通信情報保護學會誌
第 10 券 第 2 號, 2000. 6

전자 지불 프로토콜 표준화 동향

김 종 우*, 송 주 석**

요 약

인터넷이 일반화되고 전자상거래가 활성화되면서 전자화된 시장에서 참여자들의 역할과 거래절차에 대한 프로토콜을 규정하는 활동들이 계속되어 왔다. 이러한 활동들은 주로 민간 산업계와 학계에서 주도하였으며 공식 표준화 단체에 의한 활동은 아직 미미하다. 수많은 연구기관 및 산업계에서 다양한 전자 지불 시스템을 개발하였으며 각각의 프로토콜이 상이하고 장단점이 있다. 본고에서는 현재 개발된 또는 개발중인 전자 지불 시스템 전자 화폐, 전자 수표, 신용카드 기반 전자 지불 시스템으로 나누어서 각각의 상이한 프로토콜에 대한 개요와 특징 및 현황에 대해서 살펴보고 이에 대한 표준화 동향에 대해서 이야기한다. 그리고 전자지불 프로토콜의 표준화와 관련해서 앞으로의 전망에 대해서 살펴본다.

Ⅰ. 서 론

월드 와이드 웹(WWW)의 등장과 더불어 인터넷 사용자가 폭발적으로 증가하고 있으며 인터넷을 통한 전자 상거래 서비스가 시작되고 있다. 전자 상거래의 규모에 관한 각 기관의 예측을 먼저 살펴보면 다음과 같다. OECD는 세계 기업간 전자상거래 규모를 '98년도에 260억불, 2003년에서 2005년 사이에 1조불에 이를 것으로 전망했고, 미국의 시장조사 기관인 IDC는 2003년의 세계 전자상거래 시장규모를 1조불로 예측했다. 또한 국내 시장 규모도 미국의 경제연구소 WEFA에 의하면 2003년에는 96.2억불을 기록할 것으로 예측하고 있다. 이런 여러 가지 통계 자료는 기업간 전자 상거래나 기업과 소비자간 전자 상거래 규모가 폭발적으로 증가할 것임을 시사해주고 있다. 이렇게 네트워크를 통한 상거래가 활발해 지면서 다양한 형태의 전자 지불 시스템이 설계되고 운용되고 있다. 국내에서는 전자 상거래 및 지불의 기능 정의 및 구현을 위해서 정보통신부, 국제 전자 상거래 연구센터(ICEC), 정보보호센터, Korea Cyber Payment, Commerce Net Korea 등 여러 기관 및 업체에서 전자 지불 관련 표준 및 솔루션을 제공하기 위한 노력을 하고 있다.[1]

전자 지불 시스템은 사용자의 지불 방법에 따라, 크게 전자 화폐 시스템, 전자 수표 시스템, 신용카드 기반 전자 지불 시스템으로 나눌 수 있다. 이 가운데 신용 카드 기반 전자 지불 시스템과 전자 화폐 시스템은 이미 여러 업체에서 다양한 방법으로 서비스하고 있다. 본고에서는 현재 개발되었거나 연구중인 다양한 전자 지불 시스템의 프로토콜을 분석하고 표준화와 관련하여 향후 전망에 대해서 살펴본다.

Ⅱ. 전자지불 시스템 분류 및 프로토콜 분석

전자 지불 시스템은 결제방식에 따라 크게 전자화폐(Electronic Money), 신용카드(Credit Card), 전자수표(Electronic Check)로 구분할 수 있다. 전자화폐는 다시 화폐가치 저장 매체에 따른 분류로 IC카드에 전자화폐를 저장하는 가치 저장형과, 인터넷상의 가상 은행 계좌 또는 인터넷과 연결된 고객의 PC에 전자화폐를 저장하는 네트워크형이 있다. 각 유형별 시스템을 알아보고 각각에 대한 현황 및

* 연세대학교 컴퓨터과학과 (ephemera@emerald.yonsei.ac.kr)
** 연세대학교 컴퓨터과학과 (jssong@emerald.yonsei.ac.kr)

동향을 분석한다.

1. 네트워크형 전자화폐 시스템

1.1 이캐쉬 (eCash)

네덜란드의 DigiCash사가 개발하여 서비스 중인 네트워크형 전자화폐 시스템으로서, 고객이 이캐쉬 발행은행으로부터 이캐쉬를 다운로드받아 자신의 Wallet에 저장시켰다가 상품구매 시 판매자에게 구매대금으로 제시하여 지불하는 방식이다[2].

이캐쉬 시스템의 구성 요소는 고객, 판매자, 이캐쉬 발행은행으로 이루어져 있다. 거래마다 공개키 연산이 사용되며, 온라인으로 이캐쉬를 검증한다.

이캐쉬 시스템에서는 동일한 이캐쉬 발행은행을 갖고 있는 고객간 이캐쉬의 이체가 가능하며, 지불처리도중 네트워크가 다운되거나 컴퓨터가 고장나는 경우, 잃어버린 이캐쉬 동전을 복구시킬 수 있는 메커니즘을 갖고 있다. 이캐쉬 시스템은 대부분의 웹 브라우저와 서버에 쉽게 통합될 수 있는 구조로 되어 있다. 이캐쉬는 은닉서명(Blind Signature) 기술을 사용하여 은행이 이캐쉬 동전의 일련번호를 알 수 없는 방법으로 은행으로부터 전자화폐를 인출하기 때문에 지급인에 대해 완전한 익명성을 제공할 수 있고, 이캐쉬 화폐 수취인의 발행은행을 통한 온라인 확인과정과 발행은행에서 한번 사용한 화폐의 모든 일련번호의 DB 저장과정을 통해 이캐쉬가 이중으로 사용되지 못하도록 하고 있다. 그러나 이용할 때마다 진위 및 이중 사용 여부를 고객 거래은행에 의뢰하여 체크하여야 하므로 시간이 많이 소요되며, Peak 시간대에는 통신 접속이 어려워 장시간 대기하여야 한다. 또한 위·변조 방지를 위하여 많은 비용이 소요되어 이용수수료가 높고, 거래내역 추적이 불가능하여 탈세, 자금의 해외도피 등의 수단으로 악용될 우려가 있다.

현재 DigiCash사는 eCash Technologies사로 흡수되었으며, 유럽과 호주 등에서는 아직 서비스를 실시중이지만, 미국의 Mark Twain 은행은 eCash 서비스를 중단하기로 결정한 상태이다.

1.2 밀리센트 (MilliCent)

밀리센트(Milicent)는 소액 거래를 처리하기 위해 DEC(Digital Equipment Corporation)에서 개발한 대표적인 전자 화폐 시스템의 일종으로 거래규모가 0.1 센트부터 5 달러 정도인 소액 지불 시스템이다[3]. 이 시스템은 고객이 판매자 또는 브로커가 발행하는 화폐적 가치를 지니지 않는 쿠폰의 일종인 스크립(Scrip)을 브로커(Broker)를 통해 구입, 상품 구매대금으로 제시하여 결제하는 방식을 취하고 있다.

밀리센트(MilliCent) 프로토콜의 구성요소는 고객, 판매자, 브로커다. 이중에서 브로커는 스크립의 발행자 또는 판매자로서 스크립 판매와 관련된 판매자와의 자금정산, 고객과 판매자의 계좌 보유, 브로커 및 판매자 스크립의 발행, 판매, 교환 등 판매자와 고객을 연결시키는 역할을 담당하므로, 신용도가 높은 은행, 신용카드사, ISP 등이 브로커 역할을 수행할 것으로 예상된다. 브로커는 실제 화폐를 다루는 유일한 참가자이므로, 고객과 판매자로부터 신뢰받아야 한다.

대부분의 네트워크형 전자화폐 시스템이 발행 기관에 직접 접속해서 진위와 이중 사용 여부를 확인하기 때문에 병목 현상이 야기되지만, 밀리센트 시스템에서는 특정 판매자가 발행한 스크립은 특정 점포에서만 이용될 수 있기 때문에 범용성은 없는 형태이나 판매자가 직접 스크립 진위 및 이중사용 여부를 확인할 수 있는 분산처리방식이기 때문이 특정 지불 중계기관이 확인하는 집중처리방식보다 효율적이고 거래 수수료도 낮추는 효과를 가져 올 수 있게 되었다.

또한 밀리센트 시스템에서는 거래 당사자들이 서로를 신뢰를 할 수 있도록 브로커, 고객, 판매자중 어느 한쪽이 스크립을 위·변조하는 등의 부정행위를 하였을 때에는 다른 두 당사자들이 부정행위를 쉽게 증명할 수 있게 하였다. 예를 들어 판매자가 스크립을 받고도 서비스를 제공하지 않는 부정행위를 할 경우 고객이 스크립을 판매한 브로커에게 이의를 제기하여 브로커가 해당 스크립 판매를 중지시킬 수 있기 때문에 판매자가 부정행위를 할 가능성이 매우 적게 된다.

밀리센트 시스템에서 사용되는 스크립은 최대 금액이 2~3달러로 현실에서의 동전처럼 쓸 수 있게 된다. 실세계에서 동전 몇 백원을 잃어버려도 크게 개의치 않는 것처럼 엄격하게 보안성을 제공하지 않는다. 난해하고 복잡한 프로토콜을 사용하지 않고 보안에 필요한 최소한의 암호화기법을 한다. 그래서 계산량이 많은 공개키 연산 대신에 판매자의 고유키와 MD5류의 해쉬 함수를 사용해서 스크립에 대한 인증서(certificate)를 생성하고, 이 값을 사용해서

스크립을 검증하며, 대칭형 암호시스템을 사용하여 처리속도가 빠르게 된다.

밀리센트 시스템에서는 스크립(Scrip)이 기록, 추적될 수 있는 일련번호를 갖고 있기 때문에 완전한 익명성을 제공하지는 못한다. 그러나, 익명의 소액지불 시스템을 사용해 브로커 스크립을 구입함으로써 약간 제한된 익명성이 보장될 수 있다. 또한 판매자는 스크립의 정보를 DB에 저장해 놓고 고객이 스크립을 제시할 때마다 DB를 조회함으로써 스크립 자체에 있는 일련번호를 이용하여 이중사용을 방지할 수 있으며, DB의 규모를 적당하게 유지하기 위해서 스크립은 유효기간을 가진다.

현재 밀리센트 시스템을 개발한 DEC는 Compaq에 인수되었다. SSL과 SET을 사용한 스크립 구입이 지원되며, 1999년 4월에 MilliCent Version 1.0이 개발되었다. 일본의 KDD Communications (KCOM)와 일본전역에 MilliCent를 보급시키기 위한 계약을 체결하여, 본격적인 서비스를 시작하고 있다.

1.3 기타

앞에서 설명한 두 개의 프로토콜 이외에도 네트워크형 전자 화폐로 NetCash와 PayMe가 있다 NetCash는 Southern California 대학의 ISI (Information Science Institute)에서 개발한 전자화폐 시스템으로 NetCheque와 같은 전자 수표등의 금융 도구와 교환이 가능한 분산 통화 서버 (Currency Server)를 기반으로 하고 있다.

NetCash 시스템은 구매자와 상인, CS로 구성되어 있으며, CS는 전자 동전을 발행하고 전자 수표를 전자 동전으로 교환해 준다.이 과정에서 CS는 공개키 알고리즘을 사용하며 사용되는 공개키는 중앙 기관에 의해서 전자 서명이 되어 있다. CS는 또한 모든 사용된 동전의 사용경로를 유지한다. 그렇지만 이것은 동전이 어디로부터 왔는지의 경로만을 기록하고 있기 때문에 누가 발행했는지는 알 수 없다.

PayMe는 기본적으로 NetCash의 특징을 가지고 있으며 이에 더하여 eCash의 익명성의 장점을 제공하고 있다. 시스템의 구성요소는 구매자, 상인, 은행으로 이루어져있으며, 구매자와 상인은 서로 지불을 수행하고 은행과도 거래를 한다. 은행은 전자화폐를 발행하는데 일련번호를 기록하고 있어서 이중 사용을 방지한다. 또한 PayMe시스템에서는 PMTP(PayMe Transfer Protocol)을 사용하여 거래에 참여하는 개체들 사이에 통신을 하게 된다 [18].

2. 가치저장형 전자화폐 시스템

2.1 몬덱스 (Mondex)

몬덱스는 영국의 Mondex International사가 개발한 IC카드 기반 전자화폐시스템으로 현금과 통신의 기능을 한 장의 카드로 구현한다는 기본 개념하에 마이크로칩에 암호화된 전자현금을 저장하고 있는 선불카드 형태로 된 IC카드 기반 전자 화폐 시스템이다[4].

몬덱스 시스템은 Mondex International사, 발행자(Originator), 회원(Member), 가맹점, 카드 소지자, 기기 공급사 등으로 구성되어 있다.

Mondex International사는 몬덱스 브랜드의 소유주로 프랜차이즈 계약에 의해 Franchisee를 모집하고, 몬덱스 시스템에서 사용될 기기 공급업체의 라이선스 부여 및 부여에 따른 인증료를 징수하고 국제업무 지침 및 기준 등을 제정하는 역할을 수행한다. 발행자는 Mondex Value 발행주체로서 중앙은행과 유사한 기능을 수행하여, 하나의 화폐단위당 한 기관만 존재하며 회원을 모집할 수 있는 기관으로, 몬덱스 카드 발급, 회원별 몬덱스 발행한도 설정 및 관리, Mondex Value의 위·변조 등에 대한 위험관리, 발행된 Mondex Value에 대한 부유 자금운영, 국내업무 지침 및 기준 제정 등의 역할을 수행한다. 회원(Member)은 Mondex Value를 판매·수집하고 가맹점이 수집하여 제시한 Mondex Value를 현금화하고, 가맹점 및 카드소지자를 모집하고 이들로부터 수수료를 징수하는 기관이다. 기기 공급사는 몬덱스 시스템에서 사용되는 카드, 칩, 카드발급기, 단말기, CD/ATM, Screen Phone과 같은 각종 기기를 Mondex International사로부터 인증 받아 공급한다.

몬덱스 시스템은 전화기, ATM기기등의 전용 기기를 통해서 가치 충전이 가능하고, 개인간 가치 이전이 가능하다. 또한 복수 통화를 지원해서 현재 5개국의 통화가 사용 가능하며, 최근 10회까지의 거래기록이 저장되어 조회 및 인쇄가 가능하다. 또한 PIN(Personal Identification Number)을 이용한 잠금기능이 가능하다. Mondex Purse application을 가지고 있는 프로그램을 ACD (Application Carrier Device)라 하며, 현재는

IC 카드 한 종류만 존재하지만 가까운 시일 내에 다양한 종류의 ACD가 개발될 것이다.

몬덱스에서는 MULTOS(Multi-application Operating System)라는 개방형 플랫폼형의 칩운영체제(Chip Operating System, COS)를 이용하여 다양한 응용서비스를 구현할 수 있고, Visa Cash와 같은 성격이 다른 지급시스템을 하나의 운영체제로 처리할 수 있다.

Mondex Value의 발급주체인 발행자가 부실화될 때 시스템 전체의 혼란이 야기될 수 있고, 개인간 자금이체를 통해 돈세탁에 악용될 가능성이 있으며, 불법 사용내역을 인지할 수 없다는 위험이 있다. 또한 마이크로칩이 내장된 카드를 사용하기 때문에 카드 발급비용이 소요되며, 사용자에 따라 몇몇 하드웨어 장치를 필요로 한다. 인터넷에서 몬덱스가 사용되기 위해서도 컴퓨터에 장착할 특수장치가 필요하기 때문에 초기투자비용이 많이 소요된다.

또한 몬덱스는 5개국의 통화를 다룰 수 있다고는 하지만 고정환율을 적용하고 변동되는 실제환율을 반영하지 못한다. 몬덱스 카드에는 16비트 크기의 고유번호가 부여되어 있어 가맹점의 카드판독기에서 이를 포착할 수 있고, 가맹점은 이를 은행에 전송할 수 있기 때문에 일반화폐에 비해 익명성이 떨어지며, 전자서명 및 카드와 단말기 상호간 진위확인 기능이 없으며, 가치의 저장, 사용한도 및 은행간의 차액결제 체계가 없으므로 보안구조의 파괴를 인지하기 곤란하고 가치 위조 및 변조 등 부정사용의 추적이 어려워 불법적 거래에 사용될 가능성이 높음. 또 카드의 분실, 도난, 훼손시 사용자가 거액의 손실을 입을 수도 있다.

영국에서는 1995년 7월에 런던 서쪽 Swindon에서 13,000여명의 카드소지자, 700여개의 점포가 참여하여 몬덱스 카드 시범사업을 실시하였고, Aston University에서는 IC카드의 장점을 살려 몬덱스 전자지갑, 학생증, 도서관카드, 학교출입증, 각종 증명사본 등의 기능을 통합하여 실시하였다.

몬덱스는 기존의 전자화폐 사업에 비해서 비교적 활발히 진행되고 있고 있는 IC카드형 전자화폐이며, 영국, 미국, 캐나다, 일본 등 9개국에 보급중이다. 마스터카드사는 자사의 몬덱스 전자화폐를 전세계적으로 보급하려고 하고 있으나, 대부분의 경우 국가별로 자국의 전자화폐 사업을 진행하고 있는 곳이 많다.

2.2 프로톤 (Proton)

벨기에 은행들의 컨소시엄인 Banksys는 벨기에에서 EFTPOS 시스템을 운영하고 있다. 1990년대 초에 Banksys는 Proton이라는 SVC(Stored Value Cards)를 개발했고, 1994년 8월 Leuven과 Wavre라는 마을에서 처음 사용되었다[5]. 초기 구현에서 벨기에의 Proton 시스템은 Banksys가 개발하고 Dallas Semiconductor(DS 5000) core를 사용한 security module에 안전성을 의존했다. Banksys는 몬덱스 시스템 다음으로 다른 나라에서 사용하도록 허가받은 시스템이 되었으며, 네덜란드의 Interpay B.V., 호주의 Quicklink, 오스트리아의 Telekurs, 캐나다의 EXACT 등이 사용하기 시작했다.

Proton은 C-SET(Chip-Secure Electronic Transaction)과 상호 운용될 수 있음을 성공적으로 보였고, 이는 앞으로 인터넷을 통한 전자 상거래에도 커다란 역할을 하리라 보인다. 상호 운용성은 어떤 전자 지갑 방식을 가지는 카드가 다른 방식의 터미널에서 잘 동작해야 함을 의미하며, 이는 실제로 많은 전자 지갑 솔루션들이 포기하고 있는 부분 중 하나이기 때문이다. Proton은 앞으로 CEPS(Common Electronic Purse Specification)를 지원할 예정이며, 이를 통해 상호 운용성을 더 높일 수 있을 것이다. 이 외에도 관련 표준(ISO, Europay MasterCard Visa Integrated Circuit Card Specification for Credit/Debit, Visa Integrated Circuit Card Specification) 등을 수용할 예정이라고 한다.

현재까지 벨기에에서 32,000개의 카드가 발급되었으며, Banksys는 Proton에서 사용되는 모든 터미널 CAD 장비, Bull CP8 CC60 전자 지갑 등을 제작했다.

Proton 은 스낵바, 주유소, 신문 가판대, 제과점, 정육점, 약국, 병원, 도서관, 식당 등에서 사용될 수 있으며, 이 외에도 주민증, 고객 할인 카드, 출입카드로도 사용되는 등 응용 사례가 매우 광범위하다. 또한 Proton은 최근에 인터넷을 통한 전자 상거래에 사용할 수 있도록 C-ZAM/PC라는 패키지가 개발되었다. Proton을 가지고 있는 사용자는 인터넷을 통해 Proton으로 지불을 할 수 있으며, 이 외에도 Proton에 자신의 구좌에 있는 돈을 저장할 수 있는 기능이 있다.

구매자의 스마트 카드와 상인의 터미널 사이의 데이터 교환은 triple DES에 의해 암호화되어 이루어지며, RSA 인증서도 사용된다. 세션키의 개념을 이용하여 매 트랜잭션마다 다른 키를 사용하고 있다. Proton을 이용하는 트랜잭션이 원래 암호화되어서 수행되므로, 인터넷을 통해 Proton을 사용하는데 새로운 암호기법을 도입하지 않았다. 단지 개인용 컴퓨터에 Proton을 로딩할 수 있는 간단한 장치와 이를 통해 상인의 웹사이트에서 쉽게 지불할 수 있도록 소프트웨어가 설치된다.

이때 구매자의 컴퓨터에 설치되는 장치를 C-ZAM/PC, 상인의 웹사이트에 설치되는 장치를 C-ZAM/VMT라 한다. C-ZAM/PC에는 별도의 키패드가 마련되어 있어 사용자는 자신의 PIN을 위험에 노출되기 쉬운 컴퓨터를 통해서가 아닌 다양한 안전 장치를 가지고 있는 키패드를 통해 입력하게 된다. 또한 사용자의 PIN은 카드가 삽입된 터미널에서 검사되며, 인터넷을 통해 전송되지 않는다. C-ZAM/PC는 proton을 이용하여 인터넷을 통한 구매에 사용될 뿐만 아니라, 홈뱅킹 등에서 사용자 인증의 도구로서도 사용될 수 있다.

이와 같이 Proton은 현재 유럽의 많은 지역에서 광범위하게 쓰이고 있으며 유럽에서 사용 중인 다른 전자 지갑 솔루션의 기반이 된 것으로 선구적인 역할을 했다. 안전성의 측면에서도 부가적인 하드웨어 장치의 사용을 통해 사용자의 비밀 정보를 안전하게 유지하며, 인터넷을 통한 거래 시 비밀정보를 네트웍을 통해 전송하지 않음으로써 안전성을 강화했다.

2.3 비자 캐쉬(Visa Cash)

Visa 카드사에서 개발한 IC카드형 전자화폐시스템으로 내장된 마이크로칩에 지정된 금액만큼의 가치를 미리 저장해 놓고, 가맹점에서 물품 또는 용역에 대한 서비스 대가를 오프라인 인증을 통하여 전자적 가치를 가맹점 단말기로 가치이전 시킴으로써 지급 결제하는 시스템이다[6].

비자 캐쉬 시스템의 참가자는 Visa International사, 비자 캐쉬 발행기관, 가맹점 취급기관, Funds 발행기관, 가치저장 취급기관, 가맹점, 카드소지자 등으로 구성된다. Visa International사는 비자 캐쉬 및 단말기 규격개발, 제조사에 대한 관련제품 인증, 전반적인 시스템 보안관리, 거래자료 수집 및 정산, 거래내역 관리 등의 역할을 수행한다. Funds 발행기관은 신용, 직불, 현금카드 소지자의 계좌를 보유하고 있으며, 고객이 원하는 경우 신용, 직불, 현금카드를 통하여 가치저장 및 비자 캐쉬카드의 구입자금에 대해 승인한다. 가치저장 취급기관은 비자 캐쉬 소지자가 비자 캐쉬에 전자적인 가치를 저장할 수 있도록 가치저장 단말기를 운영하고, 관리하는 금융기관이다.

고객의 요구에 따라 비자 캐쉬 발행기관은 일회용 비자 캐쉬, 가치 저장형 비자 캐쉬, 다기능 비자 캐쉬의 세 가지 유형의 카드를 발행한다.

비자 캐쉬를 사용해서 구매 거래시에는 PIN이나 카드소지자의 서명이 불필요하며, 오프라인으로 거래가 이루어지고, 가맹점으로부터 직접 구매 승인이 이루어진다. 비자 캐쉬의 거래처리는 시스템 구성요소간에 사용되는 디지털 서명의 인증에 바탕을 두고 있고, 비자 캐쉬 및 PSAM 등의 보안 알고리즘은 대칭형 알고리즘인 Triple DES를 이용한다. 비자 캐쉬는 주로 소액결제용으로 사용되며, IC카드와 단말기의 보안 성능에 의존해서 이중사용을 방지하게 된다.

비자 캐쉬는 여러 나라에서 시범 서비스를 실시한 대표적인 IC카드형 전자화폐 시스템이다. 미국에서는 1996년 Atlanta 하계올림픽에서 시범 사용되기도 하였다. 그러나 저변 확대 및 고객 확보에 실패해서 향후에는 사실상 서비스를 중단할 것으로 판단된다. Visa 카드사는 비자 캐쉬 사업을 중단하는 대신에, Europay International, Visa Espana/SERMEPA, ZKA 등과 CEPS(Common Electronic Purse Specifications)를 제정하고 1999년 3월 30일에 첫 번째 Version을 발표하였다.

3. 신용카드 기반 전자 지불 시스템

3.1 SET 프로토콜

SET은 Visa카드사와 Master카드사가 공동으로 제안하고, GTE, IBM, Microsoft, Netscape, SAIC, Terisa 그리고 Verisign사 등의 기술지원하에 개발되어 1997년 5월에 발표된 Visa 카드사와 Master카드사의 신용카드 기반 전자지불시스템의 표준 프로토콜이다[7]. 현실세계의 신용카드 지불 시스템을 기반으로 인터넷 전자상거래 환경을 실현하기 위해 전자상거래 요소시스템간의 지급 및 인증 시스템을 규정한 프로토콜이다.

SET은 통신망에서의 안전한 신용카드 거래를 위하여 정보전달의 비밀성, 지급정보의 무결성, 그리

고 상점과 고객간의 상호 인증 등을 위한 보안, 다양한 하드웨어간에 다양한 프로그래밍 언어 및 데이터베이스관리시스템 등으로 구현된 SET기반 소프트웨어들이 상호 운영되도록 보장하는 상호운용성(Interoperability), 전세계에서 SET이 표준처럼 쓰이기 위해 세계인들이 SET을 받아들여 사용해야 하는 시장수용성을 제공하는 일관된 환경을 마련하기 위해서 고안되었다.

SET의 구성요소는 카드소지자(Cardholder), 판매자(Merchant), 발행은행(Issuer), 매입은행(Acquirer), 인증기관(Certificate Authority), 지불 게이트웨이(Payment Gateway)이다. 카드소지자는 인터넷쇼핑몰에서 물품 또는 서비스를 구매하는 자를 말하며, 판매자는 인터넷상에서 상품이나 서비스를 제공하는 자이다. 발행은행이란 카드소지자의 카드발급 금융기관 혹은 결제카드 소지인의 계좌가 개설되어 있는 금융기관을 말하며, 매입은행은 판매자의 가맹점 승인 금융기관 혹은 판매자의 계좌가 개설되어 있는 금융기관을 말한다. 지불 게이트웨이란 판매자가 요청한 고객의 지급정보로 해당 금융기관에 승인 및 결제를 요청하는 기관을 말하며, 인증기관은 카드소지자, 판매자 등 각 참여기관이 인터넷상에서 서로 신뢰하면서 거래할 수 있도록 각 참여기관에게 전자적인 인증서를 발급하는 기관을 말한다.

SET에서는 기본적으로 비밀키와 공개키 알고리즘에 기반한 전자 서명(Digital Signature), 전자봉투(Digital Envelope), 이중 서명(Double Signature)등을 이용하여 보안 매커니즘을 가지고 있는데 이를 통해 기밀성, 무결성, 인증, 부인봉쇄 등의 보안서비스를 제공한다. 특히 이중서명(Dual Signature)을 사용해서 완벽한 익명성을 고객에게 제공하므로, 판매자는 고객의 결제정보에 대해서 알 수 없으며, 지불게이트웨이는 고객의 구매정보를 알 수 없게 된다. 그러나 안전한 보안 서비스를 제공하는 대신 공개키 연산이 많아 시스템의 효율성은 다소 떨어진다.

SET에서는 이중 서명을 이용해서 온라인 상에서 유통되는 상품주문정보와 지급정보를 각각 분리해 암호화함으로써 쇼핑몰 사업자 등이 주문정보 이외에 개인신상정보를 함부로 들춰볼 수 없게 한다. 이렇게 하여서 구매자에게는 판매자가 결제된 신용 카드의 정당한 수령자라는 점을 보증하고, 판매자에게는 구매자가 지불카드의 정당한 소지자라는 보증할 수 있다.

이와 같이 SET에서는 판매자와 구매자가 상호 신뢰성을 높여 다른 전자 지불 방식에 비해 신용카드가 더욱 강력한 경쟁력을 갖게 한다. 그러나 고객이 Wallet 모듈을 사용하는 것을 꺼리고 있으며, 공개키 연산을 자주 수행해야 한다는 단점을 지니며, SET을 제대로 구현하기 위해서는 기술, 시간, 비용 등 제반 측면에서 상당한 투자가 소요된다. 사용자가 별도의 인증과 Wallet을 포함한 여러 가지 번거로운 절차가 있고 처리속도에서도 SSL방식에 비해 현저하게 느리다는 단점이 있다.

97년 12월에는 MasterCard, Visa, Amex, JCB에 의해 SETCo가 설립되었는데 이는 SET 프로토콜의 개발 및 향상을 도모하기 위해 창설된 것으로 Root CA의 관리, Brand 인증서 발행, 인증과 관련된 정책 수립등의 인증 기관 관련 업무를 담당하고 SET 사양을 만족하는 소프트웨어에 SET 마크를 주고, SET Compliance Certificate를 부여하는 역할을 한다.

SET 거래는 SSL상에서의 신용카드보다 훨씬 더 높은 수준의 보안성을 제공하므로 SET이 인터넷상에서 카드로 지불하는데 있어서 지배적인 방법이 될 수 있을 것이다. 그러나, 현재 인터넷상의 상거래에서 SET을 사용하는 건수는 극도로 작은 실정이며, 비자와 마스터 카드사의 추진 의지에 따라 향후 활성화 정도를 예측할 수 있을 것이다.

3.2 사이버캐쉬 (CyberCash)

사이버캐쉬란 1994년 설립된 CyberCash사에서 개발하여 운영하고 있는 인터넷 기반 전자상거래용 신용카드 기반 지불시스템이다[8]. 고객은 PC에 내장된 전용 소프트웨어에 미리 신용카드번호를 기억시키고 암호화된 신용카드정보가 사이버캐쉬 서버의 중개로 네트워크 상에서 지불에 이용되도록 하는 메커니즘을 가지고 있다. 사이버캐쉬 시스템 구성요소로는 고객용 소프트웨어인 사이버캐쉬 월렛(Cyber-Cash wallet), 상점용 소프트웨어인 SMPS (Secure Merchant Payment System) 및 고객, 상점, 은행간의 상호연결 및 결제처리 기능을 수행하는 사이버캐쉬 서버가 있다. 여기서 사이버 캐쉬 서버는 인터넷과 다른 금융망과의 자료교환, 사이버캐쉬 월렛 ID의 유지 및 인증, 메시지 추적 기능 등을 수행한다.

고객과 상점은 월렛(wallet)과 소프트웨어에 거래기록을 저장하여 검색해 볼 수 있고 상점은 고객

별 또는 카드별로 거래내역을 분류하여 볼 수 있으나, 모든 거래정보가 사이버캐쉬 서버에 저장되기 때문에 고객 및 상점의 익명성은 보장되지 않는다.

사이버캐쉬시스템은 데이터를 암호화하는데 있어서 768비트 RSA암호화방식과 56비트 DES암호화방식을 사용하고 있으며, MD5방식을 통해 전자서명을 구현하고 있음. 암호화가 금융데이터를 보호하기 위해서만 사용되기 때문에, 리비아, 쿠바, 북한 등 몇몇 국가를 제외한 모든 국가에 판매가 허용되어 있다.

사이버캐쉬사는 1995년 4월부터 사이버캐쉬 서비스를 실시하고 있으며, 매일 수천 건의 거래가 이루어지고 있고 80% 이상의 은행이 이 시스템과 연결되어 있다. 또한 이 시스템에서는 지불수단으로 신용카드 기반 방식뿐 아니라, 전자화폐인 CyberCoin 및 전자수표인 PayNow를 개발하여 사용하고 있다.

4. 전자 수표 시스템

전자수표(Electronic Check) 결제방식이란 고객이 인터넷과 같은 통신망상에서 물품을 구매하거나 서비스를 이용하고 기존의 수표를 전자화한 전자수표를 이용하여 대금을 결제하는 방법을 말한다. 전자수표는 기명날인이나 배서는 전자서명을 이용하고, 지급인, 지급인 거래은행, 거래계좌 등에 대한 인증은 전자증명서를 발급하여 확인한다.

전자수표는 원래 네트워크 상에서 이용될 수 있도록 개발되었으나 향후에는 기존의 수표 성격과 다른 다양한 용도로 개발될 것으로 예상되며, 직접 전송방식 또는 전자메일 이용방식 등 전송방법도 다양하다.

4.1 Echeck

Echeck는 FSTC(Financial Service Technology Consortium)에서 개발한 전자수표시스템이다[9]. 기존 수표와 유사한 방식으로 교환, 결제되기 때문에 일반인에게 친숙하여 쉽게 보급될 가능성이 높으며, 고객과 판매자간의 전자수표 교환으로 거래가 이루어진다. 고객은 하드웨어 기반의 서명카드를 PC에 설치하고 서명카드를 이용하여 전자수표에 서명하고 배서할 수 있다. 고객 인증은 고객의 거래은행과 연방준비은행이 공개키 방식의 전자서명을 응용하여 계층적으로 해주고 있다. 고객이 전자수표를 발행하여 판매자에게 전송하면 판매자는 동 수표에 배서를 한 후 판매자 거래은행에 제시하여 교환·결제하는 방식이다. FSTC에서는 기존의 수표결제방식과 유사한 전자수표 결제방식이외에 기존 의 수표 성격과 다른 3개 방식을 추가로 지원한다.

Echeck에서는 하드웨어 방식의 전자서명이 이용되고, 은행의 인증을 받아야하기 때문에 안전하고 믿을 수 있는 결제방식이다. 전자수표는 보증수표, 자기앞수표, 여행자수표 등 다양한 종류로 발급될 수 있고, 개인간, 개인-기업간, 기업간 등 여러분야에서 사용될 수 있어 용도가 다양하고, 은행은 전자수표를 사용하는 인터넷 이용자를 고객으로 확보할 수 있다는 장점이 있다. 여타 지불수단에 비하여 금액이 커 범죄의 표적이 될 가능성이 높고, 여타 지불 단에 비하여 수수료가 높은 단점이 있다.

4.2 Netcheque

NetCheque 시스템은 USC(University of Southern California)의 ISI(Information Sciences Institute)에서 개발된 인터넷용 전자수표시스템이다[10].

NetCheque로 발행되는 전자수표는 인터넷에서 전자적으로 사용된다는 점을 제외하고는 일반 종이수표와 매우 유사한데, 비밀키 암호방식에 기반을 둔 커버러스 인증 시스템을 사용하고 있으며 커버러스 시스템을 이용하여 산출된 전자수표는 배서될수도 있고 은행간에도 교환될 수 있다. 또한 다수의 인증 서버를 사용해서 신뢰성과 확장성을 제공한다.

NetCheque시스템은 소액용 지급결제시스템으로 적합하고, 범용으로 사용될 목적으로 개발된 Echeck 시스템과는 달리 전자상거래 어플리케이션에 초점이 맞추어져 있다.

III. 전자 지불 프로토콜 현황 및 표준화 동향

전자 지불 시스템은 주로 현실적인 필요성에 의해 금융기관이나 서비스 제공 업체들에 의해 독립적으로 개발되었다. 이와 같이 상호운영성 문제를 해결하기 위한 표준화 활동은 주로 민간부문에 의해서 추진되고 있는 실정인데, 현재 전자 지불 시스템과 관련된 표준으로는 신용카드 기반 전자 지불시스템에 대한 사실 표준으로 SET이 있으며, IC 카드의 표준으로 개발된 EMV[11], C-SET등이 있고, W3 컨소시엄과 CommerceNet의 JEPI(Joint Electronic Payment Initiative), OBI(Open Buying on

the Internet) 컨소시엄의 OBI, OTP(Open Trading Protocol) 컨소시움의 OTP[12], checkfee, microsoft intuit이 공동개발한 OFX등이 있다.

각기 다른 프로토콜이 표준에 대한 정립을 하는 필요성에 대해서는 논란의 여지가 없지만, 표준을 시장원리에 의해 이루어지는 사실 표준의 형태로 발전시켜야한다는 견해와 정부와 국제 표준화 단체에 의한 표준 제정이 우선 되어야한다는 견해 사이에 갈등이 있다. 각각 장단점을 내포하고 있으므로 표준의 공공적인 성격과 민간주도의 시장경쟁에 의한 표준설정이라는 양 측면이 조화롭게 수렴되어야 한다[17].

1. 전자 화폐 시스템

네트워크형 전자화폐는 초기에는 조기 활성화가 될 것으로 예상했으나, 사용자의 친숙도가 낮고 사용하기에 불편한 점이 많아 현재 시장에서 점차 도태되어 가고 있는 실정이다. 국내에서 사용되고 있는 전자 화폐의 예를 보면 대부분의 경우 은행과는 별도로 전자 화폐를 발행/사용하고 있으며 전자화폐의 구입 대금을 신용카드나 은행의 무통장 입금, 계좌 이체등을 통해서 지불하고 있다. 이런 접근 방법은 사용의 편리성을 상당 부분 희생하고 있으며, 사용자는 공개적으로 검증되지 않은 전자 화폐 프로토콜을 사용해야 하며 이에 따른 여러 가지 위험 요소를 감수해야만 한다.

가치저장형 전자화폐는 네트워크형에 비해 비교적 활발히 시범 및 상용서비스가 시도되었으나, 적극적인 호응을 얻어낸 시스템은 아직까지 없으며 국가별로 서비스를 추진하기도 했지만 대부분 실패하고 있다. 이러한 실패의 원인은 소비자들이 IC카드의 현금만 저장되어 있어 기존의 화폐와의 차별성이 부족하고, 처리 시스템이 다운된다든지 처리시간이 지연이 일어난다든지 하는 일이 잦아 안정성이 부족하게 되어, 결과적으로 소비자에게 전자 화폐 사용의 충분한 동기부여가 이루어지지 않았기 때문이다. 그러나 각 기업체와 화폐발행은행들간의 다각적인 제휴를 통해 전자 화폐를 재빨리 상용화시키려는 노력이 계속되고 있고, IC카드에 현금이외에 구매자들의 요구에 맞는 기능을 추가해 점차적으로 활성화시키려는 노력들이 계속되고 있으므로 가치 저장형 화폐는 널리 보급될 예정이고, 이를 바탕으로 인터넷을 통한 전자화폐의 확산도 기대할 수 있을 것이다.

국가적 차원에서 국내외 겸용 전자화폐를 목표로 추진중인 프로젝트는 없지만, Visa, Mondex, Proton, Europay등에서 관련 서비스를 추진중에 있다. 비자카드사와 마스터카드사는 각각 CEPS (Common Electronic Purse Specifications)와 Mondex 전자화폐 사업을 현재 중점적으로 추진하고 있으며, 각각 Java카드와 MULTOS를 IC카드 표준 규격으로 채택하고 있다. 비자카드사와 마스터카드사는 오는 2005년까지는 종전의 마그네틱 카드를 IC카드로 전면 교체할 계획이라고 한다

국내에서도 민간 주도의 전자 화폐포럼이 결성되어 앞으로 전자화폐의 안전성을 확보하고 다양한 전자화폐간 호환성을 확보할 수 있도록 표준화를 추진하기 위한 활동이 진행되고 있다. 전자화폐포럼은 현재 금융결제원, 몬덱스코리아, 비자코리아 등 전자화폐업계는 물론이고 카드 및 단말기업체 17개사, 한국통신 등 통신사업자 4사, 칩제조업체 2사, 소프트포럼 등 전자지불 솔루션 및 보안업체 4사, 법률사업자 1사 등 36개 기관이 참여하고 있다. 각 업체들이 독립적으로 일정한 기준 없이 전자 화폐 사업을 추진함으로 인하여 전자화폐간 호환성 확보가 어려웠으며 서로 다른 표준을 채택하고 있는 전자화폐 인프라의 확산은 산업자체의 기형적인 발전까지 가져올 수 있다 이에 따라 카드단말기 등 인프라장비의 중복투자를 초래하고 소비자도 이용상 불편을 겪어야만 하는 부담이 있었다 정보통신부에서도 민간주도의 전자화폐 포럼의 구성을 통해 이해당사자들이 서로 협의하여 관련 기본규격을 정해 시장에서 자연스럽게 사실상 표준을 정하도록 유도할 계획이라고 한다[15].

2. 신용카드 기반 전자 지불 시스템

지금까지 인터넷상의 전자 상거래를 지원하기 위한 신용카드를 이용한 전자지불 시스템이 많이 개발되었지만 보안상의 이유로 많이 사용되고 있지는 못하는 상황이다. 다만 인터넷상에서 결제시에 SSL 프로토콜을 이용하여 고객의 신용카드 번호를 판매자에게 전송하여 판매자가 VAN 사업자를 통해 카드의 유효성 여부를 검증하는 방식이 주로 이용되고 있다.

SET을 이용한 신용카드 기반 전자지불 시스템은 여러 곳에서 시험되고 있으나 속도가 느려서 활발히 사용되고 있지는 못한 실정이다. 이러한 추세를 감

안해 볼 때, 당분간 신용카드를 이용한 전자상거래의 지불을 위해서는 SSL을 이용한 방식이 우세를 보일 것으로 전망된다. 현재의 주된 관심사는 신용카드의 처리시간이지 보안성이 아니고 또한 SET을 이용한 신용카드처리시스템이 그리 많이 개발되지 못하였기 때문이다[13].

그러나 SSL이 잠재적으로 가지게 되는 판매자에 의한 신용카드 번호의 도용의 가능성이 커다란 사회적 문제점으로 등장하게 되고 이러한 도용을 예방할 수 있는 기술을 개발하지 않는다면, SET을 이용한 신용카드 지불방식이 주목받을 것으로 전망되는데, SET을 이용한 신용카드 지불방식은 높은 보안성 유지를 위한 여러 가지 기법이 사용되므로 인터넷상에서 신용카드를 이용한 지불이 활발히 이용되고 높은 보안성 유지가 가장 중요한 요소로 등장하게 될 때 각광받는 프로토콜이 될 것임에 틀림없다.

현재 Visa카드사와 Master카드사는 SET에 사활을 걸고 IC카드에 적용될 수 있는 C-SET(Chip SET)를 개발하였고, SET의 차기버전도 개발중이다. Visa카드사와 Master카드사의 의지여하에 따라 표준화에 큰 영향을 미칠 것이다.

우리 나라도 SET과 관련하여 Commerce Net Korea에서 한국형 전자 상거래 사업을 추진하고 있으며 데이콤이 SET 프로토콜을 적용한 신용카드 전자 지불 서비스를 제공하고 있다. 비씨카드등 4개 신용카드사와 한국통신등이 공동으로 출자하여 Korea Cyber Payment를 설립하여 SET 시스템을 구축중이다. 그러나 국내에서 개발된 제품들은 현재까지 SETCo에 인증 신청을 하지 않은 상태이며 국제적으로 호환이 가능하지 않은 문제점이 있다[16].

3. 전자 수표 시스템

현재 국내에서 개발된 전자 수표 시스템은 없다. 전자 수표 시스템은 현재 수표 결제시스템을 유지하면서 개발시킬 수 있고 현행 수표법에 큰 변화없이 시장에 적용할 수 있다는 점에서 흥미롭다. 현재 수표의 발행및 처리부분에 드는 비용을 간소화하면서 현행 업무 관행내에서 큰 변화 없이 수용 가능한 것이다. 안전한 전자형태로 보안 기법을 사용하여 안전하게 종이수표처럼 작동하게 하며 기존의 금융업무가 새로운 전자상거래 특성을 갖도록 향상시키는 역할을 한다. 이것은 기업간 전자 상거래가 활성화 일로에 있다는 점과 기업간 거래에서 수표의 활용을 고려해 볼 때 더욱더 구현과 표준화의 필요성이 증대된다.

전세계적으로 전자수표시스템을 도입할 예정이거나 시범서비스를 실시하고 있는 국가가 미국과 싱가포르 두 나라에 국한되어 있고 이들 국가의 수표처리체제 및 금융관행이 우리의 방식과는 차이가 있고, 또한 현재 우리 나라 금융기관들이 전자 수표 시스템 도입에 많은 관심을 아직까지 보여주고 있지 않다는 점을 고려해 볼 때, 세밀하고 신중한 분석을 토대로 표준화를 이룬 뒤 전자 수표 시스템의 구축이 추진되어야 할 것이다.

V. 결 론

인터넷의 사용의 확산에 따라 전자 상거래에 대한 관심이 증폭됨에 따라 이와 관련하여 전자 지불 프로토콜에 대한 연구가 계속되어 왔다. 다른 연구들과는 달리 실용적인 성격이 강하고 파급효과가 커서 세계각국의 정부기관이나 민간 업체에서 앞 다투어 개발을 하였고 주도권 쟁탈을 위해서 서로 노력하고 있다. 본고에서는 전자 지불 시스템을 지불 수단에 따라 분류하고 각각의 특징과 현황 표준화에 관련된 이슈와 동향에 대해서 살펴보았다.

지불 시스템은 지불 수단에 따른 각각의 용도가 다르고 표준화의 방향도 추세도 조금씩 다르다. 표준 정립에 대해서는 이견이 없지만, 표준 제정을 표준화 단체에 일임할 것인지 시장 원리에 의해서 다수의 수요자를 확보하는 것이 사실상의 표준으로 되는 것이 좋은지에 대한 의견도 분분하다. 그러나 IC카드가 향후 온라인 및 오프라인에서 가장 중요한 지급결제수단으로 발전하리란 것이 현재의 추세이고 비자카드사 및 마스터카드사가 자사의 신용카드를 IC카드로 조만간 전환할 것임을 밝힌 상황에서 IC카드 기반 전자 화폐 시스템의 개발은 더 큰 의미를 갖게 된다. 또한 전자 수표는 규모가 큰 기업간 거래 또는 기업과 정부간 거래에 사용되고 은행간 교환 작업이 가능하므로, 저자 화폐나 신용카드 기반 전자 지불과는 달리 국가 표준화를 통해 확산 및 활성화가 가능할 것이다.

전자 상거래가 기본적으로 인터넷을 통해 발전하고 지급 결제 시장이 국제화된다는 점과, 전자 지불 시스템이 개발단계에서는 특정 국가나 지역에서 운용되더라도 사용화 단계에서는 범세계화가 이루어진다는 점을 고려해 볼 때, 관련된 정부부처, 연구소, 각급 기관 및 업체들이 서로 협력하여 국제 표준화

등에도 주도적으로 참여하고, 관련 지불 기술과 보안 기술의 원천적 확보에 힘써야 할 것이다.

참 고 문 헌

[1] 백은경, 전자 대금 결제를 위한 보안 기술 현황, 정보통신 연구, 제 11권 2호, July. 1997

[2] eCash, http://www.ecashtechnologies.com

[3] Milicent, http://www.milicent.digital.com

[4] Mondex, http://www.mondex.com

[5] Proton, http://www.protonworld.com

[6] VisaCash, http://www.visa.com/pd/cash/main.html

[7] SET Secure Electronic Transaction LLC, http://www.setco.org/set_specification.html

[8] CyberCash, http://www.cybercash.com

[9] Echecks, http://www.echeck.org

[10] NetCheque, http://www.isi.edu/gost/info/NetCheque/

[11] EMV, http://www.emvco.com

[12] OTP, http://www.otp.org

[13] 금융결제원, 인터넷 기반 지급 결제 수단에 관한 연구, Sep. 1999

[14] 한국 전산원 정보화 통계자료, http://www.nca.or.kr

[15] 전자 신문, http://www.etnews.co.kr

[16] 김홍근, 최영철, 전자상거래 정보 보호 기술 현황 및 대응 방안, 정보처리학회 6(1), pp. 22-34, Jan. 1999

[17] 김범태, 김은, 전자상거래 표준화 동향 및 이슈, 정보처리학회 6(1), pp. 14-21, Jan. 1999

[18] 오형근, 이임영, 전자화폐 시스템 개발 동향, 통신 정보보호학회 9(1), pp. 13-31, March. 1999

〈著者紹介〉

김 종 우 (JongWoo Kim)

1999년 2월 : 연세대학교 컴퓨터과학과(학사)
1999년 3월~ 현재 : 연세대학교 컴퓨터과학과 석사과정
〈관심분야〉 통신망 프로토콜, 네트워크 보안

송 주 석 (JooSeok Song)

1976년 2월 : 서울대학교 전기공학과(학사)
1979년 2월 : 한국 전기 전자공학과(석사)
1988년 2월 : University of California at Berkeley 전산과학(박사)
1989년 3월 ~ 현재 : 연세대학교 컴퓨터과학과교수
〈관심분야〉 Information Security, Cryptography, ATM networks, Protocol engineering.