□정보산업동향□

전자지불 시스템 기술 및 표준 동향 분석

정 준 원† 정 성 원†† 김 영 균††† 이 민 우††††

◈ 목 차

요 약

거듭되는 정보통신 기술의 발전으로 네트워크 환경이 향상되면서 일반인들의 인터넷 사용이 폭발적으로 늘어가고 있다. 이와 같이 거대한 인터넷 사용자들을 대상으로 하는 전자상거래(Electronic Commerce)에 대한 관심이 증대되고 많은 사람들이 전자상거래에 참여하고자 하지만 여기에는 제도적, 기술적으로 선결되어야 할 문제들이 있다. 이 중에서 특히 기술적으로는 대금 결재의 안전 보장과 전자적인 처리를 위하여 전자지불 시스템이 시급하다고 할 수 있다. 본 연구에서는 그 동안 개발되어온 전자지불 시스템들에 대하여 현황을 분석하여 사용환경, 지불방식 등에 따라서 분류하고 각 지불 시스템의 기술적 특징, 장단점 및 개발현황 그리고 표준화 현황에 대해서 알아보려고 한다.

본 연구는 1997년 한국전산원이 정보통신부의 출연금으로 수행한 정보통신연구개발사업의 연구결과인 "전자지불 시스템 표준동향 분석에 관한 연구" 보고서를 발췌한 것입니다.

† 정회원 : 한국전산원 표준연구실 연구원
†† 정회원 : 한국전산원 표준본부 선임연구원
††† 정회원 : 한국전산원 주임연구원
†††† 정회원 : 한국전산원 표준연구실 주임연구원

1. 서론

인터넷 사용자의 증가에 따른 국내외 인터넷상의 전자상거래 규모의 발전 추이는 96년 약 5억 1,800만 달러를 기록했던 세계 전자상거래 시장 규모가 오는 2000년에 65억 7,900만 달러에 이를 것이며, 국내 전자상거래 시장 규모도 순수한 전자시장 매출만 96년에는 약 14억원을 기록했지만 2000년에는 약 613억에 이를 것으로 전망된다[1]. 인터넷을 통한 전자상거래에서 판매자는 인터넷상에 자신의 상품 또는 서비스를 광고할 홈페이지나 쇼핑몰을 구축하고 소비자는 쇼핑을 위해

간단히 인터넷에 접속하여 브라우저를 통해 자신이 원하는 상품 또는 서비스를 최적의 가격으로 구할 수 있다. 이러한 전자상거래에 대한 관심이 증대되고 많은 사람들이 전자상거래에 참여하고자 하지만 여기에는 제도적, 기술적으로 선결되어야 할 문제들이 있다. 이중에서 무엇보다도 가장 중요한 부분이 대금 지불에 대한 메커니즘이다. 상거래에서 돈을 주고받는 메커니즘이 명확히 제시되지 않으면 전자상거래의 기본이 흔들릴 수밖에 없다. 따라서 이러한 문제를 해결하기 위해서는 기술적으로 대금 결제의 안전을 보장할 수 있으며, 전자적인 방법으로 처리할 수 있도록 하는 전자지불 시스템이 필요하다.

전자지불이란 기존의 화폐 개념을 네트워크 상으로 옮겨 디지털화 한 무형의 화폐 또는 지불 수단을 말한다. 전자지불 분야는 거대한 인터넷 시장을 인식한 여러 은행, 신용카드 업체, 정보기술 업체 등 관련업계들의 치열한 경쟁과 연구, 실험을 통하여 몇 년 사이에 급속한 발전을 거듭하였다. 현재는 인터넷 전자상거래에 안전한 지불을 보장하는 여러 전자지불 시스템들이 상용화를 시작하고 있는 단계이다. 지금까지 경쟁적으로 개발, 발전해온 전자지불 프로토콜들은 기술적 발전에 많은 도움을 주었지만 상용화시키려는 현 시점에서는 각 지불 시스템간의 상호 호환성의 확보에 대한 문제가 심각히 제기되고 있다. 이에 작게는 각 지불 방식에 따른 지불 프로토콜의 표준화 작업과 여러 지불 방식에 대해서 상호 호환성을 가지게 하려는 사실 표준화 작업들이 진행 중에 있다. 따라서 아직 개발 초기에 있는 국내 전자상거래 시장에서의 혼란을 막고 경쟁력을 갖추기 위해서는 현재 개발되고 있는 전자지불 시스템에 대한 분류, 특징, 동향 등을 분석하고 국제 표준화 현황을 파악하는 것이 매우 중요하다. 따라서 본 연구에서는 2장에서 전자지불 시스템의 분류 및 기술동향에 대해 알아보고, 3장에서는 국내외 전자지불 표준화 동향에 대해서 논의하도록 하겠다.

2. 전자지불 시스템 기술 동향

전자지불 시스템은 지금까지 많은 연구자들 각자가 설정한 기준에 따라서 여러 가지 방식으로 분류되어 왔으며, 이러한 예로는 사용되는 기술, 지불 형태, 지불 방식 등에 따른 분류 등이 있었다 [2][3][4][5][6]. 그러나 기존의 연구는 기술적으로 매우 빠른 속도로 발전하고 있는 현재 상황의 전자지불 시스템을 적절히 분류하는데는 부족함이 있다. 따라서 본 절에서는 전자지불 시스템에 대해 가능한한 최근의 모든 전자지불 시스템에 대한 분류를 위하여 기존의 연구자들의 여러 가지 분류들을 종합하여 설정한 기준에 의해 분류 하고자 한다.

전자지불 시스템은 기존의 신용카드를 IC카드화하여 사용하는 IC카드기반 지불 시스템과 인터넷 등의 네트워크 상에서 사용되는 네트워크형 전자지불 시스템으로 크게 두 가지의 관점에서 발전되어 왔다. 따라서 본 연구에서는 우선 전자지불 시스템을 사용환경에 따라서 IC카드기반 지불시스템과 네트워크형 지불시스템으로 분류한다. 그리고 네트워크형 전자지불 시스템은 다시 지불 방식에 따라서 신용카드를 이용하며 암호화를 하지 않는 일반적인 지불 시스템, 중간에 지불 브로커를 두는 지불브로커 시스템, 전자현금 시스템, 전자수표 시스템, 소액의 지불을 위한 마이크로지불 시스템, 전자자금 이체로 분류한다. 다음절부터 앞에서 분류된 각각의 지불 시스템에 대한 특징과 국내외 개발 현황 등을 알아보도록 하겠다.

2.1 네트워크형 전자지불 시스템

2.1.1 신용카드 이용 일반 지불 시스템

기존의 통신 판매에서 인터넷을 통한 전자상거래가 이루어지면서 가장 먼저 또 가장 보편적으로 널리 사용된 방법으로서 기존에 사용되고 있는 신용카드를 그대로 사용한다. 이는 네트워크상에서 대금결제를 위해 판매자에게 자신의 신용카드 번호를 알려주는 방법이다. 이를 위해 CGI (Common Gateway Interface)를 통해 신용카드 번호를 전달하는 방법, 마찬가지로 CGI를 이용하지만 암호화를 이용하는 방법, 가입자 기반의 지불 방법 등이 이용된다[2]. 각 방법의 특징은 다음과 같다.

● CGI를 통해 신용카드 번호 전달

이 방법은 지불시스템을 쉽게 구성하여 사용할 수 있다는 장점이 있는 반면에 어떠한 암호화도 하지 않고 데이터를 보내기 때문에 신용카드 번호를 악용하기 위해 빼돌리려는 시도에 대해서 무방비 상태라고 할 수 있다. 또한 네트워크상의 판매회사에 자신의 신용카드 번호가 전달되는데, 과연 상대방 회사가 믿을 수 있는 곳인지에 대해서도 무방비 상태라고 할 수 있다. 또 매번 구매할 때마다 자신의 신용카드 번호를 입력해야 하는 불편함이 있다.

● CGI를 통해 신용카드 번호 전달

- 넷스케이프 SSL(Secured Socket Layer)

이 방식은 넷스케이프 서버와 클라이언트 사이의 SSL 암호화기법을 통해 신용 카드번호를 전송하는 것이다. 신용카드 번호가 SSL에 의해서 암호화되었기 때문에 중간에 가로채서 악용할 우려가 줄어든다. SSL은 특허관계 때문에 미국 내에서는 128bit 길이의 키(key)로 암호화를 하지만, 미국 밖에서는 40bit길이의 키로 암호화하고 있는데, RSA연구소에서는 기업의 경우에는 1024bit, 개인적인 사용의 경우에는 768bit, 증명작업의 인가를 위한 키와 같은 침해의 가능성이 높은 곳에는 2048bit를 권한다. 따라서 40bit의 키로는 여전히 완벽한 보안이 유지된다고 믿기는 힘들다.

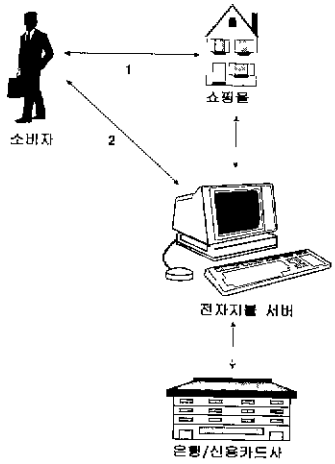
● 가입자 기반의 지불

인터넷상의 상품 판매를 위한 회사에 미리 회원으로 가입하여 가입된 사람들만 사용할 수 있도록 하는 것으로 사용자는 가입할 때 자신의 정보(주소, 이름, ID, 지불방식-신용카드번호)를 입력해서 ID와 패스워드를 부여받는다. 상품을 구매하려 할 때는 단지 자신의 ID와 패스워드를 입력하여 자신의 지불 정보를 제공하고 상거래를 하는 방식이다. 최근 규모가 큰 서버들을 중심으로 많이 이용된다. 초기 등록시 CGI를 이용하므로 이때 정보가 누출의 위험이 있으며, 인터넷 상거래 사이트가 증가해서 서버마다 가입을 요구한다면 사용자들은 수천 개의 ID와 패스워드를 가지게 되는 불편을 초래한다.

2.1.2 지불 브로커 시스템

지불 브로커 시스템은 기존의 온라인 지불 메커니즘을 최대한 활용하면서 최종 사용자들은 네트워크 상에서 온라인 지불을 가능하도록 하는 것이다. 즉 사용자가 네트워크 상에서 신용카드 번호나 계좌 번호 등을 암호화해서 전달하고 실제 지불은 기존의 신용카드 결제나 은행 계좌의 잔고에서 자금이체 형태로 이루어지는 것이다. 이를 구현하는 형태는 여러 가지가 있을 수가 있으나 가장 전형적인 형태로 사용자와 상점은 네트워크를 통해 접속하고 상점과 은행 또는 신용카드사와의 사이에 지불 브로커를 두고 이를 통하여 실제 지불이 일어나도록 하는 것이다. 이러한 지불 브로커 시스템은 크게 상점 게이트웨이 모델(Merchant Gateway Model : MGM)과 트라이앵글 모델(Triangle Model : TM)이 있다[6]. 상점 게이트웨이 모델은 상점 서버가 소비자측에서 보내는 지불관련 정보 중에 해석 가능한 정보와 해석 불가능한 정보를 모두 받아서 해석 가능한 정보(원하는 상품 규격 등)를 해석하고 나머지 해석

불가능한 부분(은행 계좌번호 또는 신용카드번호 등)을 지불 브로커에 보내 지불을 요구하는 것이며, 트라이앵글 모델은 소비자가 직접 지불 서버에 지불을 요구하는 것이다. 상점 게이트웨이 모델의 지불 시스템의 메커니즘은 <그림 2.1>과 같으며, 이에 대해 간단히 살펴보면 다음과 같다.



(그림 2.1) 지불 브로커 시스템 모델

- 소비자가 네트워크에 접속하여 쇼핑몰에서 원하는 상품을 주문한다.
- 쇼핑몰은 해당 상품의 지불요구서를 보낸다.
- 소비자는 자신의 은행계좌/카드번호 및 구매정보를 암호화하여 쇼핑몰에 보낸다.
- 쇼핑몰은 해독할 수 없는 부분을 전자지불 서버에 이를 보내 지불정보를 확인한다.
- 전자지불 서버는 계좌/카드번호를 은행/신용카드사에 보내 지불정보를 확인한다.
- 은행/신용카드사는 지불 서버에 해당 소비자의 지불 정보를 확인해주고 지불한다.
- 전자지불 서버는 판매자에게 지불을 확인해주고, 소비자에게 영수증을 발행한다.

트라이앵글 모델의 경우에는 <그림 2.1>의 2와 같이 소비자가 상품 대금의 지불을 위해 전자지불 서버에 직접 은행 계좌번호 또는 신용 카드번호를 암호화하여 보낸다는 것이 다르다.

일반적으로 지불 브로커 시스템의 경우에는 전자 지불 서버를 제공하는 측에서 사용자의 편의를 위해서 전자지갑(Electronic Wallet)을 제공한다. 전자지갑은 소비자의 PC에 있는 클라이언트 소프트웨어로 소비자가 미리 자신의 은행계좌 등의 정보를 기입해두며, 인터넷 쇼핑몰에서 원하는 상품을 고른 후 지불을 하려고 하면 자동으로 구동되어 소비자의 구매를 위한 정보들을 판매자에게 또는 지불 서버에 암호화하여 보내주는 역할을 한다. 이러한 구조는 신용카드를 사용하는 경우 기존의 지불 메커니즘을 이용하기 때문에 쉽게 구현할 수 있다는 장점이 있다. 그러나 이러한 지불 구조의 단점은 브로커를 중간에 둠으로써 브로커 시스템에 대해 조회비용 및 수수료 등이 발생한다는 것이다. 경우에 따라서는 이 중으로 수수료를 내야하는 경우도 발생할 수 있다. 따라서 소액 지불의 경우(IP에 대한 정보나 문서 조회 비용 등)에는 부적합하다고 할 수 있다. 지불 브로커 시스템의 주요 개발 현황은 다음과 같으며 현재 전자상거래의 지불 방법으로 가장 많이 사용되고 있다고 볼 수 있다.

- FV(First Virtual사) : 기본적인 웹 브라우저와 전자 메일을 이용해 전자 지불 시스템을 구축했다. 특별한 암호화를 사용하지 않고 보안상의 문제에 대한 대응책으로 전화, FAX, 메일을 이용해 보완하고 있다.
- CyberCash(CyberCash사) : 신용카드를 이용한 거래에서 발생할 수 있는 문제점을 개선한 방법으로 소비자, 판매자, CyberCash 사이에서 전자거래가 이루어진다. 소비자는 CyberCash Wallet이라는 프로그램을 이용해 사용자 계정과 신용카드 정보를 기록

한 후 이용한다. 거래처는 CyberCash로부터 상점 자격을 인증 받은 후 자신의 상점에 대한 웹사이트를 구축한다. CyberCash는 거래를 원하는 구매자와 상인에게 서로를 인증시켜 주고 신용카드 회사나 은행으로부터 대금을 인출해 상인에게 전달한다.

- SmartWallet(V-One사) : Spyglass, CheckFree, Tandem, V-One사가 공동으로 만든 EBC (Electronic Business Co-operation)의 산출물로 만든 전자 지불시스템으로 EBC wallet이라고도 한다. 사용방법 및 설치 등이 CyberCash와 유사하다.
- CFWallet(CheckFree사) : 미국의 신용카드 조회 회사인 CheckFree사가 만든 전자 지불 프로토콜
- iKP(IBM): 유럽의 EUROPAY International 신용카드 회사와 IBM이 제휴해 만든 프로토콜
- Secure Courier(넷스케이프) : MasterCard사와 넷스케이프사가 제휴해 지원하는 전자지불 프로토콜
- SEPP(Master Card) : MasterCard사가 Secure Courier를 기반으로 만든 전자 지불 프로토콜
- STT(Secure Transaction Technology): VISA사와 Microsoft사가 함께 만든 전자 지불 응용 프로토콜

국내에서는 데이콤이 자체 개발한 데이콤Wallet이 있다. 데이콤Wallet은 지불 브로커 형식의 지불시스템으로 소비자는 전자지불을 지원하는 은행의 이체 가능한 PC 뱅킹 서비스에 가입하여 자신의 은행계좌를 이용하여 전자지불을 이용할 수 있다[7].

2.1.3 전자현금 시스템

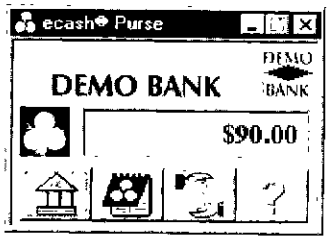
전자현금 시스템은 수표나 신용카드 등의 다른 형태의 전자 지불 시스템이 실세계의 화폐에 그 기반을 두고 운용되는 것에 반하여 인터넷상에서 통용되는 새로운 화폐의 발행 및 유통에 있다고 할 수 있다. 따라서 전자현금 시스템은 인터넷상에서 지불방법으로 가장 이상적이며, 전자지불 시스템의 궁극적인 목표라고 할 수 있다. 전자현금이 실용화되고 활성화되면 온라인 상에서의 소액 직접거래 등 실생활에서 가능한 모든 지불형태가 가능하게 된다.

실생활의 현금을 모델로 하는 전자현금이 원활하게 유통되기 위해서 가져야 할 특성으로는 익명성(Anonymity), 보안성(Security), 휴대 가능성(Portability), 양방향성(Two-way)등이 있다. 그 중 익명성은 개인의 사생활이 침해를 막고, 개인 정보가 악용될 가능성을 배제하기 위하여 매우 중요하다고 할 수 있다. 그 외에 전자현금에서 기술적으로 중요한 문제는 보안성 문제로서 전자현금의 '이중사용' 및 '불법 복제'의 금지이다. 화폐를 발행한 은행이 반드시 자신이 발행한 화폐임을 확인할 수 있어야 하는 불법 복제의 방지 및 상호 인증과 함께 앞에 언급된 익명성을 보장한다는 것은 상충되는 목표라고 할 수 있다. 따라서 이러한 두 가지의 문제를 적절하게 해결하는 것이 전자현금 시스템의 가장 큰 기술적 난점이라고 할 수 있다. 기술적인 문제 외에 사회적 경제적 요소로는 전자현금에 대한 일반의 가치 인정, 전자현금을 사용한 수입에 대한 세금 계산 문제, 실제 화폐와의 교환, 그리고 국제환전 등이 있다.

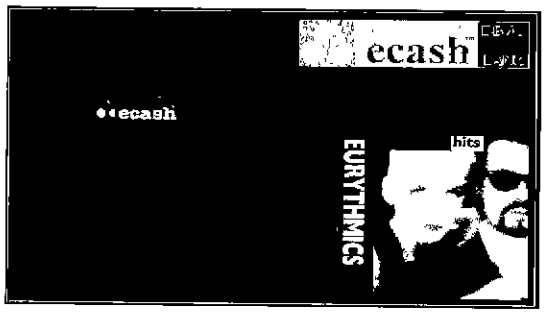
전자현금을 개발한 대표적인 예는 가장 먼저 인터넷상에서 전자현금 서비스를 시작한 네덜란드의 DigiCash이다. DigiCash는 1994년 10월부터 ECash라는 전자현금을 발행해 오고 있고 사용자

들은 Digital Wallet이라는 클라이언트 소프트웨어를 이용하여 ECash 중앙 은행인 FDB(First Digital Bank)에서 전자 현금을 인출하기도 하고 지불을 하고 예금을 할 수도 있다. 이 전자 현금은 초기에 사용자들에게 $100씩을 무료로 나누어주어 사용할 수 있도록 했던 시험 단계를 거쳐 지금은 미국의 마크 트웨인 은행과 핀란드의 EUnet에서 실세계의 화폐와 교환도 하고 은행 서비스도 받을 수 있다.

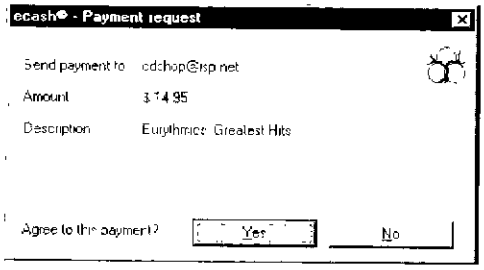
DigiCash의 사용 예를 간단히 살펴보겠다. 소비자가 인터넷을 통해서 음악 CD를 구입하려 한다면 먼저 ECash를 사용하기 위한 계정이 있어야 하고 전자지갑에 <그림 2.2.a>과 같이 일정액의 금액이 들어 있어야 한다. 다음으로 <그림 2.2.b>과 같이 ECash로 음악 CD를 살 수 있는 사이트로 연결하고 지불버튼을 누른다. 그러면 상점에서 보내는 지불 요구가 <그림 2.2.c>과 같이 나타나게 되며 구입을 하기로 결정하면 'Yes'를 누른다. <그림 2.2.d>이 보이면서 소비자의 전자지갑은 해당 금액을 상점에 지불한다. 상점이 지불을 확인하면 <그림 2.2.e>이 보이고 주문한 음악 CD는 우편으로 배달이 된다. 이때 전자지갑의 상태를 보면 <그림 2.2.f>과 같이 지불된 금액만큼이 빠진 상태가 되며 트랜젝션 로그를 확인해보면 <그림 2.2.g>과 같이 자신이 전자지갑을 이용한 기록들이 남게된다.



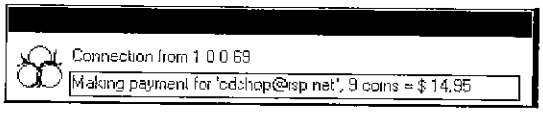
(그림 2.2.a)
ECash-지불전 전자지갑



(그림 2.2.b) ECash-CD상점 예

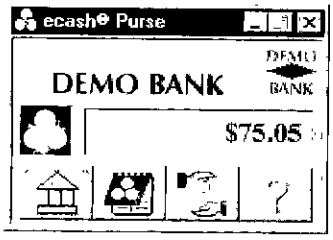


(그림 2.2.c) ECash-지불요구 화면 예

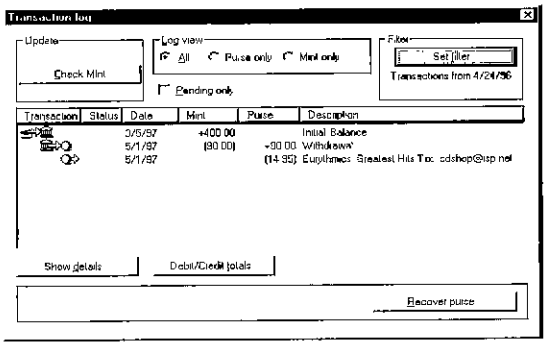


(그림 2.2.d) ECash-지불화면 예

(그림 2.2.e) ECash-지불완료 예



(그림 2.2.f) ECash-지불후
전자지갑



(그림 2.2.g) ECash-지불기록 예

DigiCash는 익명성의 보장을 위해 Blinded Withdrawal이라는 방법으로 화폐를 발행하고 있다. 또한 사용된 현금은 일단 FDB에 가서 불법적으로 복사된 전자 현금인지 아닌지 판단하게 된다. 한번 사용된 화폐를 모두 기록해야 하는 불편함 때문에 ECash는 사용 기한이 정해져 있다는 불편함이 있다. 즉, 한번 인출한 돈은 기한 이내에 사용하든지 다시 저금했다가 인출하든지 해야만 한다. 그 외에 전자현금 시스템으로는 캘리포니아 대학에서 개발한 NetCash가 있다.

국내에서의 전자현금 시스템을 개발, 활용하려는 움직임은 주로 IC카드를 이용하는 방식으로 추진되고 있다. 정보통신진흥협회 산하 전자화폐연구회에서 한국형 전자화폐의 연구 개발을 위해 법, 제도 워킹그룹(WG), 기술WG, 서비스개발WG 등 3개의 워킹그룹을 구성하여 활동중이다. 전자화폐연구회는 한국형 전자화폐의 기본 개발 방향을 오프라인 상태뿐만 아니라 네트워크를 통해 전자상거래를 할 경우에도 결제수단으로 활용할 수 있도록 개발하는 것을 기본 원칙으로 하고 있다. 또 물품과 서비스의 대금으로 받은 전자화폐는 금융기관을 통하지 않고 개인용 단말기에서도 화폐가치를 이전할 수 있도록 개발하기로 하였다.

2.1.4 전자수표 시스템

전자수표는 현실세계에서 사용되고 있는 종이로 된 수표를 그대로 인터넷상에 구현하고 있다. 전자수표의 사용자는 은행에 신용 계좌를 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 트랜잭션 비용이 많이 들게 된다. 따라서 전자수표는 상당히 큰 액수의 거래, 기업간의 상거래의 지불 수단으로서 적합하다.

이러한 시스템의 예로 캘리포니아 대학에서 NetCash와 함께 개발 중에 있는 전자 수표 시스템인 NetCheque가 있다. NetCheque는 NetCash와 마찬가지로 분산된 여러 개의 서버를 갖는 모델을 채우고 있다. 여러 대의 복수 서버를 둠으로써 규모성(scalability)을 제공하고 있는 것이다. 이 시스템은 분산된 서버 사이에서 사용자의 인증과 서명을 위해 인증을 위한 전문 시스템인 Kerberos에 기반을 두고 있다. 또한 NetCheque는 공개키 암호화 방식보다 효율적인 재래식의 암호화 방식을 사용함으로써 아주 적은 액수의 지불에 대한 정산도 가능하게 한다.

미국 정부에서 지원하는 Financial Services Technology Consortium (FSTC)에서 프로젝트로 수행 중인 ECheck도 전자 수표 시스템의 하나이다. 이 시스템은 서버가 없이 사용자간에 전자 수표의 교환으로 거래가 이루어진다. 이 시스템의 특징은 PCMCIA 카드를 이용한 하드웨어 기반 서명 방법을 쓰는 데 있다. 이 서명 카드를 인식하는 장치를 컴퓨터에 설치하고 이 카드가 있어야 수표에 서명하고 배서할 수 있다. 사용자 인증은 사용자의 거래 은행과 연방준비은행이 공개키 방식의 전자 서명을 응용하여 계층적으로 해 주고 있다. 그리고 이 시스템은 현존하는 은행간 결제 통로(ACH, ECP)를 최대한 활용하려 하고 있다[8]. 이외의 전자 수표 시스템으로는 Carnegie Mellon 대학에서 개발한 NetBill, NetChex, 영국의 가상 은행

인 BankNet에서 발행하는 ECheque 등이 있다.

2.1.5 마이크로지불 시스템

인터넷을 통한 전자상거래에서 실제로 팔리는 상품들의 가격은 지불브로커 시스템의 경우 지불에 들어가는 수수료보다 크고 지불 한도액보다는 작아야 한다. 이러한 지불 시스템은 상품의 가격이 어느 정도 되는 것일 때 유효하지만, 만약 구매하려는 상품의 가격이 소액이어서 오히려 수수료가 더 크다면 문제이다. 만일 전자지불에 소요되는 비용이 실제 거래 액보다 많을 경우에는 현실적으로 전자적인 거래가 이루어질 수 없다. 그러나 인터넷상에서 이루어지는 상거래의 많은 부분이 소액인 경우(시간당 서비스, 파일 등)가 상당히 많이 있다. 이러한 소액 지불을 위한 지불방법으로 마이크로지불 시스템이라 하는 지불방식이 개발되었다.

마이크로지불 시스템은 일반거래에 비해 트랜잭션 수가 매우 많기 때문에 이에 대해 신속한 처리가 요구된다. 따라서 소액의 경우에는 보안레벨이 낮기 때문에 빠른 처리속도와 트랜잭션의 비용을 줄이기 위해서 단순한 암호화 방식을 적용하여 구현할 수 있다. 이러한 소액지불을 위한 방법으로는 Digital사의 Millicent, W3C의 MPTP (MicroPayment Transfer Protocol)등이 최근 활발히 검토되고 있다.

마이크로지불 시스템의 예로는 이미 개발되어 운영되고 있는 것으로 CyberCash사의 CyberCoin이 있으며, 이는 수수료 없이 소액을 결제할 수 있는 시스템이다. 국내에서는 데이콤이 CyberCash사와 합작법인을 설립하여 CyberCoin을 도입하여 서비스를 실시할 예정이다.

2.1.6 전자자금 이체

최근 WWW 기반으로 인터넷상의 가상 은행이 생겨나고 있다. 가상 은행은 물리적인 지점, 본점을 운영하지 않고 모든 것을 WWW상에서 사용자와 인터페이스 함으로써 운영되는 은행을 말한다. 가상 은행이 기존의 홈뱅킹이나 현금지급기보다 편리한 점은 좀 더 폭 넓은 서비스를 시간, 공간의 제약 없이 받을 수 있다는데 있다. 또한 인터넷을 이용한 프로세스 처리가 무척 값싸기 때문에 수수료가 훨씬 적거나 없다는 점에서 우수하다[8].

인터넷상에서만 운영되는 가상 은행(Cyberbank)의 예로는 SFNB(Security First Network Bank)가 있으며, 전자자금 이체에 관한 다양한 서비스를 제공함으로서 자금이체를 이용한 전자 지불을 가능하게 해주고 있다. 우선 단순하게 자금 이체를 하는 Quick Pay 서비스가 있다. 이것은 지불대상과 금액만 입력하면 자금 이체가 일어나게 되어 있는데, 미리 자금 이체할 시간을 설정하여 지불을 예약하는 것도 가능하다. 만약 지불 대상이 전자 자금 이체를 통한 전자 지불을 받지 못할 경우 SFNB에서는 자동적으로 수표를 발행하여 지불을 하도록 해주고 예금을 인출해 간다. 또한 정기 적인 지불도 자유자재로 설정이 가능하다. 또, 고객이 수표를 쓰기 원할 때에는 수표책을 보내주어 종이 수표를 발행하는 것이 가능하도록 해 준다. 고객에게 수표를 받은 사람이 이 수표를 SFNB에 제시하면 SFNB는 이 수표를 스캐닝하여 보관함으로써 나중에 수표를 발행했던 고객이 조회, 확인이 가능하도록 서비스를 해준다. SFNB의 경우 매월 20회의 자금 이체를 통한 전자 지불을 무료로 지원하며, 200장의 수표책을 수수료 없이 사용할 수 있도록 하여준다. 또한 개인의 재무 서비스까지 함께 해 주고 있다. 고객의 지출을 분야별로, 지불 방식별로 보고서를 작성해 주며 전문가와의 재무 상담도 가능하다. 또한 SFNB는 WWW을 이용하여 모든 인터페이스를 처리하고 있어 사용자의 편리성을 극대화하고 있다.

2.2 IC카드기반 전자지불 시스템

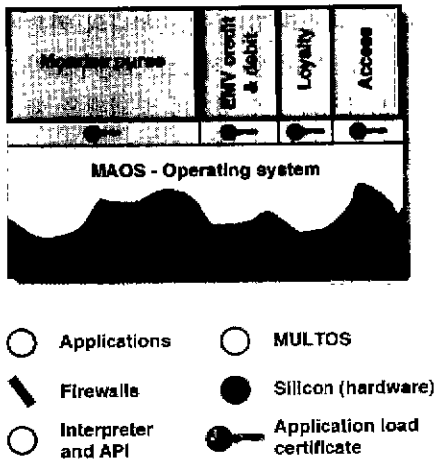
IC카드는 기존의 마그네틱 카드와는 달리 IC메모리(EPROM)와 마이크로프로세서를 카드에 봉입한 것을 말한다. CPU 내장카드는 8비트 마이크로프로세서와 2천~8천자 정도의 대용량 메모리가 내장된 것으로 판단 능력, 데이터 보호능력을 갖추고 독자적인 운영체제로 응용 서비스를 스스로 처리할 수 있다. 또한 암호 알고리즘을 내장하고 있어 카드소유자의 신분 확인이나 상호인증, 입출력 데이터의 암호화와 정보 저장 등도 가능하다. 이렇게 기존의 마그네틱 카드에 비하여 대용량의 메모리, 처리능력, 보안성 등의 장점을 가진 IC카드를 은행카드 혹은 신용카드에 적용하려는 관련 업계의 노력이 진행되어 왔다. 이러한 예로는 신용카드를 IC카드화하기 위한 통일규격인 EMV (EUROPAY, MasterCard and VISA)와, IC카드 기반기술인 MULTOS(Multi-application Operating System)가 있으며, 가장 대표적인 지불시스템으로는 몬덱스카드가 있다. 본 절에서는 우선 IC카드를 이용하는 지불시스템의 대표적인 규격, 기술 및 시스템인 EMV, MULTOS, 몬덱스에 관하여 논의하고, 전자지불 시스템 도입을 위한 국내외 여러 국가의 전략 및 동향에 대해서 알아보고, 이어서 향후 전망에 대해서 알아보기로 한다.

2.2.1 EMV

신용카드 업계의 선두주자인 VISA와 MasterCard 그리고 EUROPAY가 신용카드를 IC카드화하기 위한 통일규격인 EMV(EUROPAY, MasterCard and VISA)사양을 95년 6월에 만들었다. 그리고 VISA와 MasterCard는 향후 5년 이내에 지금의 플라스틱 신용카드를 전부 IC카드로 전환하기로 계획하고 있다. IC카드를 사용하기 위해서는 현재 전세계적으로 보급된 기존의 카드조회 단말기를 IC카드를 인식하는 단말기와 필요한 소프트웨어로 교체해야 하는 어려움이 있다. 하지만 업계의 노력으로 IC카드의 사용이 지속적으로 확산될 것으로 보인다. EMV규격의 IC카드는 기존의 신용카드와 동일한 기능을 하지만, 내부의 기술적으로는 소프트웨어 가상지갑에서 사용하는 공개키 암호화(Public Key Encryption)기법을 이용한 암호화를 사용하고있다. 또한 IC카드는 전자 현금의 기능을 가질 수 있어서 현금지급기에서 일정금액을 미리 인출해서 IC카드에 담고 다니면서 상품을 살 때, 이 금액을 지불할 수가 있다. 이는 선불/직불시스템을 응용한 전자현금과 같은 방식이다. 이러한 EMV규격의 IC카드의 실용화를 위해 MasterCard사는 95년부터 호주의 캔베라시에서 4개 은행, 1000개의 상점, 1만 명의 사용자를 대상으로 실험서비스를 시작했다. 이외에 유럽 각국 13개 회사 및 대학이 연합해서 만든 시스템으로 CAFE(Conditional Access For Europe)가 있다.

2.2.2 IC카드 기반기술(MULTOS)

MULTOS(Multi-application Operating System)는 MasterCard사의 IC카드 전략의 핵심요소일 뿐만 아니라 세계 각국이 전자화폐의 기반기술로 받아들이고 있는 핵심기술로 개방형 플랫폼을 제공하고 있다[10].



(그림 2.3) MULTOS의 구조

<그림 2.3>과 같이 MULTOS는 시스템 구조상 운영체제와 독립된 응용서비스를 구현할 수 있도록 설계되어 있다. MULTOS는 응용서비스의 상품성을 보장하고 보안성을 확보해 주는 고유의 값을 지닌 키(Key)를 응용서비스별로 가질 수 있도록 IC카드에 최적화된 MULTOS 실행 언어(MULTOS Enabling Language)와 MEL이 MULTOS 운영체제와 인터페이스하기 위한 MAOS(Multi-Application Operating System)-API(Application Programming Interface), 어플리케이션간을 분리 해주는 방화벽 등으로 구성되어 있다.

MAOS-API는 다양한 응용서비스를 구현할 수 있도록 해주는 반면 응용 서비스별로 고유의 키를 가지도록 함으로써 신뢰성과 보안성을 강화한 것이 특징이다. 방화벽은 응용서비스 프로그램이 내 외부적인 요인으로 깨졌을 경우 타 프로그램에 영향을 주지 않도록 어플리케이션과 API간을 분리하기 위해 채택한 것이다. 방화벽이 없었던 기존의 IC카드에서는 각 응용서비스의 보안체계가 동일해 성격이 서로 다른 응용서비스를 하나의 카드에 구현했을 때 어느 하나의 응용서비스의 보안체계가 붕괴된다면 시스템 전체의 보안체계가 무너지는 결과를 초래하게 된다. 이로 인해 전자화폐 서비스와 ID기능을 하나의 카드에 동시에 구현했을 경우 상대적으로 보안구조가 취약한 ID기능 서비스의 보안체계가 붕괴됐을 때 전자화폐에 영향을 미쳐 심각한 문제를 초래할 수도 있었다. 반면에 MULTOS는 방화벽기능을 통해 응용서비스간 상호 간섭하는 것을 배제함으로써 여타 응용서비스와 무관하게 서비스간 독자적인 보안체계를 구축할 수 있도록 설계되어 있는 것이다. 또 MULTOS는 원격지에서 응용서비스를 다운로드 받거나 기존의 카드 내 서비스를 갱신 및 삭제가 가능하도록 설계되어 있다.

현재 MasterCard사는 MULTOS를 이미 개발 완료하고 IC칩에 탑재, 98년초 상용화를 목표로 시험 운용 중에 있으며 MULTOS의 산업표준화를 위해 97년 9월부터 제공하고 있는 어플리케이션 라이선스도 이미 60여 개 업체에 발급했고 어플리케이션 개발도구도 공개할 예정으로 있다. 이와 관련하여 MasterCard사는 선마이크로시스템사와 자바2.0API를 개발키로 합의, MULTOS에 자바 API를 수용하기로 하고 세계적인 칩 생산업체 및 IC카드업체를 중심으로 MAOSCO 라는 비영리법인인 컨소시엄을 올 초 구성하고 활동에 들어간 상태다. 현재 이 컨소시엄에는 전세계 70여 개 기업이 참여를 타진중이며 국내 IC카드업체인 삼성전자와 LG정보통신, 등도 컨소시엄참여를 위한 제안서를 제출했다.

2.2.3 몬덱스

몬덱스(Mondex)는 IC카드를 이용한 전자지불서비스의 대표적인 시스템이며, 이는 영국의 Westminst은행과 Midland은행이 중심이 되어 "몬덱스 UK"를 설립하여 95년 7월부터 IC카드를 이용한 전자현금 서비스를 시작했다.

몬덱스카드는 IC카드의 COS(Chip Operating System)에 종속적으로 정해진 서비스만을 구현할 수 있었던 폐쇄형 플랫폼을 적용한 IC 카드와는 달리 카드발급자(은행)가 IC칩 공급자에 독립적으로 다양한 응용서비스를 손쉽게 추가, 운용할 수 있도록 지원하는 MULTOS(Multi-application Operating System)를 개발 과정에 적용하였다.

MULTOS 기술은 기본적으로 전세계 기업들에 공개하는 것을 원칙으로 하고 있어 급속한 보급이 예상된다. 따라서 앞으로 세계 각국에서 추진되는 전자화폐의 기반기술은 개방형플랫폼을 제공하는 MULTOS를 기반으로 추진될 전망이다. 그 외에도 몬덱스카드는 칩 내부에 5개국의 화폐를 입력할 수 있고 최근의 거래내역 10개를 차례로 기록할 수 있는 기능을 갖고 있다. 몬덱스카드

의 구조는 개방형 시스템방식이기 때문에 은행의 중앙시스템을 거치지 않고 카드간이나 개인간에 화폐를 교환할 수 있다. 개인간 자금이체 기능은 기존에 사용하고 있는 현금과 동일한 방법으로 IC카드 메모리에 디지털 데이터 형태로 보유하고 있는 화폐가치를 결제할 상대방과 손쉽게 주고받을 수 있도록 지원하는 것이다. 따라서 통신망 등을 통해 은행의 중앙시스템을 거치지 않고 오프라인상태에서 화폐의 가치이전 처리가 가능하다는 것이다. 이렇게 되면 화폐 발행 은행은 전산시스템 구축비용이 절감되고, 카드 발급과 가맹점 관리비용을 줄일 수 있다. 그리고 온라인 거래에 따른 시스템 과부하나 사용자의 과다한 통신비용에 대한 걱정을 덜 수 있다는 장점이 있다.

2.2.4 국내외 동향

유럽 각국의 IC카드를 이용한 전자지불 시스템 구축 및 사용 현황은 다음과 같다. 최근에 들어서 선진 10개국 중앙은행에서는 세계적인 표준으로 자리잡아 가고 있는 몬덱스카드의 개념과 규격을 수용하고 개인간 자금 이체 서비스를 허용하기로 하였다. 우선 벨기에의 경우 불사의 IC카드를 채택하여 주유소, 전화기, 가맹점 등에서 사용하고 있으며 전자지갑의 발행자 자격을 은행에 국한하고 있다. 또한 전자지갑에 저장된 가치를 상품용역 대가 이외에 사용하는 것을 허용하지 않으며 은행 계좌를 이용한 개인간의 자금이체도 허용하지 않았다. 최근 벨기에는 기존의 독자적 프로젝트를 버리고 몬덱스 방식으로 추진하려는 움직임을 보이고 있다. 프랑스의 경우 현재 IC카드 방식의 직불카드가 비교적 많이 보급되어 있는 상황이다. 또 버스, 지하철 등 교통 카드용으로 IC카드를 사용하고 있다. 프랑스는 향후 IC카드를 활용한 전자지갑을 개발, 보급한다는 계획을 세워놓고 있다. 포르투갈은 SIBS에서 직불 및 전자지갑(PMB)카드 보급계획으로 각 은행에서 발급한 직불카드와 IC카드 방식의 전자지갑을 병행하여 사용한다. 먼저 은행에 계좌를 개설한 후 카드로 현금지급기를 통해 일정금액을 인출하고 전자지갑을 삽입하면 해당금액이 전자지갑에 저장되는 방식이다. 스페인은 중앙은행 산하기관인 「SEMP」에서 전자지갑의 도입을 추진하고 있다. 스페인은 98년까지 직불카드, 신용카드, 전자지갑을 하나의 카드로 통합하고 인터넷 등을 활용해 전자지갑에 저장 및 송금이 가능하도록 추진할 계획이다. 미국의 경우 지난 애틀랜타 올림픽 기간동안 비자 인터내셔널사가 「비자캐시카드」를 시범 운용했다. 비자 캐시카드는 미국에서 처음으로 발급된 IC카드 방식의 전자지갑으로 애틀랜타 시내 1천5백 개의 가맹점에서 1백70 만장이 발급됐다. 비자 카드는 이와 함께 현금지급기를 통해 금액가치를 재 저장하여 반복 사용이 가능한 현금지갑 카드를 발급했다[3]. 일본의 경우 몬덱스카드 형식의 금융서비스를 도입하기로 하여, 일본 대장성은 "몬덱스 프로젝트" 추진 계획을 세워 전자화폐 전쟁에서 우위를 확보하여 몬덱스 관련 세계시장을 석권한다는 계획을 세워 놓고 있다.

96년 7월에는 MasterCard International이 주도하고, AT&T, 체이스맨해튼은행 등 전세계 19개 주요기관들이 참여해 설립한 몬덱스인터내셔날이라는 조직이 IC카드 이용 전자화폐의 표준화를 추진하고 있다.

국내에서는 금융결제원이 97년초 전자지갑 시범사업을 추진하기로 하고 서울은행을 비롯한 17개 시중 은행과 IC카드 관련 업체들을 중심으로 전자지갑 공동이용 시스템 구축 실무작업반을 구성하였다. 마스타카드코리아는 국내 사정상 개인간 자금이체 서비스를 제외한 몬덱스카드를 발급하기로 하였다. 동성정보통신에서는 IC카드 솔루션인 'SCIENCE'를 개발하였다. 이는 IC카드의 전자지갑 기능을 이용해 전자화폐로 직접 대금 결

제를 할 수 있으며, 온라인 상에서 인터넷 가상은행에 전자화폐의 예금 및 출금 등 다양한 뱅킹서비스를 이용할 수 있다. 한국은행은 금융결제원에서 추진하고 있던 전자지갑 표준에 국제적인 신용카드 표준인 EMV를 수용하여 신용, 직불(현금) 카드 기능을 함께 구현한 종합 금융IC카드를 개발하는 것을 골자로 하는 '금융기관의 IC카드 공동이용시스템 구축 추진방안'을 마련하고 개발을 추진하고 있다. 삼성전자, 현대전자, LG정보통신 등 3대 국내 칩 공급사의 COS를 DES암호화 알고리즘에 입각한 하나의 COS로 표준화하여 금융IC카드에 적용하며, SI업체로는 동성정보통신, 한국정보통신, 단말기는 백두정보기술이 개발하고, 10여개 시중 은행과 금융결제원 등이 개발에 참여하고 있다.

3. 전자지불 시스템의 표준화 동향

전자지불 시스템은 관련업계들의 많은 연구, 실험을 통하여 급속한 발전을 거듭하여 현재는 상용화를 시작하고 있는 단계이지만 독자적으로 발전해온 전자지불 시스템들간의 상호 운용성 확보의 문제가 제기되고 있다. 이에 많은 관련 업계 및 학계가 참여하여 SET, JEPI, MPTP 등 표준화 작업들이 진행 중에 있다. 본 장에서는 이에 대하여 자세히 알아보도록 하겠다.

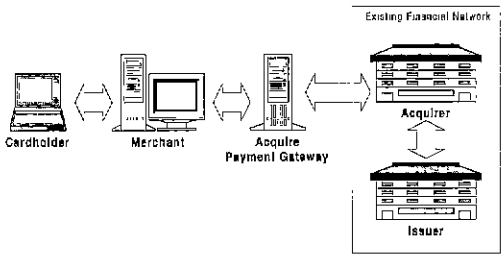
3.1 SET

3.1.1 개요

인터넷 등 네트워크를 이용한 전자상거래가 활성화되면서 상품구매, 서비스 대금을 안전하게 상점에 지불할 수 있는 방법이 필요하게 되었다. 이에 지불의 수단으로 신용카드를 이용하는 경우에 한하여 신용카드 업계와 정보기술 업계의 선두주자인 VISA와 MasterCard 그리고 마이크로소프트, IBM, 넷스케이프, SAIC, GTE, RSA, Terisa, VeriSign사가 공동으로 작업하여 SET(Secure Electronic Transaction)이라는 전자지불 프로토콜을 만들었다. SET은 안전한 지불을 위해 정보의 기밀성 유지와 메시지의 무결성 보장, 트랜잭션에 관련된 당사자간의 인증에 초점을 맞추고 있다. 그러나 SET이 이미 존재하고 있는 많은 인터넷 보안관련 프로토콜에 비하여 다른 점은 디지털 증명(digital certificate)에 대하여 정의하고 있다는 점이다. 디지털 증명은 지불 트랜잭션에 관련된 모든 당사자들(소비자, 상점, 지불 게이트웨이 등)을 인증하는데 사용된다[13].

3.1.2 SET 구조

SET은 지불 트랜잭션과 관련된 카드소지자, 상점, 취득자간의 금융정보의 전달을 막기 위한 구조를 가지고 있다. <그림 2.7>에 나타나 있는 SET의 구성요소들 간의 상호작용을 감안하여 SET에서 정의하고 있는 전자 쇼핑 모델을 단계별로 알아보면 다음과 같다.



(그림 2.7) SET의 구조

① 카드소지자(cardholder)는 원하는 상품을 찾는다. 인터넷의 경우 브라우저를 이용하여 전자 카탈로그 또는 상점 사이트를 보면서 상품을 고를 수 있고, 그 외 경우 종이로 된 카탈로그를 보면서 상품을 고를 수도 있다.

② 카드소지자는 상점으로부터 사고자하는 상품을 선택한다.

③ 카드소지자는 상점으로부터 사려는 상품의 리스트, 가격, 세금 및 선적료 등을 포함한 주문서를 받는다. 이러한 주문서는 상점 서버로부터 전자적으로 보내지거나 카드소지자의 쇼핑을 위한 소프트웨어로부터 작성된다.

④ 카드소지자는 지불 방식을 선택한다. SET은 이용자가 카드를 이용한 지불을 선택하였을 때에만 관련된다.

⑤ 카드소지자는 선택한 지불 방식과 완성된 주문서를 상점에 보내게 된다. SET을 이용하는 경우 주문서와 지불 방식에 대한 정보는 카드소지자의 디지털 서명이 되어 보내진다.

⑥ 상점은 취득자(acquirer)를 통해 카드소지자와 거래하는 금융기관(은행 신용카드회사)에 지불 인증을 요구한다. 인증이 성공하면 주문서에 대한 확인서를 보내준다.

⑦ 상점은 주문된 상품을 선적하거나 서비스를 실시한다.

⑧ 상점은 취득자(acquirer)를 통해서 카드소지자와 거래하는 금융기관(은행 또는 신용카드회사)에 지불을 요구한다.

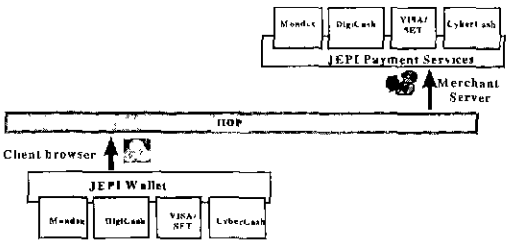
3.1.3 현황

96년 2월 VISA, MasterCard 등이 주축이 되어 SET 규격을 발표한 후 97년 현재 SET Secure Electronic Transaction 규격 1.0 버전이 발표된 상태이며, IBM, 마이크로소프트 등 많은 솔루션 제공자들이 SET를 이용하는 지불 시스템들을 개발하여 상용화하고 있다. 국내에서도 국제표준화 되고 있는 SET을 수용하여 한국적 SET을 제정하려는 움직임을 보이고 있다.

3.2 JEPI

3.2.1 개요

전자상거래를 지원하기 위해서 다양한 인터넷 지불 프로토콜이 제안되었고 적용되어 왔으나 대부분의 지불 프로토콜들은 상호 호환성이 없었고, 또한 각자의 프로토콜을 버리고 단일화할 전망은 거의 없었다고 할 수 있다. 실질적으로, 암호화 필요성, 트랜잭션 수, 트랜잭션에 따른 비용, 인증의 필요성 등 각자 다른 요구 조건을 만족시키기 위해서 각기 다른 지불 메커니즘들이 존재할 수밖에 없었다고 할 수 있다. 따라서 이미 개발된 각자의 프로토콜을 버리지 않고 호환성을 얻을 수 있는 방법에 대한 연구로 JEPI 프로젝트가 진행되고 있다. JEPI(Joint Electronic Payment Initiative)는 W3C와 CommerceNet의 많은 산업계 협력자들이 인터넷상에서의 쇼핑이 끝나고 지불이 시작되기 전까지 발생하는 프로세스를 연구하는 조인트 프로젝트이다. JEPI 프로젝트가 목표로 하는 것은 다중 지불 시스템 하에서 소비자나 판매자 모두가 주어진 어떠한 트랜잭션에 대해서도 적절한 지불 시스템을 선택하는 과정을 도와준다는 것이다. 이때 중요한 것은 지불이 이루어지는 트랜잭션이 일어나기 전에 소비자와 상점 서버 사이에 어떠한 지불 수단(신용카드, 전자현금, 전자수표 등)을 사용할 것인지에 대한 동의가 반드시 있어야 한다는 것이다[11]. JEPI에서는 판매자가 소비자에게 자신이 받아들일 수 있는 지불 방식의 리스트를 제공하고 소비자는 자신이 원하는 지불방식을 선택한다. JEPI는 <그림 2.4>와 같이 만약 서버에 A, B라는 지불 시스템이 인스톨되어 있고, 클라이언트에 C, D라는 전자지갑이 인스톨되어 있을 때는 JEPI가 변환기능을 가지지 않기 때문에 할 수 있는 일이 없다는 것이다. 그러나 만약 서버에 A, B, C 라는 지불 시스템이 인스톨되어 있고, 클라이언트에 C, D의 전자지갑이 인스톨되어 있다면 JEPI는 프로토콜 협상을 거쳐 지불을 위한 수단으로 C를 선택할 수 있다는 것이다.



(그림 2.4) JEPI 협상 프로토콜

3.2.2 JEPI 구조

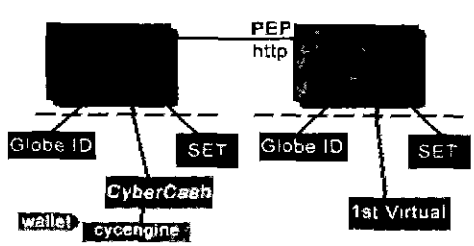
JEPI는 크게 다음의 두 부분의 협상 프로토콜로 이루어져 있다.

- PEP를 기반으로 한 일반적인 목적의 협상 프로토콜

  웹 클라이언트와 서버가 서로간에 각각 어떤 확장모듈(extension module)을 지원하는지 묻고, 이러한 확장에 대하여 협상하며, 사용가능한 확장을 이용하여 통신을 개시할 것을 요구한다.

- UPP

  특정한 확장모듈로 지불 도구(신용카드, 전자현금, 전자수표 등)와 브랜드(VISA, MasterCard 등), 그리고 지불 프로토콜(SET, CyberCash 등)에 대하여 협상한다. 이 작업이 JEPI 프로젝트에서 주로 이루어지는 부분이다. <그림 2.5>는 지불에 대해 협상과 선택을 하기 위해 PEP, UPP 층이 HTTP 통신 위에 스택과 같은 역할을 하는 JEPI의 구조를 보여준다.



<그림 2.5> JEPI의 구조

3.2.3 현황

JEPI 프로젝트는 95, 96년에 걸쳐 W3C와 CommerceNet에 의해 JEPI Phase1이 만들어 졌으며, 96년 10월 프로토콜 규격과 JEPI Demonstrator가 발표되고, 97년 2월 실행 가능한 데모가 구현됐으며, 3월에는 JEPI 논문이 나왔고, 4월에는 WWW6 컨퍼런스에서 JEPI 프리젠테이션과 데모가 있었다. 현재 JEPI의 파일럿이 개발되어 있는 상태이며, JEPI는 96년판 PEP에 기반을 두고 있는데 그 이후로 개정되어 IETF에 새로운 버전의 PEP가 제출되어 있는 상태이다. 이것이 받아들여지게 되면 HTTP의 일부분이 될 것이다. UPP 규격은 96년 PEP 드래프트에 기반하고 있으며 PEP가 개정될 때까지는 변화가 없다.

3.3 MPTP

정보의 단위가 상대적으로 작은 소액지불시스템에 대한 관심이 점차 증가하고 있는 추세이며, 이러한 시스템에서는 정보의 처리속도와 비용이 가장 큰 관건이 된다. MPTP (MicroPayment Transfer Protocol)는 잦은 거래가 발생하는 두 상대방간에 소액거래에 적합하도록 최적화된 프로토콜이다. 이 프로토콜은 사기 등 불법행위를 막을 수 있는 높은 등급의 보안을 제공하여 형태가 있는 제품의 판매를 포함하여, 넓은 범위에서 적용이 가능하도록 하였다[14]. 또, MPTP는 판매자와 소비자가 공통의 브로커를 이용하는 경우에 사용될 수 있으며, 소액지불의 보안을 위해 공개키 알고리즘 보안방식을 사용하며, HTTP와 SMTP /MIME을 포함하는 다양한 인터넷 프로토콜을 기반으로 구현된다. MPTP는 지불의 흐름이 일방적인 특정 거래를 제외하고는 소비자와 판매자간의 구분이 없는 비동기 프로토콜이며, 대칭적인 프로토콜이다. 웹을 이용한 소액지불시스템은 소규모와 대규모의 제공자 모두에게 경제적인 구

현이 가능하도록 해 주어야 하기 때문에 MPTP는 판매자 할부상환을 통하여 소액지불 거래를 제공한다. 그리고, 공개키 서명방식을 채택함으로써 소자본가들도 경제적으로 적용할 수 있다.

3.4 IC 카드 표준

IC카드란 IC메모리 또는 마이크로컴퓨터를 크레디트카드, ID카드 등에 봉입한 것으로 기존의 마그네틱 카드와 비교하여, 데이터 보관 및 자체 처리 능력 등에서 장점을 지닌다. IC카드는 때로 칩카드, 스마트카드, 인텔리전트카드 등으로도 불리며 금융결제용, 프로그램 수납용, 공중전화용, 신분증명용 등 넓은 분야에 사용된다. IC카드에 대한 국제표준으로는 국제표준기구(ISO)의 기술위원회 TC97/SC17/WG4에서 표준화했고, TC/68/SC2/ WG7에서는 IC카드 이용한 은행업무의 보안에 관한 표준화를, TC68/SC5/WG5에서는 IC카드와 단말기 사이의 메시지 데이터 교환에 대해 표준화되었다.

4. 결 론

본 연구에서는 현재 국내외에서 현재 개발되고 있는 전자지불 시스템에 대한 연구사례를 수집하여 각 지불 시스템을 사용환경과 지불 방식에 따라서 분류하였다. 그리고 각 시스템의 기술적 특징, 장단점, 국내외 개발현황 등을 알아보았다. 또 이미 개발되어 있는 전자지불 시스템의 상호 호환성을 확보하기 위한 표준화 작업(JEPI, SET, MPTP 등) 현황과 세계 각국의 전자지불 시스템 도입 현황 및 전략과 국내의 현황을 알아보았다. 그리고 전자지불 시스템의 기반이 되는 요소기술로 IC카드기술(MULTOS)에 대해서 자세히 알아보았다.

현재 전자상거래에서 가장 많이 사용되고 있는 전자지불 시스템은 지불 브로커 시스템이다. 이것은 이미 존재하고 있던 신용카드를 그대로 이용하기 때문에 시스템 구축이 용이하기 때문이라고 할 수 있다. 여기에 보안을 위한 프로토콜로 SET이 사용되어 안전한 거래를 보장하고 있다. 그러나 최근 IC카드 기술의 발전으로 점차 IC카드를 이용한 지불 시스템이 사용될 것으로 보인다. 특히 몬덱스카드는 확실한 보안 메커니즘을 가지면서 현금을 대체하는 전자현금으로 사용될 수 있고, 네트워크를 기반으로 하는 전자지불 시스템에 비해서 현금을 네트웍세계가 아니라 실세계에서 이동하면서 사용할 수 있다는 장점들이 있다. 이러한 장점 때문에 많은 나라들이 몬덱스를 수용하려는 움직임을 보이고 있으며, 국제표준이 될 전망이다. 향후에는 몬덱스로 대표되는 IC카드 이용 전자지불 시스템과 네트워크형 전자지불 시스템이 연동되어 사용되기 위해 IC카드 리더기가 장착된 컴퓨터가 보급될 것으로 보인다. 결국 전자지불시스템은 네트워크를 기반으로 한 전자지불 시스템과 IC카드(스마트카드)를 기반으로 한 IC카드 응용 전자지불 시스템이 연동되어 사용되는 방향으로 나아갈 것이라는 예측이 지배적이다. 전자지불 시스템의 개발 초기에 있는 국내 전자상거래 시장에서 복잡한 전자지불 방식에 의한 혼란을 방지하기 위해서는 국제표준 동향을 면밀히 분석하여 수용하고 우리의 현실에 가장 적절한 전자지불 시스템을 구축해 나가야 할 것이다.

참고문헌

[1] 박재천, "전자상거래 구축전략", 제7회 전산망 기술 및 표준화심포지움, 1997

[2] 권도균, "WWW 보안과 전자화폐", WWW_KR, 1996

[3] 전자신문, "전자화폐", http://ee.tamu.edu/~skjo/ibook/Journal/Ecash7.html

[4] 홍필기, "전자화폐 도입을 위한 선행연구", 한

국전산원, 1997

[5] Tatsuo Tanaka, "Possible Economic Consequences of Digital Cash", http://gea01.pangea.org/inet96/b1/b1_1.htm

[6] 윤대균, "전자상거래 구축 기술 동향", 제7회 전산망 기술 및 표준화심포지움, 1997

[7] "데이콤 전자쇼핑서비스", http://paygate.gacom.co.kr/payment.html

[8] "미래의 화폐 II", http://www.codinet.com/ money/ document/future2.html

[9] 전자신문 용어검색, "IC 카드", http://www.etnews.co.kr

[10] "MULTOS(Multi-application Operating System)", http://www.multos.com/

[11] Eui-Suk Chung and Daniel Dardailler, "White Paper:Joint Electronic Payment Initiative(JEPI)", http://www.w3.org/Payments/white-paper.html, 1997

[12] "eCo System: CommerceNet's Architectural framework for Internet Commerce", CommerceNet, 1997

[13] "SET Secure Electronic Transaction Specification", VISA and MasterCard, 1997

[14] "Micro Payment Transfer Protocol(MPTP) Version0.1", W3C Working Draft, 1995, http:// www.w3.org/TR/WD-mptp

정 준 원

1995년 홍익대학교 전기제어공학과 (학사)
1997년 홍익대학교 대학원 전기제어공학과(지능제어 전공) (공학석사)
1995년-현재 한국전산원 표준연구실 연구원
관심분야 : 인공지능, 자바, 전자지불

정 성 원

1988년 서강대학교 전자계산학과 (학사)
1990년 M.S. in Computer Science at Michigan State University
1995년 Ph.D. in Computer Science at Michigan State University
1997년-현재 한국전산원 표준본부 선임연구원
관심분야 : CALS/EC, database issues in ITS, spatial indexing schemes, distributed databases, parallel processing for database system, scientific data models, and multimedia databases

김 영 균

1991년 한양대학교 전자계산학과 (학사)
1993년 한양대학교 대학원 전자계산학과 (석사)
1993년-1998년 한국전산원 주임연구원
1998년-현재 안산전문대 교수
관심분야 : 고속통신 기술, CALS/EC, DBMS, 시험인증

이 민 우

1993년 중앙대학교 산업정보학과 졸업(학사)
1993년-현재 한국전산원 표준연구실 주임연구원
관심분야 : CALS/EC, SGML