정보학연구 제1권 제1호 1998년 3월(pp. 173~188)

전자결제의 보안성에 관한 연구

홍선의
경원전문대학 무역과 강사

요 약

최근 인터넷을 이용한 전자상거래가 점차 발전됨에 따라 고객의 서비스 구매에 따르는 전자 결제의 이용이 점차 늘어가고 있는 추세이다. 그러나 전자결제는 온라인상에서 이루어지는 활동이라는 점에서 많은 문제를 내포하고 있다. 온라인 신용카드와 전자화폐 그리고 전자수표로 대변되는 전자결제의 수단들은 흔히 해커라 불리어지는 전자상거래의 비주체들에 의하여 오용되어지고 그로 인해 많은 피해가 발생할 우려가 있다.
본 고에서는 전자상거래시의 대금결제 수단인 전자결제의 종류와 문제점에 대하여 알아보고 그러한 문제점을 극복할 수 있는 방법들에 대하여 제시해 본다.

Ⅰ. 서론

최근 정보통신기술이 발달과 인터넷 이용의 폭발적인 신장세에 편승하여 인터넷을 통한 전자상거래(EC ; Electronic Commerce)가 새로운 경제활동으로 부각되고 있다. 따라서 많은 기업들이 전자상거래에 대해 깊은 관심을 보이고 있으며 실제로 전자 상거래를 통한 기업활동을 영위하고자 하고 있다.

이는 전자 상거래가 가진 여러 가지 장점들에 기인한 것으로서 이를 살펴보면 다음과 같다. 첫째, 운송비·점포유지비·유통마진 절감 등을 통한 전면적 가격파괴가 가능해짐에 따른 가격 경쟁력을 쉽게 확보할 수 있다는 점이다.

논문접수일 : 97년 10월 게재확정일 : 98년 2월

둘째, 구매자에 대한 정보관리가 용이하므로 철저한 소비자 관리가 이루어지고 쌍방향 마케팅이 가능해짐에 따라 상품의 가격·성능·사양 등의 비교를 통한 구매가 용이해짐에 따라 적극적인 마케팅의 구사가 가능하다는 점이다.

셋째, 기존 상거래가 갖고 있는 물리적·시간적·공간적 한계를 극복하였다는 점과 마지막으로 네트웍을 통한 온라인 대금결제로 편리성이 향상되었다는 것을 들 수 있다.

이러한 여러 가지 편리성과 장점에도 불구하고 전자상거래에 대한 불신이 소비자 및 판매자 양쪽에 모두 상존하고 있는게 현실이다. 이러한 전자 상거래의 위험에 대한 첫째 이유는 바로 상거래가 컴퓨터에 의해 이루어지기 때문이다. 컴퓨터 환경이란 곧 디지털 환경을 말한다. 또한 디지털 환경이란 모든 세계가 0과 1로 가장 규격화된 세계이다. 즉 모든 것이 구분할 수 없

는 동일한 모양을 지녀 얼마든지 복제하거나 모조할 수 있기 때문에 소비자와 판매자 양쪽이 모두 불안을 느끼게 되는 것이다 .

둘째 이유는 전자상거래는 네트 워크 환경에서 이루어지기 때문에 고객이 직접 오지 않아도 거래는 이루어지므로 당사자를 확인할 마땅한 방법이 없다는 것이다.

셋째, 전자상거래는 금융정보, 즉 사용자의 신용카드 번호와 비밀번호, 은행계좌 번호, 직불카드 번호, 비밀번호 등 '결제'와 관계되는 정보가 노출되기 때문에 문제가 심각하다는 점이다.

이외에 물건 배달과 지불간의 시간·공간적 격차, 전자상거래를 위한 보안 기술의 미비 등을 들 수가 있다.

본 고에서는 원활한 전자상거래 활동에 저해가 되는 여러 가지 문제점 중에서도 전자결제의 안전성과 신뢰성을 확보하는 방안에 관하여 고찰해보고자 한다.

II. 전자결제의 의의 기능

2.1 전자결제의 의의

전자결제[1]는 전통적 화폐의 신용에 기반을 두고 일반적인 화폐에 내재되어 있는 불편함을 제거시키기 위해 전통적인 화폐의 기능에 원격지 이송에 따른 통신기능, 휴대 및 보관관리의 편의기능, 위조방지 등을 추가한 새로운 전자적 결제방법이다.

인터넷의 등장과 이를 이용한 전자상거래의 비약적인 발전은 기존의 지급결제 수단에다 새로운 상거래 활동에 적합하지 않음을 인식하기 시작하였다. 따라서 전자상거래를 이용하는 구매자와 판매자는 새로운 결제수단을 강구하기에 이르렀고 그것은 계좌이체, 대량지급이체, 타행환거래 등과 같은 초보적인 전자결제 방법들을 발전시켜 전자수표, 전자화폐, 온라인 신용카드 등과 같은 전자결제수단들을 사용하기에 이르렀다. 이는 사이버상에서 매매가 이루어지고 구매자와 판매자가 대면하지 않고서도 거래가 이루어짐으로 인해 전통적인 수단을 통한 결제가 어려워지게 되었고 격지간의 거래에서 발생되는 금융비용을 절감하기 위한 이유도 한 몫을 한 것이었다.

인터넷상에서의 유·무형의 재화는 어떠한 물리적인 지원기술을 이용하지 않고서도 거래되고 있으며, 소비자들은 웹에 기초한 카탈로그를 이용하여 상품을 선택할 수 있게 되었으며, 대금결제에 있어서도 전통적인 결제방식과는 다른 새로운 형태의 방식이 이용되게 되었다.

2.2 전자결제의 기능

2.2.1 전자결제의 순기능

전자결제시스템은 단순히 상품을 구매하고 그 대금을 결제하는 방법이 온라인을 통해 이루어진다는 점 말고도 여러 가지 기능을 갖고 있다. 그 기능을 살펴보면 구매자 측면과 판매자 측면 그리고 금융기관과 발행기관의 측면에서 살펴볼 수가 있다.

1) 전자화폐와 전자결제시스템은 같은 개념이나 혹자는 전자화폐를 전자지불시스템의 하위의 개념으로 보는 경우도 있다. 이 경우 전자화폐는 전자현금(electronic money, electronic cash)의 의미로 해석한다. '금융정보화추진분과위원회'에서 정의한 전자화폐의 의미는 전자지불시스템의 분류에서 전자현금을 기반으로 한 지불시스템이다.

먼저 구매자 측면을 살펴보면 대금을 결제하는데 따르는 현금의 보유가 필요없게 되어 편리성이 증대되며 이에 따라 원격지의 판매자와의 거래가 용이해지는 점을 들수가 있다.

둘째, 판매자 측면을 살펴보면 구매자로부터의 대금결제의 신속성 및 확실성으로 인해 물품 판매후 결제에 대한 안정성을 획득할 수 있다.

셋째, 금융기관은 고객이 사용하기에 적절한 곳에 배치하고 운용하고 있는 CD/ATM 설치에 비해 설비투자 비용이 감소하여 경영상의 비용을 절감하고 운영의 합리화를 도출해 낼 수가 있다.

넷째, 발행기관이 전자결제에 사용되는 전자화폐를 발행할 경우 은행예금의 일부가 전자화폐의 형태로 사용됨에 따라 전자화폐가 최종 결제되기까지 자금을 보유하는데 따르는 수익인 부유자금 운용수익(float interest)이 발생할 수가 있다.

또한 전자결제에 따르는 관련 기기 및 소프트웨어 시장이라는 새로운 신규시장이 창출될수 있다.

2.2.2 전자결제의 역기능

앞에서 살펴본 바와 같이 전자결제는 순기능만이 발생하게 되는 것은 아니다.

먼저 통화정책의 불안을 들 수가 있다. 이는 시중통화량의 증가 측면보다는 국제간의 자금이동이 파악이 곤란하게 되므로 외환관리 및 통화관리에 애로를 겪게 될 수가 있다는 점이다.

둘째로는 전자화폐의 장점으로 꼽히고 있는 익명성으로 인해 탈세와 돈세탁 등 각종 범죄에 악용될 가능성이 있다는 점이다.

세 번째로는 개인의 프라이버시 및 사생활 침해 가능성이 존재하게 된다는 점을 꼽을 수 있다.

III. 전자결제의 유형과 종류[2)]

3.1 전자결제시스템의 유형

전자결제시스템은 내부적인 메커니즘에 따라 크게 결제브로커시스템(Payment Broker)과 전자화폐(Electronic Money) 시스템의 두가지로 구분된다[3)]. 결제브르커시스템은 독립적인 신용구조는 아니며 신용카드나 은행의 계좌를 이용해 네트워크상에서 지불을 하도록 연결시켜 주는 구조로 되어 있으나, 현재 신용카드를 이용한 거래의 관행이 자리잡혀있기 때문에 많이 이용하고 있는 현실적인 전자결제시스템이다.

전자화폐시스템은 이론적으로 그리고 실험적으로 많이 연구되고 있으며, 전자결제시스템이 지향하는 궁극적인 목표 시스템이기는 하나 아직 실용화 단계는 아니다. 전자화폐시스템은 선불카드, 직불카드를 응용하거나 순수한 디지털 화폐를 응용하는 시스템이다. 이러한 시스템을 뒷받침할 만한 기술적인 준비는 상당히 진전되었지만 현재 금융과 사회적 관습 그리고 통화량과 경제에 미치는 영향 등 사회 경제적인 관점에서는 아직 깊은 연구가 이루어지지는 않고 있다.

3.2 결제브로커시스템의 종류

3.2.1 온라인 신용카드

전자적 환경에서 안전한 신용카드지급을 위하

2) 이 장은 정보통신연구원에서 간행된 정보사회에 대비한 일반법(II)에 실린 손진화의 '새로운 전자지급제도의 법률문제와 입법론' 중 pp.251-258을 본인의 의도에 맞게 첨가 삭제하여 수정 편집한 것 임.

3) 이남용·김대식, 전자상거래시스템의 아키텍처에 관한 연구, 국방정보체계연구소, 1997.

여 고안된 방법으로는 암호화신용카드지급과 등록신용카드지급을 들 수 있다.

1) 암호화 신용카드

암호화 신용카드지급은 안전한 신용카드거래를 위하여 처음 고안된 방법으로서, 인터넷 등의 통신망을 통한 전송중에 프라이버시를 보호하기 위하여 암호화기법을 사용하여 카드번호를 암호화하는 방법에 의하는 지급방법이다.(secure credit-card payment). 이 방법은 거래의 진정성을 확보하기 위한 디지털서명(digital signature)의 사용과 결합된다. 많은 은행과 신용카드회사들이 이 방법을 개발하고 있는 중이다. MasterCard[4]와 Visa International[5]이 공동으로 개발한 SET[6] 프로토콜(Secure Electronic Transaction Protocol)은 그 대표적인 예이다.

2) 등록신용카드

등록 신용카드 지급은 상인들을 신용카드거래를 처리하는 제3기관의 회원으로 가입하게 하고, 카드보유자로 하여금 신용카드번호를 제3기관에 등록하여 특별한 계좌번호(account number : ID number)를 얻게 하는 방법에 의한 지급방법이다.(registry credit-card payment) 여기에서 계좌번호는 카드보유자가 회원상인과 거래를 할 때 카드번호 대신 사용될 수 있다. 다만 이 방법은 고객과 상인 양자가 거래를 위하여 동일한 서비스기관에 등록하여야 한다는 문제가 있다.

같은 범주에 속하는 것으로, CyberCash사[7]는 카드 보유자가 PC에서 사이버캐시사에 의하여 무료로 제공되는 소프트웨어를 사용하여 카드번호를 암호화하고 그 정보가 상인에게 암호화한 형태로 전송되는 방법을 개발한 바 있다. 상인은 카드보유자로부터 주문을 받으면 필요한 카드수권을 위하여 전송하고 수권을 받으면 상인에게 회송하며, 상인은 카드보유자와 함께 거래를 완성한다.

3.2.2 전자수표

1) 전자수표의 의의

전자수표[8]는 실세계의 수표를 그대로 인터넷상에서 구현한 것으로 전자 수표의 사용자는 은행에 신용 계좌를 갖고 있는 사람으로 제한한다. 전자수표는 기본적으로 발행인이 거래은행에 대하여 그의 계좌로부터 다른 사람의 계좌로 자금을 이체하라고 지시하는 메시지이다. 전자수표는 직접 은행에 전송되지 않고 수취인에게 전송되며, 수취인은 여기에 배서하여 양도할 수 있다. 전자수표에서는 은행의 공개키를 사용하여 계좌번호를 암호화함으로써 사기를 방지할 수 있다. 또 지급인, 지급은행과 은행계좌의 진정성을 확보하기 위하여 디지털서명이 사용될

4) http://www.mastercard.com 참조.

5) http://www.visa.com 참조.

6) SET에서는 신용카드거래의 참여자를 Cardholder, Issuer, Merchant, Acquirer, Payment Gateway, Brand, Third Parties 로 정의하고 있다. Issuer는 brand와 계약을 맺고 cardholder에게 신용카드를 발급하는 은행이다. Acquirer는 merchant가 가맹점으로 가입한 기관이고 merchant의 계좌를 갖는다. 우리나라에서는 은행과 신용카드 회사가 issuer와 acquirer의 역할을 하고 있다. Payment Gateway는 신용카드 지불을 중계하는 서버로서 third party에 둘 수도 있고 issuer나 acquirer가 운영할 수도 있다. Payment Gateway에서는 지불 요청, 승인, 지불 정보 확인 등의 작업을 한다.

7) 또한 CyberCash사에서는 소액의 지불을 신용카드를 이용하여 결제를 가능하게 해 주는 CyberCoin 서비스를 시작하고 있다. (http://www.cybercash.com)

8) 대표적인 전자 수표 시스템으로서는 현재 개발중인 캘리포니아 대학의 NetCheque 와 NetChex(http://www.netchex.com) 그리고 영국의 가상 은행인 BankNet에서 발행하는 ECheque(http://mkn.co.uk/help/bank/echeque.html) 등이 있다.

수 있다. 미국의 금융서비스기술협회(Financial Services Technology Consortium)에 의한 전자수표와 Cyber-Cash가 대표적인 예이다.

전자수표는 종래의 수표와 같은 방법으로 기능 하도록 정교하게 고안되었다. 전자수표는 서면수표를 모델로 하여 현재 서면수표에 포함되어 있는 모든 정보를 포함하게 된다. 다만 그 정보는 서면 형태가 아니라 전자적 형태로 존재하게 된다. 전자수표는 서명과 배서를 위하여 또 지급인, 지급은행과 은행계좌의 진정성을 확보하기 위하여 디지털서명을 사용하게 된다. 전자수표는 전자우편 또는 WWW 와 같은 기타의 통신에 의하여 전송된다.

이 시스템은 발행자와 인수자의 신원에 대한 인증을 반드시 해야 하는 문제를 갖고 있다. 여기에 여러 가지 보안 기법들이 사용되고 있는데 이 때문에 트랜잭션 비용이 많이 들 수밖에 없다. 그러나 전자 수표는 상당히 큰 액수의 거래, 기업간의 상거래의 지불 수단으로서 적합하며, 또, 종이로 된 실세계의 수표보다는 처리 비용이 적기 때문에 종이 수표를 쓰는 것보다는 적은 액수의 지불에서도 사용이 가능하게 될 것이다.

2) 전자수표의 특징

전자수표는 전자화폐와 더불어 전자적 증표(electronic token)에 해당한다.

전자수표는 기능적으로 서면수표와 같이 기업과 소비자에 의하여 사용되고 기존의 결제제도를 통하여 결제된다. 전자수표는 서면수표와 같이 발행인의 계좌로부터의 출금을 위한 수권을 포함하게 되지만, 발행인의 계좌에 자금이 있다는 것을 보증하지 않을 것이고, 따라서 서면수표와 같이 부도될 수 있다.

전자수표의 장점은 다음과 같다. 첫째로, 전자수표는 종래의 수표와 같은 방법으로 기능하므로 소비자교육을 단순화할 수 있다. 둘째로, 전자수표는 소액지급제도에 적합하며, 종래의 암호화기법을 사용함으로써 거래를 신속하게 만든다. 셋째로, 전자수표는 자본의 유동기간을 만들어내고 이것은 상거래를 위하여 중요한 요건이 된다. 넷째로, 금융위험을 제2자기관인 계좌서버가 인수함을서 전자수표를 쉽게 받아들이게 만든다.

3) 전자수표의 거래구조

전자수표의 거래구조는 다음과 같다. 먼저 전자수표를 발행하고자 하는 자는 제3자기관인 계좌서버에 등록한다. 발행인(계좌보유자)은 지급인의 명칭, 금융기관의 명칭, 지급인의 계좌번호, 수취인의 명칭, 수표금액 등의 정보를 포함하는 전자수표를 발행한다.

전자수표는 인증을 위하여 서면수표에 있어서의 서명의 대응물로서 디지털서명을 사용한다. 전자수표는 은행을 통하지 않고 전자우편을 통하여 지급인으로부터 수취인에게 직접 전송될 수 있다. 수취인은 서면수표와 같이 또 다른 전자서명을 사용하여 전자수표에 배서할 수 있다. 정당하게 서명, 배서된 수표는 금융기관간에 전자결제기관을 통하여 전자적으로 교환된다.

3.3 전자화폐시스템의 종류

3.3.1 전자화폐

1) 전자화폐의 의의

전자화폐(Electronic money)는 발행자에게 미리 대가를 지급하고 플라스틱 카드에 내장된 IC 칩 또는 개인컴퓨터에 일정한 화폐가치를 저장한 다음 이를 통신망을 통하여 사용할 수 있는

화폐를 말한다. 전자화폐는 본질적으로 전자적 증표(electronic token)에 해당한다.

전자화폐는 1992년 9월 덴마크의 Danmont사가 Naestved에서 발행한 것이 시초인데, 필란드, 싱가포르, 벨기에, 포르투칼, 영국, 네델란드, 미국, 독일 등이 전자화폐를 발행하여 사용하고 있다. 전자화폐는 대소비자 전자결제제도에서 현금을 대체하는 주된 지급수단으로 고안되었다.

2) 전자화폐의 특성

전자화폐는 유형에 따라 약간의 차이는 있지만, 일반적 특성으로는 화폐가치(monetary value), 범용성(interoperability)내지 교환성(exchangeability), 원격송금성(retrievability)과 안전성(security), 휴대가능성(Portability), 그리고 양방향성(Two-way)을 들 수 있다. 그 외에 익명성(anonymity)을 들기도 하나, 익명성을 인정할 것인가에 관하여는 범죄 및 국가안전의 문제와 관련하여 논란이 있다.

전자화폐는 화폐의 주요기능을 갖추고 있는데다 현금의 단점인 원격지 송금의 불편, 보관, 운송에 따르는 비용부담, 금액 분할, 통합시의 불편 등을 보완해 주는 기능을 가지고 있다. 전자화폐는 이러한 장점으로 인하여 지폐와 동전은 물론, 거액의 수표도 상당 부분 대체할 수 있어 점차 통용이 확산될 것으로 예상되고 있다.[9]

3) 전자화폐의 유형

전자화폐는 각각 이용상의 특성이 있기 때문에 기준에 따라 여러 가지로 분류될 수 있다. 전자지갑과 디지털화폐(네트워크형), 온라인형과 오프라인형, 계좌형과 비계좌형, 범용형과 단일목적형, 개방형과 폐쇄형 등의 분류가 그것이다.

ⅰ) 전자지갑과 디지털화폐

전자화폐는 발행형태에 따라 전자지갑과 디지털화폐로 구분할 수 있다.

① 전자지갑

전자지갑(electronic purse)은 플라스틱 카드의 IC칩 속에 현금과 같은 가치를 이전시켜 놓은 전자화폐인데(Mondex Card, VISA Cahs 등), 카드형 전자화폐라고도 한다. 전자지갑은 자동입출금기(ATM)또는 전화기를 이용하여 금액을 저장한 다음 카드판독기를 장치한 자동판매기에서 사용할 수 있다. 자동판매기는 카드가 진정한 것이고 판매금액에 해당하는 충분한 금액이 있는가를 확인하기만 하면 된다. 전자지갑은 저장된 금액이 소진되면 재충전될 수 있다.[10]

② 디지털화폐

디지털화폐(digital cash, or e-cash)[11] 는 통신망상 디지털신호의 형태로 지급결제에 활용될 수 있는 전자화폐인데(CyberCoin, E-Cash 등), 네트워크형 전자화폐라고도 한다. 디지털화폐는 발행자가 디지털방식으로 서명하고 다양한 매체에 저장될 수 있는 일련의 숫자로 표창된다. 예

9) 문종진, 전자화폐의 영향과 대응방향, 금융저널, 1996. 3.

10) 디지털화폐는 네델란드의 DigiCash사가 미국의 Mark Twain 은행과 제휴하여 1995년 중 시험 서비스를 거쳐 1996년에 본격적인 서비스를 제공함으로써 상용화되기 시작하였다.

11) 네델란드의 DigiCash사(http://www.digicash.com)에서 발행하는 Ecash라는 전자화폐이다. 사용자들은 Digital Wallet 이라는 클라이언트 소프트웨어를 이용하여 중앙은행인 FDB(First Digital Bank)에서 전자현금을 인출 혹은 지불하거나 예금도 할 수 있다. 이것은 시험단계를 거쳐 현재 미국의 마크 트웨인 은행과 필란드 메리타 은행에서 실세계 화폐와 환전하여 쇼핑할 수 있다.

컨데, 디지털화폐는 마이크로칩이 내장된 신용카드 크기의 플라스틱카드(smart card라고 한다)에 저장될 수 있다. 또 전자화폐는 전화선을 통하여 은행 기타의 발행자로부터 다운로드받아 PC 또는 전자지갑(electronic purse)에 저장될 수 있다. 디지털화폐는 발행자의 비밀키(private key)에 의하여 생성된 디지털서명으로써 안전이 보장된다.

ii) 온라인형 전자화폐와 오프라인형 전자화폐

온라인형 전자화폐는 주컴퓨터 시스템과 통신망으로 연결되어 주컴퓨터에 의하여 신분 및 비밀번호 확인, 가치이전, 거래내역 입력 등이 행해지는 전자화폐를 말한다.

이에 대하여 오프라인형 전자화폐는 주컴퓨터와 연결되지 않고도 자체적으로 신분 및 비밀번호 확인, 가치이전, 거래내역 입력 등이 가능하여 금융전산망 가동시간 외에도 사용할 수 있는 전자화폐를 말한다.[12]

iii) 계좌형 전자화폐와 비계좌형 전자화폐

계좌형 전자화폐는 전자화폐의 거래기록이 은행 등의 주컴퓨터에 의하여 유지, 관리되거나 기록추적이 가능한 전자화폐를 말한다.(Visa Cash 등)

이에 대하여 비계좌형 전자화폐는 가치기록이 카드나 기록매체에만 기록되고 거래시에 단말기에는 기록이 나타나지만 은행 등의 주컴퓨터에는 거래량만이 전송되는 전자화폐를 말한다.(E-Cash 등)[13]

4) 전자화폐의 거래구조

전자화폐의 거래는 전자화폐가 카드에 기초한 것이든 소프트웨어에 기초한 것이든, 미리 지정된 프로토콜에 따라 컴퓨터장치간에 전자메시지의 교환을 통하여 실행된다. 이 메시지는 전기적 접촉에 의하여(소위 접촉식의 경우), 또는 회선없는 전송이나 통신망을 통하여(소위 비접촉식 또는 네트워크형의 경우) 전송될 수 있다.

전자화폐의 거래절차는 크게 ㉮ 발행 및 가치저장 ㉯ 가치이전과 ㉰ 결제의 3단계로 나눌 수 있다.

전자화폐의 발행(issuance)은 가치저장 또는 소비자에 대한 교부의 시점에서 행하여진다. 발행은 소비자가 가치저장을 개시할 때 행해지기도 한다. 발행은 발행자의 기록에 계좌기장을 생성한다.

가치저장(loading)은 카드형의 경우 자동입출금기(ATM) 또는 특별장치를 한 전화기를 통하여 실행되며, 또 컴퓨터에 기초한 스마트카드 판독기가 이용될 수 도 있다. 발행의 대가는 현금, 신용카드 기타의 지급수단에 의하기도 하지만, 보통은 기존의 은행계좌에 차기 하는 방법에 의한다. 네트워크형의 경우, 가치저장은 보통 통신망을 통하여 소비자의 장치와 발행자의 장치 사이의 메시지교환에 의하여 위와 유사한 방법으로 행하여 진다. 대가의 지급은 보통 은행계좌에 차기 하는 것에 의한다.

전자화폐의 가치 이전은 카드형의 경우 소비자가 상인의 단말기에 카드를 삽입하고 상인이 지급 금액을 입력하여 잔액에서 차감을 함으로써 실행되며, 컴퓨터 통신망이나 전화기를 이용하여 원격지 지급을 하거나 제도에 따라 소비자간에 가치이전이 이루어질 수도 있다. 네트워크형의 경우 화폐가치는 원격지 거래당사자간에

12) 김은기, 전자화폐의 법적 문제, 상사연구소, 제16집 제2호, 1997.

13) 김은기, 전자화폐의 접적 문제, 상사법연구, 제 16집, 1997.

직접 온라인에 의하여 교환될 수 있으며, 인터넷 기타의 컴퓨터통신망을 이용하여 소비자간에 어떤 PC에서 다른 PC로 지급을 할 수도 있다.

전자화폐의 결제(settlement)는 보통 ATM통신망, 데비트카드 또는 신용카드 통신망과 같은 기존의 은행간 정산 및 결제제도를 이용한다. 다만, 네트워크형의 경우 아직 개발단계에 있기 때문에 정산 및 결제절차가 확립되어 있지 않다.

Ⅳ. 전자결제의 문제점과 해결방안

4.1 전자결제의 문제점과 안전장치의 필요성

4.1.1 전자결제의 문제점

전자상거래에서 사용되는 신용카드 등과 같은 결제방법은 기존의 지불수단에 보안성을 가미한 방법이다. 이러한 결제시스템은 그 자체의 독립적인 구조를 갖고 있는 것이 아니므로 사용자는 신용카드 번호와 은행에 결제계좌번호를 반드시 갖고 있어야 하며 이를 이용할 경우에는 은행이나 카드사에서 발행한 카드번호를 기입하는 방법을 사용하게 된다.

이러한 결제방법은 신용카드를 이용한 기존의 시스템이 네트워크로 연결되어 있어 결제수단에 대한 아이디어 및 구현이 비교적 용이하며, 신용카드를 이용한 상거래가 이미 법적으로나, 관행상으로도 자리 잡혀 있기 때문에 전자상거래를 구현하는 많은 시스템이 사용하는 가장 현실적인 방법이라 하겠다.

단지 이러한 방법을 사용할 경우에는 매장에서 직접 카드를 제시할 경우 카드의 소유자를 명시적으로 인정할 수 있는 것과는 달리 전자상거래상에서는 단지 카드번호만 입력하는 방법을 사용하기 때문에 카드번호의 도용 등 보안에 심각한 문제가 있으며 구현되어 있는 대부분의 시스템에서도 이러한 문제 해결을 시도하고 있다.

전자결제제도에서 고려할 또 하나의 특성은 속도(speed)에 따른 안전의 문제이다. 전자거래는 실시간(real time)으로 실행되고, 때로는 부지의 당사자간에 단 1회의 거래가 시도되기도 하는 특성을 가지고 있다. 더욱이 전자상거래는 인터넷과 같은 개방통신망을 통하여 이루어지는 경향이 높아지고 있다. 개방 통신망에서는 엄격한 접근 및 사용통제가 없으므로, 시스템에 저장된 메시지의 안전과 아울러 시스템을 떠난 메시지의 안전을 고려하지 않으면 안된다.

전자결제제도에 있어서 신뢰성의 결여, 속도 및 즉시성과 통제 없는 시스템 접근은 많은 문제를 제기하고 있다.

4.1.2 전자결제시 안전장치의 필요성

1) 안전장치의 필요성

인터넷상의 해커들의 존재는 이미 잘 알려진 바 있다. 최근에는 해킹기술들이 고도로 발전하여 과거에 관리자의 실수나 OS의 실수를 악용하던 초보적인 수준에서 벗어나 Packet Sniffing, IP Spoofing 등의 고난도 해킹방법들이 등장하게 되었다. Packet Sniffing과 IP Spoofing이 전자상거래와 관련하여 문제가 되는 것은 이 방법들이 OS의 오류나 전자지불시스템의 오류와 상관없이 인터넷의 고유한 구조를 이용한 것이기 때문이다. 따라서, 구조적으로 이 문제를 해결하지 못한다면 전자적 결제 정보들은 해커들에게

완전히 노출될 수밖에 없고 이것은 인터넷에서의 전자상거래 자체를 불가능하게 하는 것이 된다. 먼저, 이 방법들을 간단히 소개하면 아래와 같다.

i) Packet Sniffing[14)]

인터넷상에서 정보를 송수신할 때 가장 기본이 되는 정보단위는 패킷(Packet)이다. 일반적으로 패킷들은 이더넷(Ethernet) 케이블을 타고 전송이 된다. 이더넷을 통한 통신방법은 매우 간단하다. A라는 호스트가 B라는 호스트로 패킷을 보내고 싶다면 호스트 A는 호스트 B와 배타적인 연결을 하는 것이 아니라 그 패킷을 이더넷에 뿌린다. 그리고 그 패킷은 일반적으로 수신 주소의 호스트만이 받도록 기대된다. 즉, 일반적으로 자신에게 오지 않는 패킷은 받지 않으므로 호스트 B만이 호스트 A가 보내는 패킷을 받게 된다.

그런데, 호스트 B가 아닌 다른 호스트가 그 패킷을 무시하지 않고 그 내용을 해커에게 전달해 준다면 이야기가 달라진다. 아무리 네트워크 보안에 신경을 쓴 호스트라도 주변의 호스트가 공격 당해서 스니핑을 위해 사용된다면 무력해질 수 밖에 없다. 스니퍼(sniffer)란 이와 같이 네트워크의 한 호스트에서 실행되어 그 주위를 지나다니는 패킷들을 엿보는 프로그램이다.

ii) IP Spoofing

IP Spoofing[15)]은 해커가 머물러 있는, 또는 단순히 악용하고자 하는 호스트의 IP 어드레스를 바꾸어서 이를 통해 해킹을 하는 것이다. 가령 A란 호스트와 B란 호스트가 하드디스크를 공유하고 있는데 A란 호스트와 B란 호스트는 보안이 잘 되어서 해킹하기가 보통 어려운 것이 아니라고 하자. 그리고, 해커는 B 호스트 안에 있는 극비 문서를 훔쳐오고 싶다고 하자. 이때 해킹방법은 다음과 같다. 우선 해커는 자신이 머물러 있는 호스트의 IP 어드레스를 B의 어드레스로 위장을 한다. 위장을 하면 B의 호스트 화면에는 duplicated IP address라는 문장이 찍히게 되고 B 호스트는 네트워크 기능을 잠시 상실하게 된다.

이때를 놓치지 않고 해커의 호스트는 A 호스트에게 자신이 진짜 B 호스트라는 정보를 보내어 A 호스트와 같이 하드디스크를 공유하도록 시도한다. 성공하게 되면 해커는 A 호스트의 하드디스크에 있는 극비 문서를 A 호스트나 B 호스트에 잠입하지 않고도 얻어낼 수 있게 된다.

2) 전자결제에 있어서 필요한 보안 기능

전자결제에 있어서 구체적인 해결방법들을 살펴보기 전에 먼저 이 취약성들을 극복하기 위하여 전자상거래 시스템 내에 구현해야 할 보안상의 기능들이 무엇인지 살펴볼 필요가 있다. 보안상의 기능들은 네 가지로 요약할 수 있는데 그것은 기밀성(Confidentiality), 인증(Authentication), 무결성(Integrity), 부인방지(Nonrepudiation) 로서 이들을 각각 설명하면 다음과 같다.[16)]

14) Ravi Kalakota. Andrew Whinston, Electronic Commerce, Addison-Wesley, 1997, USA, p.136.

15) Anup K. Ghosh, E-Commerce Security Weak Links, Best Defenses, Wiley Computer Publishing, canada, 1998. pp.109-114.

16) Anup K. Ghosh, E-Commerce Security Weak Links, Best Defenses, Wiley Computer Publishing, 1998, Canada. pp.131-135.

i) 기밀성(Confidentiality)

기밀성은 전달내용을 제 3 자가 획득하지 못하도록 하는 것이다. 예를 들어 전자결제를 위하여 은행 계좌번호와 그 비밀번호를 인터넷을 통하여 상인에게 전달할 때 암호화 하여 전송함으로써 도청자가 스니핑 등에 의하여 그 내용을 얻어 내더라도 풀지 못하도록 할 필요가 있다.

ii) 인증(Authentication)

인증은 정보를 보내오는 사람의 신원을 확인하는 것이다. 예를 들어, 상인의 입장에서 볼 때 어떤 고객이 상품의 구매대금으로 신용카드번호를 보내왔을 대 그 고객이 그 신용카드의 실제 소유자인지를 확인할 필요가 있는 것이다.

iii) 무결성(Integrity)

무결성은 정보전달 도중에 정보가 훼손되지 않았는지 확인하는 것이다. 예를 들어, 신용카드 회사의 입장에서 볼 때 카드 사용자가 "상인 을에게 100만원을 지불하겠다"는 내용을 보내왔을 때 이 내용이 원래는 "상인 갑에게 100만원을 지불하겠다"는 등의 다른 내용이었던 것이 중간에 (아마도 을에 의해서) 변조된 것이 아닌지를 확인할 필요가 있다.

iv) 부인방지(Nonrepudiation)

부인방지는 정보제공자가 정보제공 사실을 부인하는 것을 방지하는 것이다. 예를 들어, "갑에게 100만원을 지불하겠다"는 메시지를 보낸 을이 나중에 그런 메시지를 보낸 적이 없으며, 따라서 갑에게 100만원을 지불하기 못하겠다며 그 내용을 부인하는 것을 막을 필요가 있다.

4.2 전자결제의 문제 해결 방안

전자결제의 보안성 문제를 확보시켜 줄 수 있는 방법은 크게 세가지로 분류하여 알아볼 수 있다. 먼저 기밀성 유지를 위해서는 암호화 방법이 있다. 암호화 방법은 정보를 거래 당사자들만이 해독할 수 있도록 암호화 시키는 기법이다. 두 번째는 전자결제의 인증과 무결성을 확보하고 부인방지를 위해서는 전자서명이 효율적이라고 할 수 있다. 마지막으로 상대방의 공개키를 확인하는 방법으로써 전자 인증서가 필요하다 하겠다. 이 세가지의 방법으로 전자결제의 안정성과 보안성은 확보될 수 있고 전자상거래의 활성화를 위한 전제조건이라 하겠다.

4.2.1 암호화기법

가장 일반적이고 오래된 형태의 보안 유지 방법은 암호화이다. 특히 인터넷과 같은 공개채널을 이용하는 전자상거래는 전적으로 암호화에 의존할 수밖에 없다. 암호화의 목적은 네트워크에서 전달될 때 암호문(암호화된 정보)을 얻은 해커가 원래의 메시지를 복구하는 것을 불가능하게 만드는 것이다.

1) 암호화 방법

암호화 알고리즘의 보안성이 그 알고리즘이 수행하는 내용의 기밀성에 의존할 때 이 알고리즘을 Restricted Algorithm이라고 부른다. 과거의 수많은 역사적인 암호화 알고리즘들이 Restricted Algorithm이었음에도 불구하고 이러한 Restricted Algorithm은 현대의 암호 표준화를 위해서는 부적절하다. 많은 구성원으로 이루어진 한 그룹에서 Restricted Algorithm을 쓸 수는 없다. 왜냐하면, 그 그룹 구성원의 한 사람이

그 그룹을 떠날 때마다 다른 알고리즘을 사용하여야 하며, 이를 위해서는 다른 알고리즘을 고안하여 구성원에게 다시 나누어 주어야 하는 부담이 따른다. 이를 막기 위해 구성원마다 다른 알고리즘을 쓴다면 역시 그 많은 알고리즘을 고안하고 관리해야 하는 문제가 따르며, 또 그 알고리즘을 장착한 컴퓨터 하드웨어나 소프트웨어의 대량생산이 불가능하기 때문이다. 즉, Restricted Algorithm은 보안성의 유지 및 표준화를 제공하지 못하고 있다.

현대의 암호학은 이 문제를 키(Key)를 이용하여 해결하였다. 키는 매우 큰 숫자 중의 하나이며, 키가 가질 수 있는 가능한 값의 범위를 Keyspace라고 부른다. 암호화와 복호화[17]는 이 키를 이용하여 이루어지며, 키의 값을 제외하고는 모든 사용자가 동일한 암호화 및 복호화 알고리즘을 사용한다.

키 기반 암호화는 크게 두 가지로 나누어 볼 수 있다. 하나는 비밀키이고 다른 하나는 공개키다. 또한 암호화 알고리즘은 아니지만 전달된 정보의 변경 여부(무결성)나 정보를 보낸 사람을 확인(인증)할 때 사용하는 것으로 Message Digest 방법이 있다. 전자상거래 보안에서는 위의 세가지 방법이 주로 사용된다. 이들을 각각 설명하면 다음과 같다.

i) 비밀키 암호화 방식(Secret-Key)[18]

암호키로부터 복호키를 계산해 낼 수 있거나, 반대로 복호키로부터 암호키를 계산해 낼 수 있을 때 이 암호화 알고리즘을 비밀키 알고리즘이라고 부른다. 대부분의 비밀키에서는 암호키와 복호키가 동일하다.

이 방법의 장점은 암호화와 복호화가 빠르다는 점과, 다양한 암호화 기법이 개발되어 있다는 것이다. 그러나, 이 방법의 단점은 복수의 사용자가 관련되어있을 때 키의 공유 문제가 발생한다는 것과 키 자체를 상대방에게 안전하게 보내는 것이 문제가 된다는 것이다.

ii) 공개키 암호화 방식 Public-key Algorithm (Public-Key, Asymmetric Algorithm)[19]

이 방법에서는 암호키와 복호키가 서로 다르며, 또한 암호키로부터 복호키를 계산해낼 수 없다. 이 방법이 Public-Key 방법이라 불리는 이유는 암호키가 공개되어도 된다는 것 때문이다. 아무나 암호키를 이용하여 어떤 내용을 암호화 할 수 있지만, 오직 해당 복호키를 가진 사람만이 그 암호문을 복호할 수 있다. 이 때문에, 이 알고리즘에서는 암호키를 공개키(Public Key)라고 부르고, 복호키를 개인키(Private Key)라고 부르며, Symmetric Algorithm에서 키를 비밀키(Secret Key)라고 부르는 것과 구별한다.

이 방식의 장점은 키를 상대방에 보내는 것에 보안상의 허점이 없다는 점과 정보의 기밀 유지 이외에 다른 목적으로도 사용될 수 있다는 점이지만 단점으로는 암호화, 복호화 속도가 Symmetric Algorithm에 비해 매우(약 1000배) 느리고 많은 양의 자료를 암호화, 복호화 하기가 불편하다는 것이다.

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

18) Ravi Kalakota. Andrew Whinston, Electronic Commerce, Addison-Wesley, 1997, USA, p.138.

19) Ravi Kalakota. Andrew Whinston, Electronic Commerce, Addison-Wesley, 1997, USA, pp.139-141.

iii) Message Digest

Message Digest[20]는 암호화 방법은 아니다. 이것은 One-way hash 함수[21]를 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.

2) 암호화 방법의 적용

앞서 기술한 전자상거래에서 필요한 네 가지 보안기능(기밀성, 인증, 무결성, 부인방지)에 대해 3가지 암호화 방식(비밀키 암호화 방식, 공개키 암호화 방식, 메시지 다이제스트)에 의해 구현하는 방법을 네 가지 보안기능별로 설명하도록 하겠다.

i) 기밀성(Confidentiality)

기밀성은 비밀키 암호화 방식 또는 공개키 암호화 방식 모두에 의해 이룰 수 있다. 비밀키 암호화 방식을 쓴다면 보내는 사람은 미리 정해진 키를 이용하여 암호화 한 후 보내고, 받는 사람은 같은 키를 이용하여 암호문을 복호화 하면 된다. 공개키 암호화 방식을 쓴다면 보내는 사람은 받는 사람의 공개키를 이용하여 암호화 한 후 보내고, 받는 사람은 자신의 개인키를 이용하여 복호화 하면 된다.

위 두 방법은 각기 단점을 갖고 있는데 비밀키 방식의 경우 키를 미리 갖고 있어야 한다는 점이 단점이며, 공개키 방식의 경우는 암호화 및 복호화 시간이 길고 장문의 정보를 보낼 때 암호화 및 복호화가 불편하다는 것이다. 이 때문에 보통 기밀성을 위한 암호화 방법으로는 비밀키 방식과 공개키 방식을 혼용한다. 즉, 전달정보 자체는 임의의 비밀키를 이용하여 비밀키 암호화 방식으로 암호화하고, 비밀키 자체는 받는 사람의 공개키를 이용하여 공개키 암호화 방식으로 암호화한 후 두 암호문을 보내면, 받는 사람은 자신의 개인키로 비밀키를 복호화 한 후 이 비밀키를 이용하여 전달정보를 복호화한다. 이와 같이 비밀키를 주고받는 것을 키의 전달(Key Exchange Key : KEK)[22]이라고 부른다.

ii) 인증(Authentication)

인증은 공개키 암호화 방식에 의하여 이룰 수 있다. 전달될 내용을 보낼 사람과 받을 사람이

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

21) 해쉬함수는 임의의 길이를 가지고 있는 메시지를, 그 메시지의 양과 관계없이 그 메시지와 유일하게 대응하는 일정한 길이의 bit로 표현하는 함수이다. 원래의 메시지 X에 대하여 해쉬함수 f를 사용하여 나온 결과를 x라 하는 식으로 나타내면 f(X) = x 가 된다.(자세한 내용은 http://esperosun.chungnam.ac.kr/~hdpark 참조). 여기서 X의 내용에 한자라도 수정이 가하여지면 x의 값도 달라진다.

22) Peter Keen, Craigg Ballance, On-Line Profits, 1997. p.215.

모두 미리 알고 있는 상황하에서 보내는 사람이 그 내용을 자신의 개인키(Private Key)를 이용하여 공개키 암호화 방식으로 보내고, 받는 사람은 그것을 상대방의 공개키(Public Key)로 복호화한 후 그 내용을 확인해 보아 맞으면, 받는 사람은 그 내용을 보낸 사람을 확인할 수 있다. 왜냐하면, 복호화 했을 때 그 내용이 되도록 암호화를 할 수 있는 사람은 이 공개키의 짝이 되는 개인키를 갖고 있는 그 사람뿐이기 때문이다.

앞서 서술한 바와 같이 공개키 암호화 방식은 속도가 오래 걸리고 장문의 내용을 암호화, 복호화 하기 어려우므로 인증 시에도 미리 정해진 내용을 개인키로 암호화하고 공개키로 복호화하기 보다는 그 내용을 메시지 다이제스트 한 것을 암호화하고 복호화 한다. 이것을 전자서명(Digital Signature)이라 하는데 전자서명은 인증뿐만 아니라 밑에서 이야기할 무결성과 부인방지도 보장하게 된다.

iii) 무결성(Integrity)

무결성은 메시지 다이제스트를 암호화하여 보냄으로써 이룰 수 있다. 이는 앞서 기술한 내용을 참조함으로서 알 수 있다.

iv) 부인방지(Nonrepudiation)

부인방지는 인증 방법과 마찬가지 방법으로 취득할수 있다. 만약, 자신의 개인키로 암호화하여 정보를 보낸 사람이 나중에 그러한 정보를 보낸 적이 없다고 주장하면, 정보를 받은 사람은 보낸 사람에게 그 암호화된 정보를 제시하면 된다. 왜냐하면, 복호화 했을 때 그 내용이 되도록 암호화를 할 수 있는 사람은 이 공개키의 짝이 되는 개인키를 갖고 있는 그 사람뿐이며, 그 정보의 내용은 그 사람의 공개키로 풀어보면 나오기 때문이다.

4.2.2 전자서명 (Digital Signature)

전자서명[23]은 전자상거래에서 필요한 네 가지 보안기능(기밀성, 인증, 무결성, 부인방지) 중 뒤의 3가지(인증, 무결성, 부인방지)를 한꺼번에 해결해 준다. 전자서명이란 보내는 내용을 메시지 다이제스트 한 것을 보내는 사람의 개인키로 암호화한 것을 말한다. 전자서명은 메시지 다이제스트하기 전의 원래의 정보와 함께 전달되게 되는 데, 이 원래의 정보와 전자서명을 이용하여 인증, 무결성, 부인방지를 다 이룰 수 있다.

먼저 인증의 측면에서 설명하면, 전자서명을 받은 사람은, 보낸 사람의 공개키로 전자서명을 복호화 한 내용과 원문의 메시지 다이제스트를 비교함으로써 그것이 같다면, 그러한 전자서명을 만들 수 있는 사람은 보낸 사람뿐이라는 사실로부터 상대방을 확인할 수 있다.

둘째로, 무결성의 측면에서는 전자서명의 복호문과 원문의 메시지 다이제스트가 같다면 원문이 전달과정에서 바뀌지 않았음을 확인할 수 있다. 그리고, 혹시 중간에 다른 사람이 그 내용을 변조하려 한다 하더라도 보낸 사람의 공개키로 풀릴 수 있는 전자서명을 만들기 위해서는 보낸 사람의 개인키를 알아야 하는데 이를 변조자가 알 수는 없으므로 문제가 없다.

마지막으로, 부인방지의 측면에서는 보낸 사람이 나중에 그러한 내용을 보낸 바가 없다고 부인할 때 원문과 전자서명을 둘 다 제시하면 그러한 원문으로부터 그러한 전자서명을 만들 수 있는 사람은 그 사람뿐이라는 사실로부터 그

23) Ravi Kalakota. Andrew Whinston, Electronic Commerce, Addison-Wesley, 1997, USA, pp.141-142.

부인을 방지할 수 있다.

일반적으로 앞의 네 가지 보안기능(기밀성, 인증, 무결성, 부인방지)을 이루기 위해서는 전자서명을 만든 후, 원문과 전자서명을 임의의 비밀키를 이용하여 비밀키 암호화 방식으로 암호화 하고 비밀키는 받는 사람의 공개키를 이용하여 공개키 암호화 방식으로 암호화하여 두 암호문을 함께 보내는 방법을 쓴다.

4.2.3 전자인증서 (Digital Certificate)[24]

앞에서 전자서명의 기능을 설명할 때 인증, 무결성, 부인방지를 확인하기 위해 중요한 역할을 한 것이 정보를 확인하는 데 쓰인 공개키였다. 전자서명을 받은 사람은 그것을 보낸 사람의 공개키로 복호화함으로써 그러한 내용들을 확인할 수 있었던 것이다. 그런데, 상호 확인이 원칙적으로 불가능한 가상공간 내에서 다른 사람의 공개키를 어떻게 알 수 있는가 하는 것이 문제가 된다. 미리 상대방의 공개키를 모르는 상태에서, 상대방이라고 자처하는 사람이 전자서명을 보내면서 자신의 공개키를 함께 보내온다면 그 전자서명은 함께 보내온 공개키에 맞게 생성될 수 있다. 보내는 가짜의 입장에서는 하나의 공개키, 개인키 짝을 생성한 후 그 개인키를 이용하여 전자서명을 만들고 그 전자서명과 함께 앞에서 준비한 공개키를 보내면 되기 때문이다. 따라서, 상대방의 공개키를 확인하기 위한 방법이 마련되어야 한다.

이를 위하여 제시된 것이 인증기관(CA, Certificate Authority)이다. 인증기관은 한 사람의 공개키를 자신의 개인키로 암호화함으로써 그 사람의 공개키를 인증한다. 물론, 인증기관은 인증하기 전에 그 사람을 실제로 확인한 후 그 사람이 제시한 공개키를 인증한다. 인증기관의 개인키로 암호화한 공개키를 전자인증서(Digital Certificate)라고 부른다. 이 전자인증서를 받은 사람은 인증기관의 공개키로 전자인증서를 풀어서 나온 공개키를 상대방의 공개키라고 믿을 수 있다. 왜냐하면, 그러한 전자인증서를 만들 수 있는 사람은 그 개인키를 알고 있는 인증기관뿐이며, 인증기관은 믿을 수 있기 때문이다. 물론, 이 확인을 위한 전제조건은 그 인증기관의 공개키는 미리 널리 유포되어 모두가 알고 있어야 하며, 그 공개키는 누군가에 의해 조작되어 있지 않아야 한다. 그렇지 않다면 전자인증서의 확인은 틀린 것이 되기 때문이다.

V. 결론

전자상거래가 발전되고 활성화 될수록 전자결제에 대한 이용은 더불어서 급격히 증가할 것은 자명한 일이다. 그러나 현재 전자결제에 따른 법적, 제도적, 기술적인 면들은 여전히 많은 문제점들을 안고 있다.

본 고에서는 전자결제에 따르는 많은 문제점 중에서도 특히 전자결제의 보안성 유지와 안전성 확보라는 측면에 초점을 맞추어 연구하였다.

전자상거래를 보다 발전시키기 위해서는 안정적인 결제시스템의 개발과 보급이 시급하다 할 수 있다. 인터넷에서는 전자결제의 안전성과 보안을 보장하기 위해서, 몇가지 방법이 개발되어 사용되고 있다. 여기에는 암호화, 전자서명, 전자

24) Ravi Kalakota. Andrew Whinston, Electronic Commerce, Addison-Wesley, 1997, USA, pp.142-143.

인증 그리고 무결성 등이 포함된다. 정보 이동시의 보안은 매우 중요하다. 인터넷을 통한 정보의 보안 없는 전송은 부정이 쉽게 저질러지며 다른 사람에 의해 오용될 수 있다. 따라서 인터넷을 이용하여 상행위를 하고자 하는 자는 암호화와 전자서명 그리고 전자인증서를 통하여 고객의 신뢰를 구축하는데 노력하여야 할 것이다.

암호와 기술의 발전과 전자서명, 전자인증에 대해 제도적, 기술적으로 하자가 없다 치더라도 전자결제에 따른 여러 가지 문제점은 상존 하게 된다. 그 예로서 암호화에 따르는 전자결제의 혜택은 순수한 목적의 상거래활동을 영위하는 일반인들뿐만 아니라 범죄자 집단을 미칠 수 있음을 들 수가 있다. 특히 전자화폐는 경우에 따라 익명성이 보장되고 원격지에서 신속한 자금이체를 가능하게 하는 등의 특성을 가지므로 자금세탁, 세금포탈, 불법도박 등의 범죄활동에 이용될 가능성이 있다. 또 위조, 사기, 시스템 파괴 등과 같이 전자화폐상품 자체에 대한 공격이 있을 수도 있다. 따라서 이러한 부분에 대한 법률적, 기술적 장치가 마련되어야 할 것이다.

참고 문헌

남 광, UNCITRAL과 전자상거래, 통상법률, 법무부, 1997. 8.

신동민, 전자상거래(CALS/EC)의 추진 현황 및 향후 전망, 산업포커스, 1998.

이남용, 김대식, 전자상거래 시스템의 아키텍처에 관한 연구, 1997.

이신우역, 전자상거래, 중앙일보사, 1996.

이재규, 조영희, 인터넷의 상업적 활용방안, 국제전자상거래연구, 1997.

전성인, 화폐의 기능과 신용 정책의 역할-전자화폐의 경우를 중심으로, 1998.

------, 정보사회에 대비한 일반법 연구(II), 정보통신정책연구원, 1998.

함유근, 전자상거래의 구현 전략, 1998.

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

CHOI, STAHL, WHINSTON, Electronic Payment Systems and the Future of Electronic Commerce, The Economics of Electronic Commerce, 1997.

Jan Zimmerman, Doing Business with The Government Using EDI, 1996.

John R. Levine & Carol Baroudi, 인터넷의 비밀, 홍익미디어, 1995.

------, 사이버 쇼핑몰 구축의 모든 것, 월간 인터넷, 1998. 3.

Peter G. W. Keen And, Craigg Ballance, On-Line Profits, 1997.

Ravi Kalakota, Electronic Commerce-A Manager's Guide, Addison-Wesley. 1997.

A Study on the Transaction Security of Electronic Payment

Seon-Eui Hong*

Abstract

In this paper we discussed various types of electronic payment schemes that are emerging. Threats vary from malicious hackers attempting to crash a system, to threats to data or transaction integrity. An understanding of the various types of threats can assist a security manager in selecting appropriate cost-effective controls to protect valuable information resources. An overview of many of today's common threats presented in this paper will be useful to mangers studying their own threat environments with a view toward developing solutions specific to their organization.

To ensure security on the Internet, several methods have been developed and deployed. They include : authentication of users and servers, encryption, and data integrity. Transaction security is critical : without it, information transmitted over the Internet is susceptible to fraud and other misuse. So computer systems represents an intermediary with the potential to access the flow of information between a user. Security is needed to ensure that intermediaries cannot eavesdrop on transactions, or copy/modify data.

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

* Dept. of International Trade, Kyeong-Won College