The Journal of Korean
Institute of CALS/EC
Vol. 4, No. 2, September. 1999

한국의 전자화폐 시스템 구축 방안에 관한 연구

이현제*, 정일주**

Research on the Development of the Electronic Money System in Korea

Ilchoo Chung, Hyun Jea Lee

Abstract

It is expected that the elctronic money will be a major payment method in the forthcoming electronic finacial system. However, in order for the electronic money to have a widespread use among general public in their dialy life there are many properties that should be satisfied beforehand. In this study, we first analyze the characteristics of the existing electronic money systems, compare various proposals on the electronic money system so far, and then suggest a desirable model of developing an electronic money system for Korean financial institutions. It has been found that the model we propose satisfies the general requirements of the electronic money system. The results of this study will aid in various activities of technology development and standardization. Furthermore, this study will support the initiative effort of Korea in developing inter-country electronic money system.

Keyword : *Electronic money, Cybercash, IC card, Electronic commerce, Electronic signature*

* 금융결제원 전자금융부
** 홍익대학교 상경대학 부교수

1. 서론

전자화폐는 새로운 일상생활은 물론 인터넷, 유선TV 등 다양한 네트워크 환경에서 전자상거래를 위한 미래의 새로운 지불 수단으로 광범위하게 사용될 것으로 전망되며, 특히 구미 선진국에서는 가까운 장래에 전자화폐가 본격적인 지급결제 수단으로 이용될 것으로 예상된다. 한국에서도 다가오는 전자금융 시대에 경쟁력 우위를 확보하기 위해 금융기관 및 정보통신 회사들은 관련된 기술의 개발 및 전자금융의 기반체계 구축을 위한 치열한 경쟁과 활발한 활동을 전개하고 있다.

전자화폐가 일반 국민에게 널리 사용되고 새로운 지급결제 수단으로 정착되기 위해서는 기존 화폐의 화폐적 특성들, 예컨대 유통성, 범용성, 양도성, 보안성, 익명성 및 프라이버시 등이 충분히 보장되어야 한다. 본 연구에서는 지금까지 제시된 다양한 전자화폐 시스템들을 비교·검토하여 그 특성을 분석하고 유형별로 장단점을 분석한 후, 한국적 특성을 감안하여 한국형 전자화폐 시스템의 모형과 구축방안을 제시하고자 한다.

본 연구의 결과는 향후 국내의 전자화폐 시스템 구축을 위한 기술 개발 및 표준화의 방향을 제시하고 이에 관한 논의를 활성화하며, 나아가 국제적인 전자상거래에 있어서도 한국형 전자화폐의 모형이 적용될 수 있는 환경의 조성에 기여할 것으로 기대된다.

2. 전자화폐 시스템의 개념 및 기본적 특성

2.1 전자화폐의 정의

화폐란 지불, 가치저장, 가치척도의 세 가지 기능을 동시에 충족시키는 자산이다. 전자화폐란 "컴퓨터, 칩, IC 카드, 네트워크 등 전자적 수단을 이용한 화폐로서 기존 화폐의 기능을 가지면서 컴퓨터와 정보통신 기술을 이용하여 컴퓨터 및 원격통신의 기능을 화폐기능과 결합시킨 전자적 결제방법"으로 정의된다. 예컨대, ecash라는 전자화폐 시스템에서 고객은 전자화폐를 은행에서 인출하여 자신의 로컬 컴퓨터에 저장하고, 저장된 전자화폐를 ecash를 받는 어느 상점에서도 사용할 수 있다[ecash, 1999].

현재 전자화폐는 일부 상점에서만 현금과 같은 지불수단으로 그 기능을 수행하고 있지만 모든 개인과 상점에서 이를 사용한다 하여도 지불 수단으로서 거의 손색이 없다. 컴퓨터 칩과 하드디스크 내에 화폐적 가치를 축적시켜놓고 물품 및 용역 구매 시 사용할 수 있으므로 가치저장 수단으로서 화폐 본연의 역할을 수행할 수 있는 것이다.

금융기관에서는 현금과 1 : 1 또는 일정비율로 전자화폐를 발행함으로써 현금과 같은 가치척도로서의 기능을 제공한다. 그러나, 전자화폐가 화폐로서의 기능을 충분히 수행할 수는 있지만 현금을 완전히 "대체"하는 것은 아니다. 발권은행이 본원통화를 전자화폐로 발행하지 않는 한 현금을 완전히 대체할 수 없기 때문이다[탁승호, 1996].

2.2 전자화폐의 바람직한 특성

기본적으로 전자화폐는 기존화폐가 갖는 장점을 살리고, 단점은 보완하면서 동시에 새로운 정보통신 기술이 제공하는 혁신적인 기능을 갖도록 요구되고 있다. 전자화폐의 기본적 요구사항은 전문가에 따라 다소 의견을 달리한다.

Matonis는 전자화폐의 기본적인 요구사항으로서 보안성, 익명성, 양도성, 양방향성, 오프라인 기능, 분할성, 완결성, 유통성, 사용자 친숙도 그리고 자유화폐단위의 10 가지 특성을 제시하고 있다[Matonis, 1996]. 반면에 Neuman과 Medvinsky는 위의 특성 목록과 상당히 중복되면서도 약간 다른 관점에서 요구사항을 제시하고 있다. 즉, 전자화폐는 보안성, 신뢰성, 규모성(Scalability), 익명성, 수용성, 고객기반, 유연성, 전환성, 효율성, 통합 용이성, 그리고 사용 용이성의 11 가지 특성을 가져야 한다[Chaum, 1992]. 한편 DigiCash사에서는 익명성을 가장 중요한 요구사항으로 꼽고 익명성을 만족시키는 전자화폐를 개발하는데 주력하고 있다. 또 Visa와 Master 등에서 추진하는 SET에서는 상호운영성을 가장 중요시한다.

2.3 전자화폐 시스템의 분류

전자화폐 "시스템"이란 컴퓨터 하드웨어, 소프트웨어 및 IC 기술, 네트워크, 인증 및 제반 표준 및 절차, 관련된 개인 및 기관 등을 포함하는 제반 요소들이 유기적으로 작용하여 이러한 새로운 전자적 결제가 이루어지도록 하는 전체적인 체계를 말한다. 지금까지 전세계적으로 수십 종류의 전자화폐 시스템이 개발되어 사용되어 왔다. 이들 시스템이 가진 다양한 특성들은 다음과 같은 몇 가지 개념으로 분류될 수 있다.

전자화폐를 분류하는 가장 기본적인 특성은 "가치저장 및 지불의 수단"이다. 이 특성에 의해 대부분의 전자화폐는 IC카드형과 네트워크형으로 분류된다. IC카드형은 플라스틱 카드 위에 부착된 IC칩에 화폐가치를 저장하여 반복해서 지불할 수 있는 방식이며 네트워크형은 컴퓨터통신망을 통해 인터넷 등 네트워크 상에 연결된 이용자의 PC에 화폐가치를 저장하였다가 전자상거래 대금지불 등에 사용되는 방식이다.

IC카드형은 다시 개인간 가치이전의 가능성 여부에 따라 개방형과 폐쇄형으로 구분한다. 개방형 IC카드는 개인간 가치이전이 가능한 반면 폐쇄형은 그것이 불가능하다. 선불카드라고 부르는 전자화폐는 폐쇄형 IC카드의 초기 형태로 볼 수 있다.

네트워크형 전자화폐는 모두 컴퓨터 네트워크 상에서 사용될 수 있다는 공통점을 가지고 있다. 네트워크형 전자화폐에는 다양한 가능성이 존재하여, 전자화폐의 형태 및 결제시점에 따라 다시 전자현금형, 신용카드형 그리고 전자수표형으로 구분된다. 전자현금형은 네트워크 상에서 가치저장 및 지불 시에 컴퓨터 하드디스크를 사용하는 말하자면 가장 순수한 의미의 전자화폐이다. 반면에 신용카드형은 기존의 신용카드 정보를 활용하여 네트워크 상에서 전자지불을 하는 방식을 말하며, 전자수표형은 기존의 수표와 유사한 개념으로 전자수표를 발행해 하드디스크에 저장하여 지불수단으로 사용하는 형태를 말한다.

이밖에도 전자화폐는 거래에 대한 결제 시점에 있어서 예금계좌의 잔액 감소나 현금의 입금이 이용자간 지급 시점보다 "먼저" 이루어지는 선불형과 "후에" 이루어지는 후불형으로 구분할 수 있다.

위의 분류는 복잡하고 다양한 전자화폐 시스템들의 특성을 이해하고 체계화하는데 유용하다. 그러면 지금까지 분류한 다양한 형태의 전자화폐 시스템들은 Matonis가 제안한 전자화폐의 바람직한 특성들을 어느 정도까지 만족시켜 주고 있는가 분석한다. <표 1>이 현금과 앞서 분류한 다섯 가지 전자화폐의 형태에 대한 특성들을 비교하고 있다.

2.4 전자화폐 시스템의 현황

현재 전 세계적으로 실험 단계에 있거나, 시장에서 사라졌거나 혹은 실제로 사용되고 있는 전자화폐는 수십 종류에 이르고 있으나 본 절에서는 1999년 현재 개발 혹은 사용 중인 전자화폐 만을 소개하기로 한다. 전자화폐 개발과 활용은 구미 선진국에서 활발하게 진행되고 있으며, 이 중에서 벨기에, 영국, 미국 등의 전자화폐가 가장 범용성이 높고 실용화에 가장 근접하고 있는 것으로 평가된다. 미국, 영국 및 네덜란드 등은 전자화폐 시스템의 개발과 상용화가 가장 먼저 이루어진 지역으

<표 1> 현금과 기존 전자화폐시스템의 특성 분석

특성요인	현금	IC 카드형		네트워크형		
		폐쇄형	개방형	전자현금형	신용카드형	전자수표형
유통성	탁월	가맹점만 가능	참가자만 가능	컴퓨상에서 가능	컴퓨터상에서 가능	컴퓨터상에서 가능
양도성	탁월	불가능	우수	은행개입 필요	신용카드사 개입 필요	은행개입 필요
범용성	탁월	가맹점만 가능	참가자만 가능	참가자만 가능	참가자만 가능	참가자만 가능
완결성	탁월	은행개재	탁월	은행개입 필요	신용카드사 개입 필요	은행개입 필요
보안성	보통	보통	보통	미약	미약	미약
익명성 및 프라이버시	탁월	보통	탁월	탁월	미약	미약
분할성	없음	있음	있음	없음	있음	없음
오프라인 처리 가능성	가능	가능	가능	불가능	불가능	불가능

<자료원: 한국은행, "전자화폐의 영향과 대응방", 1996. 2.>

로 First Virtual, CyberCash, Ecash, 몬덱스(Mondex) 등의 전자화폐 시스템이 개발되었다. First Virtual와 CyberCash는 신용카드형이고, Ecash는 전자현금형 그리고 Mondex는 IC카드형 전자화폐 시스템이다.

네트워크형 시스템의 개발은 특히 미국에서 활발한데, 그 이유는 컴퓨터의 보급률과 정보 통신 기술수준이 높고, 국토가 넓어 컴퓨터 통신망을 이용한 전자상거래의 효과가 세계 어느 곳보다 높기 때문이다[한국금융, 1997]. 미국 캘리포니아 대학에서는 Net_Cash라는 전자현금형 그리고 Net Cheque라는 전자수표형 전자화폐가 개발/시험 중이다. 신용카드형 전자화폐로 CyberCash사의 Cyber Cash, 비자/마스타 사의 SET 등이 시험 중에 있다.

미국에서는 IC 카드형 전자화폐도 활발히 개발되고 있다. IC카드형 전자화폐의 대표적인 예로서, 비자캐쉬(VISA CASH)를 들 수 있다. 비자캐쉬는 비자카드사가 1996년 아틀란타 올림픽을 대비하여 개발하였으며 은행의 ATM, 현금충전 전용 단말기 등을 통해 IC카드에 가치를 저장시키고 이것을 일반 상점, 자동판매기 및 공중전화기 등에서 사용한다. 개인간의 자금이체에도 편리하게 이용될 수 있는 몬덱스와 달리, 비자캐쉬는 가치이전, 즉 IC카드에 저장되어 있는 가치의 일부를 다른 사람에게 이전시키는 것이 불가능하여, 엄격히 말하면, 선불카드 기능에 범용성을 추가시킨 것에 불과하다 할 수 있다.

IC카드의 보급 측면에서는 유럽이 항상 선두를 유지하고 있다. 특히, 프랑스에서는 1989년 IC카드가 보급되기 시작한 이래 모든 은행계 카드는 IC카드로 100% 대체되었다. 벨기에서는 프로톤((Proton)이라는 IC카드형/폐쇄형 전자화폐가 1995년 2월부터 실험되고 있다. 프로톤은 ATM 등을 통해 전자화폐를 재충전할 수 있지만 개인간의 자금이체에는 사용할 수 없는 단점이 있다. 덴마크에서도 덴마크 은행의 자회사와 전화회사가 공동으로 설립한 단몬트(Danmont) A/S에서 "단몬트"라는 전자화폐를 발행하고 있다. 단몬트 역시 IC카드형/폐쇄형 전자화폐로서 대금 지불 방법은 프로톤과 비슷하지만 전자화폐의 재충전은 불가능하다[한국은행, 1998]. 반면에 영국에서 개발된 몬덱스는 IC카드형/개방형 전자화폐로서 1995년부터 시험 사용중이다. 한편, 네델란드에서는 Ecash라는 전자현금형 전자화폐를 1995년부터 실용화하고 있으며 이는 은닉서명 기법을 이용하는 익명성이 높은 시스템이다[DigiCash, 1999].

이제 전자화폐 시스템의 실용화를 위한 기술적 문제는 어느 정도 해결된 상태이며, 조만간 범용성과 보안성이 탁월한 전자화폐가 출현할 것으로 예상된다. 관련 기업들의 경쟁도 치열하게 전개될 것으로 보인다. 비자캐쉬사의 경우 최근에는 비자캐쉬를 보완한 CEPS(Common Electronic Purse Spec)를, 마스터카드사는 몬덱스를 발행하여 세계 시장을 선점하려는 계획을 추진하고 있다. 특히 이 두 회사는 기존의 신용카드 및 직불카드에 전자화폐의 기능을 추가하여 실질적인 원(One)카드의 개념을 현실화시킨 다기능카드도 개발하고 있어, 앞으로 전자화폐의 이용도가 크게 높아질 것으로 전망된다[국제전자상거래, 1997].

2.5 한국의 전자화폐 시스템 개발 현황

한편, 한국의 경우는 구미 국가들에 비해

전자화폐의 개발 및 활용이 뒤떨어져 있다. 현재 금융기관이 공동으로 추진하는 한국형 전자화폐 시스템이 본격적인 전자화폐 시스템의 개발 사례이다. 국가기관인 금융정보화추진위원회가 주관하고 금융결제원이 운영기관으로, 은행과 카드사가 카드 발행기관으로 지정되어 있는 이 전자화폐는 기본적으로 복합다기능 범용IC 선불카드로 앞의 개념에 의하면 폐쇄형 IC카드형 전자화폐로서 각 금융기관의 창구와 CD/ATM에서 충전이 가능하도록 되어있다.

국내 전자화폐의 다른 사례는 선불카드 방식의 교통카드이다. 서울, 부산, 경기 및 인천 지역에서 도입된 교통카드는 상품권 성격의 카드로서 현재 1천만 장 이상 발행되어 사용중이지만, 기술 부족, 국내 관련산업의 준비미비, 보안성과 안전성 취약, 각 지역간의 시스템 호환성 미확보 등 많은 문제점을 안고 있다. 특히, 전체 전자화폐 시스템의 핵심 부분인 카드 및 단말기의 안전성 및 신뢰성을 향상시키는 것이 시급한 것으로 평가된다.

그러나 앞으로의 발전 전망은 어둡지 않은 것으로 보인다. 금융기관 공동의 IC카드형 전자화폐 시스템 및 관련 기기가 개발되고 있고, 한국형 알고리즘인 SEED의 개발을 완료하는 등 한국의 전자화폐 시스템 기술은 빠른 발전을 보이고 있다. 앞으로 금융기관들이 선도적으로 전자화폐의 보급에 앞장서고, 적극적인 홍보활동을 편다면, 전자화폐에 대한 국민들의 마인드는 급속히 제고 될 것이다. 이 때 전자화폐 보급의 관건이 될 핵심적 과제는 몬덱스나 2000년 CEPS 상용화 예정인 비자캐쉬 등과 같이 전자화폐로서의 바람직한 특성 및 상품성을 충분히 보유한 전자화폐의 개발이 될 것이다.

3. 한국형 전자화폐 시스템의 요구사항 정의

그러면 지금까지의 논의를 중심으로 본 장에서는 한국형 전자화폐 시스템의 모형, 즉 바람직한 특성 및 요구사항을 정의하기로 한다. 한국형 전자화폐시스템의 모형을 구축하는 문제는 기본적으로 "이론적" 관점에 기반을 두고 실용적 측면을 조화시키는 방향으로 접근해야 한다. 이를 위해 본 논문에서 채택한 기본적인 접근 방향은 먼저 세계 각국에서 개발 혹은 사용 중인 다양한 전자화폐 시스템과 관련 기술을 벤치마킹하고, 중장기적인 기술 발전 추세를 분석하는 동시에 한국적 특성을 고려하여 한국형 전자화폐 시스템의 모형을 도출하고 요구사항을 정의하는 것이다.

3.1 한국형 전화화폐 시스템의 기능적 요구사항

먼저 한국형 전자화폐 시스템 모형의 골격인 기본적 형태를 IC카드형으로 할 것인가, 네트워크형으로 할 것인가 아니면 제 3의 방안이 존재하는가에 대한 심도 있는 검토가 필요하다. 앞서 소개한 <표 1>의 분석에 의하면 IC카드에서는 "개방형"이 그리고 네트워크형에서는 "전자현금형"이 익명성에서 뛰어나다. 그러나 각 형태에 속한 전자화폐 시스템을 세부적으로 분석하면 또다시 상당한 다양성이 나타난다. 따라서 앞서 분류한 IC카드와 네트워크형에 속한 각각의 전자화폐 시스템을 보다 구체적으로 비교하고 분석하기로 한다.

현재 세계 각국에서는 다양한 개방형 혹은

폐쇄형 IC카드형 전자화폐가 시험 혹은 사용 중이나 이들 시스템은 대부분 인터넷 환경을 고려하지 않은 시스템이어서 인터네트 상에서의 전자지불에는 적용될 수 없는 실정이며, 최근에야 이에 대한 대응이 시작되고 있다. IC카드형 전자화폐 시장을 주도하고 있는 두 대표적 시스템은 마스터카드사의 개방형 시스템인 몬덱스와 비자사의 폐쇄형 시스템인 비자캐쉬이다. 몬덱스의 가장 큰 장점은 개인간 가치이전이 가능하고 높은 익명성을 제공한다는 점이나 유통성이 취약한 것이 흠이다. 몬덱스는 개인간 가치이전이 가능하나 보안성은 취약한 반면에 비자캐쉬는 카드 훼손 시 환불이 가능하고 돈세탁 및 불법사용을 방지하는 보안성이 뛰어나지만 익명성과 유통성이 취약한 약점을 가지고 있다[한국전산원, 1996]. 이 두 회사 모두 향후 카드를 이용한 인터네트 전자지불시스템의 구현, 접촉식 및 비접촉식 카드의 개발, 그리고 비대칭 암호방식의 채택을 추진하고 있어 앞으로 이러한 추세가 세계 전자화폐 시장을 선도할 것으로 예상된다[한국전산원, 1996]

네트워크형 전자화폐 시스템의 경우 DigiCash의 Ecash, NetCash, Millicent Protocol, PayMe Protocol 및 NetBill 시스템은 모두가 전자현금형에 속하지만 이들은 각기 상이한 시스템 아키텍쳐, 보안체계 및 익명성 전략을 가지고 있다. 익명성에서는 Ecash와 PayMe Protocol이, 보안성에서는 Ecash가 그리고 확장성에서는 NetBill과 NetCash가 가장 우수한 것으로 평가된다[성기윤, 1996; 임채호, 1999].

신용카드형 전자화폐의 가장 큰 장점은 신용카드를 이용한 구매와 관련한 거래처리 절차가 잘 정의되어 있어, 인터넷 기반의 신용카드형 시스템을 구축하기가 용이하다는 점이다. 신용카드형 전자화폐 중 First Virtual Holdings는 소액거래가 가능한 반면 이용절차가 복잡하며, CyberCash와 SET는 사용이 편리한 대신 소액거래가 불가능하다[임채호, 1999].

전자수표형은 추적·감사가 가능한 지급결제 수단이며 거액의 결제를 지원하기 때문에 기업들에게 유용하다. 전자수표형은 또 EDI 또는 회계정보시스템에 전자수표형 전자화폐를 통합하는 것이 용이하다는 장점이 있으나 부도 위험 때문에 광범위하게 수용되기 어렵다. 전자수표형 전자화폐 중에서 ECheck은 유연성에서 NetCheque는 소액결제 가능성에서 우수하나, 수표의 기본적 특성 때문에 모두 복잡한 암호화와 인증체계를 가질 수밖에 없다는 단점을 가지고 있다[임채호, 1999].

지금까지의 논의를 요약하면 첫째, 개방형 IC카드는 양도성과 완결성에서 현금 수준의 우수성을 보이고 있고, 오프라인 처리 기능도 제공하고 있다는 점에서 기존의 형태에서는 가장 바람직한 것으로 평가된다. 그러나 IC카드형은 아직은 네트워크에서의 운용이 정착되지 못하여 최근에 폭발적으로 그 이용이 확대되고 있는 인터네트 환경에의 적용이 제한적이라는 취약점을 안고 있다.

둘째, 최근 같은 형태 안에서도 다양한 전자화폐가 등장하는가하면 아예 IC카드형과 네트워크형의 구분을 넘어서는 혼합된 형태가 등장하고 있다는 사실에 주목할 필요가 있다.

셋째, IC카드형 전자화폐 시장을 주도하고 있는 비자사 및 마스터카드사는 비자캐쉬 및 몬덱스 카드의 기능을 개선하여 인터네트 환경에서 네트워크형 전자화폐로 사용할 수 있

도록 하기 위해 열띤 경쟁을 벌이고 있어 이러한 방향은 세계적인 추세가 될 것으로 예상되어 이에 대한 관심이 필요하다

한편, 한국의 전자화폐 시스템의 모형에 대하여 그 동안 다양한 방안이 논의되었으며 그 중 가장 종합적이며 대표적인 모형은 1999년 7월 금융정보화추진위원회에서 발표한 "금융IC카드 표준"이다. 이 표준은 그 동안의 전자화폐에 관련된 다양한 논의의 결과를 포함하고 있다는 점에서 긍정적 평가를 받고 있으나, 반면에 장기적인 관점에서 볼 때 다음의 몇 가지 제약점을 가지고 있는 것으로 평가된다. 첫째, 전자화폐와 전자화폐간의 이체, 즉 개인간의 가치이전이 불가능하고, 둘째 전자화폐가 네트워크 상에서 지불수단으로 사용될 수 없으며, 따라서 인터네트 상에서의 사용이 불가능하고, 셋째 이 전자화폐는 국가간의 거래에는 사용이 불가능하다.

이와 같은 분석 결과를 한국의 전자화폐 시스템의 환경에 적용해 보면 한국형 전자화폐 시스템에서 요구되는 중요한 세 가지 기본적 특성이 도출된다. 첫째, 현금과 유사한 수준의 유통성, 양도성, 보안성 및 익명성을 제공할 수 있어야 하고, 둘째 한국의 컴퓨터 보급 및 인터네트 이용의 급속한 확대에 맞추어 인터네트를 포함한 네트워크 환경에 적합한 전자화폐가 요구된다. 셋째, 한국형 전자화폐 시스템의 기본 방향은 세계적 추세에 부응하는 방향으로 설정되어야 한다.

요약하면, 한국형 전자화폐 시스템의 기본적인 형태로서 개방형·IC카드형이면서도 전자현금형과 같이 네트워크 상에서 사용이 가능한 "혼합형"이 가장 바람직한 모델이 될 것으로 판단된다.

3.2 한국형 전화화폐 시스템의 추진 원칙

다음으로 한국형 전자화폐 "시스템"의 구현 과정에서 고려될 정책적 사항들을 검토한다. 기본적으로 한국형 전자화폐 시스템의 구현은 기술적인 관점에 집착하여 단순히 신기술의 장점만을 취하기보다는 전반적인 전자화폐 시스템의 요구와 향후 세계적인 전자화폐 시스템의 발전 방향 등의 환경 요인을 고려하여 전략적 차원에서 이루어져야 한다. 이를 위해 다음의 네 가지 기술, 제도 및 산업적 요구사항과 원칙을 제안한다.

첫째, 고객의 성향을 최대한 고려하여 이용자에게 친밀감을 주면서 값이 저렴한 새로운 장비가 개발되어야 한다. 둘째, 한국과 같이 대부분의 금융기관이 네트워크 상에서 연결된 국가에서는 전자화폐 시스템과 금융기관의 시스템과의 높은 연계성이 요구된다. 그렇지 않은 경우 막대한 신규 투자비용이 소요될 것으로 예상된다.

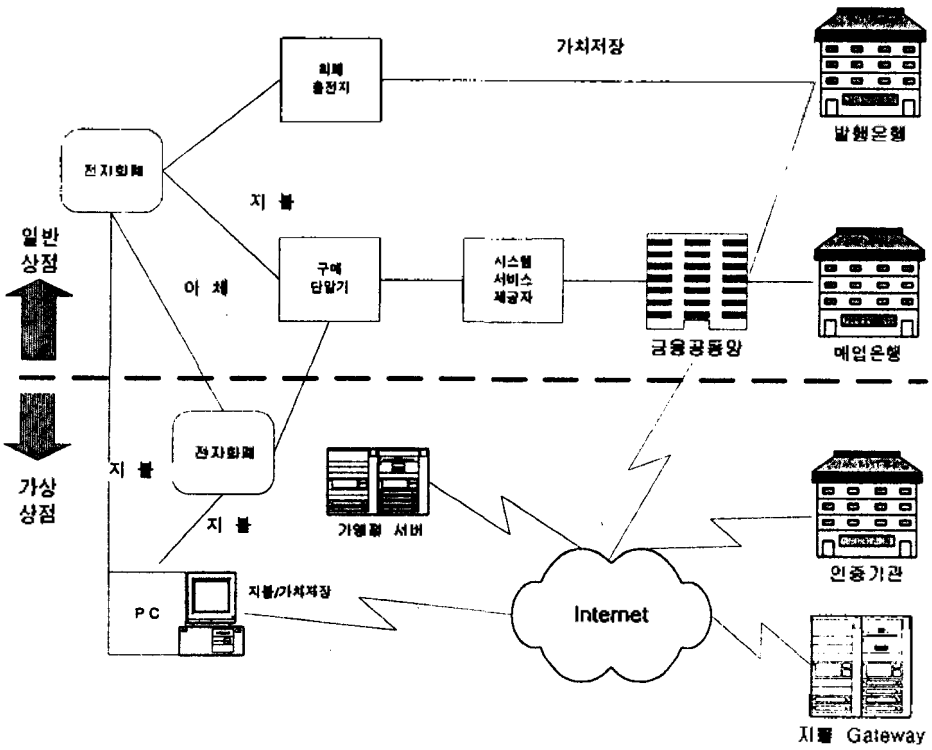
셋째, 전자화폐 시스템을 위해 도입된 제반 컴퓨터, 네트워크 및 소프트웨어 시스템의 호환성 및 상호 운영성 등이 확보되도록 하여야 한다. 이를 위해서는 각국의 시스템 통합사와의 제휴와 협력이 필요하다. 마지막으로, 전자화폐 시스템 관련 제품 시장의 합리화가 필요하다. 특히 IC카드 및 관련 단말기 제조와 관련된 표준의 제정, 개발사들의 상호 기술 협력 그리고 보급용 기기의 저렴한 가격 등이 요구된다.

4. 한국 금융기관의 전자화폐 시스템의 구축 모형

4.1 시스템의 특성

앞서 한국형 전자화폐시스템에 대한 요구사항으로서 높은 수준의 화폐적 특성의 보유, 개인간의 가치이전, 인터네트를 포함한 네트워크 상의 전자지불 그리고 높은 수준의 보안체계와 익명성의 보장 등을 제시하였다. 본 장에서는 이와 같은 요구사항들을 고려하여 <그림 1>과 같은 "한국형" 전자화폐 시스템의 모형을 제안한다. <그림 1>에서 굵은 점선의 위 부분이 1999년 7월에 발표된 "금융 IC카드 표준"이 제안하는 전자화폐 모형이다. 기본적으로 한국형 전자화폐 시스템은 가치이전이 가능한 개방형 시스템이면서 동시에 인터네트 상에서의 전자지불이 가능한, IC카드형과 네트워크형이 혼합된 형태가 바람직하다.

구체적으로 이 모형의 중요한 내용을 설명하면, 첫째 <그림 1>에서 전자화폐 간의 "이체"로 표현된 기능, 즉 개인간의 가치이전 기능이 포함되어 있고, 둘째 인터네트를 통해 가



<그림 1> 금융기관 공동의 전자화폐시스템 구축모델

맹점서버, 인증기관, 지불게이트웨이 그리고 개인의 PC가 연결되어 있다. 셋째, 이 모형에는 가상상점(<그림 1>의 하단 부분)이 포함되어 있다. 즉, 기존의 일반상점에 추가하여 네트워크 상의 가상상점에서도 전자화폐를 사용할 수 있게 된다. 넷째, 현재의 "금융 IC카드 표준" 모형에서는 전자화폐의 충전지(充電地)가 CD/ATM 단말기로 제한되어 있으나, 새로운 모형에서는 그것이 네트워크 상에서도 가능하도록 함으로써 고객이 전자화폐 충전을 위하여 일일이 은행 지점을 방문해야 하는 불편이 줄어든다.

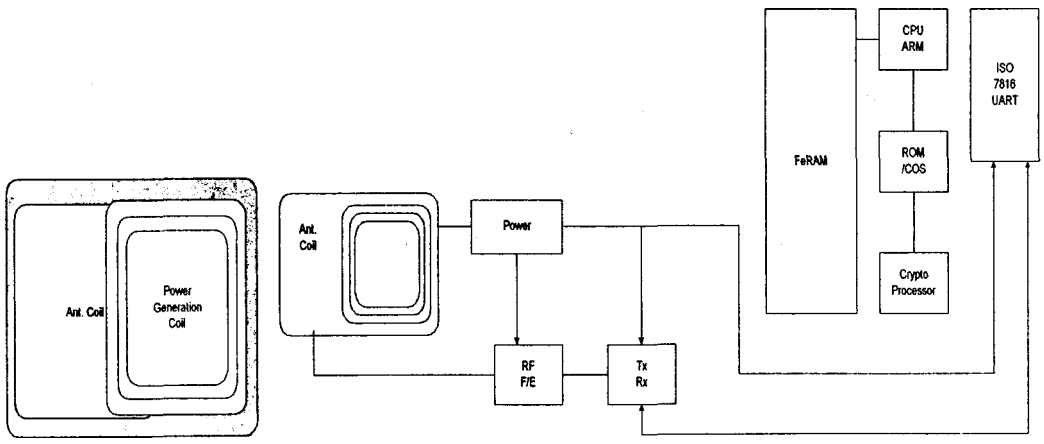
4.2 시스템 구축 모형

4.2.1 새로운 IC카드 기술의 활용 및 개발

IC카드형 전자화폐시스템의 핵심적 요소는 IC카드이다. 따라서 이와 관련된 기술, 즉 범용 IC칩 및 COS의 개발이 우선적으로 이루어져야 한다. IC칩의 범용성을 확보하기 위해서는 ISO 및 EMV(Europay, Mastercard, VISA) 관련 표준을 수용하는 것이 바람직하며, IC칩의 기술적인 유연성, 개방성, 상호운영성 및 안전성 등의 확보가 필요하다[서울대, 1997].

1999년의 금융IC카드표준에서 채택한 COS(Chip Operating System)는 범용성을 갖지 못한 "전용" 시스템인 것이 문제점으로 지적된다. 따라서, ISO 및 EMV 표준을 기반으로 한 IC칩에, 동시에 다양한 어플리케이션을 수용할 수 있으면서도 매우 안전하며 다중 어플리케이션의 지원이 가능한 새로운 운영체계의 개발, 기존의 전용 COS를 수용할 수 있는 "범용" 카드의 개발 혹은 양자를 통합한 IC칩 및 COS의 개발이 요구된다.

또한 국내 기업이 독자적으로 개발한 제품은 범용성을 확보하는데 한계가 있을 것으로 예상된다. 따라서 <그림 2>와 같이 현재 세계적으로 유수한 IC카드사들이 공동 개발 중인 비자의 범용카드인 JAVA카드 또는 마스터카드의 범용 운영체계인 MULTOS 프로젝트에



<그림 2> IC칩 및 COS의 기술발전 방향

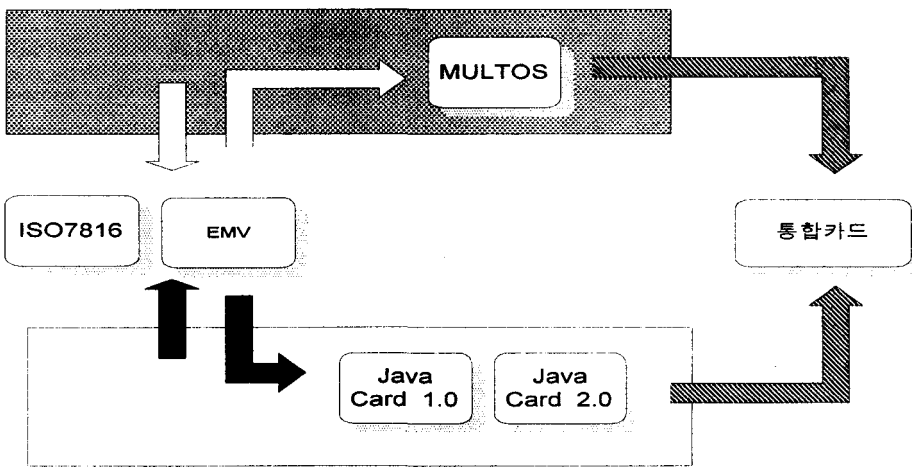
국내의 기업들이 전략적으로 참여하여 범용성 기술을 확보하는 것이 바람직하다.

다음으로 접촉식 및 비접촉식 통합카드의 개발이 필요하다. 기본적으로 IC카드는 접촉식이지만, 버스 및 지하철과 같은 교통수단에는 신속한 거래처리가 가능한 비접촉식 카드가 적합하다. 따라서 향후 사용할 접촉식 카드와 비접촉식 카드를 하나로 통합한 형태로 <그림 3>과 같이 메모리를 공유하고, 비대칭형 알고리즘을 신속히 연산할 수 있는 복호화처리기(Crypto-processor)가 내장된 카드를 개발하는 것이 바람직하다[Matonis, 1995].

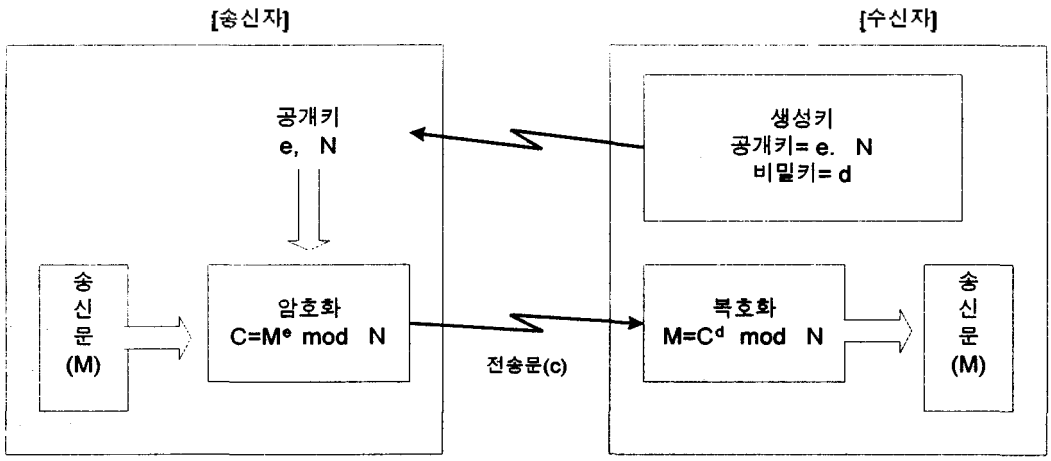
이와 같은 특성을 가진 IC카드를 금융기관이 발행하면, 첫째 카드의 발행에 따른 제반 비용을 절감할 수 있고, 둘째 다양한 제품 및 서비스의 제공이 가능하며, 셋째 교통기관의 요구을 만족시켜 상호 연계가 용이하다는 장점이 있다. 동시에 고객 입장에서는 여러 개의 카드를 소지함에 따른 불편을 해소하면서 다양한 제품 및 서비스를 선택할 수 있게 되어 편리성이 높아진다.

4.2.2 비대칭형 암호 방식의 채택과 설계

국내 금융기관이 발행한 전자화폐가 범용성, 호환성 및 안전성을 보장받으며 거래되기 위해서는, 비교적 구현이 용이하고 암호화 속도가 빠른 기존에 개발된 전자화폐의 비밀키 암호 방식으로 데이터를 암호화 및 복호화 하여 전송할 때 사용하여야 한다. 송수신 메시지의 부인(否認)봉쇄를 위한 전자서명에는 메시지 암호화에 사용된 비밀키의 분배 및 거래쌍방이 동일한 키를 사용하는 관계로 <그림 4>와 같이 비대칭형 암호 방식을 채택하여 설계하는 것이 바람직하다. 또 인터넷에 기반을 둔 전자지불거래에 전자화폐를 사용할 때는 가상상점 서버에 SAM(Secure Application Module)을 장착하여 거래가 이루어지도록 구현할 수 있다.



<그림 3> 접촉식 및 비접촉식 IC카드의 통합 모형



<그림 4> 비대칭형 암호 방식

4.2.3 사용자 등록

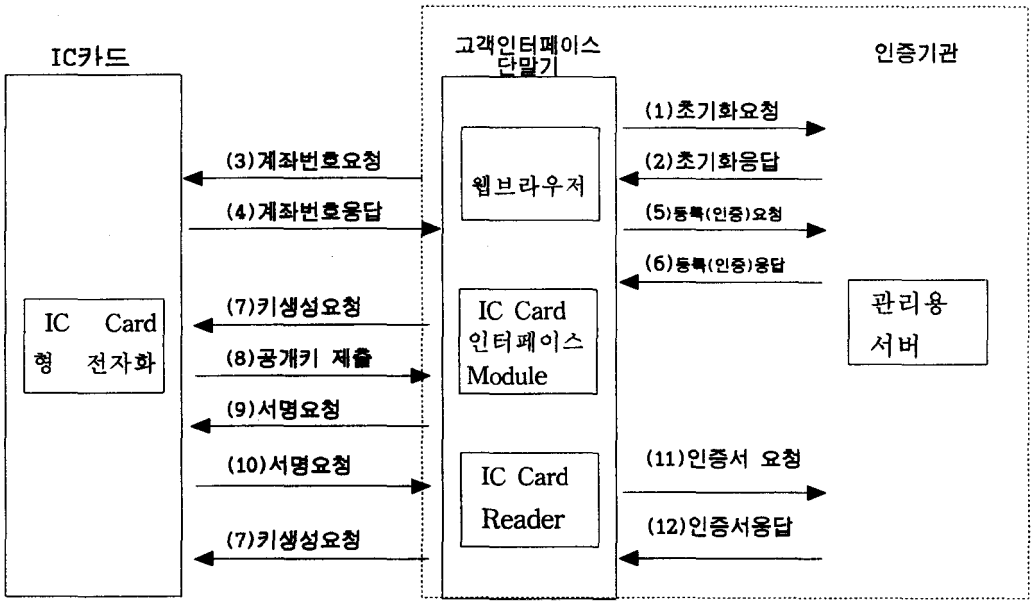
일반 가맹점뿐만 아니라 인터넷과 같은 규모가 큰 네트워크 시스템에서는 안전한 통신 링크를 확립하고자 하는 사용자들에 대하여 공신력 있는 누군가가 보증을 서주는 것이 바람직하며 이러한 기능을 수행하는 곳이 인증기관이다.

네트워크의 사용자는 공개키를 생성하게 되고 인증기관에 의해 증명되어야 한다. 사용자는 한 번의 공개키 인증을 받으면 자신의 공개키를 다른 사용자에게 보내야 한다. 그리고 네트워크의 모든 사용자는 자신의 공개키와 비밀키를 생성하여 인증기관에 공개키를 등록하고, 키 인증기관도 자신의 공개키와 비밀키를 생성하여 사용자에게 알려줌으로써 모든 사용자는 인증기관의 공개키를 알고 있어야 한다.

따라서 <그림 5>와 같이 IC카드형 전자화폐, 일반상점의 SAM 및 가상상점 SAM, 일반상점과 연계된 시스템서비스제공자의 SAM 및 지급정보 중계기관(Payment Gateway)은 모두 인증기관으로부터 인증서를 받아야 한다. 각각의 참여자 별로 인증서를 받는 절차는 상이하며 본 연구에서는 지면상의 제약 때문에 IC카드형 전자화폐의 등록 절차만 제시한다. 이러한 인증 방법은 국제표준 규격인 X.509와 SET에서 제안된 인증골격과 매우 유사하다.

4.2.4 전자화폐의 가치저장

가치저장거래는 국내 가맹점에서 전자지불을 위한 가치저장 거래와 인터넷상의 가상상점에서 전자지불을 위한 해당국통화(Multi-currency)로의 가치저장 거래로 구분한다. 이때 해외 통화의 전자화폐 내의 가치저장은 기존의 환전 개념을 이용하되, 고객의 계정에 의거 전자화폐를 발급받은 발행기관의 CD/ATM



<그림 5> 사용자 등록 및 인증 절차

또는 창구단말기 등을 통하여 가치저장 당일의 환율 기준으로 계산하여 전자화폐의 최대 저장한도 및 국내의 외환거래 관련법에 저촉되지 않는 범위 내에서 가치저장을 받는다.

가치저장 절차는 다음의 세 가지로 구분한다. 첫째, 고객에 의한 가치저장 요청 절차는 다음과 같다.

① 전자화폐의 금액에 대한 일련번호를 부여한다. 이 일련번호들은 은닉서명(Blind Signature) 기법을 사용했을 때 동일한 결과가 나오는 것을 방지하기 위해서 100자 정도의 크기를 가진다.

② 고객만이 알고 있는 숫자로 일련번호를 곱하여 은닉서명을 한 뒤에, 이 전자화폐들을 하나의 메시지로 만든다.

③ 이 메시지를 자신의 비밀키를 이용하여 전자서명을 하고, 발행기관의 공용키를 이용하여 암호화 한 뒤에 발행기관으로 전송한다.

둘째, 발행기관에서의 가치저장 절차는 다음과 같다.

① 고객이 보내온 메시지를 자신의 비밀키로 복호화 한다.

② 고객의 공용키를 이용하여 전자서명을 확인한다. 이 과정에서 아무런 문제가 없을 경우 고객의 계정에서 신청한 전자화폐에 상당하는 금액을 인출한 뒤에 은닉서명된 전자화폐를 자신의 비밀키로 전자서명 한다.

③ 이 메시지를 고객의 공용키로 암호화한 뒤에 고객에게 전송한다.

셋째, 전자화폐 내 가치저장 절차는 다음과 같다.

① 발행기관이 보내온 메시지를 자신의 비밀키로 복호화 한다

② 금융기관의 공용키를 이용하여 금융기

관의 서명을 확인한 뒤에 은닉서명 시에 사용했던 숫자로 각각의 일련번호를 나누면 금융기관이 서명하여 인정한 전자화폐가 고객의 전자화폐 내에 저장된다.

4.2.5 전자화폐를 이용한 인터넷상의 지급거래

발행기관이 발행한 전자화폐를 이용하여 인터넷상의 가상상점에서 상품을 구매하는 경우 웹브라우저와 클라이언트 소프트웨어를 이용해야 한다. 전자화폐 지불시스템에는 암호화, 전자서명 그리고 사용자인증서의 세 기술이 필요하다[허철회, 1999]. 인터넷상의 전자지불거래의 처리 절차는 <그림 6>과 같다.

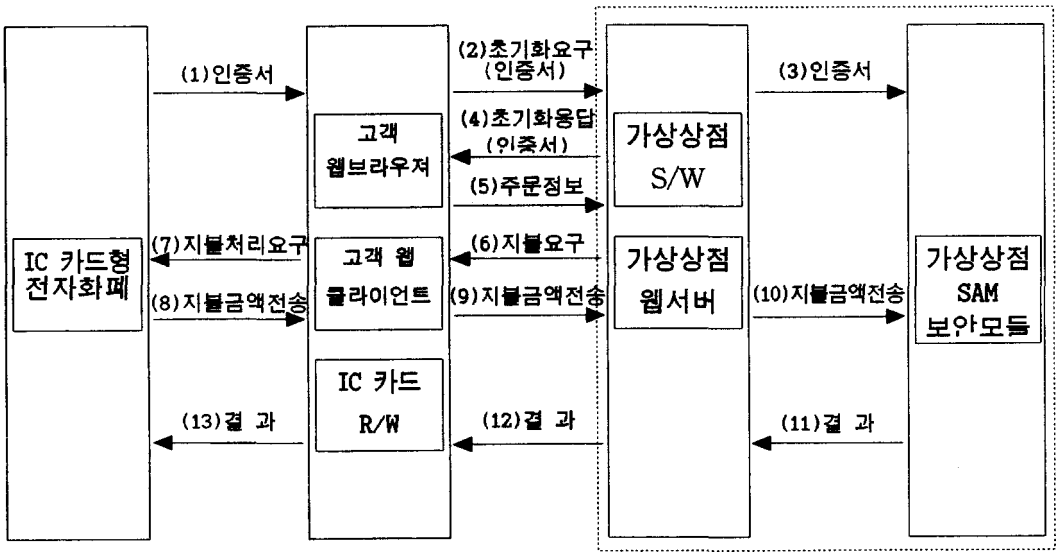
4.2.6 개인간의 가치이전

현재 개발 중인 대부분의 전자화폐 시스템이 개인간의 가치이전을 허용하지 않지만, 일부 시스템에서는 이를 허용하고 있다. 전문가들은 개인간 가치이전을 허용할 경우 돈세탁 수단으로 악용될 위험성이 높고 특히 마약구매 등 불법거래 대금의 지급 시 현금대용으로 사용될 가능성이 높다는 이유로 이를 반대하고 있다.

그러나 본 연구에서는 막대한 발권, 폐기 및 화폐관리 비용을 절감하고, 개인간의 가치이전을 용이하게 하여 현금에 보다 가까운 기능을 부여함으로써 높은 사생성을 확보하기 위해 개인간의 가치이전이 가능토록 하였으며 개인간의 가치이전에 따른 부정사용을 방지하기 위해서 가치저장한도의 설정과 가치이전 및 소유주에 대한 제한 등을 통해 이러한 문제를 해결토록 한다. 개인간의 가치이동 절차에 대해서 구체적으로 살펴본다.

① 전자화폐 지불인이 전자화폐 수취인에게 전달하고자 하는 금액을 자신의 비밀키로 서명을 하고, 전자화폐 수취인의 공용키를 사용하여 암호화하여 수취인에게 전달한다.

② 전자화폐 수취인은 자신의 비밀키로 복



<그림 6> 인터넷상의 전자지급거래 절차

호화 하고, 전자화폐 지불인의 공용키를 사용하여 전자서명을 확인한다.

③ 확인된 금액은 수취인의 전자화폐에 저장된다.

4.2.7 인터넷상 전자지급거래에 대한 자금정산

인터넷상의 전자지불 거래에 대한 자금정산 방법은 기본적으로 기존의 전 세계적인 네트워크를 운영하고 있는 국제적인 지급결제기관인 비자 및 마스터카드 사의 지급결제망을 이용하거나 국제간지급결제망인 SWIFT망 등을 이용할 수 있다. 따라서 국내 금융기관이 자체 해당국 통화를 발행할 경우 SWIFT 망을 이용하여 자금정산을 하며, 비자의 비자캐쉬 및 마스터카드의 몬덱스 상품을 발행할 경우에는 비자 또는 마스타카드의 지급결제망을 이용하여 다국가용 전자화폐를 발행한 국내 금융기관과 해외에 위치한 가상상점의 웹서버 운영 지역 금융기관간에 자금정산을 한다.

4.2.8 익명성 및 프라이버시 보호 방안

전자화폐를 이용한 거래의 익명성 및 프라이버시의 문제는 여러 가지의 경우가 있다. 법원의 명령에 의해 사용자와 거래의 내용을 밝혀야 할 경우도 있고, 상세한 거래 내역을 필요로 하는 경우, 또는 자신의 재무정보 시스템을 개선하기 위한 자료가 필요한 경우 등 익명성 및 프라이버시를 포기하지 않으면 안 되는 경우가 존재한다. 한편 한국형 전자화폐는 교통, 통신 및 인터넷의 소액시장을 대체하는 것이 주목적이기 때문에 익명성 및 프라이버시 보호로 인한 불건전한 지금이동, 즉 돈세탁 문제는 심각하지 않을 것으로 판단된다.

중요한 것은 개인정보의 프라이버시 보호의 움직임이 강화되는 경향으로서, 미국에서는 1994년, EU에서는 1995년에 각각 개인정보의 보호에 관한 법을 제정하였다. 한국에서도 공공기관의 개인정보에 대한 법률, 신용정보의 이용 및 보호에 관한 법률, 형법, 전파법 등에서 공공기관, 신용기관 및 금융기관 등이 보유한 개인정보를 보호하도록 규정하고 있다.

익명성 및 프라이버시 보호는 전자화폐의 광범위한 보급에 필수적이다. 특히 금융기관에서 취득한 고객의 개인정보 중에는 신상에 민감한 항목도 포함될 것이며 이러한 정보가 누출될 경우 고객들의 강력한 항의와 이에 따른 전자화폐 시스템 전체의 이미지 손상이 우려된다.

이러한 점들을 고려할 때, 익명성 및 프라이버시를 보장할 수 있는 방법으로는 우선 일반 가맹점이나 가상상점 등에서 전자지불을 할 경우 각 시스템에서 거래내역 중 전자화폐 발행기관의 식별자, 총건수 및 금액 등 최소한의 항목만을 관리하도록 설계한다. 더 많은 정보를 포함하면 결국 시스템 상에서 추적이 가능하기 때문에 익명성의 근본적인 보장이 어려워지기 때문이다. 아울러 전자화폐의 발행시 은닉서명을 이용한 익명성의 보장, 이중사용의 방지, 신용정보의 안전성 확보 등을 기본적 요구조건으로 하여 이를 만족시키는 프로토콜을 설계함으로써 고객의 프라이버시가 보호되도록 구현할 수 있다[Chaum, 1992: 1999].

5. 결론

본 논문에서는 IC카드와 네트워크형을 혼합하면서 개인간 가치이전이 가능하고 인터넷 환경을 지원하는 새로운 한국형 전자화폐

시스템의 모형과 구축방안을 제시하였다. 이 모형은 현재 가용한 기술을 최대한 활용하고 있기 때문에 실현가능성이 높으면서도 화폐적 기능이 높아 전자화폐로서의 바람직한 특성을 충분히 갖춘 이상적 전자화폐 시스템을 정의하고 있다고 판단된다. 이 모형은 최근 제안된 "금융IC카드표준"의 모형의 몇 가지 잠재적 문제점들을 보완해 줄 것으로 기대된다.

이와 함께 한국형 전자화폐 시스템의 범용성, 유통성 및 상호운영성 등을 확보하기 위해서 새로운 카드 기술을 활용한 IC카드 및 운영체제로서 "범용성"을 갖춘 COS의 개발 그리고 접촉식 및 비접촉식 카드를 통합한 카드의 개발을 제안하였다.

또 전자화폐 시스템의 보안성 및 거래에 따른 안전성을 보장받으며 거래가 수행되도록 하기 위해 국제적 호환성에서 한계를 가진 것으로 평가되는 현행 금융IC카드표준의 대칭형 SEED 알고리듬 대신에 "비대칭형" 암호 방식을 채택하여 설계토록 하였다. 아울러 사용자 인증, 개인 간 가치이전, 인터넷상의 전자지불 및 자금정산 방안 등을 제안하고 전자화폐 시스템의 익명성 및 프라이버시 보호방안을 제시하였다.

그러나 본 연구에서는 한국형 전자화폐 시스템의 기능적, 기술적 측면을 중심으로 모형을 도출하고 구축방안을 연구하는 것이 목적이기 때문에 현행 법·제도상의 제약점에 대해서는 다루지 못하였다. 본 연구와 관련하여 앞으로 계속 관심을 가져야 할 연구 대상 분야는 첫째, 전자화폐 시스템의 법·제도에 관한 연구, 둘째 IC카드형 및 네트워크형 전자화폐와 교통카드의 통합 방안에 관한 연구, 셋째 전자화폐 시스템의 안전성 확보를 위한 보안기술 연구 그리고 마지막으로 전자화폐 시스템의 인증체계에 대한 연구 등이다.

참고문헌

[국제전자상거래, 1997] 국제전자상거래연구센터, "전자상거래, 전자지불, 전자화폐 및 정보시스템", *'97추계 한경금융포럼*, 한국경제신문사, 1997. 11.

[김영달, 1996] 김영달외 1인, "전자지불시스템의 기능요건과 기술동향", *정보처리*,제 3권, 1996. 7, p.17.

[김현일, 1996] 김현일, *전자화폐 전쟁*, 전자신문사, 1996. 8.

[서울대, 1997] 서울대컴퓨터신기술공동연구소, "IC카드연구센타 창립2주년 기념워크숍", 1997. 10.

[성기윤, 1996] 성기윤, "인터넷 기반 지불시스템의 분석 및 설계", KAIST 테크노경영대학원 석사학위논문, 1996. 7.

[신진원, 1996] 신진원, "스마트카드의 카운터에 기반을 둔 안전한 전자화폐시스템에 관한 연구", 석사학위논문, 연세대학교대학원, 1996. 6, p.2.

[이영숙, 전재현, 1998] 이영숙, 전재현, "주요국의 전자지갑 개발현황", 한국은행금융결제부, 1998.

[임채호, 1999] 임채호, "인터넷기반 전자상거래의 활성화를 위한 전자지급결제 시스템 구축 방안", 석사학위논문, 테크노경영대학원, 1999.

[탁승호, 1996] 탁승호, *전자화폐와 결제시스템*, 더빵커사, 1996. 2.

[한국금융, 1997] 한국금융연구원, "전자기술의 발달과 은행산업의 미래", *전자금융·화폐국제심포지엄*, 1997. 3.

[한국은행, 1998] 한국은행 금융결제부, "각국의 전자화폐 개발현황", 국제지급결제제도 실무위원회, 1998. 12.

[한국전산원, 1996] 한국전산원, "전자상거래 환경을 위한 기술조사 연구", *국가기간전산망 표준화 연구*, 1996. 10.

[허철회, 1999] 허철회외 2인, "전자화폐지불시스템의 위험요소분석 및 프로토콜 설계", *한국전자거래학회지*, 제4권1호, 1999, 102-115.

[홍승필, 1998] 홍승필, 고재욱, *정보보안 기술과 구현*, 도서출판 파워북, 1998.

[Brands, 1995] Brands,S., "Electronic Cash on the Internet", *Proceedings of the Internet Society 1995 Symposium on Network and Distributed System Security*, 1995.

[Chaum, 1992] Chaum, D., "Achieving Electronic Privacy", *Scientific American*, 1992, p.96-101.

[Chaum, 1999] Chaum, D., "Online Cash Check", http://www.digicash.com/news/achive/online.html/, 1999

[ecash, 1999] "The ecash concept", http://nii.nist.gov/g7/10_global_mp/testbeds/ecash.html.

[DigiCash, 1999] "How ecash Work Inside", http://www.digicash.com/ecash/docs/index.html, 1999

[Matonis, 1995] Matonis, J., "Digital Cash and Monetary Freedom", 1995, http://www.isoc.org/in95pr/HMP/PAPER/136/html/paper.html.

저자소개

이현제 (e-mail : lhje@kftc.or.kr)
금융결제원 전자금융부 과장
Korea Financial Telecommunications & Clearings Institute
관심분야: 전자상거래, 전자금융

정일주 (e-mail : chungic@wow.hongik.ac.kr)
홍익대학교 상경대학 경영정보학과 부교수
Department of Information Systems, Hongik University
관심분야: 정보시스템, 전자상거래, 전자금융, 데이터베이스