인터넷 쇼핑몰 구축 패키지용 CM-Wallet 개발†)
(Development of CM-Wallet for Internet Shopping Mall Package)

권영직*) 박유경**) 김우헌**)
(Young Jik Kwon)(You Kyoung Park)(Woo Hun Kim)
대구대학교 컴퓨터 정보공학부

<요 약>

본 연구에서는 인터넷 쇼핑몰 패키지용 전자지불시스템에서 구매자가 인터넷상에서 안전한 지불을 하기 위해 사용하는 전자지갑인 CM-Wallet을 SET프로토콜기준에 따라 개발하였다. CM-Wallet은 RSA 1024bit, Triple DES 168bit 암호키 및 전자서명, 이중서명을 생성하므로서 메시지 보안도가 SET 기준을 만족하였다. 그리고, 복잡한 절차는 내부적으로 처리하여 구매자가 사용하기 쉽게 화면으로 보여지는 절차를 간소화하였으며, 전자지갑을 사용할 때 복잡한 절차에 대한 불편함을 해소하였다.

1. 서 론

1.1..1 연구의 배경과 목적

인터넷을 통한 전자 거래는 여러 가지 이점을 제공하지만, 안전한 전자거래를 위해서는 해결해야 할 몇 가지 과제들이 있다. 그 가운데 가장 중요한 것의 하나가 지불절차의 보안 문제의 해결이다. 전자거래를 위해서는 신용카드 정보와 같은 중요한 정보들이 네트웍을 통해 전송되게 되는데 이러한 정보들에 대한 보호가 이루어져야 하는 것이다. 전자거래에서의 인증이나 암호기술이 필요한 것은 인터넷상의 전자상점에서 쇼핑할 때, 구매자나 전자상점이 진짜 당사자인지를 확인하기 위한 수단으로 주로 이용되며, 전자거래의 모든 상황에서 이용되고, 특히 전자지불 시스템을 개발 시에는 주요 요소 기술이 된다.

전자지불 시스템에는 대중적인 신용카드 기반의 전자지불 시스템 모델을 위한 전자지불 프로토콜이 많이 개발되고 있다. 신용카드 기반의 전자지불 프로토콜은 비자와 마스터카드사에서 공동 개발한

*) 대구대학교 컴퓨터정보공학부 교수

**) 대구대학교 대학원 컴퓨터정보공학과 석사과정

SET(Secure Electronic Transaction)프로토콜이 표준화되고 있으며 일본에서는 이미 일본상거래용 SET 프로토콜의 확장판인 JPO(Japanese Payment Option)를 인증 받았다[1]. 그러나, 국내에서는 아직까지 SETCo에서 정식으로 인증 받은 SET기반의 전자지불 시스템이 없는 상황이며, 이에 관한 관련 연구가 진행되고 있으며 특히 SET 규정에 맞는 메시지 개발기술 연구가 필요하다 하겠다[1].

이러한 필요성에 따라 본 연구에서는 인터넷 쇼핑몰 구축 패키지용 전자지불 시스템에 있어서 구매자가 사용하는 프로그램인 전자지갑 CM-Wallet을 개발하였다.

1.1.2. 연구 방법

본 연구에서는 전자지불 시스템에 필요한 전자지갑 개발을 위하여 전자지갑의 구성과 지불처리 흐름도와 기존 전자지갑의 분석, 전자지갑의 동작원리에 대하여 고찰하여 보았다. 전자지갑의 요소기술인 대칭키/비대칭키 암호기술에 대해서도 고찰하여 보았다.

†) 본 연구는 1999년도 중소기업 기술혁신 개발과제의 위탁연구 사업비 지원에 의한 연구임

그리고, 특히 SET의 분석에서 CM-Wallet 설계 개발에 필요한 SET protocol, SET 구성원간의 메시지와 필요기술을 규명하여 두었다.
전자지갑 설계 방법은 객체지향적 설계방식을 따라 각 모듈별로 암호생성, 사용자관리, 지갑관리 모듈로 나눠 설계를 하였고, 개발언어는 비주얼 C++을 사용하여 전자지갑의 GUI 구현과 RSAEuro를 이용한 암호모듈을 개발하였다.

2. 관련연구

2.1 전자지갑의 개요

신용카드기반 전자지불 시스템에서는 카드 소지자, 카드 소지자의 지불 정보를 관리하는 어플리케이션인 전자지갑을 사용하는데 이 장에서는 기존의 전자지갑에 대하여 알아보고 전자지갑 개발을 위한 요소기술에 대하여 고찰하여 보았다.

2.1.1 전자지갑의 정의

전자지갑은 인터넷상에서 상품을 구매한 후 상품대금을 인터넷을 이용하여 바로 지불할 수 있도록 도와주는 프로그램이다. 전자지갑에는 지불하려는 사람의 카드/계좌 정보가 등록되어 있어서 카드/계좌를 선택하고 비밀번호를 입력하면 PC에서 모든 일을 처리할 수 있는 편리한 프로그램이다.

2.1.2 전자지갑의 용도

전자지갑의 용도는 인터넷과 같은 네트워크 공간에서 상품을 구매한 후 상품 대금을 인터넷을 이용해 바로 지불할 수 있도록 도와주는 프로그램이다. 따라서 사용자의 지불수단에 대한 인증서를 발급 받을 수 있는 기능과 이를 통해 쇼핑몰에서 구매한 상품에 대해 지불할 수 있으며 자신이 주문한 구매 정보를 계속적으로 조회할 수 있으므로 가계부로도 사용할 수 있다.

2.1.3 전자지갑의 구성

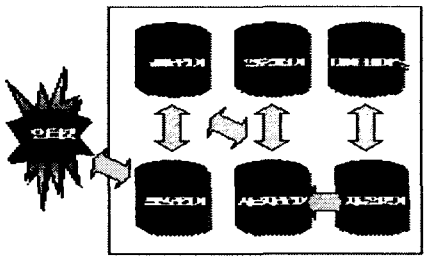
전자지갑의 구성은 [그림 1]과 같다. [그림 1]을 보면 사용자가 전자지갑을 사용하려고 할 때 사용자의 인증과 사용자 신용정보 관리를 위한 사용자 관리기와 구매정보를 관리하는 구매 관리기 , 사용자의 정보를 입력하는 자료 입력기와 공급자와 정보를 교환할 시 그 정보를 암호화 시켜주는 암호 생성기 그리고 통신을 위한 통신 관리기와 데이터 베이스를 관리하는 데이터 베이스 관리기로 나눌 수 있다.

2.1.4 전자지갑의 동작원리

전자지갑의 동작원리를 분류해 보면 Plug-in 형 전자지갑과 Proxy 형 전자지갑 그리고 Helper 형 전자지갑으로 나눌 수가 있다.

Plug-in 형 전자지갑은 사용자가 브라우저 상의 지불 버튼을 클릭하는 순간 전자지갑이 자동 동작하여 지불 처리를 하며 HTTP 기반의 전자지불 프로토콜을 이용한다.
Proxy 형 전자지갑은 암호화/복호화, 전자서명의 생성 및 확인 등의 지불처리는 전자지갑에서 처리를 하며 그 외의 통신은 브라우저와 서버간의 HTTP 통신으로 처리한다.

Helper 형 전자지갑은 지불 처리시 별도의 지불 프로토콜을 통해 통신을 하며 현재 대부분의 전자지갑이 Helper형을 채택하고 있다. CM-Wallet도 Helper 형을 채택하였다.



[그림 1] 전자지갑의 구성도

2.1.2 기존의 전자지갑

이용자들이 인터넷을 이용해 보다 편리하게 쇼핑할 수 있도록 지원하는 것이 바로 전자지갑이다. 전자지갑이란 말 그대로 현실 세계의 지갑을 가상으로 만들어놓은 것을 말한다. 인터넷상에서 이용하는 네

트워크형 전자지갑을 이용하면 상품을 구입할 때마다 인적 사항을 일일이 적어 넣지 않아도 되고 자신이 가지고 있는 카드 중 원하는 것으로 대금을 치를 수 있다. 또 암호화 기능을 가지고 있어 해킹이나 카드번호 유출 등을 걱정하지 않아도 된다.

이와 함께 전자지갑에 따라서는 온라인 영수증 기능이 있어 일일이 거래내역을 적어놓지 않아도 지출한 내용을 일목요연하게 알 수 있다.

이와 같은 편리함 때문에 미국·일본 등 선진국에서는 다양한 전자지갑을 개발해 선보이고 있다. 미국의 사이버 캐시사는 최근 자바를 기반으로 한 네트워크형 전자지갑 「인스터바이」를 선보였다. 이외에 디지 캐시사에서 「e캐시」란 제품을 내놓았으며, 유럽과 호주·일본 등에서도 전자지갑을 이용한 쇼핑몰 운영이 활기를 띠고 있다.

국내에도 여러 업체들이 다양한 전자지갑을 개발하여 자사의 지불 서버를 이용하는 홈쇼핑업체들을 대상으로 제공하고 있다. 데이콤은 자체 개발한 전자지갑 프로그램을 데이콤 내 전자거래 호스팅 업체들을 대상으로 제공하고 있다. 또 최근에는 커머스넷 코리아를 주축으로 「아이캐시(ICash)」란 전자지갑을 개발, 보급을 추진중이다. 이 전자지갑은 신용카드 결제와 은행 계좌이체를 함께 지원하고 있으며 IC카드를 지원하는 골드형과 네트워크만을 지원하는 실버형 두 가지가 있다.
인터넷 보안 전문업체인 이니텍도 「이니텍 페이」란 Non-SET방식의 전자지갑을 내놓았다. 이 제품은 2천48비트의 길이를 갖는 RSA기술을 사용하고 있다. 이 외에 메타랜드가 SET방식을 지원하는 전자지갑을 내놓고 있으며, LG인터넷[http://lgis.channel.net/]도 Non-SET방식의 전자지갑 「넷크레딧」을 선보였다.

2.2 전자지갑 요소 기술 연구

2.2.1 전자지갑의 요소 기술

전자지갑의 주문, 지불과 관련해서는 구현기술, 보안기술, 암호화 기술, 과세 관련 기술들이 필요하다.

전자지갑을 구현하기 위해서는 기본적으로 GUI(Graphic User Interface)기술과 함께 보안기술도 적용해야 한다. 보안기술로는 암호화, 메시지다이제스트, 인증, 방화벽 기술들 외에 IC 카드 관련 기술들이 최근 각광을 받고 있다. IC 카드를 지불처리에 사용하기위해서는 IC 카드용 운영체제인 COS(chip operating system)와 DES, RSA 등의 암호화를 지원하는 코프로세서의 개발이 필요하다.

지불처리에 참여하는 공급자, 카드소지자, 금융기관, 인증기관간에 전달되는 자료의 통일성을 위해 특히 중요한 것이 암호화 기술이다. 현재 서로 다른 컴퓨터간에 전달되는 자료의 통일성을 위하여 국제표준으로 제정되어 있는 것이 ASN.1(abstract syntax notation 1)과 DER(distinguished encoding rules)이다. ASN.1은 자료의 표현 규칙이고 DER은 자료를 Bit들의 열로 암호화하는 규칙이다[6].
또한, 위에서 언급한 주문, 지불처리 기술들을 통합, 적용해 전자거래 규약으로 정리한 것들이 SET(secure electronic transaction), OFX(open financial exchange), OTP(open trading protocol) 등이 있다[2].

2.2.2 기본적인 암호기술 연구

(1) 대칭키 암호방식(symmetric key)

평문(plaintext)을 암호화하는 암호키와 암호화된 평문을 복호(decryption)하는 복호키가 같은 암호화 방식을 비밀키 암호화 방식 또는 대칭키 암호화 방식이라고 한다. 장점은 뒤에 설명할 비대칭키(asymmetric key) 암호화 방식에 비해 암호/복호하는데 소요되는 시간이 빠르나 키가 이전에 미리 분배되어 있어야 하고 분배된 키에 대한 안전성을 확보하는데 어려움이 있다[3][4][5].

(2) 비대칭키 암호방식(asymmetric key)

비밀키 암호화 방식과 달리 암호화하는 키와 복호화하는 키가 다른 경우 이를 비대칭형 암호화 방식이라고 한다. 즉 암호화나 복호화할때 서로 다른 키를 사용하고 이 두 키의 유추는 불가능하다. 공개키는 다른 사람이 알 수 있도록 하고 개인키(private

Key)는 공개하지 않는다[3][4][5].

(3) 단방향 해쉬함수(One way hash function)

임의의 길이의 메시지에 적용하여 일정한 길이의 코드(Code)값 (단, 다른 메시지마다 상이한 값)을 만들고, 결과 코드값으로 원래의 메시지를 확인할 수 없는 일방향 함수(또는 메시지 다이제스트 함수)를 말하며 전 참가기관이 동일한 함수를 사용한다. 대표적으로 MD5(message digest 5), SHA-1(secure hash algorithm 1)을 많이 쓴다[3][4][5].

2.3 SET 프로토콜

2.3.1 SET 프로토콜의 개요

인터넷 기반의 전자 거래에서 신용카드 이용률이 증가하자 신용카드사들은 신용카드를 전자 거래에서 보다 안전하게 이용할 수 있는 방안을 모색하게 되었다.
이에 마스터 카드사와 비자 인터네셔날의 주도로 정보산업계의 주요 기업들인 Microsoft, IBM, 등의 기술적인 자문 파트너들과의 협력에 의해 SET이 제정되었고, 지속적으로 관리되어 나가고 있다[1][5].

현재 SET은 SETCo라는 기구에 의해 관리되고 있으며, SET 관련 제품들은 SETCo에서 규정한 Test를 통해 SET 표준 제품임을 인증 받는다.

SET은 인터넷과 같은 공개된 네트워크상에서의 신용카드 지불을 위한 프로토콜이라 할 수 있다. 즉, 인터넷 쇼핑 시 신용카드를 사용하여 대금을 결제하고자 할 때 공개된 네트워크 상에서 보다 안전하게 지불처리를 할 수 있도록 암호화 및 정보보안에 관해 제정된 표준안이다. 초기에 SET은 소프트웨어 구현에 국한하여 출발하였으나, 최근에는 SET을 칩 카드(chip-card)로 구현하려는 시도가 진행중이다. 즉, SET은 소프트웨어뿐 아니라 소프트웨어 구현에 대한 표준까지 포괄하고 있다.

SET은 네트워크상의 안전한 지불처리라는 기본적인 요구에서 비롯되었다. SET 표준안에서 정의한 주요 비즈니스 요구는 다음과 같다[5].

- 지불정보와 주문정보에 대한 기밀성(confidentia-lity)의 제공
- 전송된 데이터에 대한 무결성(integrity)의 보장
- 카드 소지자(cardholder)가 적법한 사용자임을 확인하는 인증(authentication)제공
- 공급자(merchant)에 대한 인증제공
- 최고의 시스템 설계 및 보안 수단 확보
- 전송암호화 방식에 종속되지 않는 프로토콜의 개발
- 소프트웨어 및 네트워크 공급자의 상호 운용성(interoperability) 제공

이러한 SET에 대한 요구사항을 반영하기 위해 SET은 다음과 같은 특징을 갖는다[5].

- 메시지의 기밀성 (confidentiality of information)
- 데이터의 무결성 (integrity of data)
- 카드 소지자 인증 (cardholder account authent-ication)
- 공급자 인증 (merchant authentication)
- 상호운용성 (interoperability)

이들에 대하여 아래에 좀더 구체적으로 고찰하여 두었다[5][6][7].

(1) 메시지의 기밀성

기밀성은 전송된 메시지가 의도되지 않은 다른 사람에게 노출되지 않는 것을 의미한다. SET은 기밀성를 보장하기 위해 DES, RSA등의 암호화 기법을 복합적으로 이용하여 메시지를 암호화한다.

(2) 데이터의 무결성

무결성은 전송되는 정보가 도중에 의도되지 않은 제3자에 의해 변경되지 않는 것을 의미한다. SET은 전자서명이라는 방식을 이용하여 정보의 무결성와 더불어 메시지의 작성자가 누구인지를 확인할 수 있게 한다.

(3) 카드 소지자 인증

공급자는 지불을 위해 제시된 카드가 카드 소지자가 적법하게 사용할 수 있는가를 확인해야 한다.

SET에서는 전자서명과 카드 소지자 인증서를 통해 카드 소지자의 카드 계정에 대한 승인을 수행할 수 있다.

(4) 공급자 인증

공급자와 마찬가지로 카드 소지자 또한 거래하는 공급자가 자신이 제시한 지불카드에 대해 정상적인 가맹점으로 등록되어 있는가를 확인할 수 있어야 한다. 또한 카드 소지자는 거래하고자 하는 공급자가 자신의 신용정보를 안전하게 처리할 수 잇는가를 확인할 수 있어야 한다.

이를 위해 SET은 역시 전자서명과 공급자 인증서에 의해 공급자에 대한 승인기능을 제공한다

(5) 상호운용성

SET은 산업표준으로 제정되었으므로, 다른 벤더(Vendor)가 생산한 제품이라 하더라도 상호 문제없이 수행되어야 한다. 이를 위해 SET은 specification protocol과 message format에 표준을 제공하고 있다.

2.3.2 SET에서 보안 문제를 해결하기 위한 기술

(1) 전자봉투(digital envelope)

송신자가 송신내용을 암호화하기 위하여 사용한 비밀키(secret key)를 수신자만 볼 수 있도록 수신자의 공개키(public key)로 암호화시킨 것을 전자봉투라 한다[5][6][7][8].

메시지 자체는 암호화 속도가 빠른 비밀키 암호화 방식으로 암호화하고 암호화에 사용된 비밀키를 공개키 암호화 방식을 이용하여 상대방에게 전달함으로써 공개키 암호화 방식의 장점인 보안성을 유지하면서 공개키 암호화 방식의 단점인 처리속도 지연문제를 해결할 수 있다[5][6][7][8].

(2) 전자서명(digital signature)

전자서명은 서명자 인증, 메시지의 위/변조방지, 송신부인방지 등의 기능을 제공하는 암호화 기술로써 공개키 암호화 방식에서의 개인키를 이용한 메시지 암호화는 서명 당사자밖에 할 수 없다는 점을 이용하여 구현한다[5][6][7][8].

전자서명에서 사용되는 암호기술은 다음과 같다.

메시지다이제스트(message digest)는 메시지에 단방향 해쉬함수를 적용한 결과값 160비트로 아무리 긴 메시지라도 일정한 길이로 압축이 된다. 메시지다이제스트를 사용하는 이유는 메시지 전체를 공개키방식으로 암호화하는 대신 메시지다이제스트를 암호화함으로써 처리시간을 단축하고 전송된 메시지의 무결성을 확인하기 위해서다.

RSA를 암호화 알고리즘으로 사용한다고 가정할 때 1Kbyte 메시지를 그대로 암호화 할 경우 소요시간은 약 8초, 메시지다이제스트를 암호화하는 경우는 약 0.16초가 소요된다[9]. 메시지다이제스트를 사용시에는 50배정도 속도가 빨라지는 것이다[9].

전자서명 처리절차는 송신자가 메시지의 메시지다이제스트를 생성하여 자신의 개인키를 이용하여 암호화시킴으로써 전자서명을 하여 송신메시지와 전자서명을 수신자에게 전송한다. 수신자는 수신한 전자서명을 송신자의 공개키를 이용하여 복호화함으로써 송신자가 생성한 메시지다이제스트를 추출하고 송신메시지에 동일한 해쉬함수를 적용하여 새로운 메시지다이제스트를 생성한다. 수신자는 수신 받은 메시지다이제스트와 자신이 생성한 메시지다이제스트를 비교하여 동일한 경우 정당한 송신자의 전자서명으로 판단한다[5][6][7][8].

(3) 이중서명 (dual signature)

SET에서는 카드 소지자의 결제정보가 공급자를 통하여 해당 PG로 전송됨에 따라 카드 소지자의 결제정보가 공급자에게 노출될 가능성과 공급자에 의한 결제정보의 위,변조의 가능성이 있으므로 공급자에게 결제정보를 노출시키지 않으면서도 공급자가 해당 카드 소지자의 정당성 및 구매내용의 정당성을 확인 할 수 있고 PG는 공급자가 전송한 결제요청이 실제 카드 소지자가 의뢰한 전문인지를 확인할 수 있도록 하는 이중서명 기술의 도입이 필요하게 되었다.

이중서명을 이용한 거래처리절차는 다음과 같다[5][6][7][8].

첫째, 카드 소지자의 주문정보와 지불정보에 대한 이중서명을 생성한다.

카드 소지자의 이중서명 생성절차는 주문정보(OI:order information)에 대해 해쉬함수를 적용하여 160 비트의 메시지 다이제스트 M1을 생성하고 결제정보(PI:payment information)에 대해 해쉬함수를 적용하여 160 비트의 메시지 다이제스트 M2를 생성한다.
생성된 두개의 메시지다이제스트 M1, M2를 연접(concatenation)한 후 연접 된 결과인 M1 · M2에 해쉬함수를 적용하여 메시지 다이제스트 M을 생성한다. M에 카드 소지자의 개인키로 전자서명한 것이 이중서명이다.

둘째, PG에게 전해질 전자봉투 생성 및 필요 데이터를 공급자로 전송한다.
PG에게 전해질 전자봉투 생성 및 필요 데이터를 공급자로 전송하는 절차는 비밀키를 랜덤생성하여 결제정보(PI)를 암호화시킨 후 해당키를 PG의 공개키로 암호화하여 전자봉투 생성한다. 주문정보, 암호화된 결제정보, M1 · M2, 카드 소지자의 전자서명, 전자봉투를 공급자에게 전송한다.

셋째, 공급자는 주문정보와 이중서명 확인 후 암호화된 결제정보를 PG에게 전송한다.
공급자가 주문정보와 이중서명을 확인하는 절차는 수신된 주문정보에 카드 소지자와 동일한 해쉬함수를 적용하여 메시지다이제스트 M1을 생성한다. 그리고 수신된 M1 · M2 중 M1을 새로 생성한 M1으로 대체시킨 후, 대체된 M1 · M2에 동일한 해쉬함수를 적용하여 메시지다이제스트 M을 구하고 수신된 이중서명을 카드 소지자의 공개키로 복호화하여 추출한 메시지다이제스트 M과 비교하여 동일한 경우 정당한 구매 요청으로 간주하여 처리한다.
주문정보의 무결성과 정당성을 확인한 후, 공급자는 카드 소지자로부터 전송받은 암호화된 결제정보, 전자봉투, 이중서명, M1 · M2를 자신의 승인요청전문 전송시 PG로 전송한다.
넷째, PG는 전자봉투 및 결제정보 복호화한다.
PG의 전자봉투 및 결제정보 복호화 절차는 PG는 자신의 개인키를 사용하여 전자봉투를 복호화하여 획득한 비밀키를 이용하여 결제정보, M1 · M2값, 카드 소지자의 서명값을 추출한다.

PG는 복호화된 결제정보에 카드 소지자와 동일한 해쉬함수를 적용하여 메시지 다이제스트 M2를 생성한다. 수신된 M1 · M2 중 M2을 새로 생성한 M2으로 대체시킨후 대체된 M1 · M2에 동일한 해쉬함수를 적용하여 새로운 메시지다이제스트 M을 구한다. 수신된 카드 소지자의 이중서명을 카드 소지자의 공개키로 복호화하여 메시지 다이제스트 M을 추출하여 새로운 메시지다이제스트를 비교하여 동일한 경우 정당한 결제요청으로 간주하여 처리한다.

3. 실험 및 결과 분석

3.1 CM-Wallet의 구성과 개발내용

3.1.1 개발시스템 환경

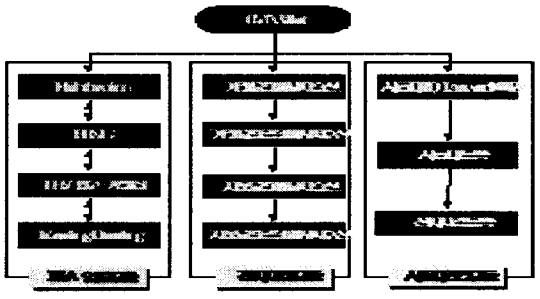
프로그램언어는 Visual C++를 사용하여 GUI환경의 프로그램을 개발하였으며 Client의 운용환경은 Windo-ws 95, 98, NT 4.0 이상이며 통신프로토콜은 TCP/IP를 사용한다.

3.1.2 기술개발내용

(1) 난수, 대칭키/비대칭키 생성을 하여 암호알고리즘을 구현하였다.
(2) RSA 1024 bit, Triple DES 168bit를 이용한 전자봉투, 전자서명, 이중전자서명을 위한 메시지를 개발하였다.

3.1.3 CM-Wallet의 모듈별 개발 내용

CM-Wallet은 [그림 2]와 같이 모듈별로 구성되어져 있다.



[그림 2] CM-Wallet의 구성도

RSA 암호모듈은 메시지 보안을 위한 암호키 생성과 메시지 다이제스트, 전자서명, 이중서명을 생성한다.

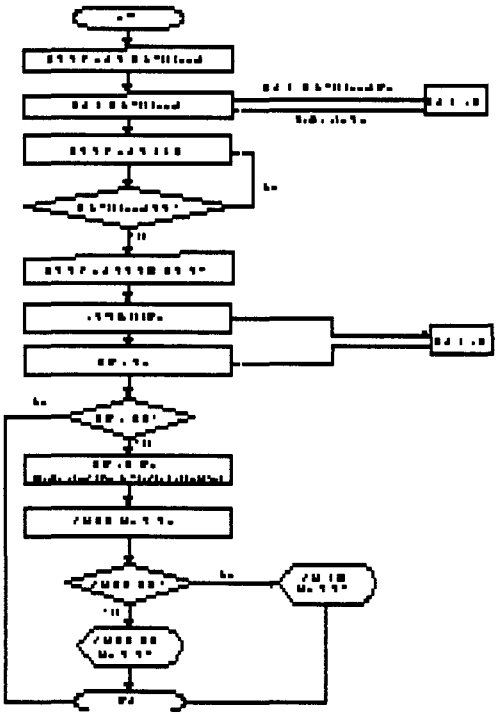
전자지갑모듈은 프로토콜에 따라 서버와의 통신 메커니즘을 구현하며 이는 실제 웹을 통하기 위한 TCP/IP 프로토콜과 HTTP 프로토콜 그리고, SET 프로토콜로 이행된다.

사용자관리모듈은 전자지갑 사용자 등록과 전자지갑 등록을 하고 이를 다시 데이터베이스에 저장 관리하는 기능을 가진다.

특히 RSA 암호모듈은 따로 다른 프로그램에 적용시킬 수 있어 프로그램의 재활용성이 높다.

3.1.4 CM-Wallet의 전체 세부 흐름도

다음 [그림 3]은 CM-Wallet의 사용자 로그인에서 전자 지불 후 거래 완료까지의 전체 세부 흐름도이다.



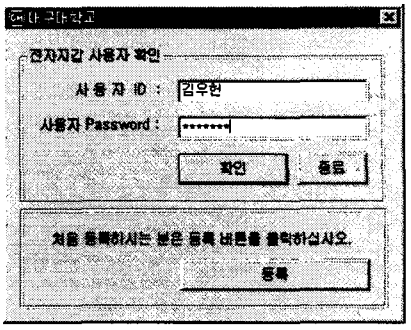
[그림 3] CM-Wallet 전체 세부 흐름도

3.2 CM-Wallet의 개발결과 및 분석

CM-Wallet은 암호생성, 이중서명 생성, 판매자의 인증서 확인 등의 복잡한 절차는 내부적으로 처리하여 화면으로 나타나는 절차를 간소화하였다. 이는 기존의 전자지갑의 절차가 복잡하여 사용자가 불편한 문제를 해결하였다.

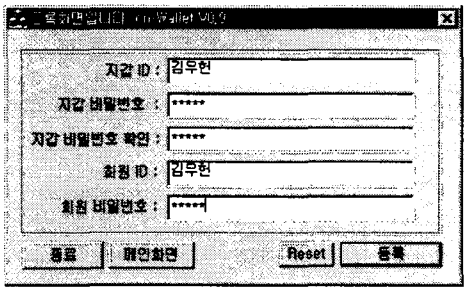
다음은 화면으로 보여지는 CM-Wallet의 개발결과에 대한 설명이다.

[그림 4]는 사용자가 웹브라우저에서 구매버튼을 클릭하여 전자지갑을 다운받아 등록 후, 로그인 하기 위한 CM-Wallet 초기 화면이다.



[그림 4] CM-Wallet 초기화면

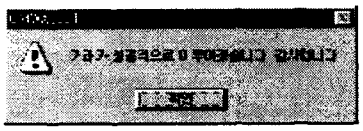
다음 [그림 5]는 사용자 로그인후, CM-Wallet은 쇼핑몰 서버에서 수신한 주문정보와 판매자인증서를 확인 후, 결제정보를 확인하게 된다. 이때 결제과정 계속 버튼을 선택하게 되면, 내부적으로 구매정보와 결제정보에 대한 이중서명값을 생성하여 쇼핑몰서버로 지불요청메시지를 송신하게 된다.



[그림 5] 결제정보 확인 화면

지불요청메시지 송신 후, 잠시 후에 쇼핑몰 서버에서 지불확인 메시지를 수신하여 [그림 6]과 같이 거

래성공메시지를 출력을 하게 되면 전자지불을 안전하게 종료한다.



[그림 6] 거래 성공 상태 표시 화면

3.2.1 소프트웨어 품질적인 측면의 분석

(1) 사용의 편리성
클라이언트 프로그램을 GUI환경으로 프로그램을 개발하여 사용자가 손쉽게 사용하도록 개발하였다.

(2) 유연성
OMT기법을 이용하여 모듈별로 설계하여 수정과 재사용이 용이하도록 개발하였다.

(3) 효율성
클라이언트 프로그램을 사용자중심으로 간편하게 화면 설계하여 복잡한 과정은 프로그램 내부적으로 처리하도록 하였으며, 암호모듈의 성능을 최대화하였다.

(4) 보안성
사용자의 아이디와 패스워드를 입력하여 인증 받은 사용자만이 지불프로그램을 사용하였으며, 개인키 저장시 바이러리(binary)형태로 저장하여 인증받지 않은 사용자가 알아볼 수 없도록 하였다.

3.2.2 경제적인 측면의 분석

(1) 저가형 지불 솔루션제공
국내 기술에 의한 전자지불 시스템 개발은 전체적으로 시스템 개발비를 경감시키며 저가형 지불 솔루션을 제공할 수 있는 결과를 가져올 수 있다.

(2) 수입대체효과
이 연구를 바탕으로 국내 자체 전자지불 시스템을 상품화하게 되면 점차적인 수입대체 효과를 기대할 수 있다.

5. 결 론

본 연구에서는 SET프로토콜에 따라 전자지갑을 설계, 개발하기 위하여 암호기술, 메시지구현기술에 관련된 기반 연구를 바탕으로 CM-Wallet을 설계, 개발하였다.

CM-Wallet은 RSA 1024bit, Triple DES 168bit 키를 생성하여 전자서명, 이중서명을 생성하여 메시지 보안도가 SET 기준을 만족한다. 그리고, 복잡한 절차는 내부적으로 처리하여 구매자가 사용하기 쉽게 화면으로 보여지는 절차를 간소화하여 전자지갑을 사용할 때 복잡한 절차의 불편함을 해소하였다.

본 연구에서는 CM-Wallet을 중심으로 전자지갑에 관련된 프로토콜만 설계 개발하였으나 국내실정에 맞는 SET을 응용한 사용자, 공급자, 금융기관간의 SET 기반 전자지불 시스템 개발로 이어지도록 하여야 할 것이다.

참고문헌

[1] 한국정보보호센터. 대학원생 정보보호 기술 교육. 한국정보보호센터. (1999).
[2] 최인영. 전자상거래의 혁명. 동일출판사. (1998).
[3] Alfred J. Menezes, Paul C. Handbook of cryptography. CRC Press.
[4] 김철. 암호학의 이해. 영풍문고. (1996).
[5] RSA사. RSA Laboratory FAQ 4. rsa.com. (1999).
[6] Secure electronic transaction specification Book 1: Buisiness guide. setco.org.(1997).
[7] Secure electronic transaction specification Book 2: Programmer's guide. setco.org. (1997).
[8] Secure electronic transaction specification Book 3: Formal Protocol Definition Version 1.0. setco.org. (1997).
[9] 금융결제원. 전자상거래 보안 프로토콜 SET 조사연구 보고서. 금융결제원. (1997).