□특집□

전자지불 시스템의 기능요건과 기술동향

김 영 달† 한 선 영††

목 차

1. 서론

하루가 다르게 인터넷의 이용자수가 증가하면서 이들이 인터넷을 이용하여 구현하고자 하는 목적도 다양해지고 있다. 특히 정보의 공유라는 차원을 넘어서 인터넷을 이용한 상거래에 대한 관심이 높아지고 있는 시점에서 전자 상거래에 관련된 여러 가지의 기술과 시제품들이 발표되고 있어 이 분야에 관심을 가진 개인이나 기업들에게 커다란 도움을 주고 있다. 그러나 이들 중 어는 것도 아직은 국제적인 표준으로 정해지지 않은 상태이기 때문에, 이 분야에서의 주도권 확보와 시장 쟁탈을 위한 치열한 경쟁의 양상을 보이고 있는 것이 현실이다. 그 중에서도 전자 상거래의 핵심이 되는 전자 화폐 또는 디지털 화폐 시스템의 구현 방안들은 수많은 기업체에 의해서 제안되어 일부는 이미 사용되고 있다. 새로운 화폐 시스템의 등장이라는 면에서 일반 사용자에서부터 기업체까지 관심을 끌고 있으며 혁명적인 화폐 시스템일 될 수도 있는 이 기술에 대해서 우리 나라에서도 여러 기관에서 연구를 하고 있으며, 시험용 시스템도 구현되어 있다. 그러나 국가 초고속 전산망이 머지 않은 장래에 모든 금융거래의 신경망이 될 것이라는 예측을 해 볼 때, 이 초고속 전산망상에서 전자 화폐 시스템이 성공적으로 구현되어 정착되기 위해서 정부를 포함한 금융관련 기관과 일반 사용자의 입장에서 지금부터 준비해야할 내용이 무엇인지는 별로 알려 진바가 없다. 이에 전자 상거래분야에 관심을 가지고 있는 개인이나 기업들의 이해를 돕기 위해서 전자지불 시스템의 요건과, 관련 핵심 기술들에 대해서 정리해 보고, 지금까지 발표된 시스템과 각 시스템들의 특성에 대해서 알아본다. 이 시스템중의 몇 개에 대해서는 각각의 장점과 개선해야 할 점에 대해서 비교 검토한 뒤에 그 문제점들을

† 정회원 : 한국IBM(주) 전문위원
†† 정회원 . 건국대학교 전산과 교수

개선하기 위해서 제안된 시스템에 대해서 기술한다.

2. 전자지불 시스템의 운용 요건

2.1 배경

역사적으로 볼 때, 상거래를 위한 여러 가지의 요건들은 정보기술의 발전에 가장 중요한 요인이 되어 왔다. 오늘날 사용되고 있는 많은 정보시스템은 상거래에 관련된 목적으로 사용되고 있으나, 청구서의 전달이나 대금의 지불은 대부분 우편을 이용하거나 직접 방문하여 이루어지고 있다. 비용의 지불은 현금, 수표, 신용카드 등으로 이루어지고 있으나, 이것들중 어느 것도 최근의 발전된 전산망상에서 지불수단으로 사용하기 위해 필요한 요건이나 가능성에 대해서는 연구된바가 별로 없다. 그림 1에서 보는 바와 같이 최근에 미국에서 조사한 바에 의하면, 2005년경에 가서는 미국 내에서 일어나는 모든 구매액의 20%가 전자지불 시스템을 통하여 이루어질 것으로 예상하고 있다.

	1994	2000	2005
기존 구매방법 (도/소매, 통신판매)	$5,150	$8,500	$12,000
전자 구매방법	$ 245	$1,650	$2,950
- TV/Cable	$ 45	$ 400	$ 650
- 기업간	$ 140	$ 450	$ 650
- 인터넷	$?	$ 600	$1,250
- 기타	$ 60	$ 200	$ 400
전자구매의 비율	4.5%	$ 16.2%	19.7%

그림 1. 전자구매의 성장률(1994 - 2005)

이와 같이 전자 구매의 급진적인 신장이 예상되는 네트워크로 연결된 장래의 새로운 사회구조 속에서, 어떻게 하면 모든 사람들이 전자지불 시스템을 이용하여 빠르고 안전하게 서비스나 상품 및 정보의 구매 및 지불을 할 수 있겠는가에 대해 알아보고자 한다.

2.1.2 전자지불 시스템에 대한 고려사항

현재 우리 사회에서는 현금, 수표, 직불카드, 신용카드, 여행자수표, 신용장, 또는 물물교환등 각자의 필요에 따라서 이용할 수 있는 일일이 기술하기조차 힘들 정도로 많은 다양한 지불방법들이 사용되고 있다. 이들 각각의 지불 방법들은 전자상거래의 특성이 무엇인가에 따라서 장단점을 가지고 있는데, 이들중 어느 것도 앞으로 구축될 국가 초고속 전산망상에서 예상되는 전자 상거래의 지불방법으로는 완벽한 수단이 되지 못하고 있다. 왜냐하면 현재 사용되고 있는 지불방법들의 경우, 거래에 관련된 당사자들이 직접 개입하거나 오용을 방지하기 위해서, 지불거래의 처리에 상당한 시간을 할애하는 조건을 가정하고 있기 때문이다. 이들중 상당수의 방법들은 전자상거래상에서 이용될 수 있도록 하기 위해 많은 노력이 진행되어 왔으나, 사회적 및 보편적인 확산이 가능하기 위해서는 새로운 형태의 전자지불 방법이 필요한 실정이다.

예를 들어서, 지금도 컴퓨터 단말기에서 입력한 구매자의 신용카드 번호는 암호화된 메시지의 형태로 판매자한테 안전하게 보낼 수 있다. 그러나 이 시스템도 적절한 금융시스템이 갖춰야 할 요건들인 변조의 불가, 빠른 속도, 안전성, 개인정보의 보호 및 보안성 등이 아직 완전하지 못하다.

신용카드를 이용한 거래가 보안성과 변조가 불가능한 환경에서 이루어지기 위해서는

1) 고객은 자신의 신용카드에 대한 정보와 인증된 서명을 안전하게 판매자에게 제시해야하며,

2) 이 정보를 이용하여 판매자는 이 고객이 제공된 신용카드의 주인임을 검증해야한다.
3) 그후에 이 정보와 서명은 판매자의 은행에 전달되어
4) 고객의 은행에 승인을 요구하는데 사용된다.
5) 그런 후에 은행은 신용카드 정보와 비용청구에 대한 검증 결과를 판매자에게 보내게 되며, 그 후에 실질적인 상품이나 서비스, 자금의 흐름이 흐르기 시작하게 된다.

신용카드를 이용한 구매시점과 상품이나 서비스의 제공시점사이에 충분한 시간상의 여유가 있다면 고객에 대한 검증과정은 좀더 단순해 질 수 있다. 그러나 고객이 자신의 컴퓨터에서 받아 볼 수 있는 전자 항공 표를 원한다거나 다른 정보 서비스를 구매한 경우, 여러 단계에 걸친 메시지의 전송과 인증과정이 고객이 기다리고 있는 동안에 수행되어야 한다. 이 경우 여러 단계간에 암호 키의 교환과 이 암호 키를 이용한 암호화 및 복호화 과정이 반복되기 때문에 고객이 허용할 수 있는 시간 내에 끝나지 않을 수도 있다. 이 과정이 초고속 전산망에서 가능할 것으로 예상되는 모든 종류의 소액거래에까지 확산될 경우, 초고속 전산망은 데이타량의 폭주로 이용불능 상태에 빠지게 될 것이다. 따라서 신용카드를 이용한 거래에 있어서 일정액에 미치지 못하는 소액거래의 경우 초고속 전산망에서의 전자 상거래는 바람직하지 못한 것이 될 수도 있다.

오늘날 여러 나라에서 시험적으로 사용되고 있는 전자 화폐를 이용한 상거래 시스템도 그 기능을 개선하거나 약점을 보완하면, 국가 초고속 전산망에서의 안전한 상거래 시스템으로 사용할 수 있다고 생각한다. 그러나 이 시스템들이 아직은 완전하지 못하기 때문에 전자지불 시스템의 계획 단계에서부터 고려해야 할 요건들에 대해서 알아보고자 한다.

2.1.3 전자토큰(전자 화폐, 디지털 화폐)

현재 일부에서 시험중인 전자 화폐 또는 디지털 화폐가 초고속 전산망상에서의 전자 상거래를 위한 지불 시스템으로 사용될 가능성을 가지고 있기는 하나 현재 유통되고 있는 지폐와는 차이가 있다. 즉 앞의 시나리오에서 볼 수 있는 바와 같이, 전자화폐는 지폐가 가지고 있는 익명성과 같은 특성들을 그대로 가져야 할 필요는 없으며, 반대로 지폐에서는 불가능한 완전한 분리성, 사용조건의 부여 및 현재의 주인과의 연계 등과 같은 특성은 바람직하다.

전자화폐는 전자토큰의 한 형태이나, 전자토큰은 수표나 직불카드와 같은 여러 가지의 지불 방법에 대한 전자적인 지불형태로도 사용될 수 있기 때문에 적용되는 제한 조건에 따라 여러 가지의 형태로 제안된 모든 형태의 전자화폐 시스템을 전자토큰 시스템으로 통일하여 정의하고, 가장 바람직한 전자토큰 시스템의 개념에 중점을 두고 알아보고자 한다.

전자토큰 시스템의 경우, 토큰들은 사용자의 카드나 컴퓨터에 저장될 수 있으며, 원격지의 거래 당사자와 직접 교환할 수 있다. 이 토큰의 교환을 위해서 고정된 통신망이 필요한 것은 아니며 무선전화 망을 통해서도 교환이 가능하다. 거래가 진행되기 위해서는 지불 서버가 온 라인으로 가동되어야 하는 전자지불시스템이 제안되어 있다. 이 시스템도 익명성을 포함한 전자토큰의 여러 가지 특성을 포함하여 설계될 수 있다.

그러나 이 시스템은 전자토큰과 다음과 같은 면에서 차이점이 있다.

1) 그들은 통신망에 의존성을 갖는다, 즉 전용 통신망이 있어야 한다
2) 구매자와 판매자이외에 최소한 하나의 조정역할자가 있어야 하며, 경우에 따라서는 복수의 조정 역할 담당자가 있어야 한다.

매 거래마다 제 3의 조정역할 담당자와 연결해야 하는 것은 전산처리와 통신 데이터의 폭주를 유발하여 그 이용도가 저하될 수 있는 시스템이다.

2.2 기본 특성

전자토큰 시스템을 구현하는 방법에는 여러 가지가 있다. 이들 모든 시스템들은 다음과 같은 몇 가지의 기본 특성들을 만족시켜야 한다.

• 화폐 가치

전자토큰은 화폐로서의 가치를 가지고 있어야 한다. 즉 전자토큰은 현금, 은행이 보증하는 신용 또는 은행이 보증한 전자 수표 등을 상징해야 한다. 은행의 인증이 없는 전자 수표가 화폐로서의 가치를 가지고 있을 수는 있으나, 은행에 지불 청구를 했을 경우 자금의 부족으로 반려될 수도 있다. 따라서 전자토큰은 현재 통용중인 현금을 포함한 모든 형태의 지불 시스템을 전자적인 유사 시스템으로 대체할 수 있다.

• 교환성

전자토큰은 다른 전자토큰이나 지폐, 상품이나 서비스, 은행구좌에의 저축, 신용의 축적 또는 이와 유사한 것들에 대한 지불 수단으로 사용이 가능해야 한다.

• 저장성

전자토큰은 저장할 수 있어야 하며, 또 저장되었던 토큰은 다시 찾아서 사용할 수 있어야 한다. 원격지에서의 저장과 인출(즉 공중 전화 망이나 개인 통신망을 통해서도 저축과 인출이 가능해야 한다)은 사용자가 가정이나 사무실 또는 여행 중에도 전자토큰을 교환할 수 있도록 해준다. 전자토큰은 원격지의 컴퓨터 기억장치나, 스마트 카드, 또는 쉽게 이동이 가능한 장비 내에 저장될 수 있을 것이다. 컴퓨터나 컴퓨터를 통해서 읽어야 하는 카드에 저장된다면 위조가 가능하기 때문에 변경이 불가능한 전용 장비에 저장하는 것이 필요하다. 이 장비는 개인 식별 번호나 다른 유사한 수단을 이용하여 사용자에 대한 인준을 수행하기 위한 적절한 인터페이스를 가지고 있어야 하며, 카드의 내용을 볼 수 있는 모니터가 달려 있어야 한다.

• 변조의 방지

전자토큰은 수명을 다할 때까지 변조나 복사, 위조가 어려워야 한다. 유통되는 과정에서 복사나 이중사용의 방지 및 탐지가 가능해야 한다. 전산망 내에서 이루어지는 위조행위는 전세계의 어느 곳에서도 발생할 수 있기 때문에 적절한 국제적인 협약이 없이는 포착하기가 쉽지 않다. 방지책이 제대로 작동하는지를 확인하기 위해서는 포착할 수 있는 방법이 반드시 있어야 한다.

2.3 반드시 필요한 시스템의 기능

사용자들이 쉽게 사용할 수 있도록 하기 위해서, 전자토큰 시스템은 거래가 검증되고 인증될 수 있는 방법을 제공해야 한다. 이 시스템은 또 사용의 편리성, 안정성, 개인 비밀의 보장 및 보호가 가능해야 한다.

• 인증

사용자는 전자토큰이나 그 것들의 저장장치가 쉽게 변조되거나 위조되지 않도록 해야 하며, 변조되었을 경우 토큰이나 저장장치를 조사하면 쉽게 그 증거가 밝혀 질 수 있도록 해야 한다. 전자토큰을 교환 할 때, 받는 측에서는 그 토큰들이 누구나 인정할

수 있도록 인증된 것임을 확인 할 수 있어야 한다. 이 인증을 위해서 제 3의 통제 기관과 온 라인으로 연결될 필요가 있을 수도 있으며, 또는 거래 당사자 간에 직접 이루어 질 수도 있다. 만약에 거래 당사자가 동일한 곳에 위치하고 있다면, 이 과정은 오프 라인으로 이루어 질 수 있다.

• 거래의 부정불가

사용자는 전자토큰을 이용한 거래가, 관련된 당사자들간에 이루어 졌다는 것을 검증할 수 있어야 한다. 이 검증은 영수증이나 지불 증명을 위한 시스템을 통해서도 이루어 질 수 있다. 이러한 시스템들에는 전자토큰에 함께 기록된 자료나 별도의 영수증, 또는 필요에 따라 거래가 재 추적되거나 재구성 또는 검증되어야 할 때 이를 가능케 하는 수단들이 있을 수 있다. 영수증이나 지불관련 정보는 서비스나 상품의 전달과정이 장기간이 소요되든, 서비스의 제공과정에서 문제가 발생했든 또는 여러 명의 서비스 제공자들 사이에 비용의 청구와 수금과정에서 차이점이 있다 할지라도 거래 사실을 부정할 수 없도록 하기 위한 장치가 있어야 한다. 상품이나 서비스의 전달과정이 오래 걸리는 경우, 관련된 영수증이나 지불 증명의 안전한 전송은 매우 복잡한 과정이 될 수 있다.

• 서비스의 종류에 따른 정책의 다양성

예를 들어서, 음악서비스 제공자는 사용자가 신청한 음악이 전달되기 전까지 전송된 내용에 대해서도 비용을 부과할 수 있으며, 영화 서비스 제공자는 어느 정도의 분량이 전송되었느냐에 따라 비용의 부과 여부를 결정할 수도 있다. 서비스의 전송이 중간에 중단되는 원인도 생각해 볼 수 있다. 즉 고객의 의도적인 행동인지, 통신망이나 서비스 제공자의 장비 잘못인지에 따라서 비용 부과 정책은 바뀔 수 있다. 일반적으로 비용지불 정책의 구현은 현금보다는 신용카드의 경우가 좀 더 단순하다.

• 사용성

전자토큰을 이용한 거래 시스템은 필요시 항상 사용할 수 있어야 하며, 빨라야 한다. 특히 처리 속도의 향상을 위해서는 통신망의 성능, 각지역별 컴퓨터 시스템의 성능 및 전자토큰의 종류 등이 고려되어야 한다.

• 안정성

전자토큰의 유통을 위한 기반 구조의 안정성이 확보되어야 한다. 사용자는 초고속 통신망과 여기에서 사용되는 전자지불 시스템의 기반구조를 신뢰할 수 있어야 하며, 일부분의 고장이나 거래량이 증가할 지라도 별 무리 없이 전자토큰 시스템은 운용될 수 있다는 확신을 가질 수 있어야 한다.

• 비밀의 유지

전자토큰 시스템은 비밀을 보장할 수 있어야 하며, 유지할 수 있어야 한다. 사용자는 거래에 관련된 정보는 비밀로 유지되며, 관련된 당사자나 지정된 대리인만이 알 수 있다는 확신을 가질 수 있어야 한다. 통신망에의 침입자나 인가되지 않은 내부자로부터 비밀은 반드시 보호되어야 한다.

• 보안성

사용자들은 자신들이 사기성이 있거나 잘 못된 상거래에는 관련되지 않을 것이라는 확신을 가질 수 있어야 한다. 사용자는 위장, 위조 등으로부터 보호되어야 한다. 이 보안성은 전자 상거래의 전 과정에 걸쳐 확보되어야 하며, 많은 경우 관련 당사자들에 대한 인증과 믿음을 확인해 줄 수 있는 제 3의 대리인이 필요할 수도 있다.

2.4 추가적인 시스템의 기능

전자토큰 시스템의 설계과정에서 추가적으로 고려되어야 기능들에는 여러 가지가 있다. 이 추가적인 기능들을 통해서 안전성, 편리성 및 사용자에 대한 추가적인 가치의 부여 등이 가능하다. 이들 추가적인 기능들이 전자토큰 시스템이 운용되기 위해서 반드시 필요한 것은 아니지만 실제로 대부분의 기능들은 지금까지 제안된 여러 가지의 토큰 시스템에 포함되어 있다.

2.4.1 회계

회계와 거래내역의 기록이라는 면에서 고려되어야 할 기능에는 다음과 같은 것들이 있다.

• 분리성

전자토큰은 임의의 소액 단위로 분리되거나 일정 금액 단위로 증가될 수 있도록 설계되어야 한다. 원거리에서 큰 액면가의 토큰에서 작은 토큰을 얻을 수 있다면, 분리성은 필요하지 않을 수 있다.

• 영수증

구매자들은 여러 가지 이유로 해서 상품이나 서비스의 대가로 지불한 금액을 환불할 수도 있다. 구매가 지폐나 신용카드로 이루어졌던, 전자토큰으로 이루어 졌던, 영수증이나 구매사실의 증명이 필요하다. 현재의 영수증을 대체할 전자적인 새로운 대안이 개발되어야 한다.

2.4.2 전환

사용자가 전자토큰과 지폐를 상호 교환할 수 있도록 하기 위해서는 여러 가지의 기능이 필요하다.

• 전자토큰의 현금구매

어떤 사용자는 지폐로 전자토큰을 구매하고자 할 수도 있다. 이 경우 사용자의 익명성이 보장될 수 있으며, 은행에 구좌가 없는 사용자의 경우도 전자토큰을 사용할 수 있는 방법을 제공하게 된다.

• 교환

사용자가 원할 경우, 전자토큰을 지폐나 다른 형태의 화폐로 변환할 수 있도록 해주는 기능은 전자토큰의 가치나 용도를 향상시킬 수 있을 것이다. 특히 초고속 통신망이 구축되고 있는 과정이나 완전한 성숙 단계에 진입하기 전까지 그 활용도와 참여도를 증진시키기 위해서 필요한 기능중의 하나이다. 그러나 반대로 토큰의 교환성 때문에 토큰이 범죄의 대상이 될 수도 있다.

• 국제적인 사용과 다양한 화폐

궁극적으로 내국인들은 토큰을 이용하여 외국의 서비스를 이용할 수 있어야 할뿐만 아니라, 외국에서 국내의 서비스를 이용할 수도 있어야 한다. 이것이 가능하기 위해서는 전자토큰이 다양한 화폐로 사용 가능해야 한다. 한나라의 서비스 제공자는 여러 나라의 사용자들로부터 다양한 화폐로 되어 있는 전자토큰을 받을 수 있으며, 이 돈을 국내의 은행에 예치할 수도 있다. 화폐가 국경을 초월하여 전자적으로 유통될 수 있다는 것은 무역이나 국제간 금융거래에 또다른 반대 효과를 줄 수도 있다.

2.4.3 제한 조건

전자토큰 시스템의 운용을 위해 필요한 많은 요건들은 운용상에 제한 조건들을 부여함으로써 완화시키거나 위험을 감소시킬 수 있다.

제한 조건을 부여할 수 있는 분야에는 다음과 같

은 것들이 있을 수 있다.

1) 한번에 전자토큰을 이용하여 전송하거나 저축할 수 있는 화폐의 량,
2) 특정의 전자토큰이 유효한 기간
3) 전자토큰이 은행이나 유사기관에 다시 저장되기 전까지의 최대 유통횟수
4) 특정 기간이나 유사한 조건하에서 동일한 토큰을 이용하여 이루어 질 수 있는 거래의 횟수.

이러한 조건들은 이 시스템을 구현하는 데에 있어서 여러 가지의 새로운 과제를 제기할 수도 있다.

• 기간의 제한

일정기간이 지나면 그 토큰을 더 이상 사용할 수 없게 하는 조건이다. 이 경우 사용자는 제한된 기간이 되기 전에 그 토큰을 교환해야만 한다. 이 기능이 원활히 작용할 수 있도록 하기 위해서 토큰에는 날짜와 시간이 표시되어야 하며, 초고속망 전체에 걸쳐서 허용된 범위내의 정확성을 가지고 날짜와 시간이 동일하게 관리되어야 한다.

• 최대 금액과 거래횟수

하나의 전자토큰장치에 허용되는 최대한의 토큰 금액이나, 일정 시간내에 동일한 전자토큰장치로 전송될 수 있는 총 토큰 금액의 양을 제한할 수 있다. 그러나 이 조건은 토큰 발행자의 책임범위를 제한하는 방법도 될 수 있다. 사용자의 토큰 장치는 통신망상에서 소액거래를 짧은 시간 내에 다량 발생시키도록 프로그래밍할 수 있기 때문에 일정 금액 이상의 거래만 추적한다는 것은 별도움이 되지 못한다. 그러나 변조가 불가능한 장치를 사용토록 할 경우, 거래금액의 크기나 시간상의 제한 조건을 반드시 준수하도록 할 수 있을 것이다. 예를 들어서 익명성을 가진 동전지갑의 경우, 24시간 내에는 50,000원내에서만 돈을 받거나 쓸 수 있도록 하는 것이다. 또 다음 24시간내의 거래 횟수는 사용율이나 재발급을 위해 은행에 다시 저축하기까지의 남아 있는 거래 횟수 등에 따라서 정할 수도 있다. 전자토큰을 특정 서비스나 상품에만 사용하게 할 수도 있다.

• 조건부 지불과 지불 날짜의 지정

구매자의 지시에 따라서, 장래의 특정 시간 내에 구매한 상품이나 서비스가 전달되기 전에는 토큰을 이용한 지불이 발생하지 않도록 할 수 있어야 한다. 반대로 지불이 완료되기 전까지는 서비스나 상품의 전달을 보류할 수 있도록 해야한다.

2.4.4 추적가능성

전자토큰을 이용하여 이루어진 거래를 추적할 수 있도록 하기 위해서는 다음과 같은 기능이 필요하다.

• 토큰의 등록

발행된 모든 토큰에는 식별번호를 부여하여, 모두 등록해야 할 필요가 있을 수 있다. 현재 우리가 사용하고 있는 동전이나 지폐가 일련번호를 이용하여 식별되듯이, 전자토큰도 유사한 방법으로 관리될 수 있다. 이렇게 할 경우 등록되지 않은 토큰이나 복사된 토큰을 쉽게 찾아낼 수 있게 된다.

• 익명성

전자토큰을 이용한 거래의 익명성에 대해서는 여러 가지의 입장이 있을 수 있다. 많은 사용자들은 판매자가 누구인지 아는 상태에서 자신들의 거래에 대해서는 익명성을 가지기를 바랄 수 있다. 그러나 법원의 명령이 있을 경우, 사용자가 누구인지, 거래의 내용이 무엇인지를 밝히지 않으면 안될 수도 있다. 또 상세한 거래 내역을 필요로 하거나 자신의 정보

시스템을 개선하기 위한 자료가 필요한 경우, 또는 판매 전문회사에 거래 내역을 판매하고자 할 경우에는 익명성을 포기하지 않으면 안된다. 이런 다양한 요건을 충족시키기 위한 방법으로 부분적인 익명성만 유지할 수도 있다. 즉 거래 당사자나 법원이 익명성의 포기를 허락하지 않을 경우 거래 당사자의 익명성을 유지하는 방법이다. 기술적인 면에서 보면, 익명성을 어느 정도까지 유지하기 위해서는 추가적인 암호화 기술과 아울러 회계나 제한 조건에 관련된 기능들의 일부가 완화될 필요가 있다.

2.4.5 안전성

전자토큰 시스템은 안전성에 관련된 새로운 과제를 야기시킨다. 초고속 통신망상에서의 전자토큰을 이용한 상거래의 익명성이나 편리성, 또는 가밀성은 사용자의 입장에서는 여러 가지의 문제점을 야기시킬 수도 있다. 예를 들어 범죄자가 사용자의 구좌에서 통신망에 연결되어 있는 범죄자의 토큰 장치로 전자토큰을 전송하도록 강요한 뒤에, 다른 나라에 있는 자신의 구좌로 전송한 뒤 도망가는 경우를 생각해 볼 때, 이 일이 피해자의 집이나 범죄자가 선택한 어떤 장소에서도 가능하기 때문에 피해자를 납치한 뒤 ATM에서 현금을 찾게 하는 경우보다 범죄자의 입장에서는 훨씬 안전하게 된다. 전자토큰의 전송과정이 익명으로 이루어진다면 범죄자는 더욱더 추적하기 어렵게 된다. 이러한 안전상의 문제점들 때문에 다음과 같은 기능들이 필요할 수 있다.

• 소유권

특정 토큰에 대한 인증된 소유권을 확인하기 위해서 토큰과 소유자가 연계될 수 있다. 이를 위해서 전자토큰은 물론 소유자의 인증이 필요한데, 이 인증은 패스워드나 암호 키를 이용하는 방법이나 음성 인식, 글씨체의 감식, 지문 또는 안구 인식 등과 같은 생물학적인 방법을 사용할 수 있다. 이 기능을 이용할 경우, 잃어버린 토큰이나 훔친 토큰은 무용지물이 되게 할 수 있다. 전자 서명은 전자토큰의 소유자가 아니라 전자토큰 자체를 인증하는 수단이다. 개인 식별번호나 비밀번호는 이 것들을 법적인 소유자만 알고 있다는 가정 하에서 인증되기 때문에 소유자가 알지 못하는 사이에 다른 범죄자가 사용할 수도 있다.

생물학적인 인증 방법은 전혀 복제가 불가능한 방법이기는 하나, 강요되는 듯한 느낌을 줄 수 있다. 전자토큰이 소유자의 비밀번호나 신체적인 특징과 연결되어 있을 경우에, 새로운 소유자에게 토큰을 전송하기 위해서는 이 연결관계가 변경되어야 한다. 또한가지 방법으로 토큰의 소유자를 토큰을 저장하거나 발행하는 장치로 식별할 수도 있다. 잘못된 패스워드나 비밀번호를 사용하는 경우에도 정상적인 거래인 것처럼 처리를 하되, 정당한 소유자가 아닌 경우 토큰을 파기시키거나 범죄행위가 진행되고 있음을 관련 통제기관에 알려 주는 기능을 전자토큰 시스템에 추가할 필요가 있다.

• 동일한 장소에 적용업무와 관련 데이터의 유지

지불 방법으로서의 전자토큰과 전자토큰과 함께 저장되는 비밀정보간의 관계는 주의 깊게 정의할 필요가 있다. 특히 여러 가지 용도로 사용하는 장치 내에 이 것들이 함께 존재하는 경우에 주의가 필요하다. 운전면허 관련 정보, 건강관련 정보, 선호하는 구매 형태, 화폐와 관련된 정보를 포함한 기타 개인적인 정보는 동일한 컴퓨터나 카드, 또는 장치에 보안을 유지하는 상태에서 보관해야 하며, 전자토큰은 지역적으로 완전히 다른 장소에 보관되어야 한다. 이렇게 함으로서 전자토큰과 소유자의 관계를 추정함에 의해서 발생될 수 있는 전자토큰의 잘 못된 사

용을 방지 할 수 있기 때문이다.

2.5 시스템의 관리와 통제

전자토큰 시스템의 구현과 사용의 의무화가 얼마나 용이할 것인가는 전적으로 이 시스템의 가지고 있는 기능의 다양성에 달려 있다. 예를 들어, 전자토큰이 사용되어 그것의 소유권이 전번 소유주나 거래 기록과의 연계 없이 오프 라인으로 이전될 수 있다면, 정부의 규제나 상거래 관련 규정을 따르고 있는지를 감사하고 추적하는 것이 어려워진다. 전자토큰의 위조나 변조도 방지하기가 쉽지 않게 된다.

그러나 단순히 기능의 구현만으로 안전한 시스템을 보장할 수는 없다. 시스템의 안전성과 보안성을 확보하기 위해서는 하드웨어와 소프트웨어는 물론 사용자의 행동 양식과 금융거래의 모든 과정을 포함한 시스템의 모든 면이 면밀하게 검토 및 고려되어야 한다. 어떠한 전자토큰 시스템이라도 암호화나 전자 서명 기술만으로는 방어할 수 없는 취약점이 있을 수 있으며, 이 취약점들은 많은 경우에 무지하거나 잘못된 사용자와 업무절차를 통해 전자토큰 시스템을 위협하는 창구가 된다.

구현된 시스템은 돈의 세탁, 암거래 행위 또는 내부자의 오류 등이 어렵게 해야 하며, 동시에 이러한 것들이 쉽게 감지될 수 있도록 해야 한다.

이러한 목표를 달성하기 위한 시스템의 관리/통제 방안, 정책 및 절차에 대해서 알아본다.

2.5.1 법적인 요건

무거운 형벌 조항을 담은 법률을 만들 수는 있다. 그리고 이 무거운 형벌을 무서워하는 사람들이 이 시스템에 대해서 범죄행위를 하는 것을 줄일 수는 있을 것이다. 그러나 범죄행위를 시도하기가 쉬우며, 발각될 가능성도 적고 그 결과로 얻는 범죄자의 이익이 클 경우, 법만으로 범죄 행위를 막는 것은 불가능하다. 이 시스템은 범죄의 방지를 최우선으로 하여 설계되어야 한다. 범죄 발생후의 법적 처리는 전자토큰 시스템에 아무런 도움이 되지 않기 때문이다.

2.5.2 기술적 및 관리적 통제

보안성과 기밀성을 확보하고 사기 행위를 방지하기 위해서 다양한 기술이 이용될 수 있다. 기술을 이용한 통제 방법에는 변조가 불가능한 전자 회로가 들어 있는 스마트카드, 암호화, 전자 서명, 암호 키의 안전한 교환을 위한 관리 체제, 취약점 분석기술, 생물학적인 인증 방법 등이 있다. 어떠한 기술을 사용하는가에 따라서 비용이나 성능, 그리고 바라는 기능들의 목표가 달성되는 정도가 달라질 수 있다.

관리적인 면에서도 통제 방안이 적용되어야 한다. 예를 들어서 전자토큰이 원거리에 있는 구좌로부터 인출되거나 저축될 경우 금융기관과 사용자는 서로를 인증해야만 한다. 스마트 카드를 사용할 경우, 이 카드를 판독하는 장치는 자신을 스마트 카드에게 인증시킬 수 있는 방안이 있어야 한다. 이 방법들은 잘못해서 정당한 사용자들에게 서비스를 거부하는 일이 있어서는 안된다. 잘못된 사용을 방지하기 위해서 범죄의 가능성이 있는 카드나 토큰의 목록을 관리할 수도 있다.

2.5.3 감사

전자토큰의 상세한 유통과정을 추적할 수 있도록 시스템이 설계되어야 한다. 이 추적 자료들은 전자토큰의 발행 및 교환에 관련된 내용을 포함해야 하며, 중복된 사용의 검출을 위해서도 이용될 수 있다. 또 전자토큰을 이용한 서비스 비용이 구매자로부터

판매자에게 보내졌고, 판매자에 의해서 수령되었으며, 토큰의 유효여부가 검증되어 지불이 완료되었고, 관련된 서비스나 상품이 전달되었음이 추적 가능해야 한다.

2.5.4 정책과 운용관련 과제

전자토큰 시스템의 구현에 관련되어 먼저 해결되어야 할 과제는 다음과 같은 것들이 있다.

• 인증기관

전자토큰 시스템의 구현을 위해서는 거래 당사자가 아닌 제 3의 인증기관이 필요한데, 이 인증기관은 거래 당사자의 인증이나 이 당사자들간의 거래에서 사용되는 암호화나 전자 서명을 위한 키의 인증을 담당하게 된다. 예를 들어 공용키 암호화 기법을 이용한 전자 서명의 경우, 서명을 하는 당사자는 상대방의 공용키를 가지고 전자서명을 한 뒤에 자신의 비밀키를 가지고 이 메시지를 암호화하며, 이 암호화된 메시지를 상대방이 확인할 수 있도록 자신의 공용키를 상대방에게 보내게 된다. 메시지를 받는 상대방은 메시지를 보낸 측의 공용키를 가지고 전자서명된 메시지를 복호화하고 자신의 비밀키를 가지고 전자 서명을 검증하게 된다. 그러나 이 과정에서 받는 측은 상대방이 보낸 공개키가 신뢰할 만한 것인지를 어떻게 확신할 수 있겠는가 ?. 이런 경우 보낸 측의 공개키가 잘 알려진 제 3의 통제기관에서 인증된 것이라면 문제가 되지 않을 것이다.

이 제 3의 통제기관에서 공개적으로 배포된 공개키의 적법성을 지원하고 전자토큰을 이용한 상거래와 관련된 장치의 소유권에 대한 인증 및 등록을 담당한다. 이러한 통제 기관은 하나가 아니라 여러 개의 기관으로 구성된 계층구조로 되어야 할 필요가 있을 수 있다. 이 경우 각각의 통제기관들의 기능, 정책, 업무 절차 및 관계는 미리 정립되어야 한다. 예를 들어서 인증서가 어떻게 발행되어야 하며, 배포되어야 하는지에 대한 정책을 결정하는 기관, 암호 시스템을 운영하는 기관, 거래 관련 당사자들을 검증하여 인증서를 발행하고 인증된 당사자들에 대한 목록을 발행하며, 또 자격이 미달할 경우 인증을 취소하고 그 목록을 발행하는 기관 등이 있을 수 있다.

• 전자토큰의 발행자

전자토큰을 발행한 조직은 그들이 발행한 토큰을 실제의 화폐로 교환해 줄 수 있어야 한다. 누가 전자토큰을 발행해야 하는가 ?, 은행이나 정부는 별도로 토큰을 발행할 것인가 ?, 이 경우에 각각의 기관은 상대방이 발행한 토큰을 함께 사용해야만 하는가 ?, 또는 각각의 기관들은 공통의 풀에서 토큰을 발행해야 하는가 ?, 이 경우에 중심이 되는 발행기관이 있어야 하는가 ?, 이 기관은 재무부나 한국은행이 되어야 하는가 ? 등의 과제들에 대한 결정이 이루어 져야 한다.

• 전자토큰의 가치에 대한 책임

현재 유통되고 있는 화폐의 가치에 대해서는 정부가 책임을 지고 있다. 전자토큰에 대해서는 누가 책임을 질 것인가 ?. 어떤 은행이 전자토큰을 발행했을 경우, 그 은행만 책임을 지면 되는가 ?등의 과제가 고려되어야 한다.

• 손실에 대한 책임

전자토큰을 잃어 버렸거나 절도 당했을 경우, 누가 그 손실을 책임질 것인가 ?. 잃어버렸거나 절도당한 토큰은 여행자 수표처럼 원래의 발행자에 의해서 재 발행되어야 하는가, 아니면 현금처럼 재 발행될 필요가 없는가 ?, 만약에 위조된 토큰을 이용한

지불이 실수로 인증되었다면, 누가 이 손실에 대해서 책임을 져야 하는가 ?등의 과제가 고려되어야 한다.

● 미사용 전자 화폐의 귀속

현행법에 의하면 일정기간이 지난 휴면계좌나 사용하지 않은 여행자 수표의 경우 정부재산으로 귀속되게 되어 있다. 전자토큰의 경우에도 동일한 방법으로 처리해야 하는가 ?. 만약 동일한 방법을 적용한다면, 모든 발행된 전자토큰과 현재 유통중인 토큰에 대한 관리가 이루어지지 않으면 안된다.

● 범용성

범용성은 전자지불 시스템의 기본적인 요건이다. 은행에 구좌가 없거나 은행과 신용관계가 없는 사람일지라도 전자토큰을 사용하기 원할 경우, 언제든지 취득하여 사용할 수 있어야 한다. 즉 현행의 화폐로 언제든지 구매가 가능해야 하며, 구매나 사용을 위한 특별한 자격요건이 필요해서는 안된다. 그러나 범용성은 익명성을 의미하는 것은 아니기 때문에 구매 시에 구매자기 누구인지를 밝혀야 할 필요가 있을 수는 있다.

● 규약

전자토큰 시스템은 사기나 오용을 막기 위한 국제법, 국가의 법, 또는 지방자치 단체의 법에 저촉되어서는 안된다. 예를 들어서 한거래당 최대의 금액을 설정하는 것은 의미가 없다. 전자토큰의 사용이 보편화될 경우, 큰 거래 하나에 해당하는 작은 금액의 거래를 여러 번 수행함으로서 규정을 피해 가는 것은 어려운 일이 아니기 때문이다. 대신에 초고속 전산망에서 각각의 사용자나 전자토큰 장치가 할 수 있는 토큰의 전송율을 규정하는 것이 필요하다. 추가적으로 일정 기간내에 각각의 사용자나 토큰 장비에 의해서 전송된 토큰의 총량에 대한 추적이 필요하다. 이 추적기능의 필요성은 전자토큰 시스템이 어떻게 구현될 것인가에 많은 영향을 끼칠 수 있다. 일정액 이상의 토큰이 외국으로 전송되는 것을 감시하기 위해서는 국제 전자 상거래 규약과 국가간의 협력이 필요하다.

● 토큰의 발행료, 이윤 및 상환 수수료

사용자가 토큰을 구매할 때, 토큰의 발행료를 구매자한테 부과할 것인가 ?. 부과한다면 발행시점에 부과할 것인가, 아니면 토큰을 이용한 첫 번째 지불시점에 부과할 것인가 ?. 전자 화폐를 현금으로 상환할 경우, 수수료의 부과는 정당한가 ?, 토큰을 구매한 시점부터 현금으로 교환하기 위해 토큰이 발행자에게 돌아 올 때까지, 토큰대신에 보관되어 있는 현금은 투자하여 이윤을 얻을 수도 있으며, 또는 이미 현금이 인출된 것처럼 처리할 수도 있을 것이다. 투자에 의해 이윤이 발생한 경우, 누가 이 이윤을 관리해야만 하는가 ?, 현금으로의 상환시점에서 지불 총액이 인출된 총액과 일치하는지를 점검해보는 것과 같은 검사나 특별 보고서가 작성되어야 하는가 ?등의 과제가 고려되어야 한다.

● 거래내역의 관리

전자토큰을 이용한 거래의 내역을 어느 정도까지, 누가 어디에 기록/보관할 것인가에 대해서는 여러 가지의 방안이 있을 수 있다. 이 방안들은 거래에 관련된 기밀보호라는 면에서 좋지 않은 영향을 줄 수 있다. 거래의 내역은 물론 전자토큰 잔고의 증감내역도 기록될 것인가 ?, 이 내용들은 사용자의 카드나 토큰장비에 기록할 것인가, 아니면 통제 은행이나 발행자의 데이터베이스에서 관리될 것인가 ?, 관리 기간은 ?, 거래내역의 기록 및 관리에 대한 정부나 지방자치 단체의 법이 별도로 있는가 ? 등의 과제가

고려되어야 한다.

3. 전자지불 시스템의 모델

최근에 여러 회사에서 인터넷상에서의 구매 서비스를 지원하기 시작했다. 이들중 어느 것은 신용카드를 이용한 구매나 비용의 청구 및 지불 서비스를 제공하며, 다른 것들은 전자화폐 서비스를 제공한다. 이제까지 제안된 전자지불 시스템의 모델은 크게 두 가지로 구분해 볼 수 있다. 첫째는 앞에서서 정의한 전자토큰의 일부 기능만을 구현하는 전자화폐를 이용하는 모델이며, 또하나는 신용카드를 이용한 모델이다. 전자 화폐를 이용하는 모델의 경우, 기존의 현금을 이용하는 경우와 유사한 모델과 수표를 이용하는 경우와 유사한 모델로 구분하는 경우도 있으나, 다양한 요건을 모두 충족시키기보다는 특정분야가 강조된 다양한 시스템들이 제안되어 있기 때문에 일률적으로 구분하기는 쉽지 않다.

• 전자 화폐 모델

전자지불 시스템에서 사용되는 현금은 전자화폐로 구성되어 있는데, 이 전자화폐는 발행자와는 독립적으로 인증될 수 있다. 이 인증은 변조가 불가능한 장치를 이용하거나 스스로를 인증할 수 있는 기능을 가진 전자화폐를 통해 가능하다. 기존의 화폐 시스템에서 수표와 현금의 큰 차이는 익명성의 보장에 있다고 볼 때, 전자화폐의 경우 현금 모델이나 수표 모델 모두의 경우에 익명성에 관련되어서는 동일한 요건의 적용이 가능하기 때문에 실제로는 동일하게 취급할 수 있다.

• 신용 카드 모델

전자지불 시스템에서의 신용카드 모델은 기존의 신용카드 시스템을 이용하는 방법이다. 이 모델은 기존의 신용카드 시스템이 가지고 있는 특성을 그대로 적용하면서 보안성의 확보를 위해 암호화 기술을 적용하는 모델이다. 카드 모델의 중요한 특성중의 하나는 모든 거래가 보험을 수반한다는 것이다.

또 한가지 어떤 모델의 경우, 독자적인 전자화폐를 만들어서, 기존의 상품 할인 쿠폰처럼 특정 구역에서만 사용할 수 있게 하는 모델을 구현한 경우도 있다.

4. 전자화폐 시스템의 예

현재 구현되어 사용되는 전자지불 시스템 중에서 가장 많은 사용자들을 확보하고 있는 시스템은 신용카드를 이용하는 시스템이다. 이 전자지불 시스템에서는 거래 관련자들의 신용카드 번호를 안전하게 전송하는 것이 가장 중요한 목표이다. 이 시스템은 기존의 거래 방법을 전자적으로 변환한 형태이기 때문에 사용자들의 신뢰성을 확보하는데 가장 큰 장점을 가지고 있다. 그러나 앞에서 살펴 본 전자지불 시스템의 요건에 비추어 볼 때, 가장 효율적인 시스템의 구현을 위해서는 현금/수표를 사용한 모델이 더 유리하다. 아직은 현 시스템과의 차이점 때문에 확산에 어려움이 있기는 하나 새로운 정보처리 기술을 이용한 화폐 시스템으로의 전환이라는 면에서는 훨씬 더 유리하기 때문에 여기에서는 현재 제안된 2가지의 현금/수표 모델의 전자화폐 시스템을 비교 검토하고, 각각의 문제점을 개선하기 위해서 제안된 모델에 대해서 알아보고자 한다.

4.1 Ecash 시스템

4.1.1 개요

DigiCash사의 David Chaum이 제안한 모델로써,

전자화폐의 소유자에 대한 우수한 익명성의 제공이 특징이다. 이 모델에서의 전자화폐(Ecash)는 실제의 지폐를 전자적으로 전환한 것으로 나타낸다. 인터넷 상에서 모든 거래가 이루어지는 모델이기 때문에 보안을 위해서 공용키 암호화 기법을 사용하며, 구매자와 판매자는 CyberWallet이라는 특수 프로그램을 사용하여 모든 거래를 수행한다. 이 시스템의 구성요소와 기능은 다음과 같다.

• CyberWallet

은행에서 전자화폐를 인출하거나 저금할 때, 또는 판매자에게 대금을 지불하거나 받을 때 사용하는 클라이언트 소프트웨어로써 판매자와 구매자가 사용한다.

• 보안성 및 기밀성의 확보 방안

이 시스템의 사용자는 모두 공용키 암호화 기법을 사용하기 때문에 비밀키와 공용키를 가지고 관련 당사자간의 모든 메세지의 통신에 사용한다. 상대방의 인증을 위해서는 전자 서명 방식을 이용한다.

• 익명성의 확보

전자화폐의 익명성을 확보하기 위해서는 David Chaum이 창안한 Blind Signature 기법을 사용한다. 고객이 전자화폐의 발행을 요구할 때, 필요로 하는 액면금액과 일련번호도 함께 은행에 보내게 되는데, 이때 각각의 전자화폐에 부여된 일련 번호에 고객만이 알 수 있는 비밀 숫자를 곱해서 보냄으로써 은행이 서명한 전자화폐와 신청자의 관계를 알지 못하게 함으로써 기존의 화폐와 동일한 익명성을 확보한다. 고객은 은행이 인증하여 발행한 전자화폐를 수령한 뒤, 자신만이 알고 있는 숫자로 각각의 일련번호를 나누면 본래의 일련번호를 알 수 있게 된다.

• 은행

은행은 고객이 신청한 전자화폐를 발행하며, 구매자와 판매자간에 유통되는 전자화폐의 유효성을 검증한다. 또한 전자화폐를 소유한 고객이 원할 경우 전자화폐를 실제의 화폐로 교환해주기도 한다.

• 구매자 및 판매자

이 시스템을 이용하기 위해서는 은행에 구좌를 개설해야 하며, 전자화폐가 필요할 경우, Cyber Wallet 프로그램을 이용하여 은행에 발행을 요청한다. 발행된 전자화폐를 은행에 저축할 수도 있으며, 상품을 구매하기 위해서 인출할 수도 있다. 물론 판매자는 판매하는 상품이나 서비스의 대금을 전자화폐로 받을 수 있어야 한다.

4.1.2 전자화폐의 발행

고객의 요구에 의해 전자화폐가 발행되는 과정은 다음과 같다.

1) 고객의 CyberWallet에 의한 발행의 신청
   - 고객은 CyberWallet을 이용하여 각각의 액면금액별 필요 량을 계산하고,
   - 그 각각에 대해 일련번호를 부여한다. 이 일련 번호들은 Blind Signature기법을 사용했을 때 동일한 결과가 나오는 것을 방지하기 위해서 100 digits정도의 크기를 가진다.
   - 고객만이 알고 있는 숫자로 일련번호를 곱하여 Blind Signature를 한 뒤에, 이 화폐들을 하나의 메시지로 만든다.
   - 이 메시지를 자신의 비밀키를 이용하여 전자서명을 하고
   - 은행의 공용키를 이용하여 암호화 한 뒤에
   - 은행으로 전송한다.

2) 은행에서의 발행
- 고객이 보내온 메시지를 자신의 비밀키로 복호화하고
- 고객의 공용키를 이용하여 전자 서명을 확인한다. 이 과정에서 아무런 문제가 없을 경우
- 고객의 구좌에서 신청한 전자화폐에 상당하는 금액을 인출한 뒤에
- Blind Signature된 전자화폐를 자신의 비밀키로 전자 서명한다.
- 이 메시지를 고객의 공용키로 암호화한 뒤에
- 고객한테 전송한다.

3) 고객의 CyberWallet에 의한 전자화폐의 접수
- 은행이 보낸 메시지를 자신의 비밀키로 복호화하고
- 은행의 공용키를 이용하여 은행의 서명을 확인 한 뒤에
- Blind Signature시에 사용했던 숫자로 각각의 일련 번호를 나누면,
- 은행이 서명하여 인정한. 그러나 각 전자화폐의 일련 번호는 자신만이 알 수 있는 전자화폐의 발행이 완성되게 된다.

4.1.3 전자화폐를 이용한 상품이나 서비스의 구매

전자화폐를 이용하여 상품을 구매하기 위해서는 웹브라우저와 CyberWallet를 이용해야 한다.

웹상에서 자신이 원하는 상품을 발견했을 경우(그림 2 참조),

1) 판매자의 Ecash 프로그램을 가동시키기 위한 HTTP메시지를 웹서버에게 보낸다.
2) 판매자의 Ecash프로그램이 가동되면, 웹 서버는 구매자가 원하는 상품과 구매자의 시스템에 대한 내용을 판매자의 Ecash프로그램에게 보낸다.
3) 판매자의 Ecash프로그램은 TCP/IP를 이용하는 별도의 선로를 이용하여 구매자의 CyberWallet프로그램에게 지불을 요구한다.
4) 구매자가 동의할 경우, 구매자의 CyberWallet은 정확한 액수의 전자화폐를 수집하여 하나의 메시지로 만든 다음, 판매자의 공용키로 암호화 한 뒤에 판매자에게 전송한다. 만약에 구매자가 지불 요구에 동의하지 않을 경우나 정

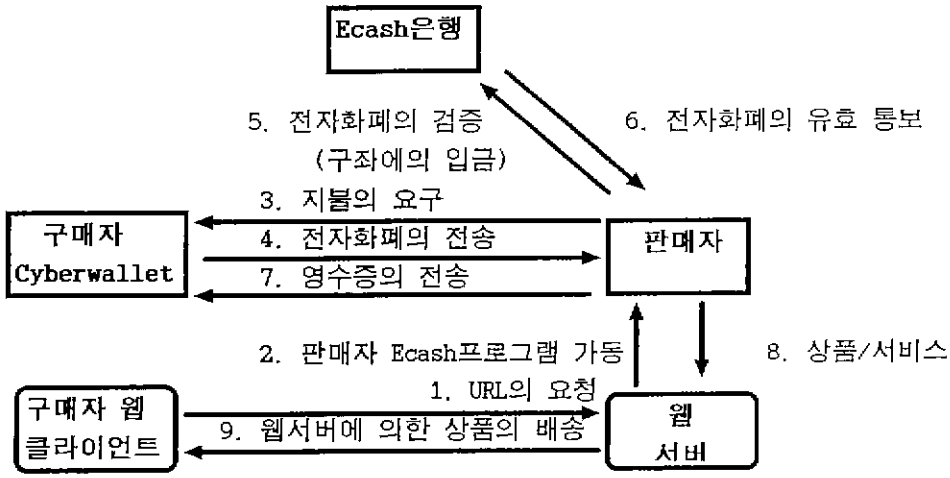


그림 2. 전자화폐(E-cash)를 이용한 구매

확한 (잔돈이 남지 않는)액수의 전자화폐가 없을 경우, 거절 메시지를 보낸다.

5) 판매자는 전자화폐를 받은 후, 유효성을 검증하기 위해서 이 화폐들을 하나의 메시지로 만들어서 자신의 비밀키로 전자 서명을 하고 은행의 공용키로 복호화한 뒤에 은행에게 전송한다.
6) 은행은 판매자가 보낸 전자화폐들의 일련 번호를 이미 사용된 화폐나 반납된 화폐의 일련 번호를 관리하고 있는 데이터베이스와 비교하여 유효성을 검증한다. 만약에 판매자가 보낸 화폐의 일련 번호가 데이타베이스내에 없고 은행의 전자 서명이 있다면, 유효한 화폐이기 때문에 판매자의 구좌에 전자화폐에 상당하는 금액이 입금된다. 이 전자화폐는 사용이 끝났기 때문에 파기한 뒤, 일련 번호만 데이터베이스에 기록된다.
7) 판매자의 Ecash프로그램은 전자화폐가 판매자의 구좌에 입금되었음을 통보 받으면, 판매자가 서명한 영수증을 구매자의 CyberWallet에게 보낸다.
8) 판매자의 Ecash프로그램은 동시에 웹서버에게 구매가 완료되었음을 통보하고
9) 웹서버는 이 사실을 구매자의 웹클라이언트에게 통보한다.

4.1.4 장점과 단점

이 시스템의 장점으로는 메시지의 전송을 위해서 완전한 익명성과 보안성을 제공하며, Blind Signature때문에 거래의 추적이 불가능한 점이다. 단점으로는 사용된 전자화폐를 관리하기 위한 데이타베이스가 중앙 집중적인 관리일 경우, 매우 커질 수밖에 없다는 점이다. 또 발행된 전자화폐는 고객이 사용하는 시스템 내에서 관리되어야 하는데 이 화폐들의 안전한 관리를 위해서 보안책이 강화되어야 한다. 확장성을 위해서 하나의 은행이 아닌 여러 은행에서 전자화폐를 발행할 수 있도록 함으로써 거대한 데이터베이스로 인한 문제점을 줄일 수 있을 것이다.

4.2. NetCash 시스템

4.2.1 개요

University of California의 Information Science Institute에서 제안한 시스템으로 확장성이 장점이다. 이 시스템의 구성 요소와 기능들은 다음과 같다.

• 중앙 인증 기관

전자화폐를 발행할 수 있는 기능을 가진 화폐 서버(Currency Server)를 인준하는 기관으로써 서버의 이름이나 공용키 등을 포함하는 인증서를 발행한다.

• 화폐 서버

중앙 인증기관으로부터 인증을 받아서 전자화폐(NetCash)를 발행하는 기능을 가지며, 인증기관이 인증하는 내용은 인증번호, 화폐 서버의 이름, 화폐 서버의 공용키, 인증 날짜 등이다. 이 서버가 발행하는 전자화폐는 발행한 서버의 이름, 서버의 주소, 전자화폐의 유효기간, 일련 번호, 액면금액등이 표시된다. 이 서버는 자신이 발행하여 유통중인 모든 화폐의 일련 번호를 데이타베이스내에 관리하며 자신의 고객이 원할 경우, 전자화폐를 전자 수표로 교환해 주기도 한다.

• 구좌 서버

화폐 서버나 구매자, 또는 판매자가 이 시스템을

이용하기 위해서는 은행에 구좌를 개설해야 한다. 이 때 이 은행들의 역할이 구좌 서버이며, 이 은행이 화폐 서버의 역할을 할 수도 있다.

4.2.2 전자화폐를 이용한 구매

구매자는 판매자와 거래를 시작하기 전에 판매자의 공용키를 알고 있어야 하며, 판매자는 화폐 서버의 공용키를 알고 있어야 한다.

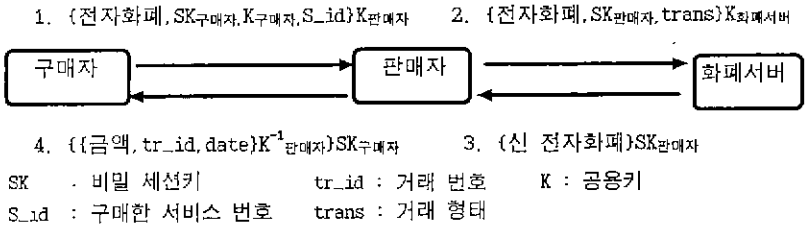


그림 3. 전자화폐(NetCash)를 구매

전자화폐를 이용한 구매는 다음과 같이 이루어진다(그림 3 참조).

1) 구매자가 원하는 상품이나 서비스의 금액, 자신의 새로운 비밀 세션키와 공용키를 하나의 메세지로 만들어 판매자의 공용키로 암호화하여 전송한다. 이 메시지에 포함된 새로운 비밀 세션키는 판매자가 구매자와 별도의 전송로를 설정하고자 할 때 사용할 수 있도록 하기 위한 것이며, 공용키는 거래 중에 구매자가 판매자에게 보낸 메시지를 검증하기 위한 것이다.
2) 판매자는 구매자한테서 받은 전자화폐와 자신의 새로운 비밀 세션키를 하나의 메시지로 만들어 화폐 서버의 공용키로 암호화한 뒤에 화폐 서버한테 전송하여 구매자가 보낸 전자화폐를 검증하도록 한다.
3) 화폐 서버는 판매자가 보낸 전자화폐의 일련번호를 자신이 발행한 전자화폐의 일련번호를 관리하는 데이터베이스와 비교하여, 그 번호가 데이타베이스내에 있으면 유효한 것으로 판정한다. 유효한 화폐로 판정되면, 새로운 전자화폐나 전자 수표를 발행하여 판매자가 보낸 비밀 세션키를 사용하여 암호화 한 뒤에 판매자에게 전송한다. 판매자가 보낸 화폐는 더 이상 유통될 수 없으므로 데이터베이스에서 일련 번호를 삭제함으로써 파기해 버린다.
4) 대금 지불이 완료된 징표로써 새로운 전자화폐나 전자 수표를 받은 판매자는 수령한 금액과 거래 번호, 날짜 등을 포함하는 영수증을 만들어 자신의 비밀키로 전자 서명을 하고, 구매자가 보낸 비밀 세션키로 암호화한 뒤에 구매자에게 전송한다.
5) 영수증을 받은 구매자는 영수증에 포함된 거래 번호를 이용하여 자신이 구매한 서비스나 상품의 배달을 요구할 수 있다.

4.2.3 장점과 단점

이 시스템의 장점으로는, 복수개의 화폐 서버가 기능하기 때문에 확장성이 뛰어나며, 보안성이 강화된 별도의 전송로를 확보하기 위해 새로운 비밀 세션키를 사용하고 있는 점이다. 전자화폐를 발행하는 시점에서 전자화폐의 일련번호를 화폐서버가 부여하기 때문에 완전한 익명성을 보장하지는 않으나 복수개의 화폐서버와 전자화폐를 이용해서 거래 시마

다 새로운 전자화폐를 발행하기 때문에 어느 정도까지의 익명성을 확보할 수는 있다. 또한 보안성의 강화를 위해 관련자간에 비밀 세션키를사용하기 때문에 처리에 많은 시간이 추가적으로 소요되는 단점이 있다. 또한 판매자가, 구매자의 전자화폐에 대한 은행의 검증을 거친 뒤 구매자에게 영수증을 보내주지 않고 그냥 사용해 버릴 경우에 대한 대비가 부족하다.

4.3. PayMe 프로토콜

4.3.1 개요

아일랜드 Trinity 대학의 Michael Peirce와 Donal O'Mahony가 제안한 모델로써 Ecash의 완전한 익명성과 NetCash의 확장성을 함께 구현 할 수 있도록 한 모델이다.

• 보안성의 확보

보안성의 확보를 위해 비밀키를 이용한 암호화 기법인 IDEA와 공용키를 이용한 암호화 기법인 RSA기법을 사용한다. 또 보안과 기밀의 강화를 위해 PayMe Transfer Protocol(PMTP)을 이용하여 거래 관련자간에 메시지를 전송한다.

• PayMe Transfer Protocol(PMTP)

PayMe시스템에서의 메시지의 전송을 위해 사용하는 프로토콜로써 6가지의 메시지와 각 메시지별로 최초의 요청, 메시지에 대한 긍정의 응답 및 거절하는 응답을 하기 위해 이용하는 3가지의 방법이 정의되어 있다.

6가지의 메시지는

- Withdraw coins (고객과 은행간에 사용)
- Deposit coins (고객과 은행간에 사용)
- Request bank statement (고객과 은행간에 사용)
- Exchange coins for new ones (고객과 은행간에 사용)
- Ask for payment (고객과 고객간에 사용)
- Pay coins (고객과 고객간에 사용)

가 정의되어 있으며, 각 메시지별로 정의된 3가지의 용도는 다음과 같다.

- Request : 위에서 정의한 6가지의 메시지를 처음에 보낼 때 사용
- Response : 받은 메시지에 대한 긍정의 응답을 보낼 때 사용
- Refusal : 받은 메시지에 대한 거절의 응답을 보낼 때 사용

• 은행

은행은 구매자와 판매자의 구좌를 관리하며, 전자화폐를 발행한다. 전자화폐는 액면금액, 일련번호, 은행의 식별번호, 은행의 시스템명과 통신포트 번호, 유효기간 등으로 구성되어 있으며, 현재 유통중인 전자화폐를 데이타베이스내에 관리한다.

전자화폐의 예는 다음과 같다.

예) {10 MIK1234 BANK1 bank.cs.tcd.ie:8000 18-12-98}K[private,BANK1]

10 : 액면금액(\, $, ...)
MIK1234 : 전자화폐의 일련번호
BANK1 : 은행의 이름
bank.cs.tcd.ie : 은행의 시스템 명
8000 : 은행 시스템의 통신 포트번호
18-12-98 : 전자화폐의 유효기간
K[private, BANK1] : 은행의 비밀키를 이용한 전자서명

• 판매자와 구매자

이 시스템을 이용하여 거래를 하고자하는 경우 은행에 구좌를 개설하여 은행이 발행한 전자화폐를 이용하여 거래를 한다.

4.3.2 PMTP에 의한 보안

• 도청(Eavesdropping)의 방지

메시지 수신자의 공용키를 이용하여 메시지를 암호화하여 보내거나 별도의 방법으로 전달된 비밀키를 이용하여 암호화하여 메시지를 전송하는 방법을 이용한다.

• 메시지의 변조 방지

Message Digestion기능과 함께 전자 서명 방식을 사용한다.

• 메시지의 재사용 방지

모든 메시지에 "NONCE"옵션을 적용함으로써, 모든 메시지가 특정의 주소를 가진 클라이언트로부터 일정 시간내에 수신되도록 한다. 전송되는 모든 메시지를 추적함으로써 동일한 "NONCE"옵션을 가진 메시지가 수신되는 것을 방지한다.

• 가장(Masquerading)의 방지

모든 메시지는 전자 서명을 하여 전송하며, 전자서명이 없는 메시지의 경우 비밀키 암호화 기법을 사용한다. "NONCE"옵션을 가진 메시지내의 네트웍 주소는 정당한 사용자로 가장하는 속임수를 어렵게 한다.

• 비밀키의 보호

사용자별 비밀키는 패스워드를 사용하여 암호화하여 보관하며, 이 비밀키를 알지 못하면 PMTP메시지는 전송될 수 없다.

4.3.3 PayMe를 이용한 구매

구매자는 PayMe시스템의 Wallet프로그램과 웹클라이언트를 구동시켜 구매할 준비를 한다(그림 4 참조).

1) 판매자의 Wallet 프로그램을 가동시키기 위한 HTTP메시지를 웹서버에게 보낸다.
2) 판매자의 Wallet프로그램이 가동되면, 웹 서버는 구매자가 원하는 상품과 구매자의 웹클라이언트의 주소를 판매자의 Wallet프로그램에게 보낸다.
3) 판매자의 Wallet프로그램은 TCP/IP를 이용하는 별도의 선로를 이용하여 구매자의 Wallet프로그램에게 Ask_payment_request 메시지를 보내어 대금의 지불을 요구한다.
4) 구매자가 동의할 경우, 구매자의 Wallet은 정확한 액수의 전자화폐를 수집하여 하나의 메시지로 만든 다음, 판매자의 공용키로 암호화한 뒤에 Pay_coins_request 메시지를 판매자에게 전송한다. 이때 사용하는 Pay_coins_request는 Ask_payment_response와 동일한 역할을 하는 메시지이다. 만약에 구매자가 지불 요구에 동의하지 않을 경우에는 Ask_payment_refusal메시지를 사용하여, 거절 메시지를 보낸다.
5) 판매자는 전자화폐를 받은 후, 유효성을 검증하기 위해서, 이 화폐들을 은행에 전송한다.
6) 은행은 판매자가 보낸 전자화폐들의 일련 번호를, 현재 유통중인 화폐를 관리하고 있는 데이타베에스와 비교하여 유효성을 검증한다. 만약에 판매자 보낸 화폐의 일련 번호가 데이타베

이스내에 있다면, 유효한 화폐이기 때문에 판매자의 구좌에 전자화폐에 상당하는 금액을 입금하거나 새로운 전자화폐를 발행한다. 만약에 판매자가 구매자의 전자화폐를 발행한 은행이 아닌 다른 은행에 구좌를 가지고 있다면 그 은행의 구좌에 입금시킨다.

7) 판매자의 Wallet프로그램은 전자화폐가 자신의 구좌에 입금되었음을 Exchange_coins_response나 Deposit_coins_response 메시지로 통보 받게 된다. 판매자의 Wallet프로그램은 지불이 완료되었음을 통보 받으면, 자신이 서명한 영수증을 Pay_coins_response메시지를 이용하여 구매자의 Wallet 프로그램에게 보낸다.

8) 판매자의 Wallet프로그램은 동시에 웹서버에게 구매가 완료되었음을 통보하고

9) 웹서버는 이 사실을 구매자의 웹클라이언트에게 통보한다.

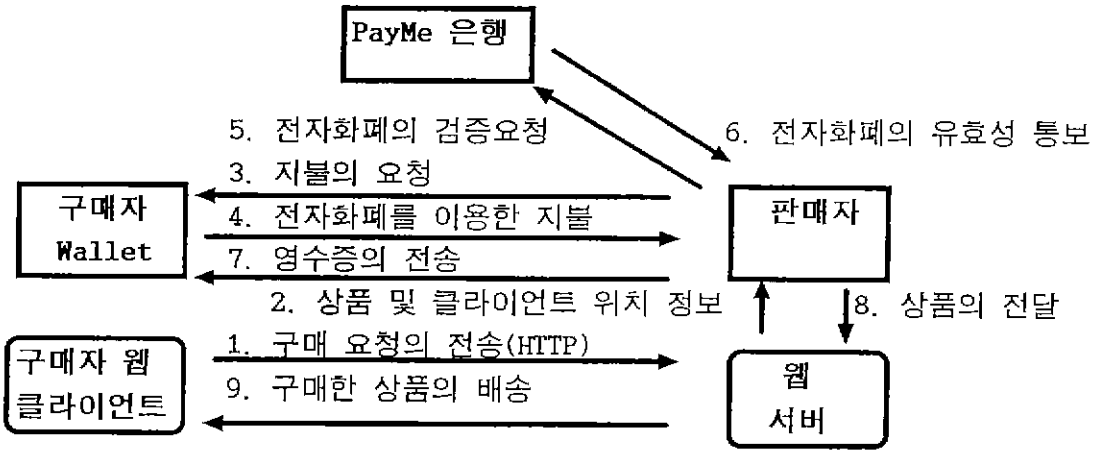


그림 4. PayMe시스템을 이용한 구매

4.4.4 장점과 단점

장점으로는, 암호화 기법과 PMTP메시지를 이용하기 때문에 보안성의 확보가 용이하며, 복수개의 은행에 의한 화폐의 발행 및 관리와 고객과 고객, 또는 고객과 은행간에 간단한 PMTP 프로토콜을 사용하고 Ecash와는 달리 전자화폐의 일련 번호가 짧아도 되기 때문에 확장성과 안정성이 양호하다. 또 신용카드가 전제 조건이 아니기 때문에 누구든 사용할 수 있으며, PMTP 메시지의 전송을 위해 별도의 전송로를 사용하기 때문에 어떤 웹서버나 클라이언트에서도 사용할 수 있다. 특정의 카드나 장비를 사용하지 않으며, 정보제공 서비스는 물론 상품의 거래에도 사용할 수 있다. 그러나 은행이 익명성의 정도를 제어할 수 있기 때문에 완전한 익명성이 필요한 경우, 명확한 통제 및 관리 절차가 구현되어야 한다.

7. 결론

국가 초고속 통신망상에서 운용 가능한 여러 가지의 전자지불 시스템이 제안되어 있지만, 그 중에서도 전자화폐를 이용한 모델은 여러 가지의 장점을 가지고 있다. 국가 초고속 전산망상에서의 상거래를 하고자 할 경우 전자화폐를 이용한 시스템은 실제의 화폐가 가지고 있는 여러 가지의 편리성과 이점을 그대로 이용할 수 있다. 나아가서 이 시스템은 안정되지 못한 통신망이나 일정 시간동안만 연결되어 있

는 통신망에서도 운용이 가능하다. 국가 초고속 전산망상에서 전자지불 시스템이 어떻게 구현될 것인가에 대해서는 여러 가지의 고려할 점이 있다. 복잡한 시스템을 구현할 경우, 지폐와 유사한 시스템만을 구현하는 것이 아니라 수표, 신용거래 등까지를 포함하는 광범위한 지불 시스템을 구현할 수도 있다. 또 전자화폐 시스템을 익명성을 포함하는 현행 지폐의 모든 특성을 갖도록 구현하여 전자화폐를 이용한 거래의 횟수가 무제한으로 그리고 오프 라인으로 이루어지게 할 수도 있다. 이러한 시스템은 관리나 통제가 매우 어려운 단점이 있다. 반대로 기능이나 제한 조건에 제한을 두어 구현 할 수도 있다. 예를 들어 오프 라인으로의 전자화폐의 유통 횟수나 발행자나 은행에 의해서 회수되기까지의 기간에 제한을 둘 수도 있다.

보안성과 편리성, 안전성과 기밀성이 확보된 전자지불 시스템이 개발되어 보편적으로 사용될 수 있기 위해서는 전자화폐의 손실에 대한 책임 소재, 전자화폐 발행자의 지정, 다국적 화폐 기능, 전자화폐의 사용에 대한 국제적 및 국내적인 법률과 규정의 제정 등에 대한 여러 가지의 과제에 대한 고려가 필요하다.

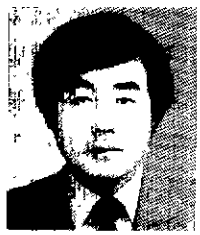
금융관련 기관이나 정보처리 전문가뿐만 아니라 정책입안자와 일반 사용자들의 다양한 의견을 수렴하여 전자지불 시스템을 설계하고 구현할 때, 이 새로운 기술이 가지고 있는 장점을 최대한 실현할 수 있다. 또한 여러 산업에 걸친 전문가들로 구성된 실무 팀은 국가 초고속 통신망을 이용한 전자지불 시스템의 새로운 가능성을 실현하기 위한 기술적인 해결책의 개발을 촉진시킬 것이다.

참 고 문 헌

1. Daniel C. Lynch and Leslie Lundquest, "Digital Money", John Wiely & Sons, Inc. 1996
2. Cross-Industry Working Team of Corporation for National Research Initiatives (CNRI), "Electronic Cash and Payments in the National Information Infrastructure", 1996
3. Dr Phillip M. Hallam-Baker, "Electronic Payment Schemes", World Wide Web Consortium, 1995
4. "World Wide Web Journal - Fourth International World Wide Web Conference Proceeding", Dec. 11-14, 1995, Boston, Massachusetts, USA. http://www.w3.org/WWW4/
5. Ecash by DigiCash, http://www.digicash.com/ecash/ecash-home.html
6 NetCash by Information Science Institute, University of Southern California, http://nii-server.isi.edu:80/info/netcash/

김 영 달

1969년~1977년 서울대학교 자연대학 계산통계학과(이학사)
1989년~1991년 서강대학교 공공정책대학원 정보처리학과(이학석사)
1992년~현재 한국 정보처리 전문가협회 회원
1994년~현재 한국 정보처리학회 회지 편집위원
1976년~현재 한국 IBM (주) 컨설팅 사업부 전문위원
관심분야 : 컴퓨터 통신, 인터넷 보안, 전자 상거래



한 선 영

1973년~1977년 서울대학교 자연대학 계산통계학과(이학사)
1977년~1979년 한국과학기술원 전산학과(이학석사)
1983년~1988년 한국과학기술원 전산학과(공학박사)
1979년~1981년 시스템공학연구소 연구원
1981년~현재 건국대학교 전자계산학과 교수
관심분야 : 컴퓨터 통신, 분산처리, HCI등