情報保護學會論文誌
第12券 第3號, 2002. 6

CEPS 인터넷 서비스를 위한 IC카드 기반의 보안 시스템 구축

이 종 후*, 라 은 주**, 백 상 수*, 지 석 진**, 이 용**, 류 재 철*

IC Card Security System for CEPS in Internet

Jong-hu Lee*, Eun-ju Ra**, Sang-su Baek*, Seok-jin Jee**,
Yong Lee**, Jae-cheol Ryou*

요 약

최근 높은 보안성과 휴대성을 지니고 있는 IC카드를 이용해 전자지갑을 구현하고, 여기에 기존의 현금과 동일한 가치를 지니는 전자화폐를 저장하여 전자거래에 즉시 이용할 수 있도록 한 IC카드 기반 전자화폐 시스템이 주목 받고 있다. 이러한 전자화폐 시스템은 금액정보를 비롯한 모든 거래정보가 디지털 형태로 저장되고 네트워크를 통해 전송되는데, 디지털 정보는 특성상 제3자에 의해서 위조되거나 변조될 위험이 매우 높다. 따라서 전자화폐 시스템에서는 안전성과 신뢰성이 매우 중요한 요소이며, 특히 인터넷에서 전자화폐를 이용할 경우에는 보다 높은 강도의 안전성이 요구된다.

CEPS 전자화폐 시스템은 비자사에서 제안한 IC카드 기반의 전자화폐 시스템이며, EMV 표준을 수용하여 EMV 보안구조를 따르고 있다. 그러나 EMV 보안구조는 인터넷 환경을 고려하여 설계되지 않았기 때문에 인터넷에서 사용하기에 적합하지 않다. 이에 본 논문에서는 EMV 보안구조를 분석하고 보완하여 인터넷에서 사용할 수 있는 CEPS 전자화폐 시스템을 설계 및 구현하였다.

ABSTRACT

As the world-wide use of the Internet increases rapidly due to development of computer network, the Electronic Commerce for business by treating it is growing as compared to the traditional one for the information exchange in the academic and research areas. The Electronic Payment System used for EC includes the Payment Broker System and the Electronic Purse System. And usually Electronic Purse System operates with IC cards. Saving the money in IC card has a high portability and security. Therefore, the Electronic purse System based on IC card is recently issued in the EC.

In this paper, we design and implement of a IC card security system for Common Electronic Purse Specifications in Internet. CEPS is a Electronic Purse System proposed VISA, and conform EMV(Europay Mastercard VISA) security structure. With our system, users easily use Electronic Purse System with only Web browser and IC card. Original EMV paid no regard to using in the Internet. But our system, conforming to CEPS and EMV, is easily used in the Internet.

Keyword : *CEPS, IC card, EMV, Electronic Purse System*

* 충남대학교 정보통신공학부
** 한국정보보호진흥원

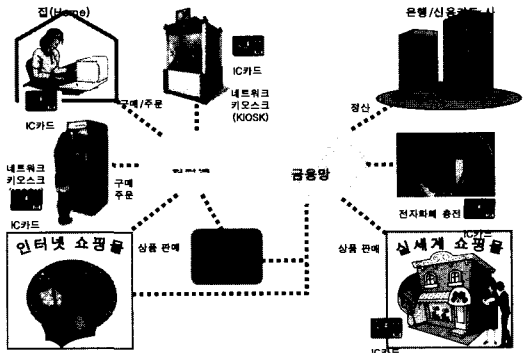
Ⅰ. 서 론

최근 몇 년동안 국내외 전자상거래 시장이 급속하게 성장하면서 전자상거래의 필수 요소인 전자지불 시스템에 대한 연구 또한 활발하게 진행되고 있다. 이러한 전자지불 시스템은 크게 지불 브로커 시스템과 전자화폐 시스템으로 구분할 수 있다.[11]

지불 브로커 시스템은 사용자가 신용카드를 이용해 인터넷 상에서 거래에 대한 지불을 수행할 수 있도록 개발된 것이다. 신용카드를 이용한 거래가 일반화되어 있는 현재 가장 널리 이용되고 있는 시스템으로 사용자와 인터넷 쇼핑몰이 서로를 신뢰 할 수 없는 상황에서 지불브로커가 사용자와 쇼핑몰 사이에서 신용카드 결제에 대한 중개인 역할을 함으로써 신용카드를 안전하게 이용할 수 있도록 하는 구조로 되어 있다. 그러나 이 시스템은 신용카드를 소지하고 있는 고객만 이용할 수 있다는 제약이 따르며, 신용카드 이용에 따른 수수료 지불과 같은 제반 환경상 고액의 거래에 적합한 특성을 지니고 있다.[11]

이와 달리 전자화폐 시스템은 기존의 현금과 동일한 가치를 지니는 디지털 정보 형태의 전자화폐를 사용자에게 발행해주는, 선불카드/직불카드를 한 단계 발전시킨 시스템이다. 이러한 전자화폐는 기존의 현금과 동일한 가치를 지니며, 신용카드와 달리 남녀노소 구분 없이 누구나 쉽고 편리하게 사용할 수 있다는 장점을 지닌다. [그림 1]에서 보는 바와 같이 사용자는 은행 또는 신용카드사로부터 전자지갑을 발급 받은 후, 자신의 은행계좌의 금액을 전자화폐로 발행 받아 실세계의 쇼핑몰에서 물건을 사고 결제 수단으로 이용할 수 있다.

최근 전자화폐 시스템은 높은 보안성과 휴대성을 지니고 있는 IC카드를 이용해 전자지갑을 구현하고, 여기에 기존의 현금과 동일한 가치를 지니는 전자화폐를 저장하여 전자거래에 즉시 이용할 수 있도록 한 IC카드 기반의 전자화폐 시스템이 주목 받고 있다.



[그림 1] 전자화폐 이용 환경

IC카드는 높은 보안성을 지니고 있음에도 불구하고 초기에 높은 개발비용이 소요되고, 다양한 어플리케이션을 제공하기 어려워 제한적으로 사용되어 왔다. 그러나 최근 IC카드 기술의 발전과 함께 IC카드와 단말기 가격이 하락하고, 자바 기술 등을 접목하면서 다양한 어플리케이션을 수용할 수 있게 되면서 전자화폐 시스템은 IC카드 기반으로 개발하는 것이 일반적이다.

이런 IC카드 기반의 전자화폐 시스템 가운데 최근에 주목받고 있는 CEPS(Common Electronic Purse Specifications) 전자화폐는 비자사에서 EMV (Europay Mastercard Visa) 표준을 수용하여 제안한 전자화폐 시스템이다. 이 전자화폐 시스템은 [그림 1]과 같이 금융망을 중심으로 하여 화폐를 충전하고 구매할 수 있도록 설계되었다. 즉, EMV 보안구조는 인터넷을 고려하지 않았기 때문에 인터넷을 통하여 화폐를 충전하거나 쇼핑몰에 접속하여 물건을 구매할 수는 없는 구조이다.

이에 본 논문에서는 ISO/IEC 7816 IC카드 및 단말기 표준을 기반으로 한 지불 시스템 표준인 EMV와 EMV 표준을 수용한 CEPS 전자화폐 시스템을 분석하고, 이를 인터넷에서 사용할 수 있도록 설계 및 구현하였다. 2장에서는 본 논문에서 구현한 전자화폐 시스템에서 사용된 관련 기술들에 대해서 살펴보고, 3장에서 CEPS의 동작방식과 보안 메커니즘을 분석한다. 4장에서는 인터넷 서비스가 가능한 CEPS 전자화폐 시스템의 설계 내용에 대해서 설명하고, 5장에서 구현 내용에 대해서 살펴본다. 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 관련 기술

본 장에서는 인터넷에서 사용이 가능한 CEPS 전자화폐 시스템을 구축하기 위해 사용되는 기술들에 대해서 살펴본다.

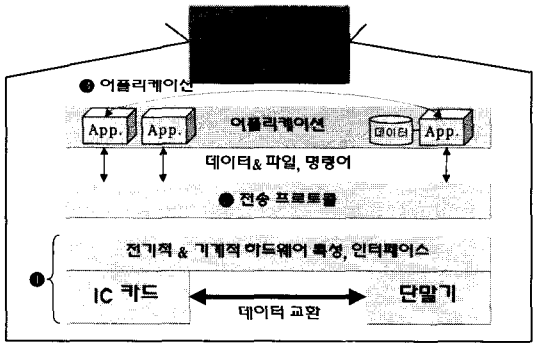
2.1 CEPS

CEPS(Common Electronic Purse Specification)는 비자카드사의 "VISA cash"를 발전시켜 제안된 전자화폐 국제 표준 규격으로 1998년 12월에 버전

6.0이 발표되었다. CEPS 전자화폐는 EMV 표준을 수용하여 IC카드와 단말기에 대한 상호호환성을 확보하고 있다. 또한 자바기술의 도입을 통해 다양한 IC카드를 수용하였으며, 어플리케이션을 애플릿 형태로 구현하여 동적으로 어플리케이션을 탑재할 수 있도록 함으로서 다양한 응용 서비스에 활용할 수 있도록 하고 있다.[1,2,3] CEPS에 대해서는 3장에서 보다 자세하게 살펴본다.

2.2 EMV

EMV(Europay, Mastercard, VISA) 표준은 1996년 유로페이, 마스터카드, 비자카드가 공동으로 제안한 IC카드를 기반으로 한 전자지불 시스템으로, IC카드와 단말기에 대한 국제 표준 규격인 ISO/IEC 7816을 기반으로 하고 있다.



〔그림 2〕 EMV 표준

EMV 표준은 〔그림 2〕와 같이 크게 IC카드 및 단말기 규격, IC카드와 단말기 사이의 통신 프로토콜, 어플리케이션 규격, 보안 등을 정의하고 있다. 따라서 지불시스템 개발에 사용되는 IC카드와 단말기는 상호호환성을 지님으로서 서로 다른 지불시스템일지라도 IC카드와 단말기를 공유하는 것이 가능해진다. 이러한 EMV 표준 IC카드는 기존의 신용카드와 유사한 기능을 가지면서 전자지갑을 안전하게 구현하는데 필요한 보안기술, 즉 공개키 암호기술을 사용한 IC카드 인증기법(SDA : Static Data Authentication, DDA : Dynamic Data Authentication), 데이터 암호화 메커니즘 등을 정의하고 있다.[4,5,6]

2.3 IC카드 기술

IC카드는 IC(Integrated Circuit)가 내장된 신용카드 크기의 플라스틱 카드이다. IC카드는 기존의 직불카드나 전화카드와 같은 마그네틱 카드에 비해 발전된 구조를 갖고 있다. IC카드는 칩 카드(Chip Card)처럼 마이크로 프로세서 없이 메모리만 있는 것이 아니라, 다양한 기능을 제공하는 작은 컴퓨터라고 할 수 있다. 즉, IC카드는 EEPROM, ROM, RAM, CPU 등으로 구성된다. 특히 기존의 칩 카드와 달리 내용을 변경할 수 있는 EEPROM을 가지고 있어 미리 프로그램된 명령어를 다시 바꿀 수 있는 유연성을 가진다. 또한 자체 운영 시스템을 사용한다.

이와 같은 IC카드는 크게 접촉형과 비접촉형으로 구분할 수 있다. 접촉형 카드는 마이크로 프로세서가 있는 카드와 없는 카드로 구분되며, 비접촉형 카드는 단순히 일련번호를 읽어오는 RF-ID 카드와 데이터를 읽고 쓰는 등 기본적인 연산기능을 갖고 있는 RF-IC 카드로 나눌 수 있다. 또한 접촉형과 비접촉형 카드 기능 함께 수행할 수 있는 하이브리드 카드와 콤비카드가 있다.[17]

IC 카드의 응용 분야로는 가장 많이 사용되고 있는 분야인 금융분야를 비롯해서 의료, 신분증, 통신, 로열티 등이 있으며, 미국 농무성에서 농부들의 땅콩 수확량 쿼터제에 사용하는 것과 같이 특수한 분야에서도 많이 이용되고 있다.

2.4 SSL

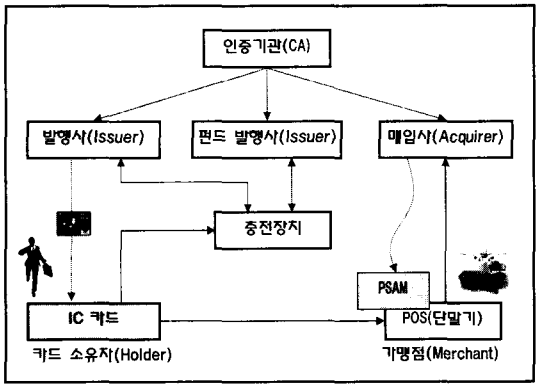
SSL(Secure Socket Layer)는 넷스케입사에서 처음으로 제안된, 웹 보안 메커니즘이다. SSL은 크게 2부분으로 구분할 수 있는데, 하나는 SSL 동작에 필요한 세션을 생성하기 위해 사용되는 Handshake Protocol, Change Cipher Spec Protocol, Alert Protocol 부분이며, 다른 한 부분은 메시지 암호화 등 실질적인 보안 서비스를 제공하는 Record Protocol 부분이다. 즉, 클라이언트와 서버는 Handshake Protocol을 통해 한 세션 동안 보안 서비스 제공에 사용되는 암호 알고리즘, 암호키, 인증서 등과 같은 암호 매개변수를 공유하며, Record Prtocol에서는 이러한 암호 매개변수를 통해 보안통신을 수행한다. SSL에 의해서 제공되는 보안 서비스는 다음과 같다.[7]

- 기밀성 : DES, RC4 등과 같은 관용 암호기술을 사용하며 제공되며, 이때 사용되는 암호키는 Handshake 과정에서 결정된다.

- 클라이언트와 서버 인증: Handshake 과정에서 RSA, DSS 등과 같은 서명 알고리즘과 X.509 인증서를 이용한 사용자 인증이 이루어진다.
- 메시지 무결성: 내부적으로 누군가 데이터 전송을 방해할 수 없도록 하거나, 재전송 공격에 이용할 수 없도록 메시지에 대한 무결성을 제공한다.

Ⅲ. CEPS 분석

3.1 CEPS의 구성요소



〔그림 3〕 CEPS 구성요소

〔그림 3〕과 같이 인증기관, 발행사, 펀드 발행사, 매입사, IC카드, 충전장치, POS(Point of Sale) 단말기 등으로 구성되는 CEPS 전자화폐 시스템의 각 구성요소의 역할을 살펴보면 다음과 같다.

■ 발행사(Issuer) 및 펀드 발행사

발행사는 사용자의 계좌를 유지하는 등의 거래 관계를 통해 사용자에게 IC카드 전자지갑을 발급하고 전자화폐를 발행하는 금융기관이다. 그리고 펀드 발행사는 전자화폐 발행에 사용할 수 있는 사용자의 계좌를 보유한 금융기관으로 발행사는 펀드 발행사의 사용자 계좌를 이용해 전자화폐를 발행할 수 있다.

■ 매입사(Acquirer)

사용자가 전자화폐를 이용해 물건을 구매할 경우, 해당 가맹점 및 인터넷 쇼핑몰의 판매대금을 지급하는 금융기관이다. 가맹점과 발행사 사이에서 정산하는 역할을 한다.

■ IC카드 소유자

발행사에 계좌를 유지하는 등의 금융 관계를 통해 전자지갑을 발급 받고, 전자화폐를 발행 받아 이를 사용하는 사용자이다.

■ IC카드(전자지갑)

충전장치를 이용해 전자화폐를 발행 받아 이를 저장하고, 대금 결제에 이용할 수 있도록 하는 장치이다. IC카드에 전자화폐 어플리케이션이 탑재된다.

■ 충전장치(Load Device)

전자지갑 발행사와 연결되어 있는 ATM과 같은 장치로, 사용자가 전자화폐를 발행 받거나 환전하는데 사용된다.

■ 가맹점

기존의 가맹점 및 인터넷 쇼핑몰로, POS 단말기를 이용해 전자화폐 결제 수단으로 제공하여 상품을 판매하는 주체이다

■ POS 단말기

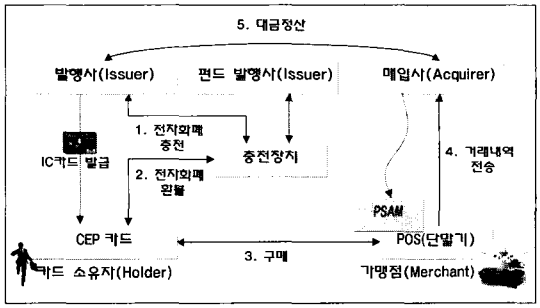
IC카드 전자지갑에 저장된 전자화폐를 이용해 대금 결제를 처리하는 장치이며, 가맹점에서 관리한다.

■ 인증기관(CA)

발행사, 매입자, PSAM, IC카드 등에서 사용되는 인증서를 발행하는 기관으로 전자화폐 시스템에서 사용되는 공개키의 신뢰성을 보장한다.

3.2 전자화폐 이용 시나리오

전자화폐 이용에 관한 시나리오는 그림 4와 같다.



〔그림 4〕 전자화폐 이용 시나리오

① 전자화폐 충전 : 전자지갑 소유자는 충전장치를 이용해 발행사 또는 펀드 발행사로부터 전자화폐를 발행 받는다. 이 때, 사용자 인증을 위해 PIN

(Personal Identification Number)을 입력하는 단계와 IC카드 인증을 거친다. PIN이 올바르게 입력되면 전자화폐 발행이 허용된다. 이때 사용자가 입력한 금액만큼 발행사는 전자화폐를 발행해주는데, 이 전자화폐가 전자지갑에 저장된다.

② 전자화폐 환불 : 필요에 따라 전자지갑에 저장된 전자화폐에 대한 가치 환불이 가능하다. 즉, IC카드에 저장된 전자화폐를 은행계좌로 입금하거나, 현금으로 찾는 것이 가능하다.

③ 구매: 전자지갑 사용자는 전자화폐를 이용해 일반 가맹점 또는 인터넷 쇼핑몰에서 상품을 구매한다. 상품 구매에 대한 대금 결제는 전자지갑에 충전된 전자화폐를 사용한다. 이 때, POS 단말기에 전자화폐 거래내역에 대한 모든 트랜잭션이 저장된다.

④ 거래내역 전송 : POS 단말기에 저장된 전자화폐에 대한 모든 거래내역을 일괄적으로 매입사에 전송하여 정산을 요청한다.

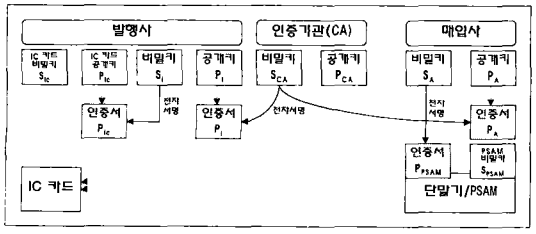
⑤ 대금 정산 : 발행사와 매입사는 전자화폐 거래내역 트랜잭션을 이용해 정산 처리를 한다.

3.3 CEPS 보안 메커니즘

CEPS의 보안 메커니즘은 크게 사용자 인증, IC카드 인증, 트랜잭션 무결성 및 기밀성 보장으로 구분할 수 있으며, 대부분 EMV 표준을 따르고 있다. 이에 대해서 살펴보면 다음과 같다.

3.3.1 공개키 인증서 발행 및 키 관리

[그림 5]는 CEPS 인증체계에서 공개키 인증서 생성 및 분배가 이루어지는 과정을 보여준다. 이는 EMV 표준을 그대로 따르는 것으로, 인증기관은 자신의 공개키쌍을 생성하여 안전하게 보관하고, 발행사와 매입사의 공개키 인증서를 발행한다. 이 때, 발행사와 매입사는 자신의 인증서와 인증기관의 공개키를 IC카드와 단말기/PSAM에 안전하게 배포할 책임이 있다.

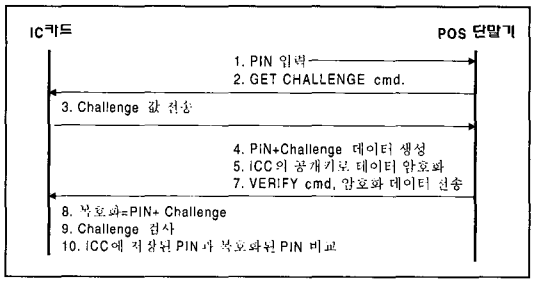


[그림 5] CEPS 인증구조

발행사는 IC카드의 비밀키와 공개키를 생성하고, IC카드의 공개키에 대한 인증서를 발행하여 IC카드에 저장한다. 또한 매입사는 PSAM의 공개키와 비밀키를 생성하여 PSAM 공개키 인증서를 발행한 후, 단말기/PSAM에 저장하는 역할을 담당한다. 이 과정에서 IC카드에는 카드 인증서, 카드 비밀키, 발행사 인증서, 인증기관 공개키, 카드와 발행사가 공유하는 MAC 키가 저장되며, 단말기/PSAM에는 PSAM 인증서, PSAM 개인키, 매입사 인증서, 인증기관 공개키, PSAM과 매입사가 공유하는 MAC 키가 저장된다.

3.3.2 사용자 인증

IC카드 소유자의 인증을 위해 보통 PIN을 사용한다. 이러한 사용자 인증은 발행사와 온라인으로 연결된 상태에서 발행사로부터 PIN을 확인하는 방식과 오프라인으로 POS 단말기와 암호통신을 통해 IC카드에 저장된 PIN을 확인하는 방식이 있다. 여기서는 보다 복잡한 절차를 거치는 오프라인 암호화 방식에 대해서 살펴본다. 오프라인 암호화 방식은 [그림 6]과 같이 이루어진다.



[그림 6] IC카드 사용자 인증 절차

먼저 사용자는 POS 단말기에 카드를 삽입한 후, PIN을 입력한다. PIN은 보통 4~8자리의 숫자가 사용된다. POS 단말기가 "GET CHALLENGE" 명령을 보내면 카드는 "Challenge" 값을 생성하여 전송한다. POS 단말기는 사용자가 입력한 PIN 값과 "Challenge"값을 IC카드의 공개키로 암호화한 후, "VERIFY" 명령어와 함께 IC카드에 전송한다. IC카드는 암호화되어 전송된 인증 데이터를 복호화하고, 여기에 포함된 "Challenge"를 IC카드에 저장된 값과 비교한다. 비교한 값이 동일하면 카드 사용자 인증이 완료된다. "Challenge" 값을 사용함으로서

매번 암호화된 사용자 인증정보는 바뀌게 된다.

3.3.3 IC카드/단말기 상호인증

IC카드 인증은 발행사가 발급한 카드가 유효한 것인지 확인하는 절차로, CEPS에서 충전 및 환전 거래를 할 경우 카드와 발행사는 상호인증을 해야 한다. 이 때, 상호인증은 MAC을 이용해 온라인으로 처리한다. 즉, 카드와 발행사가 공유하는 MAC 키를 이용해 인증정보를 생성하여 서로를 인증하는 것이다. 제3자 뿐만 아니라, 카드 소유자도 IC카드에 저장된 MAC 키를 알 수 없기 때문에 불법적으로 인증정보를 생성하는 것은 불가능하다.

또한 구매시 IC카드와 단말기/PSAM은 오프라인 상호인증을 제공해야 하며, 이 때, CEPS는 반드시 EMV 보안구조에 정의된 동적 데이터 인증 기법(DDA : Dynamic Data Authentication)을 사용하도록 하고 있다. 동적 데이터 인증은 IC카드의 비밀키로 전자서명 하는 인증정보를 매번 새롭게 생성하여 단말기에 전송하는데, 단말기는 발행사의 공개키 인증서와 IC카드의 공개키 유효성을 확인한 후, IC카드가 전자서명한 인증정보를 확인하여 IC카드를 인증하는 기법을 말한다. 단말기의 인증 또한 전자서명 기법을 이용하는데, IC카드는 PSAM의 공개키 유효성 조사와 PSAM이 전자서명한 값을 확인하는 절차를 거친다. 이 단계에서 IC카드와 단말기 사이의 상호인증이 완료된다.

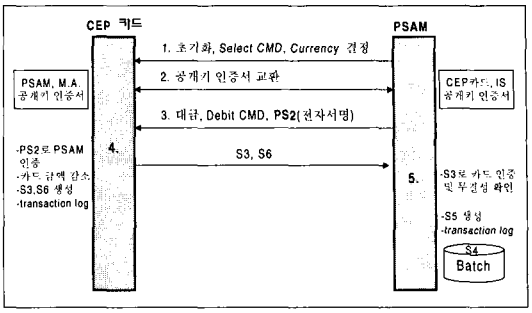
3.3.4 트랜잭션 무결성 및 기밀성

CEPS에서는 트랜잭션의 무결성을 보장하기 위해 MAC을 사용한다. 또한 거래 트랜잭션 수행시 필요한 세션키, 거래 금액 등과 같이 중요한 정보에 대해 무결성과 함께 반드시 RSA와 같은 공개키 암호를 이용한 기밀성을 제공하도록 하고 있다.

3.4 구매 트랜잭션

상품 구매시에 이루어지는 IC카드와 PSAM 간의 트랜잭션 처리는 오프라인 형태로 동작하며, 이는 [그림 7]과 같은 절차를 통해서 이루어진다.

① 구매의 시작은 IC카드를 POS 단말기에 넣은 후 통화를 결정하는 것으로 시작한다.
② 서로의 공개키를 교환한 후, IC카드 인증을 위해 동적 데이터 인증 기법을 사용한다.



[그림 7] 구매 트랜잭션

③ PSAM은 결제금액, 세션키를 포함한 정보에 대해 자신의 개인키를 이용해 전자서명을 수행한 후, 다시 IC 카드의 공개키로 암호화 한 PS_2 값을 IC카드에 전송한다. PS_2 값은 IC카드의 공개키로 암호화되어 기밀성을 제공한다. 또한 PSAM이 전자서명 했기 때문에 IC카드는 PSAM을 인증할 수 있게 된다([표 1], [표 2] 참조).
④ IC카드는 결제금액만큼 전자화폐를 감액한 후, S_3와 S_6을 생성하여 POS 단말기에 전송한다. S_3 MAC 값은 PS_2에 포함된 세션키를 사용해 POS 단말기가 IC카드 트랜잭션을 인증하기 위해 사용되고, S_6 MAC 값은 발행사가 IC카드를 인증하는데 사용된다. 이 때, S_6은 정산 단계에서 전자화폐 발행자가 거래에 대한 무결성을 확인하기 위해 사용되는 정보($MACMACKey_{CEP\_ISS}$ [RES_DATA], $MACKey_{CEP_ISS}$는 카드와 발행자만이 알고있는 암호키)이며, 제3자가 위조하는 것은 불가능하다. 또한 S_3는 카드와 PSAM 사이의 대금 결제 트랜잭션이 위조되거나 변조되지

[표 1] PS2

필드	내용	길이 (바이트)
CLA	90	1
INS	54	1
P1	00	1
P2	00	1
ID_{ACQ}	Acquirer ID	1
NT_{PSAM}	PSAM 트랜잭션 번호	4
PS_2	PSAM에 의한 전자서명 $ECEP\_PK[PSAM\_SK[PI]]$ (CEP_PK : 카드 공개키, PSAM_SK : PSAM 개인키)	$LPKM_{CEP}$
Le	00	1

〔표 2〕 PI 데이터 구조

필드	내용	길이 (바이트)
Header	6A	1
Format code	89	1
ALGH	해쉬 알고리즘 코드 (SHA-1: 901)	1
LEngth	데이터 길이	1
M_{PDA}	결제금액	4
$SESSKEY_{PSAM}$	PSAM이 생성한 세션키	16
Pad Pattern	BB	PKM_{PSAM}-45
Hash Result	서명할 데이터의 해쉬값	20
Trailer	BC	1

않았음을 보장하고 서로 결제금액을 동의했음을 의미하는 정보(MACSESSKey$_{PSAM}$〔RES_DAT A〕, SESSKey$_{PSAM}$는 PSAM이 생성하여 암호환 후, 카드에 전송한 키) 이다.

⑤ PSAM은 IC카드와 트랜잭션을 종료한 후 S_5를 생성하여 거래내역과 함께 배치파일에 추가한다. S_5는 PSAM과 매입사가 공유하는 MAC 키를 사용해 트랜잭션 각각에 대해 생성되며, 매입사가 배치 트랜잭션을 검사하는데 사용된다. S_5, S_4는 배치 파일 전체에 대한 MAC로써 배치파일 전송 시 무결성을 확인하는데 사용된다.

Ⅳ. CEPS 인터넷 서비스를 위한 IC카드 기반의 보안 시스템

4.1 CEPS 인터넷 서비스를 위한 보안 요구사항

CEPS 전자화폐를 인터넷에서 사용하기 위해서는 네트워크 상에서의 도청, 위조 및 변조, 신분 위장 등의 공격에 대해서 보안 서비스를 제공해야 한다. CEPS 전자화폐가 인터넷에서 사용되기 위해서 제공되어야 하는 보안 서비스는 크게 다음과 같은 3가지가 있으며, 이와 같은 보안 서비스가 제공될 때, 인터넷 상에서 CEPS 전자화폐를 안전하게 사용할 수 있다.[7]

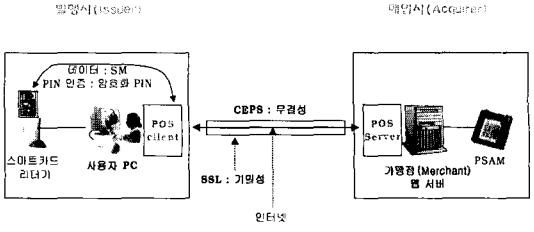
- 기밀성 : 네트워크를 통해 전송되는 데이터는 권한이 부여된 사람만이 볼 수 있어야 한다. 전송되는 데이터가 제3자의 도청에 의하여 중간에 가로채여도, 그 내용을 알 수 없게 기밀성이 제공되어야 한다. 즉, 전자화폐가 인터넷을 통해서 전송되어질 때, 제3자가 이를 가로채 액수를 비롯한 전자화폐 정보를 알 수 없어야 한다.
- 무결성 : 전송된 데이터가 전송 도중에 변경되었는지 확인할 수 있어야 한다. 전송되는 데이터가 제3자에 의해 위조 또는 변조되었다면 수신자가 위조 및 변조 사실을 알 수 있어야 한다. 즉, 제3자가 전송되어지는 전자화폐의 액수 등의 정보를 변경했을 경우, 전자화폐의 수신자가 이를 알 수 있어야 한다.
- 인증 : 데이터를 송신한 사람 및 데이터를 수신할 서버의 신원을 확인할 수 있어야 한다. CEPS 전자화폐 시스템에서는 전자화폐를 사용하는 양 당사자인 가맹점 웹 서버와 사용자에 대한 인증이 이루어져야 한다.

4.2 시스템 설계

인터넷에서 사용 가능한 IC카드 기반의 CEPS 전자화폐는 일반적인 CEPS 전자화폐가 직접 상점에서 물건을 구매할 때만 이용되는 단점을 보완하여 신용카드와 같이 인터넷에서도 사용할 수 있도록 설계한 시스템이다.

기존의 전자화폐 시스템과의 차이점을 살펴보면, 인터넷에서 지불할 수 있다는 것과 POS의 역할을 하는 전자지갑 어플리케이션(POS 클라이언트)과 POS 서버가 나뉜다는 점이다. 이 것은 사용자가 POS의 LCD를 통해 금액을 확인하고 키패드를 통해 비밀번호를 기입하던 것을 모니터와 키보드가 대신한다는 것을 의미한다.

〔그림 8〕은 전체 시스템의 구성이 어떻게 이루어지는 지를 보여주는데, IC카드, PC에서 구동되는 전자지갑 어플리케이션, SSL, POS 서버, PSAM 등 크게 5가지로 구성됨을 알 수 있다. 각 구성요소의 역할은 다음과 같다.



〔그림 8〕 시스템 구성

- IC카드 : 사용자의 PIN과 전자화폐를 저장하고, 카드의 인증서와 개인키, 발행사의 인증서, CA의 인증서 등의 인증에 필요한 정보를 저장하고 있다.
- 전자지갑 어플리케이션 : IC카드에서 데이터를 읽어 POS 서버와 통신을 하며, IC카드와 POS 사이에서 중개자 역할을 한다. 실세계의 가맹점에서 POS를 사용할 때의 입출력 수단인 LCD와 키패드를 전자지갑 어플리케이션이 대신하고 있다.
- SSL : 전자지갑 어플리케이션 POS 서버까지의 통신을 보호한다.
- POS 서버 : 웹서버 역할을 하며, 기존의 POS를 대신하여 각 전자지갑 어플리케이션에서 보내온 트랜잭션을 PSAM과 연계하여 처리하고 결과를 남긴다.
- PSAM : POS의 보안을 담당하는 부분으로 PSAM의 인증서, PSAM의 개인키, 매입사 인증서, CA의 공개키 등을 저장하고 있다.

4.3 스마트카드 내의 전자지갑

스마트카드가 제공하는 기능은 크게 2가지로 구분할 수 있다. 첫째는 카드에 화폐의 가치를 저장하고 구매와 같은 트랜잭션이 일어났을 경우 그 값을 더하거나 빼는 기능으로, 전자지갑의 역할이다. 둘째는 사용자의 개인키나 공개키 인증서를 저장하는 안전한 매체로서의 기능으로, 사용자 인증을 하는데 필요한 정보인 PIN도 저장하고 있다.

먼저 화폐의 가치를 저장하는 지갑 기능을 설계할 때는 2가지 방법으로 설계가 가능한데, 하나는 Transparent EF 파일에 일반 데이터로서 값을 저장하고, 이 EF 파일을 Write 또는 Update하지 못하게 접근제어를 설정하는 방법이다. 또 다른 하나는 카드에서 제공하는 Purse EF 파일로 지갑을 만든 후, OS에서 지원하는 기능을 사용하여 Credit이나, Debit이 일어날 경우, 각 트랜잭션의 키를 사용하여 보안을 설정하는 방법이다.

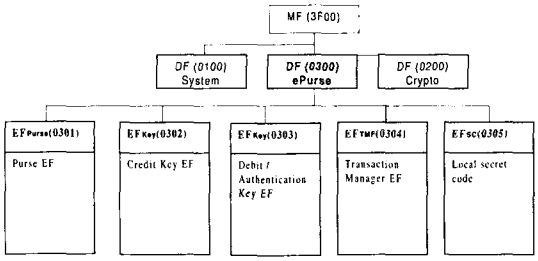
두 번째 방법을 사용하였을 때의 장점은 파일 구조 자체가 〔그림 9〕와 같이 설정되어 있어서 OS의 도움을 받을 있다는 점이다. 예를 들면, 카드에 화폐를 저장하는 도중에 사용자가 카드를 단말기로부터 억지로 빼면 카드의 데이터는 손상된다. 이런 경우에 〔그림 9〕의 백업장치 기능을 사용하여 카드는

Maximum Balance	Credit Key File CrKF
Maximum Free Debit Value	Access Dbt | Rdb
Current(Active) Balance	Cks1
Backup Balance	Cks2
Terminal Transaction Counter	Not used

〔그림 9〕 Purse 파일의 구조

OS 수준에서 지원되는 서비스로 화폐의 가치를 환원할 수 있다. 또한 각 트랜잭션마다 키를 설정하여 사용하고 있으므로, 보다 더 안전하게 사용할 수 있다.

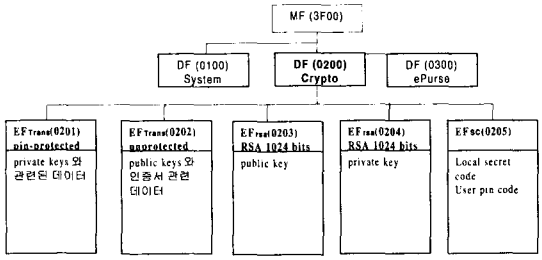
이러한 장점 때문에 본 논문에서 구현한 시스템에서 스마트카드 내의 지갑은 Purse 파일을 사용하고 있다. 이와 같이 운용하기 위해 필요한 카드의 메모리 구조는 〔그림 10〕과 같다.



〔그림 10〕 Purse DF 메모리 구조

이 DF에서 접근제어를 설정하기 위해 Secret Code 파일이 필요하고, 지갑의 역할을 수행하는 Purse 파일과 이 파일을 사용하여 Credit나 Debit 등의 트랜잭션을 수행할 때 필요한 키를 저장하고 있는 키 파일이 2개 있으며, 트랜잭션의 관리를 위해 필요한 트랜잭션 매니저 파일이 있다.

다음으로 스마트카드가 안전한 저장매체로 사용되는 경우에 개인키, 인증서, PIN 데이터를 카드 안에 저장하고, 카드 안에서 서명과 키 생성을 할 수 있도록 〔그림 11〕과 같이 DF를 구성하였다.



〔그림 11〕 키와 인증서 저장을 위한 DF 메모리 구조

먼저 DF 내부에서 Local 레벨로 접근제어를 하기위해 Secret Code File이 필요하며, 이 것을 이용하여 사용자 PIN을 확인한다. 또한 카드의 COS 명령어를 사용하여 RSA Co-processor를 이용하기 위해서 카드가 제공하는 RSA 타입의 EF를 개인키와 공개키 저장용으로 2개 설정한다. 이 파일에는 키의 일부 요소만 저장되기 때문에 나머지 관련 정보를 저장하기 위해 Transparent EF가 2개 필요하다.

이와 같이 카드 시스템 관련 파일, 카드 인증과 사용자 인증에 사용되는 정보를 저장하고 카드 안에서 전자서명을 수행하기 위해 필요한 파일들, 지갑을 사용하기 위해 필요한 파일들을 나누어서 3개의 DF로 스마트카드를 설계하였다.

4.4 인터넷 이용이 가능한 프로토콜

본 논문에서는 전자화폐 서비스 가운데 구매와 충전 부분을 인터넷에서 이용 가능하도록 하였다. 현재 국내외적으로 구매와 충전을 단말기를 사용하여 OFF-Line으로 구성한 예는 찾아보기 힘들다. 따라서 인터넷을 통한 구매, 충전은 현재 충전용 단말기가 충분히 설치되지 않은 현 상황에서 보다 더 유용하게 사용될 수 있다.

4.4.1 구매 트랜잭션

인터넷 환경을 고려하지 않은 기존의 CEPS의 구매 트랜잭션은 [그림 12]와 같이 동작한다.

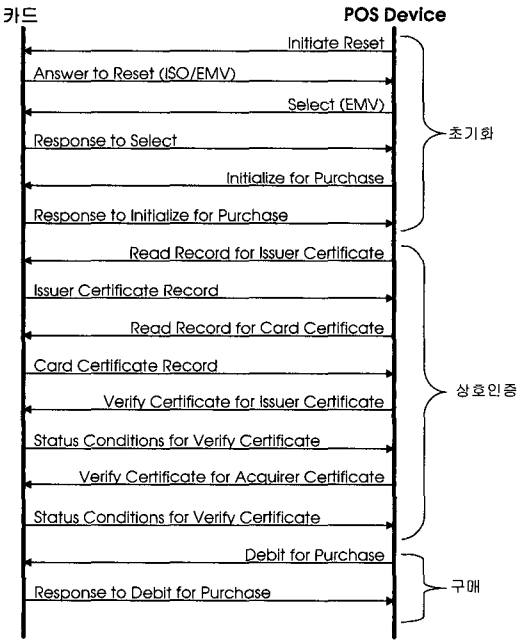
CEPS의 구매 트랜잭션은 초기화, 상호인증, 구매 등 3부분으로 나누어 생각할 수 있다.

초기화 과정에서는 카드가 리더기에 삽입되었는가를 확인한 뒤, 어떤 어플리케이션을 사용할 것인가를 결정한다.

상호인증 단계에서는 카드와 POS가 서로의 인증서를 교환하면서, 상호인증을 하는데 필요한 데이터를 주고받으며, 실질적인 상호간의 인증은 구매 부분에서 전자서명을 이용해서 이루어진다.

구매 단계에서는 실질적으로 IC카드에 있는 화폐의 값을 감소시키고 그 만큼을 POS에 전달한다. 이 과정을 인터넷상에서 서비스가 가능하도록 확장하기 위해서는 2가지 방법을 생각할 수 있다.

첫 번째 방법은 POS가 하는 역할의 대부분을 전자지갑 안에서 이루어지게 하는 것이다. 이 방법을 사용하게 되면, 사용자가 브라우저를 이용하여 쇼핑



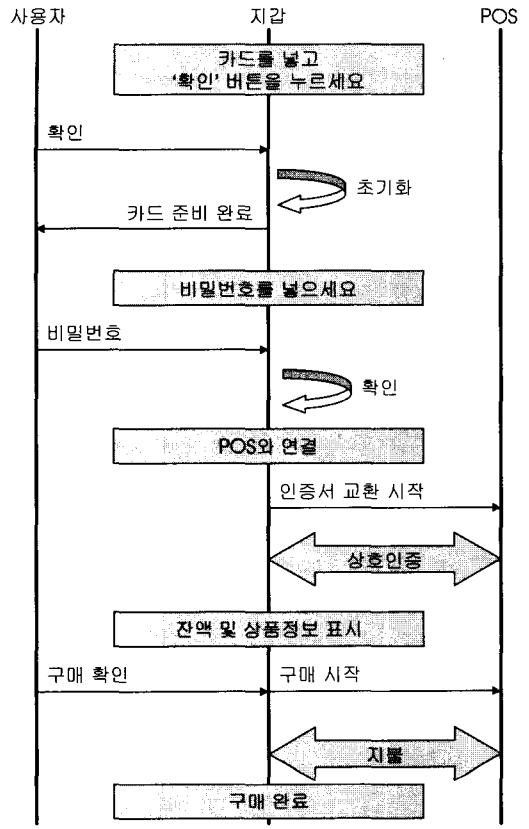
[그림 12] CEPS 구매 처리 과정

몰에 접속하였을 때, 전자지갑 어플리케이션을 다운로드 하게 되는데, 이 때, POS의 인증서도 함께 다운로드하여 지갑이 POS의 역할을 대신하게 된다. 따라서 구매가 발생했을 경우, 지갑과 IC카드 사이의 통신만 일어나고, 그 결과를 POS에 통보해 주게 된다.

두 번째 방법은 지갑은 IC카드와 POS 사이의 통신을 이어주는 매개체 역할만을 수행토록 하는 기존의 CEPS를 거의 바꾸지 않는 방법이다.

첫 번째 방법을 사용할 경우에는 지갑이 POS의 인증서를 다운로드 할 때, POS가 정당한 POS인지 인증하는 절차를 거쳐야 한다는 문제점이 있다. 또한 POS와 카드가 상호인증을 하는 것이 아니라, 카드와 POS의 모듈이 인증을 하는 것이므로 신뢰하기가 어렵다. 그렇다면 상호인증만 카드와 POS가 직접 수행하고 구매 트랜잭션은 카드와 POS 모듈이 인증을 대신하는 방법도 생각할 수 있으나, 인증이 실질적으로 구매 트랜잭션 단계에서 완료하게 됨으로, 결국 카드와 POS 사이에서 인증과 구매를 모두 처리해야 한다.

이에 비해 두 번째 방법은 트랜잭션을 바꾸지 않고 사용할 수 있어 이미 개발된 CEPS 전자화폐 시스템에 적용하기가 용이하며, 카드와 POS가 직접 연결되어 사용하던 이전의 방법을 인터넷 환경에 적



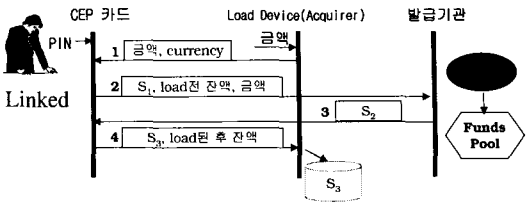
〔그림 13〕 구매 프로토콜

용하여 단지 데이터 통신만 인터넷을 통해 이루어지게 한다는 본래의 의미에도 부합된다. 이에 따라 본 논문에서는 두 번째 방법을 사용하여 설계하였다.

〔그림 13〕은 본 논문의 시스템에서 사용되는 구매 처리 프로토콜이며, 〔그림 12〕와 비교할 때, 초기화 과정에서 POS와 카드가 통신하는 것이 아니라, 지갑과 카드가 통신한다는 차이가 있다. 또 다른 중요한 차이점은 기존의 방식에서는 사용자가 POS를 통하여 구매의 의지를 나타냈기 때문에 POS에서 카드로 트랜잭션이 먼저 수행되었지만, 지금은 사용자가 클라이언트인 지갑 쪽에 위치하고 있기 때문에 클라이언트에서 카드 쪽으로 트랜잭션이 보내지게 된다는 점이다. 이와 같은 동작은 카드와 지갑이 통신할 뿐 POS는 관여하지 않게 되므로 기존의 프로토콜을 이용하기 위해서 먼저 지갑에서 POS로 트랜잭션이 시작한다는 신호를 보내게 된다.

4.4.2 충전 트랜잭션

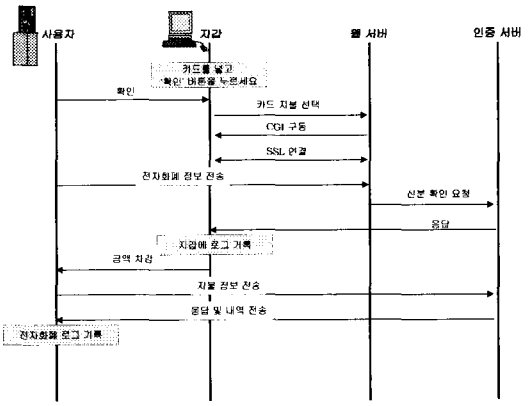
〔그림 14〕는 CEPS의 충전 트랜잭션이다.



〔그림 14〕 CEPS의 충전 트랜잭션

충전 트랜잭션은 구매에 비하여 좀더 높은 안전성을 요구하고 있다. 그 이유는 금액을 충전시키는 것이 더 많은 해킹의 위험요소를 담고 있으며, 충전 장치에서 여러 은행의 계좌에서 금액을 충전할 수도 있기 때문에 은행별로 보안 요구사항을 충족시켜야 하기 때문이다. 충전은 크게 LSAM을 사용한 오프라인 충전과 온라인 충전으로 나누어 볼 수 있다. 오프라인 충전은 현금 충전과 같은 것을 의미하는 것이고 온라인 충전은 전자화폐 사업자의 서버를 통하여 은행에서 승인을 보내주는 것을 의미한다.

〔그림 15〕는 본 논문에서 구현한 인터넷을 통한 충전 트랜잭션 절차이다.



〔그림 15〕 인터넷을 통한 충전 트랜잭션

인터넷을 통한 충전에서 기본적인 암호화나 기밀성, 무결성 보장의 수단으로 SSL을 이용하고 있다. 인터넷을 통한 지불이나 구매 트랜잭션 설계의 초점은 LSAM이나 PSAM을 어떻게 인터넷 환경에 맞게 설계하는가에 있다. 현재 〔그림 15〕에서는 전자화폐는 변경하지 않고 서버에서 인터넷 트랜잭션과 일반 트랜잭션을 구분하여 처리하는 방식을 취하고 있다. PC 상에서 구동된 지갑이 어떤 암호화 연산을 수행한 후에 승인을 내주는 것은 위험하기 때문에 대부분의 역할을 서버가 하고 있다.

4.5 구성요소간 보안 서비스

■ IC카드

IC카드가 지니고 있는 2가지 중요한 특징은 이동성과 보안성이다. 이동성은 작고 휴대하기 간편하다는 IC카드의 특성에 의해 확보되는 것이며, 보안성은 IC카드에서 제공하는 다음과 같은 요소들에 의해서 제공된다.

- 홀로그램(Holograms)
- 초미세 인쇄(Micro-printing)
- 서명띠(Signature Strip)
- Embossing
- Security Pattern
- EEPROM을 둘러싼 칩 영역을 금속 차폐물로 코팅
- 칩의 부정 변조를 탐지하는 회로 내장
- EEPROM 메모리 내의 DF들의 논리적 구성
- 비밀코드 또는 암호키로 보호

또한 IC카드는 암호 알고리즘의 사용과 데이터의 암/복호 정책을 지원함으로써 기능적 보안 특성을 가진다. IC카드가 지원하는 기능적 보안 특성은 다음과 같다.

- 메시지 암호화를 위한 키 저장
- 암호화 키를 위한 난수 생성
- MAC 계산을 위한 키 보유
- 디지털 서명으로 무결성 확인
- PKI 기반의 인증서 보유
- 디지털 서명을 위한 비밀키 저장

전자화폐 시스템에서 IC카드를 사용하는 이유는 위와 같은 보안 특성 때문이며, 본 논문에서 구현한 시스템에서는 IC카드가 제공하는 기본적인 보안기능인 접근제어와 Secure Messaging을 사용하여 카드 내부뿐만 아니라 카드와 PC 간의 통신에서도 보안 요구사항을 만족시켰다.

IC카드에서는 2가지 방법으로 접근제어를 수행할 수 있는데, 하나는 3DES 키에 의해 접근을 제한하는 것이고, 다른 하나는 secure code에 의해 접근을 제한하는 것이다. 접근 조건은 파일 기술자(File Descriptor)에 명시되어 있으며, 내용은 [그림 16]과 같다.

[그림 16]에서 key file이란 secure messaging

b7	b6	b5	b4	b3	b2	b1	b0
Val		L	Key File				
b7	b6	b5	b4	b3	b2	b1	b0
L1	SCN1			L2	SCN2		

[그림 16] 접근제어 구조

에 사용되는 3DES 키 파일 SFI(Short File Identifier)를 말하는 것이고, SCN1과 SCN2는 secure code no.의 2개를 의미한다.

어떤 파일에 대해 secure code를 이용해 접근을 제한하였을 경우에 사용자가 파일을 사용하려면 먼저 파일이 어떤 secure code로 제한되었는가를 알아서 secure code를 검증하면 된다. 또 키에 의해서 접근을 제한할 때는 사용자가 그 키를 알고 있는가는 SelFulKey 명령어를 사용하여 확인하게 되고, 확인된 사용자만 파일에 접근할 수 있다.

■ IC카드와 전자지갑의 통신

IC카드와 전자지갑은 시리얼 라인을 통하여 데이터를 주고받게 되는데, 이 라인을 도청하여 어떤 데이터를 주고받는지 확인할 수도 있기 때문에 이 라인을 통하여 주고받는 데이터는 secure messaging이라는 방식을 사용한다.

secure messaging은 기밀성과 무결성을 제공하는데, 기밀성을 제공하기 위해서 난수를 마스터키로 암호화하여 세션키로 사용한다. 이 세션키로 데이터를 암호화하여 통신하고 무결성을 제공하기 위해서 세션키로 MAC 값을 계산하여 명령어 뒤에 첨부해 사용한다. [그림 17]은 데이터의 무결성을 제공하기 위한 구조를 나타낸다.

Format 1

Tag	Length	Value
T	L	Cryptogram

Format 2

Value 1	Value 2
Cryptogram	MAC(Optional)

[그림 17] secure messaging

■ PC 상에서 구동된 지갑

PC에서 구동된 지갑은 IC카드와 통신을 담당하며 SSL을 통하여 POS 서버와도 통신을 담당한다. 또한 브라우저에서 동작되는 지갑은 구매를 할 경우, POS 서버에서 오는 CEPS 트랜잭션을 받아 IC카드에 넘겨주는 역할을 한다. 지갑이 PC 상에서 동작하기 때문에 사용자가 키보드에 입력한 내용을

가로채거나 메모리에 로드되어 있는 데이터를 가로채는 공격이 가능하다. 그러나 이러한 공격은 전자화폐 시스템을 대상으로 한다기 보다는 OS나 PC 자체의 시스템에 대한 공격임으로, OS나 시스템 차원의 보안 프로그램에서 해결할 수 있다.

- PC와 POS의 통신

SSL을 사용하여 지갑과 POS 서버 사이에서 주고 받는 데이터에 대해 기밀성 및 무결성을 제공하는 부분이다.

V. 시스템 구현

5.1 시스템 구현 내용

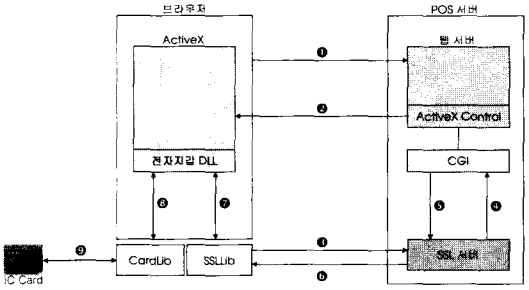
본 시스템은 크게 서버와 클라이어트 모듈로 나누어진다. 서버 모듈은 서버 측에서 수행되는 SSL 서버와 CGI 프로그램이고, 클라이언트 모듈은 사용자의 브라우저에서 수행되는 ActiceX 프로그램이다.

〔그림 18〕은 사용자가 브라우저에서 쇼핑몰에 접속한 뒤, 물건을 구매하기까지의 과정을 나타낸 구성도이다. 먼저 ❶에서 브라우저가 웹서버(쇼핑몰)에 접속하게 되면 웹서버에 있던 ActiveX 콘트롤이 브라우저로 다운로드 되어 브라우저에서 로드된다. 이 ActiveX 콘트롤은 3가지의 기능을 하고있는데, 첫 번째가 CEPS 트랜잭션의 처리를 하는 지갑의 역할이고, 두 번째는 IC카드와 통신을 하기위한 IC 카드 핸들링 부분이다. 세 번째는 SSL 통신을 위한 부분이다. 이 ActiveX 프로그램의 사용자 인터페이스는 Visual Basic으로 구현되었으며, 카드와 SSL 라이브러리를 사용하여 각각을 핸들링 하는 프로그램은 Visual C++로 구현하여 이 전체를 DLL로 만들어 사용하였다. ❷에서 받은 ActiveX 프로그램이 시작되면, ❸을 통해 SSL 서버와 통신을 하게되고, 서버 확장기술인 CGI를 사용하여 CEPS 트랜잭션을 처리한다. 그 뒤 ❺, ❻을 통하여 다시 브라우저로 전달되며, ❽, ❾를 거쳐 카드에 데이터를 전달할 수 있다.

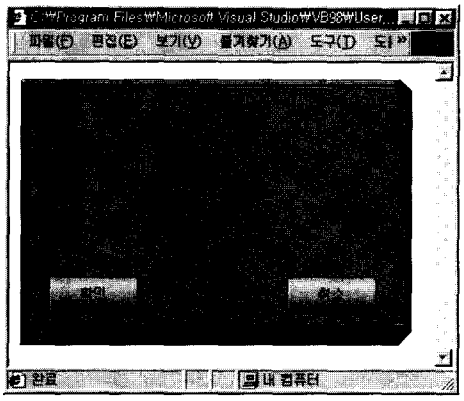
개발에 사용된 모든 암호화 라이브러리는 OpenSSL의 암호화 라이브러리를 이용하였다. 또한 IC카드는 CEPS의 동적 데이터 인증을 구현하기 위해서 RSA Co-processor가 장착된 Gemplus사의 GPK8000 카드를 선택하였다. 또한 GPK 카드와 통신하고 카드의 자원을 사용하기 위해 GPK 라이브러리를 사용하여 구현하였다. 브라우저에서 동작하는 지갑은 ActiveX 기법을 사용하여 구현하였다.

〔그림 19〕는 인터넷에서 CEPS를 이용한 구매 트랜잭션이 수행되는 그림이다. 지갑 프로그램은 PC에 연결되어 있는 스마트 카드 전자화폐와 통신을 담당하며 전자화폐사 서버와 연결되어 구매할 수 있다.

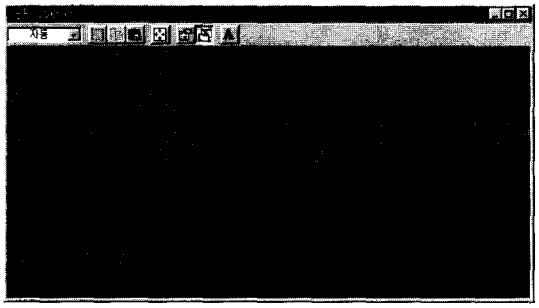
또한 〔그림 20〕은 POS Server 화면으로, 전자화폐 사의 서버를 구현한 프로그램이 실행되는 것을 보여준다. POS Server는 SSL 서버를 통하여 암호화 된 데이터를 받아 승인하고 지불 결과를 생성하여 보내주는 역할을 수행하고 있다.



〔그림 18〕 구현모듈 구성



〔그림 19〕 전자지갑 구동 화면



〔그림 20〕 POS 서버

5.2 구현 시스템의 특징

본 논문에서 구현한 시스템의 가장 큰 특징은 전자상거래 운용에 있어서 필수적인 요소인 인터넷 사용이 가능하다는 점과 공개키 암호기술에 기반한 보안 서비스를 제공한다는 점이다. 또한 국제 표준 규격인 CEPS를 따라 구현되었기 때문에 국제적인 호환이 가능한 전자화폐 시스템이라고 할 수 있다. [표 3]은 본 논문에서 구현한 시스템과 다른 전자화폐 시스템을 비교한 결과이다.

[표 3] 전자화폐의 비교

구분	MODEX	VISA CASH	K-CASH	구현 시스템
발권주체	Originator	Issuer Bank	Issuer Bank	Issuer Bank
유통주체	유통은행	Issuer Bank	Issuer Bank	Issuer Bank
인출방식	ATM, 전화	ATM	은행창구, ATM	은행창구, ATM, 전화, PC
자금이체	개인간 가능	개인간 불가	개인간 불가	개인간 불가
거래추적	가능	가능	가능	가능
가치저장	IC카드	IC, ROM, HDD	IC카드	IC카드
원격가치 이전	가능	불가	불가	가능

[표 3]에서 보는 바와 같이 구현 시스템은 거래추적 등 기본적인 전자화폐 서비스를 제공한다. 그리고 다른 전자화폐 시스템의 경우에는 인터넷 사용이 불가능하지만, 구현 시스템은 은행창구나 ATM, 전화 뿐만 아니라, PC를 이용해서 인터넷에서도 사용이 가능하기 때문에 인터넷 쇼핑몰을 이용한 물품 구매 등에 적합하며, 원격 가치 이전이 가능한 장점도 갖고 있다. 또한 IC 카드와 암호기술을 통해 전자화폐 시스템 운용에 필요한 기밀성, 무결성, 사용자 인증과 같은 보안 서비스를 제공한다. 하지만, MODEX에서는 제공하는 개인간 자금 이체 서비스는 제공하지 못한다.

Ⅵ. 결 론

전자화폐 시스템은 신용카드에 비해 남녀노소 누구나 사용 가능하고 자기띠 카드 기반의 신용카드에 비해 보안성이 뛰어나다. IC카드는 이런 높은 보안성을 지니고 있음에도 불구하고, 초기에 높은 개발 비용과 다양한 어플리케이션을 제공하기 어려워 제한적으로 사용되었다. 그러나 최근 IC카드 개발 기술의 발전과 함께 IC카드와 단말기 가격이 하락하고, 자바 기술 등을 접목하면서 다양한 어플리케이션을 수용할 수 있게 되어 전자화폐 시스템은 IC카드를 기반으로 개발하는 것이 일반적이다.

본 논문에서는 기존의 CEPS 전자화폐의 보안구조에 대하여 분석하였고, 그 결과를 기반으로 인터넷에서도 사용 가능한 시스템을 설계 및 구현함으로서 사용자의 편리성과 시스템의 안전성에 대한 새로운 방안을 모색하였다. 본 시스템의 클라이언트 프로그램은 ActiveX 프로그램으로 구현되어 사용자가 별도의 프로그램을 설치할 필요 없이 브라우저만으로 전자화폐 시스템의 이용이 가능하다. 또한 사용자의 인증 정보나 화폐 가치를 IC카드에 저장하기 때문에 사용자는 IC카드 단말기만 부착된 컴퓨터만 있으면 언제 어디서나 구현 시스템을 사용할 수 있다.

참 고 문 헌

[1] CEPSCO, Common Electronic Purse Specifications(CEPS) Business Requirements Version 6.1, 1999.

[2] CEPSCO, Common Electronic Purse Specifications(CEPS) Functional Requirements Version 6.3, 1999.

[3] CEPSCO, Common Electronic Purse Specifications(CEPS) Technical Specification Version 2.1,1999.

[4] EMVCO, EMV '96 Version 3.1.1 Integrated Circuit Card Specification, 1999.

[5] EMVCO, EMV '96 Version 3.1.1 Integrated Circuit Card Terminal Specification, 1999.

[6] EMVCO, EMV '96 Version 3.1.1 Integrated Circuit Card Application Specification, 1999.

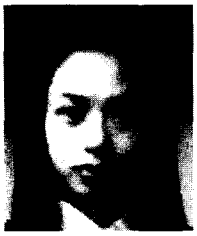
[7] The SSL Protocol Version 3.0 Internet Draft, IETF

[8] Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459), IETF, 1999. 1.

[9] Internet X.509 Public Key Infrastructure Certificate Management Protocols(RFC 2510) IETF, 1999. 3
[10] Internet X.509 Certificate Request Message Format(RFC 2511), IETF, 1999. 3
[11] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영, "전자상거래 보안기술", 생능출판사, 1999.
[12] GITS, "GITS Working Group Accomplishments Report", 1996.
[13] "Digital Signature Guidelines", American Bar Association, 1996.
[14] Secure Electronic Commerce, Warwick Ford, Michael S. Bauem, Prentice Hall 1998.
[15] GPK Interface Library manual, Gemplus.
[16] Cryptography and Network Security 2/E, Stalling.
[17] Jaca Card Technology for Smart Cards Architecture and Programmer's Guide, Zhiqun Chen.

〈著者紹介〉

이 종 후 (Jong-hu Lee)
1997년 2월 : 충남대학교 컴퓨터과학과 졸업
1999년 2월 : 충남대학교 컴퓨터과학과 석사
1999년 3월~현재 : 충남대학교 컴퓨터과학과 박사과정
〈관심분야〉 네트워크 보안, PKI



라 은 주 (Eun-ju Ra)
1999년 2월 : 충남대학교 컴퓨터과학과 졸업
2002년 2월 : 충남대학교 컴퓨터과학과 석사
2002년 1월~현재 : 한국정보보호진흥원 연구원
〈관심분야〉 네트워크 보안

백 상 수 (Sang-su Baek)
1999년 2월 : 충남대학교 컴퓨터과학과 졸업
2001년 2월 : 충남대학교 컴퓨터과학과 석사
2002년 3월~현재 : 충남대학교 컴퓨터과학과 박사과정
〈관심분야〉 스마트카드, PKI, 이동통신 보안

지 석 진 (Seok-Jin Jee)
1999년 : 세종대학교 전산학과 졸업
2001년 : 세종대학교 전산학과 석사
2001년 4월~현재 : 한국정보보호진흥원 연구원
〈관심분야〉 유·무선 PKI, 전자상거래보안

이 용 (Yong Lee)
1988년 2월 : 연세대학교 식품공학과 졸업
1994년 2월 : 덕성여자대학교 전산학과 졸업
1996년 8월 : 연세대학교 컴퓨터과학과 석사
2001년 2월 : 연세대학교 컴퓨터과학과 박사
1993년 3월~1994년 5월: 디지콤 정보통신연구소 연구원
2001년 1월~현재 : 한국정보보호진흥원 선임연구원
〈관심분야〉 유·무선 PKI, 이동통신

류 재 철 (Jae-Cheol Ryou)
1985년 2월 : 한양대학교 산업공학과 졸업
1988년 5월 : Iowa State Univ. 전산학 석사
1990년 12월 : Northwestern Univ. 전산학 박사
1991년 2월~현재 : 충남대학교 정보통신공학부 교수
〈관심분야〉 인터넷 보안