전자서명 Key와 인증 System에 관한 연구

A study on the Internet Public Key and Certification System

정 지 문, 신 정 길, 홍 창 선, 최 성
남서울대학교 컴퓨터학과
Ji-Moon Jung, Jung-Gil Shin, Chang-Sun Hong, Sung Choi
Dep. of Computer Science Namseoul University

요 약

국내 전자서명법의 제정 및 시행은 21세기 새 천년을 준비하는 시점에서 중요한 의미를 갖는다. 전자적 거래가 활성화되고 있는 현재 시점은 기존의 대면 방식의 거래 문화가 컴퓨터 네트워크나 기타 통신망을 통한 비대면 방식의 거래 문화로 자리잡아 가고 있는 중요한 시점이다. 전자서명법의 시행을 통한 전자서명 인증관리체계의 구축, 전자서명 인증관리센터의 구축, 운영, 공인인증기관의 지정, 운영 등은 전자적 거래 활성화 및 전자정부 구현에 근간이 되는 국가 공개키 기반구조 구축이라는 기술적 기반을 갖추었다는데 그 의의가 있다. 전자서명 인증관리체계의 구축은 궁극적으로 전자적 거래 활성화를 도모함과 동시에 국내 전자상거래 시장을 외국 기업의 독점적 선점으로부터 보호할 수 있는 부가적 효과도 가질 수 있다.

Ⅰ. 서론

최근 인터넷과 같은 컴퓨터 네트워크 기술이 발점함에 따라 민간이나 정부 분야에서의 전자적 거래(Electronic transaction)가 급증하고 있으며 컴퓨터 네트워크를 통한 원격지간의 비대면 거래 방식의 전자상거래 시대가 도래하고 있다.

전자상거래는 기업간 또는 기업과 개인 고객간에 가상공간 내에서 전자정보를 통해 거래 활동을 구현하고자 하는 기법이라고 할 수 있다. 즉 조직(기업, 공공 및 국가기관)과 소비자간 또는 조직과 조직간에 상품유통관련 정보의 배포, 수집, 협상, 주문 납품, 대금지불 및 자금이체 등 모든 상거래 절차를 전산화된 정보로 전달하는 상거래를 의미한다.

급속하게 성장하고 있는 전자상거래가 안전하고 신뢰할 수 있게 이뤄지기 위해서는
기밀성, 인증, 무결성, 거래사실 부인방지 등의 기본적인 보안서비스가 제공되어야 한다.
기술적인 발전으로 공개키 암호화 방식을 적용하여 메시지 암호화를 통해 기밀성을 제공하고, 전자서명을 통해 인증, 무결성, 부인방지 서비스 제공이 가능하게 되었다. 그러나 전자서명만으로 인터넷에서 거래 상대를 완전히 신뢰하기가 어려우므로, 거래 상대를 인증할 수 있기 위해 인증기관이 필요하게 되었고 세계 선진 각국은 공개키 기반 구조의 구축과 법, 제도의 제정 및 정비에 노력하고 있다.

Ⅱ. 본론

1.공개키 기반구조

1) 공개키 기반구조의 구성요소

정보시스템 보안, 전자 상거래, 안전한 통신등의 여러 응용분야에서 인증서의 사용을 용이하도록 하는 정책, 수단, 도구 등을 수립하고 제공하는 객체들의 네트워크인 공개키 기반구조를 구성하는 최소 객체들은 인증기관, 등록기관, 디렉토리, 사용자이다.

(1) 디렉토리(Dirctory)

인증서와 사용자 관련 정보, 상호인증서 및 인증서폐지목록 등을 저장 및 검색하는 장소로 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버(인증기관)는 DAP(dirctory Access Protocol)나

LDAP(Lightedweighted DAP)를 이용하여 X.500 디렉토리 서비스를 제공한다. 인증서와 상호 인증서 쌍은 유효기간이 경과된 후에도 서명 검증의 응용을 위해 일정기간동안 디렉토리에 저장된다.

(2) 사용자

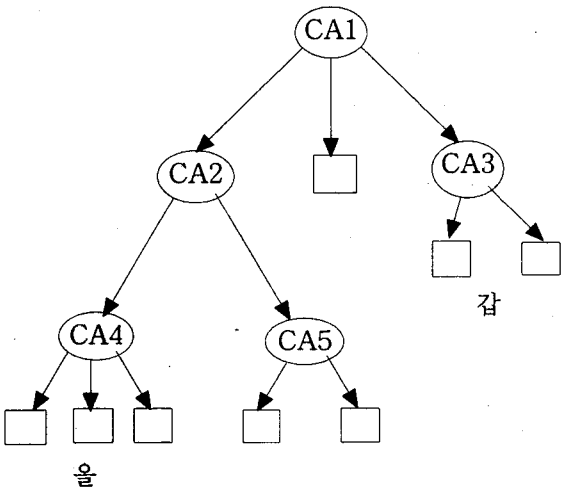
공개키 기반구조내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다.

2. 공개키 기반구조의 모델

공개키 기반구조에서 통신당사자들의 신뢰는 상대방의 인증서를 전달받는 인증경로를 통해 전달된다. 신뢰가 인증경로를 따라 전달되는 방법에 따라 공개키기반구조는 크게 두 가지로 구성될 수 있다.

1) 계층적 구성

인증기관들이 하위 인증기관에게 인증서를 발행하는 최상위 인증기관(PAA)아래에 계층적으로 배열되어 있는 구성으로 인증기관들은 자신의 아래 인증기관들에게 인증서들을 발행한다. 계층적으로 구성된 공개키 기반구조에서 최상위 인증기관의 전자서명검증키는 모든 사람에게 알려져 있어 사용자들의 인증서는 최상위 인증기관에서 자신이 신뢰하는 인증기관까지의 인증 경로를 검증함으로써 검증된다.



[그림1] 공개키 기반구조의 계층적 구성

(그림1)에서 갑이 을의 전자서명을 검증한다고 하자. 우선 갑은 을의 전자서명검증키를 획득해야 한다. 갑은 CA1과 CA3을 신뢰하고 을은 CA1과 CA4를 신뢰한다. CA1에서 CA4까지의 인증경로를 전송한다.

갑은 을이 자신과 같은 도메인에 있음을 확인한 후 자신이 알고 있는 CA1의 전자서명검증키를 이용해 CA1에서 CA4까지의 인증경로를 검증하여 을의 전자서명검증키를 획득한 후 서명문을 검증한다.

인증기관이 각각의 도메인을 형성하여 독립적으로 존재하는 구성으로 CA들이 서로를 상호인증하여 서로에게 인증서를 발행한다. 네트워크로 구성된 공개키 기반구조의 사용자는 자신의 인증서를 발행한 인증기관의 전자서명검증키만을 알고 있다. [그림2]와 같은 구성에서 갑이 을의 서명문을 검증하고자 한다고 생각하자. 갑은 CA3을 신뢰하고 을은 CA2를 신뢰한다. 을에서 갑으로의 인증 경로는 여러 개가 존재하므로 이중에서 가장 짧은 인증 경로를 찾는 탐색과정이 필요하다.

가장 짧은 인증경로는 CA3<>CA1<>CA2<<을>>이다. 갑은 이 이중경로를 이용해 을의 전자서명을 검증한다. 네트워크로 구성되었을 경우에는 인증 경로가 여러 개 존재할 수 있으므로 이중 짧은 경로를 찾는 것이 중요 관건이다.

(1) 전자서명 인증관리체계 개념

전자서명 기술은 공개키 암호기술을 이용하여 구현된다. 공개키 암호기술은 그 기술을 사용하는 사용자 각각 비밀키(전자서명생성키)/공개키(전자서명검증키) 쌍을 가지게 된다. 전자서명생성키는 그 소유자만 아는 정보이고 전자서명검증키는 인증기관의 디렉토리에 공개되어 누구나 그 전자서명검증키를 사용할 수 있도록 한다.

사용자 A와 B는 자신들이 신뢰하는 인증기관에 등록을 하고 자신들이 전자서명시 사용할 전자서명생성키와 쌍을 이루는 전자서명검증키에 대한 인증서를 받는다. 인증서는 사용자의 이름과 전자서명검증키를 포함하며 그것은 인증기관의 서명문이므로 인증기관 외의 제3자가 수정하거나 변경할 수 없다.

즉, 전자서명검증키의 무결성이 보장되는 것이다. 인증기관은 인증서를 생성한 후 디렉토리에 전자서명검증키 대신 인증서를 공개한다. 사용자 A는 전송하고자 하는 전

자문서에 자신만이 간직한 전자서명생성키를 이용하여 전자서명을 하여 사용자 B에게 전송한다. 사용자 B는 디렉토리로부터 인증서를 가지고 와서 인증서 내에 포함되어 있는 전자서명검증키를 이용하여 수신한 전자문서의 서명을 검증한다.

3. 전자서명 인증관리센터 시스템

1) 시스템 설계의 기본원칙

- 엄격한 다단계 역할 기반(Role-based)의 접근통제
- 네트워크 침입차단 및 침입탐지 체계구축
- 키생성 및 관리시스템 등 중요 시스템은 오프라인 방식으로 구축
- 핵심인증시스템의 이중화 운영 등

2) 시스템 구성

[표 1] 전자서명 인증관리센터 시스템 구성 및 기능

시스템 구성	기 능
등록관리 시스템	· 신청자 정보 등록 및 관리 · 인증서 발급에 필요한 데이터 입력
키 생성 시스템	· 인증관리센터 키 생성 · 공인인증기관 키 생성
인증서 생성 시스템	· 인증관리센터 자가 인증서 (Self-Signed Certificate) · 공인인증기관 인증서 생성 · 공인인증기관인증서폐지목록(CRL:Certuficate Revocation List) 생성
디렉토리 서비스 시스템	· 인증관리센터 인증서 공고 · 공인인증기관 인증서 공고 · 공인인증기관 인증서폐지 목록 공고
시점확인 시스템	· 공인인증기관 시점확인 서비스 요청시 제공 · GPS수신 방식을 통한 시간보정
웹 서비스 시스템	· 전자서명법홍보 및 인출관리 센터 업무소개 · 공인인증기관 목록 유지 · 공인인증기관 상태에 대한 정보제공

(1)시스템 구성 일반

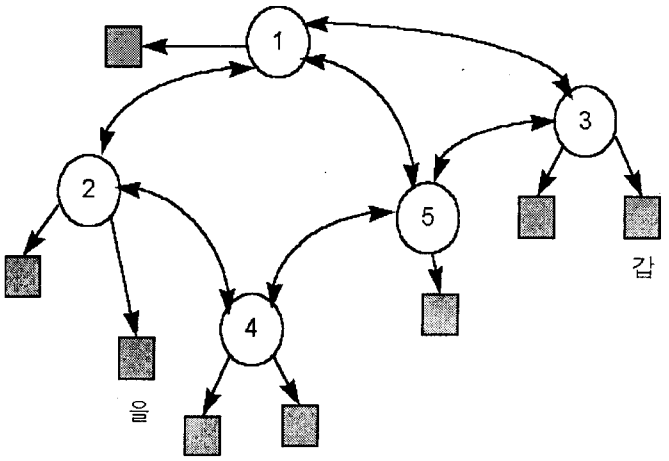
인증관리센터 시스템은 크게 등록관리 시스템, 키 생성 시스템, 인증서 생성 시스템, 디렉토리 서비스 시스템, 시점확인 시스템, 웹 서비스 시스템과 같이 주요 분야별 시스템으로 구성된다.

(2) 논리적 구성도

각각의 시스템은 물리적으로 별도의 장소에서 운용되며, 각 시스템간의 자료입,출력은 오프라인 방식으로 운영함으로써 인증관리센터 시스템의 안전,신뢰성을 극대화시킨다.

(3) 네트워크 구성도

전자서명 인증관리센터 시스템의 논리적 구성도는 다음과 같은 네트워크 구성도로 표현할 수 있다. 웹 서비스 시스템, 디렉토리 서비스 시스템, 시점확인 시스템은 외부 네트워크에 연결되어 공인인증기관이나 일반사용자들에게 온라인 서비스를 제공하며, 나머지 시스템들은 안전,신뢰성의 향상을 위해 오프라인 방식으로 구성된다.

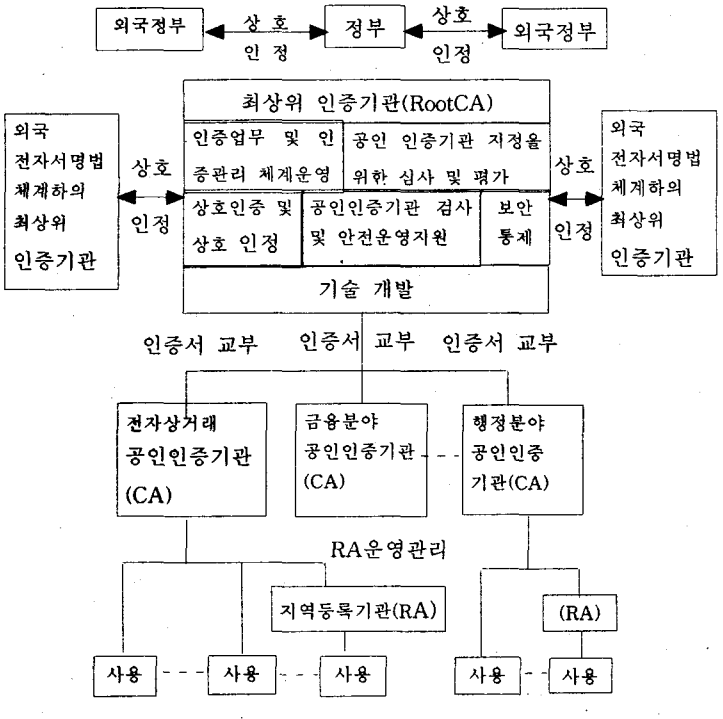


[그림 2] 네트워크 구성도

3) 적용 표준

(1) 전자서명 알고리즘

인증서 발급을 위해 사용하는 전자서명 알고리즘은 인증관리체계 모델의 원활한 적용을 위해 RSA와 KCDSA 모두를 지원한다. RSA는 PKCS(Public Key Cryptography Standard)를 준용하여 구현코자 하며, KCDSA는 별도의 ASN.1(Abstract Standard Notation)을 정의한 후, DER(Distinguished Encoding Rule) 인코딩 규칙을 적용할 것이다. 현재까지 가장 널리 사용되고 있는 전자 서명 알고리즘 RSA이기 때문에 타 전자 서명 알고리즘의 추가 적용이 당분간은 필요 없을 것으로 사료되나, 향후 안전, 신뢰성이 보장된 전자서명 알고리즘이 업계에서 사용된다면, 전자서명 인증관리센터 시스템에 추후 확장시켜 적용할 수도 있을 것이다.



[그림 3] 전자서명 알고리즘

(2)인증서 및 인증서폐지 목록

전자서명 인증관리센터에서 사영할 예정인 인증서 및 인증서폐지목록은 각각 X.509 버전3 및 버전2로서, IETF PKIX 그룹에서 1999년 1월에 RFC2759로 채택된 "Internet Public Key Infrastructure X.509 Certificate and CRL Profile"이다.

4) 시스템 보안대책

전자서명 인증관리센터 시스템은 각 시스템 부문별로 접근통제를 거쳐야만 동작 가능토록 개발하고 있으며, 각각의 접근통제는 철저한 역할분리 방식에 근간하여 구축,운영될 것이다. 또한, 각 시스템은 서로 다른 운영실에 분리되고 각각의 시스템은 오픈된 형태가 아닌 잠금장치가 있는 보안캐비넷 내에 설치하여 물릿거 및 관리적 측면에서도 안전,신뢰성을 확보할 계획이다.

5) 물리적 보안대책

전자서명 인증관리센터는 정책적으로 각 구역에 보안등급을 두어, 각 등급에 따라 물리적 보안 강도를 달리하여 다단계 통제가 가능토록 구축하고 있으며 물리적 접근 통제방식으로는 스마트카드 및 생체인식(지문인식 등)기술을 이용한 접근통제 시스템을 구축,운영할 수 있도록 추진하고 있다. 또한 화재나 홍수 등과 같은 재난에 대비하여 인증서 등과 같은 중요한 데이터를 지역적으로 분리된 원격지의 안전한 저장소에 백업할 수 있는 안전,신뢰성 확보방안도 마련하였다.

Ⅲ. 결론

이 글에서는 전자상거래 보안을 위한 공개키 기반구조와 국외 구축 현황, 전자서명 인증관리체계에 대한 내용을 기술하였다. 3절에서는 전자서명 인증관리센터의 임무 및 주요 수행업무, 전자서명 인증관리센터의 시스템 구축 및 운영에 관련된 내용을 소개하였다.

국내 전자서명법의 제정 및 시행은 21세기 새 천년을 준비하는 시점에서 상당히 중요한 의미를 갖는다. 전자적 거래가 활성화되고 있는 현재 시점은 기존의 대면 방식의 거래 문화가 컴퓨터 네트워크나 기타 통신망을 통한 비대면 방식의 거래 문화로 자리잡아 가고 있는 중요한 시점이라고 말할 수 있다.

이러한 단계에서 전자상거래의 활성화는 단지 기술적인 뒷받침만으로 이뤄내기는 어려우며, 관련 정책 및 법,제도의 제정이나 보완이 반드시 병행되어야만 한다. 이러한 측면에서 우리나라의 전자서명법 제정은 21세기 전자적 거래의 활성화를 위한 제도적 기반을 마련하였다고 볼 수 있다. 또한, 전자서명법의 시행을 통한 전자서명 인증관리체계의 구축, 전자서명 인증관리센터의 구축, 운영, 공인인증기관의 지정, 운영 등은 전자적 거래 활성화 및 전자정부 구현에 근간이 되는 국가 공개키 기반구조 구축이라는 기술적 기반을 갖추었다는데 그 의의가 있다고 말할 수 있다. 이러한 전자서명 인증관리체계의 구축은 궁극적으로 전자적 거래 활성화를 도모함과 동시에 국내 전자상거래 시장을 외국 기업의 독점적 선점으로부터 보호할 수 있는 부가적 효과도 가질 수 있으리라 예상된다.

<참고문헌>

[1] 남상조 "사이버은행의 현황", 남상조1997년11월28일 한국전문가시스템학회, 97년추계학술대회논문집, pp.243-253.

[2] 송용욱 "지불기술, 시스템동향", 인터넷백서, forthcoming.

[3] 이재규 "전자상거래 및 가상은행의 발전방향" 1997.

[4] 이재원 "기업-소비자간 인터넷상거래" 1998.