2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

전자화폐 표준화기술 현황 및 전망*

이상무**, 오행석**
**한국전자통신연구원 표준연구센터
e-mail : sangmu@pec.etri.re.kr

Current Status and Prospection of Electronic Cash Standardization Technology

Sang-Mu Lee*, Haeng-Seok Oh*
*Protocol Engineering Center, Electronics and Telecommunications Research Institute

요 약

최근 전자정보기술의 전파와 함께 정보통신 네트워크를 기반으로 한 전자상거래가 활성화되고 있고 이에 따라 인터넷상에서 이용할 수 있는 전자적 화폐 수단이 강구되고 있다. 전자화폐 자체는 이러한 네트워크 상의 거래 뿐만이 아니라 일반적으로 전자정보를 내장하고 있는 지불 가능 수단은 모두 포함하는 광범위한 의미를 가지고 있다. 이미 전자상거래 등의 활성화와 더불어 전자 지불 수단을 위한 전반적인 시스템이 구축되어 가고 있는 실정이다. 본 논문에서는 이러한 환경하에 전자화폐 개발 기술과 표준화 현황을 분석하였다.

1. 서론

전자화폐(Electronic Cash)는 IC카드나 인터넷에 접속되는 PC 등에 일정 화폐 가치를 디지털 데이터 형태로 저장하였다가 상품 등의 구매에 사용할 수 있는 전자 지급 수단으로 실물 화폐가 가지는 특성(익명성, 양도성, 이동성, 즉시 결제성)에 디지털화에 따른 부가 기능(원거리 양도성, 분할성)이 추가되어 off-line 또는 on-line으로 거래가 가능한 화폐로 정의한다. 전자화폐 이용자는 은행 및 신용 카드사 등 발행 기관으로부터 자기 명의의 예금계좌와 연결된 전자지갑을 발급받아 기존의 CD/ATM기를 통해 전자화폐를 충전하며, 미사용 잔액에 대하여는 환불도 가능하다. 이러한 전자화폐는 신용카드, 직불카드 및 현금카드로 활용할 수 있다.

전자화폐는 전자상거래의 활성화에 따른 새로운 결제 수단의 필요성과 현금시장, 특히 소액 현금을 대체할 수 있는 새로운 화폐의 필요성에 의해 등장하게 되었는데, 실물 화폐의 사용시 발생하는 단점의 보완(마모성 및 휴대 불편), 실물 화폐의 발행 및 관리 비용을 감소시키는 특징을 갖는다. 또한, 보안성이 뛰어난 IC카드 기술 및 정보통신기술(인터넷 기술)의 발달로 인해 사용 영역을 넓혀가고 있는 추세이다.

전자화폐는 크게 카드형과 네트워크형으로 구분할 수 있고, 카드형은 자금 결제 방법에 따라 직불, 후불, 선불 카드로 분류할 수 있다.

직불카드는 상거래 발생 즉시 고객의 예금계좌에서 자금 결제가 일어나고, 후불카드(신용카드)는 상거래 후 본인의 예금계좌에서 상거래 자금결제가 발생한다. 반면, 선불카드는 고객이 일정 금액을 카드 발급처에 지불한 후, 카드를 발급받아 사용하는 형태로 현재 지하철 및 공중전화 등에 활용되고 있다.

전자화폐를 직불카드 또는 신용카드와 비교하면 다음과 같은 특징이 있다. 전자화폐는 신용이 없는 계층, 예금 구좌가 없는 계층도 사용 가능하며, 매체에 저장된 화폐 가치 자체가 신뢰성을 담고 있기 때문에 사용할 때마다 신용 유무 등의 확인 절차가 불필요하다. 하지만, 실제 화폐와 같이 분실 위험성은 여전히 존재하는 단점을 갖는다.

2. 전자화폐의 핵심기술

가. 전자화폐시스템의 구성

IC카드형 전자화폐시스템은 다음과 같이 구성된다고 할 수 있다: IC카드, 단말기, 발행 은행 호스트컴퓨

* 본 논문은 한국전자통신연구원 표준연구센터에서 수행하고 있는 정보통신부 출연 표준기획연구과제의 일환으로서 정보기술분야 표준기획실무반 중간연구결과로부터 작성한 것임.

터, 매입 은행 호스트컴퓨터, 통신망 중계센터 또는 시스템 제공자 호스트컴퓨터, 통신시스템 및 통신회선

IC카드는 삽입되는 종류에 따라 단순 메모리 카드, CPU 내장 카드, 다기능 카드로 나눌 수 있다. 단순 메모리 카드는 플라스틱 카드에 삽입되는 칩이 단순 메모리 칩인 형태로 전화카드, 게임기용 S/W, 전자수첩의 메모리카드로 활용된다. 반면, CPU 내장 카드는 CPU(8bit)와 메모리가 내장된 카드를 의미하며, 다기능 카드는 CPU 내장 카드를 기본으로 정보표시 기능, 정보입력 기능을 보유하고, 카드 자체 내에 배터리가 내장되어 있어 다양한 부가 소프트웨어 기능을 가진 휴대용 단말기에 사용된다.

단말기(Read-Writer)는 IC카드의 데이터를 해독하거나 IC카드에 데이터를 입력하고 소거하기 위해 접속할 수 있는 장치를 뜻한다. 이러한 단말기의 한 형태로 응용 단말기가 존재하는데, IC카드를 사용할 수 있는 응용 단말기로는 CD, ATM, Handy Terminal, POS 시스템 등이 있다.

발행 은행 호스트컴퓨터는 카드의 발행 및 가치 저장시 단말기와 통신을 담당하고, 비밀키의 저장을 위해 명령 수행과 관련된 중요한 보안을 수행하기 위한 보안 기능을 수행한다.

매입 은행 호스트컴퓨터는 판매자 단말기와 직접 통신을 담당하고, 구매와 관련된 비밀키의 저장 및 명령 수행 등 중요한 보안 기능을 수행한다.

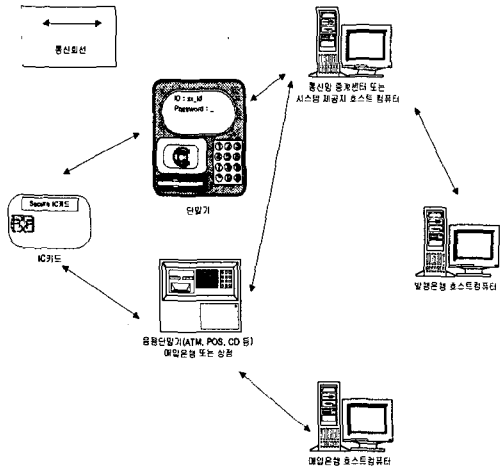
통신망 중계센터 또는 시스템 제공자 호스트컴퓨터는 보안장비를 보유하고 구매 거래에 대한 데이터 수집시 구매 단말기와 통신을 수행하며, 가치 저장 단말기와 발행 은행간 중계 기능을 담당한다.

발행 은행은 IC카드 소지자의 주계좌를 보유하고 있는 은행으로서 거래 데이터에 대한 정당성 확인 및 지불 보증에 대한 책임을 지며, IC카드의 발급· 관리 및 가치 저장, IC카드의 활성화 및 비활성화, IC카드의 계정 및 거래 내역 관리, 가치 저장 단말기의 공급 및 설치, 유지 관리를 담당한다.

매입 은행은 판매자 단말기 운용자의 주계좌를 보유하고 있는 은행으로서 단말 운용자의 계좌로 물품에 대한 가치를 입금시키며, 단말 운용자의 가치 입금 내역을 관리한다.

중계센터는 특정 VAN 사업자 또는 금융정보망을 주관하고 있는 은행간 네트워크를 운영하는 기관으로서 단말 운용자의 구매 단말기 인증, 개별 거래 내역의 무결성 인증, 구매 단말기의 공급, 설치 및 유지 관리, 발행 은행과 매입 은행간 자금 정산 기능을 수행하며, 시스템 참가자 간의 각종 분쟁 중재 및 보안 장비의 관리를 담당한다.

(그림1)은 IC카드형 전자화폐의 시스템 구성도를 나타내고 있다.



(그림1) IC카드형 전자화폐시스템 구성도

나. 전자화폐의 안전성과 적용 기술

전자화폐는 디지털 데이터 자체에 금액 가치를 포함하고 있기 때문에 제3자에 의한 네트워크상에서의 다양한 공격 가능성과 사용자/소유자에 의한 위·변조 가능성이 존재하게 된다. 따라서 이러한 공격을 방지하고 화폐로서의 가치를 유지하기 위한 여러 가지 암호학적인 기법들이 사용되어야 한다.

안전성 대책으로는 사전 조치로서 암호기술, 인증기술, Tamper resistant 장치, 제한 한도 규제, 인증 제도를 구현하는 방안과, 중간 조치로서 모니터링, 중앙 시스템과의 조회, 거래 이력의 보존과 온라인 검증, 정보 개시 등을 들 수 있다. 마지막으로 사후 조치로는 핫리스트 작성, 장치의 사용 거부, 시스템의 정지 등의 기법이 사용된다.

이중 사용 방지법은 거래 상황과 제시된 전자화폐의 미사용 여부, 수취인이 은행에 문의한 것에 따라서 사용 유무를 확인하는 방법으로, 전자화폐 정보를 부정하게 읽을 수 없는 물리적인 매체 내에 넣어서 외부로부터 매체 내부의 정보를 읽으려 하는 공격에 대한 방어 대책이다. 사용 예로는 Tamper resistance(IC카드형 전자화폐에서 사용)를 들 수 있다.

사용자 확인을 위한 기술로 디지털 서명이 주로 사용되는데, 이는 수령한 디지털 정보를 본인이 작성한 사실을 증명하는 방식이다. 디지털 서명은 공개키 암호방식을 사용하는데, 공개키 자체의 위조를 방지하기 위해 인증기관(CA:Certification Authorities)을 설치해야 한다.

전자화폐 프로토콜에서는 은닉 서명(Blind Signature)을 사용하는데, 사용자가 서명자에게 서명을 받으려는 문서를 비밀로 한 채 서명을 얻는 방법으로 사용자에게는 프라이버시를 제공하며, 유사시 추적이 가능하여, 돈세탁의 위험을 해소할 수 있다.

3. 전자화폐의 기술개발현황

가. 전자화폐의 국외 기술개발

1)전자화폐 서비스 관련 기업들의 현황

비자카드사는 마이크로소프트와 함께 STT(Secure Transaction Technology)라는 신용카드 응용 전자지불 프로토콜을 지원하며, 마스터카드사는 인터넷을 통해 급성장하고 있는 넷스케이프사의 Secure Courier라는 전자지불 프로토콜을 지원한다. 또한, 유로피(Europay International)는 IBM과 제휴를 하고 iKP 프로토콜을 이용한 전자지불 서비스를 시작하였다.

유럽에서는 '92년부터 CAFÉ (Common Electronic Purse Specifications)라는 네덜란드, 덴마크, 영국, 프랑스, 독일 등 유럽 13개국이 연합해서 전자지불 프로토콜을 표준화하고 개발하였는데, EBC (Electronic Business Cooperative) 연합은 독자적인 EBC Wallet을 만들어 스파이글래스 모자익 2.11버전에 탑재해서 '96년 1월에 출시하였다.

IC카드 기반의 전자지불 시스템을 개발한 비자와 마스터카드, 유로피는 신용카드를 IC카드화하기 위한 통일 사양인 EMV(Europay, Master and Visa) 사양을 '95년 6월에 발표하였다. IC카드는 전자 현금적 기능을 갖기 때문에 현금 지급기에서 일정 금액을 미리 인출해서 IC카드에 담고 다니면서, 상품을 살 때, 이 금액으로 지불이 가능하다. 유로피는 '96년에 IBM의 iKP소프트웨어와 컴퓨터, IC카드 리더기를 장착한 IC카드와 소프트웨어 전자지불 서비스를 통합 실험하였으며, 몬덱스는 영국의 NatWest은행과 Midland은행이 중심이 되어 '95년 7월부터 IC카드를 이용한 전자현금 서비스를 시작하였다.

2) 각국의 전자화폐 개발 동향

현재 유럽, 북미, 동남아 등지에서 여러 가지 형태의 전자화폐가 개발, 실험 운영 중이며, 여러 가지 형태의 전자화폐를 지원하기 위해서는 통일된 시스템 구축 및 표준화된 단말기 보급이 필수적이다. <표1>은 각국의 전자화폐 개발 동향을 자세히 보여주고 있다.

<표1> 각국의 전자화폐 개발 동향

국가	영국	미국/호주	벨기에	독일	싱가폴
명칭	Mondex	VISA, MASTER	Proton	Chipknip	Net's CashCard
추진현황	'95. 7. 시험	'96/ '95시험	'94.10. 시험	'95.10. 도입	'94.2. 시험
발행기관	회원 은행	회원 은행	은행공동망 회원은행	직불 공동망 회원은행	은행 공동망 회원은행
수익 귀속	몬덱스사	발행은행	발행은행	발행은행	발행은행
차액 결제	×	o	o	o	o
자금이체	o	×	×	×	×
사용 범위	전체	소액	소액	소액	소액
비밀번호	×	×	×	-	×
카드 잠금	o	×	×	×	×
국가	포르투갈	프랑스	일본	네덜란드	덴마크
명칭	MEP	Carte- Blue	미정	Ecash	Danmont
추진 현황	'95.2. 가동	'89년 도입	도입 예정	'95.2. 시험	'96.3. 도입
발행 기관	직불, CD 공동망 회원은행	회원 은행	민간 은행	-	은행과 통신 회사
수익 귀속	발행은행	발행은행	발행은행	-	발행은행
차액 결제	o	o	-	-	o
자금이체	×	×	-	-	×
사용범위	소액거래	소액	-	-	소액
비밀 번호	×	×	-	-	×
카드잠금	×	×	-	-	×

3)형태에 따른 개발 동향

- IC카드형

유럽· 북미 및 동남아 지역을 중심으로 개발 추진 중이며, 접촉식의 경우 현 은행간 차액 결제가 필요없는 몬덱스(영국)형과 다수의 참가 은행이 발행에 참가하여 은행간 차액 결제가 필요한 프로톤(벨기에)형으로 구분된다.

- 네트워크형

네트워크 상에서 활용되는 전자화폐는 E-Cash, CyberCash, First Virtual, SFNB (Security First Network Bank) 등이 시범적으로 운영되거나, 실험 운영 중이다.

E-Cash는 네덜란드 DigiCash사에 의해 개발된 전자화폐로서 '95년 10월부터 상용 서비스를 시작하고 있으며, 소프트웨어를 이용하여 은행으로부터 E-Cash를 인출하여 이용 가능 상점에서 물건을 구매하고 상점은 곧 서비스나 물품을 고객에게 제공하는 방식을 취하고 있다. 반면, CyberCash는 신용카드의 단점을 개선하기 위해 도입되었으며, Wallet이라는 프로그램을 이용하여 CyberCash에 계정을 등록하고신용 카드 정보를 기록한다. First Virtual은 미국의 First Virtual Holdings사가 '94년부터 제공하는 것으로 웹브라우저와 전자메일만을 이용해 전자지불시스템을 구축하고, 전화나 FAX를 이용하여 개인신상 정보를 전송하고 World Wide Web을 통하여 물품을 구매, 전자우편 주소로 메일을 보내 소비자의 확인을 거쳐 결제(신용카드를 이용한 결제시스템)하는 시스템이다. 마지막으로 SFNB (Security First Network Bank)는 최초의 가상 은행이라고 볼 수 있는데, 결제할 대상과 금액을 입력하면 자금 이체가 이루어지는 QuickPlay 서비스와 수표책을 보내주어 수표를 발행할 수 있는 수표발행 서비스를 실시 중이다.

나. 전자화폐의 국내 기술개발

1)금융결제원의 K-cash사업

금융결제원에서 추진하고 있는 K-cash는 IC카드형(접촉+비접촉식의 Combi형)으로서 선불 기능을 갖는다 하지만, 카드 발행기관이 자율적으로 직불· 선불기능을 추가할 수도 있다. 보안 체제로는 한국형 알고리즘(SEED)을, 운영체제로는 자체 COS를 사용하며, 국내 실정에 맞는 전자화폐 표준의 제정도 추진중이다.

2) 산업자원부의 개방형 전자화폐 개발 사업

IC카드방식의 개방형 전자화폐 시스템 개발이라는 사업으로 추진중인 전자화폐로 주요 개발 과제로 금융 표준(EMV, CEPS 등)을 바탕으로 국내외 지불시스템에서 사용 가능한 개방형 플랫폼 구성요소 및 애플릿 개발, 개방형 전자화폐 IC카드용 칩셋 및 단말기군 개발, 개방형 전자 화폐 기본시스템 및 응용 시스템 개발을 추진중이다.

4. 전자화폐의 표준화 현황

가. 전자화폐의 국외 표준화

■ **e-Cash**

Digicash에서 개발된 네트워크형 전자화폐 서비스로서 사용자는Digicash가 운영하는 eCash 결재 은행인 First Digital Bank에 등록하여 계좌를 개설한 다음, 자신의 PC환경에 맞는 eCash 클라이언트인 Digital Wallet을 다운로드 받아서 FDB에서 부여받은 비밀번호를 사용해 인터넷 상에서 대금을 결제할 수 있고 예금도 할 수 있다. 현재 미국, 호주, 독일, 핀란드, 스웨덴 등지에서 시험 운용 중이며, Gemplus, Schlumberger, Veriphone 등 카드제조사는 물론 AT&T, IBM, Toshiba등 통신 및 컴퓨터 업체가 참가해 만든 단체 표준이다.

■ **MONDEX**

IC카드를 이용한 전자지불 서비스로 영국의 NatWast은행과 미들랜드 은행이 중심이 되어 95년 7월부터 시행된 은행 중심의 전자화폐 관련 단체 표준으로 EMV와 달리 신용 카드가 아닌 은행을 중심으로 서비스가 이루어진다. 현재는 Mondex International사가 개발에 참여하고 있으며, 전세계 15개국, 1,270만개의 가맹점에서 운용중인 전자화폐이다. 현재 국제호환 결제 시스템을 구축중에 있다.

■ **CEPS(Common Electronic Purse Specifications)**

CEPS는 CEPSCO Espanola A.I.E., Visa International, Europay International, ZKA, EURO Kartensysteme에서 함께 참여하여 만들어진 전자지갑 서비스 표준이다. CEPS규격의 수정과 보완을 위해 CEPS 컨소시움이 '99년 5월에 설립되었고, 유럽 각국에서 추진됐던 독자 모델간의 호환성 확보를 위해 22개 국가들이 참여하여 만든 전자화폐 관련 단체표준(EMV규격과 호환)이다. 현재 초안이 제정된 상태이며, CEPS 기반 전자화폐시스템은 2000년초에 구축될 예정에 있다.

■ **VisaCash**

Visa International사에서는 CEPS를 기반으로 한 Visa Cash규격 (VCEPS)을 제정 중에 있다. CEPS 전자화폐 단체 표준과 금융 서비스 IC카드 단체 표준인 비자 Open Platform을 IC카드에 적용한 전자화폐이다.

나. 전자화폐의 국내 표준화

■ K-cash

금융결제원이 제공하는 전자화폐 공동 이용 서비스의 명칭으로서, '99년 4/4 분기 중 시범 실시 후 전국적으로 확대할 예정이며, 현재 K-CASH를 위해 국내에서 규격(금융IC카드, PSAM규격)을 작성 중이다.

■ 전자화폐 시스템 상호 호환 기술 표준

TTA 의 차세대 IC 카드 프로젝트 그룹에서 표준 제정 항목으로 추진중인 표준(2000 년 말에 표준 제정 완료)이다.

5. 결론

전자화폐기술을 정리하면 전자지불 및 보안, 전자카탈로그, 전자문서, 전자상거래서비스 영역으로 분류하여 적용할 수 있다.

현재 유럽, 북미, 동남아 등지에서 여러 가지 형태의 전자화폐가 개발, 실험 운영 중이며, 여러 가지 형태의 전자화폐를 지원하기 위해서는 통일된 시스템 구축 및 표준화된 단말기 보급이 필수적이다. 접촉식의 경우 현 은행간 차액 결제가 필요 없는 몬덱스(영국)형과 다수의 참가 은행이 발행에 참가하여 은행간 차액 결제가 필요한 프로톤(벨기에)형으로 구분되며, 네트워크 상에서 활용되는 전자화폐는 E-Cash, Cyber Cash, First Virtual, SFNB (Security First Network Bank) 등이 시범적으로 운영되거나, 실험 운영 중이다.

국내에서는 현재 금융결제원에서 추진하고 있는 K-cash 사업과 산업자원부의 개방형 전자화폐 개발 사업이 진행중이며, 금융결제원에서 추진하고 있는 K-cash 표준, TTA의 차세대 IC 카드 프로젝트 그룹에서 제정중인 전자화폐 시스템 상호 호환 기술 표준이 있다.

국제적으로는 네트워크형 전자화폐인 e-cash, IC 카드를 이용하는 Mondex, CEPS, VisaCash 등이 단체 표준으로 제정되어 활용되고 있다.

전자화폐의 안정적인 이용이 이루어지기 위해서는 지역적으로 타당한 신용거래 기반 형성과 네트워크 보안 등이 표준된 방식에 의해 보장될 수 있는 기술이 다져져야 하며 전자적 인식에 혼돈이 없도록 방지하여야 할 것이다.

참고문헌

[1] 몬덱스, http://www.mondex.com/mec_noflash.html
[2] CEPS (Common Electronics Purse Specifications), Visa Cash, http://www.visa.com/pd/cash/main.html
[3] E-cash, http://www.digicash.com/
[4] Cybercash, http://www.cybercash.com/
[5] 동국대학교 주재훈 교수, "인터넷 결제 시스템에 관한 비교연구", 1996 http://wwwk.dongguk.ac.kr/~givej/
[6] 이만영 외 5인, *전자상거래 보안 기술*, 1999, 생능출판사
[7] 금융결제원, http://www.kftc.or.kr/kor/index.htm