전자상거래하에서의 전자서명의 보안성에 관한 연구

전순환

중부대학교 경제통상학부 전임강사

요 약

전자문서, 전자영수증, 대금결제 서명 및 상호인증 등 전자상거래의 거의 모든 영역에서 사용되고 있는 전자서명의 경우에는 특히, 거래 상대방을 확인할 수 있는 확인 절차와 더불어 안전하고 신뢰성 있는 보안시스템의 구축을 위한 암호화가 필요하게 된다. 따라서 전자서명의 일반적 고찰과 관련하여 각국에서 제정되고 있는 법규는 물론 전자서명에 따른 보안문제를 고찰하고자 한다.

Ⅰ. 서 론

전자상거래에서의 거래는 사람이 직접 만나지 않고 익명의 사용자가 공유하는 네트워크 공간 내에서 검퓨터와 네트워크만을 이용하여 거래를 하는 방식이므로 네트워크를 통한 다양한 형태의 보안의 침해가 예상된다. 즉, 정보의 전송시 발생할 수 있는 소비자 개인의 프라이버시 혹은 기업의 노하우 등의 정보유출에 따른 문제를 해결하지 않고서는 전자상거래의 확대·발전을 도모할 수 없게 된다.

네트워크상에서의 정보의 보호뿐만 아니라 거래 상대방을 확인할 수 있는 확인 절차와 더불어 안전하고 신뢰성 있는 보안시스템의 구축을 위한 암호화가 필요하게 된다. 즉 전자상거래 시스템에서의 암호화기술은 개인 정보의 보호와 거래 당사자들의 인증기능을 동시에 제공하게 된다.

인터넷과 같은 개방형 네트워크환경에서 전자상거래를 구현하기 위해서는 상호인증, 기밀성, 무결성, 부인방지, 익명성 및 복제방지 등의 요건이 충족되어야 하며, 이러한 기본요건을 실현시키기 위한 핵심기술 중의 하나가 바로 전자서명이다. 전자서명은 전자문서, 전자영수증, 대금결제 서명 및 상호인증 등 전자상거래의 거의 모든 영역에서 사용되므로, 전자상거래 활성화와 소비자 보호 및 각종 분쟁해결을 위해서는 전자서명에 대한 법적 기반이 마련되어야 하며, 거래의 안정성 및 법적 기반 마련을 위해 우선 전자서명에 따른 보안문제가 해결되어야 한다.

따라서 본고에서는 전자서명의 개념, 기능 및 그 기법을 설명하고, 전자서명과 관련하여 각국에서 제정되고 있는 법규를 살펴본 다음, 전자상거래에서 이용되고 있는 보안기법과 전자서명에 따른 보안문제를 고찰하고자 한다.

논문접수일 : 98년 7월 게재확정일 : 98년 10월

II. 전자서명에 관한 일반적 고찰

2.1 전자서명의 의의

2.1.1 전자서명의 개념

전자서명(electronic signature)은 일반문서에서 사용되고 있는 서명 또는 도장을 전자문서나 전자화폐 등에 사용되는 전자방식의 디지털기호로 만들어진 동일인의 인식표지이다.

일리노이 ECS법안 제200조 (3)항에 의하면, 전자서명이란 전자문서에 부착되거나 논리적으로 결합된 전자적 형태의 서명을 말한다.

또한 UNCITRAL 전자서명 통일규칙 초안 제1조 (c)항에 의하면, 전자서명(electronic signature)이란 자료메시지에 부착(attached)되거나 논리적으로 결합된(logically) 전자적 형태의 서명(signature) 또는 자료(data)로써 사람의 신원을 확인하고 자료메시지의 내용에 대한 그 사람의 승인을 나타낼 목적으로 사용된 것을 말한다.[1] 이는 일리노이 ECS법안의 정의에 UNCITRAL전자상거래모델법에서 규정하고 있는 서명의 요건[2]을 덧붙인 형식을 취하고 있다.

한편, 우리나라의 무역업무자동화촉진에 관한 법률 제2조 제8호에 의하면, 전자서명이라 함은 전자문서의 명의인을 표시한 문자와 작성자를 식별할 수 있게 하는 기호 또는 부호를 말한다. 여기에는 구체적으로 어떠한 방식으로 전자문서의 작성자를 식별할 수 있게 하는지에 대하여는 언급이 없다. 그리고 동조 제7호는 전자문서는 전자서명을 포함한다고 규정하여 전자서명을 전자문서의 일부로 인정하고 있다.

일반적으로 인정되어 오던 기명날인(서명)의 개념은 인증 행위자가 당해 서류 위에 직접 자신의 이름 등을 적고 날인하는 행위를 하는 것을 의미해 왔지만 이제는 기명날인을 대신할 전자서명이라는 새로운 개념의 서명이 출현하게 되었다.[3]

2.1.2 전자서명의 기능

전자서명은 특별한 방식으로 만들어진 디지털 정보로서, 자료메시지의 무결성을 증명하는 메시지인증기능(secure record)과 서명자의 신원을 확인하는 사용자인증기능(secure signature)을 가지고 있다.

첫째, 메시지인증기능은 비록 정보가 암호화되어 있다 하더라도 이 내용이 처음에 만들어진 내용과 변경이 없었다는 것을 증명하는 기능이다. 즉, 일반문서에서의 서명과 같이 서명자 본인이 전자문서를 그 내용 그대로 작성일자에 작성하였음을 증명할 수 있어야 한다.

둘째, 사용자인증기능은 이 메시지를 보낸 사람이 정말 내가 기대한 그 사람인지를 증명하는 일종의 신분확인기능으로서, 거래의 주체가 누구인지를 입증하는 기능이다.

예를 들어 네크워크상에서 거래를 하는 각각

---

1) UNCITRAL전자서명 통일규칙 초안 제1조 (c)항.

2) UNCITRAL전자상거래모델법 제17조.
(1) 법률에서 사람의 서명을 요하는 경우 다음 각호에 모두 해당하면 그 자료메시지와 관련하여 그 요건은 충족된 것으로 한다.
(a) 그 사람의 신원을 확인하고 자료메시지에 포함된 정보에 대한 그 사람의 승인을 나타내기 위한 방법으로 사용되고
(b) 그 방법이 관련 약정을 비롯한 제반 정황에 비추어 자료메시지가 생성되고 교환된 목적에 적합하다고 믿을 만 할 것

3) Electronic Data Interchange and Paperless Trade, 3rd. ed., Blenheim Online Publications London, 1990, p.90.

의 개체가 실제 누구인지를 정확히 증명해주기 위해 디지털 증명을 이용하는 경우에는 구매자와 판매자의 신분을 네트워크 상에서 확인할 수 있게 된다. 이렇게 함으로써 메시지를 받는 수신자의 입장에서는 메시지를 보낸 상대방이 자신이 보낸 것이 아니라고 부인하지 못하게 하는 효용도 가질 수 있기 때문에 전자상거래의 신용을 높일 수 있다.

현재 인터넷상에서 사용장 인증기법으로 널리 쓰이는 것이 커버로스(Kerberos)이다. 커버로스는 제3자의 인증서버를 이용해 사용자간에 인증, 즉 신분의 확인을 인증서버를 통해 하는 것이다. 커버로스는 미국 MIT에서 Athena프로젝트의 일부로 설계됐으며, Athena 프로젝트의 목적은 고속의 교육망에 연결된 서버들간에 양질의 데이터서비스를 제공하기 위한 것으로 커버로스는 여기서 사용자/클라이언트와 서버간에 인증기능을 제공하기 위해서 개발됐다. 커버로스는 수년전에 그 개발권이 MIT에서 OSF로 이전됐으며, 이로 인해 OSF에 소속된 많는 유닉스 밴더들이 그들이 분산환경에서 필요한 여러 가지 기능을 제공하는 DCE(분산 컴퓨팅 환경)라고 하는 것에 커버로스 기능을 포함시켜 제공하고 있다.[4]

2.1.3 전자서명의 종류

1) 디지털서명(digital signature)

UNCITRAL 전자서명통일규칙 초안에서는, "디지털 서명은 변환되지 않는 원래의 자료메시지와 서명자의 공개키를 가진 사람이면 누구나 (a) 서명자의 공개키에 합치하는 비밀키를 사용하여 변환이 되었는지 여부, (b) 변환이 된 후 원래의 자료메시지가 변경되었는지 여부를 정확히 결정할 수 있도록 비대칭적 암호체계(asymmetric cryptosystem)와 메시지다이제스트(message digest function)를 사용하여 변환한 자료메시지로 이루어진 전자서명의 한 종류를 말한다"고 규정하고 있다.[5]

한편, 미국변호사협회(ABA)의 디지털서명법 제1장에서는, 「디지털 서명」이라 함은 (a) 비대칭 방식의 암호방식을 이용한 메시지의 작성으로서, (b) 그 메시지가 서명자의 비밀 키에 의해서 작성되었는가의 여부를 서명자의 공개키에 의하여 확인할 수 있는 것이라고 정의되었다.(제1-9조) 이 정의는 디지털 서명의 기능면에 착안한 정의이기도 하지만, 디지털 서명이 거래 보안의 각 국면 중 적어도 「동일성의 확인(identification)」, 「메시지의 완전성(message integrity)」의 기능을 만족시킬 필요가 있다는 취지의 규정으로서 이해할 수 있다.[6]

2) 특수펜에 의한 전자서명

송신자가 평소 자신의 문서에 하는 서명을 그 모양 그대로 상대방(수신자)의 컴퓨터 또는 중간매개자(호스트 컴퓨터)에 미리 등록시킨 다음 송신자가 문서를 작성한 후 특수 컴퓨터 펜으로 스크린 또는 특수 패드에 서명하여 문서와 함께 송신하면 수신자 컴퓨터에 그 모양 그대로의 서명이 나타나게 되고 수신자 컴퓨터는 미리 등록되어 있는 송신자의 서명과 대조하여 이를 확인하는 방식이다.[7]

4) 주석진, 인터넷에 기반을 둔 전자상거래(EC)의 활성화 방안에 관한 연구, 산업연구 제8집, 경기대학교, 1997, p.281.

5) UNCITRAL전자서명통일규칙 초안 제4조 A안. 이 안은 ABA가이드라인 제1.11조와 같은 내용이다.

6) 손경한, 전자상거래의 법적과제, 인권과 정의, Korean Bar Associatuon, 1997.10, p.29.

7) 남광, UNCITRAL과 전자상거래, 통상법률, 법무부,

3) 손가락 지문입력 전자서명

손가락지문을 미리 수신자 컴퓨터, 또는 중간 매개자에게 등록시킨 다음 송신자가 전자문서 작성후에 비밀번호 입력대신 컴퓨터에 부착된 지문인식장치에 손가락을 밀착시켜 그 지문이 수신자 컴퓨터 또는 중간 매개자에 도달하면 컴퓨터가 미리 등록된 지문과 대조하여 이를 확인해 주는 방법이다. 그러나 이와 같은 전자서명의 방식은 제한된 범위내의 사람이나 같은 기업내에서 사용될 때는 이용 가능하나 사전에 미리 서명이나 지문을 등록하거나 전달하여 놓아야 하는 제약 때문에 불특정 다수인과의 거래를 전제하는 일반 상거래에서는 통용되기 어려운 단점이 있다.[8]

2.1.4 전자서명기법

1) 추적방지서명(Blind Signatures)

디지캐시사(DigiCash)의 David Chaum이 고안한 서명기법이다. 은행은 어떤 번호의 전자현금을 인출했는지를 알 수 없도록 하는 방식으로서, 거래에 대한 추적이 방지되어야 하는 시스템에서 사용된다.

기본적인 아이디어는 발행한 화폐에 대해 화폐 발행자의 서명을 받아 화폐 자체에 대한 인증은 할 수 있지만 화폐 발행자는 자신이 발행한 화폐가 누구에게 발행되었는지 모르도록 하는 것이다.[9] 즉, 사용자가 전자현금을 전자은행 혹은 전자지불회사로부터 인출할 때 시리얼번호를 사용하는데 이때 은행은 사용자의 현금에 대한 정보를 취득하게 되고 사용자가 이를 사용했을 경우 은행은 사용자의 현금사용 상황을 역추적할 수 있는 정보가 되고 만다. 이를 방지하기 위해 사용자가 은행에 인출할 현금의 시리얼번호를 제공할 때 불특정한 숫자로 이 번호를 곱해서 은행으로 보낸다. 은행은 이 번호를 전자현금화해서 사용자에게 넘겨주면 사용자는 이 번호를 곱한 숫자로 다시 나누어 원래의 번호로 환원해서 사용하는 방식이다. 이렇게 하면 은행은 사용자의 원래의 현금번호가 무엇이었는지 알 수 없으므로 개인정보의 보호와 익명성이 보장되는 것이다.[10]

2) 확인자지정서명(Designated Confirmer Signature)

확인자지정서명은 일반 전자서명과 대화형 인증 프로토콜[11]의 중간적인 성격을 띠는 서명 방식이다. 즉, 지정된 확인자는 서명자의 도움없이 피확인자의 서명으로부터 인증이 가능하지만 다른 확인자는 서명자 또는 지정된 확인자의 도움이 있어야만 서명의 유효여부를 확인할 수 있다.[12]

3) 위조검출서명(Fail-stop Signature)

위조검출서명은 서명의 위조가능성으로부터 서명자를 보호하기 위한 기법으로서 이 알고리즘은 이산대수 방식의 공개 키 알고리즘을 사용하며 서명이 위조된 경우 실제 서명키의 소유자

1997. 8, p.90.

8) 남광, 상게서, pp.90-91.

9) D. Chaum, Blind Signatures for Untraceable Payment, Advances in Cryptology-CRYPTO '82, Springer-Verlag, 1983, pp.199-203.

10) 주석진, 전게서, pp.281-282.

11) 대화형 인증 프로토콜은 피확인자가 확인자에게 자신의 정보를 노출시키지 않으면서 자신을 인증하기 위한 프로토콜로서 전자서명 기법이 피확인자의 서명에 의해 어떠한 사실을 인증할 수 있도록 하는데 비해, 반드시 피확인자의 입회하에서 인증이 이루어지도록 한다.

12) D. Chaum, Designated Confirmer Signatures, Advances in Cryptology-EUROCRYPT '94, Springer-Verlag, 1994, pp.86-91.

가 위조 사실을 검출할 수 있는 방법이 제공된다. 그러나 암호학적인 방법에 의한 위조만이 검출 가능하며 키가 실제로 유출된 경우에는 위조를 검출할 수 없다.[13]

4) 그룹서명(Group Signatures)

그룹서명은 확인자가 그룹에 속하는 구성원에 의해 생성된 서명이라는 것은 확인할 수 있지만 어느 구성원에 의한 서명인지는 알 수 없도록 하는 서명기법이다. 또한 서명자가 부당하게 서명하였을 경우에는 그룹이 지정한 확인기관을 통해 서명자를 밝혀낼 수 있는 기능도 제공된다. 그러나 매서명때마다 서명자의 키 쌍이 새로 생성되어야 하기 때문에 그룹 구성원의 키의 양과 확인기관에 보관되어야 할 정보의 양이 계속 증가하는 문제가 있다.[14]

5) 부인불가서명(Undeniable Signatures)

부인불가서명은 서명자의 동의가 있어야만 서명을 확인할 수 있는 서명기법이다. 서명자가 자신의 서명한 문서의 인증에 협조하지 않을 경우를 대비하기 위해 부인 프로토콜도 제공된다.[15]

2.2 전자서명 관련법규

2.2.1 미국변호사협회(ABA)의 디지털서명법

미국변호사협회(ABA)의 디지털서명법은 미국변호사협회의 정보안전위원회(Information Security Committee)에서 국제적 법률전문가 및 기술전문가들과의 협력하에 4년여간의 연구 끝에 1996년 8월 1일에 발표된 입법지침이다. 이는 전자상거래에서 필요로 되는 디지털 서명 및 인증기관에 관한 법률·제도적 검토하에 작성된 것으로서, 디지털 서명 가이드라인(Digital Signature Guideline)이라고 한다.

동 가이드라인은 디지털 서명을 창설하는데 쓰이는 비밀키(private key)와 디지털 서명의 진정성을 확인(verify)하는 공개키(public key)와 같이 한쌍의 열쇠를 사용하는 방법을 채택하고 있다. 유타주가 처음으로 동 가이드라인을 기초로 디지털서명법(Utah Digital Signature Act, 1995)을 제정한 이래 1997년말까지 캘리포니아, 아리조나, 플로리다, 유타, 워싱턴 주 등을 포함하는 약 30개주가 디지털서명법(Digital Signature Law)을 마련하였고 현재 연방통일전자거래법 초안 작성작업도 진행중에 있다. 또한 독일의 디지털서명법 제1초안도 동 가이드라인에 기초를 두고 있다.

동 가이드라인은 전문, 해설 등을 포함하여, 본문 부분의 제1장에서는 정의(Definitions), 제2장에서는 일반원칙(General Principles), 제3장에서는 인증기관(Certification Authorities), 제4장에서는 등록자(Subscribers), 제5장에서는 디지털 서명에 관한 신뢰(Relying on Digital Signatures)를 규정하고 있다.

2.2.2 일리노이ECS법

미국의 일리노이주의 전자상거래안전법안(Illinois Electronic Commerce Security Act: 이하 일리노이ECS법이라 약칭한다)은 1998년 1월 16일에

13) E. Van Heyst & T. P. Pederson, How To Make Efficient Fail-stop Signatures, Advances in Cryptology-EUROCRYPT '90, Springer-Verlag, 1991, pp.389-404.

14) D. Chaum & E. Van Heyst, Group Signatures, Advances in Cryptology-EUROCRYPT '91, Springer-Verlag, 1991, pp.257-265.

15) D. Chaum & H. Van Antwerpen, Undeniable signatures, Advances in Cryptology-CRYPTO '89, Springer-Verlag, 1990, pp.212-216.

확정된 것으로서, 현재까지 나와 있는 전자서명에 관한 법규중 가장 진보된 형태라고 할 수 있다.

일리노이ECS법은 5부로 구성되어 있는데, ① 제1부는 전자문서 및 전자서명 일반에 관한 규정으로서 관계법령에서 문서의 유효요건으로서 서명, 원본 등을 요구하는 경우 메시지에 디지털서명이 되어 있으면 그 요건을 충족한 것으로 본다는 취지의 규정, 전자서명 및 전자문서의 증거능력 및 증거력에 관한 규정을 두고, ② 제2부는 안정한 전자서명에 관한 규정으로서 일정한 수준의 안전성을 갖춘 전자서명을 안전한 전자서명으로 정의하고 보다 높은 증거법적 추정을 부여하고 있으며, ③ 제3부는 디지털서명에 관한 규정으로서 디지털서명의 효력 및 인증기관의 인증서 발행에 관한 보장 및 책임 ④ 제4부는 국가기관의 전자서명 사용에 관한 규정 ⑤ 제5부는 관련 법령의 개정 등 법률시행에 필요한 부칙 조항들이다.

일리노이ECS법안은 미디어중립적 접근방식에 따라 공개키 암호화기술에 의존하는 디지털서명이라는 특정기술을 중심으로 전자서명을 정의하지 않고 먼저 전자서명 및 안전한 전자서명에 대한 일반규정 및 안전성의 요건을 확립한 다음 디지털서명을 안전한 전자서명의 한 방식으로 규정하고 있는 것이다. 그리고 인증기관은 여러 가지 전자서명 방식 가운데 디지털서명의 안전성 및 신뢰성을 보장하기 위한 것이기 때문에 디지털서명과 같은 장에서 규정하고 있다.[16]

2.2.3 UNCITRAL 전자서명 통일규칙 초안

UNCITRAL 전자서명 통일규칙 초안은 일리노이 ECS법안의 접근 방식을 수용하고 있으며, 세계 각국의 전자상거래 관련 법률전문가들이 토의를 거듭한 결과의 산물이다. 즉, 세계 주요국의 입법현황 및 최근의 기술적 진보를 반영함은 물론 영미법계와 대륙법계 국가의 사법제도의 차이점까지도 고려하였다. 그 내용은 매우 구체적이며, 추상화된 법규범 뒤에 숨은 정책적 배경을 파악할 수 있을 뿐만 아니라 입법시 파급효과를 예측하기 용이하다.

UNCITRAL 전자서명 통일규칙 초안은 제1장에서는 적용범위 및 일반규정, 제2장에서는 전자서명, 제3장에서는 인증기관 및 관련문제, 제4장에서는 외국의 전자서명 등을 포함하고 있다.[17]

2.2.4 독일의 멀티미디어법

독일은 멀티미디어 사회의 발전에 대비함과 동시에 인터넷 등의 이용에 관한 법적 체계를 정비하여 장래의 발전 기초를 다지기 위해서 멀티미디어법의 일부로서 "전자서명법(Gesetz zur digitalen Signatur)"을 1997년 6월 13일에 제정하여 1997년 8월 1일부터 시행하고 있다. 이 법은 디지털 서명을 하기 위한 법적 체계를 정비, 즉 디지털서명에 관한 기본적 요건을 정함과 아울러 인증기관과 인증서에 관하여 조직적 틀을 마련하는 것을 목적으로 하고 있다.

본 법은 디지털 서명과 관련하여, 제2조에서는 디지털 서명에 대한 정의, 제3조에서는 소관관청, 제4조에서는 인증기관에 대한 면허, 제5조에서는 증명서의 발행, 제6조에서는 인증기관의 교시의무, 제7조에서는 증명서의 내용, 제8조에서는 증명의 정지, 제10조에서는 문서화, 제12조에서는 데이터의 보호, 제13조에서는 당국의 감독, 제14조에서는 디지털 서명의 기술적 구성요

16) 한승철, 전자서명 및 인증기관의 법적문제, 저스티스 제31권 제1호, 한국법학원, 1998. 3, p.30.

17) A/CN.9/WG.Ⅳ/WP.76, 25 May 1998.

소 등에 대하여 규정하고 있다.

2.2.5 말레이시아 디지털 서명법

말레이지아에서 1997년에 제정된 디지털 서명법은 디지털 서명 자체와 디지털 서명의 이용을 규율하고 관련된 문제를 해결하기 위한 규정들을 포함하고 있다. 이 법은 7개부 92 개 조항으로 구성되어 있는데, 제1부에서는 총칙으로서 약칭과 용어정의, 제2부에서는 인증기관의 관리인과 인증기관의 허가, 제3부에서는 인증기관 허가의 요건, 제4부에서는 허가된 인증기관과 가입자의 의무, 제5부에서는 디지털 서명의 효력, 제6부에서는 보존장소와 타임스템프 서비스, 제7부에서는 기타 등을 규정하고 있다.

2.2.6 기타의 디지털 서명법

영국은 아직 전자상거래에 관한 법률을 제정하지는 않았으나, 통상산업부는 1996년 6월에 "공중통신망에 있어서의 암호화사용의 규제의사에 관한 백서"를 공표하고, 인터넷을 통하여 전송되는 정보의 무결성과 기밀성을 확보하기 위하여 노력하고 있다. 그 외에 이탈리아는 1997년에 전자문서와 디지털서명이 법적으로 효력이 있음을 규정하는 법률을 제정하였고, 덴마아크[18] 등은 디지털서명법(안)을 마련하고 있다.[19]

2.2.7 한국의 디지털서명 관련법률

현재 우리나라에서는 전자상거래 및 전자서명를 규율하는 일반적 법규가 없고, 관련 특별별, 즉 「무역업무자동화촉진에 관한 법률」을 비롯해 「공업 및 에너지 기술기반조성에 관한 법률」 「전산망보급확장 및 이용촉진에 관한 법률」 「화물유통촉진법」 등 20 여개 법률에서 전자서명, 전자문서의 효력, 전자문서의 효력발생시기, 도달 등에 관한 개별규정을 두고 있을 뿐이다.

한편, 전자상거래기본법과 전자서명법의 제정작업의 추진 결과, 산업자원부는 1998년 8월에 전자거래기본법(안)을, 정보통신부는 1998년 7월에 전자서명법(안)을 입법예고하였다. 전자거래기본법(안)은 민법, 상법 등 현행법의 원칙을 수정하는 규정, 전자거래의 안전을 위한 규정 및 전자거래촉진기반조성을 위한 규정으로 이루어져 있고, 전자서명법(안)은 전자서명과 관련하여 전자서명·전자문서의 효력, 인증기관, 인증서 등에 관한 문제를 다루고 있다. 따라서 전자상거래에 관한 통일적 규율과 전자서명에 관한 법률관계가 현재보다는 명확해 질 것으로 예상된다.[20]

III. 전자서명의 보안성

3.1 전자상거래 보안

3.1.1 전자상거래 보안의 필요성

전자상거래는 인터넷과 같은 개방통신망을 통하여 이루어지는 경향이 높아지고 있다. 개방통신망에서는 엄격한 접근 및 사용통제가 없으므로, 시스템에 저장된 메시지의 안전과 아울러 시스템을 떠난 메시지의 안전을 고려하지 않으

18) Draft Bill for Act on Digital Signatures etc.(16 Feb. 1998)

19) 손진화, 전자상거래에 관한 입법의 현황과 과제, http://my.netian.com/~profsjh/ec/syn.htm.

20) 손진화, 전게서.

면 안된다. 즉, 컴퓨터의 디지털 정보는 완전하게 동일한 다른 내용을 복제할 수 있기 때문에 위조, 변조가 용이하며, 일단 위조, 변조가 이루어진다면 그 식별이 불가능하므로 위조, 변조를 사전에 차단할 수 있는 기능을 보유할 필요가 있다. 이런 것들을 방지하기 위해 암호화 기법과 더불어 전자서명 등과 같은 추가적인 기술이 개발된 것이다.

3.1.2 전자상거래의 보안기법

1) 시스템보안(System Security)

시스템보안이란 컴퓨터시스템의 O.S.응용프로그램, 서버 등의 보안허점을 이용해 해커들이 침입해서 컴퓨터시스템을 이용하는 것을 방지하는 것을 말한다. 특히 WWW서버에서는 (1) CGI 프로그램과 관련된 부분과 (2) 디렉토리 리스팅을 보여주는 것 등이 주의를 요하는 부분이다. 특히 WWW서버를 Access한 로그파일에는 URL의 전부가 보여지므로 URL에 사용자명과 패스워드를 넣어서 사용할 경우, 그대로 로그에 남으니까 주의를 해야 한다.[21]

2) 자료보안(Data Security)

자료보안은 컴퓨터시스템 속에 들어 있는 정보자료가 불법 사용자에게 노출되지 않도록 보호하는 것을 말한다. 즉, 네트워크환경에서 정보를 전달할 때 일어날 수 있는 가로막기(Interruption), 가로채기(Interception), 수정(Modification), 위조(Fabrication) 등의 위험으로부터 정보를 안전하게 신뢰할 수 있게 전달하는 것이 목적이다. 여기에는 주로 암호화, 전자서명 등의 방식이 이용된다.

21) 권도균. WWW보안과 전자화폐

3.1.3 전자상거래의 보안기능

전자상거래는 하나의 거래이자 계약활동이므로 계약당사자간에 생길 수 있는 분쟁의 원인을 없애는 상호 확인절차가 필요하다. 서로 만나 계약할 경우에는 내용을 녹음하거나 펜이나 도장으로 서명할 수 있지만 네트워크에서는 불가능하다. 이에 등장하는 것이 바로 전자서명기술인데,[22] 암호학적 처리를 통해 기밀성(Confidentiality), 인증(Authentication), 무결성(Integrity), 부인방지(Nonrepudiation), 접근통제 등의 보안상의 기능을 수행한다.

1) 기밀성(Confidentiality)

기밀성은 정보 및 데이터에 대해 제3자의 접근을 암호화 등의 방법으로 봉쇄함으로써 거래의 내용을 노출시키지 않도록 하는 기능이다. 즉, 원문자체를 암호화하여 송신함으로써 제3자가 그 내용을 알지 못하게 하는 것을 말한다.

예를 들면 인터넷을 통해 신용카드 정보의 전송시 이를 중간에서 도청하는 행위, 또는 저장된 신용카드 정보 DB가 타인에게 노출돼 불법적으로 사용되는 것을 예상해 볼 수 있다. 또한, 신용카드의 정보뿐만 아니라 주문시 보내는 개인 신상에 관련된 정보(주소, 전화번호, 구매정보 등)가 불법적으로 유출되는 경우를 예상할 수 있다. 따라서 인터넷을 통하여 상인에게 전달할 때 암호화 하여 전송함으로써 도청자가 스니핑[23] 등에 의하여 그 내용을 얻어 내더라도

22) 권도균. 풀리지 않는 매듭 전자 상거래 보안과 전자지불. MicroSoftware. 1998. 3. p.246.

23) 해킹방법에는 Packet Sniffing과 IP Spoofing방법이 있다. 현재까지 인터넷 사용자가 주고받는 메시지가 알 수 없는 무단 침입자에 의해, 가로채고, 읽거나 혹은 심지어 변경하지 못하도록 보장하는 완벽한 안전장치는 없었다. 이러한 위협은 기술적으로 비인가된 네트워크 모니터링(Unauthorized Network Monitoring)

풀지 못하도록 할 필요가 있다.

2) 인증(Authentication)

인증은 거래에 참여하는 각 객체끼리 서로 상대방의 신분을 확인할 수 있도록 하는 기능으로 송신자와 수신자가 합법적인 사용자임을 증명할 수 있어야 한다.[24] 즉, 인증은 정보를 보내오는 사람의 신원을 확인하는 기능이다.

예를 들면, 상인의 입장에서 볼 때 어떤 고객이 상품의 구매대금으로 신용카드번호를 보내왔을 때 그 고객이 그 신용카드의 실제 소유자인지를 확인할 필요가 있으며, 또한 현금카드를 이용한 인출시에 현금자동지급기가 사용자가 입력한 비밀번호가 은행에 미리 등록해 놓은 비밀번호와 일치하는지 확인할 필요가 있다.

3) 무결성(Integrity)

무결성은 정보의 송수신과정에서 변조의 여부를 확인하는 기능으로서, 거래내용의 변조나 승인되지 않은 거래의 생성을 방지하기 위한 것이다.

예를 들면, 전자화폐의 금액을 불법적으로 변조하는 행위와 타인으로 신분을 위장해 악용하는 경우를 예상해 볼 수 있다.

4) 부인봉쇄(Non repudiation)

부인봉쇄는 정보의 송수신 여부의 확인 및 송수신사실의 부인을 방지하는 기능이다. 이는 이미 성립된 거래에 대한 부당한 번복을 방지하기 위한 기능으로서 송신부인방지와 수신부인방지로 구분된다.

송신자가 송신한 사실을 부인할 때 송신자만이 알 수 있는 비밀번호로 만들어진 전자서명이 첨부되어 있으면 특별한 사정이 없는 한 송신자가 그 전자문서를 작성하고 발신하였다고 간주할 수 있는 기능을 말한다.[25]

예를 들면, 매수인은 물건을 주문하고 대금을 지불했으나 매도인은 그러한 주문을 받은 적이 없으며 더 나아가 대금을 받은 적이 없다고 하는 것처럼, 그 거래를 부인하는 행위가 있을 수 있다.

5) 접근통제(Access control)

접근통제는 자료나 서비스 이용에 대한 해커 등의 불법적 접근을 방지하기 위한 기능이다. 이 기능은 보안기법이 수행하는 기능과 전자서명이 수행해야 하는 기능이 일치하지 않기 때문에 전자서명이 수행해야 하는 기능과는 무관하다.

3.2 전자서명에 이용되는 암호화방법

전자문서의 교환과정에서 보안기능을 수행하고 있는 보안기법을 예시하여 보면, 사용자 ID와 패스워드방법[26], 대칭적 암호화방법(Symmetric Key Encryption mechanism), 비대칭적 암호화방법(Asymmetric Key Encryption mecha-

---

혹은 Packet Sniffing이라 부른다: Ravi Kalakota & Andrew B. Whinston, Electronic Commerce, Addison-Wesley, 1997, p.136.
IP Spoofing은 해커가 머물러 있는, 또는 단순히 악용하고자 하는 호스트의 IP 어드레스를 바꾸어서 이를 통해 해킹을 하는 것이다: Anup K. Ghosh, E-Commerce Security Weak Links, Best Defenses, Wiley Computer Publishing, 1998, pp.109-114.

24) 송의진 · 박상봉, 전자상거래 보안기술, 정보통신연구, 1998. 3, p.12.

25) 남광, 전게서, p.89.

26) 이 방식은 패스워드가 대부분 4자리 내지 8자리 정도의 숫자 또는 문자로 구성되어 있기 때문에 전문해커는 물론 아무추어 수준의 해커에게도 그 패스워드가 쉽게 노출될 수 있다. 따라서 인증기능, 접근통제기능, 부인봉쇄기능을 완벽하게 수행할 수 없게 된다.

nism: 이를 공개키 암호화방법이라고도 한다.) 등이 있다.

보안을 위한 암호화기술[27]은 암호화방법과 이를 다시 풀어내는 복호화[28]방법에 사용되는 키의 적용방식에 따라 대칭적 암호화 알고리즘과 비대칭적 암호화 알고리즘으로 분류한다. 대칭적 암호화방식에서는 암호화에 사용하는 키와 복호화에 사용하는 키가 동일하며, 비대칭적 암호화방식에서는 이 두가지 키가 다르다. 비대칭적 암호방식에서는 보통 이중 한가지 키를 공개하고 한가지 키는 개인이 보관하는 방식을 취하는데, 공개하는 키를 공개키(Public Key) 개인이 보관하는 키를 개인키(Private Key)라고 한다.[29]

대칭적 암호화 방식의 대표적인 알고리즘으로는 DES(Data Encryption Standard)가 있으며, 비대칭적 암호화방식에는 RSA(Rivest, Shamir, Adleman)가 있다.

여기에서는 전자서명의 경우에 주로 이용되는 암호화방법인 대칭적 암호화방법과 비대칭적 암호화방법에 대하여 설명하고자 한다.

3.2.1 대칭적 암호화방법(Symmetric Key Encryption mechanism)

1) 비밀키암호화기법

대칭적 암호화방법은 송신자와 수신자가 동일한 키를 공유하면서 이를 이용하여 암호화와 복호화를 하는 방식이다. 즉, 자료를 암호화하는 키와 암호화된 자료를 복호화하는 키가 동일한 암호화 방식으로서, 일반적으로 많이 사용되고 알려진 암호화방식이며, 비밀키 암호화 방식(Secret-key Algorithm, Private-Key)이라고도 한다.

암호키로부터 복호키를 계산해 낼 수 있거나, 반대로 복호키로부터 암호키를 계산해 낼 수 있을 때 이 암호화 알고리즘을 Symmetric Algorithm이라고 부른다. 대부분의 Symmetric Algorithm에서는 암호키와 복호키가 동일하다.[30]

이방식의 장점은 인증성, 기밀성, 무결성, 부인봉쇄기능, 접근통제기능을 모두 수행할 있으며, 암호화와 복호화가 빠르다는 점, 여러 가지 다양한 암호화기법이 개발되어 있다는 점이다. 이 방식의 단점은 본인 외에 거래상대방도 그 비밀번호를 알고 있으므로 거래상대방이 배신행위를 할 경우 그 대처방안이 없다는 약점이 있으며, 복수의 사용자가 동일한 자료를 사용할 때 키의 공유문제가 발생한다.

2) DES알고리즘

대칭적 암호화 방식의 대표적인 알고리즘으로는 현재 가장 잘 알려지고 인터넷을 통화여 폭넓게 이용되고 있는 암호화제도인 DES(Data Encryption Standard)가 있다. DES암호화방식은 상업적으로 널리 이용된 최초의 비밀키방법으로서, 1974년 미국 통상부의 공식권유에 의하여 IBM이 국가표준국(National Bureau of Standards: 현재의 국가기술표준연구소(NIST))과의 계약에 따라 개발한 것으로서, 1977년에 미국의 연방표준으로 채택되었고, 1981년에는 금융산업 표준으로 채택되었다.

27) 암호화(Encryption)는 자료의 기밀성(Confidentiality)을 보장하는 방법으로서, 원래의 자료(Message)와 그것을 암호화하는 키와 암호화된 자료(Crypted Message)와 그 암호화된 자료를 원래의 자료로 복원시키는 키 등으로 구성된다.

28) 암호문(ciphertext)을 평서문(plaintext)으로 변환 시키는 것을 말한다.

29) 김기병, 전자상거래를 위한 지불 방법 및 보안, 정보과학회지, 1998. 5.

30) Ravi Kalakota, Andrew B. Whinston, op. cit., p.138.

DES는 정보의 암호화와 해독에 64bits의 동일한 키를 사용한다. 정보를 교환하는 양측이 암호화에 사용된 키를 상대방에게 건네주는 방식이다. 그런데 거래의 상대방이 불특정 다수일 경우에는 방대한 고객의 수만큼 키를 만들어 나누어 주어야 하고 이를 각각의 고객과 연관하여 유지하여야 하는데 이는 실제적으로 매우 비효율적이다.[31]

즉, DES는 56비트 키를 가지고 64비트 블록으로 작동되며, 각 비밀키에 대하여 별개의 알고리즘이 생성된다. DES는 많은 양의 문서 또는 암호화를 위하여 비교적 신속하게 잘 작동된다. DES는 triple-DES와 구별하기 위하여 single-DES라고 불린다. Triple-DES 암호화는 두 개의 키가 사용되어 암호화, 복호화, 암호화라는 연속 조작으로 구성된다. DES가 통신에서 사용될 때에는 발신인과 수신인 양자가 동일한 비밀키를 알고 있어야 한다. 또 DES는 하드디스크에 암호화된 형태로 파일을 저장하는 단일사용자 암호화에도 사용될 수 있다. 그러나 다수이용자 환경에서는 비밀키의 보급이 곤란하다. 이를 해결하기 위하여 개발된 것이 공개키암호화 방법이다.[32]

3) 대칭적 암호방법을 이용한 전자서명

대칭적 암호방법을 이용한 전자서명을 현재 실무에서 사용되고 있는 프로그램의 예를 들어 설명하기로 한다.[33]

우선, 송신자와 수신자는 각자의 컴퓨터에 같은 종류의 대칭적 암호 프로그램을 설치한 다음 각자의 비밀번호(인증값이라고도 함, 10자리 숫자)를 가진다. 송신자는 전자문서(A)를 작성한 후 자신의 비밀번호(X)와 상대방의 비밀번호(Y)를 입력한다.

그러면, 프로그램은 우선 그 전자문서를 이루고 있는 코드의 숫자값(A*: 컴퓨터의 입장에서 보면 전자문서도 숫자의 나열에 불과한데 이를 코드의 숫자값이라고 표현하였다)과 X, Y에 대하여 암호 알고리즘을 적용하여 이떤 결과값 10자리 숫자를 만드는데 이것을 유사 전자서명(S)이라 한다. 암호알고리즘의 원리를 대충 설명하면, A*, X, Y를 각 여러번 더하고, 빼고, 나누고, 곱하고 하여(대충 설명하면 그렇다는 것임) 결국 10자리 숫자를 만들어내는데 그것이 유사 전자서명인 것이다.

그런 다음 송신자는 자신이 만든 전자문서(A)와 유사전자서명(S)을 함께 수신자에게 발송한다.

송신자가 발송한 전자문서와 이에 부착된 유사 전자서명(S)이 수신자의 컴퓨터에 도착하면 수신자는 자신의 비밀번호(Y)와 상대방의 비밀번호(X)를 입력한다.

그러면 프로그램은 도착된 전자문서(B)에 대하여(송신자가 발송한 전자문서가 중간에 변조된 사실이 없이 그대로 왔다는 보장이 없으므로 현재 도착된 전자문서를 A가 아닌 B라고 설정한 것임) 그 전자문서(B)를 이루고 있는 코드의 숫자값(B*)과 X, Y에 대하여 송신자의 프로그램과 동일한 내용의 암호 알고리즘을 적용하여 어떤 결과값 10자리 숫자(S*)를 만든다.

그 다음 프로그램은, 도착한 유사 전자서명(S)과 위 S*를 대조하여 틀림이 있는지를 비교한다.

대조결과 S와 S*가 동일하면 송신 전자문서(A)와 수신 전자문서(B)가 동일하다는, 즉 내용

31) 김기병. 전게서.
32) 손진화. 전자서명의 법적 과제. http://my.netian.com/~profsjh/ec/digsig.htm.
33) 남광. UNCITRAL과 전자상거래. 데이터베이스 월드, 1997. 11. p.30.

에 변조가 없었다는 사실을 확인할 수 있는 것이다.

만일 송신자의 전자문서에 한자라도 수정을 가하였다면 문서의 고유 숫자값이 달라질 것이고, 따라서 위 10자리 숫자 결과값이 서로 틀리게 될 것이다.

3.2.2 비대칭적 암호화방법(Asymmetric Key Encryption mechanism)

1) 공개키 암호화기법

비대칭적 암호화방법은 암호화와 복호화에 쓰이는 키가 서로 짝을 이루어 각각 하나의 키로 암호화된 것을 그 짝으로 복호화 할 수 있는 알고리즘이다. 즉, 암호화를 위한 키와 복호화를 위한 키라는 한쌍의 키를 사용하는 암호화 방식으로서, 공개키 암호화방식(Public-Key Algorithm; Public-Key)이라고도 한다. 이때 암호화에 사용되는 키는 공개키(Public Key)로서 외부에 공개되고, 복호화에 사용되는 키는 개인키(Private Key)로서, 외부에 노출되지 않도록 비밀리에 보관해야 한다. 개인키는 대칭적 암호화 방법에서의 비밀키(Secret Key)와는 구별된다.

이 방법에서는 암호키와 복호키가 서로 다르며, 또한 암호키로부터 복호키를 계산해낼 수 없다. 한쌍의 키 중 복호키(개인키)는 사용자의 시스템내에 비밀히 보관되고, 암호키(공개키)는 공개되어 저장소(depositary)에 보관되며 누구나 검색할 수 있다. 즉, 아무나 암호키(공개키)를 이용하여 어떤 내용을 암호화 할 수 있지만, 오직 해당 복호키(개인키)를 가진 사람만이 그 암호문을 복호할 수 있다.

이 방식은 암호화, 복호화 속도가 대칭적 암호화방법에 비해 약 1000배 정도 느리고 많은 양의 자료를 암호화, 복호화 하기가 불편하다는 단점을 가지고 있다. 그러나 키를 상대방에 보내는 것에 보안상의 허점이 없다는 점과 정보의 기밀 유지 이외에 다른 목적으로도 사용될 수 있다는 점, 즉 인증성, 기밀성, 무결성, 부인봉쇄 기능, 접근통제기능을 모두 수행할 수 있으며 본인이외는 아무도 그 비밀번호를 알 수 없으므로 완벽한 보안기능을 수행한다. 이 방식에서 비밀키는 그 보유자만이 보관하고 있고, 이에 의하여 암호화된 문서는 이에 대응하는 공개키에 의해서만 복호화될 수 있기 때문에 문서작성자의 신원을 증명하고 메시지의 진정성과 무결성을 확보할 수 있다. 따라서 전자서명의 방법으로서 가장 유용하므로 사실상 미래의 전자서명방식으로 사용이 확실하게 된다.

2) RSA알고리즘

비대칭적 암호화 방식의 대표적인 알고리즘으로는 RSA(Reversible Public-key Cryptosystem)방식이 있다. RSA는 전환형 공개키암호화제도로서, 1977년 MIT의 세 젊은 교수 Ronald Rivest, Adi Shamir, Len Adleman 세사람에 의해 만들어진 Public Key암호화방식이다.

RSA알고리즘에서는 개인이 보관하는 개인키와 공개해 놓는 공개키의 두 개의 키를 이용하며, 공개키로 암호화한 문장은 공개키에 대응하는 개인키를 이용하여 해독할 수 있으며, 반대로 개인키로 암호화할 경우, 대응되는 공개키를 이용하여야만 원문을 재생해낼 수 있다.[34] RSA 계산법은 공개모듈(public modulus)이라고 불리는 수치를 사용하는데, 이 모듈은 공개키의 일부를 구성한다. 공개모듈은 비밀키의 일부를 구성하는 두 개의 素數(prime number)를 곱하여

34) 김기병, 전게서.

얻어진다. RSA의 안전성은 커다란 소수를 발견하는 것은 상대적으로 쉽지만 그러한 두 수의 곱의 결과를 인수분해하는 것은 어렵다는 사실에 근거한다. 그러한 소수가 충분히 큰 경우 인수분해는 커다란 처리과정을 밟아야 하기 때문이다.[35]

RSA이외에도 Diffie-Hellman Key Exchange 메카니즘과 LUC가 있는데, Diffie-Hellman 메카니즘은 1976년 스탠포드대학의 Whitfield Diffid와 Martin Hellman가 발표한 논문에 의해 만들어진 것으로서, 이 방식은 고전적인 Public Key 암호화방식으로 취급되지만, 아직까지도 임시키를 교환하는 메커니즘에 많이 사용되고 있다. 또한 LUC는 1993년 뉴질랜드에서 만들어진 새로운 public Key암호화방식으로서, lucas sequence 가운데 큰 정수를 이용해 public키와 Private 키를 생성하는데, RSA보다 효율이 더 좋은 암호화방식으로 알려지고 있다.

3) 비대칭적 암호방법을 이용한 전자서명

비대칭적 암호방법을 이용한 전자서명의 예를 설명하면 다음과 같다.[36]

송신자가 전자문서(A)를 작성하면 프로그램은 그 전자문서에 대하여 해쉬 알고리즘(Z)을 적용시켜 메시지 다이제스트(A*)[37]를 만든다.

그 다이제스트(A*)에 송신자의 비밀키(P)를 입력하면 암호알고리즘이 작용하여 어떤 기계어를 만드는데 그것이 전자서명(S)이다.

송신자가 전자문서(A)와 이에 따른 전자서명(S)을 송신하여 수신자의 컴퓨터에 도착하게 되면 수신자 컴퓨터의 프로그램은 도착 전자문서(B)에 대하여 송신자와 동일한 내용의 해쉬 알고리즘을 적용시켜 그 문서에 고유한 다이제스트(B*)를 만든다.

이어 전자서명(S)에 대하여 송신자의 비밀키(P)에 대응하는 공개키(P*)를 작용시켜 전자서명에 담겨있는 송신자의 다이제스트(A*)를 꺼낸다. 즉, 쉽게 말하여 공개키는 비밀키로 암호화되어서 본래의 메시지에 부착되어온 전자서명(암호화된 메시지다이제스트)를 해독하는데 쓰이는 것이다.

송신자의 전자서명안에 담겨있던 다이제스트(A*)와 수신자가 만든 다이제스트(B*)를 비교하여 양자가 일치하면 위조, 변조가 없었던 것으로 확인해 준다. 이때 공개키가 송신자의 비밀키에 대응하는 짝이 아닐 경우에는 위 다이제스트는 일치하지 않게 된다.

35) 손진화, 전게서.

36) 남광, 전게 UNCITRAL과 전자상거래, pp.30-31.

37) 메시지 다이제스트(Message Digest)는 암호화 방법은 아니라, One-way hash 함수를 이용하여 주어진 정보를 일정한 길이 내의 아주 큰 숫자(해쉬값)로 변환해 주는 것이다. 이 함수는 One-way이기 때문에 주어진 정보로부터 해쉬 값을 만들어 낼 수는 있어도, 반대로 이 해쉬값으로부터 원래의 정보를 복구해낼 수는 없다. 다만, 정보와 함께 그 정보의 해쉬값을 받은 사람의 받은 정보의 해쉬값을 구한 후, 정보와 함께 전달된 해쉬 값을 비교함으로써, 그 값이 같다면 정보의 전달 중에 정보가 변경되지 않았음을 (100%는 아니지만 거의 확실하게) 확인할 수 있으며, 만약 그 값이 다르다면 정보가 전달 중에 어떻게 든 변경되었음을 알 수 있다. 물론, 이 해쉬값은 암호화 알고리즘에 의해 암호화되어 전달되어야 한다. 그렇지 않다면, 정보를 중간에서 변조하는 사람이 정보를 변조한 후 그 변조된 정보의 해쉬값과 함께 보낼 수 있기 때문에 해쉬값이 제대로 기능하지 못하게 된다: Anup K. Ghosh, E-Commerce Security Weak Links, Best Defenses, Wiley Computer Publishing, 1998. Canada.

Ⅳ. 결론

전자상거래의 경우에 이용되는 전자문서의 교환과정에서 보안기능을 수행하고 있는 보안기법 중 전자서명과 관련되는 것으로는 대칭적 암호화방법(Symmetric Key Encryption mechanism)과 비대칭적 암호화방법(Asymmetric Key Encryption mechanism)으로 분류되고, 대칭적 암호화 방식에는 DES(Data Encryption Standard), 비대칭적 암호화방식에는 RSA(Rivest, Shamir, Adleman)가 대표적인 알고리즘이다.

우선 대칭적 암호방법과 비대칭적 암호방법을 비교해 볼 때, 대칭적 암호방법은 전자문서에 의한 거래 이전에 비밀키(비밀번호)를 공유하여야 하기 때문에 전자문서의 위조·변조를 방지하는 것은 가능하지만 상대방이 배신하는 경우에는 속수무책이다. 또한 거래상대방이 불특정다수일 경우에는 비밀키 관리와 비밀키 전달이 어렵거나 불가능하여 진다는 문제점이 제기된다. 한편, 비대칭적 암호방법은 매우 복잡한 복호 알고리즘을 사용하기 때문에 자료 처리 속도가 매우 느리며, 복잡한 암호 알고리즘을 수행하기 위하여는 고성능의 컴퓨터를 사용해야 한다. 이에 따른 기존의 컴퓨터 설비의 대체에 따른 경제적 비용의 지출을 야기시키게 된다는 문제점도 있다. 그러나 수신자는 송신자의 공개키만 알 수 있고 그 공개키는 송신자의 비밀키(비밀번호)를 추출하는 것이 불가능하고, 송신자가 사용한 비밀키를 확인하는 데에만 사용하도록 되어 있으므로 송신자 비밀키의 비밀이 완전하게 보장될 수 있다. 따라서 대칭적 암호방법보다는 비대칭적 암호방법이 전자상거래에 보다 적합한 방법이라는 평가를 받고 있는 실정인 것이다.

한편, 전자서명의 암호화방법에 관한 문제이외에, 전자서명은 전자문서, 전자영수증, 대금결제 서명 및 상호인증 등 전자상거래의 거의 모든 영역에서 사용되므로, 전자상거래 활성화와 소비자 보호 및 각종 분쟁해결을 위해서는 전자서명에 대한 법적 기반이 마련되어야 할 것이다. 또한 전자서명의 안전성 확보와 법적효력을 부과하기 위해서는 공개키 관리체계와 인증기관의 운영에 관한 엄격한 기준의 설정 및 이러한 기준에 의거한 인증기관의 승인 및 감사체계가 필요하다 할 것이다.

참고 문헌

권도균, WWW보안과 전자화폐

권도균, 풀리지 않는 매듭 전자 상거래 보안과 전자지불, MicroSoftware, 1998.3.

김기병, 전자상거래를 위한 지불 방법 및 보안, 정보과학회지, 1998. 5.

남광, UNCITRAL과 전자상거래, 데이터베이스 월드, 1997. 11.

남광, UNCITRAL과 전자상거래, 통상법률, 법무부, 1997. 8.

손경한, 전자상거래의 법적과제, 인권과 정의, Korean Bar Associatuon, 1997. 10.

손진화, 전자상거래에 관한 입법의 현황과 과제, http://my.netian.com/~profsjh/ec/syn.htm.

손진화, 전자서명의 법적 과제, http://my.netian.com/~profsjh/ec/digsig.htm.

송의진 · 박상봉, 전자상거래 보안기술, 정보통신 연구, 1998.3.

주석진, 인터넷에 기반을 둔 전자상거래(EC)의 활성화방안에 관한 연구, 산업연구 제8집, 경기대학교, 1997.

한승철, 전자서명 및 인증기관의 법적문제, 저스티스 제31권 제1호, 한국법학원, 1998.3.

Anup K. Ghosh, E-Commerce Security Weak Links, Best Defenses, Wiley Computer Publishing, 1998.

D. Chaum & E. Van Heyst, Group Signatures, Advances in Cryptology-EUROCRYPT '91, Springer-Verlag, 1991.

D. Chaum & H. Van Antwerpen, Undeniable signatures, Advances in Cryptology-CRYPTO '89, Springer-Verlag, 1990.

D. Chaum, Blind Signatures for Untraceable Payment, Advances in Cryptology-CRYPTO '82, Springer-Verlag, 1983.

D. Chaum, Designated Confirmer Signatures, Advances in Cryptology-EUROCRYPT '94, Springer-Verlag, 1994.

E. Van Heyst & T. P. Pederson, How To Make Efficient Fail-stop Signatures, Advances in Cryptology-EUROCRYPT '90, Springer-Verlag, 1991.

Electronic Data Interchange and Paperless Trade, 3rd. ed., Blenheim Online Publications London, 1990.

Ravi Kalakota & Andrew B. Whinston, Electronic Commerce, Addison-Wesley, 1997.

A Study on the Transaction Security of Electronic Signature in the Electronic Commerce

Soon-Hwan Jeon*

Abstract

In this paper, we discussed various securities of electronic signature. Merchants or sellers must address all Internet security concerns. Security technology may secure the routes of Internet communication, but it does not protect consumers from people with whom they might choose to do business.

To protect consumer information, they must maintain physical security of their servers and control access to software passwords and private keys. Techniqaues such as secret and public-key encryption and digital signatures play a crucial role in developing consumer confidence in electronic commerce.

* School of the Economics and Commerce, Joong-Bu University.