, Florida, 1995.

[4] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer Verlag, 2nd edition, 1994.

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice-Hall, 2nd edition, 1999.

[6] 박창섭, "암호이론과 보안," 대영사, 1999.

[7] 이임영, 송유진 공역, "현대암호," 생능출판사, 1999.

[8] W. Diffie and M. E. Hellman, "Newdirections in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[9] 김상균, 백종현, 이강석, 이석준, "공개키 인증 기반 구조로서의 X.509에 대한 연구," 통신정보보호학회지, 제 8권, 제 3호, pp. 33-45, 1998. 9.

[10] 김상래, "금융분야의 인증시스템 구축 및 서비스 계획," 통신정보보호학회지, 제 9권, 제 3호, pp. 23 - 30, 1999. 9.
[11] 최영철, 오경희, 이재일, 홍기융, 이홍섭, "전자서명 인증관리센터 구축 및 운영," 통신정보보호학회지, 제 9권, 제 3호, 1999. 9.