전자 상거래에 있어서 전자식 대금결제 시스템 설계

권영직 · 조현준
대구대학교 컴퓨터 정보공학부

Ⅰ. 서 론

전자 상거래의 개념에 대해서는 아직 뚜렷하게 정의내린 것이 없지만, 일반적으로 전자 상거래란 다양한 형태의 전자적인 매체를 이용하여 상품 및 서비스의 거래에 필요한 정보를 교환하고 거래하는 것을 말하는 것으로 상행위 이외에도 계약, 건설, 은행업무, 엔지니어링, 운송 등과 관련된 일체의 거래행위를 포괄적으로 의미한다. (김정평 외 1인, 1997)

ALGA(Automotive Industry Action Group)에 의하면 전자 상거래를 '거래 당사자간 비즈니스 관계의 효율성 증진을 위하여 진보된 정보기술의 지원을 받아 비즈니스 비전을 가능하게 하는것'이라고 정의했다. (김상규, 1997)

이러한 전자 상거래는 PC의 폭발적 보급, 네트워크의 개방화, 쌍방향 멀티미디어의 통신기술 발달, 글로벌화의 진전 등으로 점점 확기를 띠고 있다. 시장조사 기관들은 지난 94년 약 2천 4백 50억달러(1백 96조원)였던 세계 전자 상거래 규모가 2천년에는 약 1조 6천 5백억달러(1천 3백 20조원)에 이를 것으로 예측되며 폭발적인 성장이 있어날 것이라고 전망하고 있다. (김정평 외 1인, 1997)

전자식 대금 결제 시스템을 설계하기 위해서는 전자 상거래 특히 인터넷상의 전자적 상거래의 특징을 알아야 할것같다. 전자적 상거래의 특징은 다음 네 가지로 요약할 수 있다.

첫째, 전자적 상거래는 사람이 직접 만나지 않고 컴퓨터와 네트워크을 통해 거래를 이루는 것이므로 네트워크상의 컴퓨터시스템에 대한 확인이 필요하게 된다. 네트워크을 이용한 거래이기 때문에 특별히 기밀성(confidentiality)에 대한 고려가 필요하다. 기밀성을 얻기위해 암호화 기술을 사용한다. (Elgamal, 1995)

둘째, 모든 거래에 대한 기록이 디지털 형태이기 때문에 완벽하게 똑같이 복제가 가능하며 위조가 매우 쉽다. 그리고 디지털 자료를 거래에 대한 증거로서 사용하기 위해 보조적인 보안요소들이 필요하다.

셋째, 현재 컴퓨터 네트워크 특히 인터넷을 사용하는 사람들의 신분을 인증할 수 있는 인프라가 없다. 전자우편주소 혹은 IP(Information Provider)주소 등은 어떤 사용자의 신분을 믿을만하게 대변할 수 있는 도구가 되지 못한다. 그러므로 안전한 전자 상거래를 위해서는 거래 당사자의 신분을 인증할 수 있는 인프라가 필요하게 된다. 비자와 마스터 카드사가 공동으로 만든 인터넷전자지불 프로토콜인 SET(Secure Electronic Transaction)의 근본 구조가 인증국(Certificate Authority ; CA)을 중간으로 한 점도 바로 이런 이유 때문이다.(VISA, Master Card)

넷째, 전자 상거래는 일반적인 상거래와는 달리 거래를 일으키는 당사자가 지역적 제약을 받지않는 특징을 가진다. 즉 지구 반대편에 있는 사람과도 거래를 일으킬 수 있는 특징이다. 이 특징은 전자 상거래의 장점이자 단점이 될 수 있다. 특히 지역적을 블록화된 세계경제의 구조를 넘어서는 거래이기 때문에 환율, 배달, 지불방식, 거래물품의 품질, 환불, 소비자 보호, 문화적 차이 등에 있어서 해결해야 할 과제가 많이 발생한다.

전자 상거래의 중요성을 감안할 때 특히 대

금 결제를 원활하게 할 수 있는 설계 기법의 개발이 절실하다 하겠다. 따라서 전자 상거래에 있어서 전자식 대금결제 시스템 설계를 위해서는 여러가지 있겠지만 본 논문에서는 네트워크 설계, 보안 시스템 설계, 대금결재 시스템 설계, 사이버캐시 클라이언트 시스템 설계, 전자지불 시스템, 전자화폐 설계로 국한하였고, 연구방법으로는 이론적 고찰 및 설계를 해두었다.

Ⅱ. 이론적 고찰

1. 전자 상거래의 개요

일본 통상성에서는 Electronic Commerce를 그대로 전자 상거래로 해석하고 특별한 예고를 하지 않는한 일부 또는 전체 거래를 전자적으로 행하는 모든 것을 총칭해서 이 단어를 사용하고 있다.

전자 상거래(Electronic Commerce ; EC)의 기원은 미국의 Lawrence Livermore National Laboratory가 미국방부의 프로젝트를 수행하면서 처음으로 사용한 용어인데, 거래가 시작되면서부터 끝날 때까지 서류가 사용되지 않는 기업환경을 정보 기술에 의해 달성하려는데 그 목적이 있었다.

전자 상거래를 사용함으로써 나타나는 효과는 다음과 같다.

① 전자적으로 개방된 시장에서 공급업체간 경쟁이 강화되어 구매자의 비용이 절감 된다.

② 온라인으로 입찰정보 데이터베이스 접속, 입찰서 제출, 결과 조회가 가능하여 공급자의 비용이 절감된다.

③ 잠재고객에 대해 쉽고 저렴한 마케팅이 가능해 신규시장 개척이 용이하다.

④ 지리적인 거리를 초월한 새로운 시장 진입이 용이하다.

⑤ 비지니스과정들이 상호 연결되어 각 단계별 및 세부과정간의 시간지연이 제거되어 상거래의 신속성을 가져 오게 된다.

⑥ 제품사양이 표준화되고 경쟁이 심화되어 제품의 품질이 개선되며, 시장의 확대와 제품의 주문생산이 이루어져 제품의 다양화가 이루어진다.

⑦ JIT(Just-In-Time)와 통합화 제조기술을 통하여 제품이나 서비스에 대한 요구를 전자적으로 연결시킬 수 있으며, 재고관리 비용과 불량재고에 의한 위험이 줄어든다.

⑧ 관리과정의 표준화, 자동화, 대규모 통합을 통하여 간접비를 절감하여 원가통제에 도움을 준다.

⑨ 종이문서를 줄일뿐 아니라 실제로 움직이지 않고도 전자적으로 정보를 얻기 때문에 공해물질을 줄일 수 있게 되는 효과를 가져다 준다고 한다. 한편 전자 상거래 도입에 따른 결과는 제품 개발기간 단축, 기술 설계변경 감소, 신제품 시장 도입기간 단축, 품질 향상, 매출 영향증가, 수익성 증가가 나타난다고 하였다. (신동민, 1997)

전자 상거래를 실현하기 위해 필요한 기술은 정보시스템의 구축에 관한 모든 기술이라고 할 수 있으며, 이는 대략 5가지 서비스로 분류될 수 있다. 이를 살펴보면, 통신기술인 네트워크 액세스 서비스, 커뮤니케이션 서비스, 데이터 매니지먼트 서비스, 시큐리티 서비스, 프레젠테이션 서비스이다.

전자 상거래와 자주 비교되는 용어로는 전자문서교환(EDI)과 광속상거래(CALS)가 있다. 이들을 비교하여 보면 다음과 같다. 전자문서교환은 기존의 종이서류 대신에 컴퓨터가 읽을 수 있도록 표준화된 전자문서를 데이터통신망을 통하여 컴퓨터와 컴퓨터간에 교환하여, 재입력 과정없이 업무에 직접활용할 수 있도록 하는 새로운 전달방식이다.

광속상거래(CALS)는 모든 제조업체의 생산, 조달, 운영을 지원하는 통합정보시스템으로 전세계적 규모의 정보공유와 멀티미디어 정보를 교환할 수 있는 미래형 산업정보시스템이다.

김중한 외 3인(1997)에 의하면 전자 상거래에 대한 프레임 웍을 제시하고 있다. 이에는 첫째 보안/인증, 전자지불 등의 비지니스 서비스 기반구조, 둘째 EDI, E-mail, HTTP, FTP 등의 정보전달 기반구조, 셋째 공중망, 케이블 TV, 무선통신, 인터넷 등의 정보통신 기술 기반구조 그리고 이를 지원하는 정책및 법률, 개인 정보 보호와 같은 사회적 기반이 있다고 한다.

2. 전자 상거래의 유형

1) 인터넷 전자 상거래의 유형들을 아래에 요약하여 두었다.

(1) 광고 : 대부분 잘알려지고 접속횟수가 많은 사이트를 중심으로 아래와 같은 유형들이 있다.

- Yahoo (http://www.yahoo.com/)
- Netscape (http://home.netscape.com/)
- HotWired (http://www.hotwired.com/)
- 다물 (http://kang.dacom.co.kr/:한국)

(2) 쇼핑몰

- ISN (http://www.internet.net/)
- imall (http://www.imall.com/homepage.html)

(3) DB서비스

- Harvest : http://www.town.hall.org/brokers/www-home-pages/query.html
- lycos : http://www.lycos.com/
- opentext : http://opentext.uunet.ca:8080/omw.html
- webcrawler : http://webcrawler.com/
- infoseek : http://www.infoseek.com/
- mckinley : http://www.mckinley.com/

(4) 온라인 출판

- 중앙 : http://www.joongang.co.kr/
- 조선 : http://www.chosun.com/
- pathfinder : http://www.pathfinder.com/
- cyberspace주간지 우리 : http://www.scsn.net/wooree/wooree.htm
- infohaus : http://www.infohaus.com/index.html

(5) 오락

- theplace : http://www.theplace.com/
- matchmaking game : http://asylum.cid.com/matchmaking/
- online casino : http://www.netcasino.com/

2) 전자 상거래의 분류

전자 상거래의 분류 방법은 몇가지 되지만, 우선 거래 당사자와 네트워크의 형태를 중심으로 편의상 세 가지로 나누어 생각하고 있다. 그 첫 번째는 기업과 소비자간의 네트워크, 두 번째는 기업간의 불특정 다수 네트워크, 세 번째는 기업간의 특정 네트워크의 세 종류이다.

이들에 대해 아래에 좀더 구체적으로 고찰하여 두었다.

(1) 기업과 소비자간 네트워크

① 가상 점포(Virtual Mall)

기업과 소비자간 전자 상거래의 전형적인 예는 전자 점포(이것도 가상점포, 사이버 몰, 일렉트로닉스 숍 등으로 불리기도 한다.)를 개설하여 소비자들에게 상품 판매를 하거나 항공권, 철도, 호텔의 예약 서비스를 행하면서 동시에 결제도 행하는 소위 온라인 쇼핑이다.

상품 제공의 방법도 여러 가지로 일반 물품 판매의 경우는 당연 주문을 받아서, 후일 택배 등으로 제공하지만 컴퓨터 소프트웨어나 음악, 영상이 상품인 경우에는 네트워크를 통해서 그대로 제공하는 경우도 있다. 또 항공권 등의 티켓 예약의 경우에는 종이가 없는 것이 목적이기 때문에 예약 번호만 받아서 당일 실제로 서비스 제공을 받게 되는 것이다.

결제의 방법도 다양하다. 물건 판매의 경우는 네트워크 상에서 신용 카드로 결제하는 것이 일반적이지만 뱅킹 POS로 결제하는 것도 생각된다. 또 물건 판매의 경우는 인도하는 행위가 반드시 있기 때문에 인도시 지불이나 후일 우편대체나 은행송금이라는 수법을 취하는 것도 가능하다.

네트워크 상에서 상품이 제공되는 컴퓨터 소프트웨어 등의 경우는 거래의 성격상 신용 카드 결제나 뱅킹 POS가 통상일 것이다. 결국, 물건 판매인지 서비스인지의 거래 내용, 저가격인지 고가격인지의 가격, 소비자의 안정감, 여신 위험도를 취할지 취하지 않을지, 누가 위험도를 취할지, 이같은 조건들에 의해서 다양한 형태가 생각될 수 있다.

② KIOSK 단말

소비자를 대상으로 하는 전자 거래에서는 네트워크의 전자 점포에서 소비자가 PC를 통해서 물건을 사는 것이 전형적인 예이지만 현실적으로 점포와의 연속성을 갖는 것도 생각할 수 있다. 대표적인 예가 KIOSK 단말이다. 예를들면 기차역의 KIOSK나 24시간 영업 점포에 단말을 두어 전자 판매를 하는 것 등이다.

기차역의 KIOSK나 24시간 영업점포는 이것에 의해 매장 면적을 확장하거나, 인원을 늘리거나 하지 않으면서, 많은 수의 상품을 취급하는 것이 가능하고, 재고 위험성이 확대되는 일은 없다. 전용 단말기로 부터 직접 메이커나 서비스를 제공하는 기업에 주문을하는 구조가 가능하다.

이러한 점에서 말한다면 KIOSK 단말을 판매점이나 백화점에 설치하는것도 생각해 볼 수 있다. 잘 팔리는 상품을 중심으로 어느정도 양의 상품을 실제로 진열해 두고, 잘 팔리지 않는 것은 KIOSK 단말 내에 넣어두는 방법도 생각할 수 있다.

③ 전자 통화

전자통화는 다양한 정의를 갖고 있다. 가장 넓은 의미에서 본다면, 지금 행하여지고 있는 대체 계좌에 불입하는 데이터도 하나의 전자통화가 된다. 또 궁극적인 전자통화로서 어느 나라의 통화도 아닌 네트워크 상에서만 유통되는 통화도 이야기되고 있다. 그러나, 지금 우선 이 분야에서 주목받고 있는 전자통화 방식은 IC 카드에 은행 계좌로부터 현금을 전자 데이터 형태로 옮겨서, 전자 현금이라고 부를 수밖에 없는 이 IC 카드를 사용해서 현실 점포나 전자 점포 양쪽에서 결제에 사용하는 것이다.

이것에도 방법, 구조는 여러 가지가 있지만 제일 알기쉬운 것은 몬덱스사의 예이다. 이것은 PC를 통해서 혹은 은행의 전용 캐쉬 디스펜스를 통해서 자신의 IC 카드로 자신의 계좌로부터 전자현금을 인출해 간다. 당연히 IC 카드에 옮겨진 것만큼 은행의 계좌로부터 예금액은 줄어든다.

소비자는 전용의 전자 지갑에 IC카드를 주입하면, 예금되어있는 전자 현금이 얼마인지 알 수가 있다. 현실 점포에서는 전용의 카드리더, 레지스터가 있어서 구입가격만큼 이 IC 카드로부터 전자현금을 상점의 전용 레지스터로 옮긴다.

현실 점포만이 아니라 가상점포(네트워크 상의 전자상점)에서도 사용할 수 있다. PC와 여기에 접속되어 있는 카드리더와 같은 부속기기를 사용해서 가상점포에서 산 물건을 결제 할 수가 있다.

(2) 기업간의 불특정 다수 네트워크

편의상 기업과 소비자간 네트워크와 기업간 불특정 다수 네트워크를 나누어서 정리하고 있지만 사실은 본질적인 차이가 있는 것은 아니다. 전자점포에 의한 온라인 쇼핑 경우에도 소비자가 전자점포에 액세스하여 이 상품이 마음에 들면 전자점포에서 해당 제품을 제조 판매하고 있는 기업에 발주 데이터를 보낸다. 또 전자점포에서 결제를 위해 신용회사에 신용조회, 결제 데이터가 보내지기 때문에 전자점포 뒷편에서의 정보 흐름은 기업간 거래 그 자체가 된다.

한편, 기업간 거래의 경우는 일반적으로 거래액도 크기 때문에 시큐리티에 소요되는 비용은 크게 된다. 단, 어느 정도의 계속성이 인정되는 관계의 경우가 많기 때문에 인증 그 자체보다는 암호 기술의 강도가 요구될지도 모른다. 결제 시스템의 네트워크와 같이 사전에 장기적 신뢰관계가 형성된 정도의 특정성이 있는 경우에는 공개키 방식이 필수적인 것일지도 모른다. 다만 암호의 강도와 정보의 에러 없는 도착을 가능케하는 프로토콜이 중요하게 된다.

(3) 기업간의 특정 네트워크

기업간의 상거래는 통신망을 이용해 자사와 상대기업 간의 상거래에 필요한 정보를 전자적으로 주고받는 기존의 EDI(전자문서교환)나 최근들어 구축 움직임이 활발한 CALS(광속상거래)가 대표적이다.

종래 EDI와의 차이를 개념적으로 정리하면 EDI는 "정보의 교환"을 목적으로 하는것에 반해 CALS는 "정보의 공유"를 목적으로 한다. 따라서 EDI는 데이터 작성법, 데이터 전송방법을 표준화하면 달성되며 서로간의 시스템 내부에 관해서는 무관심해도 되지만, CALS의 경우에는 적어도 서로간의 데이터 보유 방법까지 표준화할 필요가 있으며, 서로간의 시스템 내부 구조를 어느정도 표준화하지 않으면 안된다. 더욱 이 업무흐름에 따라 정보공유 규칙에 맞는 데이터의 전송, 격납, 검색법을 표준화하여야 한다.

CALS는 예를들면 자동차, 항공기, 플랜트 엔지니어링, 전자부품 등 고도의 기술집약형 산업에 있어서 다수기업에 의한 공동개발이라는 업무 처리의 합리화에 위력을 발휘한다.

3. 전자 상거래 구성요소

1) 전자 시장에서의 구성요소

전자시장에서의 전자상거래 구성요소는 소비자가 PC상에서 정보를 검색할 수 있는 정보 검색 소프트웨어, 전자상거래를 하기위한 서버, 서버상의 전자 카탈로그, 전자 상점의 상품 광고 소프트웨어, 수주 및 지불 처리 소프트웨어, 수주 및 지불에 관계되는 서버의 여신시스템, 결제시스템, 상품 배송시스템 등으로 구성된다.

실제로 물리적인 제약을 받지 않는 것이 사이버 스페이스(가상공간) 이므로 한 개의 서버에 몇 개의 전자쇼핑몰을 넣는것도 가능하다. 소비자는 가정의 PC에서 인터넷으로 들어가 마음에드는 서버의 쇼핑몰로 접속하여 브라우저로 검색, 필요한것이나 마음에드는 상품을 발견하면 그 즉시 주문을 한다. 대금의 지불은 전자화폐, 신용카드, 전자우편환, 그리고 은행 송금등의 방법을 통해 처리된다.

인터넷상의 비즈니스, 전자 상거래를 활성화하기 위해서는 여러가지 문제들을 해결해야 한다. 네트워크 접속, 소프트웨어 하드웨어 플랫폼, 물품의 배달, 멀티미디어 정보 지불방식, 법률적 제약등의 많은 문제들을 해결해야 한다. 이런 여러가지 문제점들 가운데 아킬레스건과 같은 것이 바로 지불방식이다. 돈을 주고 받는 메카니즘이 명확히 제시되지 않으면 전자 상거래의 기본이 흔들리기 때문이다.

2) 전자 상거래 환경

판매회사 입장에서 볼때 보안 WWW 서버를 갖추는 것만으로 완전한 온라인 상거래 솔루션이 다 갖추어진 것은 아니다. 그러나 소비자 입장에서는 보안 유지 체계를 갖춘 WWW 브라우저를 갖추면 완벽한 솔루션이 될 수 있다. 즉 전자식 판매 실행과 완료를 지원하는데 필요한 전체적인 기반 시설들 즉, 대금 결제 대안을 솔루션에 통합시키는 것은 물론 신용카드 승인 네트워크들과의 연계가 갖추어 져야 한다.

Ⅲ. 전자식 대금 결제 시스템

1. 전자식 대금 결제 시스템의 개요

소비자가 온라인으로 돈을 사용할 수 있는 체제가 바로 전자식 대금 결제 시스템이다. 전자식 조회 시스템, 제3자에 의한 결제 시스템 또는 전자식 통화 시스템등이 바로 이런 전자식 결제 시스템으로서, 개인간의 가치(금액) 교환을 제공하는 수단들이다.

2. 퍼스트 버츄얼 인터넷 대금 결제 시스템

퍼스트 버츄얼이 만든 대금 결제 시스템은 IPS(Internet Payment System)로 인터넷을 통해 상품이나 서비스를 판매하는것 보다는 주로 정보 판매만을 추구하는 시스템이다. 자동화된 전화시스템을 이용해서 관련자의 대금 결제 정보를 수집하기 때문에 암호 방법(암호화나 디지털 서명)보다는 판매와 구매 감시 밀도를 높혀 사기 사례를 줄인다는 입장이다.

1) 기본가정

퍼스트 버츄얼 IPS는 세 가지 기본 가정에서 출발한다.

첫번째 가정은 퍼스트 버츄얼을 통해 판매되는 정보를 고객들이 살펴본 후 돈을 내지 않겠다는 결정을 내릴 경우 위험 부담은 있지만 실질적인 금액 손실은 없다. 그 상품에 대한 대금 결제가 이루어지지 않았다고 해서 판매 회사가 손해를 보는 것은 아니기 때문이다. 팔리지 않은 정보 상품에 대한 기회 비용은 전혀 들지 않는다. 그 정보를 찾는 사람이 그 정보를 구입할 의사가 없었지만 그 정보를 다른 사람에게 팔 수 있기 때문이다.

두번째 가정은 정보 구입자들은 다른 상품을 구입할 때와 마찬가지로 상품을 구입하기 전에 살펴보기를 원하기 마련인데, 디지털 판매에서 이를 위해 정보를 다운로드 받아 점검한 후 돈을 내고 살것인지의 여부를 결정해야 한다.

세 번째 가정은 구입과 판매는 단순해야 하고, 가능하면 시간과 비용, 노력면에서 부담이 없어야 한다는 점이다.

2) 자동화와 퍼스트 버츄얼

퍼스트 버츄얼 시스템은 전적으로 자동화된 전자메일 응답기와 WWW 상에서 이용되는 양식 그리고 자동화된 터미널 세션을 통해서 이루어지는 시스템이다. 구매자와 판매자 모두 이 시스템을 이용하면 실제 사람과의 대화나 접촉을 하지 않아도 된다.

3) 계정 구축

퍼스트 버츄얼이 IPS 계정을 구축하려면 인터넷에 전자 메일 연결이 되어 있어야 하지만 퍼스트 버츄얼 WWW 사이트나 리모트 터미널 세션(Telnet)을 통해서도 가능하다. 구매자로서 계정을 구축하려면 신용 카드가 있어야 하고 판매자 계정을 구축하려면 판매 대금이 결제되어 들어갈 계정에서 발행된 수표 대금 결제가 필요하다.

4) 퍼스트 버츄얼 거래처리 과정

퍼스트 버츄얼 IPS 거래처리 과정은 다음과 같다.

- 고객이 제시된 정보를 서버로부터 다운로드 받으려는 시도를 하면 서버에서 퍼스트 버츄얼 계정 번호를 요구한다.
- 판매 회사는 퍼스트 버츄얼을 통해 계정 식별자가 유효함을 확인하는 옵션을 갖는다. 서버는 퍼스트 버츄얼에 질의서를 보낸다. 퍼스트 버츄얼은 그 계정 ID가 유효함을 확인하는 응답 메시지를 보낸다.
- 제시된 정보는 판매 회사의 서버에서 구매자에게 직접 보내진다.
- 판매 회사의 서버는 퍼스트 버츄얼에 전자 메일 메시지를 보낸다. 이 메시지는 구매자와 판매자의 계정 ID, 구매 품목, 품목가격등 거래 세부 내역에 관한 메시지이다.
- 퍼스트 버츄얼은 고객에게 전자 메일 메시지를 보내서 고객이 그 품목 대금을 결제할 것인지 의사를 묻는다.
- 또 한가지 옵션인 '사기(fraud)'를 고객이 이용할 수 있다. 이 옵션을 이용하면 고객이 그 거래를 개시하지 않았다는 의사를 밝힐 수 있다. 그러면 거래가 무효화되고, 고객의 개정 ID는 취소되어 더 이상 사용할 수 없게된다.

5) 특징

퍼스트 버츄얼 시스템의 특징을 살펴보면 <표 1>과 같다. (김상균, 1997)

<표 1> 퍼스트 버추얼 시스템의 특징

항 목	설 명
시스템의 구성 메카니즘	인터넷 신용카드 지불 시스템
주요 특징	전자지불 처리과정 동안 사용자의 신용카드 정보가 유출되지 않음
익명성에 대한 보장	익명성 보장않됨
부가적인 하드웨어	필요없슴
부가적인 소프트웨어	필요없슴
기타 요구사항	비자 또는 마스터카드사의 신용카드 거래자여야 함
제한사항	없슴
암호화 방식	VirtualPIN

3. 사이버 캐시

1994년 8월에 창시된 사이버 캐시의 창립자들은 금융 기관 및 판매 회사들과 공조해서 인터넷에서 접근할 수 있고 수용할 만한 대금 결제 시스템의 제시를 목표로 설정했다. 사이버 캐시는 고객과 판매회사, 은행간의 안전한 대금 결제 통로를 제공하고 있다. 사이버 캐시를 인터넷 대금 결제 비즈니스의 페더럴 익스프레스(federal express)라고 한다. 인터넷을 통해 안전하고 효율적이며, 저렴한 대금 결제 방법들을 거의 즉각적으로 전달할 수 있는 시스템을 제공하기 때문이다.

사이버 캐시는 퍼스트 버츄얼의 문제점을 해결하여 인터넷에서 신용카드 결제를 실현했다. 사이버 캐시에서 제공하고 있는 서비스가 퍼스트 버츄얼과 다른점은 고도의 암호기술을 사용해 신용카드 정보를 직접 인터넷과 전달시켜 실시간 거래를 가능하게 한 것이다.

사이버 캐시를 이용하려는 고객은 클라이언트 소프트웨어를 다운 로드하고 적어도 하나의 신용 카드를 서비스에 연계시켜서 사이버 캐시 ID를 초기화한다. 이와 같은 서비스 요금은 소비자에게 부과되지 않는다. 사이버 캐

시 클라이언트 소프트웨어는 또한 브라우저 소프트웨어와도 함께 쓰일 수 있다.

CompuServe Mosaic in a Box 클라이언트에 들어 있는 디지털 지갑은 사이버 캐시와 호환 가능한 지갑이다.

사이버 캐시는 디지털 상거래를 간단하게 하고, 그와같은 서비스를 바탕으로 보안 유지를 가능하게 하고, 개인적이며 신뢰할만한 거래에 바탕을 두고 있다. 사이버 캐시가 제공하는 디지털 대금 결제 매카니즘에서는 특수한 클라이언트/서버 소프트웨어를 통해 구현된 공용/개인 키 암호화와 디지털 서명들을 비롯 현재적인 암호 테크놀로지들을 이용한다.

사이버 캐시가 소비자에게 제공하는 현실적인 가치들은 다음과 같다.

- 대금 결제 정보의 누출 방지(판매 회사에게조차 누설하지 않음)
- 편리한 전자식 지갑을 제공해서 대금 결

1) 물리적 시스템 구성

제 정보를 저장하므로 구매가 이루어질 때마다 정보를 재입력하지 않아도 가능
- 모든 거래를 처리, 추적, 다큐먼트화하는 거래 로그 유지 관리등이다.

4. 보안 시스템

인터넷이 보안에 취약한 이유는 인터넷에서 사용되는 오픈 환경을 지원하는 통신 프로토콜인 TCP/IP와 유닉스를 운영체제로 사용하기 때문이다. 인터넷에서 사용되는 표준통신 프로토콜인 TCP/IP는 공개되어 있어 인터넷과 연결된 다른 컴퓨터에 접속하는 것이 가능하다.

특히 인터넷상에서 전자상거래가 보편화되면 신용카드 번호, 비밀번호등 대금결제를 위한 중요한 개인정보가 네트워크에 노출될 수밖에 없으므로 안전한 각종 보안대책을 마련해야 한다.

1) 보안사고의 유형

(1) 정보유출

인터넷을 통해 송신자로 부터 먼곳의 수신자에게 정보를 전송할 경우 오픈 네트워크의 특성상 불특정 다수의 많은 컴퓨터와 네트워크를 통과하게 된다. 이 과정에서 해커와 같은 악의의 제3자가 불법 사용을 목적으로 네트워크상의 정보를 중간에서 가로챌 위험이 생긴다.

(2) 위장

네트워크를 통해 상거래에 필요한 정보를 주고받을 때 거래 당사자에 대한 진위 여부 확인이 어려워지므로 악의의 제3자가 사용자로 위장해 부정거래를 행할 위험이 크다

이와같은 위험을 막으려면 종래의 사용자 ID번호, 비밀번호 확인 외에 통신사업자의 서비스를 이용한 회선인증, 암호기술을 이용한 전자서명, 신뢰할 수 있는 제3자에 의한 본인 인증등과 같은 보안대책을 강구해야 한다.

(3) 변조

전자 상거래를 위해 구매자가 송신한 메시지가 전송 도중에 악의의 제3자에게 탈취되어 변조될 우려가 있다. 이를 위해서는 수신자가 메시지를 전송할 때 전자서명 기술을 이용해 전자적으로 서명하고, 수신자는 수신된 정보와 수신자의 전자서명을 대조해 변조 여부를 확인해야 한다.

(4) 시스템 침입

사용 권한이 없는 해커가 오픈 네트워크를 통해 판매자의 서버나 금융기관의 컴퓨터를 해킹할 수 있다.

이에 대한 대응책으로는 어떠한 종류의 불법침입도 저지할 수 있도록 방화벽을 설치해 인터넷망과 내부 네트워크 사이에 시스템 보호를 위한 장벽을 만들어 놓아야 한다.

2) 암호방식

현대의 암호방식은 크게 두 가지로 구분된다. 하나는 네트워크상에서 송신자가 특정 키로 암호화해 정보를 보내면 수신자가 이를 암호화에 사용된 동일키를 이용해 복호화하는 공통키 암호방식이다.

공통키 방식으로는 DES(data encryption standard), IDEA(international data encryption algorithm), RC2, RC4 등이 있다.

이 암호방식의 문제점은 암호해독을 위한 비밀키를 메시지 수신자에게 안전하게 전달하기가 어렵다는 것이다.

그래서 새롭게 등장한 것이 공개키 암호방

식이다. 수신자와 송신자가 암호화를 할 때 필요로 한는 두 개의 키중 한쪽의 키를 불특정 다수의 사람이 입수해서 암호화 또는 복호화 할 수 있도록 공개하는 방식이다. 대표적인 공개키 방식은 RSA 방식이 있다.

현재 대부분의 보안규약에서는 데이터를 암호화해서 전송하기 위한 이 두가지 방식을 적절히 결합시켜 사용하고 있다. 즉 전자서명이나 비밀키 암호방식에서 사용할 비밀키를 전달하는데에는 안전성이 뛰어난 공개키 암호방식을 사용하고 대량의 메시지 전체를 암호화하는 데에는 처리속도가 훨씬 빠른 공통키 암호방식을 병행해서 사용한다.

3) 전자서명

거래 당사자의 본인 확인을 위해서는 일반 상거래의 인감과 같은 기능이 필요한데 이를 암호기술을 응용한 전자서명이 대신하고 있다.

전자서명의 일종으로서 전자화폐인 E캐시 시스템을 운용하고 있는 디지캐시사가 고안한 블라인드(blind) 전자서명이 있다.

이 방식은 일반적인 문서형식과 비교하면, 봉투내에 비밀문서를 넣어 봉인하고 서명자에게는 이 문서의 내용을 보여주지 않고 봉투에 문서의 진정성을 증명하는 서명을 하도록 하는것이다.

4) 인증

인증은 송신자의 메시지가 전송도중에 위조·변조되지 않고 원문과 다름없음을 확인하는 메시지 인증 기능과 메시지를 보낸 사람이 정당한 수신자임을 확인하는 사용자인증 기능으로 구분된다. 또한 메시지를 받은 사람이 메시지 수신 사실을 부인하는 것을 방지하는 수신자 부인방지 기능도 인증기능 이다.

5. 전자화폐

전자화폐는 일반적으로 전자현금, 전자지갑, 디지털 머니등 다양한 용어로 사용되고 있다. 따라서 몇가지 분류기준으로 현재 실험 및 실용화되고 있는 각종 전자화폐를 분류하고, 각 유형의 성격 및 특징에 대해 설명하면 다음과 같다.

1) IC카드형 전자화폐

세계 각국에서는 여러 가지 종류의 IC카드형 전자화폐가 실험·사용되고 있는데 그중 몬덱스는 우리가 사용하고 있는 현금과 그 성격이 매우 유사하다는 점에서 가장 발달된 형태의 전자화폐라 할 수 있다.

IC카드형 전자화폐는 휴대가 간편하다는 점에서 일반 상점에서 물건을 구매 하기가 편하다는 장점이 있으나 IC카드를 전자화폐의 보관처로서 사용하기 위해서는 IC카드 및 IC카드 판독기 등을 보급시켜야 하기 때문에 막대한 투자가 필요하다. 따라서 IC카드형 전자화폐는 이러한 투자비용을 누가 부담하는가(소비자, 상점, 전자화폐 발행자)가 보급의 관건이다.

2) 네트워크형 전자화폐

컴퓨터 하드디스크에 정보가 저장되어 통신회선을 통해 각종 결제에 사용되는 것을 일컷는다. 원격지 송금에는 편리하지만 직접 소지하고 상점에서 물건을 사는 것은 불가능하다. 네트워크형 전자화폐의 장점은 전자화폐용 소프트웨어만을 구비하면 되기 때문에 보급을 위해 막대한 신규투자가 필요하지 않는다는 점이다.

네트워크형 전자화폐는 컴퓨터 통신상에서의 각종 결제행위에 사용되는 전자화폐를 말하며 네트워크형 전자화폐는 기존의 결제수단을 대체하는 형태에 따라 현금형, 신용카드형, 수표형으로 분류된다.

3) 전자화폐의 분류

다음 <표 2>에 전자화폐를 요약 정리하여 두었다.

Ⅳ. 전자 상거래에 있어서 전자식 대금 결제 시스템 설계

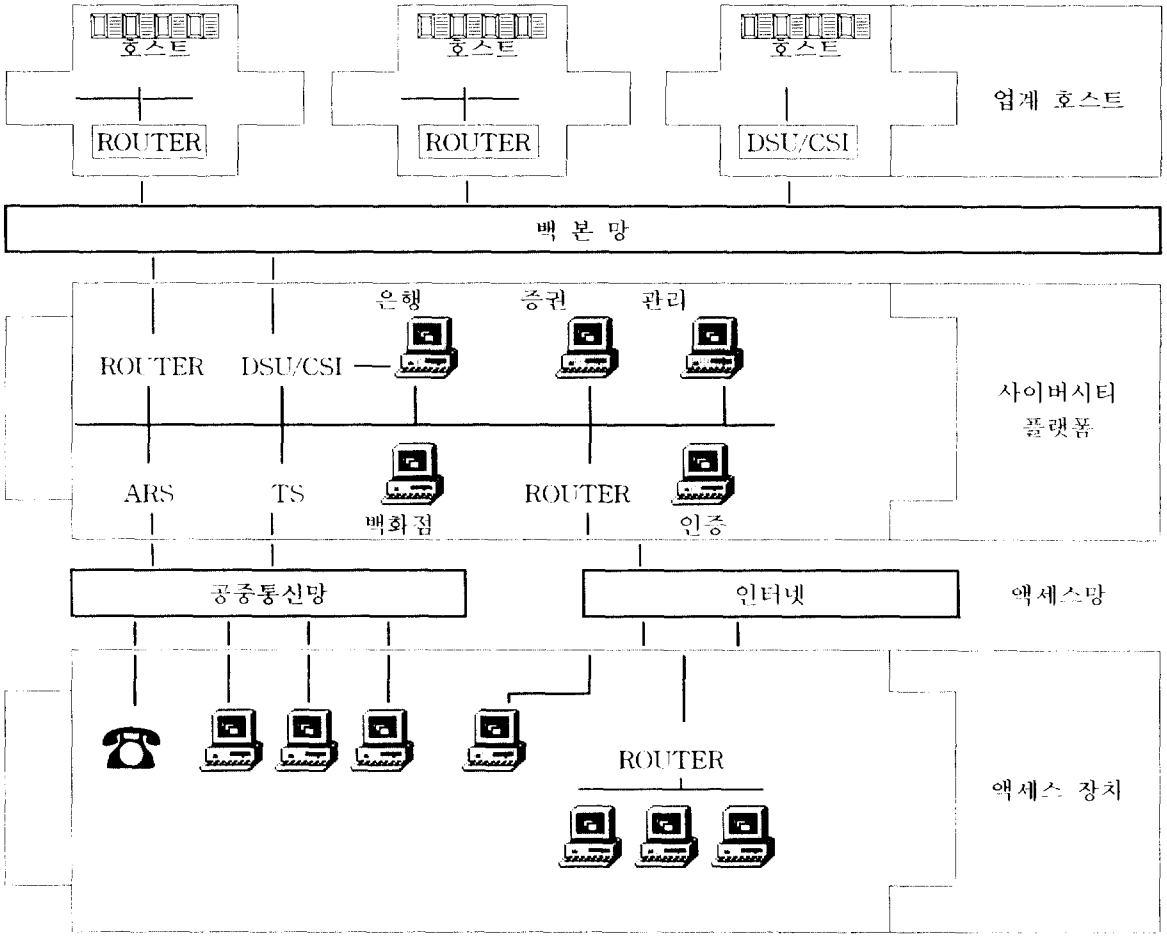
1. 네트워크 설계

앞에서 고찰한 이론적 근거를 토대로 전자 상거래에 있어서 전자식 대금 결제 시스템을 설계하기 위하여 네트워크 설계 부분에 대해서는 물리적 시스템 구성과 인증기관, 전자상

<표 2> 전자화폐의 분류

전자화폐의 유형을 살펴보면 <표 2>와 같다.

구 분		화폐명	발행기관	주요특징
IC 카드형	현금형	몬덱스	내셔널 웨스트민스터, 미들랜드은행 등의 공동출자회사	전용기기(Wallet) 또는 몬덱스용 전화기를 이용하여 카드간 가치이전 가능. 1995년 7월 이후 실험사용 중
	선불 카드형	비자 캐시카드	다수의 미국 지방은행	96년 ATM, 전화기 등을 통해 가치재충전이 가능한 카드를 발행
네트워크형	현금형	E캐시	네덜란드의 디지캐시사와 미국의 마크 크웨인은행	네트워크상에 가상의 화폐를 생성시켜 이것을 전자결제에 이용. 1995년 부터 실용화됨.
	신용 카드형	퍼스트 버츄얼	미국의 퍼스트 버츄얼사	일종의 회원등록처럼 신용카드 번호를 사전에 등록하고 전용의 회원번호에 따라 인터넷상에서 결제함.
		사이버캐시	미국의 사이버캐시사	무상으로 제공된 암호통신 소프트웨어를 이용해 인터넷상에서 결제함
	전자 수표형	네트빌	미국의 카네기멜론 대학	인터넷상에서 기존의 가계당좌수표 사용을 가능하게 함.



<그림 1> 물리적 시스템 구성

점, 전자지불, 전자 인증서 발급체계, 전자 상거래 동작체계 시스템을 중심으로 <그림 1>에서 <그림 6>까지 설계해 두었다.

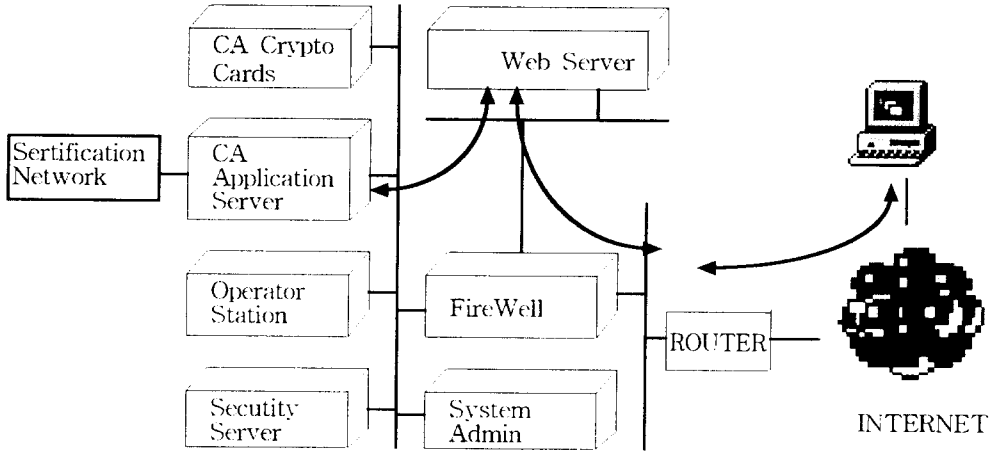
<그림 1>에서는 액세스 장치로는 PC, LAN station, 전화이며, 액세스 및 백본망은 공중통신망 및 인터넷을 이용한다. 업계 호스트는 정보 source를 제공하며, 전자 상거래 플랫폼은 중앙집중형 온라인 방식으로 요소시스템 및 네트워킹 장치으로 구성되어 있으며 세부적인 내용은 다음과 같다.

- Web Server : CA Applications Server의 Frontend
- CA Application Server : 온라인 Certificate 발급
- CA Crypto Card : 암호화 key의 생성, 저장, 삭제 및 암호화
- Operator Station : 데이터 입력, 수정, 변경, 삭제 등을 위한 운용자 시스템
- Security Server : 액세스 제어 및 방화벽 제어 서버, 시스템 로그 데이터 수집
- System Administration : 시스템 관리의 모니터
- Firewall : 외부의 침입 및 불법적인 액세스 차단을 위한 액세스 제어

2) 인증기관 시스템 구성

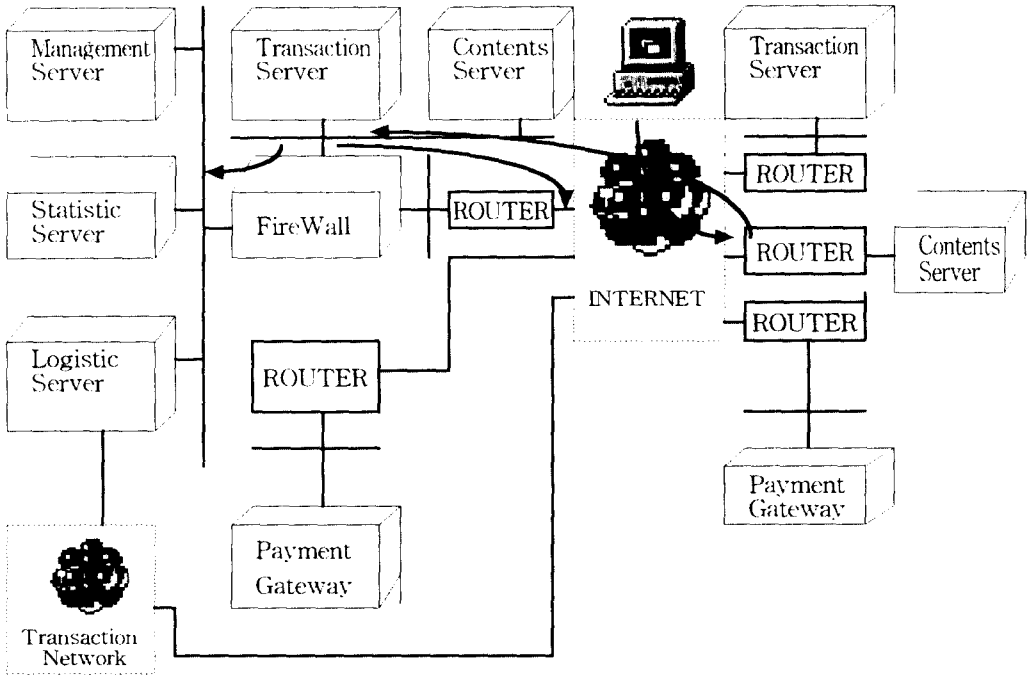
<그림 2>의 세부내용은 다음과 같다.

- 인증기관 시스템 : 전자증명서 발급
- 가상백화점 시스템 : catalog, transaction, 택배, 관리, 통계 서비스 제공
- 지불시스템 : 신용카드, 직불타드, 계좌이체, 전자화폐등 용도별 지불 서비스
- 고객 시스템 : web browser 기반의 전자지갑 (지불 수단별 전자지갑 장착)



<그림 2> 인증기관 시스템

3) 전자상점 시스템 구성

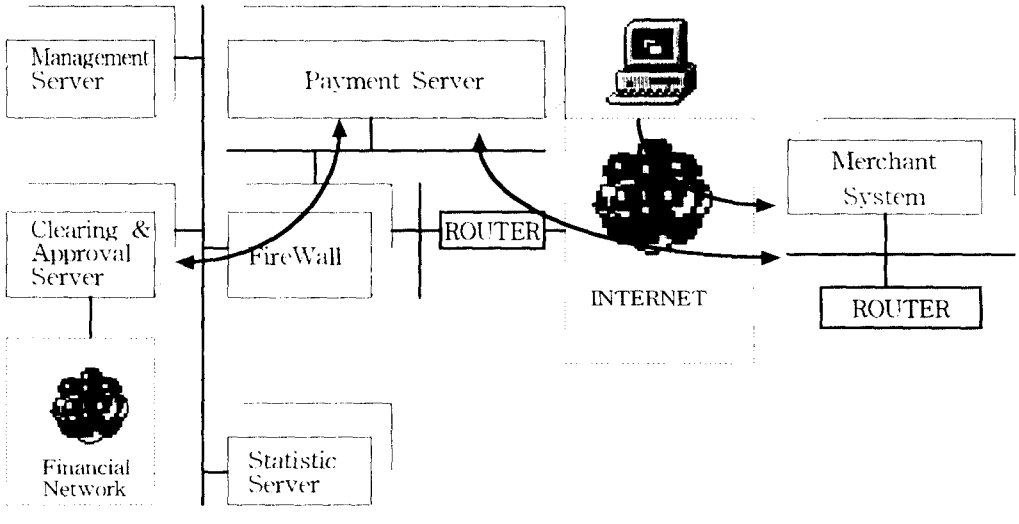


<그림 3> 전자상점 시스템 구성

<그림 3>의 세부내용은 다음과 같다.

- Contents Server : 유통사업자의 Shopping Mall 및 Catalog 서비스
- Transaction Server : Payment System과의 지불처리 및 각종 지불수단 제공
- Management Server : 거래에 따른 각종 로그정보 및 시스템 관리, 영수증 발급 및 관리
- Statistic Server : 로그정보 가공을 통한 통계치 가공정보 제공
- Logistic Server : 거래에 따른 택배지령 및 추적등

4) 전자지불 시스템 구성

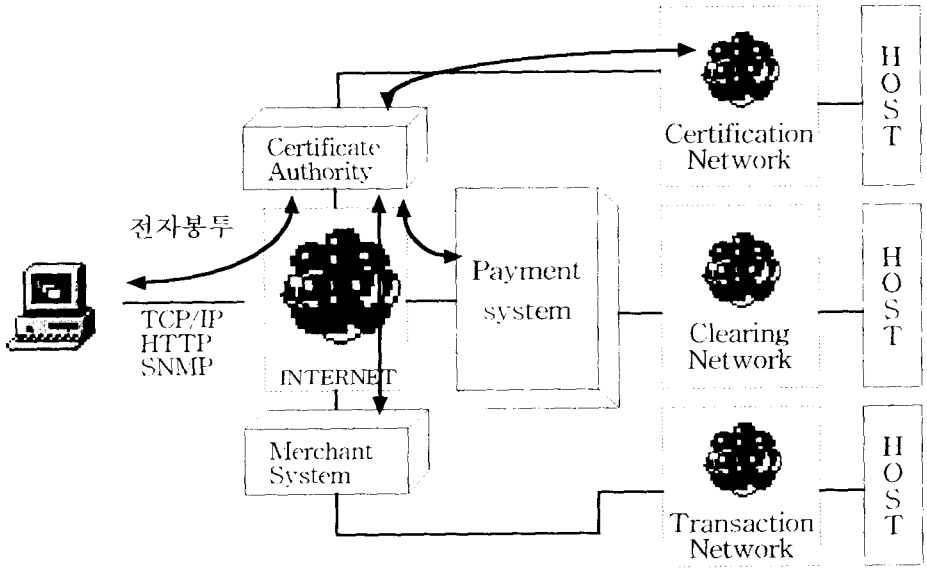


<그림 4> 전자지불 시스템 구성

<그림 4>의 세부내용은 다음과 같다.

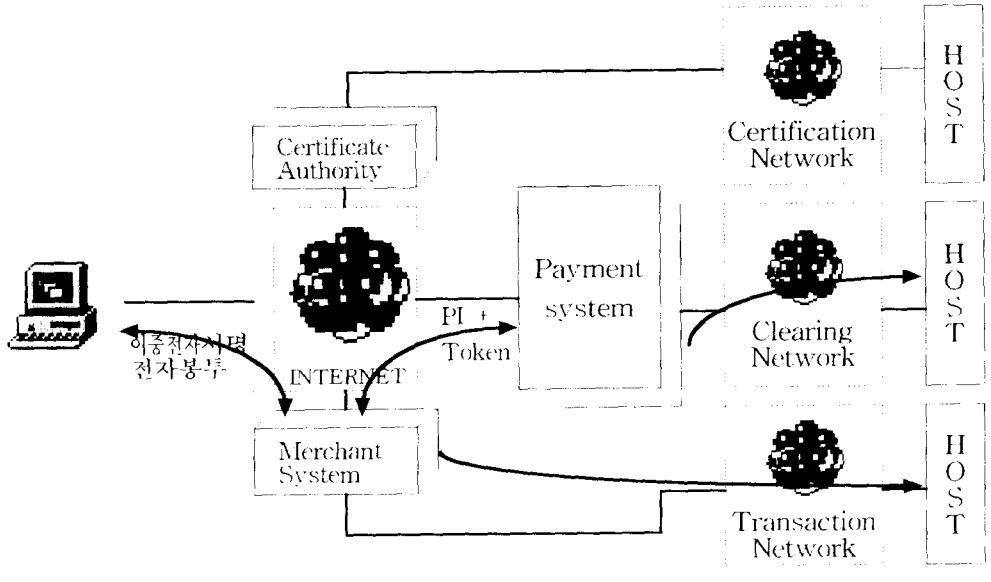
- Payment Server : 지불정보(payment information)처리, 거래 Token 생성 및 전송
- Clearing & Approval Server : 거래승인 처리, 지불 Token 매입 및 정산처리
- Management Server : 거래에 따른 각종 로그정보 및 시스템 관리
- Staistic Server : 로그정보 가공을 통한 통계치 가공정보 제공

5) 전자 인증서 발급체계



<그림 5> 전자 인증서 발급체계

6) 전자상거래 동작체계 : 온라인 지불 시스템 방식



<그림 6> 전자상거래 동작체계

2. 보안 시스템 설계

전자 상거래에 따른 대금지불을 네트워크상에서 가능하게 하는 전자지불 서비스가 인터넷 비즈니스로 성공하려면 무엇보다도 완벽한 보안이 전제되어야 한다. 최근 전자화폐를 비롯한 전자지불 서비스를 제공하는 회사들은 최신 암호기술과 보안규약을 사용해 나름대로의 보안대책을 수립하고 이를 실제 시스템에 적용하고 있다.

특히 암호기술 중에서도 공개키 암호를 이용해 인터넷을 오가는 정보에 대한 여러 가지 해킹 위험으로부터 보호하고 전자 서명 기술을 이용해 정보의 위조·변조를 막고 있다.

각 전자지불·전자화폐 서비스 업체에서 사용하고 있는 보안대책을 살펴보면 다음과 같다.

1) 몬덱스 카드의 보안대책

영국에서는 1995년 7월부터 IC카드를 이용한 몬덱스라고 불리는 세계 최초의 선불카드식 전자화폐 시스템이 시행되고 있다. 이 방식에서는 금액에 상당하는 숫자가 IC카드에 기억되고 화폐가치의 이동은 네트워크를 통해 이루어 진다.

최근 몬덱스 카드 시스템에서는 안전한 전자화폐 시스템을 구현하기 위해 공개키와 비밀키를 같이 사용한다. 소비자, 판매자 및 발행기관은 각각 공개키와 비밀키를 준비해 상대방이 암호화 또는 복호화에 사용할 공개키를 인증기관에 등록하고 자신이 사용할 비밀키는 각자가 관리하는 형태로 되어 있다. 또한 소비자 및 판매자의 IC카드에 자신의 비밀키 및 공개키, 공개키 증명서와 함께 발행자의 공개키를 격납해주고 필요할 때 이들 키를 사용한다.

2) 디지캐시의 보안대책

디지캐시(Digicash)에서 발행하는 E캐시(Ecash)는 물리적인 존재없이 네트워크를 통해 먼곳에 있는 상대방에게 전자화폐를 전달하는 것으로 대금을 지불하게 된다. 따라서 화폐에 대한 실물 확인이 불가능하므로 이에따른 보안사고에 철저히 대비할 수 있는 시스템 구성이 요구된다.

E캐시에 익명성을 보장하기 위해서는 은행이 일련번호 자체를 몰라도 사용자가 발행한 화폐임을 인증할 수 있는 기능을 가지고 있어야 한다. 이러한 전자화폐에 사용되는 일련번호는 이용자가 부여하는데, 익명성을 보장하기 위해 일련번호에 블라인드 팩터(blind factor)라는 임의의 숫자를 부가해 암호화 한다. 이렇게 사용자가 생성한 일련번호는 은행이 전자서명하고 나서 사용자에게 되돌려 보낸다.

사용자는 인터넷에서 물건을 구입하고 발행은행의 전자서명이 붙은 전자화폐로써 판매자에게 구입대금을 지불한다. 전자화폐가 사용되면 발행은행은 전자서명의 유효성을 확인하고 그 금액을 계좌에서 인출해 판매자에게 지불한다. 만일 이 경우 전자화폐에 사용된 일련번호가 발행은행의 전자화폐 사용 리스트에 이미 등록되어 있다면 그 전자화폐는 이중 사용되었다고 볼 수 있다.

전자화폐 발행은 이미 발행한 전자화폐가 사용되기 전까지는 누가 그 전자화폐를 사용했는지 알 수 없다. 따라서 E캐시와 같은 전자화폐 시스템에서는 사용자의 익명성이 보장되는 것이다.

3) 퍼스트 버츄얼의 보안대책

퍼스트 버츄얼은 별도의 전자 상거래용 보안 소프트웨어를 사용하지 않고, 신용 카드 번호등 중요한 정보는 인터넷이 아닌 전화나 팩스등 일반 통신기기를 이용해 오프라인으로 보내게 한다.

아직까지 인터넷은 보안상 안전하지 못하다고 판단하고 있기 때문이다. 또한 데이터 암호화와 전자서명등 암호기술을 이용하게 되면 처리절차가 복잡하고 별도의 추가 비용이 소요되기 때문에 사용자의 지불정보등 중요한 정보는 인터넷을 통해 전송하지 않도록 시스템을 구성했다.

최초 등록할 때에만 인터넷을 이용해 사용자의 결제 계좌번호 및 전자우편 주소등의 데이터를 퍼스트 버츄얼로 보내 대금지불용 계좌를 등록한다. 퍼스트 버츄얼 구매자에게 보내는 거래 확인정보는 전자우편을 이용하고 구매자가 이를 확인하면 결제가 개시된다. 이 과정에서 구매자가 실제 거래와 일치하지 않는 부당한 거래확인정보를 받게되면 구매자의 ID가 절취된 것으로 간주해 해당 ID를 무효화 시킨다.

또 다른 보안사고의 가능성으로는 해커가 전자우편을 전송 도중 가로채어 우편내용을 변경시키는 것도 고려해 볼 수 있다. 그러나 타인의 이름을 사용해 전자우편을 위조해 전송하는 것은 비교적 간단하지만, 전송 도중 전자우편의 내용을 변경하는 해킹 행위는 쉽지않아 발생 위험성은 거의 없다. 그러나 사용자의 ID가 도중에 위조되는 것은 현실적으로 발생할 가능성이 있다.

특히 이러한 보안사고는 사용자가 지불청구서를 받아보고 나서야 확인할 수 있기 때문에 사고에 대한 사전 확인이 어렵다. 그래서 퍼서트 버츄얼에서는 이러한 사기 행위에 대해서는 일정기간 이내에 사용자의 신청이 있으면 지불 취소를 인정하고 있다.

4) 사이버 캐시의 보안대책

사이버 캐시는 암호화와 전자서명 기능을 사용해 데이터 보호를 행하기 때문에 RSA 공개키와 DES 공통키 암호 시스템을 같이 사용하고 있다. 사이버 캐시의 보안 소프트웨어는 미국 정부로부터 인가를 받은 암호기술을 이용하고 있다. 즉 56비트 DES와 768비트 RSA를 사용하고, 또한 모든 전자 상거래는 MD5와 RSA 전자서명으로 인증된다. 사이버 캐시의 소프트웨어는 768비트 RSA키를 사용해 보안기능이 한층 강화된 버전으로서 국경을 초월한 전자 상거래 활성화를 위해 특별히 해외로의 수출을 미국정부로 부터 승인받았다.

사이버 캐시는 판매자와 구매자 사이, 판매자와 사이버 캐시 사이의 메시지 전송 도중 메시지가 탈취되거나 변경되는 위험을 막을 수 있다. 그러나 다른 시스템과 마찬가지로 사이버 캐시도 시스템에 접속할 때는 패스워드를 사용하고 있어 해커에게 노출될 가능성이 있으므로 시스템 공개를 제한하고 있고 사용자의 중요한 정보는 이를통해 입력하지 않도록 구성되어 있다.

5) 비자와 마스터카드의 보안대책

인터넷상에서 신용 카드를 이용한 대금 결제를 안전하게 수행하기 위해 활용되고 있는 암호기술로서는 비자 카드와 마이크로소프트사가 공동 개발한 STT(secure transaction technology)를 비롯해 마스터 카드와 넷스케이프, IBM 등이 공동 개발한 SEPP(secure electronic payment protocol)가 있다. 그러나 양대 그룹은 1996년 2월에 공동 제휴해 SET(secure dlectronic transaction)을 개발하여 암호기술을 통일했다. 세계 유수의 신용 카드 회사인 비자와 마스트카드가 보안표준을 공동으로 개발함에 따라 인터넷 전자 상거래의 실용화가 더욱 앞당겨지게 되었다.

비자와 마스터카드는 그 동안 독자적으로 이 기술을 개발해왔으나 거래은행과 가맹점이 단일규격을 요구함에 따라 SET라는 보안 표준안을 공동으로 개발했다. SET란 네트워크 형태에 상관없이 카드 사용에 대한 안전을 보장하는 개방된 표준 명세로서, 개인 사용정보나 거래정보를 보호할 수 있는 공용적인 암호키 사용을 포함하고 있다.

6) SFNB 보안대책

세계 최초의 가상은행인 SFNB(Security First Network Bank)는 보안에 가장 큰 비중을 두고 미국방성이 정부보안기관에서 사용하던 보안기술을 도입하여 완벽한 보안체제를 갖추고 있다. 인터넷과 같은 불특정 다수가 사용하는 네트워크상에서 안전한 은행거래를 유지하기 위해서는 네트워크의 여러 계층에 걸쳐 다단계로 보안기능이 수행되어야 한다.

우선 1단계 보안은 사용자 PC의 웹 브라우저와 은행 서버 사이의 데이터 흐름에 대한 안정성을 보장하기 위하여 SSL(Secure Sockets Layer) 프로토콜을 사용한다.

두번째의 보안장치로는 거래나 개인정보에 대한 어떠한 종류의 침입도 저지할 수 있도록 필터링 라우터와 방화벽을 통해 인터넷과 은행 내부 네트워크 사이에 보안장벽을 만들어 놓았다.

세번째 보안장치로는 은행내 컴퓨터에서 발생하는 보안문제를 해결하기 위하여 시큐어웨어사의 시큐어웹 시스템이 구축되어 있다. 이 시스템을 이용하여 은행 서버에 구축되어 있는 각종 거래나 고객 정보를 보호하고 있다.

3. 대금 결제 시스템 설계

1) 기존방식 채택

전형적으로 현재의 소비자들이 상품과 서비

스 대금을 결제하는 방법은 현금, 수표, 신용 카드 등을 이용하는 것이다.

신용 카드는 세 가지 방법 중에서 온라인 거래에 채택하기 가장 쉬운 방법이다. 이는 전화 거래나 우편 주문 등에 신용 카드들을 이용하는데 익숙해져 있기 때문일 것이다. 신용 카드로 거래할 때는 소비자가 주문을 낼 때 유효한 신용 카드 번호와 만기일(그리고 청구 용지, 수신처, 주소) 등을 제시해야 한다.

현금을 디지털화하는 과정에서 해결해야할 다른 문제들이 있다. 이 과정에서는 실제 화폐를 디지털 '코인'으로 대체시킨다. 디지털 코인은 데이터 청크(chunk)들로 재현된다. 가장 확실한 방법은 중앙은행이 관리하는 테두리 내에서 디지털 서명과 공용키 암호화를 이용하는 체계이다.

2) 상거래 환경 구축

온라인 상거래 환경은 단순한 결제정보 전송 이상의 것이어야 한다. 그렇지만 온라인 상거래 환경의 토대는 바로 그 대금 결제 정보의 전송과 데이터 전송의 보안 유지이다.

대금 결제 정보는 실질적인 전송 보안 유지를 요하는 유일한 거래 부분이지만 선적, 지시, 제시 가격, 디지털 서명을 통한 기타 주문 정보와 같은 정보를 보증하는 방법들을 제공하는 시스템들이 있다. 그러나 보안 유지는 주문 정보를 암호화하는 것을 넘어, 소비자 신용 카드 정보를 받을 수 있는 권한을 부여받은 판매 회사로 가장한 범죄자들을 따돌릴 수 있어야 한다. 더욱 중요한 것은 신용 정보를 저장하고 있는 판매 회사의 서버 시스템의 보안 유지이다.

전체적인 솔루션은 상거래 환경이 가능한 한 융통성을 갖추고 시장과 업종에 맞는 서로 다른 대금 결제 방안들을 수용하는 것이다. 그 다음에는 판매 회사가 고객에 대한 정보를 수집하는데 도움이 되는 상거래 환경이 되어야 한다. 주문에 대한 조치들을 생성하는 종합적인 환경이 되어야 한다. 주문에 대한 조치들은 생성하는 종합적인 비즈니스 환경 속에서 상거래 환경을 통합시켜야 한다.

3) 디지털 통화와 대금 결제 시스템

전자 상거래 서버의 보안 유지 목적은 인터넷을 통해 전송되는 거래 데이터를 보호하는 것이지만 디지털 통화와 기타 디지털 대금 결제 체계의 목적은 인터넷을 통해 안전하게 액면 금액을 운반하는 것이다. 디지털 통화와 대금 결제 시스템은 인터넷 보안 서버나 전자 상거래 환경과 상반되는 방식만을 취하는 것만은 아니다. 디지털 통화와 대금 결제 시스템은 액면 금액을 교환할 수 있는 또 다른 방법을 추가함으로써 인터넷 보안 서버 및 상거래 환경과 같은 상품을 보완할 수 있다.

이런 유형의 서비스를 제공하는 업체들이 취하는 접근법은 두 가지이다. 하나는 고객의 대금 결제 방법(신용 카드, 당좌예금 또는 기타 자금 소스)을 서비스 프로바이더가 관리하는 온라인 ID에 연계 시키는 것이다. 그러면 고객에게 물건을 파는 판매회사들은 그 서비스 프로바이더를 통해 대금 결제 정보를 확인할 수 있다. 서비스 프로바이더는 승인과 어음 교환 서비스등도 제공한다.

직불 카드를 신용 카드와 거의 흡사하게 이용할 수 있는 것처럼, 디지털 조회 방식도 그와 같은 테크닉들을 이용할 수 있다. 즉 소비자들이 카드를 판매 회사에게 제시하면 그 판매 회사는 구매에 대한 승인을 받아야 한다. 대금 결제 방식은 월말에 청구서를 발행하는 것이 아니고 구매 승인이 떨어지는 즉시 고객의 계좌에서 인출된다.

실제 디지털 통화를 이용하는 방식은 대금 결제 시스템 이용 방식과는 상반된다. 디지털 통화 서비스를 제공하는 금융 기관에 계좌를 개설하면 누구든지 디지털 통화를 이용할 수 있다. 관계자의 컴퓨터 상에서 클라이언트 소프트웨어를 이용해서 계좌에서 돈을 인출하고, 잔액을 조회하고, 액면 금액이 입금되는 '디지털 지갑'을 유지 관리한다.

사용자와 은행간의 현금 교환에는 암호 기술을 이용한다. 디지털 서명으로 현금 양도를 보증하고 거래를 암호화 시킬 수 있다. 현금이 은행에서 사용자에게 배포될 때는 '디지털 코인' 형식으로 이루어진다. 디지털 코인은 디지털 서명을 받은 일련 번호로서 은행에 등록되어 있다.

4. 사이버 캐시 클라이언트 시스템 설계

1) 소프트웨어

사이버 캐시 클라이언트 소프트웨어는 ID 구축으로 부터 신용 카드를 거래인과 연계시키는 것, 그리고 거래 로그를 통해서 사이버 캐시 거래 정보를 추적하는 것에 이르기 까지 소비자 거래를 처리한다. 또한 클라이언트 소프트웨어에는 사이버 캐시 서비스를 개별화하고 관리하기 위한 기타 관리 및 구성 옵션이 들어 있어서 사이버 캐시 퍼스나(Persona) 정보를 백업하고 클라이언트 최신 버전으로 다운 로드 한다.

사이버 캐시 판매 회사측의 서버 구축이 제대로 이루어져야 판매 회사가 사이버 캐시 거래를 수용할 수 있다. 서버 구축 과정은 사이버 캐시 PAY 버튼을 WWW 서버의 오더링 페이지에 내장시키는 것은 물론 사이버 캐시 소프트웨어를 인스톨하는 과정 전체를 의미한다. 일단 인스톨이 끝나고 테스트를 성공적으로 마치면 판매 회사는 사이버 캐시 수용을 시작할 수 있다.

2) 대금 결제 정보 접근방법

사이버 캐시를 이용하기 위해서는 반드시 사이버 캐시 클라이언트 애플리케이션을 인스톨하고 구성해야한다.

1995년 중반에 구현된 사이버 캐시를 이용하려는 고객들은 클라이언트 소프트웨어를 CyberCash WWW 사이트에서 다운로드 받아서 자신들의 PC에 인스톨했다. 1995년 7월을 기준한 버전에서도 아직 전자식 현금/수표 전송을 구현하고 있지는 않지만 인터넷을 통한 신용 카드로 구매할 경우에는 완벽한 기능을 보이고 있다.

사이버 캐시는 CompuServe Mosaic in a Box를 비롯해서 인터넷 입문 키트와 번들로 클라이언트 소프트웨어를 배포하고 있다. 초기에는 CyberCash WWW 사이트에서 온라인으로 배포했다.

사이버 캐시의 웹 사이트에 연결하려면 다음으로 링크한다.

http://www.cybercash.com

일단 클라이언트 소프트웨어를 인스톨했으면, 소비자들은 CyberCash PAY 버튼을 이용해서 선택 품목에 대한 대금을 결제 할 수 있다.

3) 구성과 관리 대안

사용자는 사이버 캐시 클라이언트 애플리케이션으로 신용 카드 정보를 이용할 수 있고 링크시킬 수 있으므로 새로운 카드를 추가하거나 기존의 카드를 지울 수 있다. 관리 기능에는 정보 수정에서 부터 사이버 캐시 데이터 백업이나 복구, 최신 애플리케이션 버전 확보에 이르는 모든 것이 포함된다.

더욱 중요한 것은 클라이언트가 거래 로그에서 거래 정보를 추적한다는 것이다. 거래마다 그 정보는 로그에서 유지 관리되고, 필요에 따라 인쇄 또는 취소될 수 있다.

판매 회사용 소프트웨어의 관리 기능들로 다음과 같은 사항들을 실행할 수 있다.

- 주문 데이터 단위로 주문을 확인 검토한다.
- 지원하는 거래들을 처리한다.
- 전화 주문을 받았을 때처럼 판매회사 위주의 거래를 수행한다.

이 소프트웨어의 다른 기능으로는 암호화와 해독, 디지털 서명, 확인 등에 필요한 암호 수행 기능이 있다는 것이다. 또, 정보 파일, 테스트 소프트웨어, 주문을 로그할 수 있는 데이터베이스 프로그램 그리고 판매 회사 쇼핑 페이지 샘플 등도 들어있다.

가장 중요한 것은 사이버 캐시가 인터넷을 통한 신용 카드 거래를 위한 비자/마스터 카드 표준을 따르는 입장이며, 무엇보다도 사이버 캐시는 인터넷 상거래에 안전하고 단순하며 수용할만한 솔루션을 제공한다는 입장이다. (Loshin, 1997)

(4) 구매 및 판매전략

사이버 캐시 고객들은 사이버 캐시 로고를 디스플레이하고 있는 판매회사들의 WWW 사이트들을 브라우징함으로써 인터넷을 통해 상품을 구매할 수 있다.

고객들은 구매 품목을 선택한 후 판매 회사의 대금 결제 페이지로가서 사이버 캐시 PAY 버튼을 클릭한다. 그러면 서버에서 고객의 시스템으로 거래 정보 전송이 개시되어 사이버 캐시 클라이언트 애플리케이션이 시작된다. 이 애플리케이션은 주문 번호와 판매 회사의 사

이버 캐시 ID 그리고 구매 금액 등의 대금 결제 요구를 디스플레이 한다.

계속해서 고객이 구매 과정을 속행하면 애플리케이션 소프트웨어는 판매 회사에서 받은 모든 정보(가격, 신용 카드)와 고객의 대금 결제 정보를 모아서 디스플레이한다.

신용 카드를 선정했으면 클라이언트 소프트웨어는 그 정보를 암호화 서명해서 판매회사에게 보낸다. 판매회사가 받은 서명된 메시지의 내용이 바로 구입 품목과 암호화되어 서명된 대금 결제 정보이다. 이 두가지 정보는 확인을 받는다. 대금 결제 정보는 사이버 캐시 대금 결제 서버에 보내진다.

사이버 캐시에서 정보를 은행으로 보낸다. 판매회사는 수초 내에 승인을 받는다. 거래가 성공적으로 완료되면 거래 정보 정리와 함께 클라이언트에게 다시 보고한다.

5. 전자지불 시스템

1) 인터넷상의 전자지불 시스템

(1) 전자 현금 시스템

이상적인 사이버 스페이스에서의 지불방식으로 생각되고 있는 전자현금 시스템이 있다. 네덜란드의 디지캐시(DigiCash)사에서 만든 전자현금(Ecash)과 캘리포니아 대학에서 개발중인 넷캐시(NetCash)가 있다.

전자현금시스템은 사용자의 익명성 보장문제와 이중사용의 문제 즉, 불법적인 현금의 복사 문제 등의 기술적인 문제와 경제적인 가치척도로서의 사회 경제적인 문제를 안고 있다.

(2) 신용카드 기반시스템

신용 카드 기반시스템은 두 가지로 분류 할 수 있다. 퍼스트 버츄얼(first virtual)이나 CyberCash같이 기술력을 기반으로 신용 카드를 이용한 전자적 지불을 지원하는 경우와 비자나 마스타카드 같은 신용카드 회사에서 직접 전자적 지불을 지원하는 경우로 나눌 수 있다. 신용 카드 역시 실세계의 신용카드 지불 절차와 동일하게 되므로 소액 거래보다는 신용카드 한도액을 넘지않는 범위내에서 트랜잭션 비용을 상회하는 정도의 금액 거래시 적당하다. (김상균, 1997)

(3) 전자수표 시스템

전자수표 시스템은 실세계의 수표를 그대로 인터넷상에서 구현한 것으로 사용자는 은행에 신용계좌를 갖고있는 사람으로 제한된다. 전자수표 시스템은 발행자와 인수자의 신원에 대한 인증을 반드시 거쳐야 하는 문제를 갖고 있다. 이를위해 여러 가지 보안 기법이 사용되기 때문에 트랜잭션 비용이 많이 드는 단점을 갖고 있으나 거액의 상거래시 지불수단으로 적합하다.

전자수표 시스템으로는 캘리포니아 대학에서 개발중인 넷체크(NetCheck), 카네기 멜론 대학에서 개발중인 넷빌(NetBill)과 영국 뱅크넷(BankNet)의 Echeque, FSTC에서 개발중인 ECheck 등이 있다. (김상균, 1997)

(4) 전자적 자금 이체

현재 홈뱅킹이나 ATM으로 가능한 자금 이체를 인터넷에서 구현함으로써 사용자의 편의성을 더욱 증진시킬 수 있게 된다. 인터넷에서만 운영되는 최초의 가상은행(Cyber Bank)인 SFNB(Security First Network Bank)에서는 전자적 자금 이체에 관한 다양한 서비스를 제공함으로써 자금 이체를 이용한 전자적 지불을 가능하게 해주고 있다.

2) 전자 지불시스템의 모델

전자 지불시스템들의 모델은 지불 브로크시스템, 전자 화폐시스템, 소액 전자 지불시스템으로 크게 세 가지로 구분해 볼 수 있다.

첫째, 지불브로크(Payment Broker) 시스템은 전자지불 서버 자신이 결제를 위한 방법을 제공하지 못한다. 다만 신용 카드나 은행의 계좌를 이용해 네트워크상에서 대금을 지불하는 방법을 말한다.

현재 많이 알려져 있는 CyberCash 전자 지불시스템 이나 SET등과 같은 프로토콜들은 지불브로커형 전자 지불시스템이다.

둘째, 전자화폐 시스템은 지불 서비스를 제공하는 지불 서버가 스스로 결제를 처리할 수 있는 역할을 할 수 있으며 지불형태 역시 화폐의 발행, 유통, 확인, 지불등 금융기관이 하는 모든 기능을 지불 서버가 처리한다.

전자화폐형 전자 지불시스템은 법제도적인 준비, 통화정책, 화폐의 익명성 등에 대한 보완이 필요하다.

셋째, 소액 전자 지불시스템 모델은 전자 화폐모델의 일종으로서 주로 한 번의 지불트랜

젝션에 이루어지는 지불의 규모가 1달러 이하의 소액을 전문적으로 처리하는 전자 지불시스템 모델이다. 소액 전자 지불시스템에서 주로 고려할 점은 보안보다는 효율성과 비용의 절감이다.

6. 전자 화폐 설계

전자 상거래에서 가장 중요한 문제는 지불방법에 관한 것이다. 가장 일반적으로 사용할 수 있는 방법은 신용 카드를 이용하는 것이다. 그러나 신용 카드를 이용하게 되면 은행은 사용자의 거래내역을 추적할 수 있어 개인이 어디서 무엇을 샀는지에 관한 모든 정보를 알 수 있는 문제점이 생긴다. 즉 정보화 사회에서 핵심인 개인의 프라이버시를 침해하는 문제가 발생한다.

기본적으로 전자화폐는 은행(bank), 상점(shop) 그리고 사용자(구매자 혹은 consumer)로 구성되어 사용자와 은행간에 이루어지는 발행단계(withdrawal phase), 발행단계에서 발급 받은 전자화폐를 이용하여 물건을 사고 상점에 전자화폐를 지불하는 지불단계(payment phase), 그리고 사용자로부터 받은 전자화폐를 은행에 제출하여 상점의 계좌로 자금 이체를 시켜주는 결제단계(deposit phase)로 구성되어 있다.

그러면 앞에서 언급한 RSA 서명방식을 이용하여 개인의 프라이버시를 유지할 수 있는 만원권에 해당하는 전자화폐를 구현해 보자.

D. Chaum은 프라이버시가 제공될 수 있는 전자화폐를 위하여 은닉 서명방식(blind signatures)을 제안하였다. 은닉서명방식은 메시지를 숨기는 서명방식으로 제공자(provider : 서명을 받는 사람)의 신원과 메시지를 연결시킬 수 없는 익명성을 유지할 수 있는 서명방식이다.

그러면 RSA 서명방식을 이용하여 은닉 서명방식을 이용한 전자화폐를 구현해 보자.

1) 화폐 발행단계

(1) 은행은 만원에 해당하는 은행의 RSA 공개키(n,e)와 비밀키(p,q,d)를 생성하여 공개키(n,e)를 일반 사용자들에게 공개한다.

(2) 사용자는 화폐의 기본 정보(일련번호 등)가 기록된 전자문서 m을 준비하고 난수(random number) r을 임의로 선택하여 z를 계산한 후 은행에 보낸다.

$$z \equiv r^e \cdot m \pmod{n}$$

(3) 은행은 비밀키 d를 이용하여 z에 대한 RSA 서명 $\bar{s}$를 다음과 같이 생성한다.

$$\bar{s} \equiv z^d \equiv r \cdot m^d \pmod{n}$$

(4) 은행은 사용자에게 서명 $\bar{s}$를 전송한 후 사용자의 계좌로 부터 만원을 빼낸다.

(5) 사용자는 자신만이 알고 있는 난수 r을 이용하여 $s \equiv \bar{s}/r\ m^d \pmod{n}$을 계산하면 (m,s)가 은행으로 부터 받은 전자화폐가 된다.

2) 화폐 지불단계

(1) 사용자는 은행의 서명(m,s)을 전자화폐로써 사용한다. 사용자는 원하는 물건을 사기 위해 상점에 전자화폐 (m,s)를 지불한다.

(2) 상점은 구매자가 제시한 전자화폐에 있는 은행의 도장을 확인한 후 은행의 데이터베이스에 접속하여 화폐에 기록된 일련 번호가 이미 사용된 적이 있는지를 확인한다. 정당한 화폐이면 상점은 구매자가 요구한 물건을 제공한다.

3) 결제단계

(1) 상점은 후에 사용자로 부터 받은 전자화폐(m,s)를 은행에 제시한다.

(2) 은행은 상점의 계좌에 만원을 넣어준 후 은행의 데이터베이스에 (m,s)의 일련번호를 기록하여 다른 상점들에게 전자화폐(m,s)가 이미 사용되었음을 알린다.

위에서 사용자가 전자화폐의 기본 정보를 생성하므로 은행과 상점이 결탁하더라도 사용자의 프라이버시 정보가 노출되지 않는다.

그러나 위의 방식에서는 사용자의 2개의 전자화폐로 부터 은행의 승인없이 다른 전자화폐를 만들 수 있는 부정이 가능하게 된다.

그리고 위와 같은 전자현금의 가장 큰 현실적인 문제는 이중사용 방지를 위해 은행에서 이미 사용된 모든 전자화폐들에 대한 데이터베이스를 구축해야 한다는 것이다.

그러므로 전자화폐 자체가 특수한 구조를

가지게 하여 전자화폐를 한 번만 사용할 때에는 사용자의 프라이버시를 보장해 주지만 한 화폐를 두 번 사용했을때는 두 거래기록으로부터 그 화폐의 소유자가 드러나는 오프라인 방식의 전자현금 시스템이 유용하게 사용되고 있다. 오프라인 방식은 은행이 매 지불단계시마다 상점과 접촉할 필요가 없으므로 통신량의 집중화 방지와 거래에 따른 통신 비용 감소에 적합하다.

이러한 목적으로 개발된 전자현금 시스템으로는 chaum, Fiat, Naor 등의 cut-and-choose 방식을 이용한 전자화폐, S. Brand 등의 제한적인 은닉 서명기법(restrictive blind signatures)과 표현 문제(representation problem)를 이용한 전자화폐 등이 있으며 또한 전자지갑내에 은행이 발행하는 temper-resistant 모듈(TRM)인 관찰자를 심어 전자화폐의 이중 사용을 감시하게 하므로써 이중 사용을 사전에 방지하는 사전방지 방법 등이 있다.

V. 결론

지금까지 전자 상거래와 전자 상거래에서 전자식 대금 결제 시스템을 설계해 보았다. 컴퓨터와 네트워크의 활용은 이제 정보의 전달뿐 아니라 상거래의 영역까지 확대되어 국가와 사회에 어떤 영향력을 미칠지 예측하기가 힘들게 빠른속도록 변화하고 있다. 앞으로 전자 상거래가 경제, 사회, 국제적 교역에 미칠 영향은 여러 분야에서 특별히 연구해야 할 주제라고 본다

전자화폐의 도입으로 인터넷에서의 전자 상거래 규모도 폭발적으로 확대된다. 전자화폐가 없다면 인터넷을 통해 물품을 구입하더라도 그 결제는 은행을 통한 송금이나 우편 소액환에 의존할 수밖에 없다. 전자화폐는 이러한 문제를 해결해 주는데 특히 컴퓨터 소프트웨어, 신문, 잡지, 각종 정보 등을 인터넷에서 판매할 경우 포장 및 유통에 드는 비용이 거의 제로에 가깝기 때문에 소비자는 훨씬 싼 가격으로 이용할 수 있기 때문이다.

인터넷은 누구에게나 열려져 있는 오픈 네트워크라고 할 수 있다. 누구나 사용할 수 있는 인터넷의 범용성은 전세계의 모든 사용자를 고객으로 삼을 수 있는 전자 상거래의 가장 큰 장점으로 이어진다. 그러나 인터넷은 오픈 환경을 지원하기 때문에 악의의 목적을 가진 해커들에게도 노출되어 있어 보안에 취약하다고 할 수 있다. 인터넷이 보안에 취약한 이유는 인터넷에서 사용되는 오픈 환경을 지원하는 통신 프로토콜인 TCP/IP와 유닉스를 운용체제로서 사용하기 때문이다.

본 논문에서는 인터넷상에서 전자 상거래가 보편화될 경우 전자식 대금 결제를 위한 네트워크 설계, 보안시스템 설계, 대금 결제 시스템 설계, 사이버 캐시 클라이언트 시스템 설계, 전자지불 시스템 설계, 전자화폐 설계와 각종 보안대책을 마련하였다.

그리고 전자식 대금 결제 시스템은 일반분야와는 달리 학문적인 가치뿐 아니라 산업계에서도 파급효과가 크므로 산업계와 학계가 연계해 발전시켜야할 분야이다. 향후 연구 과제로는 전자식 대금 결제 시스템 설계 기술의 확보는 물론 설계된 내용을 중심으로 실제 시스템을 구현하기 위한 기술이 요망된다.

참고문헌

권도균, "WWW보안과 전자화폐", http://madang.dacom.co.kr/~dgguen/.

김상균, "21C 신경제의 새로운 비전 SET", 데이터베이스 월드, 1997, 10

김정평, 김충수, "전자 상거래와 인터넷", 경영정보연구, 제1호, 1997.6.

김중한 외 3인, "전자 상거래 기회와 도전", 정보처리, 제4권 제1호, 1997.1.

신동민, "전자 상거래의 추진현황 및 향후 전망", 신한리뷰, 1997. 3., pp. 60-77.

제일금융원, "전자화폐", 한국경영신문사, 1997.

한국과학기술원 전자 상거래 연구실, "전자 상거래의 구성요소", 월간 INTERNET, 1996. 5.

Loshin, Pete, "전자 상거래의 모든 것", 성안당, 1997.

Medvirsky, Gennady and B. Clifford Neuman, NetCash: A Design for Practical Electronic Currency on the Internet, Proceedings of the First ACM Conference on Computer and Communication Security, Nowember, 1993

Elgamal, Taher. "CREDIT CARD PAYMENT APPLICATIONS OVER THE INTERNET" http://home.netscape.com/newsref/std/credit.html, July 14, 1995.

VISA, Master Card, SET(Secure Electronic Transaction) http://www.visa.com.http://www.mc.com/.