主題

전자상거래를 위한 전자지불시스템 동향

순천향대학교 류종호, 염흥열

차 례

요 약

정보통신 기술이 최근에 급진적으로 발달함에 따라 통신망 환경이 크게 향상되고 있다. 일반인들도 인터넷을 통한 온라인 서비스 및 상품 구매의 이용이 증가하였으며, 이에 따라 전자 온라인 거래에 적합한 다양한 전자지불시스템이 각각 이용되고 있다. 현재 전자지불시스템들은 온라인 거래에 상용화되어 전자상거래 활성화에 많은 도움이 되었지만 각 지불 시스템간의 상호연동 확보와 관련된 문제점이 제기되어 이를 표준화하려는 연구가 활발히 진행 중이다. 본 논문에서는 전자거래에 적용한 전자지불시스템에 국내외 연구동향 및 이에 대한 중요 보안 사항을 살펴보고 전자지불의 표준화 그리고 차후의 개발 방향에 대하여 알아본다.

Ⅰ. 서 론

전자상거래란 거래 주체의 사이의 거래가 물리적인 교환이나 물리적인 접촉의 형태가 아니라 전자적으로 수행되는 비즈니스 거래의 한가지 형태라 정의할 수 있다. 현시점에서, 컴퓨터와 네트워크의 보급으로 전자상거래의 시장규모가 급속도로 확대되어 가고 있으며 그에 대한 연구가 활발히 진행되고 있다. 연구 기관마다 추정하는 전자상거래 시장의 규모는 모두 다르지만, 급속하게 시장 규모가 성장한다는 점에서는 모두 일치하고 있다. 전자상거래의 확대는 다양한 형태의 전자지불시스템이 형성되도록 해주는 기초가 되었으며 각 전자지불시스템마다 사용자에게 편리성과 용이성을 제공하는 동시에 시스템 측면에서 보다 안전적인 보안 기술이 되도록 구성되어 가는 추세이다. 이에 각 기술 선진국(국가주도 및 민간주도)들은 자국 시장경제의 확대 및 전자상거래의 이점을 최대한 살리기 위한 기술 개발에 총력을 기울이고 있으며 새로운 글로벌 사이버 시대의 중요 테마로 떠오르고 있는 사항이다.

일반적으로 전자상거래는 비즈니스의 모든 과정

에서 발생하는 정보교환, 즉 상품 및 서비스 판매, 발주, 광고 등을 개방형 통신망에서 전자화 하여 실행하는 것으로 거의 모든 경제활동이 함축되어 있다. 이 전자화 비즈니스 정보교환은 상거래의 신속화 효율화를 실현하고자 하는 것으로 인터넷상에서 거래처의 선택을 비롯한 상품 구매, 가격 교섭, 계약 체결, 대금 결제 등 상거래에 관련된 모든 업무를 전자적으로 처리할 수 있는 환경 구축에 목적을 두고 있다. 예컨대 그림 1과 같은 참여 주체 중에서 상점과 고객간의 거래의 경우 고객은 상점이 인터넷상에 개설한 가상 쇼핑몰에 진열된 상품을 선택해서 구매할 수 있다. 모든 구매절차는 간단한 조작으로 끝나며 이에 관련된 전자지불시스템을 이용해 구매와 결제가 동시에 이루어진다.

그림 1. 전자상거래의 참여 주체

불특정 다수의 개인이나 상점을 대상으로 한 인터넷 상거래는 현실의 상거래와는 다른 특징을 몇 가지 지닌다. 이러한 특징에는 통신망 기반 구조의 확립, 가상공간 상의 신뢰 및 보안 유지, 지불 그리고 마케팅 등의 측면에서 찾아 볼 수 있다. 따라서 이러한 특징들로부터 전자상거래를 구축하기 위해 반드시 요구되는 몇 가지 사항이 존재한다[1].

우선, 거래 측면에서 가격이나 구입 행위를 추후에 부인할 수 없는 구조가 요구된다. 또한 상호간의 신원확인이 어렵기 때문에 신뢰 및 보안 유지를 위해 서버나 클라이언트의 인증 구조를 구축하여야 한다. 이와 함께 인터넷상에서 거래 정보에 불법 도청 등의 침해 행위를 방지하기 위한 암호기술, 디지털 서명, 공개키기반구조(PKI: Public Key Infrastructure), 인터넷 보안기술 등이 요구된다.

둘째로, 고객이나 거래정보 위협에 대한 대책 수립이 요구된다. 전자상거래는 인터넷상의 불특정 다수간에 거래를 가능하게 하는 장점과 다양한 서비스를 제공하고 있으나 대부분이 비밀성, 메시지 인증, 구매자/판매자 인증, 송수신 부인방지, 재전송 방지 등과 같은 정보 위협에 대한 대책 수립이 완전하지 않은 실정이다. 이와 같이 서비스를 안전하게 제공하기 위해서는 고도의 안정성을 유지하며 사용자의 신뢰성을 보장해 주는 정보보호 기술이 필요하다.

셋째로, 현실의 상거래에서 사용되는 지불수단인 현금, 신용카드, 수표 등을 모두 인터넷상에서 전자적으로 처리하기 위해 전자지불 정보에 대한 결제방법, 확인방법, 청구방법, 고객의 신용 관리방법을 구축하여야 한다. 현시점에서는 이러한 요건을 위해 SET(Secure Electronic Transaction) 프로토콜, SSL(Secure Socket Layer) 통신, 전자화폐 등의 전자지불 기술이 적용되고 있다.

전자지불시스템(electronic payment system)은 기존의 지불방법을 네트워크 상으로 확장하여 무형의 전자적 정보를 상거래 행위나 서비스 이용에 대한 지불수단으로 활용하는 것을 의미한다. 전자지불은 이전에 널리 공인된 신용을 바탕으로 기존 물리적 화폐가 지니지 못했던 편리성, 위/변조 방지성, 원격지 통신가능성, 불법사용 방지성 등의 새로운 기능을 추가하여 불특정 다수 개인과 기업/상점이 안심하고 자금 이체/결제를 수행할 수 있도록 하기 위한 효율적인 방식이라 할 수 있다. 또한 국가에서 독점적으로 물리적 화폐를 발행함으로써 얻게 되는 혜택인 시너지 효과를 전자지불수단 발행 민간부분에 이전함으로 국가의 독점적 혜택의 일정부분이 고객에게 서비스 향상, 편리성 증대 형태로 되돌아 갈 수 있는 방법이기도 하다[2].

최근에 인터넷을 통한 전자상거래가 활성화됨에

따라 전자지불에 대한 관심과 중요성이 더욱 커지고 있다. 현재 개발된 전자지불시스템은 과거의 단순한 계좌번호나 신호카드 번호 전달에서 벗어나 불법적 행위를 사전에 방지할 수 있는 보안 요소가 추가된 형태로 개발되고 있다. 전자지불 분야는 신용카드 업체, 은행 연합, 정보기술 개발업체 등 관련 기관이 연구를 통하여 몇 년 사이에 급속한 발전을 거듭하였고, 현재는 전자상거래에 안전한 지불을 보장하는 여러 지불시스템들이 상용화를 발주한 단계에 놓여 있다.

본 논문에서는 이러한 전자지불시스템의 동향을 분석하고, 이러한 전자지불이 향후 정보화 사회에 정착하기 위하여 필요한 보안 기술들을 분석하고 대표적인 전자상거래를 위한 지불 시스템의 동작원리를 분석함에 그 목적으로 두고 있다. 따라서 다음과 같은 몇 가지 주제를 기반으로 기술하고 한다.

• 전자지불 방식의 기술적 요소

보안 문제가 크게 부각되고 있는 인터넷상에서 전자지불을 수행하는 것은 매우 위험한 일로 여겨지고 있다. 따라서 안전한 전자 상거래에 대한 연구가 필수적임에 따라 이를 위해 보안 기술적 요소를 분석해야 한다. 이에 관한 사항은 2장에서 논하고자 한다.

• 전자지불 프로토콜의 분석

현재까지 개발된 지불시스템은 대부분이 OSI 참조모델의 응용부문(OSI계층 7)에 사용된다. 시스템 대부분이 사용자 측면을 고려하여 개발되었기 때문에 인터넷에서 지불거래를 위해 직접적으로 사용할 수 있거나, 다른 지불시스템에 이용될 수 있도록 연구되었다. 전자상거래에서 일반적으로 많이 사용된다고 알려진 프로토콜로는 SSL, SET, iKP, S-HTTP(Secure Hypertext Transfer Protocol), PCT, Millicent 프로토콜, MPTP 그리고 Mini pay 프로토콜 등이 있다. 이중에서 몇 가지 사항을 3장에서 논한다.

• 전자지불시스템 동향 분석

인터넷상의 비즈니스인 전자 상거래는 네트워크를 통한 상품의 구매와 판매로서 정의 될 수 있는데 이러한 전자상거래의 기본이 되는 요소는 전자지불시스템이다. 전자지불시스템에 관한 사항은 4장에서 논하고자 한다. 4장에서는 또한 개발된 몇몇 국내 전자지불시스템에 대한 분류 및 특징을 분석하여 논할 것이다.

Ⅱ. 전자지불방식의 기술적 요소

전자지불시스템에서의 요소기술로 암호 메커니즘, 전자서명(digital signature), 공개키 기반구조, 은닉서명(blind signature)에 대해서 알아본다. 보안은 전자지불시스템에서 가장 중요한 요소기술의 하나라 할 수 있다. 전자지불시스템에서의 보안은 시스템 보안 차원이 아니라 거래 정보, 카드번호 등의 자료 보호(data security)하는 것을 말한다. 특히 네트워크 환경에서 정보를 주고받아야 하는 전자지불시스템의 경우 각종 위협 요소(위조, 부인봉쇄, 이중사용, 돈 세탁, 강제적인 전자화폐 인출 등)가 있으며, 이런 위험으로부터 정보를 안전하게 신뢰할 수 있게 전달하는 것을 핵심 요구사항이다[1].

암호화를 통해서 정보의 비밀성을 유지시킬 수는 있지만 받은 메시지가 정말 자신이 기대하고 있던 사람이 보낸 것인지, 원본 내용의 수정이 없는지에 대해서는 보장할 수가 없다. 이러한 문제에 대한 보완으로 전자서명 기법이 사용된다. PKI는 공개키 암호 메커니즘을 응용한 전자서명 및 인증 그밖에 다양한 응용시, 공개키를 안전하게 관리하고 전달하기 위한 키관리(key management) 체계이다.

전자지불시스템 중에서 전자화폐를 사용하는 경

우, 고객의 익명성을 보장해야 하고 현금이 이중으로 사용되는 경우 이를 검출하고 이를 사전에 방지하는 위해서는 여러 암호 기술이 요구된다. 그 중에서도 익명성 보장은 은닉서명 기법으로 실현된다. 이 기법은 은행이 전자화폐를 발급할 때 자신이 발행한 화폐의 세부 내용을 모르고 사용자에게 전자화폐를 발행하는 기법이다. 따라서 이 방식을 이용하면 은행은 사용자가 어디서 전자화폐를 사용했는지를 알 수 없으므로 사용자의 프라이버시를 보장받을 수 있게 된다.

1. 대칭형 암호 알고리즘

암호(cryptography)는 평문(plaintext)을 해독 불가능한 암호문(ciphertext)으로 변형하거나 암호화된 통신문을 복원 가능한 형태로 변환하기 위한 방법을 제공한다. 전자지불시스템에서 일반적으로 이용되는 대칭형 암호 알고리듬은 실시간 처리가 가능한 암호방식으로서 표 1에 대표적인 블록암호(block cipher) 알고리듬 현황 및 특성이 나열되어 있다[3]. 대칭키 암호 알고리듬은 키분배, 메시지/사용자 인증 그리고 전송 데이터의 암호화에 사용되며 스마트카드형 전자지갑에서도 사용된다. SSL(Secure Socket Layer)에서는 IDEA (key size: 128bits), RC2-40(40 bits), DES-40(40 bits), DES(56 bits), 3DES(168 bits), Fortezza(80 bits)을 이용한다[4]. SET (Secure Electronic Transaction)는 DES-CBC(56 bits)을 기본으로 이용한다[5].

128~256 bits의 가변길이 키를 갖는 새로운 블록 암호 알고리즘 표준으로 AES(Advanced Encryption Standard)가 전세계적으로 공모되었고 금년 10월 2일에 최종 결정이 내려졌다. AES의 5개의 후보 Twofish, Serpent, Rijndael, RC6, MARS 중에서 Rijndael이 선정되었다[6].

2. 공개키 암호 알고리즘

공개키 암호 알고리즘은 암호용 키와 복호용 키가 서로 다른 키쌍을 지닌 알고리즘이다. 공개키 암호 알고리듬은 주로 인증 및 디지털 서명 등에 주로 사용되며 현재로서는 RSA가 주로 이용된다. 최근에는 RSA 방식보다 비도가 높은 ECC(Elliptic Curve Cryptography) 방식이 연구 중에 있다. 대칭형 암호 알고리즘 보다 처리속도가 느린 단점을 지닌 공개키 암호는 일반적으로 키분배를 위해 많이 사용된다[3].

가. RSA 공개키 암호 시스템

Rivest, Shimir, Adleman에 의해 1977년 개발된 가장 폭넓게 많이 알려진 암호 알고리듬으로 큰 수의 소인수분해가 어렵다는 점에 안전도의 기반

표 1. 대표적인 블록 암호 알고리듬 현황 및 특성 분석

동록명	년도	발표 기관	블록 (bits)	키 크기 (bits)	라운드	표준화	특징
DES	1977	IBM	64	56	16	ANSI X3.92, FIPS PUB 46	비선형함수인 S-Box사용
3중 DES		ANSI	64	112		ANSI X9.52/X9.17, ISO 8732	DES EDE 모드 사용
RC2	1994	RSA	64	다양	없음	ISO RC2-sbc	S-Box 사용 안 함
IDEA	1994		64	128	8	ISO idea-tm	DES보다 2배 빠름
FEAL	1987	NTT	64	64	8이상	ISO feal	불안전하여 라운드 수 확장
ICE	1994		64	64, 128, 192		ICE standard	키 관련 암호분석에 면역성
AES	2000	NIST		120~256			Rijndael로 선정됨

을 두었으며 소수성 테스트와 효율적 소인수분해 알고리듬을 찾는 연구가 활발히 진행 중이다. 현재 RSA는 다양한 제품과 플랫폼, 산업 등에서 이용되고 있으며, 많은 상용 소프트웨어 제품에 들어 있고 앞으로 더 많은 것이 포함될 것이다. 현재 Microsoft, Apple, Sun, Novel의 운영체제에 내장되어 있고, 하드웨어 형태로는 전화, 이더넷 네트워크 카드, 스마트카드에서 사용되고 있다. RSA는 SET(RSA를 전용으로 사용), SSL(RSA를 전용으로 사용), S-HTTP, SET, S/MIME, S/WAN, PCI등의 안전한 이더넷 통신을 위한 모든 프로토콜에 포함되어 있다. 또한 미정부기관, 대기업, 국가연구소, 대학 등의 많은 기관에서 사용되고 있는 사실 표준 암호 알고리듬이다. RSA는 SWIFT(Society for Worldwide Interbank Financial Telecommunication) 표준, 프랑스 금융산업의 ETEBAC 5 표준, 미국 은행 산업의 ANSI X9.31 표준의 일부이다. 호주의 키관리 표준 AS2805.6.5.3에도 RSA를 명시하고 있다.

나. ElGamal 공개키 암호 시스템

이산대수 문제(discrete logarithm problem)에 공개키 암호 시스템으로 ElGamal이 Diffie-Hellman의 키 분배방식을 이용하여 개발한 공개키 암호 알고리듬으로 암호화 및 복호화 그리고 서명이 가능하다. ElGamal의 공개키 암호 시스템은 먼저 키 생성과정을 수행하고 생성한 키를 이용하여 암호화 및 복호화를 수행한다.

다. 타원 곡선 암호 시스템

타원곡선 이산대수 문제에 안전도의 기반을 두고 있는 암호 시스템으로 Koblitz와 Miller가 독립적으로 개발하였다. 1990년 Menezes, Vanstone, Okamoto에 의해 타원곡선의 이산대수 문제가 유한체 위에서의 이산대수 문제로 바뀔 수 있음을 보안 후 급속도로 발전하였고 짧은 키 길이로 인하여 스마트 카드에 적절한 암호 시스템이다.

3. 전자 서명(Digital Signature)

컴퓨터 네트워크를 통한 비대면 방식의 전자거래는 대면방식의 기존 거래 방식의 단점을 극복케 한다. 전자거래는 기존 거래방식에서 시간적·공간적 제약의 문제점을 해결해 준다. 그러나, 전자거래는 많은 장점을 가지고 있음에도 불구하고, 사용자에게 역기능을 제공할 수 있다는 문제점 때문에 보안 요구사항이 먼저 해결되어야만 전자거래의 활성화를 기대할 수 있다.

전자서명(digital signature)은 위에 언급된 문제를 해결해 주는 방법으로써 암호(cryptography) 기법을 응용해 서명 이후 부인방지(non-repudiation), 합법적 서명자만 정확한 전자서명을 생성하는 위조방지(unforgeable), 문서 변경불가능(unalterable), 서명자/메시지 인증(authentication), 이후에 재사용불가능(not reusable)을 제공한다.

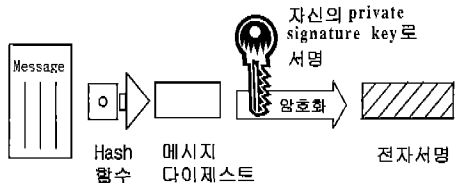

그림 2. 디지털 서명

그림 2에서와 같이 디지털서명은 공개키 암호(public key cipher)를 기반으로 서명자 자신만이 알고 있는 비밀키(private key)로 암호화한다. 여기에서 Hash 함수는 일방향(one-way)함수로 출력인 메시지 다이제스트로부터 원래 메시지를 유도하는 것이 불가능한 암호기법이다.

국내에서는 1997년 6월에 PKI(Public Key Infrastructure)의 인증서(certificate)를 기반

으로 규정된 KCDSA(Korea Certificate based Digital Signature Algorithm)을 표준으로 삼고 있다[7]. 미국에서는 1991년 NIST (National Institute of Standards and Technology)에서 이산대수 문제 해결의 불가능에 근거한 전용 서명알고리즘 DSS(Digital Signature Standard)을 표준으로 제정하고 있다. 그 외에도 대칭키 암호 시스템을 이용한 Rabin 서명 방식, ID를 이용한 Fiat-Shamir 방식과 Ohta 방식, Knapasck 문제를 이용한 Merkle-Hellman 방식, 독일의 Schnorr방식과 Nyberg-Rueppel 방식 등 많은 디지털서명 방식들이 나와 있는 상태이다[5].

표 2는 KCDSA 서명 과정을 설명한 것이다. 여기에서 p, q, g는 공개정보이고 y는 공개키, x는 비밀키이다. || 는 이진스트링간에 연결을 충돌저항 해쉬 함수는 $h_{Hash} : \{0,1\}^* \rightarrow \{0,1\}^{\ell}$로 가정한다. 서명자 A는 $(M, g, x, Cert)$ 구성요소를 지니며 표 2의 관계식을 계산한 다음 메시지 M과 서명문쌍 (c, S)를 검증자 B에게 전달한다.

표 2. KCDSA signature

서명자 A $(M, g, x, Cert)$		검증자 B $(g, y, Cert)$
choose randomly $k \in_R Z_q^*$ *where,* $(0 < k < q)$ *compute* $Z = h_{Hash}(Cert)$ *where, Cert is a certificate of signer A* $W = g^k \bmod p$ $c = h_{Hash}(W)$ $H = h_{Hash}(Z, M)$ $E = H \oplus c$ $S = x(k - E)$	*Send* (c, S) M *to Verifier B* ⟶	*compute* $Z = h_{Hash}(Cert)$ $H = h_{Hash}(Z, M)$ $E = H \oplus c$ $W' = y^S g^E = g^{k-E} g^E = g^k$ *check the validity of following equation* $h(W') \stackrel{?}{=} c$

검증자 B는 표 2의 식을 계산한 다음 메시지 M에 대한 서명문쌍 (c, S)를 검증한다. 여기에서 메시지 M에 대해 (c, S)가 서명문쌍이 된다.

표 2에서와 같이 송신자(서명자 A)는 자신만이 알고있는 전자서명키(비밀키)를 이용한 수학적 연산을 통하여 자신만의 고유한 전자서명 값을 계산한 후, 그 결과를 수신자(검증자 B)에게 송신한다. 수신자는 송신자가 제공하는 전자서명 검증키(공개키)를 사용하여 전자서명 값의 진위 여부를 수학적 연산으로 확인할 수 있으며, 올바른 결과 값이 나오는 경우에만 전자문서를 접수한다. 그러나 이와 같은 방법은 그림 3과 같은 위협에 노출되게 된다.

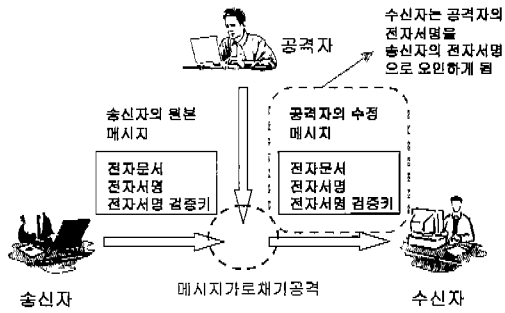

그림 3. PKI의 필요성

따라서 송신자 공개키의 신뢰성과 안전성에 대한 보장에 필요하게 된다. 공개키기반구조(PKI)는 공개키 암호시스템에서 사용자의 공개키를 안전하고 신뢰성 있게 공표 하는 수단을 제공한다.

4. 공개키기반구조(Public Key Infrastructure)

공개키 기반 구조(PKI: Public Key Infrastructure)는 인터넷상에서 서로 초면인 사용자간에 민감한 데이터를 안전하게 교환함으로서, 금융거래를 전자적으로 가능케 하기 위하여 인증서

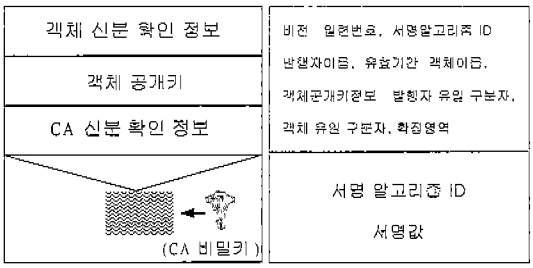

그림 4. 인증서의 기본 구조

(certificate)를 분배하고 전달하는 시스템이라고 정의할 수 있다. PKI를 이용하면 기밀성(privacy), 접근제어(access control), 무결성(integrity), 인증(authentication), 그리고 부인봉쇄(non-repudiation) 서비스를 제공받을 수 있다. 이들 서비스는 전자상거래 응용들과 결합하여 전자상거래의 재정적 거래를 지원한다. PKI는 공개키와 비밀키 쌍들을 생성하고 분배하며 이를 관리한다. 또한 공개키에 대한 인증서를 이용하여 사용자의 공개키를 게시판(open bulletin board)에 공개한다. PKI는 공개키에 대응되는 비밀키(private key)를 안전하게 저장하고 특정 공개키와 특정 비밀키가 정확히 연결되도록 한다[8].

PKI 인증기관(CA: Certificate Authority)은 계층 구조로 구성된다. 이들 CA들은 논리적 트리 구조를 갖는다. 각 사용자에 대한 공개키와 사용자의 ID는 인증서에 포함된다. CA는 사용자의 ID와 공개키를 CA의 비밀키로 서명하여 인증서를 생성하고, 다른 사용자들은 공개적으로 액세스가 가능한 게시판(X.500 directory)을 통해 다른 사용자의 인증서를 구하여 통신하고자 하는 다른 사용자의 공개키를 확신한다. 그러므로 어떤 사용자도 다른 사용자들의 공개키를 공개 게시판(public directory)으로부터 가져올 수 있고, CA의 서명용 공개키를 이용해 인증서에 있는 CA 서명문을 확인함으로서 사용자의 공개키의 정당성을 검증할 수 있다. 계층에서 제일 위층에 위치한 CA는 하위 CA 디렉토리의 공개키를 포함하는 인증서들을 서명하고 서명을 받은 인증기관들은 다시 아래의 인증서들을 서명한다. 이 과정은 공개키들이 검증된 CA들의 하부구조에서 다른 CA들을 서명하도록 한다. 이를 통해 하부구조에 있는 CA들간에 신뢰할만한 구조를 이뤄나간다[9].

5. 은닉서명(blind signature)

세계 여러 나라에서 급부상하고 있는 전자상거래에 관한 연구가 수행되고 있으며, 특히 전자화폐(electronic cash)의 역기능에 관한 논의가 중요한 논쟁이 되고 있다. 은닉서명은 디지털서명 기술, 익명성 그리고 추적불가능성(untraceable)을 제공한다. 그러나 전자화폐의 완전한 익명성 확보에 따른 역기능인 돈세탁(money laundering), 탈세 등의 사회적 범죄가 발생함에 따라 완전한 익명성 확보의 부작용을 방지하기 위한 기술이 요구되어지게 된다. 이 해결책은 공정한 은닉서명(fair blind signature)이 개발로 완료가 된다[10].

표 3. Blind Signature

송신자(고객)		서명자(은행)
$r \in_R Z_n$ $data_1 = r^e M \bmod n$	$data_1$ →	$n = p*q$ $\gcd(e, \varphi(n)) = 1$ $e*d \equiv 1 \bmod \varphi(n)$
$S \equiv data_2 / r \bmod n$ $\equiv M^d \bmod n$	← $data_2$	$data_2 \equiv data_1^d \bmod n$ $\equiv rM^d \bmod n$

고객이 은행으로 전자화폐를 인출 받고자 하는 때에는 고객만의 고유번호(serial number: 표 3에 메시지 M)를 이용하는데 이 경우에 은행은 고객이 사용한 고유번호를 얻게 되며, 이후에 고객이 전자화폐 사용했을 경우 이를 통해 고객의 익명성을 파기함으로써 사용자의 프라이버시를 침해하게 된다. 은닉서명은 이를 막기 위한 기술로써 고객이 어떤 고유번호가 무엇인가를 은행이 알지 못하도록 해준다. 표 3은 은닉서명을 설명한 것으로서 e는 서명자의 공개키, d는 서명자의 비밀키이며 파라메터 $n = p*q$이다. 여기에서 (n, e)는 공개한다.

은닉서명 기법은 82년에 D. Chaum에 의해서 발표되었다[11]. 이러한 은닉서명 기법은 개인의 사생활 보호를 위해서 발표되었지만, 탈세나 돈세탁과 같은 여러 가지 사회적인 역기능을 발생시켰다. 범죄자들이 전자자금이체를 이용하여 돈을 예치하는 경우 수사당국은 예금자에 대한 정보를 입수할 수 없게되고, 특히 범죄자들이 불법으로 입수한 현금을 인터넷 카지노 등에서 칩으로 교환하고 다시 칩을 카지노의 계좌에서 발행하는 수표로 바꾸는 경우 합법적인 도박으로 얻은 수표가 되기 때문에 돈세탁이 가능하게된다. 이와 같은 문제를 해결하기 위해서 공정한 은닉서명 기법이 공개되었다. 이것은 명확하게 정의된 조건하에 참가자의 익명성을 폐지할 수 있는(anonymity-revocable) 메커니즘이 제공된다. 익명성 취소는 신뢰할 수 있는 제3자(trustee, judge 등) 또는 그와 같은 영향력을 가진 기관에 의해 인정될 때에만 가능하다.

III. 전자지불 프로토콜의 분석

현재까지 개발된 지불시스템은 대부분이 OSI 참조모델의 응용부문(OSI계층 7)에 사용된다. 표 4는 전자상거래 보안 적용 위치에 대하여 설명한 것이다.

시스템 대부분이 사용자 측면을 고려하여 개발되었기 때문에 인터넷에서 지불거래를 위해 직접적으로 사용할 수 있거나, 다른 지불시스템에 이용될 수 있도록 연구되었다. 본 장에서는 전자상거래를 위한 지불방식으로 널리 사용되고 있는 SET, SSL 프로토콜에 관하여 살펴본다.

1. SET(Secure Electronic Transaction)

SET은 VISA사와 MasterCard사가 주축이 되어 "인터넷상에서 안전한 신용카드 지불 거래를 위한 기술적 표준"을 합의한 결과로써 전자지불의 참여자간의 모든 거래를 정의하고 이에 대한 안전성을 확보하도록 구성되어 있다. SET은 VISA와 MasterCard 이외에 관련 기업인 GTE, IBM, Microsoft, Netscape communication, SAIC, Terisa systems, Verisign 등 7개 업체가 공동 제안하고 RSA Data Security사의 암호기술을 기반으로 한 신용카드 결제 프로토콜이다. 1996년 2월에 합의한 이후 VISA사의 STT(Secure Transaction Technology)와 MasterCard사의 SEPP(Secure Electronic Payment Protocol)의 결합된 형태로 1997년 5월에 SET v1.0을 발표하였으며 현재는 SET v2.0 문서를 거의 확정한 상태이다. 그러나 SET v2.0에 관련된 제품이 나오기까지는 적어도 1~2년은 기다려야 될 것이다.

이 프로토콜은 신용카드 거래와 비슷한 형태의 전자지불 특성과 이중서명을 지원하여 상점에 카드번호가 노출되지 않고 전자지불이 가능하다. 이중 서명 방식을 이용함으로써 상점은 카드소지자의 신용카드 정보와 같은 개인 정보를 알지 못하며, 은행은 클라이언트가 구매한 상품의 세부 내용을 알 수 없도록 하였다. 그림 5는 SET의 구성 요소 및 공개키 기반구조의 신뢰의 구조를 도시한 것이다. SET에

표 4. 전자상거래 보안 적용 위치

적용위치	특 징
Application Sockets Transport IP Sec IPv4 IPv5 Physical	○ 네트워크 계층(IPSec) - IP 계층에 보안 기능을 둠 - 투명 보안(transparent security) - 종단간 보안 문제 - VPN(Virtual privacy network)에 적합 (방화벽간 또는 호스트와 호스트간) - 표준에서 압축에 대한 세부 사항이 정의되지 않음
Application SSL Transport Network Physical	○ SOCKETS LAYER(SSL: Secure Socket Layer) - 종점간 보안 - 투명한 보안 기능 제공 - 프락시 서버와의 문제점 - 잘 정의되어 있는 보안 프로토콜 - 특정의 압축 알고리듬이 정의되어 있지 않음 - 무연결 서비스의 지원이 안됨, 부인방지 서비스가 없음
Application Sockets Transport IP Sec IPv4 IPv5 Physical	○ 응용 계층 - 응용 프로토콜의 변경이 요구됨 - 특정 응용에 한정된 보안 요구사항을 만족하는 것이 용이함 - 액세스 제어, 부인 방지 등의 서비스 예) SET(Secure electronic transaction) OTP(Open trading protocol), 전자화폐

참여하는 참여자들은 인터넷상에서 물건을 구매하는 카드소지자(cardholder), 카드소지자의 은행인 발행사(issuer), 인터넷에서 물건이나 서비스를 파는 상점(merchant), 상점의 은행인 매입사(acquirer), 은행의 업무를 대신하여 수행하는 은행이 직접 운영하거나 은행의 대리인이 운영하는 지불게이트웨이(PG: Payment Gateway)그리고 SET 내의 구성 요소간의 믿음의 연결 고리를 제공

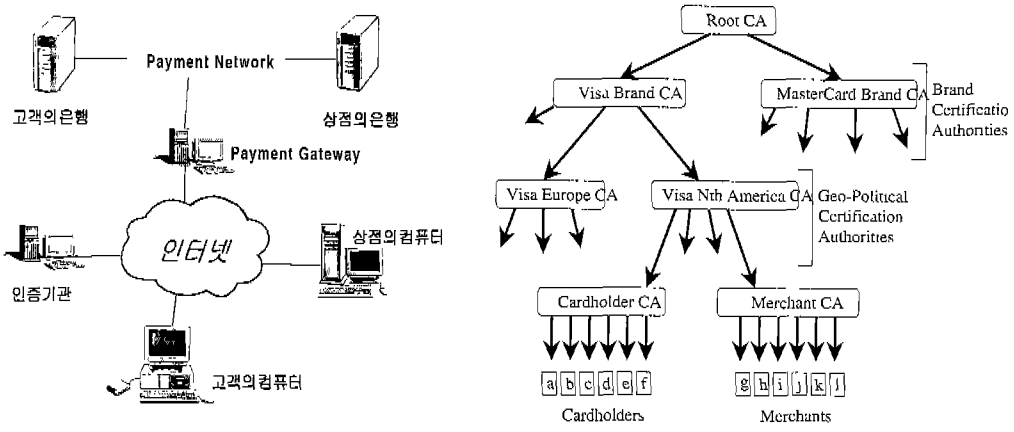

그림 5. SET 구성요소 및 SET 신뢰계층

하는 인증기관(CA: Certificate Authority)으로 구성되어 있다[12].

SET의 PKI는 계층 구조를 가지며, 루트 CA, 브랜드 CA, 지역 CA, 카드 소지자 CA, 상점 CA로 구성되어 있다. 루트 CA는 모든 인증 경로의 시작으로서, 오프라인으로 유지되며 브랜드 인증기관에 인증서를 발급하는 역할을 한다. 브랜드 CA는 비자와 마스터 카드사에 의해 각각 유지되며, 자체 내의 인증서를 관리하게 된다. 지역 CA는 지역적인 상황에 따라 하위 인증서를 어떻게 관리할 것인가를 결정하고 각기 다른 인증 정책을 가질 수 있다. 카드 소지자 CA는 카드 소지자에게 인증서를 발급한다. 상점 CA는 일반적으로 카드거래 구입자의 허가를 토대로 상점에게 인증서를 발행한다.

SET의 가장 큰 장점은 암호화 기술을 이용하고 있다는 점이다. SET에서 유통되는 정보는 신용카드 정보 등을 나타내는 지불정보(PI: Payment Information)와 상품이나 서비스의 종류와 전체 가격 등을 나타내는 구매정보(OI: Ordering Information)로 구분된다. SET가 사용하고 있는 암호화 방법은 지불 정보를 64-비트 대칭형 암호화 알고리듬을 이용해 지불 정보와 구매 정보를 암호화하고, 대칭형 알고리듬에 이용되는 세션키를 다시 1024-비트의 RSA 공개키 알고리듬으로 암호화하여, 암호문과 세션키를 암호 한 암호문을 동시에 전송하도록 구성되어 있다. 표 5는 SET 암호 메커니즘에서 RSA의 키 길이를 적은 것이다.

표 5. RSA 키 길이

	메시지 서명	키 교환용	인증서 생성	CRL 생성
카드소지자	1024			
가맹점 / PG	1024	1024		
카드소지자/ 가맹점 CA	1024	1024	1024	
PG CA	1024	1024	1024	1024
지역/브랜드 CA			1024	1024
루트 CA			2048	2048

매 트랜잭션마다 새로운 형태의 키 값을 설정하며 또한 전자서명(digital signature), 전자봉투(digital envelope), 이중서명(dual signature)을 사용함으로써 제삼자에 의한 공격을 방지할 수 있다. 이중 서명은 지불 정보와 구매 정보를 서로 직접 연결시키면서, 상점은 지불 정보를 알지 못하게 하고, 은행은 주문 정보를 알지 못하게 하는 아주 중요한 기법이다. SET 프로토콜은 지불 메시지에 대한 암호화를 하거나 카드소지자를 인증(authentication)할 수 있는 인증서를 채용함으로서, 인터넷에서 안전한 전자 상거래가 이루어질 수 있도록 하고 있다. 또한 SET 규격은 관련 업계에 공개 사양으로 배포되었으며, 어떠한 지불 서비스에도 적용이 가능하고, 어느 소프트웨어 업체도 응용 프로그램을 개발할 수 있다.

SET은 크게 다섯 가지의 주요 보안 기술로 구성된다. 이 보안 기술은 공개키에 대한 인증서 기술, 암호화 기술, 전자 서명, 지불시스템과의 연결, 그리고 운용 규칙의 설정 등이다.

SET에서 이용되는 공개키 인증서는 다음과 같은 방식으로 동작된다. CA는 P/G(Payment Gateway), 발행은행, 매입은행에게 인증서를 각각 발행해 주고, 발행은행은 카드 소지자에게 인증서를 발행하고, 매입 은행에서 상인에게 인증서를 발행한다. CA는 보다 상위의 CA로부터 인증서를 발급 받고, 최상위에는 루트 CA가 존재한다. CA에서 발급한 인증서는 일방향 함수에 기초한 암호기술을 사용하므로 CA이외의 어떤 개체도 인증서의 내용을 수정할 수 없으며 인증서는 CA에서만 발행할 수 있다. 인증서는 거래자 상호간의 신분을 확인하는데 이용되며, 인증서에는 거래시 필요한 최소한의 정보를 갖고 있다. 그림 6은 SET 거래의 기본 절차를 도시한 것이다.

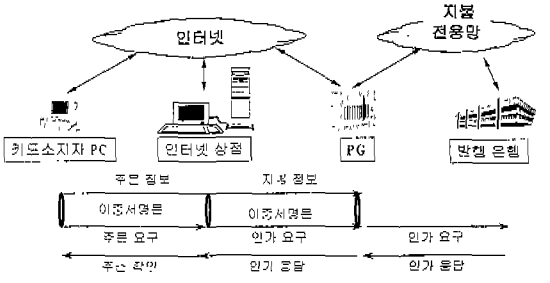

그림 6. SET 거래 기본 절차

SET는 거래는 인증서 기반 프로토콜이기 때문에 거래 참여 당사자들은 우선적으로 자신의 인증서를 소유하고 있어야만 한다. 따라서 전체적인 SET 지불처리 과정을 수행하기 위해 우선 카드소지자는 카드소지자와 인증기관 사이에 카드소지자 인증서를 발급 받기 위한 카드소지자 등록(cardholder registration)을 수행하여야 하며, 역시 동일하게 상점도 상점(가맹점)과 인증기관 사이에 상점 인증서를 발급 받기 위한 상점 등록(merchant registration)을 수행하여야 한다. 두 참여자 모두 인증기관으로부터 인증서를 수령한 다음 그림 7과 같이 카드소지자와 상점이 구매 요청과 응답을 수행하기 위한 주문요청(purchase request) 수행한다. 그런 이후 고객(카드소지자)으로부터 주문요구를 받은 상점은 신뢰할 수 있는 거래를 확신하기 위해 카드소지자의 금융기관으로부터 지불이 가능한지 조사한다. 그림 8에서와 같이 이 과정을 지불인가(payment authorization)라고 한다. 만일 은행에 의하여 지불인가가 허용된다면 상점은 카드소지자와 거래를 완료(상품전달 완료)한다. 그리고 상점은 한 주 단위나 하루 단위로 상점은 P/G를 통해 지불한 상품에 해당하는 금액을 자신의 계좌로 입금하여 줄 것을 금융기관에 요청한다. 이 과정을 그림 9와 같은 지불캡쳐(payment capture)라 한다.

SET는 인터넷을 통하여 안전하게 전자 거래를 하기 위해 요구되는 핵심 기술이다.

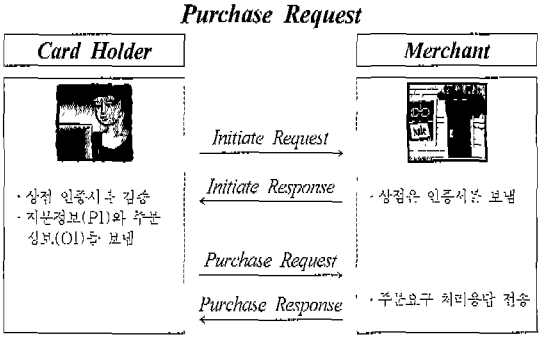

그림 7. 주문 요청/응답

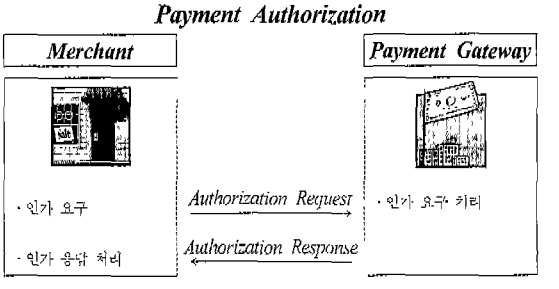

그림 8. 지불인가

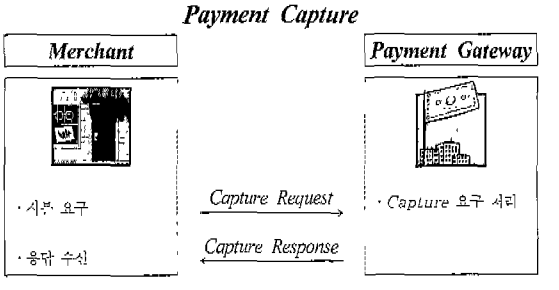

그림 9. 지불요구

SET는 VISA나 MasterCard 등으로 구성된 몇 개의 업체가 모여서 만든 이론적이고 원칙적인 규격이며, 구체적으로 실현할 수 있는 프로토콜을 지니고 있다. 그러나 현재까지는 SET의 전체 모든 구성 요소를 실현하여 이용하지는 않는다. 국외 업체 Microsoft, IBM, Verisign, 후지 은행 등이 SET을 응용한 전자상거래 시스템을 개발하고 운영

하고 있으나 크게 활성화되지는 않고 있다. 왜냐하면 비즈니스 중심이 VISA와 MasterCard가 아니라 은행연합이라 점에서 은행이 결재 프로토콜로써 SET를 표준으로 승인할지는 미지수이고 또한 SET 실현에 있어 많은 기반구조가 요구되기 때문이다. 현재로서는 SET의 높은 안전성에도 불구하고 전체 전자지불 시장에 10%도 차지하지 못하고 있는 실정이다.

2. SSL(Secure Socker Layer)

SSL 프로토콜은 Netscape사가 개발하여 인터넷상에서 기밀 통신과 인증기능 및 무결성을 제공하기 위해 제안되었다. SSL은 종점간의 안전한 데이터 전송을 위하여 응용 프로토콜(HTTP, SMTP, Telnet, NNTP, FTP 등) 과 TCP 프로토콜 사이에 존재하는 소켓 계층 역할을 수행한다[4].

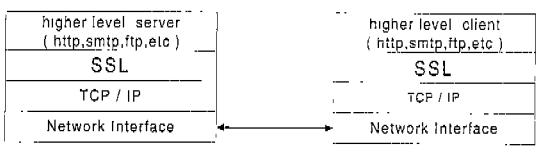

그림 10. SSL 계층의 위치

SSL은 메시지를 블록 단위로 분할하고, 선택적으로 압축하며, 이에 대한 MAC(Message Authentication Code)를 계산하고, 다시 암호화한 후 그 결과를 상대방에 전송한다. 수신된 데이터는 복호화, MAC 검증, 압축 풀기, 역분할의 과정을 거쳐 상위 계층의 개체로 전달된다. 현재 IETF(Internet Engineering Task Force) TLS(Transport Layer Security) 워킹 그룹에서 TLS1.0으로 발전한 상태이다. SSL은 CA의 사용에서의 융통성부여, 쉬운 구현, 클라이언트 브라우저에서의 자체지원 되는 것 등의 요인으로 널리 사용되어 지고 있다. 그러나 상점에서 고객의 지불정보를 볼 수 있는 단점이 있어서 고객의 정보의 악용 및 고객 프라이버시를 침해할 소지가 있으므로, 상점이 개인정보보호 원칙을 준수한다는 가정이 있어야만 안전을 보장받을 수 있다. 이와 같은 단점에도 불구하고 SSL은 이용의 편이성과 융통성에 기인하여 현재 전자지불시스템의 90% 이상에 응용되고 있다.

가. SSL의 개요

SSL은 상위 프로토콜 데이터를 캡슐화 하기 위한 SSL 레코드 프로토콜과 서버와 고객간의 서로를 인증하고 추후에 이용될 암호 알고리듬을 선택하며, 암호키를 계산하는 SSL 핸드쉐이크(Hand-shake) 프로토콜로 구성된다. SSL은 데이터의 암호화 기능, 비대칭형 알고리듬을 이용한 개체 인증, 그리고 메시지에 대한 무결성 기능을 제공한다.

SSL은 세션 상태와 연결 상태로 구성된 두 상태를 갖는다. 세션 파라메터는 특정 세션을 확인하기 위한 세션 ID을 비롯한 암호 슈트 등의 정보로 연결보다 오래 지속되는 값이고, 연결 파라메터는 서버 write key, 고객 write 키 등의 연결과 관련된 정보이다. SSL 핸드쉐이크 프로토콜은 고객과 서버간의 암호 알고리듬 선택, 키 분배 방식의 선택, MAC 알고리듬의 선택 등의 암호 알고리듬 슈트를 선택 및 조정하고, 추후 레코드 계층이 이를 활용할 수 있도록 하는 기반 프로토콜이다. 따라서 핸드세이크 프로토콜이 수행되고 나서 레코드 계층은 암호 관련 서비스를 제공할 수 있다. SSL 세션은 안전한 다중 연결들을 포함한다.

세션 상태에서 요구되는 파라메터는 서버와 고객간의 세션을 유일하게 구별하는 Session Identifier, 개체의 공개키의 정당성을 확인케 하는 공개키 인증서(Certificate), 사용되는 압축 알고리듬(Compression Method), 추후의 암호 통신용 Cipher Spec, 그리고 암호키 생성을 위한 MS(Premaster Secret) 등이 있다. 연결 상태

파라메터는 Server/client Random, 무결성을 위한 Server/client Write MAC 비밀 정보, 데이터 암호를 위한 대칭 암호키인 Server/client Write 키, CBC 암호 모드에서 사용되는 초기 벡터(initialization vectors), 데이터 전송 순서를 결정하는 순서 번호(sequence numbers) 등이 있다.

나. 레코드 계층의 기능

SSL 레코드 계층은 상위 계층으로부터 데이터를 수신하여 분할하고, 압축하며, 암호화하는 기능을 수행한다. 레코드의 종류는 ChangeCipherSpec, 경고(alert), 핸드쉐이크, 그리고 응용 데이터(Application Data) 등이 있다.

분할은 상위 층으로부터 수신된 데이터를 여러 개의 평문 블록들로 나눈다. 모든 레코드들은 현재의 세션에서 정의된 압축 알고리듬을 사용해 압축된다. 압축 알고리듬은 평문 메시지를 압축된 메시지로 변환한다. 압축 기능은 CipherSpec이 바뀔 때마다 자신들의 상태 정보를 삭제한다. 압축은 손실이 없어야 하고, 규정된 길이를 초과해서는 안되며, 압축되어 있는 메시지를 풀 때 기준 길이를 초과하면 치명적인 압축 경고 메시지를 발령한다.

모든 레코드들은 현재의 CipherSpec 에 정의된 MAC 알고리듬과 암호 알고리듬을 사용해 보호된다. 핸드쉐이크 과정이 완료되면, 고객과 서버는 MAC용 키를 이용하여 MAC 값을 계산할 수 있고, 공유된 PMS로부터 복구된 암호키를 이용하여 메시지를 암호화할 수 있다. 특정 암호알고리듬과 MAC 알고리듬의 종류는 CipherSpec에 의해 정의된다. 암호 기능은 압축된 메시지에 대하여 수행된다. 복호화 기능은 이 과정의 반대이다. 메시지를 전송할 때, 분실, 변경, 메시지 삽입을 발견하기 위해 순서 번호를 포함한다.

압축된 메시지를 암호 하는 방법에는 암호를 하지 않은 방법과 표준 스트림 암호 또는 블록 암호를 이용하는 방법이 있다. 스트림 암호는 MAC를 포함해 전체 블록을 암호 한다. RC2 또는 DES 등의 블록 암호는 압축된 메시지를 블록 단위로 암호화한다. CBC 블록 체이닝에 이용되는 초기 벡터는 핸드쉐이크 프로토콜 과정에서 유도된다.

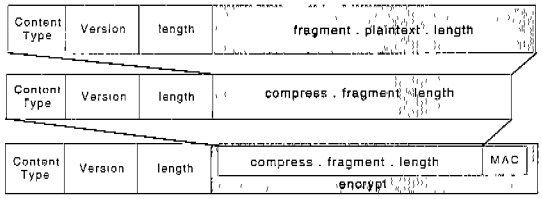

그림 11. 레코드의 분할, 압축, 암호된 형태

다. Change Cipher Spec 프로토콜

Change Cipher Spec 프로토콜은 하나의 메시지로 구성되며 이 전 상태의 예비 암호 규격을 현재의 암호 규격으로 변경하는데 이용되고, 고객과 서버는 이후의 레코드가 협상된 암호 메커니즘과 암호키를 이용하여 보호된다는 사실을 통보한다. 고객은 암호키 교환(key exchange) 과 공개키 검증(certificate verify) 메시지를 보낸 후에 Change Cipher Spec 메시지를 전송하며, 서버는 고객으로부터 받은 암호키 교환 메시지를 처리한 후에 고객에게 Change Cipher Spec 을 보낸다. 이전에 이미 설정된 세션을 다시 사용하려 할 때 Change Cipher Spec 메시지는 hello message 다음에 송신된다.

라. 경고 프로토콜

경고 메시지들은 경고의 중요성(warning, fatal)과 종류를 전달한다. 심각한 경고 메시지는 연결을 종료할 수 있다. 에러가 발견될 때, 발견한 상대는 다른 상대에게 이에 대한 경고 메시지를 보낸다. fatal 경고 메시지는 현재의 연결을 종단하게 하며, 종단된 연결과 관련된 세션 인증자와 키 및 비밀키들은 무시된다. 경고 종류는 Unexpected-

Message(fatal), BadRecordMAC(fatal), DecompressionFailure(fatal), Handshake Failure, NoCertificate, BadCertificate, Unsupported Certificate, Certificate-Revoked, CertificateExpired, Certificate Unknown, IllegalParameter(fatal) 등이 있다. 여기서 (fatal) 은 항상 치명적인 오류를 나타낸다.

마. 핸드쉐이크 프로토콜의 개요

고객과 서버는 암호 파라메터들을 SSL 핸드쉐이크 프로토콜로 협상하여 설정하며, SSL 레코드 층의 상위 층에서 동작한다. 고객과 서버가 처음으로 통신을 시작할 때, 선택적으로 서로 인증하고, 비밀키의 공유를 위해 공개키 암호 방식을 사용하며 구체적인 암호 알고리듬을 선택한다.

고객은 client hello를 서버에게 보내고 서버는 server hello로 응답한다. 그렇지 못할 경우 치명적인 에러가 발령되고, 연결은 실패한다.

client hello와 server hello는 고객과 서버간의 보안 기능을 협상하기 위하여 사용된다. client hello와 server hello는 서버와 고객간에 Protocol Version, Session ID, Cipher Suite, Compression Method 등의 보안 기능을 협상하고, ClientHelloRandom과 ServerHelloRandom 의 랜덤 값들을 교환한다.

서버는 ServerHello 전송 후 서버가 인증 될 필요성이 있을 때 자신의 공개키 인증서를 전송한다. 만일, 서버가 자신의 공개키 인증서를 가지고 있지 않거나, 서명을 위한 공개키 인증서만을 가진다면, 서버는 서버 키 교환 메시지를 이용하여 관련 키 메시지를 고객으로 전송해야 한다. 서버가 고객이 인증 될 필요가 있을 경우 CertificateRequest 메시지를 고객으로 보내고, 이후 핸드쉐이크의 Hello 메시지 단계의 종료를 의미하는 Serverhellodone 메시지를 고객으로 전송한다.

고객이 서버로부터 CertificateRequest 메시지를 수신하면, 고객은 자신의 공개키가 유용하면 공개키 인증서를 전송하거나 유용하지 않으면 NoCertificate Alert 경보를 응답한다. 또한 선택적으로 ClientKeyExchange 메시지를 서버로 보낸다. Certificate Verify 메시지는 고객의 공개키 인증서의 유효성을 서명문을 이용하여 검증하기 위해 서버로 전송된다..

고객은 ChangeCipherSpec 메시지를 보내고, 새로운 암호 및 MAC 알고리듬, 암호키, 그리고 비밀 정보를 이용하여 암호화한 finished 메시지를 서버로 전송한다. 여기서 ChangeCipherSpec은 현재의 세션 정보를 버리고 지금 협상한 세션 정보로 새로운 암호 세션을 개시할 것을 명하는 메시지이고, Finished 메시지는 현재 협상된 세션 정보가 정상적으로 교환되었음을 상대에게 알리기 위한 메시지이다. 이후 서버는 ChangeCipherSpec 정보로 응답하며, 새로운 Cipher 규격에 의한 finished 정보를 구하여 고객으로 전송한다. 이렇게 함으로써 핸드쉐이크는 완료되고 고객과 서버는 이후 응용 데이터 계층을 통해 안전한 데이터의 교환을 수행한다. 그림 12는 처음 연결을 설정하거나 새로운 세션 인증자를 원할 경우의 핸드쉐이크 프로토콜을 나타낸 것이다.

고객과 서버가 이전 세션을 다시 시작하기를 원할

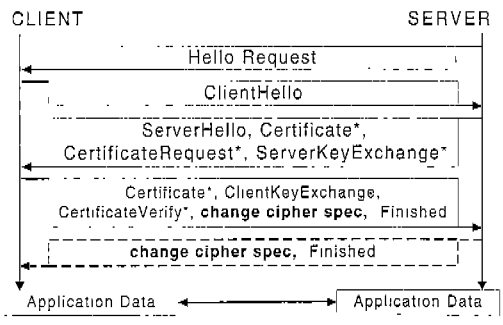

그림 12. 핸드쉐이크 과정

경우 고객은 이전 Session ID를 ClientHello 메시지를 통해 보낸다. 서버는 자신의 세션 캐쉬에 있는 세션 ID 와 일치하는가를 검사하고 일치된 세션 ID 가 발견되면, 서버는 명시된 세션 상태로 연결을 설정한다. 서버는 동일한 Session ID값을 Server Hello 메시지를 통해 보낸다. 이때, 고객과 서버 모두는 Change Cipher Spec 메시지를 보내고, Finished 메시지를 전송한다. 재 연결 설정이 완료되면, 고객과 서버는 응용 계층 데이터를 교환한다. Session ID와 일치하는 값이 발견되지 않으면, 서버는 새로운 Session ID를 생성하고 고객과 서버는 그림 12와 같은 핸드쉐이크 전과정을 수행해야 한다. 한편, 이미 합의된 세션을 통하여 연결을 다시 시작하는 경우 클라이언트헬로우 메시지의 세션 ID를 "0" 이 아닌 다른 값으로 설정하여 보냄으로써 수행된다. 재 연결을 위한 핸드쉐이크 과정의 메시지 흐름은 그림 13과 같다.

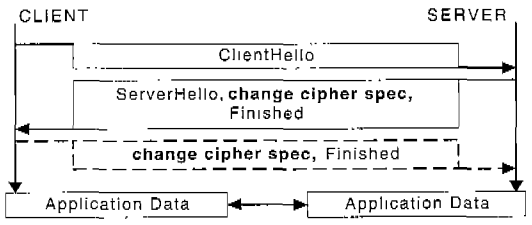

그림 13. 재 연결을 위한 핸드쉐이크 과정

사. 응용 데이터 프로토콜

응용 데이터 메시지들은 레코드 계층에 의해 전달된다. 그리고 이 메시지들은 분할, 압축, 그리고 암호화된다. 메시지들은 레코드 계층으로 투명한 데이터로 취급된다.

3. S-HTTP(Secure Hypertext Transfer Protocol)

S-HTTP는 1994년 가을 EIT(Enterprise Integration Technologies)社, NCSA (National Center for Supercomputing Applications)와 RSA社로부터 HTTP의 보안성이 향상되고, HTTP통보가 캡슐화(capsule)된 버전으로 개발되었다. 이도 HTTP와 마찬가지로 응용부분에서 적용되며, 일반적인 WWW의 보안방법이 유효하고 지불정보의 안전한 전송에도 이용된다. 상호처리과정통신의 확증, 통지의 완전성, 그리고 출처의 비삭제성을 지원한다[13].

이 프로토콜은 RSA 암호문서와 Kerberos에 기초한 보안장치를 지니고 있다. 응용시 다른 암호문서장치(예를 들면, PGP, PEM)를 선택할 수 있다. HTTP에 대해서는 단지 클라이언트 내지는 서버가 S-HTTP를 지원 시에는 비보호적 연결형태에서 통신을 할 수 있는 호환성이 있다

S-HTTP는 대칭키 동작 모드를 지원하기 때문에 각 사용자(고객)들은 공개키를 갖지 않고도 비밀거래를 할 수 있다. SHTTP는 end-to-end 보안 transaction을 지원하고, 고객은 메시지 헤더에 제공된 정보를 통해 trans-action을 시작하는 개시자(primmer)가 된다. SHTTP는 융통성 있는 암호 알고리듬들, 모드들, 그리고 파라메터들을 제공한다. 옵션 협상을 통해 고객과 서버는 transaction 모드에 동의하게 된다. 여기에서는 SHTTP 버전 1.2를 바탕으로 설명한다. 이전 버전과 다른 점은 단일 헤더 라인에 대한 모든 옵션 협상 헤더들이 연합되었고, PEM을 MOSS(MIME Object Security Services)로 대치했으며 SHTTP와 HTTP와의 관계가 명확해졌다는 것이다. SHTTP는 보안서비스 옵션들을 제공하면서 다양한 보안 메커니즘들을 HTTP 고객들과 서버들에게 제공하며 고객과 서버에게 우선권뿐만 아니라 요청과 응답에 동등한 대우가 주어지는 대칭성을 제공한다. SHTTP는 HTTP와 관련하여 설계되었기 때문에 거의 HTTP와 흡사하며 호환 가능하다.

Ⅳ. 전자지불시스템 동향

전자지불시스템은 표 6과 같이 지불방식, 가치저장 매체 등을 기준으로 다양한 형태 분류가 가능하다. 본 장에서는 전자상거래 지불방식에 의한 두 가지 형태 및 가치저장 매체에 따른 네 가지 형태로 분류하여 설명하고자 한다. 전자지불시스템은 지불 수단에 따라 각각의 용도가 서로 다르고 국제단체의 의한 표준화 추세도 상호간에 조금씩 다르게 정의되고 있다. 각 국제단체들은 표준화 정립에 대하여는 필요성을 강조하면서도 사용자 추세에 따른 시장원리에 의해 사실상 표준으로 되어야 한다는 관점과 표준화 단체에 위탁하여 이루어져야 한다는 의견으로 이슈화되어 있다.

네트워크로 거래가 이루어지는 온라인 지급 결제 수단과 IC 카드를 이용하여 지불을 수행하는 오프라인이 현재 중요한 지불결제 방법으로 알려 있기 때문에 본 논문에서는 두 가지 지불 방법을 전자화폐 지불시스템 및 스마트카트 지불시스템으로 나누어 설명할 것이며, 또한 현재 전자지불 시장의 80%을 장악한 신용카드지불 시스템과 현재 수표 결제시스템을 그대로 유지하면서도 수표의 처리 및 발행을 간략화 할 수 있는 것으로 알려진 전자수표지불 시스템도 설명하고자 한다.

표 6. 전자지불시스템의 분류

분류기준	시스템 예
지불방식	1. 지불 브로커 시스템 2. 전자화폐 시스템
가치저장 매체	1. 전자화폐 지불시스템 2. 스마트카드 지불시스템 3. 신용카드 지불시스템 4. 전자수표 지불시스템

1. 지불방식에 따른 분류

전자상거래 지불방식에 따른 분류는 지불브로커 시스템과 전자화폐시스템으로 분류할 수 있다.

가. 지불브로커시스템(payment broker system)

독립적인 신용구조를 갖고 있지 않고 신용카드나 은행의 계좌를 이용해 네트워크 상에서 지불하는 구조를 지닌다. 지불브로커시스템은 현재 널리 이용되고 있는 신용카드시스템(credit card system) 및 전자수표시스템(electronic check system)으로 나누어 볼 수 있다. 이 시스템은 이미 상당히 구축된 금융시스템을 이용하여 구축할 수 있기 때문에 법/제도적 문제의 어려움을 쉽게 탈피할 수 있다. 또한 기존의 다수의 이용자가 존재하기 때문에 거래 방법에 있어 사용자가 상당한 친밀감을 느낄 수 있는 시스템이다. 그러나 특정 거래에 대한 추적이 가능하기 때문에 사용자의 프라이버시 침해 문제와 개인에 대한 기밀정보(예: 신용카드번호 등)의 노출위험성이 상당히 존재한다. 이 시스템에서는 보안을 위해 SET(Secure Electronic Transaction), Cyber Cash, First Virtual, SSL/TLS, S-HTTP 등의 프로토콜을 이용한다.

나. 전자화폐시스템(electronic cash system)

지불브로커 없이 독립적인 신용구조를 가지고 있기 때문에 물품 구입시 은행이나 카드발행사로 부터 거래 승인이 필요 없다. 전자화폐시스템은 플라스틱카드 위에 부착된 IC 칩을 이용한 오프라인 대금결제에 활용하는 IC 카드형 전자화폐와 네트워크를 통한 온라인 대금결제가 가능하도록 한 네트워트형 전자화폐로 나눌 수 있다. 이 시스템은 사용자의 프라이버시를 보호하고 실제 화폐를 대체할 수 있으며 개인정보 노출 위험성이 제거되어 있다. 그러나 법/행정적 제도의 지원이 현재로서는 미비한 상태이며 현재 효율성에 대한 문제가 강하게 대두되고 있는 상태이다. 이 방식의 문제점은 고객의 익명성에

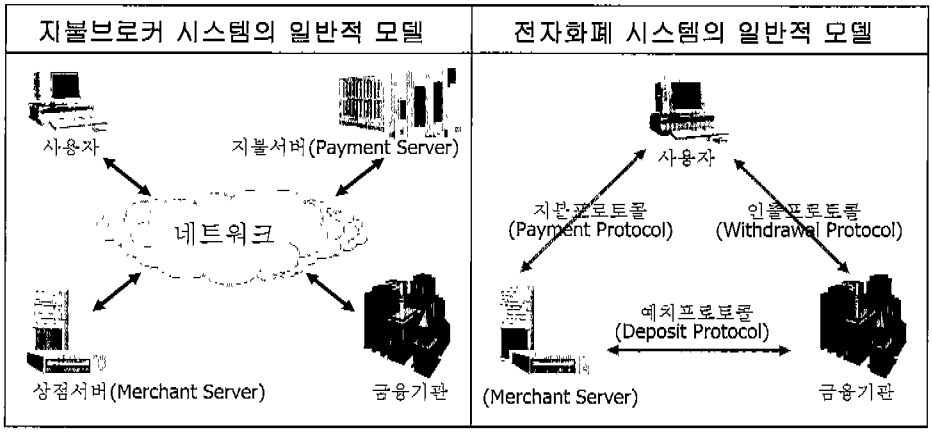

그림 14. 지불방식에 따른 분류

대항하여 은행이나 국가에 의한 화폐 추적 기능을 보장하는 것으로 요약될 수 있다. 이는 고객의 익명성도 중요하지만 불법 단체나 개인에 의한 화폐의 불법 사용과 돈세탁 등과 같은 불법 사용을 사전에 차단하기 위함이다. 이 시스템의 대표적인 예로 Modex card(IC카드형), E-cash(네트워트형), Millicent(소액지불), Proton(선불형) 등을 들 수 있다. 그림 2는 지불브로커시스템과 전자화폐시스템에 대하여 도시한 것이다.

2. 가치저장매체에 따른 분류

전자상거래 가치저장매체에 따른 분류는 네 가지 형태(전자화폐/스마트카드/신용카드/전자수표 지불시스템)로 분류해 볼 수 있다[1].

- 우선, 전자화폐 지불시스템(electronic cash payment system)은 은행이 발행하고 은행의 공개키로 검증할 수 있는 전자서명으로 구현된다. 또한 지불의 익명성을 실현하기 위해 은닉서명(blind signature) 기술이 이용된다. 은닉서명방식은 서명 발행시 서명 의뢰자인 소비자가 은행에 보내는 정보에 랜덤요소를 부가함으로써 소비자가 얻은 서명과 은행이 얻은 서명을 연결시킬 수 없는 서명방법이다. 은행은 예금시 전자화폐가 은행에 되돌아 온 시점에서 이전에 사용된 전자화폐 데이터와 비교해서 이중사용 여부를 검사한다. 지불할 때 소비자와 상점뿐만 아니라 은행도 관여하는 경우를 on-line형 전자화폐라 한다. 이 지불 방식은 이미 사용된 전자화폐 데이터를 저장하고 온라인으로 상점의 검사요구에 대응할 수 있는 검색속도가 요구되므로 데이터베이스의 비용은 막대하게 된다.
- 둘째로, 스마트카드 지불시스템(smart card payment system)은 거대한 데이터베이스에 온라인으로 검색을 요구하는 이중 사용(double-spending) 방지책과 데이터베이스 검색, 조회시의 통신 등 큰 부하를 요구한다. 따라서 지불 프로토콜에 은행이 관여치 않고 사용자와 상점간의 통신만으로 실현하는 오프라인 전자화폐가 요구된다. 오프라인의 이중사용 방지책은 사용자와 상점의 거래가 완료한 후에 상점이 예금할 때에 이중사용을 검출한다. 부정행위 발생시 익명성을 제거하고 부정자의 신분을 노출하는 시스템을 소프트웨어만으로 실현하는 프로토콜이 제안되고 있다.

- 셋째로, 신용카드 지불시스템(credit card payment system)은 기존의 신용카드 지불시 교환되는 정보를 전자화 하는 것만으로 실현이 쉽지만 지불은 최종적으로 하나의 은행계좌에 대하여 행하여지므로 추적불가능성(사용자 사생활)은 보장할 수 없다. 신용카드 결제를 위해서 상점은 미리 신용카드 회사와 계약을 맺을 필요가 있다.
- 넷째로, 전자수표 지불시스템(electronic check payment system)은 현행 금융수표법과 수표 결제시스템에 변화를 주지 않고서도 시장에 적용할 수 있는 장점을 지니고 있다. 현행 수표 결제시스템의 처리 및 발행부분에 비용을 감소시키면서 현행 업무형태를 그대로 유지하는 것이 가능한 방법이다. 이러한 점은 기업간의 거래시 고액 지불이나 개인 대 개인 간의 소액지불도 가능하게 하며 기존의 금융업무가 전자상거래 특성을 지니도록 해주는 역할을 수행한다. 국외에서는 몇 개국(미국과 싱가폴 등)만이 관심을 갖고 시범서비스 도입할 예정으로 되어 있으며 국내에서는 아직 추진할 기미를 보이지 않고 있다.

가. 전자화폐 지불시스템

전자화폐에 의거한 지불시스템은 이용자들에게 높은 유연성과 안전성을 제공한다. 데이터에 의해 명시된 화폐는 작은 단위로 이루어지며 소액상품의 경제적인 구입을 가능하게 한다. 사용자 익명성의 보장으로 인하여 이 지불시스템은 스마트카드와 유사한 구조를 지닌다. 전자화폐에 의거한 지불시스템의 이용을 통하여 금융기관에 소비자는 익명(anonymity)으로 남을 수 있게 된다. 기타 지불시스템과 달리 소비자가 아닌 전자화폐를 인증 한다. 또한 자유롭게 자금이체가 가능하며 복제/이중복사 방지된다. 일반적으로 전자화폐의 데이터는 다음과 같은 정보를 내포한다:

- 일련번호(복수 발급되는 것을 검사하기 위하여)
- 화폐가치
- 발급기관
- 유효일
- 발급일

소비자는 이러한 데이터를 웹(www)-서버나 은행의 인터넷을 통한 특정한 지불소프트웨어, 또는 하나의 통화서버에 보관할 수 있는데, 이를 구매에 사용할 때까지 개인 컴퓨터에 저장한다. 이 지불시스템의 단점은 전자화폐의 중복 사용이 야기되기 때문에 화폐의 재검사에 많은 비용이 발생한다는 데에 있다. 현재 발표된 전자화폐의 종류는 다음 표 7과 같이 몇 가지를 예로 들 수 있다[14].

나. 스마트카드 지불시스템

이 시스템은 IC카드 등 부정방지장치(tamper resistant device)를 이용하는 시스템이다. 부정방지장치란 장치내의 내부정보에 대한 read/write가 불가능하다는 의미로서 소유자일지라도 데이터의 부정사용이 곤란한 IC카드를 전자지갑으로서 사용하여 안전한 전자화폐를 실현하려고 하는 것이다. 또한 개인간의 자유로운 자금이체가 가능하며 신용보증이 불필요한 장점을 지니고 있다. 또한 관리가 편리하며 높은 안전성을 지원한다. 가장 성공적인 사례가 Modex이다.

Mondex는 스마트카드기술에 기반을 두고 은행계좌와 연결된 off-line 카드지불시스템이다. 전화나 컴퓨터 네트워크 상에서 카드입력기를 통해 입출금을 하고 다른 Mondex카드로부터 현금교환도 가능하며 총 5종류의 통화로 저장할 수 있다. 이 시스템의 특징은 거래시 어떤 사인이나 카드 발행사로부터 거래 승인이 필요 없고 각 사용자간의 자금 이체가 자유롭게 이루어 질 수 있으며 개인의 프라이버시가 완벽하게 이루어질 수 있다는 점에서 많은 주목을 받고 있다[1].

표 7. 대표적인 전자화폐들의 특징

종 류	특 징
Digicash Company의 Ecash 전자화폐	· 네덜란드 Digicash사의 D.Chaum이 1994.10~1995.10에 연구 개발한 프로토콜 · 소비자와 상점이 Ecash를 이용하려면 이 지불시스템에 연결된 은행에 계좌를 개설 · 전자화폐를 유용하게 사용할 수 있도록 고안된 프로토콜 · 기본 암호 기법은 D.Chaum에 의해 개발되고 발표된 은닉서명의 방법 · 이를 통해 고객은 지불시 안전한 익명성이 보장 · 전자화폐는 전자지불 시스템에 가입된 상점만 이용가능 · Ecash 시스템에서는 RSA 공개키 암호 방식을 사용 · 은행으로부터 전자화폐를 인출하고 예금할 때는 사용하는 사용자의 전자지갑인 Cyberwallet과 Merchant 소프트웨어가 필요
남캘리포니아 대학의 Netcash	· NetCash는 남캘리포니아 대학의 정보과학 연구소(ISI: Information Sciences Institute)에서 개발한 전자화폐 · PayMe 시스템의 기초가 되었음 · NetCheque와 같은 전자수표 등의 금융도구와 교환이 가능한 분산 Currency Server(CS)를 기반으로 하고 있으며 전자화폐로 바꾸어 사용 할 수가 있음 · 즉, NetCash는 NetCheque시스템과 결합될 수 있음
PayMe	· Ecash와 Netcash 시스템들의 장점만을 취합하여 만들어 짐 · Netcash의 특징에 Ecash의 익명성의 장점을 제공하기 위한 것 · 은행은 일련번호를 가지고서 자기 자신의 전자화폐를 발행 · 전자화폐의 이중사용은 은행이 전자화폐에 대한 DataBase를 유지함으로써 방지 · PayMe 시스템에서는 두 개체 사이에서의 안전한 통신 프로토콜을 사용하기 위해 PMTP(PayMe Transfer Protocol)이라는 자체 통신 프로토콜을 사용하고 있음
CyberCash사의 Cybercoin	· Cybercoin은 Cybercash사에서 1996년부터 도입한 지불시스템 · 화폐는 Cybercoin과 연결이 되어있는 등록된 상점에서 발행 · Cybercoin의 일반적인 주요 기능 : 신용카드나 은행계좌를 통한 화폐발행, Wallet에서 입출 금된 사항의 명세서, 지불이행의 자동화, 복합은행기능 · 소액지불에서 이루어지는 pay per view 응용과 같은 값싼 디지털 컨텐츠 사업 범위에 유용하게 활용 · Cybercoin시스템에 가입하기 위해서는 소비자와 상점이 우선 Cybercoin에 계좌를 개설한 후, 전용프로그램 설치
Millicent	· Millicent는 Digital Equipment사에 의해 개발된 시스템 · 소액금액의 센트와 센트 미만까지도 지불을 허용 · Millicent 시스템의 주된 특징 : 화폐의 유통은 신용카드 또는 다른 지불시스템(고액 거래 기구)을 통하여 이루어짐, 은행으로부터의 독립 · 상점이 Millicent의 사용을 원할 경우 중개인(broker)과 상인 전용 증권(Millicent화폐)의 발급에 대한 계약을 체결하여야 함

다. 신용카드 지불시스템

신용카드형 지불시스템은 이미 널리 고객에게서 이용되고 있는 신용카드를 인터넷 전자상거래에서 사용하는 것으로 개방형 네트워크에서 많이 사용되고 있는 지불 방법이다. 그 이유는 이미 전세계적으로 널리 퍼져있고 표준화가 이루어져 있기 때문이다. 신용카드를 이용한 거래는 인터넷 거래와 같이 당사자간의 신용확인이 어려운 상황에서도 거래를 원활하게 하는 장점이 있다[1].

인터넷 신용카드 지불시스템 신용카드 기반의 지불시스템은 두 가지로 분류할 수 있는데, First Virtual이나 CyberCash와 같이 자체 기술력을 바탕으로 하는 신용카드를 통해 전자지불을 지원하는 방법과 비자나 마스타카드와 같이 신용카드 회사에서 직접 전자지불을 지원하는 방식이 그것이다. 신용카드 역시 실세계의 신용카드 지불 절차와 동일하게 이뤄지는데, 따라서 소액 거래보다는 신용카드 한도액을 넘지 않는 범위 내에서 거래(transaction) 비용을 상회하는 상당한 정도의 금액 거래 시 적당하다.

First Virtual의 그린커머스(Green Commerce) 모델은 전자상거래 상에서의 메시지 전달 모형이다. 이 모형은 신용카드 정보유출에 관한 대책, 상품 전달의 오류에 관한 대책을 메시지 전달의 절차를 통해 해결하고 있다. 이것은 기존의 인터넷 소프트웨어에 대한 사용자의 친숙성을 최대한 강조한 것이다. 고객이 상인에게 상품의 구입의사를 밝혔을 때 우선 상인은 그린커머스 서버에 대금의 지불을 요구하는 transfer_request 메시지를 전달한다. 그린커미스 서버는 고객에게 transfer_query 메시지를 전달해 준다. 그러면 구매확인 전자우편이 도착한다. 이 전자우편에 회신을 보냄으로써 구매의 절차가 완료된다. First Virtual은 거래비용을 절감하기 위해 대금지불을 일괄처리하고 있다. 한편, CyberCash는 CyberCash Wallet이라는 클라이언트 소프트웨어에 사용자 자신의 신상정보와 신용카드 정보를 입력한 후 사용한다.

신용카드를 이용한 지불은 거래와 보안상의 문제를 해결하는 것이 가장 중요하다. 이를 위해 VISA와 MasterCard는 SET(Secure Electronic Transaction) 프로토콜을 이용해 신용카드 지불 시스템을 만들고 있다. SET는 거래비용을 줄이고 보안을 유지하는 것을 목적으로 둔 프로토콜이다. SET에서는 신용카드 참여자를 카드소지자(cardholder), 발행자(issuer), 상인(merchant), 가맹점 모집업체(acquirer), 지불게이트(payment gateway), 브랜드(brand), 제3자(third parties)등으로 정의하고 있다. 발행자는 브랜드와 계약을 맺고 카드소유자에게 신용카드를 발급하는 은행이다. 가맹점 모집업체는 상인이 가맹점으로 가입한 기관이고 상인의 계좌를 갖는다. 지불게이트웨이는 신용카드 지불을 중개하는 서버로서 제3자에 둘 수 있고, 발행자나 가맹점 모집 업체가 운영할 수도 있다. 지불 게이트웨이에서는 지불요청, 승인, 지불 정보 확인 등의 작업을 한다. 이외에 인증기관(CA: Certificate Authority)이 있다. SET에서는 전자 상거래에서 고객과 상인이 서로를 확인할 수 없는 점을 이용해 상대방을 속이는 악의의 고객이나 상인을 막으려는 의도에서 고객과 상인에게 인증서를 발급해 주도록 하고 있다. 인증서를 발급하는 기관이 CA인 것이다.

신용카드 거래는 인터넷상에서 가장 활발히 이용되고 있는 지불시스템이다. 신용카드 지불 시스템의 가장 중요한 관건은 상인의 위치에서 믿을 수 있는 신용카드 소지자임을 확신하는 것과 고객의 입장에서 자신의 개인 정보유출이 없음을 확신할 수 있도록 해주는 것이다.

라. 전자수표 지불시스템

전자수표시스템 전자수표는 현실세계에서 사용되고 있는 종이로 된 수표를 그대로 인터넷상에 구현하고 있다. 전자수표의 사용자는 은행에 신용계좌를

갖고 있는 사용자로서 제한된다. 이 시스템은 발행자와 인수자의 신원에 대한 인증을 반드시 해야 하는 문제를 갖고 있다. 여기에 여러 가지 보안 기법들이 사용되고 있는데 이 때문에 거래 비용이 많이 들 수밖에 없다. 그러나 전자수표는 상당히 큰 액수의 거래, 기업간의 상거래의 지불 수단으로서 적합하며, 종이로 된 실세계의 수표보다는 처리비용이 적기 때문에 종이수표를 쓰는 것보다는 적은 액수의 지불에서도 사용이 가능하게 될 것이다[13].

전자수표는 전자 네트워크 상에서 안전한 가계 수표의 사용을 가능케 하는 전자 수표 시스템을 의미하며, WWW의 환경에서 스마트 토큰을 이용하여 실현되고 있다. 전자수표는 근본적으로 전자 서명 방식을 사용하므로 공개키 인증서를 이용해야 한다. 공개키 인증서는 X.509 공개키 인증서 표준을 채용하고 있으며, 전자 서명 시스템은 미국 표준 DSS(Digital Signature Standard) 서명 방식이다. 이 전자 수표에 대한 데모는 1995년 9월 21일 미국의 샌프란시스코 아메리카 은행에서 시행되었으며, 이 컨소시엄에 참여하고 있는 주요 은행은 미국 은행, 보스턴 은행, 몬트리올 은행, Bank one, 화학 은행 등이며, 전자화폐를 실현하는 기술을 지원하는 회사는 IBM, Sun Microsystems, Telequip 사, 그리고 Bellcore 등이다. 전자수표의 대표적인 흐름은 아래 그림 15와 같다.

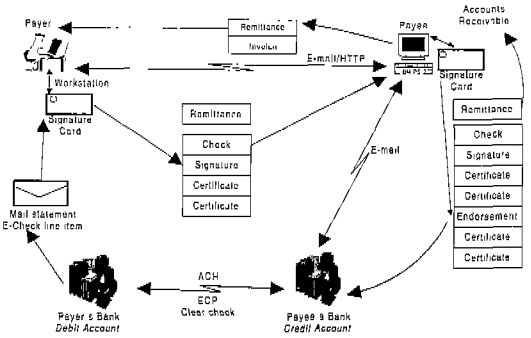

그림 15. 전자 수표의 흐름

먼저 수표 발행기관 또는 지불자는 수표 수신인 또는 수표 수취인으로부터 수표의 발행을 요구하는 인보이스(Invoice)를 수신한 후 자신의 스마트 토큰에 저장되어 있는 서명용 개인키로 전자 수표를 발행하고, 발행된 전자 서명문과 자신의 서명용 공개키에 대응되는 공개키 인증서를 전자 우편으로 전자 수표 수취인에게 전송하며, 전자 수표 수취인은 자신이 거래하는 은행으로 전자 수표 발행기관의 서명문과 공개키 인증서를 함께 보낸다. 은행은 전자 수표를 처리한다. 그리고 수취인의 은행과 지불자의 은행은 금융 거래를 정리한다. 이와 같은 전자 수표의 장점은 실현 비용이 낮고, 실현이 용이하다는 점이다.

미국 정부에서 지원하는 FSTC(Financial Services Technology Consortium)에서 프로젝트로 수행중인 Echeck도 전자수표시스템의 하나이다. 이 시스템은 서버가 없이 사용자간에 전자 수표의 교환으로 거래가 이루어진다. 이 시스템의 특징은 PCMCIA카드를 이용한 하드웨어 기반서명방법을 쓰는 데 있다. 이 서명카드를 인식하는 장치를 컴퓨터에 설치하고 이 카드가 있어야 수표에 서명하고 배서할 수 있다. 사용자 인증은 사용자의 거래은행과 연방준비은행이 공개키 방식의 전자 서명을 응용하여 계층적으로 해 주고 있다. 그리고 이 시스템은 현존하는 은행간 결제통로를 최대한 활용하려 하고 있다.

이외에 전자수표시스템으로는 캘리포니아 대학에서 Netcash와 함께 개발한 전자수표시스템이 NetCheque이고, NetChex,영국의 가상은행인 BankNet에서 발행하는 ECheque 등이 있다.

3. 전자지불시스템의 비교

다음 표 8은 대표적인 국외 전자지불시스템을 특징별로 비교한 것이다. 국외에서는 주로 신용카드 기반의 지불시스템이 많이 사용되고 있으나 더불어

스마트카드와 전자화폐형도 급속히 개발되고 있다. 전자화폐와 스마트카드형은 기본적으로 사용자의 익명성 및 이중사용방지 기술이 접목되어 있다[1][15].

표 8. 전자지불시스템을 특징별로 비교

제 품	지불 메커니즘	비 고
Mondex	스마트카드형	· 마이크로칩을 이용한 보안 · 하드웨어형, 양도 가능
Cyber Coin	전자화폐	· RSA, DES을 이용한 보안 · 소프트웨어형, 양도 불가
Ecash	전자화폐	· RSA을 이용한 보안 · 소프트웨어형, 양도불가
PayMe	전자화폐	· 대칭/비대칭키 암호를 이용한 보안 · 소프트웨어형, 양도불가
NetCash	전자수표	· Kerberos authentication을 이용한 보안 · 소프트웨어형, 양도불가
Millicent	전자화폐	· 소프트웨어형, 양도불가
EIPaN	스마트카드형	· microchip을 이용한 보안 · 하드웨어형, 양도불가
NetFare	스마트카드형	· card number & PIN을 이용한 보안 · 하드웨어형, 양도불가
Cyber Cash	신용카드형	· 전자지갑을 이용
Net Cheque	전자수표형	· Kerberos를 이용한 보안
Echeck	전자수표형	· 서버 불필요
VISA Cash	스마트카드형	· 1회용과 재충전용으로 구분
First Virtual	신용카드형	· 암호화 미사용

4. 국내의 전자지불시스템 현황

국내에서도 현재 신용카드 결재 및 은행을 이용한 온라인 현금송금을 중심으로 한 전자지불 시스템에 대한 연구를 수행하고 있다. 표 9는 국내 전자지불 시스템의 동향을 나열한 것이다. 현재 국내 지불방법으로는 신용카드 결재와 은행을 통한 온라인 현금송금이 주류를 차지한다. 대부분이 SSL 방식이며 전자지갑, 선불카드, 사이버카드 등이 있다[15].

표 9. 국내 전자지불시스템 현황

전자지불시스템	지불수단	특 징
한국정보통신(주)의 EasyCash	전자 현금형	· 선불형, 네트워크형, 가치충전형 소액결제 · 128비트 SSL 암호화기능
이니시스의 Inipay	전자 현금형	· 신용카드, 계좌이체, 직불카드 지불방식 · SET과 non-SET 기반 지불처리 지원
동성정보통신(주)의 Icash	전자 현금형	· 1024비트 RSA 및 DES 암호 사용 · 소액지불 가능
MSI Korea의 eGate	전자 현금형	· 결제 서비스: 국제간, USD 결제, 대금정산 · 인증 서비스: SSL 적용
데이콤의 eCredit	신용 카드형	· SET 프로토콜 적용 · RSA/DES/SSL 암호알고리즘 적용
한국정보통신(주)의 EasyPayDirect	신용 카드형	· 128비트 SSL 암호화 및 키 사용 · 지불서버에 의한 결제
LG-EDS System의 SmartPay	신용 카드형	· 카드 승인 : 결제대행 및 결제중계 · 결제방식 : SSL, 전자지갑, SET 방식
Altwell I&C의 Mypay.net	신용 카드형	· 1024비트 RSA 암호사용 · 지불 결과의 전자메일전송
한국사이버페이먼트(주)의 PayPlus	신용 카드형	· SSL 지불중계 서비스 · SET 지불중계 서비스
Dreamdata의 Paymatics	신용 카드형	· SET 프로토콜 적용 · CA, POS 지원

V. 결 론

정보화 시대에 가장 큰 변화는 경제활동의 변화를 들 수 있을 것이다. 기존에 존재하던 많은 실물 시장(real Market)은 가상 공간(cyber Space)상으로 발전하게 되고 이 속에서 디지털데이터를 근간으로 각종 구입, 판매 그리고 대금 지불이 이루어지게 될 것이다. 이러한 환경에서 가장 중요하게 거론되고 있는 것은 환경변화에 따른 기존 지불 방법의 문제점이다. 따라서 이와 관련된 지불시스템에 관한

연구가 지속적으로 계속되어 왔다. 다른 연구분야와 달리 실질적인 경제효과를 거둘 수 있고 파급효과가 커서 각 선진기술 국가나 선진기술 민간 업체들에 의해 앞다투어 개발되고 있다.

전자지불시스템의 확대는 사용자의 편이성 및 거래비용의 감소를 제공한다. 국내 지불시스템 중에서 앞으로는 소지가 간편하고 신용카드에 비하여 상대적 낮은 비용이 제공되는 전자화폐형 지불시스템이 많이 사용될 것으로 예상된다. 왜냐하면 비즈니스 설문조사에 의하면 국내 소비자들이 수표를 선호하는 국외와 달리 지불수단으로 현금을 선호하는 경향으로 조사됐기 때문이다. 이것은 향후 전자지불시스템 중에서 전자수표보다는 전자현금 기반 시스템이 많이 사용될 것을 시사한다고 볼 수 있다.

이에 따라 국내 각 기관에서는 이후에 예상될 수 있는 몇 가지 이슈에 대비해야 할 것이다. 우선 안전한 전자지불시스템은 강력한 암호방식에 그 바탕을 두고 있다. 따라서 현재 미국주도에 의해 개발된 암호방식의 법/기술적 한계를 이겨내기 위한 방안을 제시하여야 한다. 국내 전자지불시스템의 활성화를 위해 공개키기반구조를 적극 활용하고 독자적 암호기술 개발에 정부차원의 투자가 더욱 가속화하여야 할 것이다. 둘째로 전자지불시스템에서 제공하는 편리함에 역기능을 막기 위해 개인정보 보호원칙을 더욱 철저히 하여야 할 것이다. 전자지불시스템에 확산에 따른 개인정보 노출은 개인의 프라이버시를 침해하고 나아가 사회적 물의를 일으키게 된다. 따라서 정부정책기관에서는 이러한 오용을 막을 수 있는 적합한 정책 및 법제도를 점진적으로 강화해 나가야 할 것으로 본다.

※참고문헌

[1] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영, "전자상거래 보안 기술", 생능출판사, 1999.

[2] 주재훈, "한국의 전자상거래 환경을 고려한 전자지불 시스템의 성공요인 분석", 경영정보학연구, 제9권 제1호, 한국경영정보학회, 1999. 3.

[3] A. Menezes. P. Van Oorschot and S. Vanstone, "Handbook of Applied Cryptography". CRC Press. 1997.

[4] Philip Karlton, Paul C. Kocher, "The SSL Protocol Version 3.0", Netscape Communications, November 18, 1996, Http://home.netscape.com/eng/ssl3/

[5] William Stallings, "Cryptography And Network Security: Principle and Practice" second edition.

[6] Advanced Encryption Standard (AES) Development Effort, Http://CSRC.NIST.GOV/encryption/aes/aes_home.htm

[7] 한국정보보호센터, "KCDSA(Korea Certificate-based Digital Signature Standard)", 1997.6.

[8] 강경식, 류영규, 류종호, 봉호, 이재로, 염흥열, "선진국의 정보보호기술 개발사업 동향분석 및 국내 대응방향 연구", 정보통신부진흥원, 1999.6-1999.12.

[9] NIST PKI Program, Http://csrc.nist.gov/pki/welcome.html

[10] Jan Camenisch, Ueli Maurer, Markus Stadler, "Digital Payment Systems with Passive Anonymity-Revoking Trustees", Journal of computer Security, IOS Press. 1997.

[11] D. Chaum, "Blind signature systems", In D. Chaum, editor, Advance in Cryptology-CRYPTO '83,

pp. 153. Plenum, 1983.
[12] SET LLC, 웹사이트 Http://www.setco.org/
[13] 한국전산원, "전자지불 표준 동향분석에 관한 연구 (CALS/EC 기술 및 모델 개발 사업)", 연구보고서 1998.6.
[14] 한국전산원, "EUREKA 프로젝트 : 전자지불시스템", 연구보고서
[15] 박영수, 정교일, 손승원, "전자지불시스템 개발 동향", 개방형보안기술과 정보보호응용 워크샵-3rd OSTA'00, 93-109, 2000.4.5,

류 종 호

1998년 순천향대학교 전자공학과 졸업
2000년 순천향대학교 전자공학과 석사
2000년~현재 순천향대학교 전자공학과 박사과정
관심분야 : 네트워크보안, 전자화폐

염 흥 열

1981년 한양대학교 전자공학과 졸업
1983년 한양대학교 대학원 전자공학과 석사
1990년 한양대학교 대학원 전자공학과 박사
1982년~1990년 한국전자통신연구소 선임연구원
1990년~현재 순천향대학교 공과대학 정보기술공학부 부교수
1997년~2000년 순천향대학교 산업기술연구소 소장
2000년~현재 순천향대 산학연컨소시엄사업단 단장
1997년~현재 한국통신정보보호학회 총무이사
관심분야 : 전자상거래 보안, 공개키 기반 구조, 암호 이른, 부호이른, 이동통신보안