사용자 위주의 새로운 공개키 기반구조 제안

이병천, 김광조

한국정보통신대학원대학교

A Proposal for User-oriented Public Key Infrastructure

Byoungcheon Lee, Kwangjo Kim

Information and Communications University

요 약

공개키 기반구조는 실생활에 빠르게 접목되고 있으며 정보화 사회에서 다양한 응용분야에 사용될 것으로 예상된다. 현재의 X.509 기반의 공개키 기반구조에서는 인증서와 인증기관이 일대일 연관성을 갖는데 개인마다 다수의 인증서를 사용하게 될 경우에는 인증서 및 개인키 관리에 많은 비용이 소요될 것으로 예상된다. 본 논문에서는 개인인증서(self-certificate)와 인증서명(certification signature)을 사용하여 하나의 공개키/개인키 쌍을 다수의 인증서에 공유하는 것을 특징으로 하는 사용자 위주의 새로운 공개키 기반구조를 제시하고 그것의 장단점을 분석해 본다.

1. 서론

공개키 인증서란 개인의 인적 정보에 공개키를 결합하여 인증기관이 서명한 문서로서 정보화 사회에서 개인의 신분증 역할을 하게 된다. 공개키 인증서에 등록된 공개키는 정보보호 응용 시스템에서 메시지의 암호화, 키 분배, 전자서명의 검증에 사용되며 개인은 자신만이 비밀히 보관하는 개인키를 사용하여 메시지 복호화, 키 분배, 전자서명 작성에 사용하게 된다. 여기에 사용된 공개키/개인키 쌍은 인증기관이 발급한 공개키 인증서에 의해 그 권위를 인정받게 된다.

한편 두 사용자가 사용하는 공개키 인증서의 인증기관이 서로 다른 경우에는, 공

개키 기반구조(Public Key Infrastructure)에 의해 각 인증기관이 상위 인증기관에 의해 상호 연관성을 가지며 인증통로(certification path)를 검증함으로써 개인의 신분을 상호 인증하게 된다. 공개키 인증서 및 PKI는 향후 전자상거래, 인터넷 보안, 이동통신 등 다양한 분야에 적용될 것으로 예상된다. 그러므로 PKI는 국가의 중요한 기반구조(Infrastructure)중의 하나로서 세계 각국은 PKI를 조속히 구축하기 위하여 노력을 경주하고 있다.

PKI 분야에서 지금까지 개발되고 있는 주요 기술로는 크게 X.509 기반 시스템(X.509, PKIX, PEM)과 비-X.509 기반 시스템(PGP, SDSI, SPKI) 등으로 나눌 수 있으며 이에 대한 자세한 내용은 참고문헌을 참조하기 바란다[1, 2, 3, 4, 5, 6].

1.1 다수 인증서 사용의 필요성

공개키 인증서는 개인의 신분증 역할을 하는데 향후의 발전된 정보화 사회에서 각 개인은 다수의 공개키 인증서를 사용할 것으로 예상된다. 예를 들면 주민등록증, 사원증, 신용카드 등이 공개키 인증서 방식으로 대체되는 것을 예상해 보자.

- o 개인이 부동산 거래를 할 경우에는 국가에서 발급한 주민등록증에 해당하는 공개키 인증서를 이용할 것이며 그에 대응하는 개인키를 이용하여 거래에 대한 서명을 하고 상대방은 제시된 인증서를 이용하여 서명을 검증함으로써 거래의 정당성을 확인할 것이다.
- o 개인이 회사의 업무와 관련하여 물품 구매를 하거나 문서에 결재를 하는 경우 회사에서 발급한 사원증에 해당하는 공개키 인증서를 이용할 것이며 그에 해당하는 개인키를 이용하여 서명을 하고 상대방은 제시된 인증서를 이용하여 서명을 검증함으로써 신분을 확인할 것이다.
- o 개인이 입금, 출금, 계좌이체 등의 금융거래를 한다면 금융기관에서 발급한 신용카드에 해당하는 공개키 인증서를 이용할 것이며 그에 해당하는 개인키를 이용하여 서명을 하고 상대방은 제시된 인증서를 이용하여 서명을 검증함으로써 거래의 정당성을 확인하게 될 것이다.

이때 주민등록증, 사원증, 신용카드 등은 개인의 신분을 나타내고 확인할 수 있는 유용한 도구이며 기존에 전통적으로 사용되던 신분증이 공개키 인증서 형태로 바뀐

것이다. 이러한 신분증의 발급 및 사용은 기존의 사회적 관습에 영향을 받으며 응용분야에 따른 다양한 요구사항을 만족시킬 수 있어야 한다.

한편 PKI가 확립되어 독립적인 인증기관들 사이에 계층적인 인증체계를 가져서 상호인증이 가능한 경우에도 다수의 인증서가 사용될 것으로 생각된다. 이러한 요구사항들을 살펴보면

- o 각각의 공개키 인증서는 특정한 신분을 나타내며 다양한 용도를 갖는다. 즉 어떤 개인이 주민등록증을 가졌다고 하더라도 어떤 회사의 소속인지 여부를 나타내지는 않으며 이를 위해서는 별도의 수단이 필요하다.
- o 사회적 관습상 이러한 신분증은 각 소속기관에 의해 독립적으로 발급되고 사용된다. 또한 각 기관마다 인증정책이 다를 수 있다.
- o 개인의 신분은 가변성을 가지며 신분증은 필요에 따라 쉽게 발급 및 폐기될 수 있어야 한다.

이러한 다양한 요구사항 때문에 향후의 정보화 사회에서 하나의 공개키 인증서만으로 사회생활을 영위하기는 어려울 것이며 각 개인은 다수의 인증서를 사용하게 될 것으로 예상된다. 이러한 환경에서 개인은 다수의 공개키 인증서를 적절히 사용해야 하고 그에 해당하는 개인키들을 비밀히 보관하고 사용하여야 하기 때문에 많은 불편이 따르고 비용부담이 클 것으로 예상된다.

1.2 개인키 보관 방법

인증기관에 의해 발급된 공개키 인증서는 직접 배포하거나 디렉토리 서비스 등을 이용하여 널리 공표되어야 하지만 그에 해당하는 개인키는 비밀히 보관되어야 한다. 개인키의 보관 방법으로는 암호화된 데이터 파일 형태로 컴퓨터 내에 보관하는 방법과 IC카드 등의 접근이 제한된 하드웨어 내에 보관하는 방법이 있을 수 있다. 현재로서는 IC카드 등 하드웨어 장비가 많이 보급되지 않아 전자의 방법이 많이 사용되고 있지만 이것은 개인키 사용시 개인키가 컴퓨터 메모리 내에서 복구되어 사용되고 네트웍에 연결되어 있는 컴퓨터의 경우 해킹에 의해 개인키가 유출될 가능성이 있기 때문에 제한적으로 사용되어야 한다. 또한 시스템의 고장에 의한 개인키 분실의 위험성도 크다. 반면 개인키가 IC카드 등 제한된 하드웨어내에 보관되고 개인

키를 사용하는 동작이 하드웨어 내로 제한되는 경우 매우 안전하게 보관될 수 있다. 향후 IC카드 장비가 널리 보급될 경우 개인키는 주로 IC카드 내에 보관될 것으로 예상되며 본 논문에서는 IC카드 등의 안전한 보관 수단을 이용하는 것을 가정한다.

1.3 기존 PKI 기술의 단점

1) 경제적 측면

현재 널리 보급되고 있는 X.509 기반의 공개키 기반구조에서는 공개키 인증서를 발급하고 유지하기 위하여 경제적으로 많은 비용이 소요될 것으로 예상된다. 예를 들면

- o 인증기관에의 가입비 및 년회비
- o 공개키 인증서의 발급에 따르는 인증기관의 운영비용
- o 디렉토리 서비스 운영비용
- o 인증서 폐기를 위한 CRL의 운용 비용 및 CRL 점검에 따르는 통신비용
- o IC카드 형태의 신분증 발급시 하드웨어 비용의 중복투자
- o 다수의 인증서 사용 시 사용하지 않는 인증서 발생에 따르는 낭비 요소
- o 부주의한 보관으로 인한 개인키의 분실가능성 및 인증서 폐기 비용의 증가
- o 상호인증 과정의 복잡성 및 그에 따르는 통신비용의 증가

2) 기술적 측면

X.509 기반의 공개키 기반구조는 기술적으로 다음과 같은 문제점이 있다.

- o 개인키 소유 증명을 제공하지 못한다. 인증서 발급시 인증기관은 사용자가 개인키를 소유하고 있음을 확인해야 한다는 의무사항이 있으나 이를 공개적으로 증명하는 수단은 제공하지 못한다.
- o PKI를 이용한 상호인증은 매우 복잡하다. 인증통로를 검증하는 것은 많은 계산량과 통신량을 요구하며 인증기관간의 상호인증서를 이용하는 방법도 운영이 매우 복잡하다.
- o 인증기관에 등록하지 않은 개인 사용자에겐 적절한 키분배 수단이 없어서 별도의 메커니즘을 사용해야 한다. PGP 등의 Web of trust에 기반한 인증 시스템과는 상호 호환되지 않는다.

이 논문에서는 다수 공개키 인증서의 사용과 하드웨어 방식으로 개인키의 안전한 보관이 이루어지는 환경에서 기존 PKI 기술의 이러한 경제적, 기술적 문제점을 해결할 수 있는 방안을 제시하고자 한다. 즉 개인인증서(self-certificate)와 인증서명(certification signature)이라는 새로운 개념을 사용하여 하나의 공개키/개인키 쌍을 다수의 공개키 인증서에서 공유할 수 있는 방안을 제안한다. 아울러 제안된 인증체계의 장단점을 분석하고 향후의 연구방향을 제시한다.

2. 공개키 기반구조의 설계

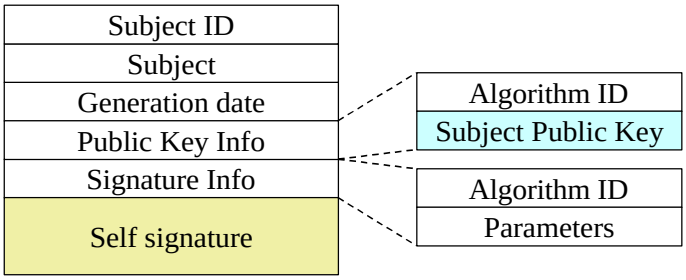
본 논문에서 제시하는 새로운 공개키 기반구조는 기존의 X.509 기반의 시스템과는 달리 개인이 먼저 공개키/개인키 쌍을 IC카드 내에서 생성한 후 자신의 개인정보와 공개키를 결합하여 개인키로 서명함으로써 개인인증서를 발행하고, 이를 인증기관에게 제시하고 신분 확인 후 인증서명을 받아서 사용한다는 데에 있다. 필요에 따라서는 하나의 개인인증서에 대해 여러 인증기관으로부터 인증서명을 발급 받아 사용함으로써 하나의 키쌍을 다수의 인증서에 공유하는 방법을 제공한다. 이하 개인인증서 발행 과정과 인증서명 발급 과정을 상세히 설명한다.

2.1 개인인증서(self-certificate)의 발행

개인인증서는 개인의 사용자 정보와 공개키를 결합하여 개인키로 서명한 문서로서 IC카드 내에서 발행된다. (그림 1)에는 제안된 개인인증서의 구조를 나타내었다. X.509 인증서의 구조를 참조하였으나 복잡한 확장 필드를 제거하고 단순화하였다. X.509 인증서와의 차이점은 다음과 같다.

1) 개인의 고유번호를 나타내는 subject ID를 추가하였다. Subject ID는 주민등록번호와 같이 사회에서 개인의 유일성을 나타낼 수 있는 고유번호이며 개인인증서의 효율적인 처리를 위하여 중요한 인식 필드로 사용될 수 있다.
2) 사용기간을 없애고 개인인증서의 생성일시(generation date)를 추가하였다. 개인인증서는 개인이 발행하는 것이며 개인키를 소유하고 있다는 증명을 제공하기 위한 것이므로 특별한 사용기간을 설정할 필요가 없기 때문이다.
3) 개인인증서에서는 복잡한 확장필드가 제거되었으며 이것은 인증서명에 포함되

어 있다.



(그림 1) 개인인증서의 구조

개인인증서의 발행 과정은 다음과 같다.

1) IC카드를 카드리더에 입력한다.
2) IC카드에 대한 접근제어 암호를 설정한다.
3) 사용자 개인정보를 입력한다.
4) IC카드 내에서 공개키/개인키 쌍을 생성한다(개인키는 외부 접근이 차단된 안전한 장소에 보관).
5) 사용자의 개인정보와 공개키를 결합한 데이터를 개인키로 서명하여 개인인증서를 발행한다(그림 1의 구조)
6) 개인인증서는 IC카드 내부(외부에서 접근 가능한 장소) 및 외부(컴퓨터)에 저장된다.
7) 개인인증서를 디렉토리서비스에 등록한다.

개인인증서는 개인이 발행한 것이기 때문에 신분 증명의 기능은 없지만 개인키를 실제로 보유하고 있다는 증명을 제공할 수 있다. 또한 인증기관에 등록하지 않은 개인사용자들은 개인의 책임하에 이것을 효율적인 키분배 수단으로 이용할 수 있다.

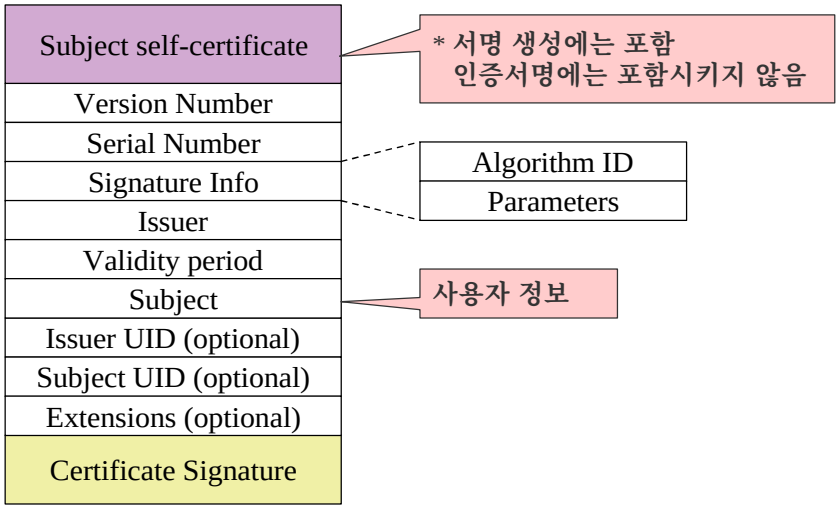
개인인증서는 개인이 발행하는 것이지만 사실은 인증기관 등 IC카드 관련 하드웨어 장비를 보유한 기관에서 발행할 수 있다. 다만 인증기관의 개인키로 서명하는 것이 아니라 개인이 사용할 키쌍의 개인키로 서명하는 것이다.

한편 서명/검증용 키쌍과 암호화/복호화용 키쌍을 서로 다르게 사용하는 경우에는 두 개의 키쌍을 생성하고 두 가지 개인인증서를 함께 발행하여 하나의 하드웨어 신

분증에 저장하여 이용할 수 있으며 본 논문의 제안내용을 간단히 확장할 수 있다.

2.2 인증서명(certification signature)의 발급

개인인증서는 그 자체만으로는 신분증명의 기능이 없으며 인증기관으로부터 인증서명을 발급 받아서 함께 사용해야만 신분증명 기능을 제공할 수 있다. (그림 2)에 인증서명의 구조를 나타내었다. 여기에서는 X.509 기반의 공개키 기반구조에서 필요로 하는 버전번호, 일련번호, 발급자, 사용기간, 사용자, 기타 확장필드들을 포함시켰다. 여기에서 사용자(subject) 필드는 인증기관이 작성하는 사용자 신분을 나타내는 고유정보이다. 반면 사용자의 공개키에 관한 정보는 따로 넣지 않고 개인인증서를 포함하여 서명하는 것으로 대신하였다. 즉 인증서명의 생성시에는 개인인증서를 (그림 2)에서와 같이 앞부분에 포함하여 서명하되 이것은 중복데이터이므로 인증서명 자체에는 포함시키지는 않도록 설계하였다. 인증서명에 개인인증서를 포함시킬 것인가의 여부에 관해서는 장단점이 있으므로 향후 좀더 구체적인 논의가 필요하다고 하겠다.



(그림 2) 인증서명의 구조

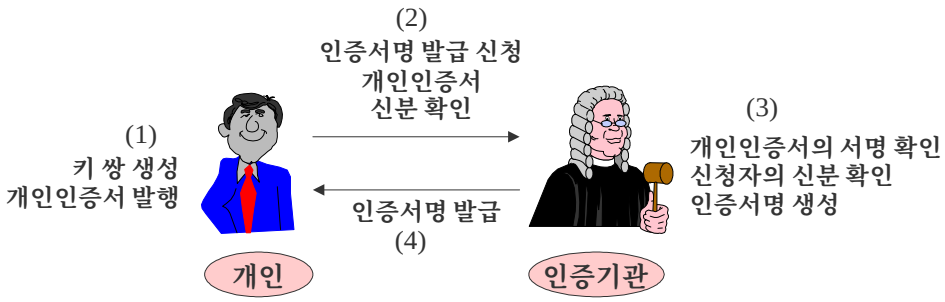
(그림 3)에는 인증서명의 발급 프로토콜을 제시하였다.

1) 개인은 IC카드 내에서 키쌍을 생성하고 개인인증서를 발행한다.

2) 개인은 인증기관에게 인증서명 발급을 신청한다. 이때 개인인증서를 제시하고 신분확인 절차를 거친다.

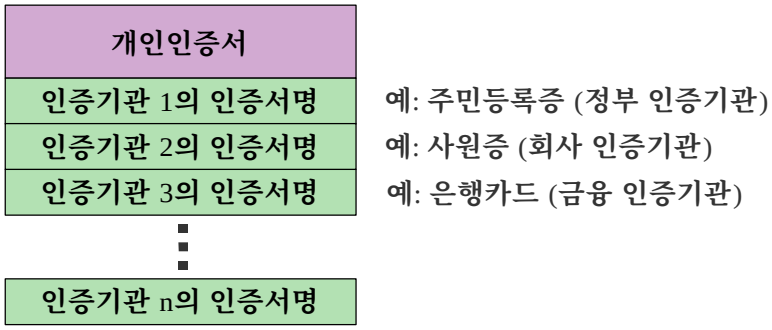
3) 인증기관은 개인인증서의 서명을 확인하여 개인키 소유 여부를 검증한다. 신청자의 신분을 확인한 후 (그림 2)와 같은 형태로 인증서명을 생성한다.

4) 인증기관은 생성된 인증서명을 개인에게 발급하고 디렉토리 서비스에 등록한다.



(그림 3) 인증서명 발급 프로토콜

하나의 개인인증서에 대해 필요시 여러 인증기관으로부터 인증서명을 발급 받을 수 있으며 이 경우 공개키/개인키 쌍을 여러 개의 인증서에 공유하는 것이 된다. (그림 4)에 하나의 개인인증서에 대해 복수의 인증기관으로부터 인증서명을 발급받아 사용하는 경우의 예를 나타내었다. 즉 정부, 소속회사, 금융기관 등 자주 이용하게 되는 인증기관에 대해서는 미리 인증서명을 받아놓은 후 그 인증기관의 신분인증이 필요한 경우에는 개인인증서와 그 인증기관의 인증서명을 함께 제시하면 된다.



(그림 4) 복수 인증기관으로부터의 인증서명의 발급

3. 공개키 기반구조의 활용

3.1 개인인증서와 인증서명의 사용

이 논문에서 제시한 새로운 공개키 기반구조는 기존의 공개키 인증서를 개인인증서와 인증서명의 두 부분으로 나누고 개인인증서 부분을 여러개의 인증서명에서 공유하자는 것이다. 그러므로 전체적인 인증서의 구조는 바뀌었지만 인증서명을 이용하는 상호인증 과정은 기존의 X.509에서의 인증방식과 호환될 수 있다. 이에 덧붙여서 제안된 인증구조에서는 여러 인증기관으로부터 인증서명을 발급받아 사용하는 것을 허용하기 때문에 복잡한 상호인증과정 대신 인증서명을 이용한 직접인증이 가능하다는 장점이 있다. 즉 자주 사용하는 인증기관에 대해서는 미리 인증서명을 발급받아 놓고 필요시 개인인증서와 인증서명을 함께 제시함으로써 직접적인 인증이 가능하며, 자주 사용하지 않는 인증기관의 인증이 필요한 경우에는 다른 상호인증 가능한 인증서명을 제시하고 X.509 기반 인증구조의 계층적인 상호인증과정을 통하여 인증받을 수 있다. 즉 인증서명을 이용한 직접인증 방식과 X.509 기반의 상호인증방식을 병행하여 사용할 수 있다. 이것은 다수의 독립적인 X.509 인증서를 발급받아 사용하는 것과 같지만 하나의 공개키/개인키 쌍만을 이용하기 때문에 개인키 및 인증서의 보관과 사용이 편리하다는 장점이 있는 것이다.

제안된 공개키 인증구조의 적용 예로써 위의 (그림 4)에서와 같이 복수의 인증기관으로부터 인증서명을 발급받아 사용하는 경우를 생각해 보자.

1) 부동산 계약시 : 부동산 계약서에 개인키로 서명 후 개인인증서와 정부 인증기관의 인증서명을 함께 제시한다(직접 인증 방식).
2) 회사내의 문서 결재시 : 문서를 개인키로 서명 후 개인인증서와 회사 인증기관의 인증서명을 함께 제시한다(직접 인증 방식).
3) 금융 거래시 : 거래요청서를 개인키로 서명 후 개인인증서와 금융 인증기관의 인증서명을 함께 제시한다(직접 인증 방식).
4) 쇼핑몰에서 물품 구입시 : 쇼핑몰의 인증서명은 받지 않았다고 가정하자. 물품 구입 및 지불 내용에 대해 개인키로 서명 후 금융 인증기관의 인증서명을 함께 제시한다(금융 인증기관과 쇼핑몰과의 X.509 기반 상호인증과정을 통해 신분 인증).

3.2 디렉토리 서비스

제시된 새로운 인증구조를 적용하면 통합적인 디렉토리 서비스가 가능하다. 각 개인은 하나의 개인인증서에 대하여 다수의 인증서명을 가지게 되고 이 경우 각 인증기관별로 독립적인 디렉토리 서비스를 제공하는 것보다 (그림 5)에 나타낸 바와 같이 통합적인 디렉토리 서비스를 제공하는 것이 더 효율적이다. 각 개인은 고유의 subject ID로 구분될 수 있으며 하나의 개인인증서와 다수의 인증서명이 나열되게 된다. 사용자가 특정인의 인증서를 획득하고자 하는 경우에는 그 사람의 개인인증서와 함께 현재의 응용시스템에서 필요한 특정기관의 인증서명만을 획득하면 된다.

번호 (주민등록)	성명	개인인증서	인증서명 1 (정부기관)	인증서명 2 (회사)	▪▪▪▪▪▪
1	홍길동				▪▪▪▪▪▪
2	임꺽정				▪▪▪▪▪▪
3	유관순				▪▪▪▪▪▪

(그림 5) 통합적 디렉토리 서비스

3.3 인증서 폐기 목록(Certificate Revocation List)

인증서 폐기 목록(CRL)은 이미 발급된 인증서를 폐기하기 위해서 사용된다. 인증서 폐기의 주된 사유로서는 사용자 신분의 변동, 인증서 갱신, 개인키 노출 등이 있을 수 있다. 기존의 X.509 v2 기반의 CRL은 폐기된 인증서의 수가 증가할수록 데이터가 커지고 통신량이 크게 증가하는 단점이 있으며 이를 해결하기 위하여 다양한 방식이 제안되고 있다[7, 8, 9, 10]. 제안된 공개키 인증구조에서는 (그림 6)에 제안된 바와 같이 집중식 CRL 서비스가 가능하다. 개인키가 노출되거나 분실된 경우에는 개인인증서를 폐기하며 사용자 신분의 변동 등에 의한 경우에는 인증서명을 폐기한다. 기존의 X.509 기반의 인증구조에서는 위에 제시된 모든 폐기 사유에 대하여 인증서 전체를 폐기하기 때문에 많은 비용이 소요되었으나, 제안된 인증구조에서는 개인키 노출이나 분실시 이외에는 키쌍을 계속 사용할 수 있는 방안을 제공한다.

이러한 CRL 구조는 개인별로 개인인증서 및 인증서명의 폐기 여부를 효율적으로

나타내 주기 때문에 검색 시간이 빠르다는 장점이 있다. 또한 디렉토리 서비스와 효율적으로 통합되어 운영될 수 있다.

번호 (주민등록)	성명	개인인증서 폐기	인증서명폐기 1 (서명,사유,일시)	인증서명폐기 2 (서명,사유,일시)	▪▪▪▪
1	홍길동				▪▪▪▪
2	임꺽정				▪▪▪▪
3	유관순				▪▪▪▪

(그림 6) 인증서 폐기목록 서비스

4. 제안된 공개키 기반구조의 장단점 분석

4.1 경제적 측면의 장점

제안된 공개키 기반구조에서는 하나의 키쌍을 다수의 공개키 인증서에서 공유하고 디렉토리 서비스 및 CRL을 통합 운영할 수 있기 때문에 다수의 공개키 인증서를 인증기관별로 독립적으로 발급하는 것과 비교할 때 비용을 획기적으로 줄일 수 있다.

1) 공개키/개인키 쌍을 다수의 인증서에 공유하므로 개인키 보관을 위한 신분증(IC카드)의 중복 발급을 억제
2) 디렉토리 서비스, 인증서 폐기 목록의 효율적인 통합 운영에 따른 비용 감소
3) 직접 인증 방식의 이용에 따른 계산비용, 통신비용의 감소
4) 개인키의 부주의한 관리를 방지하여 인증서 폐기비용의 감소

4.2 기술적 측면의 장점

기술적인 측면에서는 다음과 같은 장점이 있다.

1) 개인인증서에 의한 개인키 소유증명의 제공
2) 직접인증 방식의 적용에 의한 인증시간 감소
3) 직접인증 방식과 X.509 방식의 병행 사용 가능
4) PKI가 확립되기 이전이라도 유연한 방식으로 효율적으로 운영 가능
5) 인증기관에 등록하지 않은 개인 사용자에게도 효율적이고 안전한 키분배 수단

을 제공

4.3 단점

제안된 인증구조는 경제적, 기술적 측면에서 많은 장점을 가지고 있지만 다음과 같은 단점을 생각해 볼 수 있다.

1) 통합화되고 집중적인 관리 방식을 사용함으로써 다양한 요구사항에 대한 유연성이 부족하다. 이것은 제안된 인증구조가 X.509 기반의 인증구조와 병행 사용 가능하기 때문에 큰 문제가 되지는 않는다.
2) 여러개의 신분증이 하나로 통합됨으로서 분실시의 위험성이 커진다. 이를 해결하기 위해서는 적절한 키 위탁 방식의 적용이 필요하다.
3) 정보의 집중에 의한 프라이버시 보호 문제가 대두된다.

5. 결론

이 논문에서는 공개키/개인키 쌍을 다수의 공개키 인증서에서 공유할 수 있는 방안으로서 개인인증서와 인증기관의 인증서명을 이용하는 새로운 공개키 인증구조를 제시하였다. 이를 이용하면 공개키 인증서를 발급하고 유지하는 경제적인 비용을 크게 줄일 수 있을 뿐만 아니라 직접인증에 의한 빠른 상호인증이 가능하며 기존의 X.509 인증방식과도 병행 사용할 수 있다는 기술적인 장점이 있다.

이것은 기존의 공개키 기반구조가 인증기관 중심의 인증체계였던 것에 비교할 때 사용자 중심의 인증체계라고 할 수 있다. 즉 X.509 공개키 기반구조에서 사용자는 인증기관과 PKI로부터 인증을 받는 수동적인 존재였던 것에 반하여 제안된 공개키 기반구조에서는 자신의 개인인증서를 기반으로 자신이 자주 이용할 인증기관들의 인증서명을 받아서 신뢰를 쌓아가는 능동적인 존재가 된다.

이러한 방식은 PKI의 구축 및 운영에 있어서 큰 효율성을 제공할 수 있기 때문에 향후 제안 방식에 대해 지속적인 연구가 필요하다고 생각된다.

참고문헌

[1] 조한진, 김봉한, 이재광, “사용자 인증을 위한 공개키 기반구조 시스템 비교 분

석", CISC98논문집, pp. 21-32, 1998

[2] ITU-T Recommendation X.509, The Directory: Authentication Framework, 1993

[3] Public-Key Infrastructure (X.509) (pkix), http://www.ietf.org/html.charters/pkix-charter.html

[4] Simple Public Key Infrastructure (spki), http://www.ietf.org/html.charters/spki-charter.html

[5] Marc Branchaud, A Study of Public Key Infrastructure, McGill University, 1997

[6] A Simple Distributed Security Infrastructure (SDSI), http://theory.lcs.mit.edu/~cis/sdsi.html

[7] 오중효, 박기철, 이국희, 조갑환, 문상재, "공개키 확인서 취소 방식의 비교", CISC'98 논문집, pp. 9-20, 1998

[8] S. Micali, "Certification Revocation System", U.S. patent 5666416

[9] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, ftp://ftp.isi.edu/in-notes/rfc2560.txt

[10] Paul Kocher, "A Quick Introduction to Certificate Revocation Trees (CRTs)", http://www.valicert.com/resources/bodyIntroRevocation.html