主題

정보보안과 인증기관

한국정보인증(주) 김 주 현

차 례

1. 서 론

인터넷의 급속한 확산과 인터넷 사용자 수의 폭발적인 증가에 따라 가상공간을 무대로 하는 전자거래의 규모 역시 기하급수적으로 늘어나고 있다. 전자거래의 규모가 늘어남에 따라 폐쇄된 네트웍에 비해 정보누출이 비교적 쉬운 인터넷상에서의 안전한 전자상거래를 위해 정보보안이 상대적으로 중요시되고 있다. 인터넷을 기반으로 한 각종 서비스, 쇼핑몰 등의 활성화는 비대면 상대방에 대한 효율적인 인증과 유통되는 정보의 안전성을 전제로 한다. 이제 국내에서도 전자서명법의 시행과 함께 본격적인 전자상거래의 시대가 전개되고 있다. 인터넷상의 전자거래의 보안과 관련한 암호방식과 인증체계 및 인증시스템에 대해 살펴보기로 한다.

2. 전자거래의 특성

전자거래는 대개의 경우 비대면에 의해 이루어지는 특성으로 인해 기존의 서면거래와는 다른 특성을 나타내고 있다. 전통적인 거래에서는 ① 인증(authenticity), ② 무결성(integrity), ③ 부인봉쇄(non-repudiation), ④ 기밀성(confidentiality)을 요건으로 하며, 이러한 요건은 대면에 의한 거래에 의해 어렵지 않게 만족된다. 이러한 특성을 전자적 환경하에서 구축하기 위해서는 상당한 노력과 기술을 필요로 한다. 그러나 전자거래에서도 교환되는 메시지와 보존되는 기록은, 상황에 따라 다르기는 하지만, 일반적으로 통용되는 서면거래에서 요구되는 것과 동일한 요건들을 필요로 한다.

2.1 인증 (Authentication)

비대면에 의한 거래에 있어서 가장 큰 문제는 상

대방이 타인을 사칭하는 지의 여부를 판단하는 것이다. 타인에 의한 사칭이란 비대면의 특성을 이용하여 타인의 ID를 도용하여 개인정보를 빼내거나 파괴한다든지, 물건을 사고 대금을 타인에게 전가하는 것을 말한다. 이에 대한 대책으로는 상대방의 진정성을 확인하는 것이다. 즉, 진정성은 전자메시지가 누구로부터 전송되었으며 진정한 것인가를 확인하는 것이다. 수신인은 발신인에 대한 진정성을 믿을 수 있어야 거래를 진행할 수 있으며, 또한 향후 문제 발생시 수신한 전자메시지가 증거로 채택되기 위해서는 진정성이 확보되어야 한다. 이러한 진정성을 확보할 수 있는 방안으로 인증서의 사용을 들 수 있다. 전자메시지를 수신한 당사자는 인증서를 활용하여 그 메시지가 발신인으로부터 왔기 때문에 진정하다는 것을 알 수 있다.

2.2 무결성 (Integrity)

내용의 변경은 어떠한 수단에 의해 통신이 되는 메시지의 내용이 변경되는 것을 말한다. 전송되는 메시지가 정확하고 완전하다는 것, 즉 발신인이 전송한 메시지가 전송되는 중에 변경되지 않고 수신인이 수령한 전자메시지와 비교하여 동일한 것이며 완전하다고 보증하는 것을 무결성이라고 한다. 이러한 무결성은 실제적인 전자거래에서 필요충분 조건과 동시에 법적인 요건이다. 비대면에 의해 이루어지는 전자거래상의 특성으로 인해 쌍방이 교환하는 전자적인 메시지를 믿기 위해서는 그 메시지에 대한 무결성이 보장되어야 한다. 특히 전자거래에 있어서 온라인상에서 계약을 체결하거나, 후에 그 계약을 증명하기 위하여 이전에 보낸 전자정보를 이용하고자 할 때 무결성은 매우 중요하게 된다.

무결성을 보증하는 기술로는 Parity, Checksum, 그리고 Hash함수 등이 주로 사용되고 있다. 그러나 단순히 이러한 방법들만으로는 파라미터 자체가 변경될 위험이 있기 때문에 내용의 변경을 방지하기에는 충분하지 않다. 이에 대한 대비로 암호기술과 병행하는 것이 전자서명 (Digital Signature)이다. 전자서명은 전자메시지의 무결성을 확인하는 수단을 제공한다.

2.3 부인봉쇄 (Non-repudiation)

부인이란 실제로 행한 통신을 하지 않았다고 주장하는 것이다. 비대면으로 거래가 이루어지는 전자적 환경에서는 발신인이 수신인이 수신한 문서가 위조 또는 변경된 것이라고 주장하면서 그러한 메시지 전송을 부인하는 거래부인(repudiation)의 위험을 증가시킨다. 따라서 부인을 막는 것은 전자거래의 유효성을 확인하기 위해서는 매우 중요하다. 부인봉쇄는 보안의 관점에서 보면 외부의 공격자로부터의 보호가 아니라 합법적으로 전자메시지를 활용하는 이용자로부터의 위협에 대한 보호라는 특성이 있으며, 전자메시지를 신뢰한 당사자가 상대방에게 그 메시지를 귀속시키려고 할 때 법적 요건이 된다. 기존의 우편제도에는 내용증명이나 배달증명에 의해 부인봉쇄를 방지하고 있으며, 전자거래에서는 이러한 부인봉쇄를 전자서명에 의해서 행할 수 있다. 전자서명은 발신인이 발신인만이 아는 정보를 메시지에 첨부하여 보내는 것으로 수신인은 수신한 정보중에서 이 정보를 확인함으로써 발신인의 신원을 확실히 보장할 수 있게 된다.

2.4 기밀성 (Confidentiality)

교환되는 정보가 개방된 통신망을 통하여 이동함에 따라 거래 당사자간 외의 제3자에게 정보에의 접근을 통제하는 것이 어렵게 되고, 따라서 전자거래에서는 필요한 경우 메시지가 전송되는 과정에서, 그리고 거래 당사자의 시스템에 저장되어 있는 중에 기밀성이 확보되어야 한다. 특히 상호간에 교환되는 메시지 정보가 신용카드번호, 개인 신상에 대한 정

보, 또는 당사자간의 기밀을 요하는 경우에는 특히 기밀성이 반드시 확보가 되어야 한다. 이러한 전자거래에서의 메시지에 대한 기밀성을 확보하기 위하여 메시지에 대해 암호화를 하는 방법을 활용하고 있으며, 다음과 같은 암호화 방식이 주로 사용되고 있다.

3. 암호화의 방법

전자거래에 있어서 발생될 수 있는 기밀성과 관련된 문제점들을 해결할 수 있는 방안이 바로 암호화이다. 암호화란 메시지를 구성하는 정보를 직접 표현하는 데이터, 즉 평문(plaintext 또는 메시지)을 허용된 사람 (특정인)이외에는 알아볼 수 없는 형태의 암호문(cyphertext)으로 바꾸어주는 변환과정을 말한다. 이에 대하여 복호화는 암호문에 적용하여 원래의 평문 데이터를 재생성하는 과정이다. 즉, 암호화의 방법은 암호화(encryption)와 복호화(decryption)라고 불리는 한 쌍의 데이터간의 변형이라고 볼 수 있다.

전자거래에 있어서의 문제점을 해결하기 위한 암호화 기술에는 크게 암호화와 복호화를 동일한 키로 하는 비밀키 암호방식 (대칭키 암호화 방식)과 암호화와 복호화를 별도의 키로 하는 공개키 암호방식 (비대칭키 암호화 방식)의 2가지로 구분될 수 있다.

3.1 비밀키 암호방식 (대칭키 암호화 방식)

메시지를 암호화하고 암호화된 메시지를 원래의 상태로 바꾸어주는 복호화를 동일한 키를 이용해서 하는 비밀키 암호방식은 암호화 키와 복호화 키가 동일하다고 해서 대칭키 암호화 방식(Symmetric Cryptosystem)이라고도 불린다.

상업적으로 널리 이용된 최초의 대칭키 암호화방식은 미국 통상부의 공식권유에 의하여 IBM이 NIST 와의 계약에 따라 1974년에 개발한 DES (Data Encryption Standard)이다. DES는 1977년에 미국의 연방표준으로 채택되었고, 1981년에는 금융산업표준으로 채택되었다. 현재 DES는 가장 잘 알려지고 인터넷을 통화여 폭넓게 이용되고 있는 암호화 표준이다. DES가 통신에서 사용될 때에는 발신인과 수신인 양자가 동일한 비밀키를 사용하여야 한다.

대칭키 암호화 방식은 데이터의 전송중에 제3자가 암호화한 문서와 키를 가로챌 경우, 그 키를 사용하여 암호화된 메시지를 해독할 수 있다는 단점이 있으며, 다수의 이용자 환경에서는 관리하여야 하는 비밀키가 기하급수적으로 늘어나게 되어 비밀키의 보급 및 관리에 대한 문제가 대두된다. 실제로 N명이 상호 통신하는 경우에 필요한 총 키의 개수는 N명의 조합 〔1/2*N*(N-1)〕만큼의 키가 필요하게 되어 불특정 다수를 상대로 하는 전자거래에 있어서는 대칭키 암호화 방식을 적용하는 데에는 상당한 무리가 따른다. 뿐만 아니라 서로 모르고 멀리 떨어

	비밀키 암호방식	공개키 암호방식
키방식	대칭키 (Symmetric)	비대칭키 (Asymmetric)
History	BC 500년경	1976년
관련 알고리즘	DES, RC5, SEED, FEAL, IDEA 등	RSA, RPK 등
장 점	계산속도 빠름	암호키 사전 공유 불필요
단 점	암호키 사전 공유 필요 키의 분배 및 관리의 어려움	계산속도 느림

표 1. 비밀키와 공개키 암호방식의 비교

져 있는 사용자간 비밀키를 공유하고 관리하는 일이 쉬운 것은 아니다. 또한 발신인과 수신인 사이에 문제가 생겼을 때 수신인이 받은 메시지를 증거로 사용하고자 하는 요구가 있을 수 있다. 하지만 비밀키 암호 방식은 이 요구에 부응하지 못한다. 이유는 수신인과 발신인 사이에서 공유하는 비밀키는 아무도 알 수 없고 설사 수신인이 발신인에게서 온 메시지와 비밀키를 가지고 있다고 해도 그 메시지가 과연 발신인이 보낸 것인지, 수신인이 메시지를 조작했는지 알 수 없다. 이러한 문제점을 해결하기 위하여 개발된 것이 공개키 암호방식이다.

3.2 공개키 암호방식 (비대칭키 암호화 방식)

비밀키 암호방식에서의 키의 관리 문제를 쉽게 하고 부인봉쇄(non-repudiation)를 위한 디지털 서명을 가능하게 하기 위해 공개키 암호시스템이라 부르는 방식이 생겨났다. 공개키 암호방식에서는 서로 다른 두개의 키를 이용하여 암호화 및 복호화를 수행하는 방법으로 1976년에 스탠포드 대학의 Diffie와 Hellman에 의하여 처음 도입되었으며, 한 쌍의 키가 서로 다르기 때문에 비대칭적 암호방식(Asymmetric Cryptosystem)이라고도 한다.

비대칭키 암호방식에서는 하나의 키로 암호화한 메시지는 쌍을 이루는 다른 키만으로 복호화할 수 있다. 두 개의 키 중 하나는 일반인이 아무 제약없이 접근할 수 있는 저장소에 보관하여 공개하고 나머지 하나의 키는 타인에게 누설되지 않도록 사용자의 시스템에서 철저히 관리하여야 한다. 이 때 일반에게 공개하는 키를 공개키라 하고, 본인이 관리하는 키를 비밀키라 한다. N명이 상호 통신하는 경우에 각자가 2개씩의 키를 가지면 되므로 필요한 총 키의 개수는 {2*N}개가 된다.

공개키를 사용하여 메시지를 암호화하면 비밀키로만 복호화할 수 있고, 반대로 비밀키를 가지고 메시지를 암호화하면 공개키에 의해서만 복호화할 수 있게 되므로 암호화통신이 가능하다. 또한 공개키 방식에서 비밀키는 그 보유자만이 보관하고 있고, 비밀키에 의하여 암호화된 문서는 이에 대응하는 공개키에 의하여만 복호화할 수 있기 때문에 문서작성자의 신원을 증명하고 메시지의 진정성과 무결성을 확보할 수 있으며, 이러한 특성으로 인해 전자서명에 많이 이용된다. 그러나 공개키 암호방식은 비밀키 암호방식에 비해 암호처리에 시간이 걸리기 때문에 메시지 암호화에는 데이터의 길이가 작은 경우를 제외하고는 일반적으로 비밀키 암호방식을 사용한다.

현재 비대칭 암호방식중에서 전세계적으로 가장 폭넓게 사용되고 있는 것이 바로 RSA방식이다. RSA는 공동 개발자인 MIT의 Rivest, Shamir와 Alleman의 첫 글자를 딴 것이다. RSA계산법은 공개모듈(public modulus)이라고 불리는 수치를 사용하는데, 이 모듈은 공개키의 일부를 구성한다. 공개모듈은 비밀키의 일부를 구성하는 두 개의 소수(prime number)를 곱하여 얻어진다. RSA의 안전성은 커다란 소수를 발견하는 것은 상대적으로 쉽지만 그러한 두 수의 곱의 결과를 인수분해하는 것은 상당한 처리과정 및 시간이 필요하며 또한 매우 어렵다는 사실에 근거한다.

메시지의 기밀성과 무결성을 확보하기 위해 RSA 방식에서 활용하는 전자서명 기법은 다음과 같다. 메시지 발신인은 본인의 비밀키를 이용하여 메시지의 암호문을 생성하고 메시지의 사본에 첨부하여 수신인에게 전송한다. 수신인은 발신인의 공개키를 이용하여 암호화된 메시지 내용을 복호화하고 이것을 전송된 메시지와 비교한다. 만약 양자가 일치하면 수신인은 메시지 내용이 전송과정에서 변경되지 않았다는 것과 발신인이 보냈다는 사실을 확인할 수 있다.

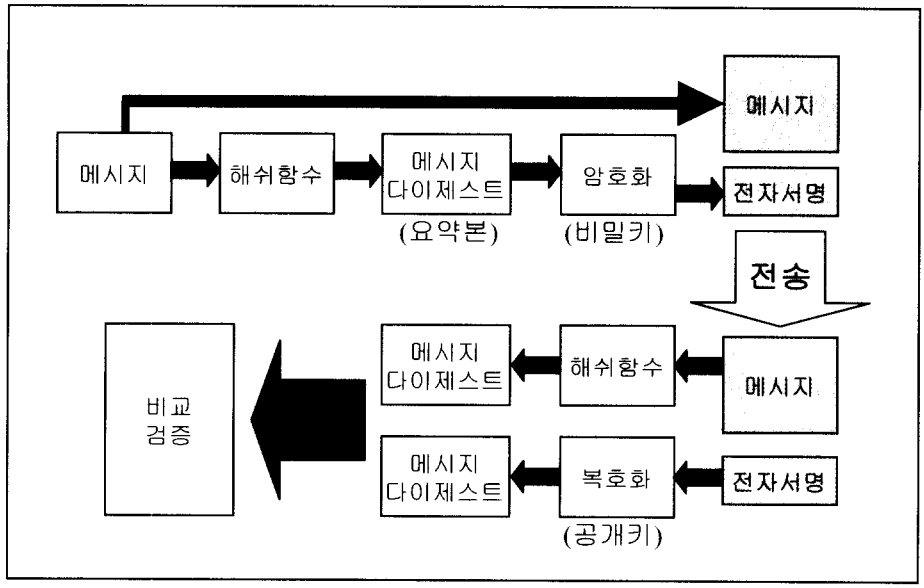

그림 1. 전자서명 생성 및 검증과정

4. 인증기관

4.1 인증기관의 필요성

전통적으로 사람과 사람사이에서 이루어지는 일은 대부분 직접적인 대면을 통함으로써 가능하였다. 하지만 인터넷 등 네트워상에서 비대면으로 행해지는 거래에 있어서는 이러한 직접적인 대면이 어렵기 때문에 온라인상에서 활용될 수 있는 보다 확실한 신원인증 방법이 필요하게 되었다. 기밀성, 진정성, 무결성, 부인봉쇄 등의 기능을 수행하기 위하여 공개키 암호방식이 폭넓게 활용되고 있다는 것은 이미 앞에서 언급한 바와 같다. 그러나 공개키를 신뢰할 수 있다는 가정하에서 전자서명에 의해 거래 상대방을 신뢰를 할 수 있기 때문에 단순히 전자서명만으로는 상대방을 신뢰할 수가 없다. 예를 들어 갑이 문서를 작성한 후 전자서명을 하여 을에게 전송하였다 하더라도 을의 입장에서는 갑이라는 사람이 실제로 존재하는지, 또는 갑이 실제로 존재하긴 하지만 병이 갑인 것처럼 가장하여 등록한 후에 갑을 사칭하는지 등에 대한 사실은 제3자의 개입이 없이는 입증을 하지 못한다. 특히 전자거래의 경우와 같이 불특정다수가 비대면의 상태에서 거래를 하게 되는 경우에는 더욱 큰 문제가 된다. 또한 전자거래에서는 전통적 의미에서의 자필에 의한 서면작성이나 수기의 서명도 존재하지 않으므로 법령이 당사자에 의한 서면작성과 서명을 요구하는 거래에서는 이러한 요건을 충족시킬 장치가 필요하게 된다.

이러한 문제점을 해결하기 위하여 제3자의 입장에서 공개키 및 소유자의 신원정보 등을 포함하는 인증서를 유지관리할 수 있는 공신력있는 인증기관(Certificate Authority, CA)의 존재가 필요한 것이다. 즉, 공개키 암호기술이 인터넷을 이용한 많은 응용분야에 사용되면서 발생될 수 있는 여러 문제점들을 해결하고 상대방의 인증서에 대한 신뢰를 높이기 위한 해결책으로 인증서를 책임지고 관리할 수 있는 인증기관이 대두되게 된 것이다. 따라서 국내에서도 전자상거래의 인프라를 구축하고 활성화시키기 위하여 전자서명법상에서 공인인증기관의 설립을 명시화하고 있는 것이다.

4.2 국내 인증기관의 체계

PKI란 사용자의 공개키를 인증하여 주는 인증기관들의 네트워크로 지역적으로 멀리 떨어진 상대방끼리의 비대면하에서의 안전한 통신을 가능하게 하는 암호학적 키와 인증서의 배달시스템으로 공개키 방식을 사용하는 전자서명, 전자상거래 등 모든 분야가 안전하게 구축되기 위해서는 반드시 필요한 것이다.

그림.2는 국내의 공개키 기반구조의 형태를 나타낸 것이며, 각 조직별 역할은 다음과 같다.

- 정보보호분과위원회
  - 국가 공개키 기반구조 구축 운용에 관한 정책의 심의
  - 국가간 상호인증 체계 구축방안 심의
- 정보통신부
  - 전자서명 인증관리 체계의 신뢰성있는 운영과 관련된 정책/감독기관
- 한국정보보호센터
  - 전자서명 인증관리체계에서 최상위 인증기관의 임무와 역할을 수행
- 공인인증기관
  - 가입자의 공개키를 인증하여 주는 역할
  - 가입자의 인증서(공개키)를 유지/관리
  - 기타 공인인증과 관련한 역무를 제공
- 등록기관
  - 공인인증기관의 인증서 발급신청 업무를 대행

5. 한국정보인증㈜

5.1 설립배경

1999년 2월에 전자서명법이 공포된 후, 국내에서는 전자상거래의 활성화를 위하여 전자서명법에서 규정한 공인인증기관의 설립이 필요하게 되었다. 그러나 국내 인증시장이 아직 성숙되지 않은 상태이

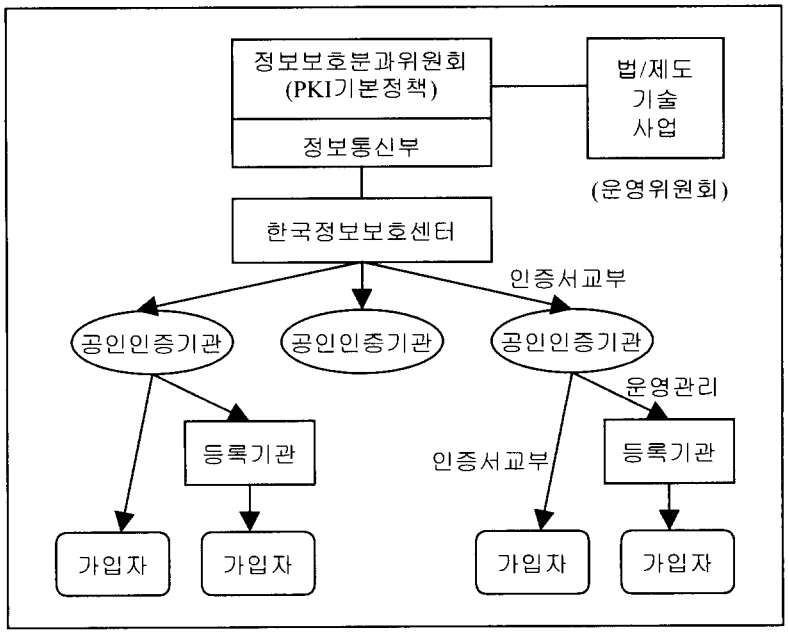

그림 2. 국가 공개키 기반구조 (NPKI)

고 외국과의 기술 격차가 많이 나는 시점에서 인증기관의 난립을 막는 것이 국가 자원이 중복투자를 방지하고 국내 보안시장 및 전자 상거래의 활성화에 도움이 된다는 판단 아래 국내 유수의 정보통신 관련 기업들이 컨소시엄을 구성하기로 합의하고 1999년 4월에 삼성SDS, SK텔레콤, LG인터넷, 포스테이터, 한국무선국관리사업단, 한국전기통신공사 등 6개사가 참여하는 설립추진위원회를 구성하였다.

1999년 6월에 주요주주 9개사 (다우기술, 삼성SDS, SK텔레콤, LG인터넷, 일진, 제일화재해상보험, 한국무선국관리사업단, 한국전기통신공사, 한국정보통신) 및 일반주주 13개사를 포함한 컨소시엄이 구성되어 초기 자본금 200억원으로 1999년 7월 1일에 한국정보인증㈜가 설립이 되었으며, 2000년 1월부터 상용서비스를 제공함을 목표로 하여, 현재 공인인증기관의 인가 신청중에 있다. 공인인증기관 인가를 위해서 전자서명법은 공인인증기관의 인증시스템이 갖추어야 할 요건들을 자세히 정하여 놓고 있다. 다음은 한국정보인증㈜의 인증시스템이 구비하여야 할 시스템 기능에 대해 간단히 설명하기로 한다.

5.2 인증시스템의 구성 및 기능

한국정보인증의 인증시스템은 공인인증기관의의 역할을 수행하기 위해서 전자서명법 및 전자서명법 시행령에서 제시하는 기능들을 수행하는 시스템들과 고객에게 인증서를 발급해주고 유지관리를 해 주는 시스템들로 구성된다. 그 외에 이러한 시스템들을 네트워상에서 안전하게 보호할 수 있는 네트워 및 서버보안시스템과 이들 설비를 안전하게 보호, 관리할 수 있는 물리적인 보안설비 등으로 구성되어 있다. 그림은 인증시스템의 구성도이며, 각 주요 시스템들에 대한 주요 기능은 다음과 같다.

5.2.1 등록관리 시스템

- 가입자의 전자서명 생성키에 대한 유일성 확인 기능
- 가입자 식별을 위한 고유한 명칭(DN) 부여 기능
- 가입자 정보를 등록, 관리하는 기능
- 권한 있는 직원만이 가입자 정보에 접근가능하도록 하는 기능
- 가입자의 등록정보를 등록기관으로부터 공인인증기관에 안전하게 전달하는 기능
- 가입자 등록정보 관리에 대한 감사기록, 보존 기능
- 등록관리 시스템을 위, 변조 및 무단삭제로부터 보호하는 기능
- 감사기록을 위, 변조 및 무단삭제로부터 보호하는 기능

5.2.2 전자서명 생생키 생성 및 관리시스템

- RSA의 1,024비트 이상의 안전성에 준하는 전자서명 키 생성기능
- 전자서명 생성키를 생성하여 저장한 후 전자서명 생성키를 시스템에서 즉시 삭제하는 기능
- 전자서명 생성키를 암호화하여 전자서명 키 저장장치에 저장하는 기능
- 3인 이상의 권한 있는 직원이 공동으로 전자서명 생성키를 생성하는 기능
- 전자서명 키를 생성한 사실, 시각, 행위자 등 내역의 감사기록, 보존 기능
- 공인인증기관의 전자서명 키를 유출, 복제하는 위협을 방지하는 기능
- 감사기록의 위, 변조 및 무단삭제로부터 보호하는 기능
- 가입자의 전자서명 생성키를 암호화하여 다양한 저장매체에 저장하는 기능
- 저장장치에 대한 봉인기능
- 저장장치에 대한 접근권한 확인기능

- 전자서명 생성키의 유출, 변경을 방지하는 기능
- 전자서명 생성키에 대한 접근내역을 기록, 유지하는 기능
- RSA, KCDSA 등 안전성을 검증 받은 국제, 국가, 단체 표준 알고리즘 지원 기능
- SHA-1, HAS-160 등 160비트 이상의 해쉬값을 생성하는 알고리즘의 지원 기능

5.2.3 인증서 생성 및 관리 시스템

- X.509 V3 인증서 규격을 준수하는 인증서 생성기능
- X.509 V3 인증서 규격을 준수하는 인증서 폐지 목록 생성기능
- 2인 이상의 권한 있는 직원이 공동으로 인증서를 생성, 발급, 갱신, 효력정지 또는 폐지하는 기능
- 인증서를 생성, 발급, 갱신, 효력정지 또는 폐지한 사실, 시각, 행위자 등의 내역을 감사기록, 보존 기능
- 인증서 생성 및 관리 시스템을 위, 변조 및 무단삭제로부터 보호하는 기능
- 감사기록의 위, 변조 및 무단삭제로부터 보호하는 기능

5.2.4 디렉토리 시스템

- 가입자의 인증서를 등록 관리하는 기능
- 가입자의 인증서 효력정지 및 폐지에 관한 기록을 등록, 관리하는 기능
- 가입자의 인증서 현황을 LDAP/DAP을 통해 항상 검색할 수 있도록 하는 기능
- 가입자 인증서를 등록, 관리한 사실, 시각, 행위자 등에 관한 내역을 보존하는 기능
- 디렉토리 소프트웨어를 위, 변조 및 삭제하는 위협을 방지하는 기능
- 인증서 등을 삭제하는 위협을 방지하는 기능
- 감사기록을 위, 변조 및 삭제하는 위협 등을 방지하는 기능

5.2.5 시점확인 시스템

- 초단위로 표현 가능한 정확한 표준시를 수신하는 기능
- 시점확인 시스템의 시간을 보정하는 기능
- 시점확인용 전자서명 생성키를 이용하여 전자문서의 시점을 확인 할 수 있는 기능
- 전자문서를 시점확인한 사실/시각/행위자 등에 관한 내역을 보존하는 기능
- 시점확인 시스템 및 감사기록의 위, 변조 및 무단삭제하는 위협을 방지하는 기능
- 시점확인 시스템의 시간을 변경하는 위협을 방지하는 기능

6. 결 론

1999년 7월 1일부터 전자서명법이 시행됨에 따라 비대칭키 암호화 방식에 의한 알고리즘을 이용한 전자서명에 법적인 효력이 부여됨에 따라 인증서를 기반으로 한 각종 서비스들이 더욱 많이 제공될 것으로 보인다. 전자거래의 특징, 암호화 방식의 종류 및 한국정보인증(주)이 갖추고 있는 각종 시스템들과 이들이 갖추어야 할 기능들에 대하여 간략히 기술하였다.

공인인증기관을 통하여 발급되는 인증서는 전자거래상의 주민등록증의 역할을 맡게 될 것이며, 이를 이용한 각종 새로운 서비스가 제공될 것이다. 인증서를 활용한 온라인 민원서류 발급, 전자문서 내용증명, 전자문서 공증 및 각종 온라인 계약 등과 같은 서비스에 활용될 것이며, 공인인증기관으로서 한국정보인증㈜는 전자문서 인증사업을 효율적으로 수행함으로써 인터넷상에서의 거래를 안전하게 추진할 수 있는 기반을 구축하고 전자거래를 활성화시

킴으로써 정보화 사회를 선도하여 국민의 편익증진과 공공복지의 향상에 기여할 수 있도록 부단한 노력을 경주할 것이다.

※참 고 문 헌

[1] 한국정보보호센터 공인인증기관 세부지정기준(안), 전자서명 인증관리센터 개원 자료집, pp. 49-61, July 7, 1999.

[2] Encryption and Digital Certificate, White Paper (VeriSign), 1999.

[3] 한국통신정보보호학회 전자상거래 보안기술, 이만영 외 5인 공저, 1999.

[4] Housley, R., Ford, W., Polk, W., Solo, D., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC2459, January 1999.

[5] TrustPro Userss Manual ver 2.0, September, 1999.

[6] 전자상거래론, 윤광운 외 2인 공저, 삼영사, 1999.

김 주 현

1986년 2월 한양대학교 산업공학과 졸업(학사)
1986년 현대전자 근무
1988년 5월 미국 아리조나 주립대 석사 학위 취득(산업공학)
1993년 12월 미국 아리조나 주립대 공학박사 학위 취득(산업공학)
1994년 1월~1999년 7월 삼성SDS 컨설팅사업부 근무(경영컨설턴트)
1999년 현재 한국정보인증(주) 근무

※관심분야:
Supply Chain Management (SCM)
Enterprise Resource Planning (ERP)
Business Process Reengineering (BPR)
정보처리