전자화폐 표준화 동향 분석에 관한 연구

A Study on the analysis of the Standardization trend of electronic money

한 국희
대구과학대학 컴퓨터정보공학과

초록

최근 정보통신 기술의 발전과 인터넷의 활용은 기존의 화폐제도의 개념을 근본적으로 바꿔놓고 있다. 이른바 전자지갑, 전자화폐 등 다양한 이름으로 불리는 전자지불 수단의 등장이 바로 그 형태이다. 전자화폐는 정보보안, 전자인증, 암호화 등과 함께 전자상거래의 성공적인 확산에 있어서 가장 핵심적인 하부 구조 중의 하나이다. 현재 전자화폐시장은 기술표준, 카드 단말기 호환, 위·변조에 대한 안정성 확보, 법·제도적 장치 등 해결해야 할 문제가 산적해 있다. 본 연구에서는 전자화폐의 기술적 요구사항과 표준화 동향에 대하여 분석한 후 상용화된 전자화폐 기술이 가진 기술상 문제점 및 해결방안을 제시한다.

I. 서 론

교환의 매개체로 출발한 화폐는 처음에는 조개와 같은 물품으로 그 가치를 대용하는 물품화폐로부터 출발하여 금, 은, 동 등의 금속화폐로 대체되기까지 그리고 금속화폐에서 지폐로 바뀌기까지 인류는 거래와 가치 저장수단으로서 더욱 편리한 화폐사용을 위하여 노력하여 왔다.

현재 사용중인 지폐가 정보통신 기술과 컴퓨터 기술이 급속하게 발전하는 오늘날의 사회구조나 경제구조에 비하여 볼 때 여러 모로 적합하지 않은 점이 많고, 인간의 끝없는 편의성의 추구, 경제규모의 증가, 제도의 변화 그리고 현금이나 지폐발행의 폐단(화폐 발행, 관리의 고비용, 휴대의 불편성,…)등 여러 복합적이 원인들이 기존 화폐를 대체할 수 있는 새로운 형태의 전자화폐를 개발하게 되었으며, 급속한 정보통신기술의 발달로 등장한 전자상거래는 기존의 화폐나 지급결제 수단의 불편한 점을 개선한 새로운 전자적 방식에 의한 지급수단의 수요를 발생시켰고, 이에 따라 전자화폐의 개념이 등장하는 계기를 마련하였다.

전자화폐는 정보보안, 전자인증, 암호화 등과 함께 전자상거래를 위한 요소기술 중 하나이며, 실제 상거래에서 지급수단으로 이용되는 주화나 지폐와 동일한 가치를 갖는 디지털 형태의 정보로, 은행 등 발행자가 IC칩이 내장된 카드나 공중정보통신망과 연결된 PC등에 일정 화폐가치를 저장하고 이의 지급을 보장함으로써 on-line,

off-line상에서 자금결제가 이루어지도록 하는 화폐를 말한다.

현재, 전세계적인 인터넷 사용의 급증에 따라 이를 이용한 제품 홍보, 판매, 그리고 은행과의 거래 등이 빈번하게 이루어지고 있어, 이를 뒷받침할 수 있는 전자상거래 및 전자화폐 시스템들이 카드회사, 은행 및 서비스 사업자들을 중심으로 국가를 초월한 컨소시엄 형성 등의 방법으로 활발히 개발 및 상용화 되고 있는 실정이다.

또한 전자화폐시장은 기술표준, 카드단말기 호환, 위·변조에 대한 안정성 확보, 법·제도적 장치 등 해결해야 할 문제가 산적해 있다. 본 연구에서는 전자상거래 활성화 추세에 맞추어 그 중요성이 점차 부각되고 있는 전자화폐의 기술적 요구사항과 표준화 동향에 대하여 분석한 후 상용화된 전자화폐 기술이 가진 기술상 문제점 및 해결방안을 제시한다.

Ⅱ. 전자화폐의 기술적 요구사항

전자화폐는 일반적으로 물리적 화폐와 비슷한 기능을 가지도록 설계하는 것이 기본원칙이다. 그러나 완벽하게 물리적 화폐와 같은 기능을 갖는 전자화폐 기술을 구현하기는 매우 어려운 일이다. 그것은 물리적 화폐의 다양한 기능성을 전자화폐에 적용하기 위한 수학적 방식의 수용이 기술적으로 어렵기 때문이다. 그럼에도 불구하고 전자화폐가 필요한 것은 물리적 화폐가 다음과 같은 문제점을 가지고 있기 때문이다.

① 물리적 화폐의 제작, 유통, 관리 및 폐기에 따른 인력과 비용 소요

② 컬러 복사기 및 프린터의 발달로 위조 화폐 제작 용이

③ 급속한 컴퓨터 네트워크의 발달에 따른 전자상거래 시대에 온라인 결제 수단으로서 사용

결국 위와 같은 이유로 전자화폐가 물리적 화폐의 특성을 완벽하게 제공하지 못함에도 불구하고 개발되고 있는 것이다. 전자화폐의 기술적 요구사항은 다음과 같다.

1. 안전성(security): 전자화폐의 안전성 정의는 여러 학자들에 의해 크게 두 가지로 대별되며, 본 논문에서는 다음과 같은 두 가지 관점으로 분류한다.

(1) 물리적 안전성(physical security): 물리적 안전성이란 전자화폐 자체에 대한 위조의 어려움을 의미하는 것으로서, 전자화폐가 쉽게 위조될 수 없어야 한다는 것을 의미한다. 일반적으로 전자화폐는 스마트카드라는 물리적 보안장치에 저장되는 것을 원칙으로 하기 때문에 결국 물리적 안전성이라는 것은 스마트 카드의 안전성으로 귀결된다.

(2) 논리적 안전성(logical security): 논리적 안전성이란 전자화폐 자체에 대한 위조 여부를 의미하는 것이 아니라 전자화폐 시스템의 각 구성원은 나머지 다른 구성원들의 공모 공격(collusion attack)에 대해 안전해야 함을 의미하는 것이다.

즉, 전자화폐의 안전성은 일반적으로 논리적 안전성을 의미하는 것으로 해석할 수 있을 것이다. 물리적 안전성이라는 것은 전자화폐의 안전성이라고 하기보다는 IC 카드 자체의 안전성을 의미하기 때문이다. 본 논문에서는 전자화폐의 안전성 요구사항을 논리적 안전성으로 간주한다.

2. 이중사용(double-spending) 방지: 전자화폐는 그 자체가 가치 있는 디지털 정보이다. 디지털 정보는 종이 문서와는 달리 복사본의 생성이 용이하기 때문에 원본 및 사본의 구별이 불가능하게 된다. 결국 이중사용의 의미는 악의(惡意)의 사용자가 전자화폐를 불법 복제하여 반복적으로 사용하는 것을 의미하는 것이며, 이것은 전자화폐 설계 시 가장 중요하게 고려해야 될 부분이다. 이중사용 문제에 대한 해결방법으로는 다음과 같은 두 가지 방법이 존재한다.

(1) 사후검출(after the fact): 사후검출이란 사용자가 전자화폐를 발급 받을 때 금융기관이 전자화폐 내에 사용자의 ID 정보를 입력한 후, 사용자가 전자화폐를 이중사용하는 경우, 사후에 금융기관은 이것을 감지하여 전자화폐 내에 삽입되어 있는 사용자의 ID를 추출하여 이중사용자를 추적하는 방법을 의미한다. 은행은 정당한 사용자(전자화폐를 단지 한 번만 사용한 자)의 전자화폐로부터는 사용자 ID를 추출할 수 없게 된다. 사후검출 방식은 많은 오버헤드를 가지게 된다. 이중사용자를 사후에 검출해야 하기 때문에 기존에 사용된 전자화폐에 대한 데이터베이스를 유지시켜야 하며, 또한 범죄가 발생한 이후에만 해결 가능한 방식이 되기 때문에 이중사용 행위를 사전에 막을 수 없다는 문제가 있다.

(2) 사전검출(before the fact): Chaum 등이 처음으로 사전검출 방법을 제안하였다. 사전검출의 기본 개념은 스마트 카드를 이용하여 사용자가 전자화폐를 이중사용하는 경우, 같은 정보가 반복적으로 이용되는 것을 감지함과 동시에 작동을 중지시키는 방법을 취하는 것이다. 이것은 사후검출 방식의 문제점을 해결함과 동시에 전자화폐 시스템의 실질적인 구현에 발판을 마련하는 계기가 되었다. 현재 온라인 방식의 전자화폐는 기본적으로 사전검출이 적용된다. 즉, 예치 단계에서 은행이 개입하게 되어 판매자가 전자화폐를 은행에 예치하는 경우, 은행은 기존에 사용된 전자화폐의 저장 정보와의 동일 여부를 비교하여 이중사용을 사전에 검출할 수 있는 것이다. 그러므로 온라인 전자화폐는 전자화폐의 이중사용 문제를 해결하였다고 볼 수 있다.

3. 프라이버시(privacy) 보장: 전자화폐 기술과 지불 브로커 기술간의 차이는 사용자 프라이버시의 보장이다. 즉, 전자화폐는 실제 현금과 같이 사용자의 거래 내역이 추적되지 않는다. 이러한 사용자 거래의 불추적성을 일반적으로 사용자의 프라이버시라고 하며 사용자 프라이버시의 보장은 전자화폐의 가장 큰 장점이 되며, 프라이버시 보장 수준에 따라 다음과 같이 두 가지로 나뉜다.

(1) 불추적성(untraceability): 은행과 판매자가 어떠한 공모를 행하더라도 전자화폐를 지불한 사용자의 지불정보와 인출정보는 서로 연결될 수 없는 것을 의미한다. 즉, 은행은 판매자와 공모하더라도 사용자의 지불 내역을 추적할 수 없게 된다.

(2) 불연계성(unlinkability): 은행과 판매자가 공모하는 경우 은행은 비록 사용자의 거래내역을 추적할 수는 없지만 두 가지의 지불이 같은 사용자에 의한 것임을 알 수 있는 경우가 있는데, 이러한 경우 연계성(linkability)이 있다고 본다. 이러한 연계성

이 전자화폐에 존재할 경우 궁극적으로는 사용자의 불추적성이 보장되지 않을 수도 있게 된다. 그러므로 전자화폐가 완벽하게 사용자의 프라이버시를 보장하기 위해서는 불연계성이 보장되어야만 한다.

보통 전자화폐의 프라이버시라고 언급되는 것은 대부분이 ②의 불연계성을 의미하는 것이다.

4. 오프라인(off-line)성 : 전자화폐는 온라인 방식과 오프라인 방식으로 대별될 수 있다. 온라인 전자화폐는 사용자와 판매자의 거래 시 은행의 개입이 필요한 시스템으로 사용자가 판매자에 전자화폐를 지불하는 경우 네트워크 상으로 은행의 개입이 있어야 한다는 것이다. 반대로 오프라인 전자화폐는 사용자와 판매자의 거래 시 은행의 개입이 필요치 않은 것이다. 일반적으로 전자화폐는 오프라인 방식을 채택하고 있는데, 이것은 물리적 화폐의 기본 성질에 따른 것이며 컴퓨터 네트워크를 통해서 뿐만 아니라 일반 상점의 오프라인 단말기를 통해서도 거래를 보장하는 장점이 있기 때문이다. 다음 <표 1>은 온라인 방식과 오프라인 방식을 비교 설명한 것이다[9].

5. 전자수표(electronic check): 최초의 오프라인 전자화폐는 잔액 처리 문제를 해결코자 전자수표라는 방식을 제안하였다. 이것은 사용자가 전자화폐를 발급 받는 경우, 금액이 큰 전자화폐를 발급 받은 후 사용할 때에는 자신이 지불할 금액만큼 만을 지불할 수 있는 형태이다. 이것은 잔액 처리의 문제를 해결해 줄 수 있으며, 더불어 상점에서 잔액을 위한 전자화폐를 별도로 마련치 않아도 된다는 장점이 있다. 그러나 인출·지불·예치 프로토콜 외에 또 다른 프로토콜을 필요로 하게 된다는 단점이 있다. 즉, 사용자는 발급 받은 전자수표를 사용한 후 발급 금액에서 지불 금액을 뺀 나

<표 1> 온라인 방식과 오프라인 방식의 전자화폐 비교

구 분	온라인(on-line)방식	오프라인(off-line)방식
방 식	전자화폐의 지불단계와 결제단계가 동시에 수행(지불 프로토콜과 예치 프로토콜이 실시간으로 수행)	수신된 전자화폐를 일괄 처리하여 은행에 결제를 요구하는 방식(지불 프로토콜 이후 예치 프로토콜 수행)
장 점	지불단계와 결제 단계가 거의 동시에 이루어지므로 이중사용을 지불단계 전에서 사전방지 가능(사전검출)	통신량 분산과 더불어 네트워크 인프라가 구축되지 않아도 사용가능
단 점	통신량 집중화 현상과 통신량 증가에 따른 오버헤드 증가	이중 사용이 이루어지고 난 이후 은행에서 이중 사용자에 대한 신분 검출이 가능하므로 이중 사용의 범죄 발생 가능
적용 분 야	고액거래로 높은 안정성을 요구하면서 운용비에 대한 부담이 크게 작용하지 않는 현금 시장에 적합	많은 양의 소액거래가 이루어지는 곳으로 이중사용으로 인한 부정 사용금액이 소규모인 거래에 적합
발달 국 가	미국(통신망의 발달)	유럽(스마트 카드의 발달)

머지 금액을 은행으로부터 상환 받기 위해서 상환 프로토콜(refund protocol)을 수행해야만 한다.

6. 분할성(divisibility): 분할성은 전자수표와 비슷한 개념으로서, 사용자가 전자화폐를 발급 받는 경우 발급 받은 전자화폐를 사용자 마음대로 나누어 사용할 수 있는 성질이다. 즉, 인출 받을 당시의 금액을 기준으로 사용한 총액이 지정된 금액을 넘지 않을 때까지 사용자가 나누어 사용할 수 있음을 말하는 것이다. 이것은 전자수표와는 달리 한 번 발급 받은 전자화폐를 여러 번 나누어 사용할 수 있으며, 또한 전자수표가 가지고 있던 상환 프로토콜(refund protocol)이 필요 없다는 장점을 갖는다. 그러나, 이것은 완벽한 프라이버시 보장을 할 수 없다는 단점을 가지게 된다. 즉, 불추적성은 만족하나, 불연계성은 만족되지 않는다는 것이며, 결국 분할성은 완벽한 프라이버시가 보장되지 않는다는 문제점을 가지고 있다.

7. n회 사용가능성(n-spendability): 이것은 분할성의 개념과 비슷하지만 본질적으로는 큰 차이가 있다. 분할성은 사용자가 발행 받은 전자화폐 금액 내에서 사용자가 지불하기 원하는 금액만큼 사용금액에 맞추어 지불할 수 있는 기능이다. 반면에 n회 사용가능성은 금액을 나누어 사용한다는 개념보다는 지하철 정기권과 같이 동일한 금액을 횟수 기준으로 n번 까지 사용한다는 개념이다. 즉, n회 사용가능성은 어느 일정한 금액을 일정 횟수만큼만 사용 가능케 하는 것이다. 그러나, 이 기능도 분할성과 같이 불연계성을 만족시키지 못한다는 문제점이 생긴다.

8. 양도성(transferability): 실제 화폐의 성질들 중 가장 특기할 만한 것은 쉽게 양도 가능하다는 것이다. 즉, 발행기관으로부터 만들어진 화폐는 그것의 수명이 다할 때 까지 계속해서 사회에 유통된다. 그러나, 기본적인 요구 사항만을 만족하는 전자화폐는 그러한 양도 기능이 없으며, 이것은 전자화폐가 실제 화폐를 대치하지 못하고 있는 이유중의 하나가 된다. 이러한 문제점을 해결하고자, T. Okamoto 등은 양도성 기능을 갖는 전자화폐 시스템을 제안하였다[7]. 그러나, 양도성 성질에는 두 가지 문제점이 존재하게 된다. 첫번째는 사용자의 프라이버시가 보장되기 어렵다는 것이다. 즉, 양도 가능한 전자화폐가 이중 사용되었다고 가정할 경우, 은행은 이중사용자를 추적하기 위해서는 반드시 중간 양도자들에 대한 조사를 해야만 한다. 이 과정에서 부득이하게 이중사용된 양도 가능한 전자화폐의 사용자들은 그들의 신분을 노출시킬 수밖에 없는 것이다. 두 번째 문제는 양도 가능한 전자화폐는 양도횟수가 증가할 수록 양도 내역에 대한 정보 크기가 증가한다는 것이다.

9. 확장성(Scalability) : 전자화폐 시스템은 가입자(고객, 상인, 은행)가 증가하더라도 성능에 크게 영향을 받지 않도록 설계되어야 한다. 아직 전자화폐 시스템이 시험 단계에 있으며 특히 인터넷 사용자들의 증가 추세를 감안할 때 초기 가동 후 사용자 수가 급격히 늘어날 것으로 예상되므로 전자지불 시스템의 하부 구조는 확장에 따른 성능저하를 최소화하도록 설계하는 것이 바람직하다.

10. 상호 연동성/교환 가능성 (Interoperability/Exchangeability) : 하나의 전자화폐 시스템만이 전 세계적으로 통용되는 것은 불가능하며 또한 거래의 종류에 따라 보다 적합한 지불방식을 택할 수 있으므로 다수의 전자지불 시스템이 공존할 때 상호 연동성을 고려할 필요가 있다. 가능한 한 많은 화폐 단위를 지원해 주는 것이 바람직하며 다양한 형태의 전자화폐들을 서로 변환해 주는 메카니즘을 갖추는 것도 한 방법이 될 것이다.

11. 효율성(Efficiency) : 전자화폐 시스템은 거래당 그 시스템을 이용하는데 드는 비용이 거래액에 비해 충분히 작아야 한다. 이는 보안성이나 신뢰성 등과 비용 사이에 타협이 존재할 수 있으며 또한 하나의 지불 메카니즘이 모든 종류의 거래에 사용될 가능성은 희박함을 의미한다.

Ⅲ. 표준화 동향

1. SET(Secure Electronic Transaction)

SET은 인터넷과 같은 오픈 네트워크상에서 신용카드 거래를 안전하게 하기 위한 기술사양을 말한다. SET은 보안상의 허점을 보완하고자 신용카드 회사인 비자, 마스터카드와 IBM, 넷스케이프, 마이크로소프트 그리고 VeriSign의 기술적인 도움으로 1996년 1월 개발된 산업 표준 프로토콜로 주요 기술 제공업자에 의해 수용되고 있다. SET은 RSA 데이터 보안회사의 암호화 기술에 기초를 두고 있으며, 기술사양 자체가 공개이므로 누구나 자유롭게 SET 프로토콜을 사용하는 소프트웨어를 개발할 수 있다.

개발된 현재 SET은 제조업체 독자적인 또는 사설 솔루션을 구축하는 것보다 저렴하게 패키지 솔루션을 개발하려는 제공업자가 이용하고 있다. SET은 고객으로부터 상인과 은행으로 인터넷 상에서의 지불거래를 지원한다. SET은 설계상 이들 주체간의 전통적인 관계를 유지하고 있으며, 어떤 새로운 주체의 참여도 있을 필요가 없다. 부가적인 특징, 기능, 소프트웨어 및 하드웨어가 요구된다고 해도, 기존 시스템과 인프라는 계속 이용된다. <그림 1>에 SET에 의한 지불처리 과정을 나타낸다.

1997년 12월 19일 SETCo(SET Secure Electronic Transaction LLC)가 설립되어 SET 1.0의 실행과 광범위한 전개를 관리/촉진하는 역할을 담당하고 있다. 1999년 5월 SETCo는 SET 1.0에 다음과 같은 내용을 확장할 계획임을 발표하였다[3].

(1) SSL에서 SET으로의 이전: SSL, 우편 또는 팩스를 통해 고객으로부터 거래를 받는 지에 상관없이, 상인들이 자신의 금융기관으로부터 SET 인증을 이용할 수 있도록 함.

(2) 스마트카드 확장: 칩-기반 거래를 SET을 통해 할 수 있도록 함.

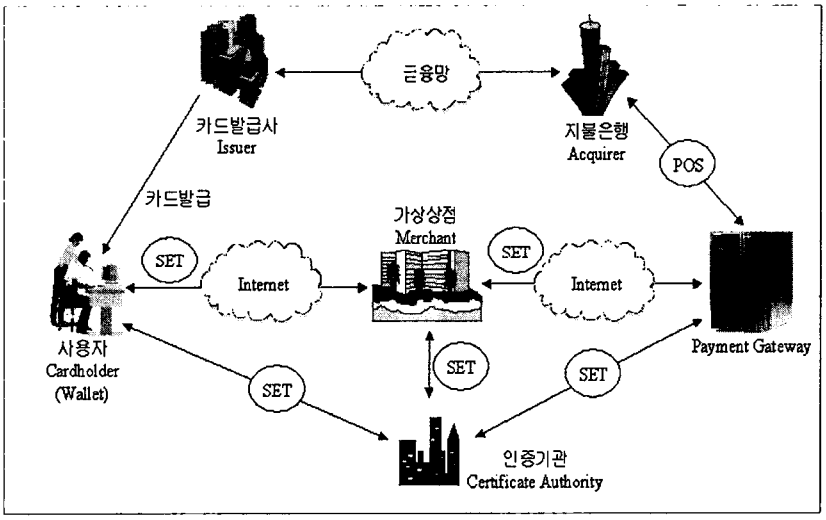
(3) PIN 확장: 직불카드 거래를 촉진하기 위함.

(4) 주요 상인 은행의 표준 프로파일: SET 머천트 소프트웨어와 금융 게이트웨이의 도입을 단순화 시킴.

한편, SET 2.0에 다음과 같은 사항들이 제안되어 있다.

(1) 칩 카드(EMV, 다중 어플리케이션, non-EMV)와 직불 PIN을 포함하기 위한 기능적인 향상

<그림 1> SET에 의한 지불처리 과정



(2) 알고리즘 독립성과 하드웨어 제조업체 지원을 포함하기 위한 암호화 대안

(3) 적은 크기와 HTML에서 포맷팅 된 등록양식을 가진 보증서를 포함하기 위한 보증 향상

(4) 단일 주문, 주문 취소, 주문을 위한 재협상, 전자배달을 위한 배달 영수증에 대한 다중 지불 안내를 포함하기 위한 주문 향상

(5) 지불 협상, 자금 이체, 구매카드 지원 및 여행 에이전트 비즈니스 모형을 포함하기 위한 지불 향상

(6) 어플리케이션에 대한 향상된 오류 메시지 및 감소된 처리부담을 포함하기 위한 거래처리 향상

2. CEPS(Common Electronics Purse Specification)

CEPS 란 Visa 를 비롯하여 전세계의 주요 전자화폐 업체들이 서로간의 호환성이 가능케 하기 위하여 개발된 저자화폐 국제 규격으로 현재, 전세계에 발급된 모든 전자화폐 카드중, 90%이상을 차지하는 전자화폐 업체들이 CEPS채택을 공식 발표했으며 2년 내에 유럽지역을 시점으로 하여 CEPS 사용지역을 아태지역 및 남-북미 지역으로 확산시킬 예정이다.

1999년 3월 마련된 CEPS는 전자지갑 프로그램에 대한 상호 운용성을 성취하기 위한 중요한 시도 중 하나로, 이런 전자지갑 프로그램을 도입하려고 하는 특정 조직에 필요한 모든 컴포넌트의 요구사항을 규정하고 있다.

CEPS는 다음에 기술할 스마트카드를 위한 EMV 규격과 호환되어야 하며, 상호 운용 가능한 카드 어플리케이션, 카드-대-단말 인터페이스, POS(point-of-sale) 및 로드 거래를 위한 단말 어플리케이션, 데이터 구성요소, 그리고 거래처리를 위한 권고된 메시지 포맷을 정의해야 한다. 또한, CEPS는 전자지갑 구성 참여자를 위한 기능적

요구사항을 제공하고, 진보된 보안을 위한 공개 키 암호화를 이용한다.

2000년 8월 현재 전세계 전자지갑 카드의 90% 이상에 해당하는 30여 국가의 기관들이 CEPS 도입에 합의하고 있으며, 200여 기관들이 CEPS에 대한 면허협정에 서명하고 규정을 받아들이고 있다. 즉, 약 6,000만 GeldKarte, 3,000만 Proton-기반 카드, 그리고 약 1,000만 Visa Cash 카드를 포함해 전세계 전자지갑 카드의 90% 이상이 상호 운용될 것이다. 또한, 약 50개 기술업체가 CEPS-호환 제품을 개발하기로 합의한 바 있다.

한편, 1999년 10월 CEPSCO Espanola A.I.E., EURO Kartensysteme, Europay International, VISA International에 의해 CEPSCO, LLC가 공식 설립되었으며, 2000년 7월 Groupement des Cartes Bancaires와 Proton World가 동참하였다[15]. CEPSCO, LLC의 기본적 역할과 책임은 다음과 같다:

(1) CEPS의 지속적 개발과 유지/전개 지원

(2) 전자지갑 사업자, 업체 등의 CEPS 채용을 촉진하기 위한 CEPS와 관련 기술의 확장, 촉진, 관리

(3) 산업계로부터 수집된 CEPS에 관한 주요 사항과 제안을 위한 포럼 역할

(4) 모든 호환 체계를 위한 독특한 보증 승인(certification approval) 절차 규정

(5) 현 CEPS의 발전을 위해 서비스와 기술 차원에서 시장 진화를 평가

CEPS는 세 가지 종류의 규격을 발표하고 있는데, 기술 규격은 버전 2.2(2000년 5월), 기능 규격은 버전 6.3(1999년 9월), 그리고 비즈니스 규격은 버전 7.0(2000년 3월)이 각각 발표되었다[15].

3. ECML(Electronic Commerce Modeling Language)

ECML은 그동안 EC지불결제 프로토콜로 양분화됐던 「SET(Secure Electronic Transaction)」과 「SSL(Secure Socket Layer)」을 모두 지원하는 점이 특징이다. 최근까지, 고객들은 전자지갑과의 통신용 소프트웨어를 가진 특정 상인 사이트에 있는 특정 전자지갑을 이용할 수 밖에 없었다. 전자지갑 제조업체들은 다양한 기술을 개발해 왔으며 다양한 독자적 프로토콜을 만들어 내었다.

좀더 새로운 전자지갑은 미지의 지불 형태에 대한 구조를 읽을 수 있어야 하며 공통적인 표준이 필요하다. ECML은 America Online, American Express, Brodia, Compaq, CyberCash, Discover, FSTC, IBM, MasterCard, Microsoft, Novell, SETCo, Sun Microsystems, Trintech 및 Visa U.S.A. 등이 공동 개발하였다.

1999년 6월 발표된 ECML 버전 1.0은 고객-대-상인 구매를 설명하고 있으며, 호환되는 전자지갑 제품이 제공하는 웹 양식의 완성을 용이하게 하도록 설계되어 있다. 또한, ECML은 보안 프로토콜-독립적이고, 폭 넓은 전개와 어떤 지불도구도 지원하도록 설계되어 있다. 그리고 상인들이 그들의 웹 주문/지불 양식 상의 정보 영역을 위해 이용하는 획일적인 내부 영역 이름 셋을 정의한다. ECML 영역 유형은 배송 정보, 요금 정보, 지불카드 정보, 영수증 정보 및 관리 영역을 포함하고 있다. 이것은 고객이 보는 영역에 영향을 미치지 않는, 단지 내

부적인 영역 이름일 뿐이다. ECML-호환 상인 사이트와 만난 하나의 전자지갑은 양식 요소를 학습하지 않고 양식을 자동 상주시킬 수 있을 것이다.

ECML을 지원하기 위해 상인은 획일적인 영역 이름과 웹사이트의 체크아웃 페이지를 통합하기 위한 변화와 CGI/ASP 스크립트로의 변화를 필요로 한다.

다음에 발표될 ECML 버전 1.1은 다음을 지원할 예정이다.

(1) 기업 구매 카드의 이용
(2) 비카드 지불 메커니즘의 이용
(3) 사생활-관련 문제
(4) 상인이 의무적으로 정할 영역의 완성
(5) XML 바인딩
(6) 새로운 지불 유형
(7) 국제화
(8) IETF로의 이전(2000년 12월 목표)

현재 Costco, Crutchfield, EBWorld.com, Genuine ClipArt, Herrington & Company, IBM, Toy Shoppe 등의 온라인 상인들이 ECML 표준을 도입하고 있으며, Brodia, CyberCash, IBM, Microsoft, Trintech 등의 주요 디지털 전자지갑 제조업체들이 ECML 표준을 채택하고 있다.

4. EMV

1994년부터 Europay, MasterCard, Visa 사의 컨소시엄인 EMV가 자기카드(Magnetic Stripe card)의 취약한 보안성을 극복하고, 다양한 금융 서비스를 제공하기 위한 일환으로 신용/직불 카드 서비스를 위해 기존 자기카드의 스마트 카드화를 추진하게 되었다.

이를 위해서 3사는 전세계 공통으로 사용할 수 있는 EMV 2.0규격을 '95년 6월에 발표하였으며, 다음해(1996년) 6월 개정본 EMV 3.0규격을 발표하였다. EMV규격에서는 "smart card"용어 대신 IC카드 용어를 사용하고 있으며, 신용/직불 카드 서비스 제공을 위한 IC카드에 대한 규격사항을 기술하고 있다.

현재 이 규격에 준하여 대부분의 스마트 카드형 신용/직불카드가 발행되어 시험 서비스 상태이고 국내 한국형 전자화폐에도 많은 부분이 가미된 규격이다.

1999년 2월에는 Europay, MasterCard 및 VISA가 EMV ICC 규격을 관리, 유지 및 향상을 목적으로 EMVCo, LLC를 설립하고 1998년 5월에 발간한 EMV ' 96 version 3.1.1을 수정한 EMV 2000 규격(version 4.0) 초안을 2000년 4월에 발표하였다[16].

Ⅳ. 상용 전자화폐

1. 전자화폐의 기술적 분류

전자화폐는 화폐의 고유 기능을 제공하는 방법과 용도 등에 따라 여러 가지로 분류될 수 있다. 일반적으로 범용의 전자결제 시스템은 실용 가능성과 방법 등의 분류 기준에 따라 ① 신용카드 결제의 발전형 방식, ② PC 뱅킹 방식, ③ IC 카드형 전자지갑 방식, ④ 전자화폐 방식 등과 같이 4가지로 구분된다[9]. 전자화폐의 경우, 위의 전자결제 방식의 분류에 대하여 온라인 및 오프라인 방식으로 세별되며 ③의 IC 카드형 전자지갑 방식과 ④의 전자화폐 방식은 온라인 및 오프라인 기술 모두 적용 가능하다.

2. 상용 전자화폐(Commercial Electronic Cash) 시스템

전자화폐 시스템의 목적은 선불카드/직불카드를 응용하거나 순수한 전자화폐를 응용하기 위한 시스템이다. 전자화폐 시스템을 구축할 수 있는 기술적인 요구조건의 해결은 진전됐지만, 현재 금융과 사회적 관습 그리고 통화량과 경제에 미치는 영향 등 사회·경제적인 관점에서는 미흡한 부분이 있으나 이 부분이 기술적인 대안과 합하여 현실적인 방안을 제시하는 것이 필요하다.

전자 수표나 신용카드 등의 전자결제 시스템이 실세계의 화폐에 그 기반을 두고 있는 것에 반해 전자화폐 시스템은 완전히 새로운 화폐의 발행을 목표로 한다. 실세계의 화폐와 사용방법을 동일하게 하기 위해 전자화폐가 갖추어야 할 특성은 익명성, 휴대가능성, 양방향성 등이 있을 수 있다. 즉, 전자화폐가 실세계의 현 규모와 같이 소액의 거래, 개인의 물품 구입이나 서비스에 적합한데 반해, 물건의 구입 또는 서비스를 받을 때마다 그 정보가 어딘가에 저장된다면 개인의 사생활이 침해될 수 있으며, 또한 이 정보가 악용될 수 있음을 의미한다. 이를 막기 위해서는 전자화폐의 익명성이 요구된다. 전자화폐 시스템은 사용자의 익명성 보장 문제와 함께 전자화폐의 중복사용 문제, 즉 전자화폐의 불법적인 복사 문제 등을 해결해야 할 것이다. 다음은 세계적으로 인지도가 높은 상용화된 전자화폐와 국내 현황을 기술체계를 중심으로 소개한다.

(1) eCash

eCash는 네트워크상에 생성되는 가상 코인으로 DigiCash사가 개발하여 서비스하는 전자결제 시스템이다. DigiCash사는 네델란드에 본사가 있으며, 컴퓨터 암호기술에 관한 수많은 특허를 가지고 있다. eCash는 네트워크 상에서 지불행위를 하기 위한 전자화폐 개념으로서 소비자는 미리 은행구좌를 개설하여 자금을 입금해 두고, 전자메일과 전화 또는 편지 등으로 '민트(Mint, 전자통화조폐국)'에 이체한다. 전자 통화를 이용할 때에는 민트에게 이용자 PC로 전자통화의 발행을 요구한다. 민트에서는 요구액에 상당하는 금액을 이용자 민트 잔고에서 끌어내어 이용자가 전자 통화를 이용할 수 있는 상태로 만든다. 이용자는 이 전자통화를 이용하여 네트워크 상에서 지불을 하게 된다. 판매자는 받은 전자 통화를 민트에 송신하여 정당성을 체크한다. DigiCash에서는 민트라는 인증기능을 경유함으로써 전자 통화의 정당성을 확보하고 있다. 이 기술은 중앙 집중적인 계좌 관리 때문에 거래의 많은 처리비용, 사용자 수의 제한 등의 단점이 있다.

(2) NetCash

캘리포니아 대학에서 개발한 넷캐시(NetCash)는 복수의 서버(서버)를 도입하는 분산 시스템으로, DigiCash가 갖고 있는 중앙 집중적인 계좌 관리의 단점을 해결하려 하고 있다. 넷캐시는 DigiCash보다는 약한 익명성을 지원하고 있다. 그리고 사용자의 계좌를 분산된 여러 대의 서버에서 관리하며 사용자의 수를 극대화하는 데

에 역점을 두고 있다. 또한, 넷체크(NetCheque)라는 전자 수표 시스템과 교환이 가능하도록 배려하고 있다.

1995년 제 4회 WWW 학회에서 Steve Glassman이 밀리센트 프로토콜(Milicent Protocol)이라는 아주 적은 액수의 지불에 사용하는 전자 지불 프로토콜을 제시했다[17]. 기본적으로 고객(customer)과 판매자(merchant)가 있으면 이 사이에 scrip이라고 부르는 전자화폐를 주고 받는데 이 서비스를 브로커(broker)라는 서버가 중간에서 중개한다는 기본적인 구조를 가지고 있다. 공개키 암호화 방식과 메시지 다이제스트 암호화를 혼용하여 정보보호를 제공하고 있는데, Glassman은 악의의 사용자가 scrip의 보안을 깨뜨리는데 드는 비용이 scrip의 지불 액수보다 커지도록 하면, 특별히 보안을 강화하지 않아도 적은 액수의 지불이 가능하다는 점에 착안하고 있다.

(3) MONDEX

MONDEX는 Tamp와 resistant 특성을 갖는 IC카드 상에 현금가치를 이전하는 선불형 전자지갑으로서 영국의 내셔널 웨스트민스트 은행에서 고안된 전자결제 시스템이다[18]. MONDEX는 은행구좌에서 IC카드로 화폐가치를 옮겨 사용하는 방식으로 3.5초 정도면 현금처럼 결제할 수 있다. 특히, 크레디트 카드와 같이 거스름돈을 주고받는 번잡함이 없다. MONDEX의 실용화 실험은 웨스트민스트 은행과 미드랜드 은행이 공동출자로 세계 최초의 전자화폐 운영회사인 "MONDEX UK"를 설립, 인구 19만 명의 영국 스윈던(Swindon) 지역에서 실용실험에 들어간 것이 최초이다. 영국 통신회사 BT가 개발한 공중전화를 사용하여, 사용자는 은행창구에 가지 않고도 돈을 MONDEX카드로 옮길 수 있게 되어 있다. BT는 가정용 전화기에도 동일한 기능을 제공하는 장치를 개발하였다.

이와 함께 현재는 인터넷을 매개로 화폐가치를 주고받는 메카니즘 개발에 주력하고 있으며,일부는 좋은 결과를 도출하고 있다. 평상시에는 외부에서 쇼핑대금 지불에 MONDEX카드를 사용하고, 집에서는 인터넷을 통하여 전자결제에 쓸 수 있도록 하자는 것이 MONDEX의 목표이다.

MONDEX 카드는 IC의 위치나 치수, 이용하는 전압 등이 ISO에 근거하고 있으며, 현재의 실용화 실험은 홍콩, 미국, 캐나다의 주요은행을 통해 실시되고 있기도 하다. 또한, PC에 접속되는 카드리더는 미국 웰스파고 은행과 공동 연구중이다. 참고로 MONDEX는 1996년경 마스터카드 인터내셔널에 합병되었으며, 마스터카드는 MONDEX를 통하여 전자화폐 시장을 개척하고 있다.

(4) Proton

Proton은 카드형 시스템으로서 선불(Prepaid) 체제이나 제 3자에게 가치이전을 할 수 없다는 점이 MONDEX와 다르다. 벨기에의 Proton은 1995년 2월부터 레우벤 등 2개 도시에서 시험을 개시했다. 이 카드는 소액결제 시장을 목표로 자동판매기 등에서 지불이 가능하도록 한 전자화폐 시스템이다. 시험서비스에 참가한 상점은 약 300개이고, 지불 단말 1,322대, 자동판매기 73대, 공중전화 50대 등이다. 그리고 소매점에서 취급대금의 0.7%, 자동판매기에서

2%를 수수료로 징수한다. 현재 Proton은 벨기에 국내에 3만매 이상의 카드를 발행하여 브뤼셀 등 대도시에서도 사용이 가능하다. 현재는 은행의 크레디트 카드와는 별도로 발행하고 있으나, 일체화 계획으로 본격적인 "전자지갑" 형태로 발전될 전망이다.

(5) K-Cash

정보화촉진기본법에 의거 금융정보화추진 은행소위원회에서 추진하고 있는 금융기관 공동의 전자화폐인 K-Cash는 2000년 7월 시범사업을 시작으로 2001년 1월부터는 본 사업이 실시중이다. K-Cash가 여타 전자화폐(몬덱스, V캐시, A캐시 등)와 차별화되는 특징 및 장점은 인프라, 보안성, 국익측면의 한국형 전자화폐이다[8].

먼저, 인프라 활용 측면에서 전 은행이 사업에 참여하고 은행권의 기 구축 인프라를 활용할 수 있다는 점이며, 구체적으로는 2001년 2월 현재 10개은행에서 카드를 발급하고 있고 지방은행으로 확산 중이며 은행 창구 및 CD/ATM을 통해 충전이 가능하고 또한 금융 결제원(중계센터)을 정산시스템으로 활용함으로써 별도 정산 시스템 구축이 불필요하다는 점이다.

다음으로, 보안성 확보 측면에서 보면 K캐시는 2000년 3월 국가정보원으로부터 보안성을 승인(보안알고리즘 및 키관리 체계) 받은 바 있다. 이것은 국가 중요 보안 시설의 관리 체계 및 기준을 충족하고 있다는 의미이다. 또한, 전국 호환성 측면에서는 단일 정산시스템 및 Key 관리(금융결제원) 체계에 따라 호환성이 기 확보된 상황이며, 대고객 접점이 광범위(전 은행 창구에서 K-CASH 발급, 은행 창구 및 CD/ATM에서 충전, 금년 상반기중 인터넷 뱅킹 및 인터넷상거래 사용 가능, 인터넷 충전, 지불 및 전자서명공인인증서 저장 등)하여 지자체 정보화사업 추진시 강점이 있다

또한, K-CASH는 국익 측면에서 볼때에도 국산 알고리즘 및 IC칩을 활용함으로써 대외 로열티 지급이 불필요 하며, 관련 국내 산업의 보호 육성에도 기여하고 있다.

채택하고 있는 칩운용시스템(COS)의 기능과 전자화폐규격(표준SPEC) 은 카드국제표준(ISO 7816, 14443 및 EMV ver 3.0)을 준수하여 제정되었고, COS는 K-COS(K-CASH COS)로서 일반적인 스마트카드의 기능과 은행공동시스템 (발급/매입)으로서의 구비사항, 신용·직불카드 규격(EMV ver 3.0) 수용 및 Application (응용영역) 확대 등을 반영하여 개발되었다.

한편, 전자화폐로서 K-CASH는 순수 국내용 화폐로서 국제호환은 불가능 하다

그러나 신용·직불카드 기능이 통합 구현된 다기능 카드로서의 K-CASH는 신용·직불기능을 제한없이 사용할 수 있다. 신용·직불카드 기능은 K-CASH(IC카드)의 Chip 내에 전자화폐와 신용카드 기능을 통합 구현하는 방식과 K-CASH 뒷면의 Magnetic Stripe에 신용기능을 첨가하는 두 방식을 모두 사용할 수 있다.

K캐시는 콤비카드로서 단일 Chip 내에 접촉/비접촉식 기능이 통합 구현되며, ISO 표준상의 B type 으로서 ISO 7816(접촉식) 및 14443(비접촉식)의 표준에 따라 설계 되었다.

On/Off-line 겸용카드로서 구매는 Off-line 방식을, 충전은 One-line 방식을 적용하게 되며, 다기능 카드로서 신용·직

불카드 기능을 수용할 수 있게 되어 있다.

위변조 및 부정이용방지를 위해 채택하고 있는 보안기술은 SEED를 사용하고 있다.

보안 알고리즘인 SEED는 국가정보원에서 개발된 16 Round DES로서 A-CASH 및 마이비카드의 3 Round DES 보다 고보안(高保安) 알고리즘이다.

현재까지의 운영실적(카드발급수, 가맹점수, 거래건수 및 금액, 이용자들의 평균저장금액 등)을 보면 먼저, 서울 역삼동 일대의 시범사업 기간(2000.7.26~2001.2.1) 중의 운영실적은 카드발급수가 3840매, 가맹점수가 600개, 거래건수가 26천건, 이용금액은 79백만원이다. 평균저장금액은 미파악 상태이다.

향후 사업계획은 지자체 정보화사업 추진에 있어 춘천시(2000. 9. 15 협약) 및 수원시 (2001. 1. 30 협약)의 Cyber City 구축 프로젝트를 완료하고, 전자화폐의 기능개선 측면에서 상반기중에 인터넷상거래/뱅킹/인증시스템과 PC 및 가맹점단말기 상에서의 충전시스템을 구축할 예정이다. 지자체 정보화사업 측면에서는 서울시, 인천광역시 및 경기도 군소지자체 정보화사업을 지속 추진할 계획이며, 적용영역 확대 측면에서는 2001년 상반기중 춘천시 교통시스템을, 하반기중 수도권 교통시스템을 구축하고 자판기, PC방, 복사기, 출입통제 및 톨게이트, 주차장 요금징수시스템 등으로 적용영역을 지속적으로 확대해 나갈 계획이다.

2001. 2. 1 현재 K-CASH 발급·매입업무 실시은행은 10개로서 기업, 주택, 신한, 한빛, 외환, 서울, 하나, 조흥, 제일, 농협 등이고, 여타 시중은행 및 지방은행은 현재

<표 2> IC 카드형 전자화폐(발급기관:금융권)

구 분	K-Cash	몬덱스	V-Cash
추진기관	금융결제원,한국은행	몬덱스코리아	비자코리아
참여업체(2000.12월기준)	21개은행, 7개 카드사	조폐공사,국민·조흥은행, 현대종합상사, 한통프리텔	삼성물산, SK, 롯데
전자화폐 발행 및 정산	회원사가 발행, 회원사간 정산 필요	Orginator가 발행, Orginator와 정산	회원사가 발행, 회원사간 정산 필요
보안체계	SEED	DES, RSA	DES, RSA
표준	국내금융기관	몬덱스	CEPS
운영체제	자체 COS	MULTOS	javacard
서비스 일정	역삼동, 춘천시에서 시험서비스 중	코엑스, 제주시에서 시범서비스	올 상반기로 예정
특징	개인간 가치이전 불능, 복수통화 사용 불능, 국내에서만 사용가능	개인간 가치이전 기능, 5개의 복수통화 사용가능·국제적 호환가능,	개인간 가치이전 기능, 복수통화 사용가능·국제적 호환가능,
기능	선불기능. 신용/직불기능 추가 가능	시용/직불/선불 기능	시용/직불/선불 기능
로열티 지급	없음	있음	있음

시스템 구축 중에 있다. 현재, K-CASH에 컨소시움 참가하거나 Solution을 개발·공급하고 있는 업체로는 COS 개발업체(삼성SDS, 현대ST, SCT), K-CASH 컨소시움 참여업체(지자체 정보화사업 관련), IC 카드 공급 및 COS 개발업체(삼성SDS), 지역커뮤니티시스템 구축 및 On-line VAN 업무(미래시티닷컴), 유통 단말기 설치·보급(On-line VAN 업무)업체인 씨씨케이밴회사, 교통단말기 및 여타 Solution 개발업체(뷰텍, SST회사 등) 등이 있다.

<표 2>는 국내 주요 전자화폐의 현황이다[10].

IV. 문제점 및 해결방안

1. 위조 방지 문제

전자화폐 시스템에서 오가는 정보는 위조가 불가능해야 하며, 어느 한 쪽이 거래 사실을 부인하거나 다른 쪽에 누명을 씌웠을 때 그 진위여부를 판별할 수 있어야 한다.

전자화폐는 위조를 막기 위해 고도의 암호기술이 적용되고 있지만 완전한 암호는 아직 존재하지 않는다. 암호해독에 뛰어난 컴퓨터 해커가 전자화폐를 위조할 염려는 없는지도 점검할 사항이다. 현재의 기술로는 전자화폐에 사용되고 있는 암호를 해독하는데 슈퍼컴퓨터를 계속 가동해도 수년에서 수 십년이나 걸린다고 하지만 점차 연산에 소요되는 비용이 감소하기 때문에 안전하다고는 말할 수 없다. 컴퓨터 처리성능은 더욱 진보하고 있고 전자결제 시스템에 관계하는 당사자 중에 범죄의 유혹에 넘어가지 않는다는 보장도 없다. 결국 이러한 역기능을 방지하는 기술과 그것을 해독하는 측의 기술은 악순환 관계 또는 모순관계를 유지하게 될 것이고 그 이상의 방지 기술을 안정적으로 운용하기 위한 사회제도(법, 제도와 조직이용형태 등)의 검토가 무엇보다 중요하다고 말할 수 있을 것이다. 또한 암호화된 신용카드 결제에 대해서도 극히 간단한 방법으로 해독될 가능성이 있는 것이 실증되고 있는 만큼 많은 연구가 필요하리라 본다.

2. 양도성으로 인한 국가 통화 관리 문제

금융행정 당국에 의한 현금 흐름의 제어가 곤란하게 될 수 있다. 이는 도중에서 새로운 신용창조가 되지 않는 한 문제는 없다, 그러나 현행 지폐와의 태환성을 보증하지 않고 전자화폐가 발행되면 재차 신용을 창조하게 되어 거시 경제에 혼란을 가져올 수 밖에 없다. 이러한 문제는 법, 제도나 운용규칙을 정해서 대처 해야겠다[7].

또한, 전자상거래가 본격화되는 시대에는 복잡한 결제, 거래는 자연스러운 현상이 될 것이므로 이를 위한 하부 기술의 연구개발과 함께 국가별로 관리하던 통화 관리 체계를 글로벌 개념으로 확대할 필요가 있다. 이를 위한 각국별 그리고 국제 통화 관리를 관장할 수 있는 국제 기구의 출현이 요구될 것으로 전망된다.

3. 경제 통제 불능 가속화의 문제

네트워크내의 전자화폐에 의해 상거래의 속도는 가속될 것이고 통화량이 늘어나는 것과 똑같은 효과를 겪게 될 것이다.

전자화폐의 유통이 확대될 경우 통화정책과 지하경제 등에 적지 않은 영향을 미칠 것으로 예상된다. 따라서 정책당국은 새로운 결제수단의 등장으로 초래될 부작용

을 최소화하는 데 각별히 유의해야 할 것이며, 지하경제의 확산을 억제하고 거래의 투명성을 제고하기 위해 전자화폐 1회 인출의 사용한도를 설정한다거나, 거액결제시 신고를 의무화하는 방법 등으로 제도를 보완해야겠다.

4. 익명성 확보로 인한 범죄 발생 가능성의 문제

누가 사용했는가를 추적할 수 없고 자금의 흐름을 또한 추적할 수 없는 전자화폐는 사용방법에 따라서는 교묘한 범죄를 조장하는 수단이 될 수도 있다. 마약판매 등 범죄 행위에 의해 얻은 자금을 복잡한 조작을 거쳐 깨끗한 돈으로 바꾸는 돈 세탁을 전자화폐 사용으로 간단히 할 수 있는 가능성이 있다. 국가가 전자화폐의 흐름을 파악할 수 없으면 탈세도 횡행할 두려움이 있다. 지금으로서는 eCash는 은행구좌를 경유하지 않으면 현금으로 바꿀 수 없지만 전자화폐의 유통이 본격화되고 비합법의 자금을 취급하는 Black Market이 성립하지 않는다는 보장은 없다. 이러한 신종 범죄 발생 가능성을 원천적으로 차단하기 위하여 기술적인 대안이 요구된다.

5. 운용비용과 피해비용 부담의 문제

전자화폐를 도입하기 위한 운용비용을 누가 부담할 것인가라는 문제도 발생한다.

또한, 오프라인은 물론 전자상거래에서도 많이 쓰이는 전자화폐는 소비자가 위·변조나 도용 등 금융사고를 막기에는 현실적으로 어려움이 있는데 이에 대한 보상책임 규정도 정해야겠다.

국내 전자지불시장 활성화의 가장 큰 걸림돌은 전통적인 지불 관련 법규가 새로운 시장환경에서도 그대로 적용되고 있다는 점이다. 온라인 전자화폐가 기존 오프라인 환경의 여신전문금융업법에 규정받고 있는 것이 대표적 사례다. 따라서, 전자상거래 시장이 조기 활성화하기 위해서는 각종 표준약관 및 법·제도의 정비가 시급히 요구된다.

V. 결 론

본논문에서는 전자상거래분야에서 지불수단으로 이용되고 있는 전자화폐의 기술적 요구사항과 표준화동향, 국내외의 상용화된 전자화폐와 전자화폐기술이 가진 기술상 문제점과 해결방안을 살펴보았다.

2004년는 전자화폐가 전체화폐의 20%를 차지해 4조3천억의 규모에 달할 전망이다. 최근 대한상공회의소가 발표한 '전자화폐시대 열린다' 라는 보고서에 따르면 서비스 시범중인 전자화폐가 본격적으로 통용될 경우 기존화폐를 대체할 액수는 2002년 1조9천억, 2004년 4조3천억원, 2008년에는 7조4천억언에 달할 것으로 예상됐다. 이에 따라 연간 발행되는 화폐 총액중 전자화폐가 차지하는 비율도 2002년 9.9 %에서 2004년 20% 2008년 28.9% 까지 높아질것으로 추산됐다.

전자화폐는 화폐 공급량과 통화속도를 높이고 중앙은행의 발권비용 감소와 정산의 효율성 제고에도 상당한 영향을 미칠 것으로 전망된다. 그러나, 전자화폐는 시장 유동성을 증가시켜 물가상승 및 인플레이션을 유발할 가능성도 있고, 새롭게 등장하는 전자지불 시스템이 기존의 시스템에서 드러나지 않은 문제점이나 한계점을 보일 경우를 대비하여 정부는 저작권, 특허권 및

상표보호를 위한 효과적인 법적 기준을 마련하고 업계는 암호화와 같은 기술적 보호 수단 개발에 주력해야 할 것이다.

따라서, 시장활성화에 앞서 기술표준화 및 위변조에 대한 안정성 확보, 법적 제도 마련이 시급하다. 즉, 금융기관의 공동 시스템 구축이 필요하며 국제적으로 호환가능해야 하고, 카드와 단말기의 호환성은 필수적이다. 그렇지 못할 경우 소비자들은 사용하는데 불편하고 시스템 업체간의 불필요한 중복투자나 시행착오로 어려움을 겪을 수 있다. 또한, 법·제도적 장치로 전자화폐의 기술력을 검증할 수 있는 객관적 기준이나 공인인증기관의 도입이 필요하다. 그리고, 보안성, 안정성 문제도 시급하다. 최근 전자화폐 표준화 포럼을 출범시킨 것은 전자화폐의 안정성확보와 다양한 전자화폐간 호환성 확보를 위한 표준화 마련을 위해 바람직하다.

참고문헌

1. 강 원진, 『전자결제시스템』, 삼영사, 2000.12.

2. 김 영진 역, 『전자화폐란 무엇인가』, 대광서림, 1997. 7.

3. 김 정환·이 윤철·이 동일, "최신 전자지불 기술 표준화 동향", 『주간기술동향』 982호, 2001. 1. 31.

4. 김 정환·이 윤철·이 동일, "전자지불 시스템 및 시장 동향", 『주간기술동향』 994호, 2001. 4. 24

5. 명 승욱, "전자화폐 금융사고 때 원칙적으로 발행업자 책임" , 전자신문, 2001. 4. 9.

6. 심 규호, "전자화폐 표준화 가속페달", 전자신문, 2001. 4. 19.

7. 이 만영·김 지홍·류 재철·송 유진·염 홍렬·이 임영, 『전자상거래 보안기술』, 생능출판사, 2001. 2.

8. 이 현제, "금융기관 공동의 전자화폐(K-Cash) 추진현황과 전망, "http://www.e-payworld.com/e-payzine/2001_Spring/e-pay-2001_spring_sub10.htm

9. 임 신영·이 관용·함 호상, "전자화폐 기술 동향", 『주간기술동향』,959호, 2000. 8. 16.

10. 조 지영, "전자화폐 시장 사공이 너무 많아.....", 『경영과 컴퓨터』, 2001. 1.

11. 주 재훈, "전자화폐와 패러다임의 변화",
http://wwwk.dongguk.ac.kr/~givej/dm.html

12. 주 재훈, "전자화폐",
http://wwwk.dongguk.ac.kr/~givej/Ecash.htm

13. 최 경진, 『전자상거래와 법』, 현실과 미래, 1998. 3.

14. 최 승우·김 성배·김 종걸, 『전자화폐』, 한국경제신문사, 1997. 4.

15. http://www.cepsco.org, 2000.

16. http://www.specifications.com

17. http://www.millicent.com

18. http://www.mondex.com

19. http://www.visakorea.com

20. Donal O'Mahony, Michael Peirce, Hitesh Tewari, "Electronic Payment System", Artech House,(1997).

21. Warwick Ford · Michael S. Baum, "Secure Electronic Commerce", Prentice Hall, (2001).