스마트카드를 이용한 전자지불시스템
(Electronic Paymentsystem using Smart Card)

이 창 순*
(Chang Soon Lee)

요 약 전자상거래를 위한 전자지불시스템은 크게 전자화폐형, 전자수표형 그리고 신용카드형으로 분류할 수 있다. 각 방식에는 사용상의 특성으로 인하여 장단점이 있으나, 현재 현실세계에서와 같이 전자화폐지불시스템이 가장 활발하게 사용될 것이다. 그러나 전자화폐 지불시스템의 가장 큰 위험요소는 전자정보의 근본적 속성 즉 복사가 가능하다는 것이다. 이로 인하여 야기되는 화폐 검사에 대한 많은 비용이 발생한다. 본 연구에서는 기존의 전자화폐지불시스템에 따른 요구조건들을 알아보고, 스마트카드를 사용한 전자지불시스템에서 구현되어야 할 부가적 요구조건들을 제안한다.

Abstract The most important technical problem in EC is about secure electronic payment systems. Electronic payment systems come three different types distinguished by the payment method.: electronic cash, electronic check, and creditcard. In these types, electronic cash payment system is popular and practical as in real commerce. But electronic cash can be copied easily, then it is infeasible to prevent user from double-spending a coin. In this paper, we overview several requirements for secure electronic payment system and present other proposed additions to the results. At last we present a model system which considers requirements above examined.

1. 서 론

개방형 네트워크인 인터넷 사용이 일반인들에게도 폭발적으로 증가하고 있다. 이와 같이 거대한 인터넷 사용자들을 대상으로 유무형의 각종 서비스를 제공하여 경제가치를 창출하려는 전자상거래(Electronic Commerce)라고 하는 새로운 상거래가 활발히 연구되고 있다. 그리고 이미 세계 경제 질서는 정보화를 통해 재편되고 있는 실정이다. 그래서 현재 세계 각국이 초미의 관심을 보이고 있는 현안은 전자상거래이다. 이러한 전자상거래에 대한 관심이 증대되고 많은 사람들이 전자상거래를 이용하고자 하지만 여기에는 제도적, 기술적으로 선결되어야 할 문제들이 있다.

그 중에서도 전자상거래가 더욱 구체화되면서 가장 중요한 선결과제는 신뢰할 수 있고 안전한 전자지불시스템(Electronic Payment System)이다. 소비자나 판매자가 안심하고 전자상거래를 할 수 있도록 하기 위해서는 대금결제를 전자적인 방법으로 처리할 수 있도록 하는 편리하고 효과적인 새로운 전자지불 방법이 제공되어야 한다. 전자지불시스템은 구분 방법에 따라 여러 가지로 분류되나 대체로 전자화폐형[1], 전자수표형 그리고 신용카드형[2]으로 구분된다. 이들 전자지불시스템들은 각각의 특징들이 있으나, 신용카드형은 지불행위시 항상 은행과의 트랜잭션이 이루어지며, 따라서 소액의 거래에 있어서는 부가되는 처리비용이 문제가 되며, 여기에 신용카드를 발급받지 못하는 사용자에게는 이용이 불가하다. 전자화폐지불시스템은 현실 세계의 실물화폐와 같은 기능을 하도록 고안된 디지털화된 화폐이며, 소액거래에 있어서는 매우 가능성이 있는 전자지불시스템이다. 그러나 전자정보의 근본적인 특성상 복사가 가능해, 즉 이중사용에 대한 대책이 반드시 고려되어야 한다.

한편 하드웨어기술의 발달로 기존의 신용카드 크기에 고성능 프로세서, 메모리 등을 갖춘 지능형 IC카드인 스마트카드의 등장은 기존의 전자지불 프로토콜에 상당한 변화를 가져다 줄 것이다. 특히 현재의 전자지불시스템이 제공하지 않고 있는 기능이나, 지불거래 이후에야 판별가

† 경산대학교 학술연구비 지원에 의한 논문임
* 경산대학교 정보과학부 부교수

능한 기능도 현장에서 즉시 제공해 줄 수 있다. 또한 스마트카드의 위조가 어렵고, 도난, 분실의 경우에도 부정사용이 어려우며 공중전화나 교통이용 등에 적용할 수 있는 복합기능이 포함될 것이다. 이와 같은 특성으로 인해 전자상거래의 다양한 분야에서 온라인과 오프라인을 동시에 지원하는 범용 화폐로 사용될 것이다[3]. 이런 장점을 바탕으로 머지 않아 스마트카드형태의 전자지불시스템에 대한 연구가 활발해 질 것이다.

본 연구에서는 전자화폐지불시스템의 안전성 보장과 보호기술을 알아보고 기존의 전자화폐지불시스템들의 동작과정을 분석한다. 그리고 여기에 보완해야 할 안전성 요소들도 제안한다. 끝으로 앞의 분석을 검토하여 스마트카드를 이용한 전자지불시스템 모델을 제안한다.

2 전자화폐지불시스템

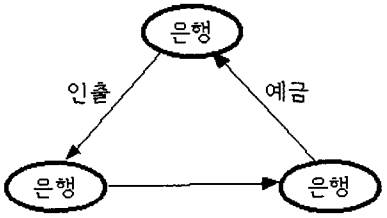
전자화폐지불시스템이란 전자화폐를 사용하여 전자상거래에서 발생하는 유무형의 지불을 수행하는 시스템으로 전자상거래의 기본요소 중에서 제일 중요한 사항이다. 그림1은 전자지불시스템의 기본 모델을 설명한 것이다.

2.1 전자화폐의 개념

전자화폐란 기존의 화폐가 가지고 있는 현금가치저장, 지불 등의 기능을 보장하는 디지털 화폐이며, 발행은행이 전자서명으로 보장한다. 전자화폐는 네트워크 상에서 이루어지는 지불 수단이며, 무형의 전자정보이기 때문에 원격지 이동, 휴대 및 보관의 편리성 등에서 실제화폐보다 장점이 있으나 위조 등에서는 심각한 단점이 있어 안전한 전자화폐지불시스템의 구현이 무엇보다 중요하다.

2.2 전자화폐지불시스템의 기본 요건

전자상거래를 통한 지불행위에서 상점주인뿐 아니라 고객들도 안전하다는 신뢰감을 부여하려면 여러 가지 안전성이 보장되어야 한다. 먼저, 현실세계의 현금이 제공하는 익명성이 보장되어야 한다. 즉 사용자의 프라이버시 보호이며, 사용자의 전자화폐 사용내역이 거래 상점뿐 아니라 제 3자에게도 알려져서는 안된다. 그리고 직접적인 거래가 아닌 인터넷을 통한 거래에서는 거래가 완료된 후에도 어느 한쪽이 거래 사실을 부인할 수도 있으므로 부인방지성이 있어야 한다. 전자화폐는 위변조가 쉬우므로 이에 대한 대책이 필요하다. 여기에 전자화폐를 두 번 이상 사용이 불가능하도록 이중사용방지성이 보장되어야 한다. 다음으로 사용자가 다른 사용자에게 자신의 가치를 양도할 수 있는 양도성도 기본적인 요건이다. 상점에서 지불시 은행의 개입없이 처리가 가능하도록 오프라인성도 가지고 있다면 더욱 활용가치가 높을 것이다. 지불금액이 은행에서 인출한 금액까지 가능하도록 분할해서 사용할 수 있도록 기능이 포함되어야 한다[4][5].



<그림 1> 전자화폐지불시스템 모델

3. 기존의 전자화폐지불시스템의 분석

본 절에서는 지금까지 연구된 전자화폐지불시스템들에 대하여 살펴본다. 앞의 ecash와 넷캐시는 일반 전자화폐지불시스템이고 뒤의 것들은 IC카드를 사용한 전자지불시스템들이다.

3.1 ecash

네덜란드의 디지캐시에서 개발한 전자화폐이다[6][7]. 현재는 미국의 Mark Twain은행과 유럽의 EUnet 그리고 핀란드의 Marita은행이 시범 사업을 실시하고 있다. 사용자가 ecash를 사용하기 위해서는 거래 은행에 실물 현금을 예치하고 전자화폐로 교환하여 전자지갑에 저장하였다가 가맹점으로 가입된 상점에서 물건을 구입시 이를 상점주인에게 지불한다. 화폐는 화폐번호와 이에 대한 발행자의 서명으로 구성되며 화폐발행시 사용자는 자신이 직접 화폐번호를 생성하여 이에 대한 발행자의 서명을 받게 되는데, 추적방지서명(Blind Signature)[4]이라는 기법을 사용하여 익명성을 보장된다. 그러나 중복사용의 검출을 위해 거래 도중에 발행은행의 서버에 중복사용여부를 확인하기 때문에 트랜잭션 비용이 큰 단점이 있다. 그리고 사용된 화폐에 대한 DB가 너무 커지는 것을 방지하기 위해 일정기간만 유효한 화폐를 발행하여 사용하기 때문에, 기간 내에 사용하거나 주기적으로 재발행 받아야 하는 불편함이 있다. 또한 분할성이 제공되지 않아 정확한 지불이 성립되기 어렵다. 그러나 현재까지 가장 발전된 전자화폐지불시스템으로 인식되고 있다.

3.2 NetCash

캘리포니아 대학에서 개발 중인 넷캐시(NetCash)[8]는 근본적으로 똑같은 시리얼번호와 가치를 지닌 여러 개의 전자화폐를 고객에게 발행한다. 다만 이 화폐들은 유효기간이 서로 다르다. 즉 유효기간에 따라 적법한 전자화폐를 사용하도록 한다. 분산 시스템으로 디지캐시가 갖고 있는 중앙 집중적인 계좌 관리에서 오는 단점을 해결하려 하고 있다. 다음은 넷캐시의 지불과정을 간략히 설명한 것이다. 먼저 고객은 하나의 화폐 M을 통화 서버에 전송하고, 통화서버는 이 화폐로부터 여러 개의 화폐 M1, M2, M3에 동일한 가치와 일련번호 그리고 상이한 유효기간을 지정한다. 다음으로 고객이 공급자로부터 하나의 상품을 선택하면 일정한 유효기간을 갖는 M1을 통하여 지불한다. 그리고 공급자가 이 화폐를 유효기간 내에 통화서버에 입금했을 때, 상품을 배달하지 않으면 고객은 M1의 유효기간이 지난 다음 통화서버에 질의를 통하여 잘못을 찾아 상쇄할 수 있다. 그러면 통화서버는 고객에게 M1의 가치가 있는 새로운 화폐를 지불하고 이를 판매자의 계좌에서 부담시킨다.

넷캐시는 디지캐시보다 약한 익명성을 지원하고 있다. 고객이 원하는 수준의 여러 단계의 익명성을 지원 한다는 계획이다. 그 대신 사용자의 계좌를 분산된 여러 대의 서버에서 관리하며 사용자의 수를 극대화하는 데에 역점을 두고 있다. 또한 넷체크(NetCheque)라는 전자 수표 시스템과 교환이 가능하도록 하고 있다.

3.3 몬덱스

영국의 Westminst은행과 Midland은행이 중심이 되어 95년 7월부터 IC카드를 이용한 오프라인 전자화폐시스템 서비스를 시작했다. 몬덱스카드는 폐쇄형 플랫폼을 적용한 IC 카드와는 달리 카드발급자(은행)가 IC칩 공급자에 독립적으로 다양한 응용서비스를 손쉽게 추가, 운용할 수 있도록 하였다. 이 시스템은 공개하는 것을 원칙으로 하고 있어 누구나 손쉽게 이용할 수 있으며, 칩 내부에 5개국의 화폐를 입력할 수 있고 최근의 거래내역 10개를 차례로 기록할 수 있는 기능을 갖고 있다. 다음으로, 몬덱스 화폐는 IC카드를 사용하고 있으므로 화폐정보를 컴퓨터 하드디스크에 보관하는 것보다 안정성 측면에서 뛰어나다는 점이다. 몬덱스카드의 구조는 개방형 시스템 방식이기 때문에 은행의 중앙시스템을 거치지 않고 카드간이나 개인간에 화폐를 교환할 수 있다. 개인간 자금이체 기능은 기존에 사용하고 있는 현금과 동일한 방법으로 IC카드 메모리에 디지털 데이터 형태로 보유하고 있는 화폐가치를 결제할 상대방과 손쉽게 주고받을 수 있도록 지원하는 것이다. 따라서 통신망 등을 통해 은행의 중앙시스템을 거치지 않고 오프라인 상태에서 화폐의 가치이전 처리가 가능하다는 것이다. 이렇게 되면 화폐 발행 은행은 전산시스템 구축비용이 절감되고, 카드 발급과 가맹점 관리비용을 줄일 수 있다. 그리고 온라인 거래에 따른 시스템 과부하나 사용자의 과다한 통신비용에 대한 걱정을 덜 수 있다는 장점이 있다[9].

3.4 CAFE

Digicash사, 독일의 Hildesheim 대학과 Freiburg 대학 그리고 Simens사 등 세계 각국의 13개 협력자가 이 프로젝트에 참여하고 있다. 서로 다른 5 종류의 통화가 SmartCard에 저장 가능하다. 카드 분실의 경우 잔액이 통보되면서 상환된다. 이러한 개방 구조는 많은 은행, 상인 그리고 고객들의 참여를 가능하게 한다. 1995년 10월부터 1996년 2월에 걸쳐 CAFE는 유럽연합위원회에서 검증되었다. 그 결과 이 시스템은 시장성이 상당히 큰 것으로 입증되었으며 지불 거래시 7 Mhz에서 약 1.2초에서 1.5초가 소요된다[7]. CAFE 시스템의 경우에는 추적방지 서명을 이용하여 익명성의 보장까지도 가능하다[9].

4. 전자화폐지불시스템 모델

4.1 추가적 고려사항 검토

· 상호인증시 상대의 기만행위를 확실히 방지해야 한다.

먼저 카드판독기와 카드간의 상호인증이 선행되어야 불법적 공격행위를 초기 단계에서 막을 수 있다. 상점측에서 불순한 의도가 있다면 고객을 기만하여 판독기와 카드간 상호인증이 성공적으로 이루어진 것처럼 한 후 카드사용자에게 카드비밀번호를 입력시키도록 하여, PIN번호를 알아낼 수가 있다. 즉, 카드에 사용자비밀번호(PIN)를 입력할 버턴과 화면창을 마련할 기술적 한계성이 있다면 판독기에서 PIN번호를 입력시켜야 하는데, 여기서 상호인증이 성공하지 못했을 경우에도 성공한 것처럼 PIN번호를 입력시키도록 요구한다면 비록 프로토콜 전체는 성공하지 못하더라도 판독기는 PIN번호를 획득할 수 있다.
이를 막기 위해서는 상호인증시 판독기와 마찬가지로 카드에도 화면창이 있어 인증의 성공 여부를 카드주인에게 표시할 수 있어야 한다. 인증 성공여부를 알려주는 메시지도 카드사용자가 선택하여 카드 내에 보관해야 한다.

· 전자현금, 전자수표 및 신용카드 기능을 통합한 카드형태가 가능하다. 양 당사자가 전자지불 방식에 상호 동의

만 한다면 어느 방식으로나 전자지불을 행할 수가 있다. 그러나 통합한 형태가 좋을 수도 있으나 한 방식에서 허점이 발견된다면 같은 메모리를 공유할 경우 다른 전자지불시스템도 위험해 질 수 있으므로 반드시 각 전자지불시스템은 독립된 형태로 카드 내에 구현되는 것이 바람직하다.

· 지불금액에 관계없이 정확한 지불이 필요하다.

여기에는 하나의 전자화폐를 인출해서 분할 지불이 가능하게 하는 방법이 있고, 처음부터 가능한 지불금액에 맞추어 무수히 많은 코인을 인출해서 카드 내에 저장해 두는 방법이 있다.

· 은행이 자의적으로 고객에게 범죄에 대한 책임을 전가시킬 수 있다.

이에 대하여는 고객이 은행에 전자화폐 인출에 관한 사항을 전자서명하여 요구한다면, 나중에 없던 내용을 가지고 고객에게 그 책임을 전가시키지는 못할 것이다.

· 익명성취소 요건의 강화가 가능한가.

지금까지 연구된 결과들은 대부분 제3의 신뢰기관을 둠으로써 조건부 익명성취소 기능을 부가하였다. 그리고 익명성취소시 신뢰기관과 발행은행과의 합의만 있으면 언제든지 가능하다. 그래서 사용자는 본의 아니게 자신의 전자지불 내역이 공개될 수도 있다. 이를 예방하기 위하여 익명성취소 요건으로 사용자 자신의 동의도 포함시킨다면 보다 강화된 익명성을 부여할 수 있을 것이다.
이를 위해서는 신뢰기관에 등록하는 정보를 사용자의 공개 키로 암호화하여 저장하도록 한다.

· 이중사용방지는 지불과정에서 소프트웨어적으로는 근본적으로 불가능하다.

전자정보의 특성상 근본적으로 복사가 가능하기 때문에, 오프라인 상에서 지불이 이루어지기 전에 전자화폐의 이중사용을 방지하기는 거의 불가능하다.

스마트카드 내에는 기본적으로 하드웨어적인 TRM (tamper resistant module(device))이 장착된다. 따라서 TRM내의 특수장치와의 연동을 통하여 전자화폐의 사용이 가능하도록 한다면, 전자화폐 자체의 복사만으로는 적법한 지불이 성립되지 않는다. 특히 이 장치는 은행에서도 수리를 위한 핑계로 그 내용을 알아낼 수 없어야 한다.

· 오프라인으로 전자지불이 가능해야 한다.

온라인으로의 안전한 전자지불을 위해서는 여러 가지 부가적 트랜잭션과 시간이 요구된다. 이로 인하여 처리비용이 상대적으로 비싸진다. 따라서 소액의 전자지불에서는 적용이 어렵다.

앞의 항과 같이 TRM부분을 이용한다면 가능하다.

4.2 전자화폐지불시스템 모델 제안

· 익명성취소 요건 강화

신뢰 기관에 고객 및 상점의 인적사항 등록시 자신의 공개키로 암호화하여 저장한다. 그러면 나중에 익명성취소를 위하여는 본인들의 동의가 있어야 가능하다.

· 발행은행에 의한 고의적 범죄조작에 대한 대책

전자화폐 발행을 요청할 때, 요청 내용을 본인의 비밀키로 서명하여 제출한다.

상점도 예금을 요청할 때 본인이 서명하여 제출한다.

· 이중사용 방지 대책

스마트카드 TRM내에 자체적으로 생성되는 난수를 각각의 전자화폐와 연동시킨다면 카드주인 혹은 상점주인은 불법으로 전자화폐를 지불하는 것을 막을 수 있다.

· 사용 전자화폐 연결 불가능성

전자화폐와 사용자간의 유일한 연결고리를 화폐발행 번호로 한정한다. 따라서 화폐발행 번호에 대한 익명성(익명성 취소 요건시 제외)만 부여하면 가능하다.

5. 결 론

본 연구에서는 기존의 전자화폐지불시스템들을 분석을 한 후, 보다 안전한 전자화폐지불시스템을 위한 요구조건들을 검토하였다. 그리고 그 요구조건을 해결하기 위한 방안을 제안하였다. 향 후 제안된 방안을 바탕으로 구체적인 프로토콜을 구현하여, 새로운 기능제공과 함께 보다 안전하고 신뢰할 수 있는 전자화폐지불시스템 개발이 진행되어야 한다.

참 고 문 헌

[1] David G.W. Birch, "Paying for Electronic Commerce-Smart Cards on the Superhighway", Electronic Commerce '95, 1995.b.

[2] Cummings, Elain M., "EC Payment Schemes",

CIO's Electronic Commerce Resource Center, 1996.

[3] Buck Peter S., "From Electronic Money to Electronic Cash:Payment on the Net", 1995.

[4] D. Chaum, "Blind signatures for untraceable payments," Advances in Cryptology-CRYPTO '82, pages 199-203, Springer-Verlag, 1983.

[5]Oracle Magazine, "인터넷 전자상거래의 기술적 메카니즘", volumeXIV/Nr.2, 한국어판, 1998.

[6]http://www.digicash.com/ecash/ecash-home.htm.

[7] Himmelspach Andrea; Runge Alexander; Schubert Petra und Zimmermann H.D. (1996,10b), "Analyse und Bewertung von elektronischen Zahlungssystemen", BusinessMedia/52.

[8] http://nii-server.isi.edu/info/NetCash

[9] 이용호 외 "전자지불 표준 동향분석에 관한 연구", 1998.6