[UCI]I804:24011-200000236008

2008년 2월
석사학위논문

네트워크형 전자상거래를 위한 인증 프로토콜 개선

조선대학교대학원
정보통신공학과
김 상 언

네트워크형 전자상거래를 위한 인증 프로토콜 개선

Certification Protocol Improvement for Networked Electronic Commerce

2008년 2월 25일

조선대학교대학원
정보통신공학과
김 상 언

네트워크형 전자상거래를 위한 인증 프로토콜 개선

지도교수 한 승 조

이 논문을 공학석사학위신청 논문으로 제출함.

2007년 10월

조선대학교대학원
정보통신공학과
김 상 언

김상언의 석사학위 논문을 인준함

위원장 조선대학교 교수 박 종 안 인

위 원 조선대학교 교수 최 광 석 인

위 원 조선대학교 교수 한 승 조 인

2007년 11월

조선대학교 대학원

목 차

도목차 ····· iii

표목차 ····· iv

ABSTRACT ····· v

제*1*장 서 론 ····· *1*

제*2*장 전자지불 시스템 현황 및 기반기술 ····· *5*

제1절 전자상거래 개요 ····· 5

제2절 전자상거래 보안 ····· 6

제3절 전자화폐 ····· 8

1. 전자화폐의 개념 ····· 8

2. 전자화폐의 장점과 문제점 ····· 10

3. 전자화폐의 분류 ····· 10

4. 전자화폐의 안전성 ····· 12

5. 전자화폐의 요구조건 ····· 12

5. 전자화폐 프로토콜 ····· 14

제*3*장 전자지불 시스템 분석 ····· *16*

제1절 지불 시스템 동향 ····· 16

제2절 지불 시스템 비교 분석 ····· 19

1. 시스템 비교 분석 ····· 19
2. NetBill 시스템 ····· 20
3. E-Cash 시스템 ····· 22
4. NetCash 시스템 ····· 23
5. SET(Secure Electronic Transaction) 시스템 ····· 24

제4장 프로토콜 설계 및 구현 ····· 29

제1절 제안한 프로토콜의 설계 ····· 29
제2절 제안한 프로토콜의 구현 및 결과 ····· 38

제5장 제안한 프로토콜의 분석 ····· 54

제1절 기존 전자지불 프로토콜과의 비교 및 성능분석 ····· 54
제2절 제안한 프로토콜의 안전성 및 효율성 ····· 60

제6장 결론 ····· 61

참고 문헌 ····· 63

도 목 차

그림 1 NetBill 거래 프로토콜 ····· 21
그림 2 제안된 프로토콜의 전체 흐름도 ····· 30
그림 3 상품 주문과 대금 지불의 동시처리 ····· 34
그림 4 주문 상품의 대금결제 및 접수 처리 ····· 35
그림 5 대금 지불에 대한 영수증 발행 ····· 36
그림 6 영수증 확인 및 검증 ····· 37
그림 7 로그인 ····· 39
그림 8 전자화폐지불시스템의 초기화면 ····· 40
그림 9 사용자 신규 등록 및 인증서 발급 ····· 41
그림 10 발급된 인증서 조회 ····· 41
그림 11 상품 구입을 위한 선택 ····· 42
그림 12 암호화 과정(주문 및 결제 요청) ····· 43
그림 13 복호화 과정(결제) ····· 45
그림 14 영수증 발행 ····· 48
그림 15 영수증 확인 ····· 51
그림 16 전자화폐 신청 및 구입 ····· 53
그림 17 상품 등록 ····· 53

표 목 차

표 1 전자화폐의 장·단점 ····· 10
표 2 전자화폐의 분류 ····· 11
표 3 각 시스템의 유형 및 기능 ····· 19
표 4 각 시스템의 추진 모체 ····· 20
표 5 C-Pay 프로토콜의 암화화 횟수 ····· 54
표 6 C-Pay 프로토콜의 실행시간 ····· 55
표 7 기존 전자 지불 프로토콜과의 비교 ····· 56
표 8 암호화 횟수 비교 ····· 59
표 9 통신 횟수 비교 ····· 59

ABSTRACT

Certification Protocol Improvement for Networked Electronic Commerce

Kim, Sang-Eun
Advisor: Prof. Han, Seung-Jo, Ph.D.
Department of Information & Communications,
Graduate School of Chosun University

In 21st century, only the society having the information can have competitive power. In this "Information Era", with rapid growth of use of Internet, the individual privacy and the personal information are becoming a major issue.

The method of payment is an important factor to success the commerce using the Internet. One of them is an electronic cash (e-cash) that has all characteristics of traditional commodity cash and ensures security for all transactions. Accordingly, an Internet billing system based on electronic cash is expected as the safe and efficient paying method in future e-commerce.

Though various services for the e-commerce on the Internet are being used, there is still lacking measures for ensuring the essential certification, the

security for the purchase and payment processes and the protection against information threats that may be happened in various types of transactions through the e-commerce. Accordingly, the researches into the electronic payment system are needed to guarantee the confidence and the service maintenance for protecting information.

Due to the fact that the e-cash can provide several merits including convenience, security and simplicity for an user and curtailment of cost such as marketing management expenses for a member store, the paying method with an e-cash also has lots of problems such as an individual information leakage and illegal use that should be solved in accordance with the demands of users because of the specificity of data being used in the network.

In this paper, we propose an electronic payment protocol with a network-type e-cash based on Public Key Infrastructure (PKI). The proposed protocol overcomes the problem of NetBill which deals with only contents and can't ensure anonymity. It also prevents illegal copy and distribution and insures the greatest safety by means of giving a certificating number to the digital contents offered on the on-line.

The operation is based on an E-mail sending program that has a distinguished security, PGP. The technique about certification and security is designed using Public Key Infrastructure. And the protocol is embodied in order to guarantee all kinds of the safeties, the efficiencies and the trusts on the threatening elements and the demands of the electronic payment protocol in the greatest degree.

제1장 서 론

제1절 연구 목적

무선 LAN은 매력적인 이동성과 유선 LAN에 근접한 속도를 지원하면서 개인 또는 기업의 사용자들에게 빌딩이나 캠퍼스 환경에서 전자상거래, 전자 메일, 데이터 전송과 같은 중요한 정보를 비밀리에 전달하고자 하는 보안성 요구가 더욱 증가하고 있다. 이는 무선매체의 공개성(Openness)에 따른 해킹의 용이성과, 단말의 이동에 따른 보안 체계의 복잡성에 기인한다. 따라서 최근 무선 LAN 기술에 있어서 보안성이 가장 중요한 영역으로 자리잡고 있다[1].

무선 LAN은 전파라는 전송매체를 사용함으로써 매체의 특성상 보안에 대한 취약성을 내포하고 있다. 물리적으로 접근이 어려운 유선과는 달리 무선 구간은 접근이 용이하므로 데이터를 암호화함으로써 기밀성을 유지하고 인증 된 사용자에게만 네트워크 접속을 허용해야한다[2]. IEEE 802.11b에서는 이러한 사용자 인증 및 기밀성을 위하여 SSID(Service Set Identifier), MAC(Media Access Control) 주소, 그리고 WEP(Wired Equivalent Privacy)키를 이용하고 있다[3]. 하지만 IEEE 802.11b 보안 메커니즘에는 이미 많은 취약점들이 알려져 있다[4]. 이러한 취약점들을 보완하고자 고안된 것이 IEEE 802.1x EAP(Extensible Authentication Protocol)이다[5]. 여기서는 네트워크에 접속을 허용하기위해 여러 가지 인증유형들을 제공하고 있으며, 이러한 인증유형들에는 EAP-MD5, EAP-TLS, EAP-TTLS등이 대표적이지만, 이 또한 상호 인증과 실시간 인증에 있어서 문제점을 가지고 있다. 이와 더불어 최근 인터넷 환경에서 제공되는 응용서비스에 암호화 기술을 이용한 보안시스템이 많이 등장하고 있다. 현재 보안 기능을 일관성 있게 제공해 주는 기술로 PKI(public key infrastructure)를 들 수 있다. PKI를 이용한 서비스들은 서로 통신하는 상대방을 인증하거나 또는 향후 거래 사실의 부인을 방지하기 위하여

인증기관(CA : Certification Authority)에서 발급한 인증서를 이용하는데 사용자는 수신한 인증서를 이용하기 전에는 반드시 인증서의 진위를 검증해야 한다. 인증서 소유자가 인증서를 분실하였거나 인증서의 비밀키를 잊어버렸을 경우 등의 이유로 인증서 유효기간 내에 CA에게 인증서 폐지신청을 할 수도 있기 때문에 반드시 인증서를 발급한 CA에게 인증서 폐지신청을 할 수도 있기 때문에 반드시 인증서를 발급한 CA에게 문의하여 인증서의 진위를 검증해야 한다. 그 동안 주로 이용되고 있는 인증서 검증 방법에는 인증서를 발급한 CA로부터 인증서 폐지목록(CRL : Certificate Revocation List)을 다운로드 하여 자신이 직접 검증하는 방법과 인증서 검증을 대신해주는 온라인 인증서 상태 검증 프로토콜(OCSP : Online Certificate Status Protocol) 서버를 이용하는 방법이 있다[6, 7].

이러한 무선 LAN을 이용하려는 클라이언트는 인증서버가 필요하며 인증서버의 인증서를 검증하기 위하여 네트워크로부터 CRL을 전송받거나 OCSP와 같은 인증서 검증서버에 접속해야 하는데 포트기반 접근제어방식을 이용하는 IEEE 802.1x에서는 클라이언트가 인증서버로부터 인증을 받기 전에는 인증서버 외의 네트워크 자원에 접속할 수 없다. 따라서 클라이언트가 인증서버를 실시간으로 인증할 수 없는 문제가 발생한다.

본 논문에서는 IEEE 802.1x기반의 EAP 인증의 문제점인 상호 인증과 실시간 인증의 문제점을 해결하고자 한다.

제안한 프로토콜은 인증서의 유효성 검증을 빠르고 정확히 할 수 있으며, 특정 검증 서버에 부하를 집중시키지 않음으로써 시스템의 안정화를 이룰 수 있는 보안 시스템을 설계하고자 한다.

제2절 연구내용 및 방법

정보통신기술의 발전은 정치, 경제, 사회, 문화 등 다양한 분야에서의 혁신을 가져왔다. 특히 인터넷을 통한 사이버 서비스는 사회 전반의 모든 프로세스를 대체할 만큼 다양하고 매력적이어서 사회 참여 인구의 대부분을 사이버 세계의 구성원으로 만들었다.

가공되지 않은 데이터를 그대로 사용했던 초기의 인터넷과는 달리, 현재의 인터넷은 가공된 정보를 제공하며, 전자상거래, 전자정부, 사이버 커뮤니티, 문화 콘텐츠 등 개인의 사회에서 요구하는 대부분을 서비스 하고 있다. 또한 이러한 정보들이 재화적인 가치를 가지고 있다고 점차적으로 사람들에게 인식되고 있으며, 유용한 정보들에 대한 대가를 유·무형적으로 지불해야 한다는 사고가 보편화 되고 있다.

현재 전자상거래에서 사용되는 전자지불수단은 크게 접속형 결제방식과 가치저장형 결제수단으로 나눌 수 있다. 접속형 결제수단은 온라인 뱅킹형, 신용카드형, 전자수표형 등이 있으며, 가치저장형 결제수단은 IC 카드형, 네트워크형 등이 있다. 또 지불 금액 정도에 따라서는 고액지불시스템과 소액지불시스템으로 분류되는데, 고액지불시스템은 높은 보안성과 익명성이 요구되어 보안을 위한 비용이 많이 필요하게 되며 대부분 지불브로커시스템에 포함된다. 현재 네트워크를 이용한 전자화폐시스템의 지불은 비용이 적게드는 소액지불에만 사용되고 있는 실정이다. 따라서, 인터넷을 통해 물품을 구입하는데 익숙하지 않은 구매자들에게 신뢰성과 익명성을 보장하여 전자화폐시스템을 고액지불시스템에서도 사용할 수 있도록 하여야 한다.

본 논문에서는 기존에 제시되었던 소액 및 고액 전자지불 프로토콜이 만족해야 할 요구사항과 위협요소에 대해서 알아보고, 전자적으로 이동되는 전자화폐에 대해 자금의 흐름을 현재의 당좌 수표의 거래와 같은 형태를 갖도록 하였다. 또 사용자

의 익명성과 신뢰성있는 네트워크형 전자지불 프로토콜을 제안하고 구현하였다. 제안된 프로토콜은 NetBill 시스템의 문제점인 익명성이 보장되지 않는 부분을 보완하였으며, 거래내역 DB에서는 접속 ID를 사용하여 잔액 및 사용내역을 제공받을 수 있도록 하였다. 각각의 구매단계에서 SMS를 통한 인증 및 제공된 디지털 콘텐츠에 대해 인증번호를 부여함으로써 무단 복제 및 배포를 방지하고 최대한 안전성이 확보되도록 하였다.

전자지불시스템의 운영방식은 보안성이 뛰어난 PGP(Pretty Good Privacy)에 기초하였으며, 인증 및 보안에 관한 기술은 공개키 기반구조를 이용하여 설계하였다. 제안한 프로토콜은 네트워크형 지불시스템에서 야기되는 각종 위협 요소와 요구사항에 대해 최대한 안전성이 확보되고 효율성과 신뢰성이 확보될 수 있는 프로토콜이 되도록 구현하였다.

본 논문의 구성은 다음과 같다. 2장에서는 전자지불 시스템의 현황 및 기반 기술에 대하여 설명하고, 3장에서는 전자지불 시스템의 현황 및 문제점 등 기술 요소에 대하여 설명한다. 그 후, 4장에서는 디지털 콘텐츠 거래를 위한 전자지불 프로토콜을 설계 및 구현하고, 5장에서는 제안된 전자지불 시스템에 대하여 다른 시스템과 비교 및 성능 분석을 한다. 마지막으로 6장은 결론으로서 본 논문의 전체 결과를 정리, 요약한다

제2장 전자지불 시스템 현황 및 기반 기술

제1절 전자상거래 개요

현재 전자상거래에서는 인터넷 서비스에 대한 대가를 지불하는 방법에 있어서 과거부터 현재까지 사용했던 전통적인 결제서비스를 전자적 통신 수단을 통해 이용할 수 있게 해주는 방법이 주로 사용되고 있다.

최근 인터넷을 통해 대가를 요구하는 유료 콘텐츠가 풍부하게 제공되기 시작하면서, 소액지불분야에 한해서는 전자화폐가 주요 지불 방법으로 자리잡기 시작했다. 특히, 기존의 금융시스템 영역에서 안정적으로 성장했던 IC 카드형 전자 지불시스템과는 달리 내트워크형 전자 지불시스템은 인터넷 기업들의 콘텐츠 유료화 정책과 맞물려 최근에 다양한 형태로 많은 영역에서 그 위치를 점하기 시작했다.

인터넷상에서의 전자상거래는 모든 인터넷 사용자가 고객이 될 수 있기 때문에 지역적인 제한이나 시간적인 제한이 없는 전 세계인을 대상으로 할 수 있다는 점에서 현재도 많은 발전과 이용이 있으며, 향후 발전 방향과 거래량 또한 폭발적으로 성장할 수 있는 거래 형태의 경제활동이 될 전망이다.

전자적 형태의 상거래는 1960대부터 전용 네트워크에 의한 전자 데이터 교환(EDI) 또는 은행간 전자송금(EFT)의 형태로 일반 사용자가 아닌 대기업 및 정부위주로 행하여져 왔다. 하지만 인터넷이라는 개방형 네트워크의 발달로 현대 사회에서는 대기업뿐만이 아닌 중소기업과 일반 소비자까지도 포함하는 광범위한 정보사회의 거래 수단이 되었다. 이처럼 전자상거래가 발달하게 된 가장 큰 원인은 인터넷이라는 거대한 네트워크의 발달에 있다고 볼 수 있다. 인터넷의 발달은 많은 기업의 비즈니스 형태를 변화시키고 있으며 향후 일반적인 거래 형태로 발전될 전망이다. 인터넷 등과 같은 통신망을 이용한 전자상거래가 활성화되기 위해서는 여러 가지 요구사항이 뒤따르게 된다. 안정성이 뛰어난 네트워크의 확보와 자료가 모두 디지털로 처리되기 때문에 익명성을 비롯한 개인 인증 등 기존에는 필요하지 않던

법적, 제도적 문제도 필요성을 인식해야 된다. 전자상거래의 커다란 장점은 매장이 필요하지 않으므로 해서 임대료 및 관리비 등의 비용 절감 효과와 시간 제약이 없으며, 거래 대상자도 인터넷이 가능한 전 세계의 모든 사용자가 될 수 있다. 이러한 전자상거래의 신뢰성을 유지하기 위해서는 기술적인 면과 국가 정책적인 제도 개선이 필요하다고 할 수 있다.

제2절 전자상거래 보안

인터넷 상에서 전자상거래가 부각됨에 따라 인터넷 사업의 필수 인프라인 정보보호에 대한 인식과 요구가 절실해지고 있는 실정이다. 현재 전자상거래를 하는데 있어서 가장 큰 장애요인은 정보보호에 대한 불신과 개인정보 유출에 의한 개인 프라이버시 침해 문제이며, 전자상거래 사이트에 개인정보보장 정책의 공표가 온라인 쇼핑몰 재방문 결정에 중요한 요인이 되는 것으로 나타났다[4].

이처럼 불안전한 환경에서 안전한 전자상거래를 하기 위해서는 안전한 통신망의 확보와 중간에 가로채거나 조작되지 않는다는 보장을 제공하기 위한 기술, 정책, 인프라의 제공이 필요하다.

보안상 위협요소와 취약성은 다음과 같다.

▶ 브라우저 소프트웨어의 취약성 : 현재 브라우저는 OS를 포함하여 보안상 많은 취약점들을 지니고 있다. 따라서 판매자나 기타 적법하지 않은 통로를 통하여 구매자의 웹브라우저를 공격함으로써 구매자의 컴퓨터에 부당하게 접속하여 내에 수록된 중요한 정보를 이용할 수 있는 문제점이 발생한다.

▶ 프라이버시 침해 : 구매자가 물품 구입을 목적으로 해당 네트워크에 제공한

개인 정보가 본인의 승인 없이 부당한 용도나 목적으로 사용되어 개인정보의 유출로 인한 피해가 발생할 수 있다.

▶ 액티브 콘텐츠에 대한 위험 : 사용자들이 인터넷을 통한 거래를 위해서 네트워크에 제공한 개인 정보들이 인터넷을 통해 전달되는 동안 중요한 개인신상 정보가 부당한 사용을 위해 자료를 수집하는 제3자에게 노출될 수 있다.

▶ 웹 서버 취약성 : 웹서버 관리 업체가 중립성을 지키지 못하거나 보안이 취약하여 경쟁업체의 의도적인 조작으로 인해 네트워크 사용상에 문제를 야기함으로써 서비스 불능 상태에 놓이거나 로봇 에이전트를 이용해 재고량이나 가격정보가 유출될 수 있다.

▶ 데이터베이스 위협 : 개인신상 정보 중 은행정보 등 중요한 데이터를 보관하고 있는 데이터베이스는 범죄자의 공격 대상이 됨으로써 자료의 유출로 인한 중요 정보의 보안 및 신뢰성을 잃을 수 있다.

▶ 거래부인 : 구매자는 자신이 주문한 제품을 제 때에 수령하지 못하거나 판매자의 물건이 잘못 배달될 수 있다. 이러한 문제점을 악용하는 구매자들로부터 판매자는 자신이 납품한 물건에 대해 구매자가 인수 사실을 부인함으로써 대금을 받지 못하는 문제가 발생할 수 있다.

상기와 같은 문제들은 기존의 오프라인 거래에서도 존재해 왔다. 하지만 인터넷을 통한 거래에서는 이 위험성이 확대된다. 익명성을 기반으로 쉽게 타인을 공격할 수 있기 때문이다.

안전한 전자상거래를 하기 위해서는 앞서 기술한 위협요소와 취약성을 해결하고 다음과 같은 요구사항이 충족되어야 한다.

▶ 인증 : 판매자들은 고객들의 신분이 맞는지 적어도 구매하기 적합한지를 인증해야 한다. 또한 시스템에 대한 접근 권한을 적절하게 제어할 수 있도록 사용자 인증이 필요하다.

▶ 상호프라이버시 : 개인정보가 그 목적지에 도달한 이후에 개인의 것으로 남아 있다고 확신할 수 있도록 프라이버시 침해에 대한 해결이 필요하다.

▶ 무결성 : 지불 거래와 관련된 약정들을 상대가 모르게 수정하지 않는다고 확신할 수 있어야 한다.

▶ 기밀성 : 네트워크를 통해 전송되는 메세지를 송신자 및 적법한 수신자를 제외한 제3자는 볼 수 없도록 하는 방법이 필요하다.

▶ 거래부인봉쇄 : 고객과 판매자 양측은 합의한 어떤 것도 부인하지 못한다는 확신을 가져야 한다.

제3절 전자화폐

1. 전자화폐 개념

디지털 시대에 가장 큰 경제 활동의 변화는 기존의 실물시장이 가상공간상으로 변화되고 있다. 이러한 환경에서 가장 중요하게 거론되는 것이 지불 방법에 관한 문제이고 기존의 지불 방법으로는 한계가 발생하게 된다. 따라서 인터넷 환경에 적합한 새로운 지불방법이 요구되고 있으며 그 해결책으로서 전자화폐가 등장하게 되었다. 이 전자화폐는 실물 화폐가 가지고 있는 익명성, 독립성, 양도성, 재사용방

지, 오프라인 등의 특성을 지니고 있어 전자상거래에서 가장 중요한 지불 수단으로 등장하게 되었다[2].

전자화폐란 실물화폐의 신용성에 기반을 두고, 기본 화폐가 지니고 있는 불편함을 해소시키기 위해 일정한 화폐 가치를 IC 카드나 PC 등에 디지털 가치로 저장했다가 온라인이나 오프라인 형태로 상품을 구매하거나 비용을 지불함으로써 원격지 이송에 따른 통신 기능, 휴대 및 보관의 편익 기능, 위조방지 기능 등을 추가한 새로운 전자적 결제 방법이라고 정의할 수 있으며, 화폐로서의 기능상 전자동전(Electronic Coin)방식과 전자수표(Electronic Check)방식으로 분류하는데, 액면가치를 보증하기 위해 은행이 서명한 디지털 신호로 표현된 가치정보이다[5][6].

전자화폐 시스템은 독립적인 신용구조를 가지고 있어서 물품 구입시 은행이나 카드 발행사로부터 거래 승인이 필요 없는 시스템이다. 실생활에서 사용하고 있는 기존의 화폐를 인터넷상에서 사용이 가능하도록 하는 시스템이 전자화폐의 궁극적인 목표 시스템이다.

전자화폐는 디지털정보 그 자체가 화폐가치를 갖기 위하여 전자화폐의 부정한 이용을 방지하는 것이 중요한 과제로 떠오르고 있다. 디지털정보는 쉽게 복사가 가능하고 또 아무런 흔적도 없이 위조, 변조 및 중복 사용이 가능한 문제점이 대두되고 있으며, 실물 화폐의 경우 정보화에 대응할 수 없다는 점이 현대 사회에서의 문제점이다. 즉 종이(금속)라는 물리 매체에 의해 실현되기 때문에 실제 사용시 그 물리적 이동을 전제로 하고 정보로써 취급할 수 없다는 점이다. 여기서 인터넷 등의 네트워크상에서 지불이 요구되는 정보화 시대의 지불 수단으로써 전자화폐의 필요성이 대두된다.

2. 전자화폐의 장점과 문제점

전자화폐는 현금을 사용하는 지불방법을 정보화 사회에 적합하게 하기 위해 개발한 시스템이다. 우선 지폐나 동전을 사용할 경우와 비교했을 때 전자화폐의 장점은 표 1과 같다.

표 1. 전자화폐의 장단점

결제수단 / 구 분	현 금	신용카드	신용카드를 사용한 전자결제	전자화폐
전자적 처리	X	△	○	○
도난/분실시 처리	X	X	○	○
프라이버시	○	X	X	○
결제비용	△	X	△	○
개 방 성	○	X	X	○
양 도 성	○	X	△	○

전자 화폐는 거의 완전한 익명성을 확보할 수 있기 때문에 범죄에 이용될 우려가 다분하다. 즉 돈 세탁이나 유괴범이 몸값을 받아내는 수단 등으로 악용될 가능성이 있다. 전자화폐를 도입하기 위한 비용을 누가 부담할 것인가라는 문제도 발생한다. 은행, 상점, 이용자 등 각각에게 전자화폐를 도입하는 동기를 어떻게 부여할까라는 문제도 검토해야만 할 것이다.

3. 전자화폐의 분류

전자화폐를 저장하는 경우에는 디지털 숫자인 금액을 그 외 필요정보와 함께 암호화 기술로 암호화하여 보호하는 것이 기본이다. 이것에 의해 전자화폐 발행자의

정당성 확인, 위조의 방지, 정보의 유출방지, 전자화폐 거래의 부인방지를 실현하고 있다. IC카드형은 IC카드 내의 소프트웨어에서, 네트워크형은 노트북 등 컴퓨터 내의 소프트웨어에서 실현되고 있다.

표 2. 전자화폐의 분류

전자화폐	기본개념	유 통 경 로	사용 목적	실현수단	프라이버시 보호	추적성	재충전성
Mondex	현금형	개방형	복수	IC 카드형	익명성	無	가능
E-Cash	현금형	개방형	복수	소프트웨어	비익명성	無	가능
NTT 전자화폐	현금형	개방형	복수	IC 카드형	익명성	有	가능
VISA 캐쉬	선불형	폐쇄형	복수	IC 카드형	비익명성	有	개발중
사이버코인	선불형	폐쇄형	복수	소프트웨어	비익명성	有	가능
게르트칼트	선불형	폐쇄형	복수	IC 카드형	비익명성	有	가능 불가능
캐쉬카드	선불형	폐쇄형	복수	IC 카드형	비익명성	有	가능
프로톤	선불형	폐쇄형	복수	IC 카드형	비익명성	有	가능

4. 전자화폐의 안전성

현재에도 신용카드의 부정사용은 큰 문제가 되고 있다. 본인의 서명과 전화로의 확인을 생략하게 되면 더욱 많은 문제가 발생할 것은 뻔하다. 전자화폐 지불에서는 신뢰할 수 있는 방법으로 각 개인의 신원을 온라인으로 증명하는 방법이 요구된다. 또한 종이와 펜을 사용하지 않고 서명하는 방법, 신분증을 제시하지 않고 본인이라는 것을 증명시키는 방법, 물리적인 것을 일체 보내지 않고 현금을 보내는 방법 등도 요구된다. 이들 방법은 전부 수학적인 암호 알고리즘을 사용해 실현할 수 있다.

5. 전자화폐의 요구조건

▶ 디지털 정보의 독립성(Independence) : 완전하게 디지털로만 실현되는 것을 의미하며, 컴퓨터를 매개체로 인터넷과 같은 네트워크 상에서 사용할 수 있기 위해서 전자화폐는 다른 물리적인 형태에 의존하여서는 안 되며 디지털 데이터 자체로서 완벽한 화폐 가치를 가져야 한다. 화폐의 정당성을 인증 받기 위한 은행의 서명, 복사 방지를 위한 기술 등과 같은 모든 조건을 디지털 데이터의 조작만으로 만족시켜야 한다. 이때에만 비로소 네트워크상으로 전송될 수 있다.

▶ 재사용 불가능성(보안성, Security) : 복사, 위조 등으로 인한 부정사용을 할 수 없도록 하는 것으로 화폐 가치를 포함하고 있는 전자화폐는 디지털 데이터 형태로 구성되어 있기 때문에 가치 정보에 대한 조작이 가능하면 실물 화폐보다 손쉽게 대량으로 복사할 수 있다. 따라서 화폐 발행자들은 부정한 조작이 불가능한 위·변조 방지형 마이크로칩으로 안전장치를 내장하고 고성능 암호처리 프로토콜 설치 등 정교한 위·변조 방지장치를 개발하여야 할 것이다.

▶ 익명성(Privacy, Untraceability : 프라이버시 보호, 추적불가능성) : 이용자의 구매정보 및 신상정보에 관한 프라이버시가 상점과 은행이 결탁해도 노출되지 않아야 하는 조건이다. 현금을 사용한 경우 물건을 사고나면 누가 무슨 물건을 얼마만큼 언제 구매 했는지 전혀 정보가 남지 않지만 전자화폐는 발행에 필요한 개인 식별 번호를 비롯하여 많은 정보가 남기 때문에 전자화폐를 추적하면 개인의 프라이버시에 해당하는 정보가 유출될 수 있다. 이러한 이유로 인하여 전자화폐 사용을 꺼리고 있으며, 전자상거래 확대에 커다란 장애물이 되고 있는 실정이다. 따라서 사용자의 구매 정보에 대해서는 어느 누구에 의해서도 추적이 불가능해야 한다.

▶ 오프라인성(offline) : 사용자가 상점에 지불을 수행할 경우 사용자와 상점 사이의 거래는 오프라인 방식으로 처리되어야 한다. 지불되는 전자화폐 자체만으로도 유효성이 검증되어야 한다. 처리할 때마다 은행에 화폐의 정당성을 검증 받아야하는 부분이 없어지므로 그만큼 처리할 때마다 비용의 감소 효과도 가져올 수 있다. 따라서 대금의 지불 형태는 오프라인 상에서 대금 지불이 이루어져야 한다.

▶ 양도 가능성((Transferability) : 전자화폐를 한번만 사용하는 것이 아니라 상점이나 개인이 제3자로부터 받은 화폐를 은행을 통하지 않고 바로 다른 곳에 사용할 수 있어야 한다. 처리비용 및 전자화폐 데이터베이스의 유지비용 등을 절감할 수 있다.

▶ 분할 이용 가능성(Divisibililty) : 액면이 가지고 있는 가치만큼 분할하여 사용이 가능해야 한다. 분할된 화폐가치도 분할되기 전과 똑같은 효력을 가지

면서 아주 작은 단위의 가치라도 지불이 가능해야 된다.

▶ 부정 사용자의 익명성 취소(Anonymity Revocation of illegal user) : 전자화폐는 데이터가 디지털로 저장되기 때문에 화폐의 양에 관계없이 작은 자료로 많은 화폐 가치를 가질 수 있다. 따라서 세금 및 거래 관계에 관한 기록을 회피하거나 돈 세탁 등의 부정한 방법에 악용될 가능성이 많다. 자금 이체시 은행을 경유하지 않는 경우의 불법적인 사용에 관한 제도 및 법률 정비가 필요하다.

▶ 기타 사용자 위주의 편리성을 위한 요구 조건 : 간편성, 낮은 관리비용, 원거리 이전 가능 등

6. 전자화폐 프로토콜

가. 사용자 개인정보의 불추적성

사용자가 은행으로부터 서명을 받으려는 문서를 비밀로 한 채 은행의 서명을 받는 방법으로 고객이 만들어 보낸 은닉된 데이터에 은행이 금액 정보만 확인하고 고객의 신상 정보에 관한 내용은 알지 못한 채 서명을 하는 방식으로, RSA 방식을 기반으로 하는 은닉서명, 영지식 증명을 근거로 한 은닉서명 방법, 이산 대수 방식에 근거한 은닉서명 방법, 오프라인형 전자화폐시스템 등이 나와 있으며, 이러한 방법은 사용자의 신원 정보와 은행의 서명 정보는 연결이 되지 않아서 불추적성 기능을 만족시켜 준다[5][8][9].

이러한 불추적성이 제공되는 대표적인 방식인 D.Chaum의 은닉서명 방식을 이용한 전자화폐 방식에 대한 흐름을 정리해 보면 다음과 같다.

① 사용자는 화폐 생성 자료를 만든 후 사용자만 알고 있는 랜덤 값을 곱하여 이를 은닉시킨 후 은행에 전송한다.

화폐 생성 데이터 : 데이터 M, 랜덤 값 r, 은행의 공개키 e

은닉된 화폐 생성 데이터 : $r^e M \bmod n$

② 은행은 은닉된 화폐 생성 데이터에 서명한 후 사용자에게 전송한다.

은행의 서명이 된 화폐 생성 데이터 : $rM^d \bmod n$

③ 사용자는 은닉 서명 r을 제거한다.

$rM^d / r = M^d \bmod n$, 전자화폐 : (M, M^d)

④ 사용자는 전자화폐를 상점에 전송한다.

⑤ 상점은 은행의 서명을 확인한다.

⑥ 상점은 은행의 서명이 맞으면 사용자에게 상품을 전송한다.

⑦ 일정한 금액이 모아지면 상점은 은행에 지불 사본을 전송한다.

⑧ 은행은 상점으로부터 모아진 지불 사본을 은행의 DB를 검사하여 이중 사용 여부를 검사하여 확인되면 상점의 계좌에 해당 금액을 이체한다.

나. 전자 화폐의 분할이용 가능성

현재의 지폐나 동전은 그 가치를 쪼개어 사용할 수가 없다. 필요에 따라 큰 화폐를 제시하고 거스름돈을 받아한다. 네트워크상에서 이러한 거스름돈을 주고받는다면 전자화폐의 거래에 커다란 문제점이 발생할 것이다. 이러한 문제를 해결하기 위해 전자화폐의 분할사용을 제안한 가장 대표적인 논문은 1991년에 T.Okamoto와 K.Ohta에 의해 제시되었으며, 대부분의 전자화폐 분할 사용은 계층적 구조 테이블을 사용하고 있는데 다음과 같은 규칙을 따른다[10][11].

① 어떤 노드 N에 있어서 해당 금액은 자식 노드들의 합과 같다.

② 어떤 한 노드가 사용되면, 모든 자식 노드와 부모 노드는 사용할 수 없다.

③ 어떤 노드도 한번 이상 사용될 수 없다.

제3장 전자 지불 시스템 분석

제1절 지불 시스템 동향

1. 전자 현금형 시스템

전자 현금 시스템은 실제 사용되고 있는 화폐 형식을 그대로 모방하여 실제 사용 방법과 특성을 같게 만든 것으로 선불 카드 또는 직불 카드를 응용하거나 순수한 디지털 현금을 응용하는 시스템이다. 이 방식의 특징은 주로 소액 거래시 사용되며, 익명성, 확정성, 휴대 가능성, 양방향성을 가진다.

2. 전자 수표형 시스템

전자 수표는 현실 세계에서 사용하고 있는 종이로 된 수표를 그대로 인터넷에서 구현한 것이며, 사용자는 은행에 신용 계좌를 갖고 있는 사용자로 제한된다. 인증 과정은 여러 가지 보안 기법이 사용되고, 이 때문에 거래 비용이 많이 들 수밖에 없다. 그러나 수표는 상당히 큰 액수의 거래, 기업간의 상거래 지불 수단으로 적합하다.

이 시스템의 대표적인 것으로 캘리포니아 대학에서 넷캐시와 함께 개발 중에 있는 넷체크가 있으며, 카네기 멜론 대학에서 개발한 NetBill이 있는데, NetBill은 상당히 복잡한 형태로 거래가 이루어지고 있으며, 그 이유는 전자 수표의 부도를 막기 위한 것이다.

3. 신용카드형 시스템

이미 널리 사용되고 있는 신용카드를 그대로 인터넷 상거래에 적용하려는 것으로 다음과 같은 이점과 단점이 있다.

① 장점

- 신용카드사의 신분 보증으로 인터넷상에서 쇼핑이 가능하다.
- 신용카드사는 이미 전 세계적으로 광범위하게 사용되고 있다.
- 법적, 제도적인 문제를 변경시키지 않아도 된다.

② 단점

- 소액 결제에 부적당하다.
- 대금 결제에서 안전성을 보장할 수 없으므로 인하여 안전성 확보를 위한 노력이 절실하다.
- 신용이 열악한 사람은 신용카드를 발급 받지 못한다.

4. 전자 자금 이체형 시스템

인터넷상의 가상 은행은 최근 웹을 기반으로 생겨나고 있다. 가상 은행이란 물리적인 은행을 운영하지 않고도 모든 것을 웹상에서 사용자와 연결함으로써 운영되는 은행을 말한다. 전자 자금 이체는 현재도 홈뱅킹이나 ATM으로 가능하나, 인터넷상의 웹기반에서 가상 은행의 전자 자금 이체가 시간과 공간의 제약이 없고 수수료가 적다는 점에서 유리하다.

5. 시스템의 전제 조건

a. 암호화 방식의 이용

암호화 방식을 이용한 결제 시스템은 암호화 알고리즘이 파괴되지 않을 때에만

그 안전성이 유지된다. 안전성을 유지하기 위해서는 키를 수시로 변경하거나, 거래 당사자간에 신뢰성을 제공하는 등의 다양한 다단계 보안 능력이 제공되어야 한다. 보안 시스템이 너무 복잡하거나 엄격하면 사용자에게 불편을 초래하고, 그에 따른 비용과 소액 거래의 비활성화를 가져올 수 있다.

b. 개인 정보와 익명성

소비자가 프라이버시와 익명성이 보장되지 않는 결제 시스템으로 구매하는 경우, 소비자의 개인 정보가 중앙의 데이터베이스에 전자적으로 기록될 수 있으며, 이러한 개인 정보는 특정한 기술을 이용하여 분석될 수 있고, 그 정보는 기업의 고객 선호도, 생활 양식 등을 파악하기 위한 자료들로 판매되는 경우 소비자의 프라이버시를 침해하게 된다. 따라서 적절한 감시·추적장치를 가지면서 개인의 프라이버시와 익명성을 보장하는 결제 시스템이 가장 이상적이다[31][32][33].

c. 소액 지불과 처리 비용

인터넷 결제 시스템의 소액 거래 지원 여부는 결제 시스템 평가의 대단히 중요한 요소라 할 수 있다. 웹 정보, 논문, 사진, 뉴스, 그림 등의 거래는 소액에서부터 고액에 이르기까지 그 액수가 다양하다. 소액 거래를 지원하기 위해서는 결제 처리 비용이 낮아야만 가능하다.

제2절 지불 시스템 비교 분석

1. 시스템 비교 분석

각종 시스템의 특징 및 기술적 측면에서 비교 분석하면 표 3, 4와 같다[2][34].

표 3. 각 시스템의 유형 및 기능

유 형			명 칭	기 능
전 자 현금형	네트워크형	즉 시 지불형	E-Cash	네트워크상에서 가상의 코인을 생성하여 이를 결제에 이용
		후불형	Net Bill	네트워크상의 소비자와 판매자의 계좌를 설정하여 POS처럼 이해함
	카드형	즉 시 지불형	Mondex	IC 카드상에서 현금 가치를 이전하는 잔고 보충 가능한 선불형 지갑 카드, 제3자에게 가치 이전 가능
		선불형	Proton	선불형이나 제3자에게 가치 이전을 할 수 없음
전자수표형		후불형	FSTC	카드에 내장된 전자 수표장과 전자 서명 방식을 이용한 네트워크상의 수표
신 용 카드형	네트워크형	후불형	Cyber Cash	PC에 내장된 전용 소프트웨어가 미리 카드 번호를 기억, 암호화된 카드 정보는 Cyber Cash의 중개로 네트워크상에서 결제에 이용
	카드형	후불형	First Virtual	일종의 회원 등록과 같이 카드 정보를 사전 등록, 전용 회원 번호로 네트워크 상에서 결제
전자 자금 이 체 형		후불형	SFNB	Quick Pay 서비스를 제공, 지불 대상과 금액만 입력하면 자금 이체가 일어남

표 4. 각 시스템의 추진모체

유 형	명 칭	추 진 모 체
전자 현금형	E-Cash	UCLA Information Science Institute
	Net Bill	카네기 대학 Information Networking Institute
	Mondex	몬텍스 UK(내셔널 웨스트민스터 은행, 마스터 인터네셔널
	Proton	뱅크시스(벨기에), 인터페이(네델란드), 미텔(브라질)
전자수표형	FSTC	City Bank, Chemical Bank, Bank of America
신용 카드형	Cyber Cash	사이버 캐시
	First Virtual	퍼스트 비추얼 홀딩스
전자 자금 이체형	SFNB	Security First Network Bank, FSB

2. NetBill 시스템

a. NetBill 개요

NetBill은 콘텐츠만을 거래하기 위한 지불브로커 방식의 소액 지불 시스템이다. NetBill은 구매자(Customer), 판매자 (Merchant), NetBill 서버의 세 구성원으로 구성된다. 가격 협상, 정보 배달, 지불의 세 단계로 거래가 이루어지며, 프로토콜의 절차는 그림 1과 같이 표현된다.

(1) 가격협상 단계

① 가격 요구 단계 : 구매할 상품의 가격을 제시함으로써 판매자와 가격 협상

② 가격 절충 단계 : 판매자와 구매자 사이의 가격 협상이 이루어진다.

(2) 정보 배달 단계

③ 상품 요구 단계 : 가격 협상이 이루진 후 판매자에게 정보 상품을 요구한다.

④ 암호화된 상품 전달 단계 : 구매자에게 암호화된 정보 상품을 전송한다.

(3) 지불 단계

⑤ 주문서 발송 단계 : 구매자는 전자 서명된 물건의 주문서를 판매자에게 보낸다.

⑥ 거래 승인 단계 : 판매자는 전자지불 주문서를 NetBill 서버에 보낸다.

⑦ 영수증 전송 단계 : NetBill 서버는 거래의 결과를 확인하여 영수증을 판매자에게 보낸다.

⑧ 영수증 전송 단계 : 판매자는 영수증과 정보 제품 복호화 키를 구매자에게 전송한다.

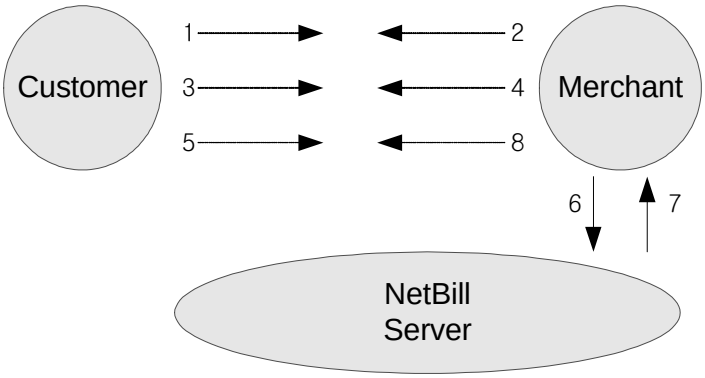

그림 1. NetBill의 거래 프로토콜

b. NetBill 시스템의 장・단점

구매자는 NetBill 서버의 지불 승인을 받은 후 상품을 수령하고, 판매자는 결제가 일어난 후 상품을 전달하기 때문에 구매자와 판매자 모두가 상호 신뢰할 수 있으나, 매 서비스마다 NetBill 서버에 접속하여 확인 절차를 거쳐야 하고, 거래 단계가 복잡함으로 다른 지불 프로토콜에 비해서 전자 서명이 많이 쓰이는 단점이 있다. 또한, 판매자는 구매자의 신원을 파악하고, NetBill에 의한 모든 거래 정보는 서버에 기록되므로 거래를 추적할 수 있기 때문에 구매자와 판매자 모두 익명성이 보장되지 않는다.

3. E-Cash 시스템

a. E-Cash 개요

E-Cash 시스템은 디지캐쉬사에서 개발한 결제 시스템으로 전자동전을 사용하여 실제 지폐와 동일한 전자화폐 기능을 갖는 인터넷 상거래 결제 시스템이다. 공개키 암호화, 전자 서명 등을 사용하여 구현하였으며, 구성원은 은행, 구매자 그리고 판매자로 구성된다.

고객은 등록된 계좌에서 전자동전을 인출하여 자신의 컴퓨터에 저장해 두고 판매자의 웹사이트에 접속하여 제품을 구매한 후 결제 대금으로 전자동전을 지불한다. 판매자는 전자동전에 대하여 은행에 정당한 사용자의 전자동전인지 확인과정을 거친 후에 구매자에게 제품을 인계한다. 이러한 확인 과정을 거치는 이유는 전자동전이 두 번 중복해서 사용되는 경우를 방지하기 위함이다. 이렇게 함으로써 지불인의 익명성은 보장되지만, 수취인의 익명성은 보증되지 않는 단점이 있다. 은행은 입금된 전자동전의 일련번호를 사용하여 수취인의 입금내역을 파악할 수 있다. 따라서 자금세탁 등 불법적인 목적으로 전자동전을 사용하는 경우에 대하여 수취인의 익명성이 보증되지 않기 때문에 사용이 제한되는 특징이 있다.

이러한 전자동전은 자신의 컴퓨터에 계속해서 저장해 둘 수도 있으며, 등록된 계

좌에 입금하여 사용할 수도 있다. 이 시스템을 사용하기 위해서는 E-Cash 소프트웨어가 필요하며, 이 소프트웨어로 전자동전의 인출, 지불, 예금, 수령 등에 대한 정보를 제공받을 수 있다.

b. E-Cash 시스템의 장・단점

E-Cash의 장점은 익명성이 뛰어나기 때문에 안전하다는 것에 있다. 전자동전의 사용은 전자화폐를 사용할 때 블라인드 서명을 이용하기 때문에 추적이 불가능하다. RSA 공개키 암호화 방식을 사용한 안전한 프로토콜의 사용으로 시스템의 도청이나 메세지 무결성에 안전하다는 커다란 장점을 지니고 있다. 하지만 수취인이 은행에 전자동전을 입금하게 되면 은행에서 전자동전의 일련번호를 사용하여 수취인의 사용 내역을 파악할 수 있어서 수취인의 익명은 보장되지 않는 단점이 있으며, E-Cash라는 소프트웨어를 사용하면서 모든 전자동전에 일련번호가 부여되어 계속 발생되는 데이터들의 양이 데이터 베이스의 처리 속도를 저하시켜 관리에 무리를 줄 수 있다.

4. NetCash 시스템

a. NetCash 개요

NetCash 시스템은 1997년 캘리포니아 대학의 정보과학연구소에서 개발되었으며, 은행의 서명을 통하여 발행되는 온라인 전자현금을 사용한다. 구매자, 판매자 그리고 통화서버로 구성되며, 통화서버는 전자화폐를 주조하며, 화폐의 진위를 조사하고 화폐와의 교환을 추적하여 소유자의 익명성을 보호한다. 그리고 중앙의 금융기관으로부터 네트워크상 통제를 받으며 이들로부터 전자화폐를 발급할 수 있는 권한을 승인 받게 된다. 이러한 일련의 과정은 중앙 인증국의 비밀키로 모두 서명된다.

NetCash 시스템은 전자수표처럼 전자화폐들을 위해 통화서버를 교환할 수 있다. 통화서버는 화폐를 누가 발행했는지를 기록하지 않음으로써 익명성을 제공한다.

b. NetCash 시스템의 장・단점

NetCash의 장점은 확장성과 안전성에 있다. 화폐에 통화서버의 이름과 통화서버 네트워크 주소를 기록하여 다중 통화 서버를 사용하기 때문에 확장성을 가지며, 보안은 대칭키 암호화 프로토콜과 비대칭키 암호화 프로토콜을 사용한다.

이 시스템은 많은 세션키를 사용하고, 특히 공개키를 생성하는 대칭형 세션키를 생성하는 것을 포함하여 비교적 많은 시간이 걸리는 단점이 있으며, 은행이 구매자에게 화폐를 인출할 때 화폐의 일련번호를 확인하고 온라인 데이터베이스에 기록하여 익명성을 제공하지 못하는 문제점이 있다.

5. SET(Secure Electronic Transaction) 시스템

a. SET의 개요

SET은 신용카드를 사용할 때의 방법을 기초로 하여, VISA와 MasterCard가 제휴하고, 7개 컴퓨터 및 보안업체가 공동 제안하여 1997년 5월 31일에 버전 1이 발표되어 가장 안전하다는 평가를 받고 있는 신용카드 기반 결제 프로토콜의 규격이다. 가맹점은 신용카드 번호 등의 결제정보를 받아 금융기관에 넘겨주게 되지만 신용카드의 내용은 금융 기관만이 볼 수 있도록 암호화되어 처리된다.

이러한 처리가 가능하도록 SET 프로토콜은 메세지의 암호화, 전자증명서 그리고 디지털 서명 등을 사용하고 있다.

b. SET 지불 시스템의 참여자

① 구매자 : 발생사로부터 허가된 지불카드를 사용하며, 신용카드로 구매 대금을 지불하려는 사람

② 판매자 : 카드 사용자가 안전하게 전자상거래를 할 수 있도록 서비스를 제공하며, 카드로 대금 결제를 받는 상인은 매입사와 관계를 가져야 한다.

③ 발행사 : 카드 소지자의 계정을 개설해 주고 신용카드를 발급해주는 업무를 담당하며 금융기관에서 거래에 대한 지불 보장을 해준다.

④ 매입사 : 상인과 계정을 체결하고 결제된 신용카드에 대하여 신뢰성과 지불을 담당하는 금융기관이다.

⑤ 지불 게이트웨이 : 매입사에 또는 제3자가 운영하는 결제 처리를 위해 사용되는 시스템이다.

⑥ 브랜드 : 신용카드 소지자와 가맹점이 상호 거래할 수 있도록 하고 발행사와 매입사의 역할을 조절한다.

SET은 고객을 Cardholder라는 용어를 사용하는데 이것은 지불의 수단이 신용카드라는 것을 알 수 있다. 대금 지불을 담당하는 곳을 Payment Gateway라고 하며, Cardholder, Merchant, Payment Gateway는 각각의 공개키를 생성하여 인증기관으로부터 인증서를 발급 받아 사용한다.

c. SET 암호 메커니즘

SET은 공개키 암호, 관용키 암호, 서명, 해쉬함수 등을 사용하여 안전성을 보장해 주고 있다. 사용자가 신용카드 정보를 상점에게는 숨기고, 주문 정보는 은행에 숨김으로써 사용자의 프라이버시가 보호되도록 하는 이중 서명이라는 특별한 암호 메커니즘을 사용하고 있다.

이중 서명 처리 과정을 식으로 나타내면 다음과 같다.

(1) 식에 사용된 기호

OI : 주문정보

PI : 지불정보

OI_{MD} : OI를 해쉬한 값

PI_{MD} : PI를 해쉬한 값

Es() : 상점의 공개키로 암호

Eb() : 은행의 공개키로 암호

Su() : 사용자의 개인키로 암호

(2) 사용자 → 상점

Es(OI) || Eb(PI)

OIMD, PIMD

Su(OIMD||PIMD)

(3) 상점 → 은행

Eb(PI)

Su(OIMD||PIMD)

사용자의 주문 정보(OI)는 상점의 공개키로 암호화하여 전송하고, 지불 정보(PI)는 은행의 공개키로 암호화하여 전송함으로써 상점은 지불 정보만을 볼 수 있고, 은행은 주문 정보만을 볼 수 있도록 한다. 해쉬와 서명을 사용하여 전송된 데이터가 정당한 자료인지를 인증할 수 있다.

d. 지불 처리

(1) Cardholder 등록

SET을 사용하려는 사용자가 CA로부터 자신의 신원을 인증 받고 Cardholder를 등록하는 절차를 거쳐야만 Merchant와 정당한 거래를 할 수 있다. 이 절차는 7단계로 이루어지며 처리 순서는 다음과 같다.

① Cardholder는 사용하고자 하는 신용카드를 사용하여 가맹점에 보내기 전에 인증기관에게 인증을 요청한다.

② 인증기관에서 Certificate를 Cardholder에게 전송함으로써 인증 요청을 받아들인다.

③ Cardholder는 CA의 Certificate를 검증하고, 등록양식을 암호화하여 요청한다.

④ CA는 디지털로 서명하고 등록양식을 Cardholder에게 전송한다.

⑤ Cardholder는 자신의 공개키/비밀키 쌍을 생성하여 Certificate 발급 요청을

하며, 등록양식에 전자서명을 추가하여 전송한다.

⑥ CA는 Cardholder의 신원을 확인하고 Certificate를 작성하여 전송한다.

⑦ CA로부터 전송 받은 Certificate를 복호화하여 보관한다.

(2) Merchant 등록

SET을 사용하려면 Cardholder뿐만이 아닌 Merchant도 CA로부터 Certificate를 받아 놓아야 한다. 이 절차는 5단계로 이루어지며 처리 순서는 다음과 같다.

① Merchant는 Cardholder로부터 SET 지불 거래를 처리하기 위해서는 CA에 적당한 등록 폼을 요청한다.

② CA는 Merchant가 요구한 적당한 등록 폼을 키-교환 Certificate와 함께 전송한다.

③ Merchant는 SET 거래를 하기 위해 두 쌍의 공개키/비밀키를 생성한다. 완성된 등록 폼에 전자서명을 추가하고 CA의 공개키로 전송한다.

④ Certificate 요청 내용이 합당하면, Merchant Certificate를 생성하여 전자서명을 추가한 후 Merchant의 공개키로 암호화하여 전송한다.

⑤ CA로부터 전송 받은 Certificate를 복호화하여 보관한다.

(3) 구매 요청

Cardholder가 상품을 주문, 처리하는 단계이다. SET 메세지를 Merchant에게 보내기 위해서는 Merchant의 Key-exchange 공개키뿐만이 아니라 Payment Gateway의 Key-exchange 공개키도 소유하고 있어야 구매 요청을 할 수 있다.

① Cardholder는 상품을 검색, 선택, 주문 후 사용하려는 신용카드 지불 수단을 포함한 메세지를 생성하여 SET 프로토콜을 호출한다.

② Merchant가 요청을 받으면 메세지에 유일한 거래 구별자를 할당한다. 그런

후 Merchant는 Cardholder가 알려 준 지불카드 브랜드와 일치하는 Payment Gateway의 Certificate를 거래 구별자와 함께 Cardholder에게 전송한다.

③ Cardholder는 주문정보(OI)와 지불정보(PI)를 생성하여, OI와 PI의 해쉬함수값을 계산하여 상호서명을 생성한 후 Merchant에 전송한다.

④ Merchant는 상호서명을 확인함으로써 PI의 내용을 확인할 수 없으면서도 내용의 변경여부는 확인할 수 있다.

(4) Merchant의 지불 승인 처리 과정

① 인증요청과 Cardholder의 지불명령은 Payment Gateway로 전송한다.

② Payment Gateway는 Cardholder가 전송한 PI의 내용과 Merchant가 전송한 OI의 내용이 일치하는지 검사한다. 이것은 Cardholder가 생성한 상호서명으로 확인할 수 있다. Payment Gateway는 Merchant가 대금 지불을 요구할 수 있는 Capture Token을 생성하여 전송한다.

③ Merchant는 Capture 요청을 통해 지불을 요청할 때 Capture Token이 사용되며, Merchant는 상품 주문에 있는 서비스를 수행함으로써 Cardholder의 주문처리를 완료한다.

제4장 프로토콜 설계 및 구현

제1절 제안한 프로토콜 설계

콘텐츠만을 취급하는 NetBill 시스템의 경우 고객과 상점 모두 익명성이 보장되지 않는 단점을 가지고 있으며, 고객은 지불승인을 받은 다음 상품을 수령하고, 상점은 결제가 일어난 후 상품을 전달하기 때문에 고객과 상점 모두 상호간에 신뢰할 수는 있지만, 구매 결정에서부터 콘텐츠를 이용할 수 있는 거래 단계가 복잡하다. 매 서비스마다 서버에 접속하여 확인 절차를 거치고, 거래 단계도 복잡함으로 다른 지불 프로토콜에 비해서 전자 서명이 많이 쓰이는 단점도 있다.

E-Cash의 경우도 수취인이 은행계좌에 동전을 입금하게 되면, 은행에서는 동전의 일련번호 등을 기록하여 두 번 이상 사용될 수 없도록 하는 과정에서 수취인의 입금내역을 파악할 수 있어서 수취인의 익명성은 보증되지 않으며, NetCash의 경우도 은행이 구매자에게 화폐를 인출할 때 화폐의 일련번호를 확인하고 온라인 데이터베이스에 기록하여 익명성을 제공하지 못하는 문제점이 있다.

따라서 본 논문에서 제안하는 전자지불 프로토콜의 전체 흐름도는 그림 2와 같으며 디지털 콘텐츠 거래를 위해 개발된 NetBill 시스템, 네트워크형 지불 시스템인 E-Cash 및 NetCash 시스템에서 익명성을 보장하지 못했던 단점을 보완하고 복잡한 지불 과정을 동일 네트워크에서 처리함으로써 SET 보다 지불단계를 간략화하여 암호화 횟수 및 통신횟수를 감소시킴으로서 시스템의 효율성 및 안전성이 확보되도록 한 네트워크형 전자지불 프로토콜을 설계 및 구현하였다.

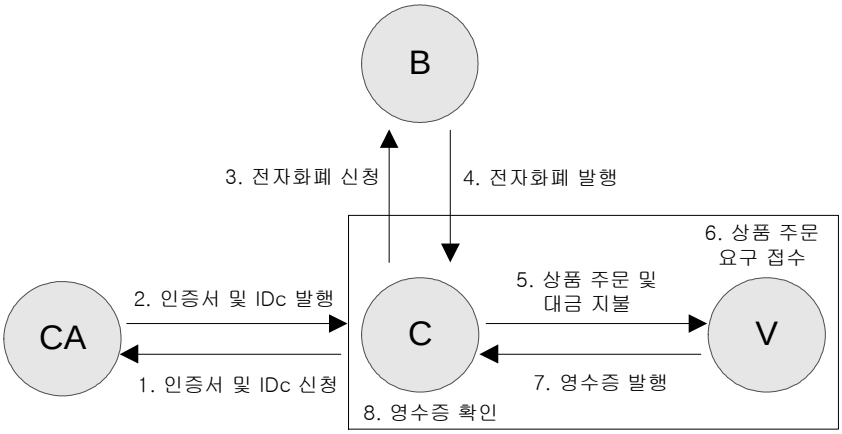

그림 2. 제안된 프로토콜의 전체 흐름도

◈ **제안된 전자지불 프로토콜을 설명하는데 사용되는 기호는 다음과 같다.**

CA : 인증기관

B : 은행

V : 판매자

C : 구매자

M : 문서

ER : 공개키 암호 알고리즘

DR : 공개키 복호 알고리즘

Z : 압축 알고리즘

KU_A : A의 공개키

KR_A : A의 개인키

E : 관용키 암호 알고리즘

D : 관용키 복호 알고리즘

K_S : 세션키

H : Hash 알고리즘

Certificate A : A의 인증서

|| : 연접(Concatenation) 연산

1. 인증서 및 IDc

a. 인증서 및 IDc 신청

구매자의 익명성을 보장하기 위해서 구매자는 인증기관(CA)에 자신의 실명정보를 제공하고, 인증서와 익명성 유지를 위한 가상 ID를 신청한다. 구매자(C)는 자신의 실명정보(Customer), 인증서 암호와 콘텐츠 구매에 사용할 가상 ID(IDc)를 CA의 공개키로 (식 1)과 같이 암호화하여 인증기관에 전송한다.

***C* 구매자 → *CA* 인증기관**

ER_{KUca} { Customer || IDc || Pswd}……(식 1)

[Customer : 구매자, IDc : 가상 ID, Pswd : 패스워드]

b. 인증서 및 IDc 발행

인증기관(CA)은 구매자(C)의 신원을 확인하고 (식 2)의 인증서를 구매자(C)에게 신청 즉시 전송한다.

***CA* 인증기관 → *C* 구매자**

Certificate C……(식 2)

2. 전자화폐 신청 및 발행

a. 전자화폐 신청

구매자는 자신이 사용할 전자화폐의 금액만큼을 은행에 입금하고, 인증서와 IDc를 전송하여 전자화폐 발행을 요구한다. 구매자는 개인의 실명정보가 아닌 인증서와 IDc만을 사용하기 때문에 은행은 구매자의 개인실명 정보를 알 수 없고, 대신

에 IDc만으로 거래를 하게 된다. 구매자는 인증서, IDc 및 전자화폐로 전환하고자 하는 금액(Cash)을 (식 3)과 같이 은행의 공개키와 사용자의 비밀키로 암호화하여 전송한다.

***C* 구매자 → *B* 은행**

ER_{KUb} {ER_{KRc} {Cash || IDc || Certificate C}}……(식 3)

[Cash : 현금 금액]

b. 전자화폐 발행

은행은 인증서와 IDc를 검증하고 입금된 금액에 맞는 전자화폐를 발행한다. 검증된 자료의 전자화폐 금액은 IDc의 정보로 DB에 저장하고, 구매자가 접속할 경우 상품 구매 내역 및 전자화폐 발행내역을 표시하고, 사용 가능한 전자화폐의 금액을 나타낸다. 구매자에게 전자화폐 발행금액(E-Cash)에 은행의 인증서를 첨부하여, 구매자의 공개키와 은행의 비밀키로 암호화하여 전송한다. 이때 은행은 신청한 전자화폐 금액과 은행 잔액을 비교한 후에 발급여부를 결정하고 정당한 발급 신청일 경우 (식 4)와 같은 전자화폐를 발급한다.

***B* 은행 → *C* 구매자**

ER_{KUc} {ER_{KRb} {E-Cash || IDc || Certificate B}}……(식 4)

[E-Cash : 전자화폐]

3. 상품 주문과 대금 지불의 동시처리

상품 주문 및 대금지불 블록도는 그림 3과 같으며, 구매자(C)는 인증기관으로부터 발급 받은 IDc로 DB에 접속하게 되고, 접속과 동시에 IDc의 구매자가 사용 가

능한 전자화폐의 금액이 계산되어 사용 제한을 받는다. 구매자(C)는 판매자(V)의 준비된 상품 중에서 원하는 콘텐츠를 선택한 후 전자화폐금액과 콘텐츠 정보를 전송하고 전송과 동시에 DB에 주문서의 내용을 등록한다. 주문서(M)를 Hash 변환하고 자신의 개인키로 암호화하는 과정을 통하여 주문서에 (식 6)과 같이 자신의 서명을 한다. 하지만 사용자의 실명정보는 알 수 없다.

M={IDc, 콘텐츠 번호, 전자화폐 금액, 전자 화폐발행 번호}……(식 5)

ER_{KRc}{ H(M) }……(식 6)

그리고 차후에 발생될 전송 및 변조여부의 시비를 확인할 수 있도록 Hash 변환된 주문서(H(M))를 보관한다. 그리고 M, ER_{KRc}\{H(M)\}, Certificate C를 함께 압축하고 세션키(Ks)를 사용하여 (식 7)과 같이 관용키 암호알고리즘으로 암호화한다.

EKs { Z{M || ER_{KRc} {H(M)} || Certificate C}}……(식 7)

세션키(Ks)는 (식 8)과 같이 판매자(V)의 공개키(KU_V)로 암호화한 후

ER_{KUv}{ Ks }……(식 8)

(식 9)와 같이 세션키로 암호화한 주문서를 판매자(V)에게 전송한다.

***C* 구매자 → *V* 판매자**

E_{Ks} { Z{M || ER_{KRc}\{H(M)\} || CertificateC }} || ER_{KUv}(Ks)……(식 9)

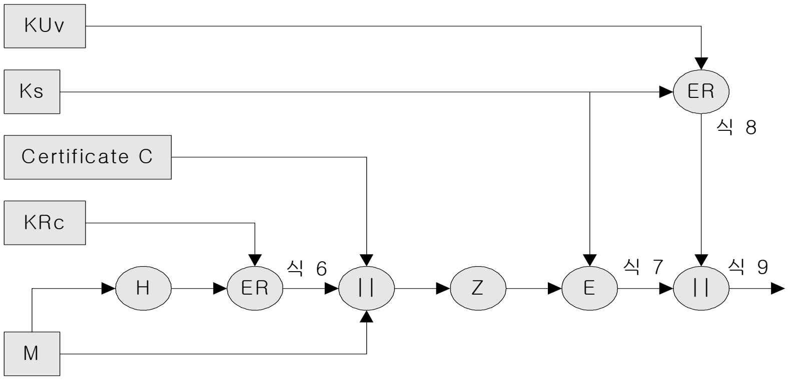

그림 3. 상품 주문과 대금 지불의 동시처리(암호화)

4. 주문 상품의 대금결제 및 접수 처리

구매자(C)가 원하는 콘텐츠의 번호와 대금 지불에 관한 정보를 판매자(V)에 전송하면, 판매자는 주문서의 내용을 DB에서 판매자의 정보로 그 유효성을 검사하여 정당한 주문서인지를 판단한다. 판매자(V)는 독단으로 신규 구매 DB를 생성할 수 없으며, 단지 문서의 내용을 판단하여 인증번호를 부여할지 만을 결정하고 정당한 주문서라면 인증번호를 부여한다. 따라서 판매자(V)가 부정한 거래를 할 수 없도록 하였다.

상품 주문서의 복호화 과정은 그림 4와 같으며, 판매자(V)는 구매자(C)에게서 받은 주문서 중 $ER_{KUv}\{Ks\}$를 자신의 개인키(KRv)를 사용하여 (식 10)과 같은 세션키(Ks)를 얻는다.

$$DR_{KRv}\ \{\ ER_{KUv}(Ks)\ \}\ =\ Ks \cdots\cdots (식\ 10)$$

구한 세션키(Ks)를 사용하여 관용키 암호화된 부분을 복호화 한다.

V 판매자 처리

D_{Ks} {E_{Ks} {Z {M || ER_{KRc}(H(M)} || Certificate C}}}

= Z {M || ER_{KRc}(H(M)} || Certificate C}……(식 11)

사용된 압축을 풀어내고 Certificate C를 통하여 유효한 공개키인지 확인한다. 유효하지 않는 인증서이면 재전송을 요구하고, 유효한 인증서이면 다음 작업을 수행한다. 구매자(C)의 개인키(KRc)로 암호화된 문서를 Certificate C에 포함되어 있는 C의 공개키를 사용하여 (식 12)와 같이 복호화 한다.

DR_{KUc}(ER_{KRc}(H(M)}} = H(M)……(식 12)

압축을 풀어낸 문서에 포함된 M을 Hash 변환하고 (식 12)에서 나온 H(M)과 비교하여 다르면 재전송을 요구하고 같으면 전송도중에 변조되지 않은 것으로 인정한다.

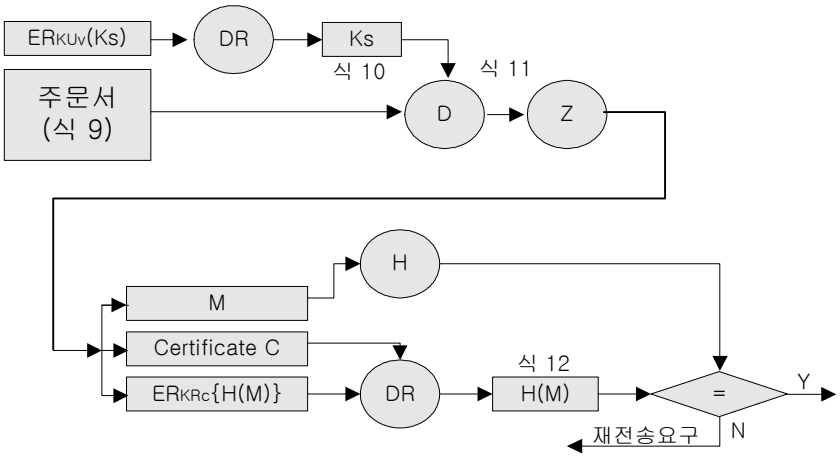

그림 4. 주문 상품의 대금결제 및 접수 처리(복호화)

5. 영수증 발행

판매자는 구매자로부터 받은 정보와 전자화폐 내용에 이상이 없으면 상품을 발송하고 영수증을 발행하며 그 과정은 그림 5와 같다. 영수증에 상품 인증 번호를 첨부하여 전송하게 되면 구매자는 상품 인증 번호를 입력하여 콘텐츠 상품을 다운로드받을 수 있다.

(식5)의 주문서와 상품인증번호(Contents_No)의 해싱된 정보를 (식 13)과 같이 판매자의 개인키(KRv)로 서명을 한다.

$ER_{KRv}\{ H(M \| Contents\_No)\}$ ……(식 13)

서명한 정보와 Certificate V, 수신한 날짜와 시간을 (식 14)와 같이 구매자의 공개키 KUc로 암호화하여 전송한다.

***V* 판매자 → *C* 구매자**

$ER_{KUc}\{ER_{KRv}\{H(M) \| Contents\_No\} \| Certificate\ V \| Date/Time\}$ ……(식 14)

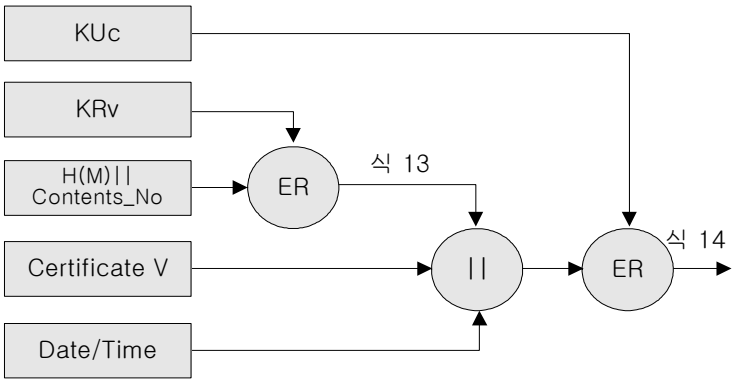

그림 5. 대금 지불에 대한 영수증 발행(암호화)

6. 영수증 확인 및 검증

판매자(V)로부터 발행된 영수증으로 콘텐츠에 대한 대금이 정확하게 지불되었는지를 확인한다. 구매자(C)는 전송된 문서를 (식 15)와 같이 자신의 개인키(KRc)로 복호화하여

C 구매자 처리

DR_{KRc} {ER_{KUc} {ER_{KRv} {H(M) || Contents_No} || Certificate V || Date/Time}}

= ER_{KRv} {H(M) || Contents_No} || Certificate V || Date/Time……(식 15)

포함된 Certificate V가 유효한지를 확인하고, 유효하면 Certificate V에 포함된 판매자(V)의 공개키(KUv)를 이용하여 (식 16)과 같이 판매자(V)의 개인키로 서명된 H(M) 문서를 복호화 한다.

DR_{KUv} {ER_{KRv} {H(M) || Contents_No} = H(M) || Contents_No……(식 16)

여기에서 얻은 Hash 변환된 문서(H(M))와 (식12)과정에서 발생한 H(M)을 비교함으로써 전송도중에 문서가 변조되지 않았음을 그림 6에서 확인할 수 있다.

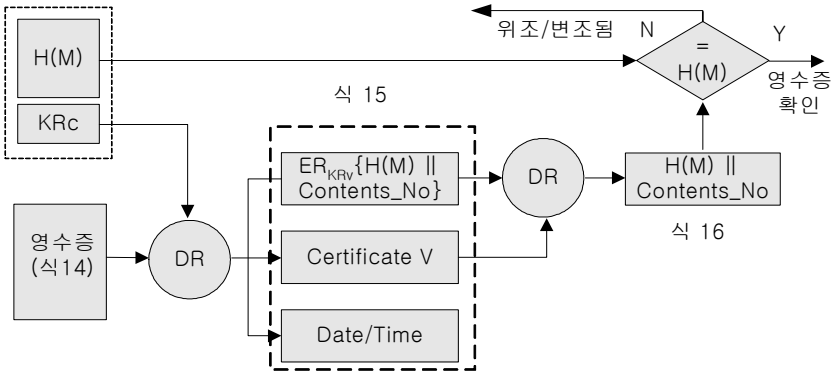

그림 6. 영수증 확인 및 검증(복호화)

제2절 제안한 프로토콜의 구현 및 결과

1. 개발환경

- 프로그램 명칭 : C-Pay
- CPU : Intel Pentium 4 CPU 2.00GHz, RAM : 1GB RAM
- OS : Microsoft Windows XP
- 데이터베이스 : MySQL 3.23.49
- 개발 툴 : DELPHI 6 Enterprise

2. 구현범위

은행과 관련된 부분은 은행과 연계된 이후에 사용될 수 있도록 은행에 전자화폐를 신청하는 부분만 처리하였고, 상품의 구입과 같은 전자화폐 사용 내역에 중점을 두고 구현하였다.

데이터베이스 서버가 존재하고, 일반 사용자들이 사용하는 클라이언트용 소프트웨어를 개발하였으며, 서버에 접속할 경우에는 ID와 비밀번호로 데이터베이스에 접속이 가능하도록 하였다. 접속이 성공적으로 이루어지면 본인이 사용한 거래 내역 및 현재 사용 가능한 잔액이 표시되며, 콘텐츠 구입시 잔액과 비교하여 전자화폐 금액 부족하면 거래가 이루어지지 않도록 하였다.

디지털 상품과 같은 정보 상품은 상품의 전달과 대금 지불이 동일 네트워크에서 이루어질 수 있다는 특성을 고려하여 구현하였으므로, 콘텐츠 구입 및 결제를 위해 자료를 전송하고, 서버에서 복호화가 완료되면 콘텐츠에 대한 결제는 완료되며 다운로드할 수 있도록 하였다.

전자화폐가 뇌물이나 자금세탁 등의 부정 및 불법적인 사용이 이루어진 것으로 짐작되면 관리자의 특별한 권한으로 개인의 전자화폐 거래내역을 열람할 수 있도록 하여 익명성 철회가 가능하도록 하였다.

3. 콘텐츠 구매 처리 화면

a. 사용자 로그인

구매자의 익명성을 보장하기 위해서 구매자는 인증기관(CA)에 자신의 실명정보를 제공하고 공개키, 개인키 및 인증서를 발급 받는다. 인증서는 모든 거래에 사용되며, 인증서가 사용될 때는 실명이 아닌 등록된 ID만을 사용하게 된다. 인증기관으로부터 부여받은 ID와 PW를 사용하여 그림 7과 같이 접근하게 된다.

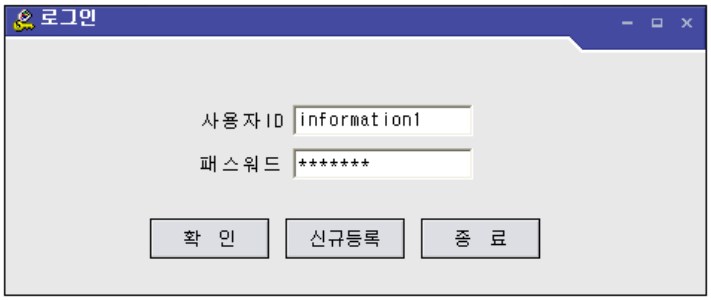

그림 7. 로그인

b. 전자화폐 지불 시스템 초기화면

등록된 ID 및 비밀번호가 정당한 구매자면 사용 가능한 전자화폐의 금액이 그림 8의 화면 하단에 출력된다. 콘텐츠 구매를 할 경우 보유하고 있는 전자화폐의 금액보다 큰 제품은 구매할 수 없도록 하였다.

그림 8. 전자화폐지불시스템의 초기화면

c. 사용자 신규 등록 및 조회

그림 9는 사용자의 신규 등록을 위한 처리화면으로 인증기관에 자신의 신상정보를 제공하면 공개키, 비밀키 및 인증서를 발행한다. 공개키, 비밀키 및 인증서는 사용자의 DB 자료에 함께 저장되어 ID와 비밀번호가 없이는 사용할 수 없도록 하였으며, 구매자 및 판매자 모두를 함께 처리하도록 하였다. 기존의 사용자들은 자신의 정보만을 열람할 수 있도록 하였으며, 개인 신상에 관한 간단한 자료는 수정이 가능하도록 하였다. 자신 이외의 자료는 열람할 수 없도록 하였다.

그림 9. 사용자 신규 등록 및 인증서 발급

d. 사용자 개인키, 공개키 및 인증서 조회

등록된 자신의 개인 신상뿐만이 아닌 개인키, 공개키 및 인증서를 그림 10의 화면에서 “인증서 조회” 탭을 클릭하면 열람할 수 있도록 하였다.

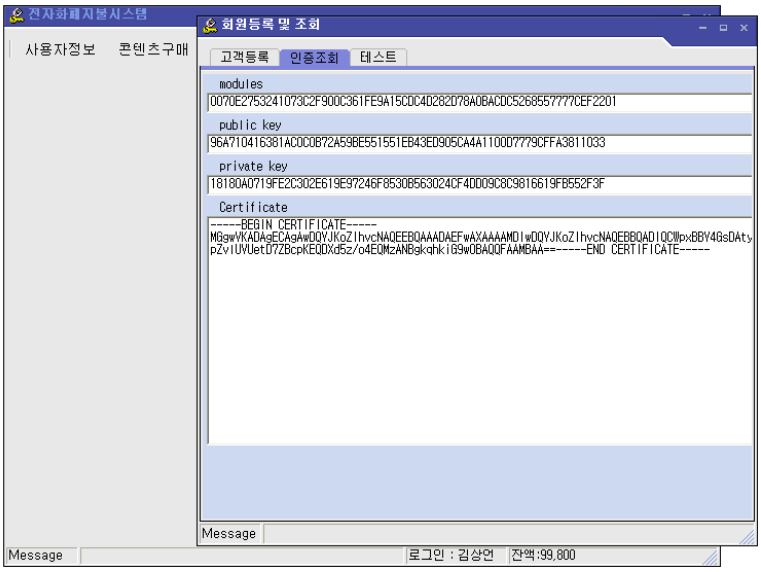

그림 10. 발급된 인증서 조회

e. 상품 구매 및 결제의 동시 처리

그림 11은 콘텐츠 구입을 위한 선택화면으로서 콘텐츠 구매 및 결제가 동시에 처리되는 특성을 이용하여 결제가 완료되면 콘텐츠를 바로 다운로드 할 수 있도록 하였으며, 우측 하단에 사용 가능한 전자 화폐를 표시하여 잔액을 초과하는 콘텐츠는 구매가 이루지지 않도록 하였다. 그림 11은 본인이 그 동안 구입한 내역을 보여준 화면으로서 결제가 완료된 콘텐츠는 언제든지 다시 다운로드 할 수 있도록 하였다.

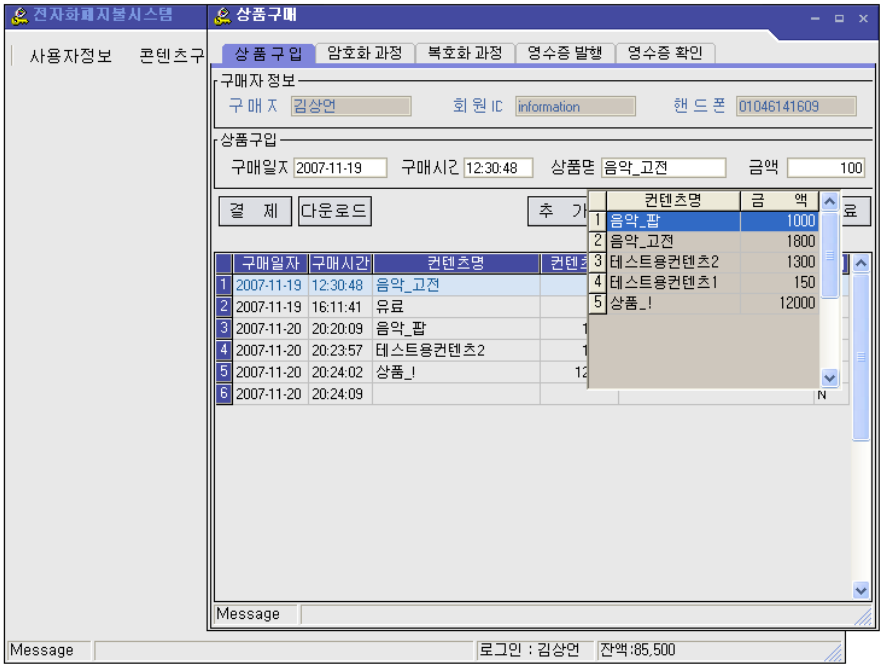

그림 11. 상품 구입을 위한 선택

f. 암호화를 통한 상품 구매 과정

암호화 및 복호화는 처리과정의 정확성을 위하여 단계마다 암호화 및 복호화 과정을 화면에 출력하도록 하였다. 실제 처리 과정에서는 사용자가 볼 수 없도록 한다. 그림 12는 상품 구매와 관련한 암호화 처리과정을 단계적으로 표현한 것이다.

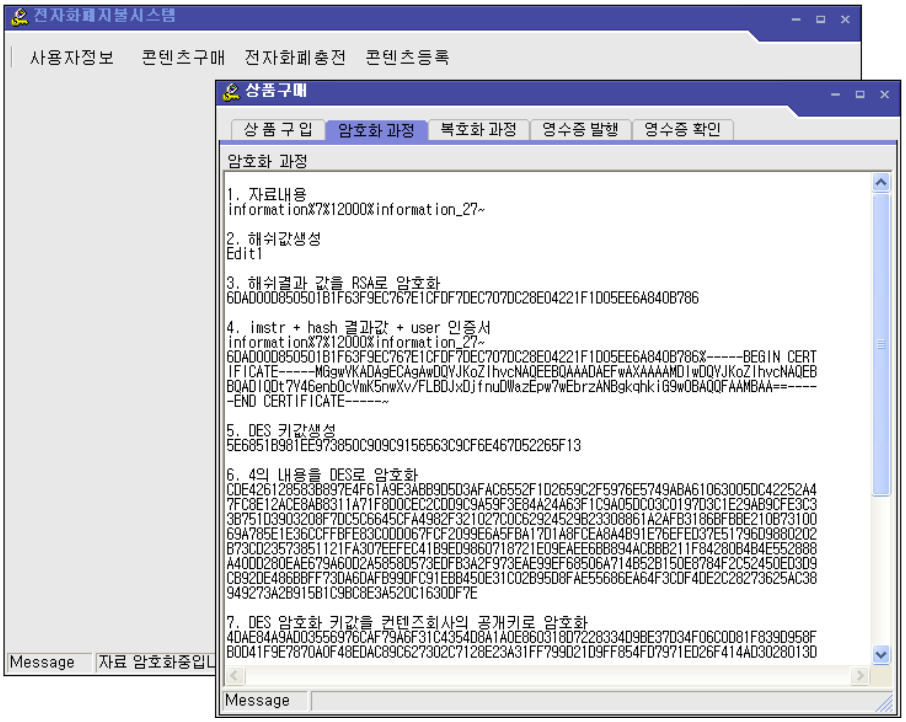

그림 12. 암호화 과정(주문 및 결제 요청)

[자료 암호화 과정 및 각 단계 값]

1. 자료내용

information%7%12000%information_27~

2. 해쉬값 생성

Edit1

3. 해쉬 결과 값을 *RSA*로 암호화

6DAD00D850501B1F63F9EC767E1CFDF7DEC707DC28E04221F1D05EE6A840B786

4. imstr + hash 결과값 + *user* 인증서

information%7%12000%information_27~

6DAD00D850501B1F63F9EC767E1CFDF7DEC707DC28E04221F1D05EE6A840B786%-----BEGIN CERT

IFICATE-----MGgwVKADAgECAgAwDQYJKoZIhvcNAQEEBQAAADAEFwAXAAAAMDIwDQYJKoZIhvcNAQEB

BQADIQDt7Y46enbOcVmK5nwXv/FLBDJxDjfnuDWazEpw7wEhrzANBgkqhkiG9wOBAQQFAAMBAA=-----END CERTIFICATE-----~

5. DES 키 값 생성

5E6851B981EE973850C909C9156563C9CF6E467D52265F13

*6. 4*의 내용을 *DES*로 암호화

CDE426128583B897E4F61A9E3ABB9D5D3AFAC6552F1D2659C2F5976E5749ABA61063005DC42252A4

7FC8E12ACE8AB8311A71F8D0CEC2CDD9C9A59F3E84A24A63F1C9A05DC03C0197D3C1E29AB9CFE3C3

3B751D3903208F7DC5C6645CFA4982F321027C0C62924529B23308861A2AFB3186BFBBE210B73100

69A785E1E36CCFFBFE83C0DD067FCF2099E6A5FBA17D1A8FCEA8A4B91E76EFED37E51796D9880202

B73CD23573851121FA307EEFEC41B9ED9860718721E09EAEE6BB894ACBBB211F84280B4B4E552888

A40DD280EAE679A60D2A5858D573EDFB3A2F973EAE99EF68506A714B52B150E8784F2C52450ED3D9

CB92DE486BBFF73DA6DAFB99DFC91EBB450E31C02B95D8FAE55686EA64F3CDF4DE2C28273625AC38

949273A2B915B1C9BC8E3A520C1630DF7E

7. DES 암호화 키 값을 컨텐츠회사의 공개키로 암호화

4DAE84A9AD03556976CAF79A6F31C4354D8A1A0E860318D7228334D9BE37D34F06C0D81F839D958F

B0D41F9E7870A0F48EDAC89C627302C7128E23A31FF799D21D9FF854FD7971ED26F414AD3028013D

4E79FFCFA63AE0E2AF7B505D98683566

*8. 6*과 *7*의 내용을 전송

CDE426128583B897E4F61A9E3ABB9D5D3AFAC6552F1D2659C2F5976E5749ABA61063005DC42252A4

7FC8E12ACE8AB8311A71F8D0CEC2CDD9C9A59F3E84A24A63F1C9A05DC03C0197D3C1E29AB9CFE3C3
3B751D3903208F7DC5C6645CFA4982F321027C0C62924529B23308861A2AFB3186BFBBE210B73100
69A785E1E36CCFFBFE83C0DD067FCF2099E6A5FBA17D1A8FCEA8A4B91E76EFED37E51796D9880202
B73CD23573851121FA307EEFEC41B9ED9860718721E09EAEE6BB894ACBBB211F84280B4B4E552888
A40DD280EAE679A60D2A5858D573EDFB3A2F973EAE99EF68506A714B52B150E8784F2C52450ED3D9
CB92DE486BBFF73DA6DAFB99DFC91EBB450E31C02B95D8FAE55686EA64F3CDF4DE2C28273625AC38

수행시간:*0.203*초

g. 복호화를 통한 콘텐츠 제공

콘텐츠 구매 요청에 따라 판매자의 복호화 처리과정을 그림13에 단계적으로 표현하였다. 복호화 처리 과정에서 정당한 구매자로 판명되면 전자화폐의 전송이 이루어지며, 자료의 다운로드 및 영수증을 발행한다.

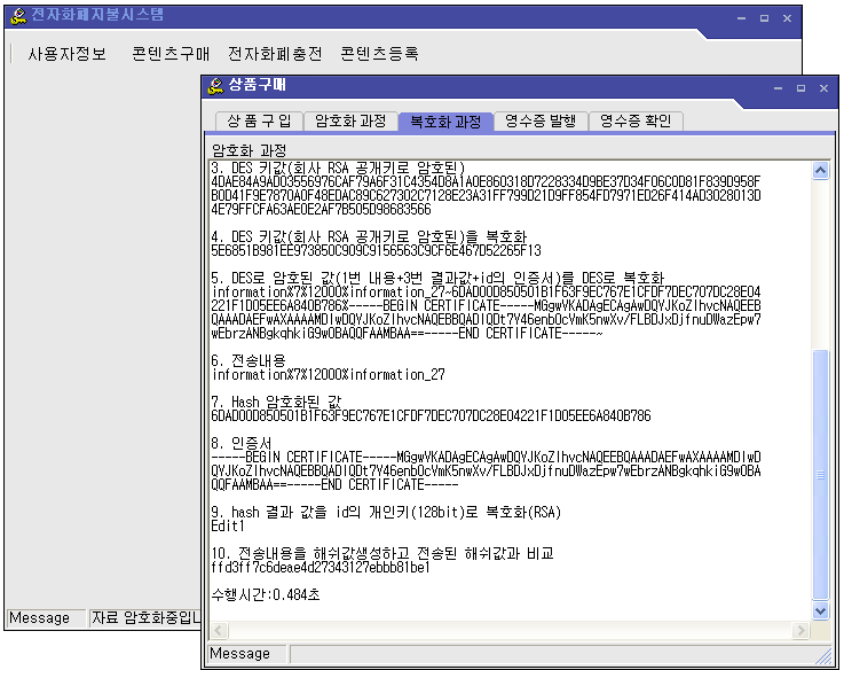

그림 13. 복호화 과정(결제)

[자료 복호화 과정 및 각 단계 값]

1. 암호화된 문자열

CDE426128583B897E4F61A9E3ABB9D5D3AFAC6552F1D2659C2F5976E5749ABA61063005DC42252A4
7FC8E12ACE8AB8311A71F8D0CEC2CDD9C9A59F3E84A24A63F1C9A05DC03C0197D3C1E29AB9CFE3C3
3B751D3903208F7DC5C6645CFA4982F321027C0C62924529B23308861A2AFB3186BFBBE210B73100
69A785E1E36CCFFBFE83C0DD067FCF2099E6A5FBA17D1A8FCEA8A4B91E76EFED37E51796D9880202
B73CD23573851121FA307EEFEC41B9ED9860718721E09EAEE6BB894ACBBB211F84280B4B4E552888
A40DD280EAE679A60D2A5858D573EDFB3A2F973EAE99EF68506A714B52B150E8784F2C52450ED3D9
CB92DE486BBFF73DA6DAFB99DFC91EBB450E31C02B95D8FAE55686EA64F3CDF4DE2C28273625AC38
949273A2B915B1C9BC8E3A520C1630DF7E%4DAE84A9AD03556976CAF79A6F31C4354D8A1A0E86031
8D7228334D9BE37D34F06C0D81F839D958FB0D41F9E7870A0F48EDAC89C627302C7128E23A31FF79
9D21D9FF854FD7971ED26F414AD3028013D4E79FFCFA63AE0E2AF7B505D98683566

*2. (1*번 내용+*3*번 결과값+*id*의 인증서*)*의 *DES* 암호화된 값

CDE426128583B897E4F61A9E3ABB9D5D3AFAC6552F1D2659C2F5976E5749ABA61063005DC42252A4
7FC8E12ACE8AB8311A71F8D0CEC2CDD9C9A59F3E84A24A63F1C9A05DC03C0197D3C1E29AB9CFE3C3
3B751D3903208F7DC5C6645CFA4982F321027C0C62924529B23308861A2AFB3186BFBBE210B73100
69A785E1E36CCFFBFE83C0DD067FCF2099E6A5FBA17D1A8FCEA8A4B91E76EFED37E51796D9880202
B73CD23573851121FA307EEFEC41B9ED9860718721E09EAEE6BB894ACBBB211F84280B4B4E552888
A40DD280EAE679A60D2A5858D573EDFB3A2F973EAE99EF68506A714B52B150E8784F2C52450ED3D9
CB92DE486BBFF73DA6DAFB99DFC91EBB450E31C02B95D8FAE55686EA64F3CDF4DE2C28273625AC38
949273A2B915B1C9BC8E3A520C1630DF7E

3. DES 키 값*(*회사 *RSA* 공개키로 암호화*)*

4DAE84A9AD03556976CAF79A6F31C4354D8A1A0E860318D7228334D9BE37D34F06C0D81F839D958FB0D41F9E7870A0F48EDAC89C627302C7128E23A31FF799D21D9FF854FD7971ED26F414AD3028013D4E79FFCFA63AE0E2AF7B505D98683566

4. DES 키 값*(*회사 *RSA* 공개키로 암호화*)*을 복호화

5E6851B981EE973850C909C9156563C9CF6E467D52265F13

*5. DES*로 암호화된 값*(1*번 내용*+3*번 결과값*+id*의 인증서*)*를 *DES*로 복호화

information%7%12000%information_27~6DAD00D850501B1F63F9EC767E1CFDF7DEC707DC28E04221F1D05EE6A840B786%-----BEGIN CERTIFICATE-----MGgwVKADAgECAgAwDQYJKoZIhvcNAQEEBQAAADAEFwAXAAAAMDIwDQYJKoZIhvcNAQEBBQADIQDt7Y46enb0cVmK5nwXv/FLBDJxDjfnuDWazEpw7wEbrzANBgkqhkiG9w0BAQQFAAMBAA==------END CERTIFICATE-----~

6. 전송내용

information%7%12000%information_27

7. Hash 암호화된 값

6DAD00D850501B1F63F9EC767E1CFDF7DEC707DC28E04221F1D05EE6A840B786

8. 인증서

-----BEGIN CERTIFICATE-----MGgwVKADAgECAgAwDQYJKoZIhvcNAQEEBQAAADAEFwAXAAAAMDIwDQYJKoZIhvcNAQEBBQADIQDt7Y46enb0cVmK5nwXv/FLBDJxDjfnuDWazEpw7wEbrzANBgkqhkiG9w0BAQQFAAMBAA==------END CERTIFICATE-----

9. hash 결과 값을 *id*의 개인키*(128*비트*)*로 복호화*(RSA)*

Edit1

10. 전송내용을 해쉬 값 생성하고 전송된 해쉬 값과 비교

ffd3ff7c6deae4d27343127ebbb81be1

수행시간*:0.078*초

h. 영수증 발행

콘텐츠에 대한 결제 및 전송이 이루어지면 판매자는 구매자에게 구매한 콘텐츠의 관련자료와 함께 영수증을 그림 14와 같이 암호화하여 발행한다. 구매자는 콘텐츠 주문시에 사용된 자료들과 영수증에 포함된 자료들을 비교 검토함으로써 구매 및 결제를 완료한다.

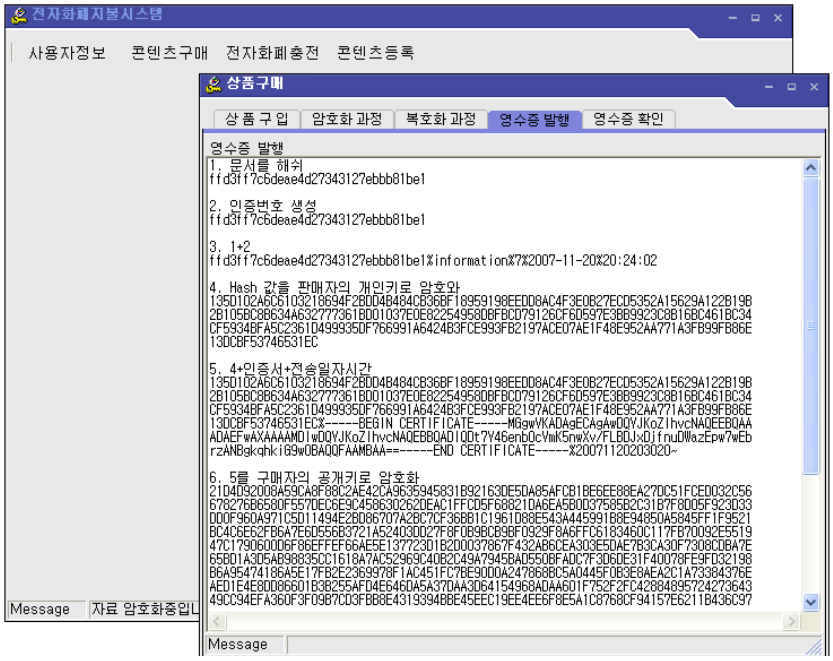

그림 14. 영수증 발행

[영수증 암호화 과정 및 각 단계 값]

1. 문서를 해쉬

ffd3ff7c6deae4d27343127ebbb81be1

2. 인증번호 생성

ffd3ff7c6deae4d27343127ebbb81be1

3. 1+2 결합

ffd3ff7c6deae4d27343127ebbb81be1%information%7%2007-11-20%20:24:02

4. Hash 값을 판매자의 개인키로 암호화

135D102A6C6103218694F2BDD4B484CB36BF18959198EEDD8AC4F3E0B27ECD5352A15629A122B19B2B105BC8B634A632777361BD01037E0E82254958DBFBCD79126CF6D597E3BB9923C8B16BC461BC34CF5934BFA5C2361D499935DF766991A6424B3FCE993FB2197ACE07AE1F48E952AA771A3FB99FB86E13DCBF53746531EC

5. 4+인증서+전송일자시간

135D102A6C6103218694F2BDD4B484CB36BF18959198EEDD8AC4F3E0B27ECD5352A15629A122B19B2B105BC8B634A632777361BD01037E0E82254958DBFBCD79126CF6D597E3BB9923C8B16BC461BC34CF5934BFA5C2361D499935DF766991A6424B3FCE993FB2197ACE07AE1F48E952AA771A3FB99FB86E13DCBF53746531EC%-----BEGIN CERTIFICATE-----MGgwVKADAgECAgAwDQYJKoZIhvcNAQEEBQAAADAEFwAXAAAAMDIwDQYJKoZIhvcNAQEBBQADIQDt7Y46enb0cVmK5nwXv/FLBDJxDjfnuDWazEpw7wEbrzANBgkqhkiG9w0BAQQFAAMBAA==-----END CERTIFICATE-----%20071120203020~

*6. 5*를 구매자의 공개키로 암호화

21D4D92008A59CA8F88C2AE42CA9635945831B92163DE5DA85AFCB1BE6EE88EA27DC51FCED032C56
678276B6580F557DEC6E9C458630262DEAC1FFCD5F68821DA6EA5B0D37585B2C31B7F8D05F923D33
DD0F960A971C5D11494E2BD86707A2BC7CF36BB1C1961D88E543A445991B8E94850A5845FF1F9521
BC4C6E62FB6A7E6D556B3721A52403DD27F8F0B9BCB9BF0929F8A6FFC6183460C117FB70092E5519
47C1790600D6F86EFFEF66AE5E137723D1B2D0037867F432AB6CEA303E5DAE7B3CA30F7308CDBA7E
65BD1A3D5AB98835CC1618A7AC52969C40B2C49A7945BAD550BFADC7F3D6DE31F40078FE9FD32198
B6A95474186A5E17FB2E2369978F1AC451FC7BE90D0A247868BC5A0445F0B3E8AEA2C1A73384376E
AED1E4E8DD86601B3B255AFD4E646DA5A37DAA3D64154968ADAA601F752F2FC42884895724273643
49CC94EFA360F3F09B7CD3FBB8E4319394BBE45EEC19EE4EE6F8E5A1C8768CF94157E6211B436C97
6C887CE813DF270088E7C47E7129E3F302A5054B997F9D1D85672CAB6A9390F092D5E9CA59741B93
4CFD546E8ABAF7CB05E54AEE7CA9DCC46AF1DA4FE3B2F226BBF92A274A6A7198B4255F30F997391D
7EF18D73099E270C72C2CA1C472BAF7982ECEADF757752AB765CF5A26545AC545EFA9F2CD1E5B0BD
192CEA0780B3173FEAC405668BECE6432F46C65C9AC46CE2873F3DD7163D4C321079A0E69DC7F776
2E7E58E7F8760E8364F4537D348ADE968F66608A08898A7F675269EC467CE1D90959CFEF0BCE124C
55B45A322E0A1469BD8A76C7ED2EF4860532DEFBF68BA99B0905EC4A2E0C25C68B32F04008B7CB45
A0948EFA3BDE03967F1E005C07AA29F8C154AD805CC00EEEC2F3BF24D035366CE3CDCE0EF2F76457
46C3D6B78BF42BD618875E9BABA2061071AE50281C9462902EF4CAE45F596B690BDCA3E002DE063E
EF531C134E70E39D0A9AA78047EAAC37EB3D6C10471D506384867D7E85B12C7A2E79AEC071B34491
0F7612F1BE992DE2DF1DF798217CE441

수행시간:*0.188*초

i. 영수증 확인

그림 15와 같이 영수증 확인은 판매자로부터 발행된 영수증을 복호화한 자료와 콘텐츠 주문시에 암호화하여 전송한 자료들을 비교 검토하여 전송된 자료와 영수증에 포함된 자료가 일치한다면 구매 및 결제를 완료한다.

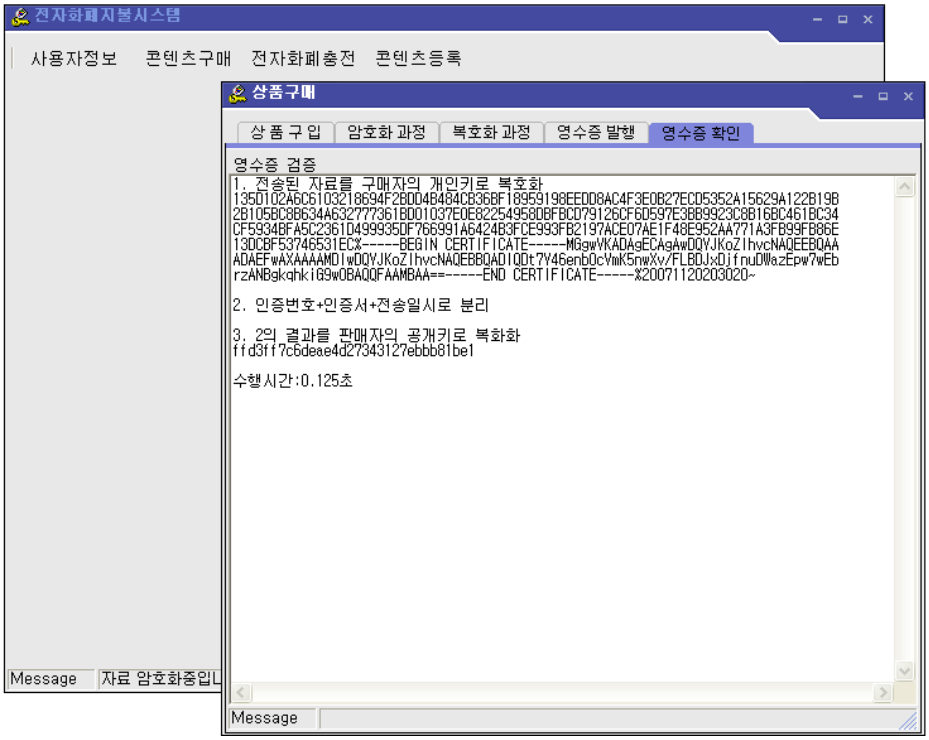

그림 15. 영수증 확인

[영수증 복호화 과정 및 각 단계 값]

1. 전송된 자료를 구매자의 개인키로 복호화

135D102A6C6103218694F2BDD4B484CB36BF18959198EEDD8AC4F3E0B27ECD5352A15629A122B19B

2B105BC8B634A632777361BD01037E0E82254958DBFBCD79126CF6D597E3BB9923C8B16BC461BC34

CF5934BFA5C2361D499935DF766991A6424B3FCE993FB2197ACE07AE1F48E952AA771A3FB99FB86E
13DCBF53746531EC%-----BEGIN CERTIFICATE-----MGgwVKADAgECAgAwDQYJKoZIhvcNAQEEBQAA
ADAEFwAXAAAAMDIwDQYJKoZIhvcNAQEBBQADIQDt7Y46enb0cVmK5nwXv/FLBDJxDjfnuDWazEpw7wEb
rzANBgkqhkiG9w0BAQQFAAMBAA==-----END CERTIFICATE-----%20071120203020~

2. 인증번호+인증서+전송일시로 분리

*3. 2*의 결과를 판매자의 공개키로 복호화

ffd3ff7c6deae4d27343127ebbb81be1

수행시간*:0.125*초

j. 전자화폐 신청 및 발행

사용자가 은행에 전자화폐를 신청하면 은행은 사용자의 잔액을 확인한 후 잔액의 한도 내에서 전자화폐를 발행한다. 지금은 가상으로 신청한 만큼 발급될 수 있도록 하였으나 은행과 정당한 연결이 이루어진다면 은행과 처리되어야 할 중요한 부분이다. 사용자가 요청한 전자화폐의 내역도 조회가 가능하도록 하였으며, 차후에는 판매자의 전자화폐가 증가한다면 전자화폐를 실명 계좌에 입금 요청할 수 있도록 하여야 한다.

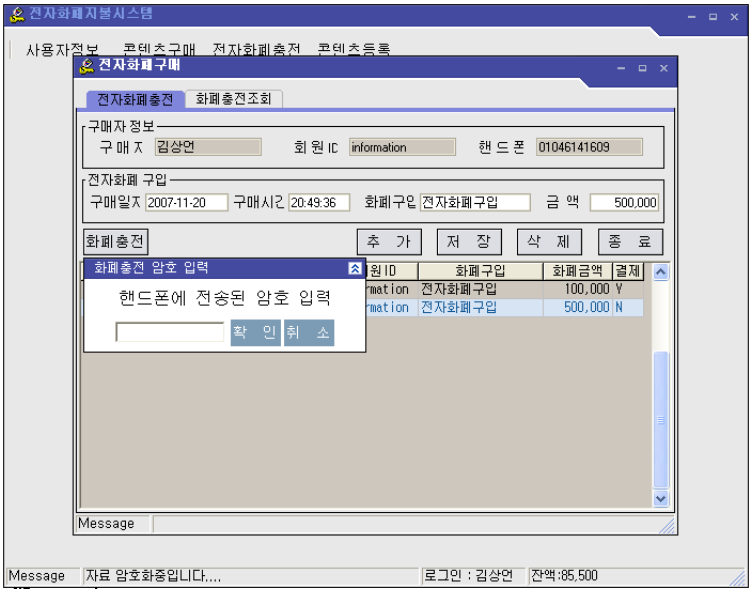

그림 16. 전자화폐 신청 및 구입

k. 상품 등록

판매자는 판매할 상품을 미리 등록한다.

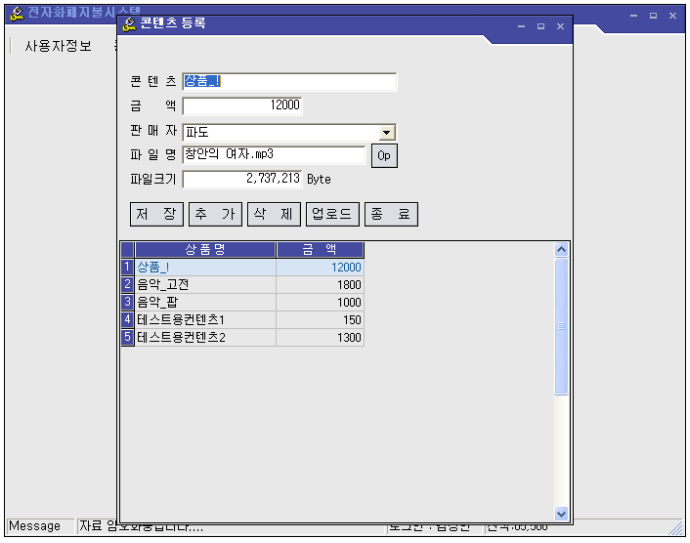

그림 17. 상품 등록

제5장 제안한 프로토콜의 분석

제1절 기존 전자지불 프로토콜과의 비교 및 성능분석

1. C-Pay 성능분석

하나의 거래를 처리하기 위해 걸리는 평균 수행시간은 표 6에서 나타난 것과 같이 0.58초이며, 총 암호화 횟수는 표 5에서와 같이 Hash함수를 포함하여 14회의 암호화 계산을 수행한다. 이러한 수행 시간은 사용자의 시스템환경에 약간의 차이는 보일 수 있으나, 전자지불 시스템을 사용하는 사용자에게 부담이 되지 않는 수행시간이라고 본다.

표 5. Contents-Pay 프로토콜의 암호화 횟수

처리구분 / 암호화구분	콘텐츠주문 (암호화,전송)	콘텐츠결제 (복호화,수신)	영수증발행 (암호화,전송)	영수증확인 (복호화,수신)	계
Hash	1	1	1	1	4
공개키암호화	2	-	2	-	4
공개키복호화	-	2	-	2	4
관용키암호화	1	-	-	-	1
관용키복호화	-	1	-	-	1
계	4	4	3	3	14

표 6. C-Pay 프로토콜의 실행시간

(단위 : 초)

처리구분 / 실험횟수	콘텐츠주문 (암호화,전송)	콘텐츠결제 (복호화,수신)	영수증발행 (암호화,전송)	영수증확인 (복호화,수신)	계
1	0.093	0.063	0.265	0.172	0.593
2	0.093	0.079	0.218	0.172	0.562
3	0.094	0.062	0.219	0.172	0.547
4	0.094	0.063	0.203	0.172	0.532
5	0.141	0.078	0.203	0.172	0.594
6	0.094	0.078	0.219	0.172	0.563
7	0.093	0.079	0.203	0.172	0.547
8	0.094	0.063	0.234	0.172	0.563
9	0.094	0.063	0.218	0.188	0.563
10	0.094	0.063	0.359	0.219	0.735
계	0.984	0.691	2.341	1.783	5.799
평균	0.098	0.069	0.234	0.178	0.580

2. Contents-Pay와 기존 전자지불 프로토콜과의 분석

대부분의 전자 지불 프로토콜이 마이크로칩과 같은 하드웨어를 사용했을 경우에는 익명성 제어가 가능하지만, 소프트웨어만으로는 익명성 제어를 제공하지 못하고 있는 실정이다. 제안된 프로토콜은 하드웨어 없이 익명성 제어가 가능하게 하였으며, 기존 프로토콜과의 전체적인 특성을 비교하면 표 7과 같다.

표 7. 기존 전자 지불 프로토콜과의 비교

비교항목 / 전자화폐	지불 형태	보안 메카니즘	*S/W* 요구 사항	*H/W* 요구 사항	익 명 성
Mondex	스마트카드	마이크로칩	X	○	○
VisaCash	선불카드	마이크로칩	○	○	○
Millicent	소액지불	소액거래	○	X	X
NetCash	전자수표	커버러스	○	X	X
E-Cash	전자화폐	RSA	○	X	X
NetBill	전자화폐	전자서명	○	X	X
Contents-Pay	전자화폐	RSA, DES	○	X	○

가. NetBill과의 비교

구매자는 NetBill 서버의 지불승인을 받은 후 상품을 수령하고, 판매자는 결제가 일어난 후 상품을 전달하기 때문에 구매자와 판매자 모두가 상호 신뢰할 수 있으

나, 매 서비스마다 서버에 접속하여 확인 절차를 거쳐야 하고, 거래 단계도 복잡함으로 인하여 다른 지불 프로토콜에 비해서 전자 서명이 많이 쓰이는 단점이 있다.

또한, 판매자는 구매자의 신원을 파악하고, NetBill에 의한 모든 거래 정보는 서버에 기록되므로 거래를 추적할 수 있기 때문에 구매자와 판매자모두 익명성이 보장되지 않는다. 하지만 새로 제안된 프로토콜의 경우 가상 ID를 사용하여 인증기관의 도움 없이는 실명정보를 알 수 없기 때문에 익명성이 보장되며, 구입과 지불을 동시에 처리함으로써 기존의 지불방식에 비해 지불 단계를 줄일 수 있다.

나. Millicent와의 비교

Millicent는 선불방식으로써 구매자가 판매자의 스크립(scrip)을 구입하여 거래하는 방식으로 암호화를 사용하지 않고 Hash 변환 연산만을 이용함으로써 구현 비용 및 연산 과정을 현저하게 줄였다. 하지만, 구매자는 각 판매자마다 다른 스크립을 구입해야 하는 번거로움이 있으며, 익명성이 보장되지 않고 판매자가 스크립 생성에 필요한 모든 정보를 알고 있기 때문에 부정한 스크립을 생성할 수 있는 문제가 있다.

그러나 제안된 프로토콜은 가상 ID를 사용함으로써 다른 판매자와의 거래도 언제든지 할 수 있으며, 판매자 독단으로는 구매와 관련된 신규 DB를 생성할 수 없도록 하였고, 영수증을 발행함으로써 판매자가 구매자를 속이고 부정한 거래를 할 수는 없다.

다. E-Cash와의 비교

디지캐쉬사에서 개발되었으며 전자동전을 사용하는 익명성을 지닌 전자화폐 시스템으로 구성원은 은행, 구매자, 상점이다. 수취인이 Ecash를 수락하기 전에 은행에 그 유효성을 검사할 때도 은행에서는 지불인의 신원을 알 수 없도록 하여 지불인의 익명성이 보장된다. 그러나 수취인이 은행계좌에 동전을 입금하게 되면, 은행

에서는 동전의 일련번호 등을 기록하여 두 번 이상 사용될 수 없도록 하는 과정에서 수취인의 입금내역을 파악할 수 있어서 수취인의 익명성은 보증되지 않는다. 또 다른 주요 단점은 사용된 화폐들을 데이터베이스에 저장하게 되는데 수많은 사용자들로 인하여 데이터베이스의 크기가 매우 커지게 되어 관리하는데 문제점이 생기는 경우이다. C-Pay의 경우 은행이나 인증기관의 개입 없이 거래가 이루어지기 때문에 거래자 모두의 익명이 보장된다.

라. NetCash와의 비교

캘리포니아 대학의 정보과학연구소에서 개발되었으며 구매자, 상점 그리고 통화서버로 구성된다. 통화서버는 전자화폐를 생성하며, 전자화폐에는 통화서버 이름, 통화서버의 네트워크 주소, 소멸날짜, 일련번호, 화폐금액 등으로 구성된다. 이러한 전자화폐는 통화서버의 비밀키로 서명되는 특징이 있다. 그러나 화폐를 교환할 때는 사용자를 알 수 없는 점을 이용하여 화폐교환에 의한 약한 익명성을 제공하고 있지만, 은행이 구매자에게 화폐를 인출할 때 화폐의 일련번호를 확인하고 온라인 데이터베이스에 기록하여 익명성을 제공하지 못하는 문제점이 있다.

3. Contents-Pay의 암호화 및 통신회수 분석

표 8에 나타낸 암호화 횟수를 볼 때 전체적으로 보면 SET에 비해 C- Pay가 공개키를 1회 더 추가로 필요하지만 SET에서는 영수증 발행에 대한 언급이 없는 상태이고, C-Pay는 영수증 발행과정을 모두 합하였을 경우의 총 동작 횟수를 나타낸 것이다. 영수증 발행과정을 제외한다면, 훨씬 적은 횟수의 동작으로 거래를 처리할 수 있다. 표 9에서 나타난 것과 같이 통신 횟수 또한 콘텐츠만을 취급하는 특정 프로토콜을 사용하여 상품 전달과 대금 지불이 동일 네트워크에서 이루어진다는 특성을 살려 주문과 결제를 동시에 처리할 때 1회 통신과, 영수증을 전달받을 때 1회로 하여 단 2회의 메세지 전달로 모든 거래가 종료 되도록 하였다. 단, 다운받을

콘텐츠의 크기와 전송 속도에 따라 약간의 시간이 추가로 소요되지만 우편으로 전송되는 시간에 비하면 많은 시간을 절약하게 되며, 배달 사고 및 파손 등의 예기치 못한 사고는 없을 것으로 본다.

암호화 횟수 및 통신횟수를 SET 시스템과 비교한 이유는 SET 시스템이 암호기술을 기반으로 한 신용카드 결제 프로토콜의 규격으로 사용되고 있으며, 디지털 서명 등을 통한 안전한 거래가 이루어지고 있기 때문이다.

표 8. 암호화 횟수 비교

	공개키		관용키		비고
	C-Pay	*SET*	*C-Pay*	*SET*	
암호화 횟수	8	7	2	3	영수증 발행과정 포함
	4	7	1	3	영수증 발행과정 제외

표 9. 통신 횟수 비교

	C-Pay	*SET*	비 고
통 신 횟 수	2	12	영수증 발행과정 포함
	1	12	영수증 발행과정 제외

제2절 제안한 프로토콜의 안전성 및 효율성

제안된 프로토콜은 안전성과 효율성 측면에서 다음과 같은 특징들을 보여 준다.

1. 모든 거래에는 항상 인증서와 일련번호를 함께 제출하여 일상의 당좌 수표처럼 인출 시점마다 금액에 일련번호를 남긴다. 그렇게 함으로써 제한적이나마 필요시에 자금의 흐름을 인증기관의 협조를 얻어 밝혀낼 수 있다.
2. 모든 거래는 할당받은 인증번호를 사용하기 때문에 은행이나 상점에서는 거래 당사자의 실명내용을 알 수 없도록 하였다.
3. 당좌 거래에 포함되는 당좌통장처럼 거래 내역을 본인이 상세하게 알 수 있도록 하였으며, 평소에는 잔액만 보관하기 때문에 자금의 흐름을 알 수 없다.
4. 상품이 모두 디지털로 되어 있기 때문에 상품 제공과 지불 사에 생기는 공백으로 인한 불신이 발생하지 않는다는 점을 감안하여, 상품 주문과 지불을 동시에 처리함으로써 거래 단계를 단축시킬 수 있었다.
5. 전자화폐 발행 및 상품 구매 등의 모든 거래를 서버의 거래 DB에 저장함으로써 구매자가 정당한 접속을 시도할 경우 구매자의 모든 거래내역을 파악할 수 있고, 거래 시점에서 사용 가능한 전자화폐의 금액을 표시할 수 있다.
6. 거래내역을 서버에서 관리하기 때문에 지불서버의 안전성과 기밀성이 확보된다면, 사용자는 안전한 거래를 할 수 있다.

제6장 결 론

본 논문에서는 디지털 콘텐츠 거래를 위해 개발된 NetBill 시스템, 네트워크형 지불 시스템인 E-Cash 및 NetCash 시스템에서 익명성을 보장하지 못했던 단점을 보완하고 복잡한 지불 과정을 동일 네트워크에서 처리함으로써 지불단계를 간략화하여 암호화 횟수 및 통신횟수를 감소시킴으로서 시스템의 효율성 및 안전성이 확보되도록 한 네트워크형 전자지불 프로토콜을 설계 및 구현하여 다음과 같은 결과를 얻었다.

1. 모든 거래에는 항상 인증서와 인증번호를 함께 제출하여 일상의 당좌 수표처럼 인출 시점마다 금액에 로그기록을 남김으로써 필요시에 작은 금액이나 큰 금액이나 자금의 흐름을 인증기관의 협조를 얻어 명확하게 밝혀낼 수 있다.
2. 당좌 거래에 포함되는 당좌통장처럼 거래 내역을 본인은 상세하게 알 수 있도록 하였으며, 평소에는 잔액만 보관하기 때문에 자금의 흐름을 알 수 없지만 불법적인 사건에 대해 조사할 필요성이 생기면 자금의 흐름을 추적할 수 있도록 하였다.
3. 제안된 프로토콜은 영수증 발행 및 검증 절차를 수행하여 거래 당사자간에 정보의 전달 내용에 대해 부인할 수 없도록 하였다.
4. 전자 화폐에 대한 사용도 일련번호를 부여하고, 접속과 동시에 잔액을 계산함으로써 잔액 이상인 초과 금액의 사용이나 이중 사용이 불가능하도록 하였다.
6. 콘텐츠의 제공도 인증번호를 부여하여 사용자가 인증번호를 입력하여 다운로드받을 수 있다.
7. 판매자가 영수증의 발급 및 검증 절차를 수행함으로써 거래의 단계가 다른 시

스템에 비하여 줄어들었으며, 전자화폐의 잔액이 허락하는 금액만큼 제약 없이 사용할 수 있다.

8. 지불 과정을 동일 네트워크에서 처리하여 지불단계를 줄일 수 있었으며, 암호화 횟수 및 통신횟수를 감소시킴으로서 시스템의 효율성 및 안전성이 확보된다.
9. 처리 속도를 측정한 결과 시스템과 통신회선에 따라 정도 차이는 발생하겠지만 상품 주문에서부터 영수증을 확인하는 과정까지 소요되는 시간은 평균 0.58초로 사용자가 처리 시간으로 인한 문제점을 제기하지 않을 만한 처리 속도를 보였다.

현대 사회는 디지털 콘텐츠의 거래가 증가하는 추세인 만큼 누적되는 거래량으로 인하여 서버의 데이터량이 증가하고, 접속이 폭주되어 서버의 과부하를 초래하는 취약성이 문제점으로 제기될 수 있다.

이러한 문제점을 보완하고 더욱 발전된 전자상거래 시스템의 개발을 위하여 향후 연구과제로는 개인의 거래 내역에 대한 일괄적이면서 빠른 계산이 요구되며, 거래 전체에 대한 일괄 계산으로 불법적인 전자 화폐의 유무를 밝혀내고, 발견되면 자동으로 추적을 하는 단계가 필요하다.

많은 양의 거래를 빠른 시간에 계산할 수 있는 빠르고 안전한 데이터베이스의 요구도 절실한 상황이고, 지금 보다도 더 빠르고 안전한 통신망 시스템의 확보와 은행권 등 금융망 및 정부의 법적 제도개선도 중요하다고 본다.

이러한 시스템의 발달은 전자적인 거래의 발달을 가져와 전자상거래 뿐만이 아닌 많은 분야에서 이용되리라고 생각된다.

참 고 문 헌

[1] David Chaum, "Blind Signatures for Untraceable Patments. " Advances in Cryptology-Proceedings of Crypto '83, pp.199-203, 1983.

[2] 이만영 외5, 『전자상거래 보안 기술』, 서울 생능출판사, 1999.

[3] http://kosis.nso.go.kr/cgi-bin/sws_999.cgi : 통계청 전자상거래 거래 내역

[4] 한재선 외3, "웹 애플리케이션 서버 : 인터넷 전자상거래를 위한 공용 플랫폼", EC/CALS 기술 워크샵 논문지, pp. 63-69, 1999.

[5] David Chaum, Amos Fiat, and Moni Naor, "Untraceable Electronic Cash," Advances in Cryptology-Crypto '88, LNCS 403, Springer Verlag, pp. 319-327, 1988.

[6] David Chaum,"Online Cash Checks," Advances in Cryptology-Eurocrypto '89, LNCS 434, Springer Verlag, pp. 288-293, 1989.

[7] Selected Implication of Global Electronic Commerce, 1996. 11.

[8] T. Okamoto and K. Ohta, "Disposable Zero-knowledge Authentications and Their Applications to Untraceable Electronic Cash," Proceeding of Crypto '89, pp. 481-496, 1989.

[9] David Chaum and T. P. Pederson, "Wallet database with observes," Proceeding of Crypto '92, Springer Verlag, pp. 89-105, 1992.

[10] T. Okamoto and K. Ohta, "Universal Electronic Cash," In Advances in Cryptology-Crypto '91, pp. 324-337, 1991.

[11] T. Okamoto, "An Efficient Divisible Electronic Cash Scheme," Advances in Cryptology, Proceeding of Crypto '95, pp. 438-451, 1995.

[12] Von Solms and D. Naccache, "On Blind Signatures and Perfect Crimes.", Computers and Security. 11, pp. 581-583, 1992.

[13] Stadler, M., M. Piveteau, and J. Camenisch, "Fair Blind Signatures," Advances in Cryptology-Proceeding of Eurocrypt '95. 1995.

[14] 한국 정보보호 센터, 정보통신망 정보보호 워크숍, "암호이론", "PKI(Public Key Infrastructure)", 특강자료집, pp. 7-52, pp. 209-252, 1998.

[15] 한승조, "Concatenation System of Compression and Secrecy Coding with Authenticity in Real-Time Communication Environment", 충북대학교 박사학위 논문, pp. 7-32, 1994.

[16] 최진탁, "An Implementation of Extended Data Base Security System Using Cryptography", 경희대학교 박사학위 논문, pp. 25-60, 1990.

[17] Whitefield Diffie and Martin E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, pp. 644-654 Nov. 1976.

[18] Whitefield Diffie and Martin E. Hellman, "Multiuser Cryptographic techniques," In proceeding of AFIPS National Computer Conference, N. Y., pp. 109-112, June 7-10, 1976.

[19] R. C. Merkle and M. E. Hellman, "Hiding information and signatures in trapdoor knapsacks," IEEE Trans. Infor. Th, vol. IT-24, pp. 525-530, Sep. 1978.

[20] William Stallings, Ph. D. Network and Internetwork Security, 1995 by Practice-Hall, Inc. pp. 395-441

[21] Federal PKI Study Final Report, MITRE, 1994.

[22] X.509 Public Key Infrastructure Certificate and CRL Progile, IETF.

[23] S. G. Aki, "Digtal signatures : A tutorial survey," IEEE Computer Magazine, pp. 15-24, Feb. 1993

[24] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public croptosystems," Communications of the Association of Computer Manufactures, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[25] C. Pomerance, J. W. Smith and R. Tuler, "A pipe-line architecture for factoring large integers with the quadratic sieve algorithm," SIAM J.Comp, vol. 17, pp. 387-403, 1988.

[26] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Infor. Theory, vol. IT-31, pp. 469-472, 1985.

[27] H. Ong, C. P. Schnorr, and A. Shamir, "An efficient signature schemo based on quadratic equations," Proc. 16th symp. Theory of Computing, Washington DC, Apr. 1984.

[28] J. M. Pollard and C. P. Schnorr, "An efficient solution of the congruence X^2 + KY^2 ≡ m (mod n)," IEEE Trans. Inform. Theory, vol. IT-33, no. 5, pp. 702-709, Sep. 1987.

[29] A. Shamir, "Identity-based cryptosystem and signature schene," in proceeding of Crypto 84, pp. 47-53, 1984.

[30] Camenisch. J., J.Piveteau, and M. Stadler. "An Efficient Fair Payment System." 3rd ACM Conference on Computer and Communications Security, pp. 84-94, 1996.

[31] Brands, S., "Untraceable off-line Cash in Wallets with Observers. " Proceddings of Crypto '93, pp. 302-318, 1993.

[32] Brickell, E., P. Gemmel, and D. Kravitz. "Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change," Proceedings of Crypto '93, pp. 302-318

[33] Camenisch. J., U. Maurer, and M. Stadler. "Digital Payment Systems with Passive Anonymity-Revoking Trustees." Computer Security - ESORICS '96. pp. 33-43, 1996.

[34] Security of Electronicmoney, Bank for International Settlements, 1996.

[35] B. Cox, J. D. Tygar and M. Sirbu, "NetBill Security and Transaction Protocol," Proceeding of 1st USENIX on Electronic Commerce, 1996.

[36] X.509 Public Key Infrastructure Certificate Management Protocols, IETF.

[37] X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Statement Framework, IETF.

[38] 'PGP', Simson Garfinkel, O'Reilly & Associates. Inc, 1995.

[39] 'Secure Commerce on the Internet,' Vijay Ahuja, AP Professional, 1996.

저작물 이용 허락서

학 과	정보통신	학 번	20067220	과 정	석사
성 명	한글: 김 상 언 한문 : 金 相 言 영문 : Sang-eun Kim				
주 소	전라남도 여수시 봉계동 대광오투빌 110동 1093호				
연락처	E-MAIL : dandylsd@daum.net				
논문제목	한글 : 전자상거래를 위한 안전한 인증 프로토콜 설계				
	영문 : Secure Certification Protocol for The Electronic Commerce				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함
2. 위의 목적을 위하여 필요한 범위 내에서의 편집·형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사 표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 또는 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물의 이용허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음
7. 소속대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의(○) 반대( )

2008년 2월 25일

저작자: 김 상 언 (서명 또는 인)

조선대학교 총장 귀하