碩士學位 請求論文

초소액지불시스템을 이용한 인터넷상에서의 학사EDI 서비스 구현

Implementation of an Academic EDI System Using Micropayment System on the Internet

仁川大學校 情報通信大學院

情 報 通 信 專 攻

邊 丙 吉

1999年 12月 日

碩士學位 請求論文

초소액지불시스템을 이용한 인터넷상에서의 학사EDI 서비스 구현

Implementation of Academic EDI system using Micropayment System on Internet

仁川大學校 情報通信大學院

情 報 通 信 專 攻

邊 丙 吉

1999年 12月 日

碩士學位 請求論文

초소액지불시스템을 이용한 인터넷상에서의 학사EDI 서비스 구현

指導敎授 : 李 基 永

이 論文을 碩士學位 論文으로 提出함.

1999年 12 月 日

仁川大學校 情報通信大學院

情 報 通 信 專 攻

邊 丙 吉

邊丙吉의 工學碩士學位論文을 認準함

1999年 12月 日

審 査 委 員 長_____印

審 査 委 員_____印

審 査 委 員_____印

仁川大學校 情報通信大學院

목 차

표 목 차

그 림 목 차

국문 요약

인터넷 상거래가 일반화되는 추세에 따라 앞으로의 전자상거래의 주요 관심대상은 온라인출판, 데이터베이스서비스, 소프트웨어유통등의 전자 정보의 교환이 될 것으로 예상된다. 대학에서의 학사서비스의 대부분은 각종 증명서의 발급인데 이를 전자거래의 형식으로 처리하려는 노력들이 시도되고 있다. 이때 주요지불수단으로 필요한 것이 소액지불 시스템이다.

본 논문에서는 소액전자 지불 시스템의 원리와 종류를 분석하고 학적증명서를 현재 상용화되고 있는 소액지불 시스템과 연결하여 인터넷을 통해 신청하고 인증과 지불을 마치고 발급 받을 수 있는 시스템을 구현하였다. 특히 인터넷을 통한 학사 시스템에서 고려해야 할 보안문제에 초점을 맞추어 해결 방안을 제시 하였다.

실험에 사용된 ASP(Active Server Page)언어는 서버에서 동작이 될 때만 그 값을 알 수 있는 것으로 그 소스 등을 침입자가 볼 수 없도록 하였고 지불처리기관과 인증기관으로 신청 시에는 이를 암호화하여 보안하도록 하였다. 전자자료교환(EDI)시스템이 국내 학교에 구축되어 있지 않으나 EDI시스템이 구축 시에는 바로 활용하여 전자상거래(EC)와 전자자료교환(EDI)이 결합된 시스템으로 사용할 수 있으리라 기대된다.

Ⅰ. 서론

인터넷이 발전함에 따라 그 대상이 첨단연구소 연구원 등 특정집단에서 기업으로 기업에서 관공서로 학교로 이제는 전국민으로 확대되고 있다.

1991년 Tim Berners Lee[16]에 의해 제안된 WWW(World Wide Web)로 인해 인터넷은 사용인구가 94년 1,000명당 9.92명에서 99연말 현재 2억6천만 명으로 5배나 증가하게 되었다.[29] 인터넷은 기업의 경영환경, 전통적인 학교형태, 일반 상거래 등 모든 분야에서 획기적인 변화를 가져오고 있다. 인터넷이 가져다준 문화방식에서 가장 큰 변화는 실시간(real time), 집에서(stay house), 손끝하나로(one touch)이다. 미국 유학생이 한국뉴스를 바로 접할 수 있고 집에서 수강신청이나 강의까지 들을 수 있으며 클릭으로 원하는 물건을 집에서 편안히 받아 볼 수 있다. 점차 사회가 복잡화, 전문화 해감에 따라 현대인은 시간(time)이라는 자본을 아껴쓰게 되었는바 전자상거래(EC)로 주부는 구매 시간을 줄이고 기업은 전자자료교환(EDI)을 구현하여 1~2일 걸리던 일을 30분내에 처리하게 되었고 학생은 등하교 시간을 낭비하지 않고 인트라넷(학교연결망)을 통해 수강신청할수 있게 되어 남는 시간인 자본을 재생산에 투자할 수 있게 되었다. 우리 나라에서도 4년제대학 180개 가운데서 30개대학은 원스톱서비스를 실시하거나 할 예정이고 인터넷 등 전산을 이용하여 수강 신청하는 대학이 약 140개로 이제 77%의 인터넷 사용율을 기록하고 있다.[8]

그러나 이러한 새로운 시스템으로 집을 짓기 위해서는 첫째로 기둥이 되는 표준화와 통신규약인 프로토콜, 개인의 정보보호를 위한 보안과 가상공간내에서의 지켜야할 법등이 만들어져야 된다. 정부에서는 전자서명법을 만들어 99년 8월1일부터 시행하는 등 바야흐로 인터넷시대의 정부의 역할을 찾기 시작하였다.

둘째로 디지털 콘텐츠를 실세계(Off-line)상태와 같이 만들어야 한다. 인터넷쇼핑몰 운영자 114명을 대상으로 설문 조사한 결과에 의하면 두 번 다시 찾지 않을 사이트의 유형은 상품에 대한 정보가 부실하고 종류 또한 다양하지 못한 곳이라고 하였다.[4] 인터넷쇼핑에 있어 네티즌들이 가장 많이 구매하는 것은 PC 관련 제품으로 조사대상자중 31.2%가 하드웨어 및 소프트웨어 구매자였으며, 뒤를 이어 도서 14.4%, 영화·공연티켓 12.6%순으로 나타났다. 이밖에 보험서비스, 주식, 부동산등으로 점차 범위를 넓혀가고 있다.[4]

본 연구에서는 대학 내에서의 전자상거래 실용화를 목적으로 대학에서 발급하고 있는 증명서를 전자상거래 개념에 도입시켜 상품으로 만들고 이를 즉시 받을 수 있는 시스템 도입을 실현하고자 하였다. 연구배경으로는 전국대학의 93.6%가 학교홈페이지를 갖고 있으며[11] 학생들이 학생서비스센터 홈페이지에서 대부분 이용하는 정보가 민원증명서 부분인 점에 착안하였다.[11] 비록 일부대학에서는 인터넷을 통하여 증명발급을 하는데 수수료를 내기 위해 은행을 직접 나가야 하는 반자동의 형태를 지니고 있는 곳이 대부분이어서 완전한 전자상거래라고는 보기 어려운 실정이다. 그래서 본 연구에서는 연구범위를 대학 내에서 쉽게 이용하기 위해 현재까지 나와있는 전자소액지불시스템중에서 국내에서 상용화된 시스템을 선택하여 구현하는 것으로 설정하였다.

대학이 데이터베이스를 구축한 서버를 운영한다고 가정할 때 학사행정을 위한 초소액 시스템 관리서버를 만들고 이를 웹상에서 초기에 로그인 시에는 학사데이타베이스와 연계하고 이후 보안문제를 해결하기 위해 인증처리할수 있도록 연동한후 증명서를 선택하고 이에 대한 지불을 하는 것은 지불처리기관에서 처리되고 그 자료를 학사관리서버를 요청하여 민원인이 요구하는 증명서를 만들고 이를 전자적으로 봉하여 민원인에게 보내면 전자서명하고 그 증명서를 기관에 전자적으로 접수시키고 기관에서는 전자자료

교환변환기(EDI Transfer)를 이용해서 받아보는 것으로 제안하는바, 실세계에 있어서는 용지에 직인을 찍은 출력형태의 증명서가 유효하므로 본 연구에서는 증명서 서버에서 출력하는 형태로 실험을 진행하였다.

논문의 구성을 보면 II장에서는 소액전자 지불시스템을 정의하고 제안된 몇가지 종류를 설명하고 III장에서는 학사EDI서비스 시스템의 모형을 제안하고, IV장에서는 이것을 구현한 실험 결과를 나타내었고 V장에서는 결론을 내리고 앞으로의 연구방향을 제시한다.

Ⅱ. 소액 전자지불 시스템

본 장에서는 전자지불의 정의 및 종류등을 알아보고 대표적인 소액지불의 메카니즘을 통해서 원리등을 서술하고 현재 상용화된 시스템의 국내외 현황을 열거하였다.

1. 전자지불의 정의

전자지불 시스템은 일반적으로 전자상거래에서 고객이 상인에게서 제공받은 상품 또는 서비스에 대한 대가의 지불을 위해 설계된 체계를 말한다. 지불 방법에 따라 신용카드, 전자현금, 전자수표, 직불카드, 선불카드 등 다양한 형태의 시스템들이 제안되고 있다. 지불금액의 정도에 따라, 신용카드나 보안성이 높고 익명성이 보장되는 전자현금과 같이 고액의 금액을 안전하게 지불하기 위한 시스템과 적은 금액을 낮은 거래비용으로 효율적으로 지불하기 위한 시스템으로 나눌 수 있다.

네트웍형 전자지불 시스템은 크게 SET(Secure Electronic Transaction)진영과 Non-SET진영으로 나눌 수 있다. SET는 비자와 마스터카드가 합쳐 신용카드용 전자지불의 표준사양을 제정하였다. 다국적 기업인 IBM이 이를 이용하고 있고 Non-SET 전자지불 진영에는 사이버캐쉬, 디지캐쉬와 같은 초기에 전자지불을 개척한 회사들이 있으며 전자화폐가 해당된다. 국내에서는 이니텍의 이니텍페이(http://www.initech.com)와 데이콤에서는 데이콤페이(http://paygate.dacom)가 있는데 Non-SET 시스템이다.

현재까지 제안된 초소액 지불 시스템들로는 Millicent, PayWord and Micromint, NetBill, Micro-iKP, MPTP(MicroPayment Transfer Protocol)등이 있으나 Millicent, PayWord, NetBill 등이 대표적이다. 소액지불의 요구

조건으로는 거래비용(계산량과 통신량)이 가능한 낮게 유지되어야 하고 지불처리에 소요되는 시간을 짧게 유지해야 한다.[2]

2. 전자지불의 종류와 원리

소액지불시스템의 거래과정은 크게 지불에 쓰일 화폐를 사거나 생성하는 사전계산과정, 실제 구매 지불과정 그리고 정산과정으로 이루어진다. 기본 모델을 그림 1과 같이 나타내었다. 구매자(User)는 중개인(Broker)에게 가치나 전자주화를 사서 상인(Vendor)에게서 전자상품정보(information)를 받고 이를 지불하며 중개인은 지불기관과 연결되어 있다.

이를 인터넷에서 응용하기 위해서는 앞절에서 언급한 SET와 Non-SET의 지불소프트웨어가 쓰인다. Non-SET인 SSL(Secure Socket Layer)은 크레디트 카드번호가 인터넷을 통해 전송될 때 암호를 부여하는 방법으로 이용되는 것이고 SET는 한발 더 나아가 물건을 판 사람과 산 사람의 신원을 증명하기 위해 전자증명서를 사용하는 것이다. 안전성을 놓고 볼 때는 SET가 뛰어나지만 복잡하다는 문제점으로 소비자들이 꺼리고 있으며 우리나라에서도 Non-SET계열의 시스템이 많이 쓰여지고 있다.[2][14] 다음으로 대표적인 소액전자지불시스템의 원리를 알아보고자 한다.

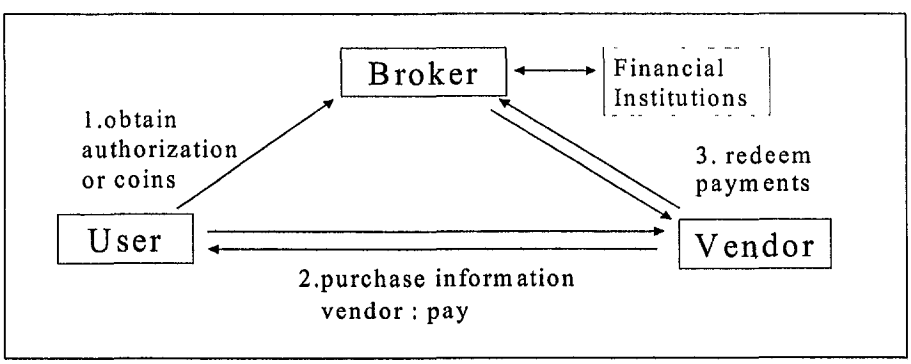

Figure 1. Basic model of the Micropayment system

1) Millicent

비용이 많이 드는 강력한 암호 알고리즘을 사용하지 않고, 해쉬함수만으로 구현함으로써 거래수립비용이 적게 들도록 설계된 시스템이다.[1]

구매자, 판매자, 중개인으로 구성되며 각각의 판매자들이 발행하는 판매자 고유의 가치를 지니는 일종의 전자화폐인 스크립(Script)을 이용한다. 스크립은 중개인이 직접 발행하는 "중개인 스크립"과 중개인이 구매자에게 판매하는 "판매자 스크립"의 두 가지 종류가 있다. 그림 2와 같이 고객이 이전에 거래가 없었던 새로운 상인과 거래하기 위한 절차를 살펴보자. 구매자는 판매자와 거래를 하기 위해 중개인 스크립과 판매자 스크립을 중개인을 통하여 구입한다. 구매자는 판매자에게 서비스 요청과 함께 스크립을 판매자에게 제공하고 판매자는 스크립의 유효성 여부를 확인한 후 서비스와 함께 서비스의 대가만큼을 감한 스크립을 새로이 생성하여 거스름돈으로 구매자에게 되돌려준다.

실제로 거래한다면 그림 3과 같이 구매자는 판매자스크립 20원을 포함하여 5000원의 스크립을 중개인에게 구입한다. 20원의 특정판매자 스크립을 특정판매자에게 지불하고 판매자는 서비스료 1원을 받고 재 발행된 19원의 스크립을 구매자에게 전달해 주는 사이클이 된다.

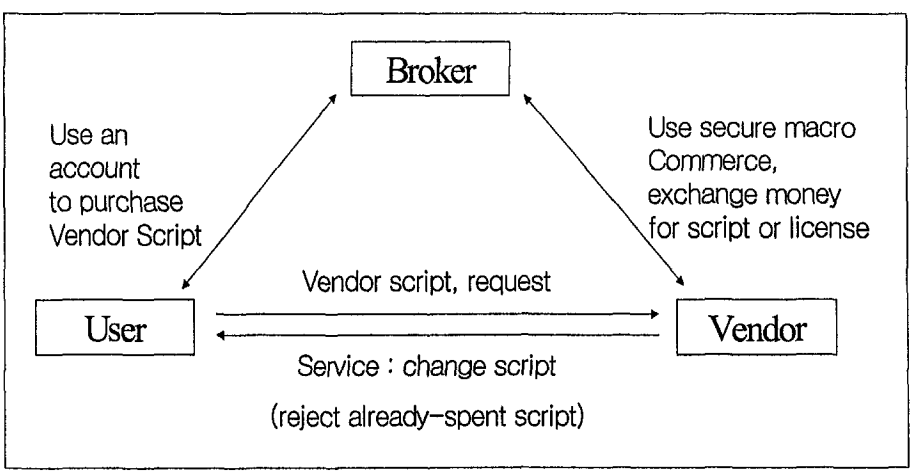

Figure 2. Model of the Millicent system

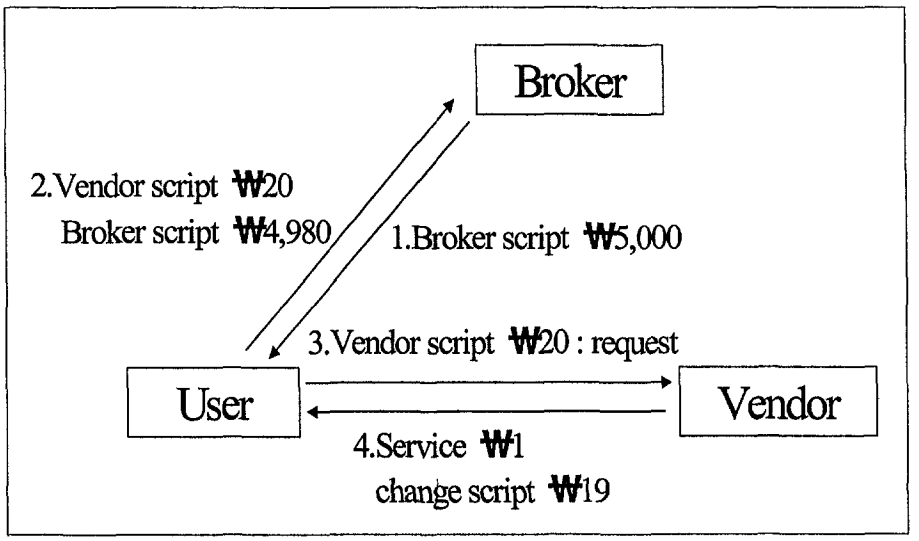

Figure 3. Example of real transaction based on the Millicent system.

Millicent는 각 상인이 고유의 화폐를 발행하여 사용하므로 상인이 독립적으로 화폐의 이중 사용이나 위조, 변조 등 부정행위 등을 쉽게 막을 수 있다는 장점이 있다. 또한 일단 거래가 성립되고 나면 거래 금액에 관계없이 일정한 횟수의 해쉬 연산만으로 거래가 완료되므로 동일 상인에 대한 연속적 구매에 효과적이다.[2]

반면 고객이 새로운 상인과 거래를 원하는 경우 중개인으로부터 그 상인이 발행한 스크립을 구입하여 사용하여야 하므로 온라인 상에서 중개인과의 상호작용이 항상 가능해야만 한다. 고객의 수에 비하여 중개인의 수가 훨씬 적으므로 지불시스템의 규모가 커질수록 중개인이 처리해야 하는 양이 많아져서 결국은 병목현상이 일어나고 고객이 체감하게 되는 지연시간 및 전체지불시스템의 효율을 떨어뜨리는 문제점을 안고 있다.

2) PayWord

해쉬 함수의 단방향성을 이용한 초소액 지불시스템중의 하나이다. 고객과 상인사이의 구매 및 지불과정을 효율적으로 유지하는데 초점을 두고 있다. PayWord에서 이용하는 화폐의 형태는 임의의 값으로부터 해쉬 연산을 연속적으로 취하여 얻은 해쉬 사슬이다. 그림 4와 같이 해쉬 사슬에서의 생성방향과 소비방향을 서로 반대로 하여 해쉬 연산의 단방향성을 이용하여 해쉬값을 지불한 고객의 신원을 확인하는 방법을 취하고 있다. 밀리센트의 지불시스템과 마찬가지로 고객과 상인이외에 중개인을 두고 있다. 고객과 상인은 중개인에게 미리 등록을 해 두어야 한다. 중개인은 은행을 비롯한 금융기관과 연결되어 있고, 고객이 지불한 돈(해쉬값)은 상인이 믿을 수 있도록 지불보증서(Certificate C_u)를 발급하는 역할을 맡는다.

PayWord에서의 고객이 이전에 거래관계가 없었던 새로운 상인과 거래를 시작하고자 하는 경우의 거래절차는 다음과 같다. 고객은 임의의 값(W_n)을 선택하여 필요한 만큼 해쉬 연산을 반복 수행함으로써 해쉬 사슬을 생성한다.

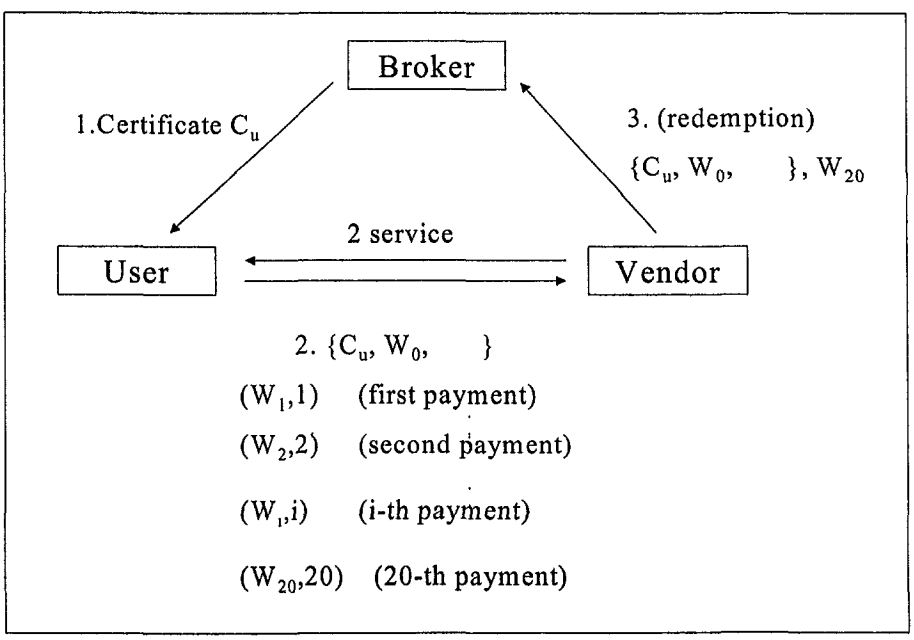

Figure 4. Model of the PayWord system

여기서 해쉬 사슬을 이루는 해쉬값 각각은 미리 정해진 만큼의 동일한 가치를 지니는 동전의 역할을 하며, 해쉬 알고리즘은 상인이 확인할 수 있도록 상인과 고객간에 협의된 것을 이용한다. 고객은 자신이 마지막으로 생성한 해쉬값(W_0)을 중개인에게 지불보증서와 함께 전자서명을 하여 상인에게 제공한다. 상인에 의해 고객과 중개인의 전자서명이 확인되면 거래준비가 완료된 것이다. 이후의 거래는 만들어둔 해쉬 사슬에 속하는 해쉬값 하나와 그 해쉬값이 해쉬 사슬에서 몇 번째 값인지를 나타내는 인덱스 값으로 지불이 된다. 즉 W_0로부터 i번째 값이라면 (W_i, i)를 상인에게 제시한다. 상인은 W_i로부터 i번만큼 해쉬 연산을 수행한 결과가 W_0와 동일한지 살펴봄으로써 제공받은 해쉬값의 유효성(Validity)을 확인할 수 있다. 이후 거래가 완료되면 주기적으로 각 상인은 고객들로부터 받은 해쉬값들을 중개인의 지불보증서와 함께 중개인에게 제공하고 중개인은 고객의 계좌로부터 상인의 계좌로 대금을 결재하게 된다.[2]

Millicent와는 달리 중개인이 거래 도중에 개입하지 않으므로 중개인으로 인한 병목현상이 발생하지는 않는다. 일단 거래관계가 수립된 고객과 상인 사이에서는 상당히 효율적인 거래가 가능하다. 그러나 공개키 암호화 방식에 따른 전자서명을 이용하므로 많은 계산량이 요구된다. 상인이 서비스하는 고객의 수가 증가함에 따라 고객들에 대한 서비스 지연시간이 늘어난다. 고객은 일단 중개인으로부터 지불보증서를 발급 받은 후 일정기간동안 해쉬 사슬을 제약 없이 생성하여 쓸 수 있어서 신용한도를 초과하여 사용할 수 있다.

3. 상용화된 전자지불 시스템의 종류

1) 국외

(1) 신용카드

실세계에서 쓰고 있는 기존의 신용카드를 인터넷에서 활용하는 것이고 신용카드 정보의 암호화를 통하여 이용하고 있다.

- First Virtual

별도의 전용프로그램이나 보안이 강화된 프로토콜을 이용하지 않고, 기본적인 WWW브라우저와 전자메일만을 이용해 전자결재 시스템을 구축하였고 기존의 인터넷 소프트웨어에 대한 사용자의 친숙성을 강조하였다. 이 경우는 특별한 암호화 기법을 사용하지 않기 때문에 보안상의 문제점을 안고 있다. 보안상의 문제로 전화, 팩스, 전자우편을 다시 이용해야 하므로 완전한 전자상거래의 구축에서 벗어난다고 본다.[28]

- CyberCash

신용카드를 이용할 시 카드번호만으로 지불이 되므로 불순한 의도를 가진 상점에 의해서 악용될 소지가 있는데 이런 문제를 개선하기 위해 설립된 회사로서 기존사와 다른 점은 CyberCash Wallet이라는 소프트웨어를 통해 대금결재내용이 CyberCash사의 중앙컴퓨터에 입력되고, 가상상점에는 신용카드의 진위여부만을 통보한다는 점이다. 즉 고객의 신용카드정보는 중앙컴퓨터에 의해 가상상점과 차단되어 보안이 이루어진다. CyberCash사는 구매자와 상인을 서로 인증하고, 구매자의 신용카드정보를 불순한 의도로부터 보호하며, 신용카드회사에서 상품대금을 인출해 상인에게 전달한다. 단점으로는 판매자 서버로부터 CyberCash지불서버로 다시 판매자거래은행과 고객거래 신용카드사와 길게 연결되어 많은 접속시 부하가 많이 발생하고 처리시간이 길어지는 점등이 개선의 요소라 할 수 있다.[23]

- SET

비자와 마스터카드사가 공동으로 개발한 신용카드결제용 보안 프로토콜로써 고객, 판매자, 지급결제중계기관(PG, Payment Gateway)간 상호인증, 거래정보의 기밀성 및 무결성을 최대한 보장하도록 설계되어 있다. SET을 이용한 구매 및 지급절차는 ①고객이 인터넷상의 판매자에게 접속하여 해당 판매자의 정당성을 검증하기 위하여 판매자 및 지급중계기관의 인증서를 수신 받는다. ② 판매자와 PG의 인증서를 확인한 후 자신의 지급정보와 인증서를 판매자에게 송부하여 구매요청을 한다. ③판매자는 고객인증서를 확인한 후 주문정보는 자신이 보유하고, 고객의 지급정보와 고객 및 판매자의 인증서를 PG에 전송한다. 이때 고객의 지급정보는 판매자가 모르게 암호화 되어있다. ④PG는 고객과 판매자의 인증서를 확인한 후 지급정보를 해당 금융기관이 이용할 수 있도록 복호화하여 신용카드결제승인을 요청한다. ⑤해당금융기관은 고객의 신용한도를 고려하여 승인여부를 전송한다. PG는 승인여부를 판매자에게 전송한다. 판매자는 PG의 응답에 따라 고객에게 영수증을 발급하고 주문을 처리한다.[3]

(2) 전자수표(Electronic Check)

신용으로 금액을 지불하거나 현금 외에 다른 방식을 통해 지불하기를 원하는 많은 개인이나 기업체를 위하여 고안되었다.

- Netcheque

캘리포니아 대학에서 개발중인 전자 수표 시스템으로서 복수서버를 두어 규모의 확장성(scability)을 제공하고 있으며 분산된 서버사이에서 사용자의 인증과 서명을 위해 Kerberos시스템에 기반을 두고 있다. 전자수표를 사용할 때 서명을 하거나 받은 수표에 배서할 때 사용하는 것은 프락시(proxy)라고 불리는 것으로 Kerobos티켓의 특별한 종류를 사용한다. 일반사용자가 이용하기에는 어려움이 있으며, Netcheque는 공개키암호화 방식보다 효율적인 재래식 암호화 방식을 사용하여 적은 액수의 지불에 대한 정산이

가능하다는 장점이 있으며 Pay Per View(PPV)라는 프로토콜을 이용하여 웹상에서 사용된다.[19]

- Echeck

1993년 9월에 미국의 산업금융에 있어서의 경쟁력향상을 위해 은행 및 금융 및 서비스기관, 국립연구소 및 기술력을 가진 민간기업체와 정부기관이 컨소시엄을 구성하여 설립한 FSTC(Financial Service Technology Consortium)에서 개발하였다. Echeck는 PCMCIA카드를 이용한 하드웨어 기반 서명방법을 쓴다. 컴퓨터에 서명카드를 인식하는 장치가 설치되어야 수표에 서명하거나 배설할 수 있다. 이외의 전자수표 시스템으로는 넷첵스 NetChex(http://www.netchex.com), 영국의 가상 은행인 BankNet에서 발행하는 Echeque(http://mkn.co.uk/help/bank/echeque.html)등이 있다.

(3) 전자현금

실세계에 있어서 가장 많은 지불수단은 현금이다. 비록 많은 신용카드등 결제 시스템이 개발되었지만 현금선호현상으로 인해 전자상거래환경에서도 이를 개발하기 위해 노력하는바 필요충분조건을 살펴보면 독립성 및 보안성, 사적인 비밀보장, 전환 가능성, 가분성 등이 있다.[3] 소액거래시에 유용하게 사용될 방법으로 추천되고 있는 바 구현 방법에 따라 네트워크형과 IC카드형으로 분류할 수 있다.

- CyberCoin

인터넷상의 소액거래에 가용중이고 CyberCash사에서 개발되어 주로 10달러 미만의 소액 디지털상품 및 서비스의 거래에 따라 유용하게 사용되고 있다. 전자지갑을 다운 받아 사용하며, 전자현금이 소비자의 은행계정이나 신용카드에서 전송될 때 금융관련 정보는 RSA로 암호화되어 안전하게 전송하는 방법을 사용한다.

- Netcash

캘리포니아 대학에서 개발중으로 복수의 서버를 도입하는 분산 시스템을 이용한 Netcash 시스템은 CyberCash가 갖고 있는 중앙 집중적인 계좌 관리에서 오는 단점을 해결하려 하고 있다. 그리고 사용자의 계좌를 분산된 여러 대의 서버에서 관리하며 사용자의 수를 극대화하는 데에 역점을 두고 있다. 또한 넷체크라는 전자 수표 시스템과 교환이 가능하도록 하려하고 있다.[20]

(4) 전자자금이체

- Netbill

카네기 멜론대학의 연구소(Information Science Institute)에서 연구용으로 개발한 시스템으로 상용화하지는 않았다. 잡지 및 신문에 실린 기사, 책, 소프트웨어 및 비디오 클립과 같은 정보를 저렴한 비용으로 인터넷을 통해 제공할 수 있으며 인터넷 대금결제 시스템을 제공한다.[18]

- SFNB

인터넷상에서만 운영되는 최초의 가상은행인 SFNB(Security First Network Bank)에서는 전자 자금이체에 관한 다양한 서비스를 제공함으로써 자금이체를 이용한 전자지불이 강해지고 있다. 또한 SFNB는 웹을 이용하여 모든 인터페이스를 처리하고 있어 사용자의 편리성이 좋다.[15]

2) 국내

(1) 전자현금

- 하나로카드

부산은행에서 서비스하는 전자지갑카드로서 IC칩이 부착된 플라스틱 카드에 고객의 예금계좌를 통해 현금을 전자적으로 입금하여 고객이 가맹점에서 물품이나 용역제공을 받은 후 현금대신 대금을 결제하는 기능을 가지고 있다. 현금이나 수표 없이 이 카드로 가맹점에서 쇼핑할 수 있으며 은행

CD기에서 신용카드 및 현금카드로 사용할 수 있다. 물품구입후 고객이 직접비밀번호를 입력하여 정당성여부를 확인한 후 대금을 결제하므로 안전하고 다른 사람의 거래내역을 알 수 없다는 장점이 있다.[13]

(2) 인터넷 카드

- 애니카드

전자선불카드로서 기업용 판촉물 형태로 제작 유통시켜 크리스마스카드등과 같은 소액이 거래상품인 경우에 이를 사용한다. 일정한 곳에서 이를 구입해야 한다.[17]

- Internet I.D card

네트워크카드로도 사용될 수 있으며 1000원이하의 소액결재가 가능하고 한번 사용 후에도 개인이 일정 금액만큼을 재 적립해서 사용이 가능하기 때문에 지속적으로 사용할 수 있다. 거래의 취소나 잔액 환불을 요청할 때도 언제든지 실시간으로 처리가 가능하며 신용카드 없이도 인터넷은 물론, 실거래에서도 사용할 수 있게 되어 있다. 본 논문에서는 위 시스템을 지불시스템으로 구현해 보고자 한다.[25]

(3) 전자지갑

- 아이캐쉬카드

사용자의 익명성에 초점을 두고 전자토큰방식과 같이 사용하는 아이캐시카드를 개발판매하고 있으며 인터넷상에서 유료 콘텐츠를 이용할 때 필요한 지불수단으로 전자상품권처럼 사용될 수 있다. 이 서비스를 이용하려면 동성정보통신이 개발한 전자지갑을 다운로드 해야 한다. 전자지갑은 전자거래 이용자가 신용카드나 전자화폐, 각종 전자상품권 등을 보관했다가 온라인에서 거래를 할 때 사이버 머니를 꺼내 쓰는 소프트웨어이다.[24]

- 이지캐쉬

부가가치통신망(VAN : Value Added Network)사업자로서 입지를 굳힌 KICC(한국정보통신)는 이용자가 전자지갑을 PC에 설치할 필요 없이 온라인 상에서 바로 대금결제를 하고 이용 내역 등을 검색해 볼 수 있는 「이지캐시」서비스를 제공한다. KICC는 실제 결제 서비스와 연계해 기존 8백만 명에 이르는 회원을 기반으로 실세계 및 사이버 통합형 지불 시스템을 구축, 포인트를 공유하도록 할 방침이다.[24]

- Daycompay

가장 먼저 전자지불서비스를 시작한 업체로서 "DACOM ECredit Service"를 개시하여 천리안(200만), 보라넷(3천개 기관), 매직링크(2만개 기관) 등 가장 많은 회원을 기반으로 종합적인 마케팅 환경을 제공하고 있다. 웹기반의 전자지불서비스가 시작된 97년 1월 15일에는 PC Banking 서비스를 이용하는 천리안 PPP(Point-to-Point Protocol)고객을 대상으로 서비스를 시작(계좌이체)하였다. 현재 전자 wallet 및 SSL Form 방식을 지원하고 있다. 국제적으로 인정된 RSA, DES 및 SSL 암호화 알고리즘을 적용하고 있으며 RSA Euro(1024 bit) 및 DES(56bit) 암호화 알고리즘을 적용, 네트워크상의 안전한 거래를 지원(Wallet S/W)한다. SSL을 적용하여 "회원정보 및 주문/결제정보" 를 암호화(사용자 입력방식, Form방식)하고 방화벽(Firewall : CyberGuard)을 이용하여 시스템 보안을 유지하고 있다.[21]

III. 학사 EDI 서비스 시스템의 모형

본 장에서는 학사 시스템 설계시에 중요하게 고려해야하는 보안의 문제를 통신선로등의 물리적인 면과, 알고리즘 등의 소프트웨어적인 면, 그리고 출력형태에 관한 면에서 살펴보고 소액지불프로토콜을 제안하며 본 논문에 맞는 업무분석을 하여 본 시스템의 흐름도를 작성하였다.

1. 보안 고려사항

1) 물리적인 면

네트워크간의 보안에 해당하는 것이 Firewall시스템으로서 사용자가 속한 기관의 네트워크에 보안침입을 할 수 있는 외부네트워크로부터 이를 보호하여 중요한 데이터를 정당하지 않은 사용자가 접근하는 것을 막고 정당한 사용자가 네트워크 자원을 방해 없이 접근하도록 하는 것이다. 내부의 신뢰성 있는 네트워크와 외부의 신뢰성 없는 네트워크 사이에(그림 5)위치

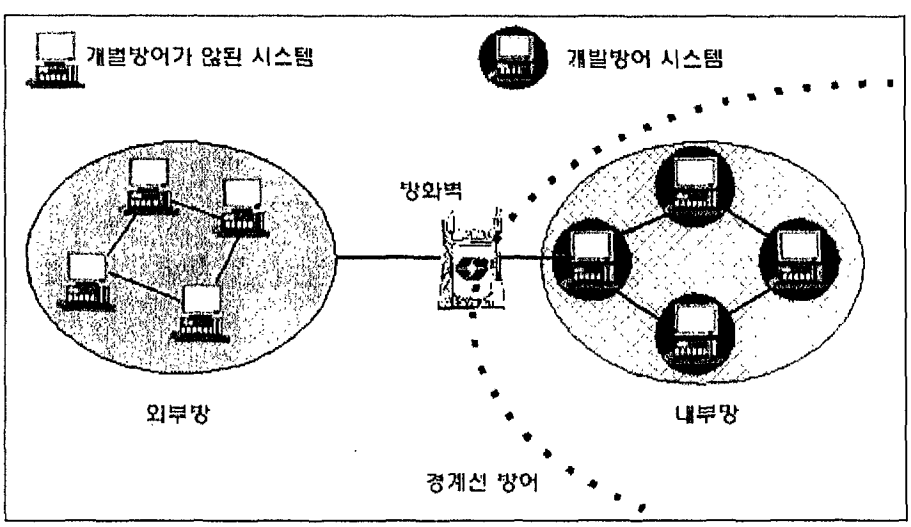

Figure 5. Firewall system

하며 내부망에서도 각각의 컴퓨터에 개별방어시스템을 구축하여야 한다. 종류로는 듀얼홈드호스트와 베스천 호스트, 스크린 서브넷, 응용레벨 게이트 웨이등이 있다.[10]

네트워크보안은 방대한 영역이므로 다양한 기술들이 총동원되어야 하며 전사적인 보안체계의 일부로서 다루어져야 한다. 인터넷의 기본전제가 되는 것은 네트워크의 신뢰성이다. 그러나 현실적으로 인터넷은 정보의 보고임과 동시에 불법정보유통, 해킹의 천국이다. 침입형태와 대처를 알아보면 스니퍼는 일반사용자들이 네트워크 상에서 가장 쉽게 이용할 수 있는 방법으로 Ethernet상을 지나는 모든 패킷을 복사하여 필요한 정보를 수립하는 바, 이 대비책으로 네트워크에 들어있는 모든 시스템을 "netstat"명령어로 검사해야하며 패스워드를 암호화하여 전송함으로서 패스워드의 비밀성을 유지한다.

둘째 TCP순서번호 추측으로 TCP/IP프로토콜의 구조적 결함등을 이용하여 침입자가 사용하는 시스템을 신뢰성있는 호스트로 위장한다. 이에 대한 대비책으로 주소기반 인증을 피하고 IP패킷필터링을 실시하여 변조된 패킷의 접근을 막는방법등이 있다.

2) 소프트웨어적인 면

전자상거래를 안심하고 할 수 있는 것이 보안기법이다. 현대 암호기술은 자국의 보안사업을 보호한다는 국가실리주의등에 의하여 국제적으로 표준화 하는데 아직 논란의 대상이 되고 있는데, 보안의 종류, 보안문제 이를 해결하기 위한 암호화 방법의 적용 및 전자서명, 전자인증에 대하여 알아보면 다음과 같다. 인터넷상에서의 보안은 시스템의 보안과 네트워크의 보안 2종류로 나뉘어 진다. 시스템의 보안이란 전자상거래 서버에 저장되어 있는 구매자들의 비밀정보가 누설되지 않고 제3자에 의해 시스템이 파손되거나 오동작하도록 변경되지 않도록 하는 것이고 네트워크의 보안이란 자료

가 인터넷상에 띄워져서 구매자, 판매자, 중개인에게 전달될 때 중간에서 누출, 변경되지 않도록 하거나 제3자가 가로채지 않도록 하는 것이다. 현재 인터넷상에서의 보안성은 전혀 없으며 그 문제는 4가지로 나눌 수 있다. 첫째 기밀성(Confidentiality) 둘째 인증(Authentication) 셋째 무결성(Integrity) 넷째 부인방지(Nonrepudiation)이다.[7]

이러한 문제를 해결할 수 있는 여러 가지 보안기법이 개발되어 있는데 비밀키 암호화방식 또는 공개키 암호화방식 등이 있다. 비밀키 암호화방식의 경우는 암호화키로부터 복호화키를 계산할수 있거나 반대로 복호화키로부터 암호화 키를 계산할수 있을 때의 알고리즘을 말한다. 키를 K라 하고 평문을 M, 암호문을 C, 암호화 함수를 E, 복호화 함수를 D라고 표시하여 아래와 같은 수식으로 표현하였다.

$$E_k(M)=C$$

$$D_k(C)=M$$

$$D_k(E_k(M))=M$$

어떤 알고리즘은 암호키 복호키를 달리 이용하는데 이때 암호 키를 K1, 복호키를 K2라고 표시하면 아래와 같은 수식이 된다.

$$E_{k1}(M)=C \quad \text{----------} \quad ①$$

$$D_{k2}(C)=M \quad \text{----------} \quad ②$$

$$D_{k2}(E_{k1}(M))=M$$

그림 6에 위의 내용을 블록도로 표시하였다.

공개키 암호화 방식은 암호화키와 복호화키가 서로 다르며 암호화 키로

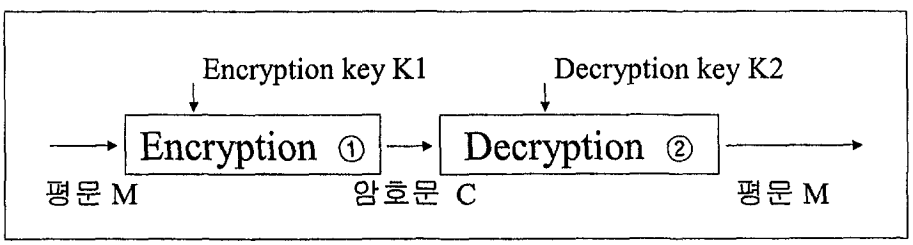

Figure 6. Procedure of encryption and decryption

부터 복호화키를 계산할 수 있을때의 알고리즘을 말한다. 보내는 사람은 받는 사람의 공개키를 이용하여 암호화한 후 보내고, 받는 사람은 자신의 개인키를 이용하여 복호화하면 된다. 그러나 이 경우 속도가 느린 단점이 있어서 그림7과 같이 이를 응용하여 비밀키(K_s)를 이용하여 비밀키 암호화 방식으로 암호화하고 비밀키 자체는 받는 사람의 공개키(K_B)를 이용하여 공개키 암호화 방식으로 암호화한 두 암호문을 보내면(1단계) 받는 사람은 자신의 개인키(K_v)로 비밀키를 복호화한 후 이 비밀키(K_s)를 이용하여 전달 정보를 복호화한다.(2단계) 이와 같이 비밀키를 주고받는 것을 키의 전달(Key exchange)라고 부른다. 위 시스템은 보안성에 중점을 두고 기밀함에 중점을 둔 제한적 알고리즘이다.

그림8에서는 인증기관에서 관리하는 공개키를 이용하여 디지털서명에서의

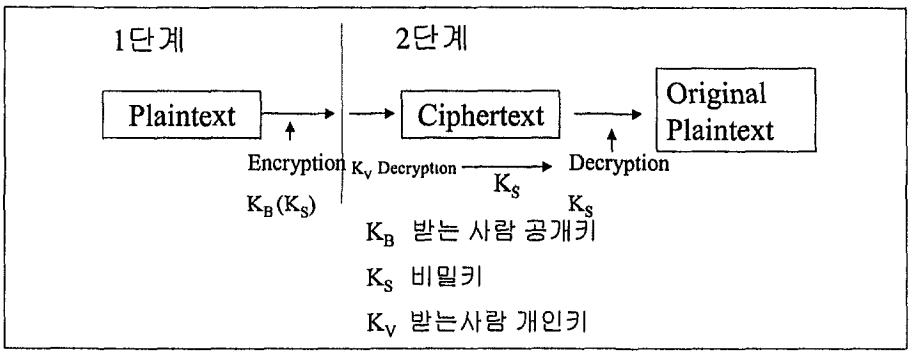

Figure 7. Procedure of key exchange

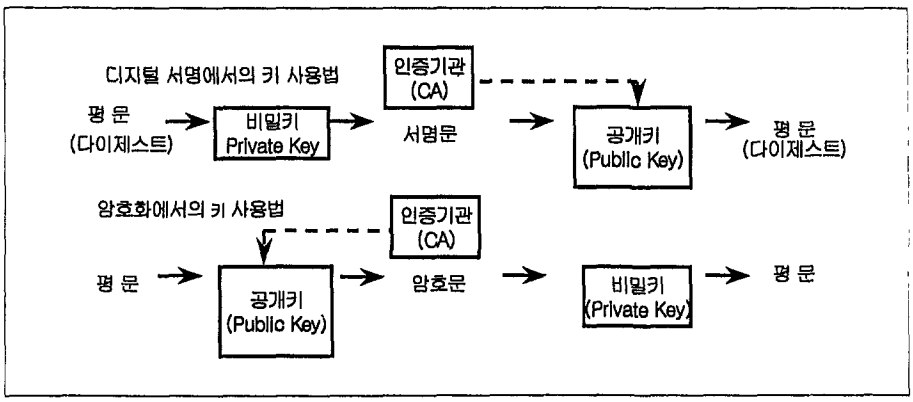

Figure 8. Examples of public key cryptosystem

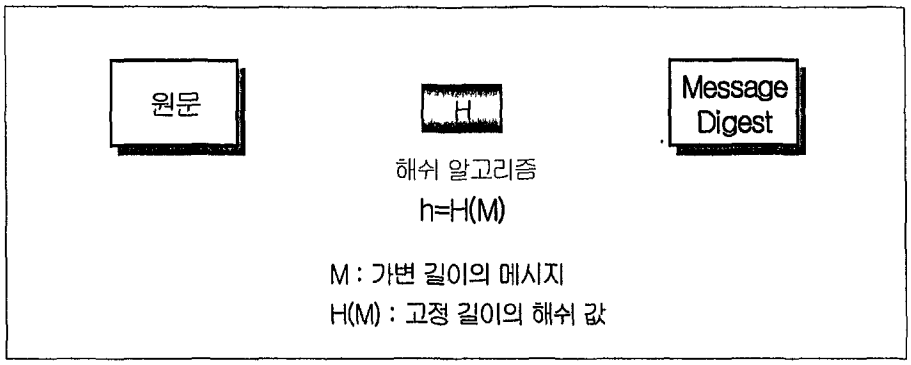

Figure 9. Message digest with hash algorithm

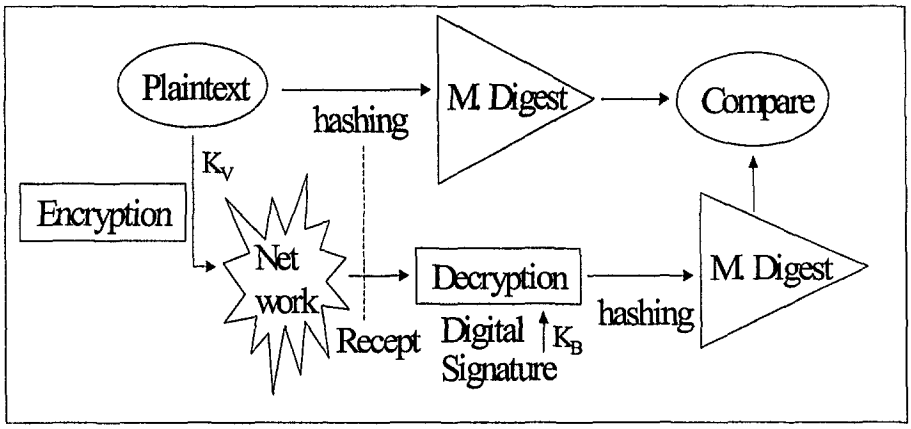

Figure 10. Procedure of authentication.

키 사용법과 암호화에서의 키 사용법을 나타내었다.

키 기반 암호화 알고리즘은 암호화 알고리즘은 아니지만 전달된 정보의 변경여부(무결성)나 정보를 보낸사람을 확인(인증)할 때 사용하는 것으로 M.D(message digest)방법이 있으며 MD5 해쉬함수등이 사용되며 그림 9에 도식화되어 있다. 전체적으로 적용하여 나타낸 그림이 10과 같은데 원문을 해싱하여 M.D화 시키고, 또한 원문을 받는사람의 공개키로 암호화하여 송신하여 네트워크상으로 보내면 받는사람의 비밀키로 복호화하여 전자서명하고 원문을 해싱하여 서로 비교한다. 이와같이 무결성, 전자서명, 부인방지를 하였고 이에 추가하여 인증의 측면도 보내는 사람의 공개키와 비밀키

를 이용한다면 접수(recept)시 보낸사람의 공개키로 전자서명을 하게 되어 그 내용을 암호화할 수 있는 사람이 이 보낸사람의 공개키 짝이 되는 개인키를 갖고 있는 그 사람뿐이므로 송신자확인을 할 수 있다.

공개키 암호화 방식은 속도가 오래 걸리고 장문의 내용을 암호화, 복호화하기 어려우므로 인증시에도 미리 정해진 내용을 메시지 다이제스트한 것을 암호화, 복호화한다. 이것을 전자서명이라 하는데 인증뿐만 아니라 무결성과 부인방지도 보장하게 된다. 그렇다면 공개키를 어떻게 알 수 있는가 하는 것이 문제이다. 이를 위해 제시된 것이 인증기관 (CA : Certificate Authority)이다. 인증기관은 인증하기 전에 그 사람을 실제로 확인한 후 그 사람이 제시한 공개키를 인증한다. 인증기관의 개인키로 암호화한 공개키를 전자인증서라고 부른다. 그림 11과 같이 인증기관 위에 상위인증기관을 둔다면 은행과 소비자간에 망으로 연결될 것이다. 현실세계에 비유하면 정부와 주민등록증이 인증기관과 전자인증서이다. 오직 한 개의 인증기관이 전세계, 전 가상공간의 인증기관 역할을 할 수는 없을 것이다.

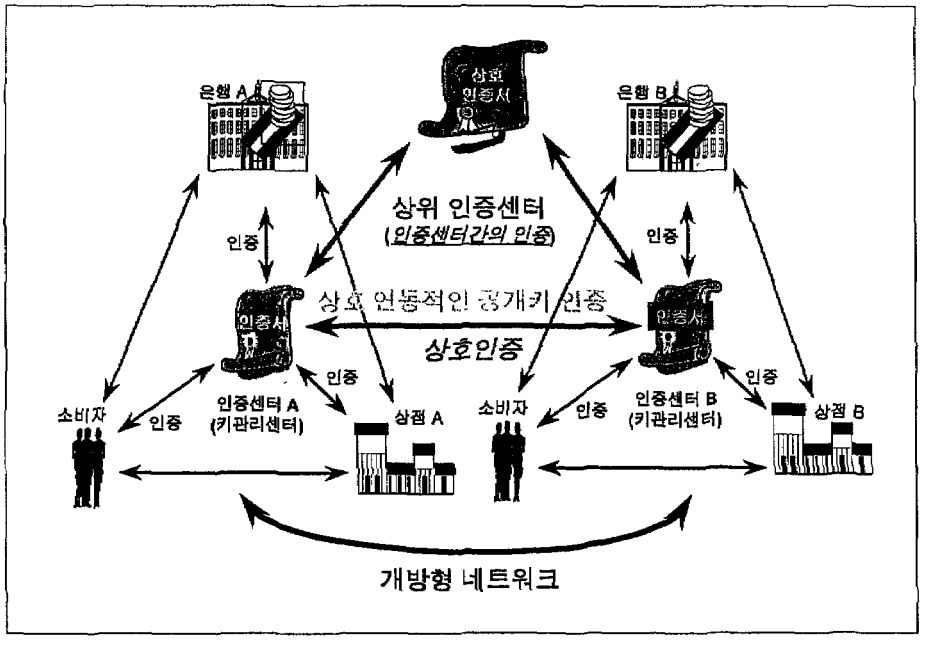

Figure 11. Typical model of electronic commerce.

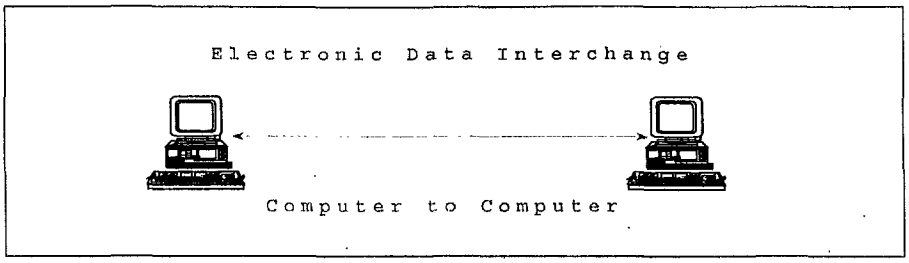

Figure 12. Way of EDI exchange

그러나 국내 전자상거래 서비스 업체의 대부분은 자체조사를 통해 인증하는 방법을 사용하는 것으로 나타났다.[6] 이럴 경우 상당한 비용과 자원이 소요되고 구매자의 경우는 쇼핑몰마다 계속 인증받아야 하는 불편함이 있다. 그래서 이런 인증문제를 풀기 위해 신뢰할 수 있는 인증기관이 설립되고 그림 11과 같은 CA 계층구조를 구성하여 편리하게 쇼핑몰을 사용할 수 있도록 해야한다.

3) 형태 면

인쇄되어 나오는 모든 문자는 컴퓨터에서 입력할 수 있게 되어있는데 행정의 근간이 되는 문서전산화의 대표적인 EDI는 Electronic Data Interchange의 약자로서 거래상대방과의 표준화된 일정 형태의 전자 문서를 합의된 통신표준에 따라 교환하는 새로운 정보전달 방식이라 할 수 있겠다.

종이대신 전자적 수단을 이용하고 문서를 우편이나 전화, 인편등 재래식 방식이 아닌 두 대 이상의 컴퓨터를 상호 연결하여 전자적 수단으로 정보를 전송하는 방법이다. EDI를 구현하기 위해서는 선결요건이 있어야 하는데 거래당사자가 주고받을 적절한 표준전자문서가 필요하고 이를 작성하고 처리할 업무처리시스템이 필요한데 전산상에서 이루어지므로 보안기능을 지닌 통신 및 변환 소프트웨어가 있어야 된다.[13] EDI는 기존의 수작업 문서처리과정에서 전산화한다는 큰 장점을 지니며 국내업계의 국제 경쟁력향상을 도모하는 산업의 기간구조라고 할 수 있다. 일찍이 마이크로소프트사

의 경우 회장인 빌게이츠가 의도적으로 전자결재등 종이 없는 사무실을 만들기 위해 노력한 결과 수백억원의 경제적 이익을 가져왔다고 한다.[5] 이처럼 최고경영자가 EDI에 관한 인식이 존재할 때 이는 급속히 발전할 수 있다. 우리 나라에서도 EDI도입을 위해 전자문서에 대한 법적인 효력인정, 세무, 회계법상의 EDI문서와 효력인정등을 요청하는 등 법제도 정비에 있고 EDI에 표준거래서식의 완료가 필요하다. 우리 나라의 경우는 한국 EDIFACT(KEB)가 지난 91년에 설립되어 UN/EDIFACT에 대응하는 한국 표준을 개발안내 보급하는 중이다. EDI는 단순O/A 프로그램이 아닌 비즈니스 리엔지니어링툴로 이해하여야 한다.

현재 시행되는 국내의 EDI를 예로 들면 무역 EDI를 시행할 경우 기존업무데이터의 70-80%가 재 입력되는 비효율성을 막을 수 있으리라 본다.

그림 13과 같이 요즘 국제규격으로 사용되는 거래문서인 EDIFACT를 보면 인터넷을 통신매체로 하여 자료교환전송- MHS(X.400), Pedi(X.435)을 사용하였고 'Data Element'는 메시지를 구성하는 기본단위로 국제 표준인 ISO 7372(TDED) 사용하였으며 데이터 항목의 명칭, 정의 , 유형, 길이, 사용 가능한 코드 목록 등을 정의하였다. 'Syntax'는 전송할 정보를 구조화하기 위한 규칙과 사용 가능한 문자집합으로 국제 표준인 ISO 9735에서 규정하였다. 그러나 이제는 인터넷시대로서 폐쇄적인 네트워크인 VAN을 경유하지 않고 자료교환 엔벨로핑(Enveloping)프로토콜이 기존의 EDI(MHS 표준인 X.400/ X.435)와는 다른 SMTP/MIME 프로토콜, FTP, Web(HTTP)등을 활용하게 될 것이다.

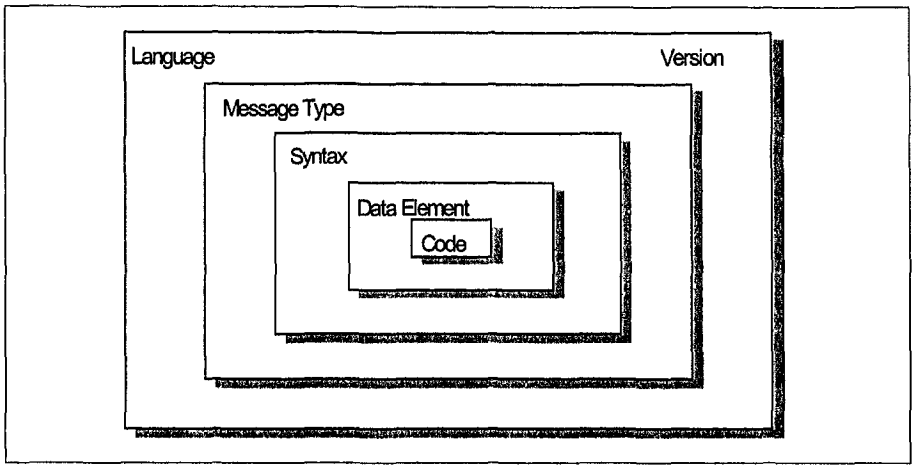

Figure 13. Structure of EDIFACT

2. 제안 프로토콜

첫 번째로는 몇 백원 정도의 금액을 지불하는 초소액 지불 시스템을 사용할 때 구매자와 판매자 사이에서 일어나는 구매요청 및 지불처리과정에 소요되는 비용을 줄여 효율성을 높이는데 있다. 판매자는 구매자가 지불하는 전자화폐의 유효성을 확인하고자 중개인과 네트워크의 상호작용을 통신으로 이용하게 되고 많은 구매자가 몰릴 경우에는 병목현상이 발생하게 된다. 또한 구매자가 새로운 판매자와 거래를 원할 때마다 거래도중에 각 판매자에게 맞는 화폐를 중개인으로부터 사오거나 혹은 생성하는 절차를 거쳐야 하는 것이 기존 소액지불시스템의 한계이다. 다음 가정에서 고객이 신용한도를 초과하여 사용하는 것을 방지하여 한도 내에서만 사용이 가능하도록 제한한다.

구매자 U

판매자 V

중개인 B

이라 할 때 B는 C라는 카드를 만든다.

회원으로 등록되는 모든 이들에게 계정을 만들어주고 계좌이체나 신용카드를 통해 구매자가 일정액을 적립한 C를 만들어 보내 준다. B는 C를 만들어 준 금액에 해당하는 값을 V에게 알려준다. V는 그 값을 일치되는 회원의 계정에 토큰링 식으로 연결하여 놓는다. 일방향 해쉬함수를 만들어 파라미터(Wn)와 토큰링수(n)를 대응시킨다. U는 구매시 판매자에게 C에 있는 고유번호로 지불을 요청한다. 이때 V는 요청한 금액만큼을 토큰링 식에서 제하여 나간다. 이와같이 선불형태로 지불하는 계정 기반 시스템의 경우를 제안하며 이는 거래 비용을 낮게 유지할 수 있을 뿐만 아니라 B와 V가 항상 연결되어 있지 않고 또한 미리 입력된 판매자의 계정으로 인해 중개인을 거치지 않고 바로 구매자와 판매자가 거래를 할 수 있는 장점이 있다.

둘째로는 인터넷에서 사용되는 하이퍼텍스트 문서들은 HTML(Hyper Text Markup Language)이라는 언어로 만들어졌는데 누구나 사용하기 쉽도록 만들어져 있을 뿐만 아니라 편집기 또한 많이 개발되어 있다. 확장성과 이식성이 뛰어나 대부분의 인터넷 사용자들이 사용하고 있는데 공통언어이므로 그 소스는 누구나 열람할 수 있고 수정 가능하다. 본 시스템은 보안상 노출되지 않는 언어를 사용해야 하는바 Microsoft사에서 만든 인터넷개발도구인 ASP(Active Server Page)를 사용하였다. ASP언어는 본 시스템이 사용되는 Window NT환경에서 사용되며 서버에서는 요청된 값만 데이터베이스에서 불러내어 웹브라우저로 돌려주므로 소스가 노출되지 않고 메모리낭비를 초래하거나 CPU에 부담을 주지 않고 마치 threading(동시병행수행)과 같이 동작하는 장점이 있다.

3. 학적서비스를 테마로한 업무분석

우리가 쓰고 있는 인터넷은 컴퓨터환경으로 디지털환경이며 모든 세계가 0과 1로 가장 규격화된 세계이다. 인터넷환경에서 오고가는 정보나 자료가 중간에 누군가에 의해 가로채지면 문제는 심각하다. 그런 보안상 허점이 있다 하더라도 중요정보가 오고가지 않는다면 그다지 큰 문제를 일으키지는 않을 것이다. 그러나 거래가 성립되기 위해서는 돈과 관계되는 정보가 노출되고 본 논문에서 다루는 증명서비스도 개인에게는 특별한 정보이므로 강력한 보안시스템이 필요하다. 열려져 있는 인터넷의 공간에서 정보를 보호막으로 싸서 안전하게 주고받는 것은 아이러니라고 할 수 있다. 학교입학이나 기업입사등에 많이 쓰이는 것이 대학의 증명서이고 종이한장이 갖는 가치는 일생을 좌우할 수 있는 것이어서 문서의 유출이나 보안등에 강력히 대응해야 하는데 그림14에 보안위협요소와 대책을 나타내었다.

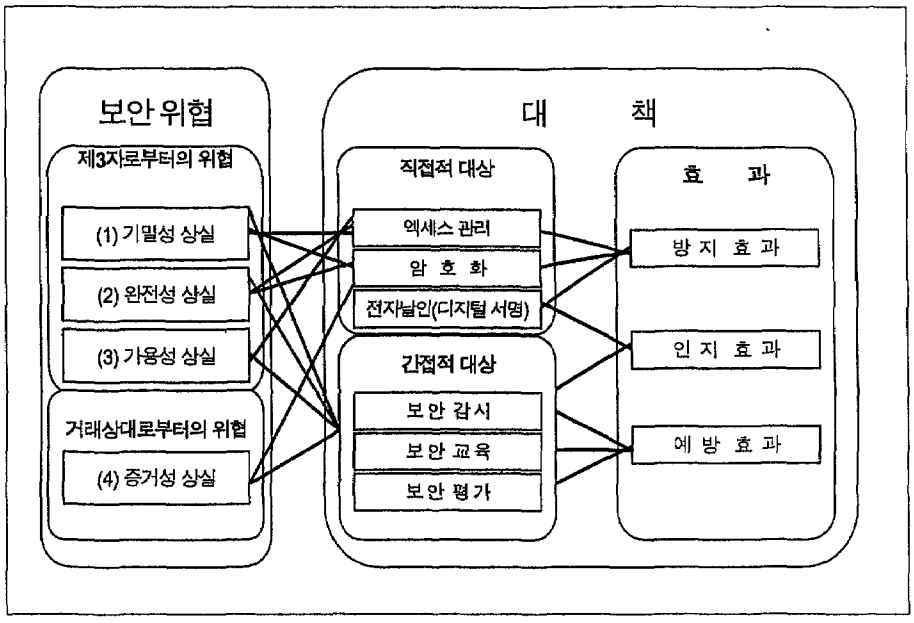

Figure 14. Violence & contract of bastion

일반전자상거래와 달리 보내는 사람이 본인이라는 증명과 또 꼭 받았다고 하는 부인방지가 필요하다. 이를 이용할 수 있는 대학의 데이터베이스 및 인증기관, 지불처리기관등의 서버도 안전을 위해 큰 용량의 것이 요구된다.

그림 15와 같이 증명서가 유출되거나 변조되는 경우 혹은 민원인이 부인하는 경우 등의 방지와 확인을 위해 물리적 보안망인 방화벽(firewall)을 구축하고 비대칭형 암호화 시스템 도입으로 공개키를 부여하고 인증부분에서 언급되었던 전자서명과 전자인증서등의 장치를 마련한 뒤 대학의 인증기관, 전자지불, 학사데이타베이스등의 서버에 연동하도록 한다.

각 컴포넌트들이 어떤 보안규약을 따르고 그 내용이 무엇인지를 Table1에 나타내었다.

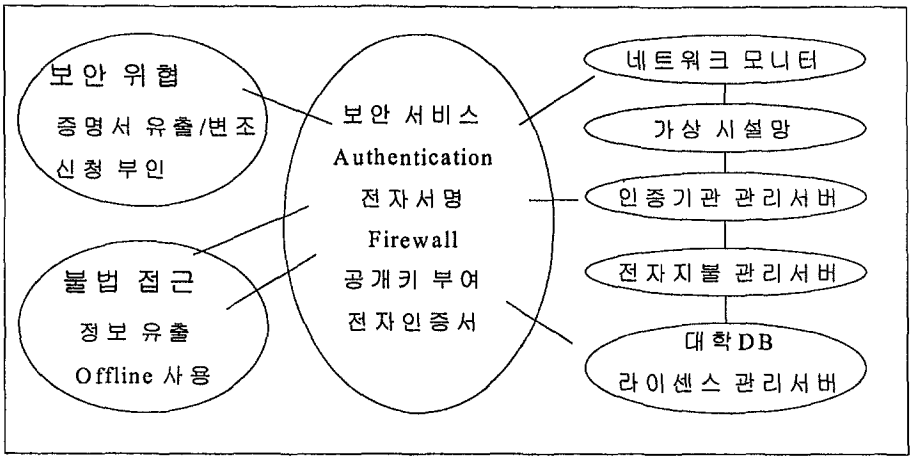

Figure 15. Model for security service

Table 1. Relation of security components

컴포넌트	지원하는 보안 규약	보안 내용
라이센스관리서버	Confidentiality(ITU-T/RFC) Integrity(ITU-T/RFC) Network Service Harmonized Secuary(ITU-T) Unauthorized Copywriting	증명서 전송의 제어 증명서 검색의 제어 지적 재산 유통의 권한 제어
네트워크 모니터	Authentication(ITU-T/RFC) Auditability(ITU-T)	크래커 감시 추적 네트워크 진단/감시 보안 침해 경고 감시 추적 정보관리(SIB)
가상 사설망	Linoting network Access(RFC) Network Service Operational Service(ITU-T) Network Connection on Firewall	가상 사설망 구축 네트워크/호스트 시스템 접속 제어 부가서비스 이용의 차등제어

4. 증명시스템의 순서도 및 흐름도

학교 홈페이지에 접속하여 ①신원을 인증받은 뒤 다시 전자인증으로 법적인 신분을 확인받는다. 다시 자동 리턴된 증명신청화면에서 전자상거래와 같이 증명서를 신청한다. ②전자 지불처리기관으로 가서 금액을 지불한다. 지불처리기관은 신용도와 본인을 확인한 후 지불OK가 떨어지면 관리서버로 와서 학사DB를 검색하여 이에 맞는 파일을 얻는다. 민원인이 요청한 메뉴로 문서를 파일화한다. ③이 문서를 암호화 시켜서 이를 전자봉투로 Parcel한다. ④전자서명하며 인터넷 공간에 띄운다. ⑤해당자는 송신자의 공개키로 전자서명을 복호화한다. ⑥수신자의 비밀키로 메시지를 복호화한다. ⑦다운받아 설치되어 있던 EDI transfer를 이용해서 증명서를 출력한다. 이에 대한 순서도를 그림 16에, 흐름도를 그림 17에 나타내었다.[5]

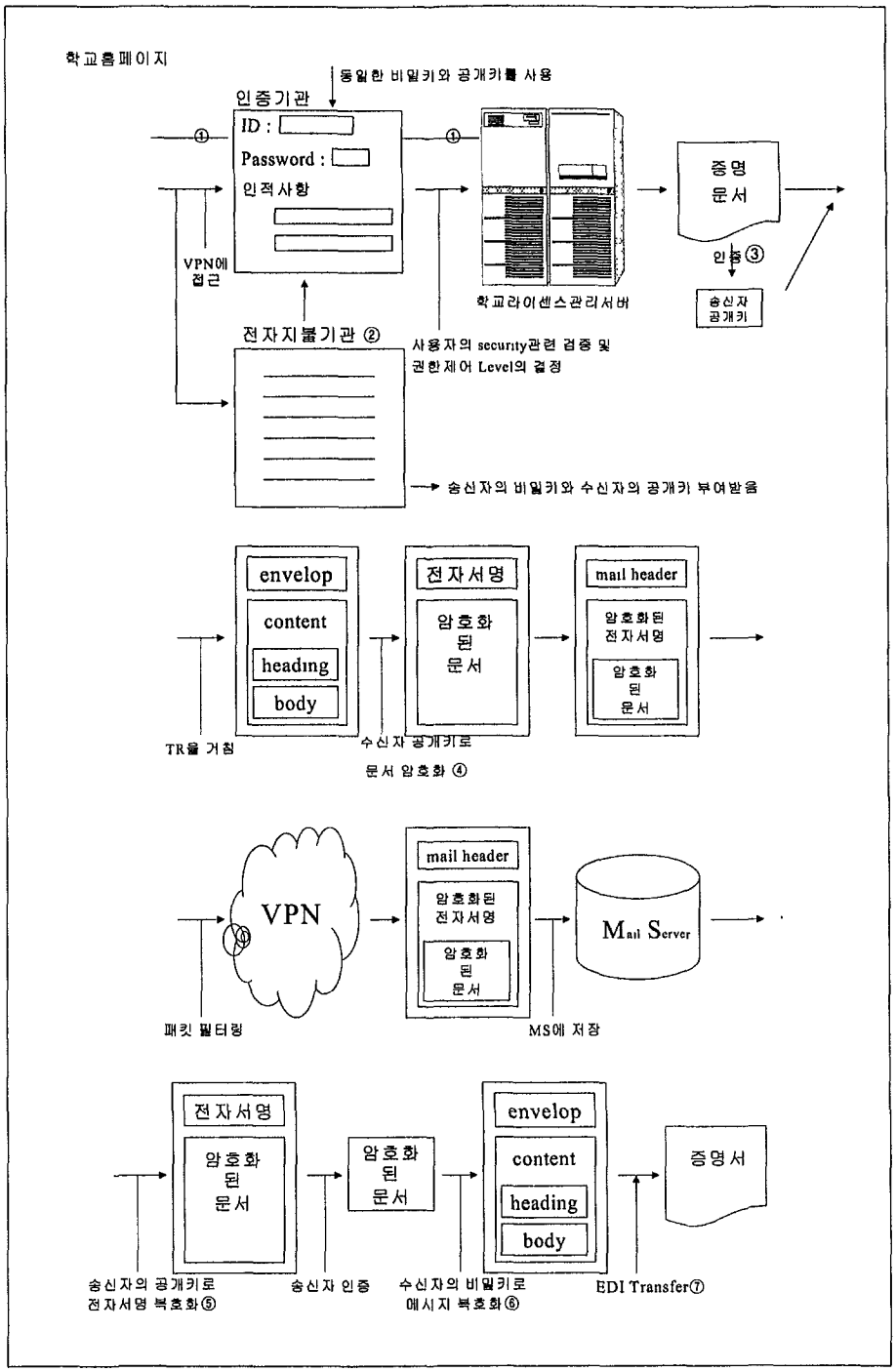

Figure 16. Process for issue of academic certificate

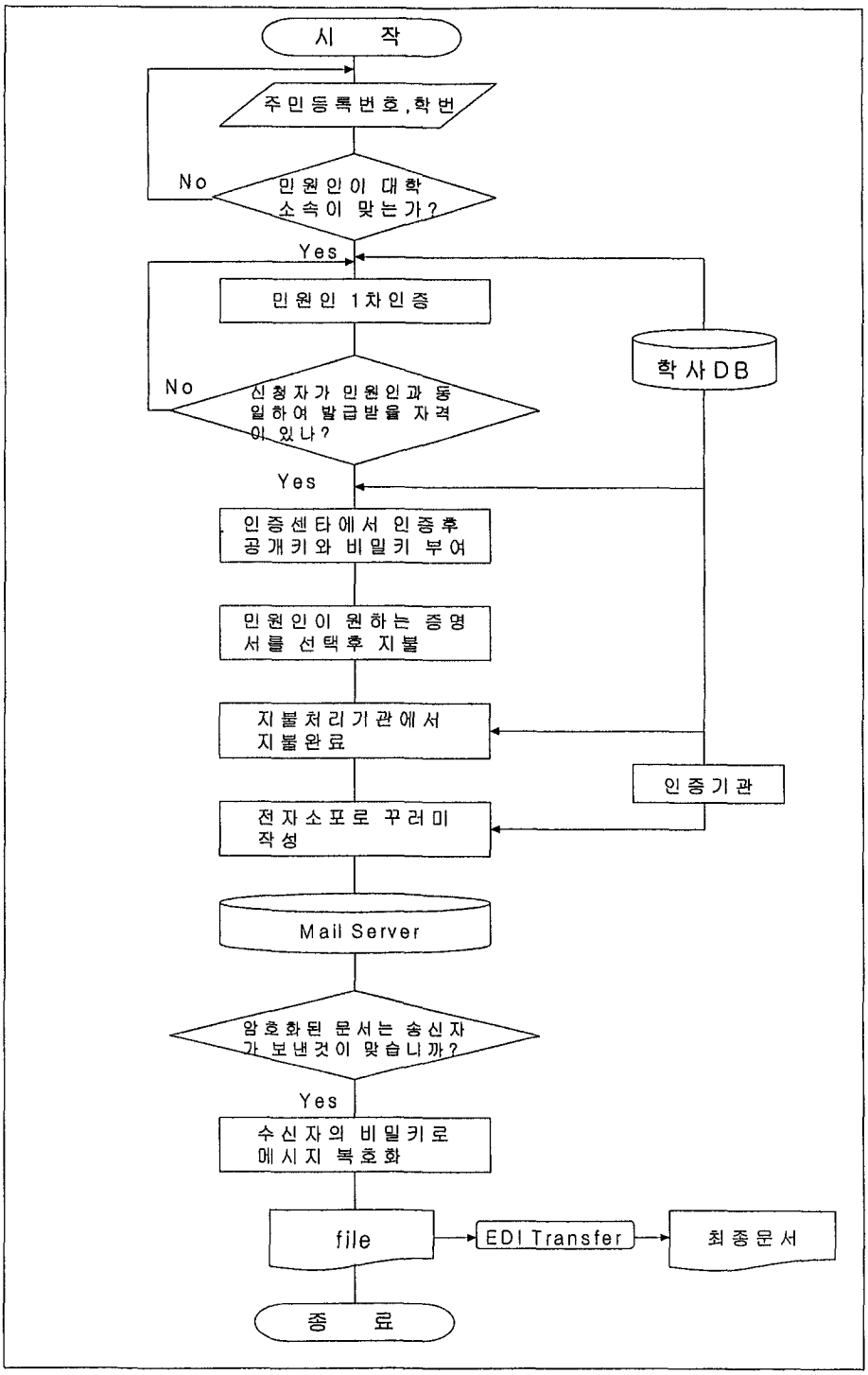

Figure 17. Flow chart of the academic certificate issuance system

IV 학사 서비스 시스템의 구현

본 장에서는 장비를 이용하여 프로그램을 만들고 이를 인터넷상에 띄어 구현하였고 그 구현되는 결과를 화면으로 나타내었다.

1. 서버 시스템 및 네트워크

인터넷 익스플로러 5.0과 IIS 서버를 이용하여 서버를 구축하였고 사용자는 486이상의 퍼스널 컴퓨터에서 사용할 수 있도록 하였다. 한국통신의 kornet망과 지불기관의 inet망으로서 연결되었고 인증기관은 학교 내에 두어 가상사설망으로 연결함이 바람직하며 본 실험에서는 사용하지 않았다. 상세한 개발환경은 표2에 정리하였다.

Table 2. Environment for the experiment

하드웨어	CPU	Pentium 400Mhz
	RAM	64MB
	Graphic Card	VIDA IGP-PCI(800*600,16bit color)
	CD-ROM Drive	삼성전자 40배속
	Moniter	삼성 SyncMaster 500p
소프트웨어	유틸리티	Front Page 98, Namo Editer, 어도비 포토샵 4.01
	운영체제	WINDOW NT Server 4.0
	프로그램	Active Server Page

2. 구현의 범위 및 결과

그림 18과 같이 학교 홈페이지에 화면을 나타내었다. 홈페이지에서 기본 신상인 학번과 주민등록번호를 입력하고 신청을 하면 인터넷을 통해 전송될 때 암호화되어 학사DB로 접속후 DB에 있을 경우 리턴 값으로 나타난다. 여기서 사용한 소스코드는 부록A-1에 수록하였다.

민원인이 확인되었다는 화면이 그림 19과 같이 나타난다. 여기서 다시 인증신청을 하는데 수신자가 본인이다라는 것과 학교측에 접수가 되었다는 법적인 근거를 받는 것이다. 그림 20에서와 같이 인증센타에서 인증을 받고 민원인은 공개키와 비밀키를 부여받았으며 이를 이용하여 수신시에도 사용하게 된다. 이제 비로소 증명을 신청할 자격이 생겼으므로 증명서 신청 페이지로 간다. 그림 21의 오른쪽 왼쪽 상단 메뉴에서 어떤 증명서를 신청할 것인가를 선택한다. 신청후 전자지불을 선택한다. 그러면 아래와 같은 화면이 나오고 소액지불전용인 인터넷카드를 이용해서 신청한다.

모든 사항을 입력한 후에 Form을 통해 지불하면 그림 22과 같은 화면으로 구성이 된다. 여기서 사용한 소스코드는 부록A-2에 수록하였다.

지불이 완료되었을 시는 그림 23와 같은 화면이 나타나고 지불이 완료되지 않았을 경우는 그림 24과 같은 화면으로 표시된다.

이렇게 지불처리가 완료되면 라이센스관리서버(증명서서버)로 자료가 넘어가고 그 자료를 가지고 학사DB를 돌려서 해당되는 문서 폼에 맞는 필드들을 불러오고 그 필드들을 조합하여 문서를 만들었다. 첫 번째 구현은 관리자는 그림25와 같이 그 문서를 출력시켜 일반문서와 같이 직인 등을 이용하여 실생활에 사용되게 하였다.

두 번째 구현은 지불완료된후 문서가 관리자 서버로 넘어가서 관리자는 이를 전자인증하고 파일화시킨다. 이렇게 문서를 인터넷상에서 받게 될 경우 이를 관리해야 하는데 그림 26와 같은 관리자모드를 만들어 매일의 증명서 발급현황을 볼 수 있도록 하였다.

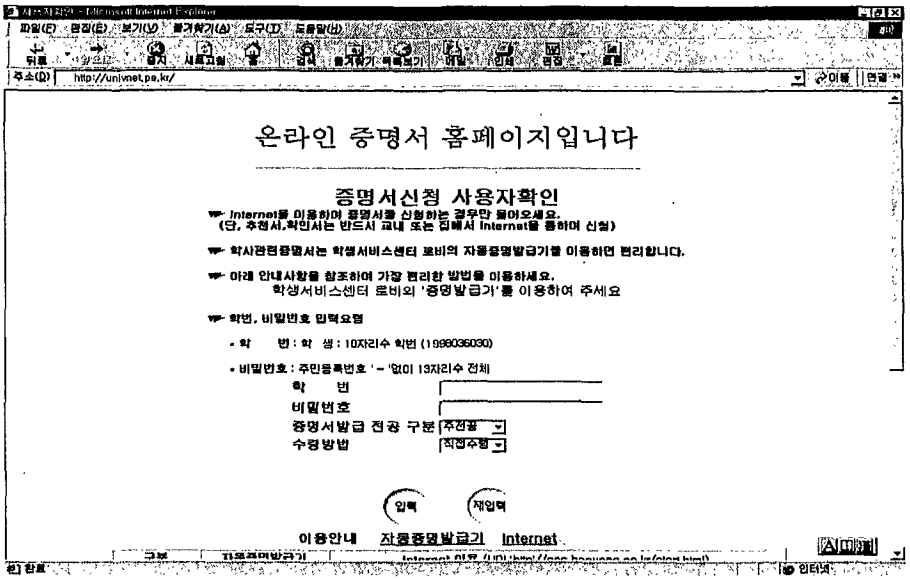

Figure 18. Display of homepage

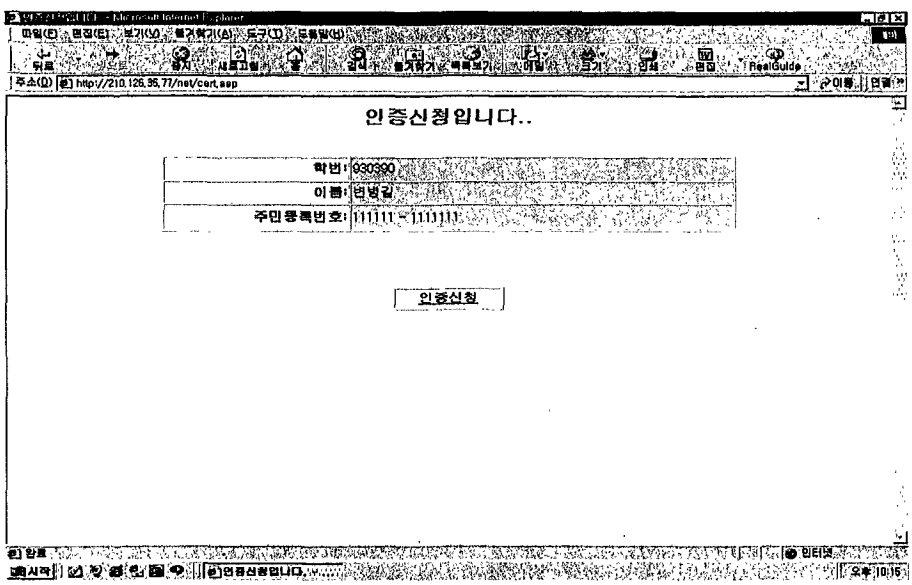

Figure 19. Display of successful login process

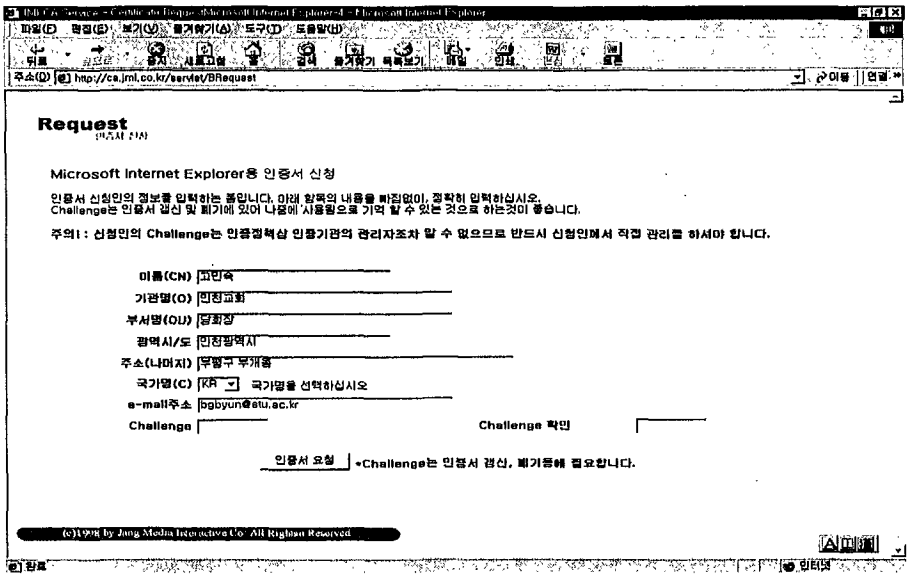

Figure 20. Display of successful authentication at CA center

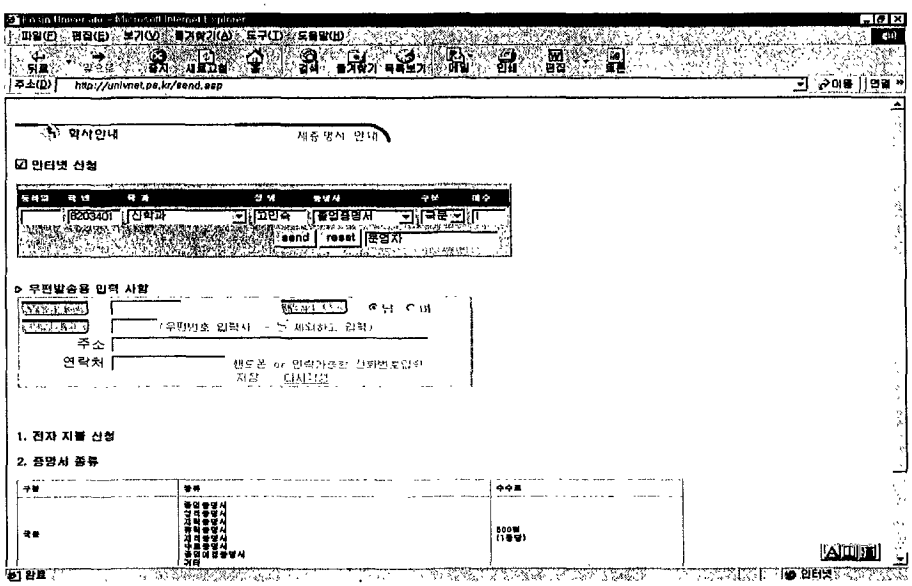

Figure 21. Display of the first order

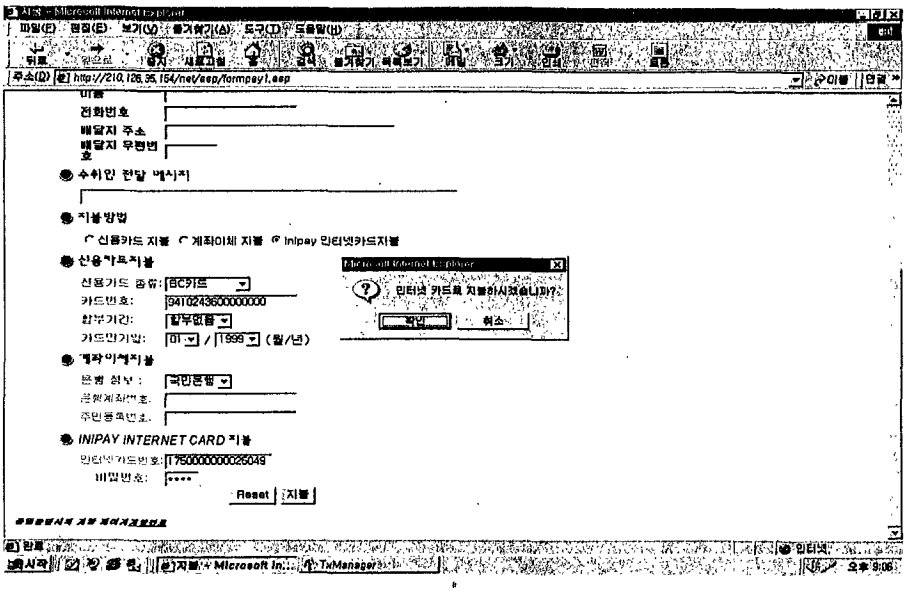

Figure 22. Display of payment order

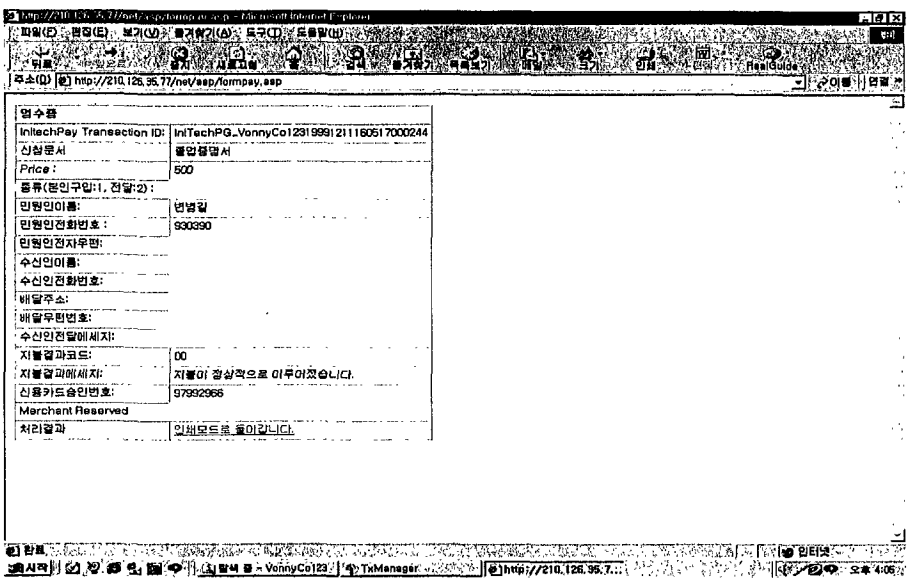

Figure 23. Display of complete payment

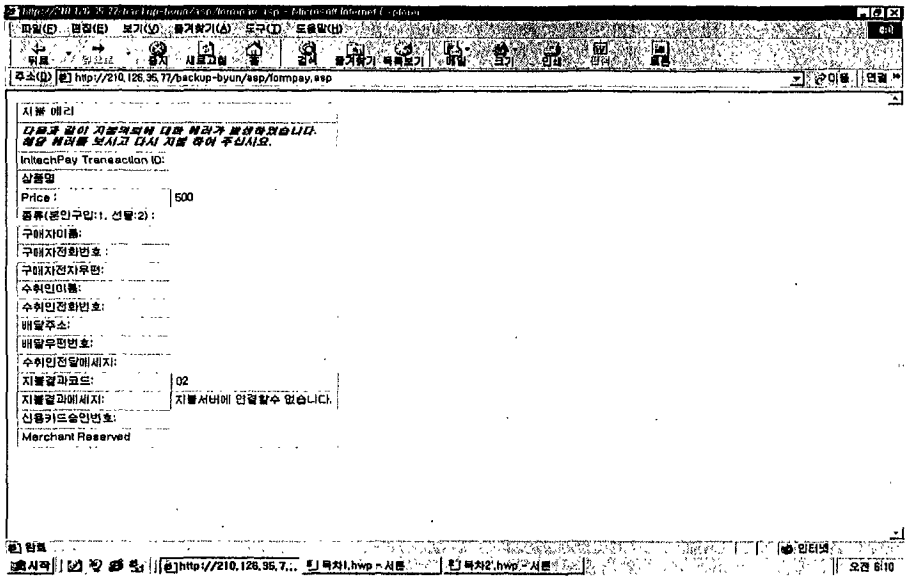

Figure 24. Display of incompleted payment

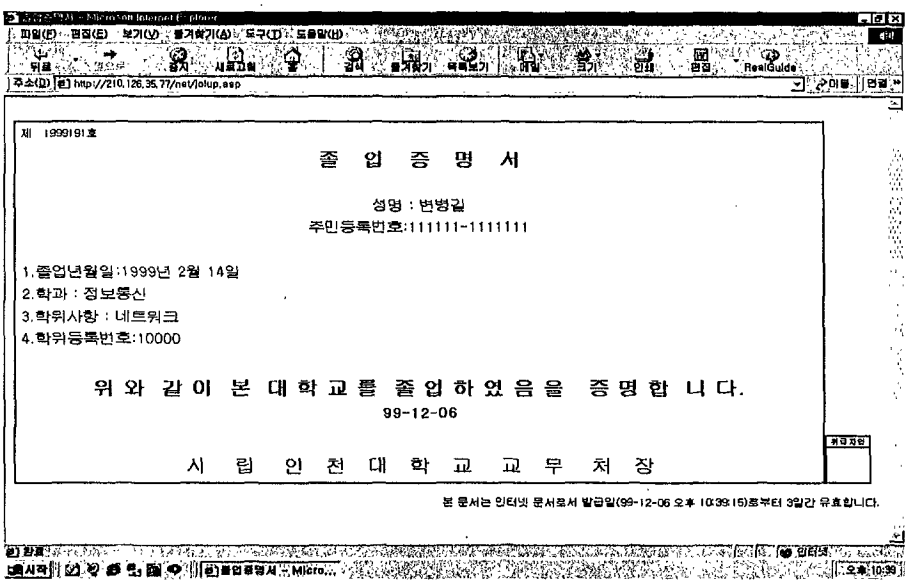

Figure 25. Display of the output certificate

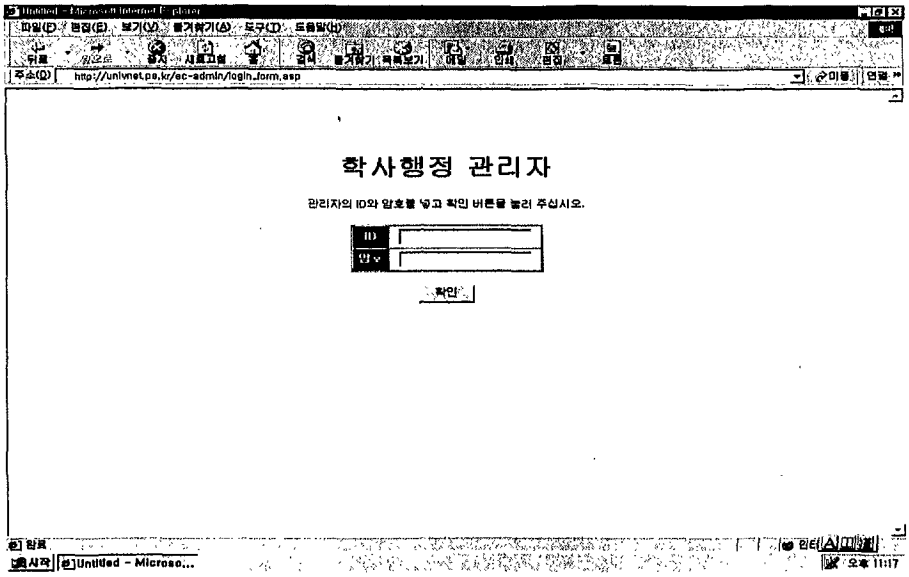

Figure 26. Display of manager mode

V 결론

전자상거래가 최근 들어 증가추세에 있으나 이에 따라 그 폐해도 있어 일부에서는 도입시기를 늦추고 있으나 앞으로의 방향성으로 볼 때 전자상거래는 필수상황이 될 것이다.

본론에서는 소액전자 지불 시스템의 원리와 종류를 분석하였고, 예상되는 보안의 문제를 공개키 암호화방식을 통한 인증과 SSL의 암호알고리즘 및 ASP언어등을 이용하여 학적증명서를 현재 상용화되고 있는 소액지불 시스템과 연결하여 인터넷을 통해 신청하고 인증과 지불을 마치고 발급 받을 수 있는 시스템을 구현하였다. 특히 인터넷을 통한 학사 시스템에서 고려해야 할 보안문제에 초점을 맞추어 해결 방안을 제시하였다.

현재까지는 많은 학생들이 휴학 등을 하기 위해서는 지도교수를 포함하여 여러 부서를 거쳐 도장을 받아와야 했으며 졸업생들은 직접학교에 나오거나 몇백 킬로미터 떨어진 곳에서는 증명서를 얻기 위해서는 우편으로 며칠씩 걸려야 했다. 이제 학교에서도 인터넷환경에 맞도록 모든 행정서비스가 이루어진다고 가정할 때 본 논문에서는 인터넷으로 학사EDI시스템을 구축하여 실시간 정보를 받고자하는 학사증명서를 소액 지불하는 시스템을 구현하였는 바 Window NT에서 잘 구현되도록 Active Server Page로 프로그램화하였으며 데이터베이스도 SQL에 맞게 변형하여 학사DB 및 Application서버, 지불서버에서 잘 연동되도록 하는 기법을 사용하였다.

앞으로 본 논문에서 다루지 못한 데이터베이스와의 연결될 때의 보안 알고리즘을 적용문제 및 자체적으로 CA서버를 구성하여 UNIX나 모든 서버에서도 연동될 수 있도록 시스템을 개발해 나가야 하며 완전한 전자 상거래가 이루어지기 위해서는 파일을 암호화하고 전자인증부분을 개발해야 될 과제를 갖고 있으며 향후 디지털 콘텐츠의 전자상거래가 발전하도록 학교기관이나 관공서 등에서도 많은 응용과 도입이 필요하다고 본다.

참 고 문 헌

1. 대니얼 C.린치/레즐리 런키스트, 「digital money」, PC Line, 1996년
2. 박도현, "인터네트상에서의 정보상품 거래를 위한 초소액지불시스템의 설계", 한국과학기술원, 석사학위논문, 1996, pp.1-7
3. 박범수, "전자상거래를 위한 전자지불 시스템에 관한 조사연구" 한양대학교 산업경영대학원, 1998, pp.46-47
4. 박상진, 「인터넷쇼핑몰운영/이용자 설문조사」,Web Business, 1999년 5월
5. 변병길,이기영,"학적서비스를 위한 소액 지불시스템의 구현",한국통신학회 추계종합학술발표회, 1999년 11월
6. 빌게이츠, 「생각의 속도」, 청림출판, 1999년
7. 이재규, 「전자상거래 원론」 법영사, 1999년
8. 전국대학학생서비스센타 연합회 1999년 4월
9. 조경훈, 「전자상거래통합 솔루션의 대결」 마이크로소프트웨어 1998년 3월 pp.222-223
10. 이재광,이용준,박성열 공역,「인터넷방화벽과 네트워크 보안」, 이한출판사,1996년
11. 전국대학홈페이지주소 ,「2000학년도대입전형계획주요사항」, 대교협, 1999년 3월
12. 한양대학교 학생서비스센터, 조정환, 설문조사 1999년 5월 홈페이지 http://hanyanguniv.pe.kr
13. Phyllis.k.Sokol, 「From EDI to Electronic Commerce」, McGrawHill, Inc 1996 p.20
14. Computer world(美), http://hitech.co.kr/past/980905/70-2.htm
15. SFNB, http://210.104.142.1/html/s_site/hnsu/sfnb/www_sfnb_com.html
16. Tim berners lee, "Weaving the web" http://www.any-book.com/weaving_the_web.htm
17. 김진호, "전자상거래의 모든 것", http://mm.ewha.ac.kr/~jhkim/ 972project/bs8/example.html
18. 넷빌, http://www.ini.cnu.edu/NETBILL
19. 넷체크, http://nii.isi.edu/info/netcheque
20. 넷캐시, http://nii-server.isi.edu/info/Netcash

21. 데이콤, http://ecredit.dacom.co.kr
22. 밀리센트, http://www.research.digital.com/SEC/milicent
23. 사이버캐쉬, http://www.cybercash.com/cybercash/wallet/userguide21
24. 아이캐쉬, http://www.icash.co.kr
25. 애니카드, http://anycard.co.kr
26. 이니텍, http://www.initech.com/about/product.html
27. 이지페이, http://easypay.kicc.co.kr
28. 퍼스트버츄얼, http://www.fv.com
29. 한국전산원, http://www.nca.or.kr/

부 록

A-1 사용자 확인 프로그램
A-2 지불요청 프로그램

A-1 사용자 확인 프로그램

```
'민원인이 증명서를 신청하기 위해 학번과 비밀번호 입력시 확인하는 프로그램
<html>
<head>
<title>사용자확인</title>
<script language="javascript">
<!--
function sendit()
{
  var str;
  str = document.login._id.value;
  if(str==""){
    alert("학번을 기입하여야 합니다.");
    document.login._id.focus();
    return true;
  }
  var ssn1 = document.login._ssn1.value;'비밀번호를 DB에서 체크
  var ssn2 = document.login._ssn2.value;'비밀번호를 DB에서 체크
  if((ssn1.length !=6)||(ssn2.length !=7)){
    alert("주민등록번호가 제대로 기입되지 않았습니다.");
    document.login._ssn1.focus();
    return true;
  }
  document.login.submit();
  return true;
}
function OnlyNumber()
{
  if((event.keyCode<48)||(event.keyCode>57))
    event.returnValue=false;
}
//-->
</script>
</head>
```

A-2 지불요청 프로그램

```
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=KS_C_5601">
<title>지불</title>
<meta name="generator" content="Microsoft FrontPage 4.0">
</head>

<body background="../img/back_2.gif" bgcolor="white" text="black" link="blue
 vlink="purple" alink="red">

<p><!--------
 1. verifyflag 는 hidden tag 로 넘긴다.
 2. merchantreserved 는 hidden tag로 넘기되,
    merchantreserved2, merchantreserved3와 구별되어야 한다.
 3. quotainterest 는 hidden tag로 넘긴다.
 4. authentification 는 hidden tag 로 넘긴다.
 5. authfield1,2,3 는 입력을 받도록 한다.
---------->></p>
<!--------
----------------------------------------
인터넷 카드 지불
----------------------------------------
1. 페이지를 같이 하는 경우
 - paymethod는 'card' 이고
 - 지불방법중 인터넷 카드의 구별은 paytype쿼리로 한다.

   인터넷 카드의 경우
     - 인터넷카드의 쿼리명은 icardnum, 비밀번호는 icardpwd로 한다.
     - 비밀번호(숫자) 4자리를 받아 cardexpy, cardexpm에 두자리씩 복사한다
     - icardnum을 cardnumber에 복사한다.

2. 페이지를 따로 가는 경우
        - cardnumber,cardquota,cardexpm,cardexpy는 hidden으로 한다.
        - 인터넷 카드번호의 쿼리명은 icardnum, 비밀번호는 icardpwd로 한다
        - 비밀번호(숫자) 4자리를 받아 cardexpy, cardexpm에 두자리씩
복사한다.
        - icardnum을 cardnumber에 복사한다.
```

```
---------->
<script language="javascript">
function valid_check(form)
{
  var Digit='1234567890'
  var target= form.icardpwd
  var ipass=form.icardpwd.value
  var icard= form.icardnum.value
  var i

  m= form.creditcardexpm.selectedIndex
  y= form.creditcardexpy.selectedIndex


  //인터넷카드지불
  else{
        if(ipass.length != 4) {
        alert('비밀번호는 네자리만 가능합니다.')
    target.focus()
        return false
        }
        for(i=0;i< ipass.length;i++)
    if(Digit.indexOf(ipass.substring(i,i+1))<0) {
        alert('비밀번호는 숫자만 가능합니다.')
        target.focus()
        return false
    }

        form.paymethod.value = "Card"

        form.cardexpy.value= ipass.substring(0,2)
        form.cardexpm.value= ipass.substring(2,4)
        form.cardnumber.value= icard

        if(confirm('인터넷 카드로 지불하시겠습니까?') == false)
                return false
  return true
  }
}
```

```
<input
            type="radio" name="paytype" value="icard" checked><font
size="2">Inipay
            인터넷카드지불</font> </td>
    </tr>
    <tr>
        <th align="left"
colspan="3"><p>        <img
src="../img/tit_06.gif"
            width="116" height="30" border="0"></th>
        <td></td>
    </tr>
    <tr>
        <th width="75" align="center"><p> </th>
        <td><p><font size="2" color="red">주민등록번호:</font></td>
        <td width="416" height="25"><p><input type="text"
name="regnumber"></td>
        <td></td>
    </tr>
    <tr>
        <th align="left"
colspan="3"><p>        <img
src="../img/tit_08.gif"
            width="227" height="29" border="0"></th>
        <td></td>
    </tr>
    <tr>
        <th width="75" align="center"><p> </th>
        <td><p><font size="2" color="red">인터넷카드번호: </font></td>
        <td width="416" height="25"><p><input type="text" name="icardnum"
value="1750000000025049"
            size="16"></td>
        <td></td>
    </tr>
    <tr>
        <th width="75" align="center"><p> </th>
        <th align="center"><p><font size="2" color="red">비밀번호:
</font></th>
        <td width="416" height="23"><p><input type="password"
```

```
name="icardpwd"
                value="5555" maxlength="4" size="4"> </td>
            <td></td>
h       </tr>
        <tr>
            <th align="center" colspan="3"><p><input type="reset" value="Reset">
                <input type="submit" value="지불"></th>
            <td></td>
        </tr>
</table>
</form>
<h6><i><%=session("list")%>의 지불 페이지<a
href="../print.asp">지불완료</i></h6>
        </a>
</body>
</html>
```

ABSTRACT

Implementation of an Academic EDI System Using Micropayment System on Internet

Byung Kil, Byun
Graduate School of Information and Telecommunications,
University of Inchon
Inchon, Korea.

As the Electronic Commerce (EC) based on the Internet is widely used the main concerns of EC in the future is going to be exchange of electronic information such as online publishing, database service, and software distribution.

Major of the academic registrar service at the universities is issuance issuance of various academic certificate, and many educational institutions try to do this process using the EC concept. The micro-payment system is necessary as major payment method.

In this thesis, the principle of micro-payment system is reviewed and several kinds of practical system are analyzed. And we design and implement the proposed system that can offer request, payment and issue the certificate and user authentication based on the Internet by micro-payment system.

Especially, we focus on network security problems that may occur at the academic registrar system through the internet and suggest some possible solutions.

감사의 글

먼저 하나님께 감사드립니다.

어둡고 긴 터널에서 길을 찾고 있을 때 종착점까지 밝은 횃불로 인도하여 주신 이 기영교수님께 깊은 감사를 드립니다.

또한 저의 미천한 논문을 심사해주시고 격려해 주신 최승국 교수님과 김연수교수님께 감사의 마음을 전합니다.

정보통신대학원에서 좋은 말씀으로 지도해주신 민홍기교수님, 우요섭교수님, 최진탁교수님, 조중휘교수님, 민병준교수님께 감사드립니다.

네트워크 연구실에 한자리 내어준 연구원생들, 한 밤을 같이 세우고 많은 도움을 주었던 송영부(대학원 졸업 및 입사를 축하) 및 이기영학형에게 감사 드립니다.

같이 졸업하는 김영언씨,송길조 형님, 스터디 멤버였던 지차남, 이강운 원생 내 뒤를 이어 논문을 쓰게 될 정균이에게도 고마운 마음을 전합니다.

2년반동안 주경야독할 때 많은 배려를 해주셨던 이순성 과장님과 김정숙 과장님, 선배졸업자로서 좋은 말씀 해주신 김문섭 주임님, 이무옥, 윤택, 새신랑 문정호 선생님, 영원한 똥변설님의 성전도사님, 새내기 나은미 선생 및 서울신대 교직원 여러분, 옥자, 유진, 유미에게도 감사를 드립니다.

끝으로 자식 잘되기만을 위해 평생 살아오신 사랑하는 부모님, 학업을 이어주신 누님, 애정 어린 염려해주신 처식구들, 육아에 전념하느라 힘든데도 불구하고 묵묵히 뒷바라지해준 사랑하는 아내와 세상 빛을 본지 9개월된 하나님의 귀한 선물인 우영이에게 이 논문을 바칩니다.