웹 상에서의 스마트카드 지불 시스템 설계 및 구현

○
김소희, 김증섭, 유기영
경북대학교 컴퓨터공학과

Design and Implementation of Smart Card Payment System on the Web

So-Hee Kim, Jeung-Seop Kim, Kee-Young Yoo
Department of Computer Engineering, Kyungpook National University

요 약

웹 상에서의 전자 상거래는 고객과 상인간의 정보 보호와 대금 결제의 신뢰성이 보장되어야 한다. 스마트카드는 자체내의 메모리기능과 연산기능을 가진 IC카드로써 사용자 인증과 개인 정보 보호 기능이 탁월하다. 따라서, 신용 카드 기반의 전자 지불 프로토콜의 표준인 SET을 사용하여, 보안 기능이 뛰어난 스마트카드를 지불 수단으로 하는 안전하고 효율적인 스마트카드 전자 지불 시스템을 설계하고 자바로 구현하였다. 본 논문에서 구현한 지불 시스템은 지불 정보와 주문 정보의 기밀성을 제공하고, 공개키 기반의 암호 체계로 데이터의 무결성을 보장한다.

1. 서 론

스마트카드는 다양한 응용 서비스들을 하나의 카드로 처리할 수 있는 요구와 사용자 보안성을 높이기 위해 마이크로 프로세서와 메모리가 내장된 IC카드이다[1]. 스마트카드가 제공하는 전자 지갑 기능을 이용하여 홈뱅킹 서비스에서의 전자화폐의 입출금 기능 및 전자 상거래에서의 결제 기능을 구현할 수 있고, 개인의 정보를 스마트카드 안의 메모리에 저장함으로써 사용자 정보 보호를 보장할 수 있다[2]. 또한, 스마트카드의 인증 기능에는 터미널, 카드 그리고 사용자 인증이 있다. 웹 상에서 스마트카드를 이용한 전자 상거래에서 고객과 상인이 상호 신뢰성을 확보하면서 대금 결제의 부담 및 사용자 사생활에 관계된 정보를 보호할 수 있다.

웹을 통한 전자 상거래에서 고객과 상인이 서로 신뢰하면서 대금 결제의 수단으로 스마트카드를 이용한다면, 대금 결제의 부담 및 사생활에 관계된 정보를 보호할 수 있다. 본 논문에서는 웹 상의 가상 쇼핑몰에서 스마트카드를 결제 수단으로 하는 전자 지불 시스템을 자바로 구현하였다. 지불 시스템 구현은 스마트카드와 네트워크로 연결된 클라이언트-서버 프로그램으로 구성된다.

스마트카드 운영체제는 ISO-IEC 7816-1, 2, 3, 4 규정을 준수하는 운영체제로 지불을 위한 응용 프로그램을 구현하였고, 웹 상에서의 지불을 위해 소켓을 이용한 클라이언트-서버의 지불 시스템은 SET(secure electronic transaction) 프로토콜을 이용하였다.

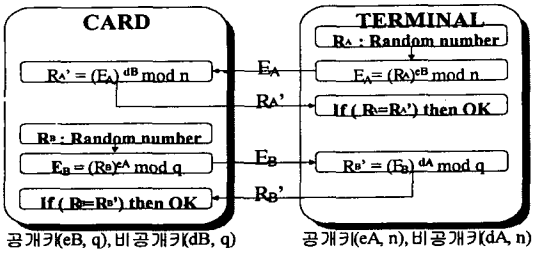
본 논문의 구성은 다음과 같다. 2장에서는 스마트카드의 인증에 대해서 설명하고, 3장에서는 지불 시스템 구조와 프로토콜에 대해서 설명하고, 4장에서는 지불 시스템 구현에 대해서 설명하며, 마지막으로 5장에서는 결론 및 향후 연구방향에 대해서 기술한다.

2. 스마트카드 인증

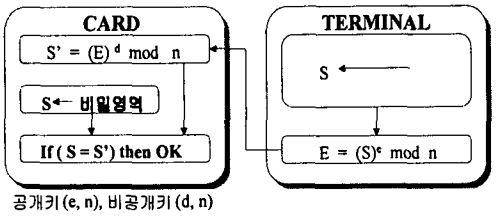
스마트카드란 플라스틱 카드에 0.3mm 두께의 마이크로 프로세서와 메모리를 내장한 IC 카드로, ISO에서 규정한 IC 카드의 물리적인 구조와 인터페이스를 준수하고 있다[3]. 구현에 사용된 스마트카드는 i80196 마이크로 컨트롤러, 32kbyte의 ROM, 32kbyte의 RAM, RS232C 입출력장치, 리셋장치, 16비트 어드레스 버스, 8비트의 데이터 버스로 구성되고, 통신속도는 9600 보레이트(baud rate)이다. 32kbyte의 RAM 중 16kbyte는 RAM으로 사용하고, 나머지 영역은 EEPROM으로 사용한다. 카드와 통신할 터미널은 PC이고, 터미널에서 제공되는 통신 및 응용 프로그램은 C++ Builder 3으로 구현하였다.

스마트카드 인증에는 터미널 인증, 카드 인증 그리고 사용자 인증이 있다[6]. 터미널 인증과 카드 인증은 양방향으로 인증되며, 인증할 때마다 난수를 발생하기 때문에 터미널과 카드의 위조가 어렵다. 터미널 인증과 카드 인증 과정은 [그림 1]과 같다.

사용자 인증은 세션 시작시 발생하며, 사용자가 입력한 PIN (Personal Identification Number)이 스마트카드에 저장된 값과 비교함으로써 이루어진다. 사용자 인증 과정은 [그림 2]와 같다.



[그림 1] 터미널인증과 카드인증



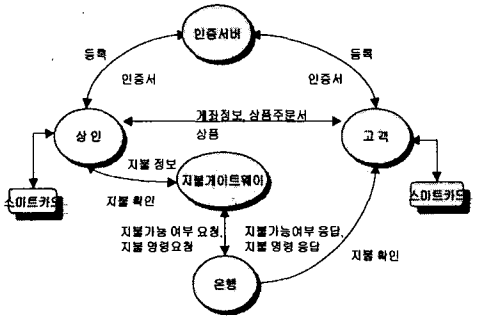
[그림 2] 사용자 인증

3. 지불 시스템 설계

지불 시스템이란 스마트카드의 자동적인 인증 절차를 거쳐 사용자의 보안을 보장하고, 웹 상에서 온라인으로 대금 결제를 안전하게 수행하는 시스템이다. 고객이나 상인은 지불 시스템에서 스마트카드로 대금을 결제하기 위해서는 인증 기관으로부터 공인된 인증서를 가져야 한다. 이러한 과정을 등록 과정(registration process)이라 한다. 등록이 된 고객과 상인은 지불 과정(payment process)을 통해 지불 서비스를 이용한다.

3.1 지불 시스템 구조

본 논문에서 구현한 전자 지불 시스템은 자체 보안 기능이 뛰어난 스마트카드를 지불 수단으로 사용하고, 고객과 상인간의 대금 결제를 웹 상에서 안전하게 서비스한다. 이러한 지불 시스템은 참여하는 개체들의 신분이 인증기관을 통해 인증 되어야 하며, 메시지 암호화 기법을 사용하여 신뢰성 있는 정보 전송을 보장해야 한다. 지불 시스템의 구조는 [그림 3]과 같다.



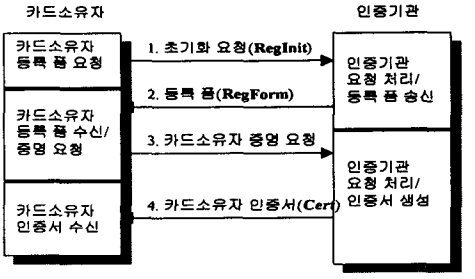
[그림 3] 지불 시스템 구조

3.2 지불 시스템 프로토콜

본 논문에서 구현한 시스템 프로토콜은 등록 프로토콜과 지불 프로토콜로 구분되며, SET 프로토콜을 기반으로 한다. SET 프로토콜은 비자 카드(VISA Card)와 마스터 카드(Master Card) 회사들이 협력하여 만든 프로토콜로서 웹 상에서 신용카드를 기반으로 하는 전자 지불 프로토콜이다[4]. SET 프로토콜에 참여하는 개체들간의 통신은 지불 정보의 기밀성과 무결성을 보장하기 위해 인증 절차와 암호화 과정을 거친다.

3.2.1 등록 프로토콜

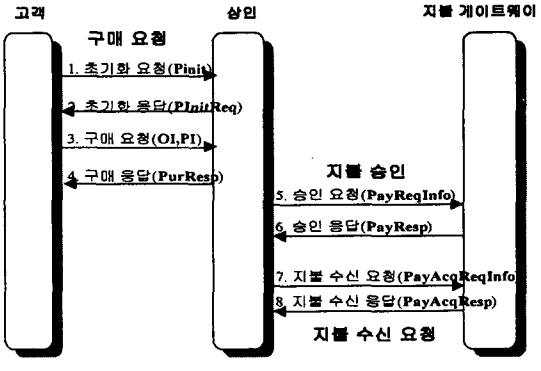
등록 프로토콜은 공인된 인증 기관으로부터 고객이나 상인이 공인된 인증서를 발급 받는 과정이다. 인증서의 양식은 ITU-X.509 표준을 따른다. ITU-X.509는 X.500 계열의 일종으로 디렉토리 서비스에 대한 사항을 기술하고 있으며, 공개키 암호화 방식을 사용하며 메시지 암호 알고리즘은 RSA를 사용하고, 서명에는 SHA 해쉬 함수를 사용한다[5]. 등록 프로토콜은 다음 [그림 4]와 같다. [그림 4]에서 카드소유자는 고객 또는 상인이다.



[그림 4] 등록 프로토콜

3.2.2 지불 프로토콜

지불 프로토콜은 등록된 사용자가 상품에 대한 대금 결제를 스마트카드로 결제할 때 동작한다. 지불 프로토콜은 [그림 5]와 같다.



[그림 5] 지불 프로토콜

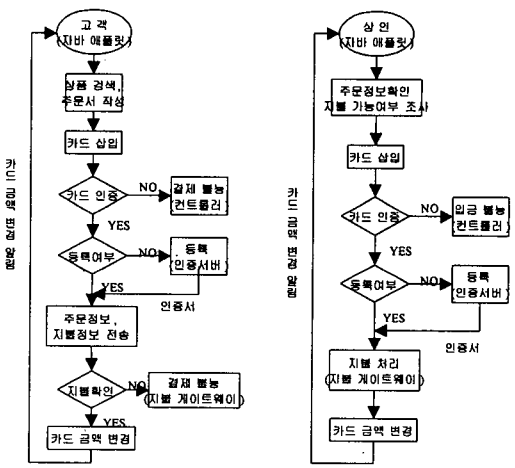
지불 프로토콜 과정은 구매 요청 단계, 지불 승인 단계, 지불 수신 요청 단계로 나눈다. 고객이 상인에게 구매할 상품에 대한 결제의 의사를 표시하고, 요청을 받은 상인은 지불 게이트웨이를 통해 결제 가능 여부를 판단하여 지불 수신 요청을 한다.

4. 지불 시스템 구현

스마트카드 운영체제는 ISO-IEC 7816 표준에 근거하여 i80196 마이크로 컨트롤러에서 C언어와 어셈블리어로 구현하였으며, 컨트롤러와 PC간의 통신 응용 프로그램은 C++ Builder로 구현하였다. 지불 시스템은 웹 상에서 지불 서비스를 가능하게 하기 위해 자바로 구현하였다. SET 프로토콜에 참여하는 각 서버들은 JDK1.2.1을 이용하여 소켓을 이용한 클라이언트-서버 프로그램으로 구성되어 있으며, 고객이나 상인을 위한 프로그램은 자바 애플릿으로 구성하였다. 또한, 각 서버들은 펜티엄급 이상의 컴퓨터를 사용하고, 고객이나 상인 서버는 아파치(Apache) 웹 서버를 사용한다. 그리고, 자바 직렬 통신 API를 이용하여 카드와 PC간의 통신 기능을 통해 고객과 상인의 카드에 금액에 대한 정보를 변경한다.

4.1 지불 시스템 흐름도

지불 시스템은 고객이 상인에게 상품에 대한 대금을 결제를 안전하게 수행하고 난 뒤, 고객과 상인은 각각의 스마트카드의 금액 정보를 변경한다. 고객과 상인은 웹 상에서 정보를 주거나 받게 되고, 그 하위에서 서버 프로그램이 실제로 인증 서버와 지불 게이트웨이 서버와 통신하면서 서비스한다. 인증 서버는 인증 프로토콜을 사용하여 고객과 상인의 카드에 대한 인증서를 발급한다. 지불 게이트웨이는 고객의 카드 정보를 은행과 연결하여 지불 가능 여부를 상인에게 알리면, 상인이 지불 승인을 하면, 고객과 상인 은행으로부터 정보를 변경하고, 상인과 고객에게 지불 확인 메시지를 준다. 전체 시스템 흐름을 고객과 상인 측에서 보면 [그림 6]과 같다.



(a) 고객 시스템 (b) 상인 시스템

[그림 6] 시스템 흐름도

4.2 메시지 포맷

본 논문에서 구현한 지불 시스템에서 사용되는 메시지는 등록 과정과 지불 과정으로 나눈다. 등록 과정에서 사용되는 등록폼은 자바 명령어 키툴(keytool)을 사용하여 인증서를 만드는 데 필요한 정보로 구성된다.

등록폼 : **RegForm(CN,OU,O,L,ST,C)**

인증서 : **Cert(카드 일련번호|서명 알고리즘ID|발행자 이름|유효기관|사용자이름|공개키|발행자ID|사용자 ID|서명)**

지불 과정에서 사용되는 주문 정보와 지불 정보 메시지는 다음과 같다. 주문 정보는 주문할 상품과 수량 가격으로 구성되며, 지불 정보는 지불 승인 정보와 지불 수신 요청 정보가 있다.

주문정보 : **OI(상품ID|수량|상품가격)**

지불 승인 정보 : **PayReqInfo(고객카드일련번호|고객카드 발행은행ID|고객계좌번호)**

지불 수신 요청 정보: **PayAcqReqInfo(PayReqInfo|상인카드발행은행ID|상인계좌번호|지불금액)**

5 결론 및 향후 연구 과제

본 논문에서는 ISO-IEC 7816-1, 2, 3, 4의 규정을 준수하는 스마트카드를 결제수단으로 하고, SET 프로토콜을 사용하는 웹 상에서의 전자 지불 시스템을 구현하였다. 스마트카드는 터미널과 카드를 인증하는 양방향 인증 단계와 사용자 인증 단계를 거쳐 높은 보안성을 지닌다. 그리고, 웹 상에서의 지불 시스템을 구현하기 위해 자바로 SET을 응용한 프로토콜을 구현하여 보안성 높은 스마트카드 지불 시스템을 구현하였다. 지불 시스템의 보안 요구 사항인 기밀성, 데이터 무결성, 부인방지 기능이 있다[7]. 따라서, 본 논문에서 구현한 시스템은 메시지에 인증서를 항상 첨부하여 전송함으로써 부인 방지가 가능하고, 메시지는 인증서에서 공개키를 획득하여 암호화 처리를 하여 전송됨으로 메시지 무결성도 제공한다. 향후 연구방향은 자바 카드에 적용, ECC(elliptic curve cryptography) 암호 알고리즘을 SET 프로토콜에 적용시켜 작은 키 사용으로 암호 연산 속도 증가를 가지는 지불 시스템 구현 연구가 계속되어야 할 것이다.

[참고 문헌]

[1] J. L. Zoreda, J. M. Oton, *Smart Cards*, ARTECH HOUSE Boston London, 1994.

[2] 김종률, "전자상거래에서 IC카드 소프트웨어 및 활용 방안 연구", http://forum.nca.or.kr/journal/96/ 4-rp2.htm, 1996.

[3] ISO/IEC 7816-1, Identification cards-Integrated circuit(s) cards with contact-Part 1: *Physical characteristics*, 1987.

[4] *Secure Electronic Transaction(SET) Specification, Book 1 : Business Description, Version 1.0*, May 31, 1997.

[5] ITU-T Recommendation X.509, *DATA NETSORK AND OPEN SYSTEM COMMUNICATIONS : DIRECTORY*, 1997.

[6] 김증섭, "RSA 암호화 기능을 가지는 스마트카드 운영체제 구현", 석사학위 논문, 경북대학교, 1998.

[7] 박필승, 남길현, "스마트카드를 이용한 보안성 높은 전자지불시스템 제안", *한국통신정보보호학회 종합학술발표회 논문집 vol 8. No.1*, 1999.