2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

IMT2000 단말기 상에서의 USIM 카드를 이용한 쇼핑몰 마일리지 통합 관리 시스템에 대한 연구

강병모*, 백장미*, 홍인식*
*순천향대학교 정보기술 공학부
e-mail:kbm1006@hotmail.com

A Study on United Mileage Management System for Internet Shopping-Mall using USIM Card in IMT2000

Byung-Mo Kang*, Jang-Mi Baek*, In-Sik Hong*
*Division of Information Technology Engineering,
Soonchunhyang University

요약

차세대 이동통신 서비스인 IMT2000에서 기본적으로 탑재될 예정인 USIM 카드는 스마트 카드의 또 다른 이름으로서 보다 더 안전하고 다양한 기능을 수행할 수 있다. 본 논문에서는 USIM 카드의 유효성을 입증하기 위하여, 쇼핑몰 마일리지 통합 관리 어플리케이션을 제안한다. 마일리지 통합 관리 어플리케이션은 USIM 카드의 메모리에 저장되어, 한 개인의 독립적인 프로그램으로서 작동되며, 적립된 마일리지의 현금화를 가능하게 한다. USIM 카드의 연산 기능을 이용하여, 각기 다른 마일리지 체계를 가지는 여러 쇼핑몰들간의 통합 마일리지를 직접 계산하고 적립할 수 있는 프로그램을 제안하였다. 본 시스템의 핵심은, 공인기관의 디렉토리를 참조하여 USIM 카드로 서베이 한다는 점이다.

1. 서론

차세대 이동통신인 IMT2000(International Mobile Telecommunications 2000) 기술은 음성 서비스를 기본으로 하여 다양한 형태의 어플리케이션 활용이 가능한 기술이다. IMT2000 서비스 상용화시 단말기에 내장될 핵심 장비인 USIM(Universal Subscriber Identity Module) 카드는 UMTS(Universal Mobile Telecommunications System) 특유의 스마트 카드를 지칭하는 또 하나의 이름으로서, 개인의 이동성을 강조하며, 사용자의 인증을 위한 기능을 기본적으로 제공한다. USIM 카드는 CPU를 통해 간단한 연산을 수행할 수 있으며, RAM과 ROM, EEPROM을 내장하고 있어서 다양한 어플리케이션을 개발하여 저장할 수 있다.

현재, 썬 마이크로시스템의 자바카드(Java Card), 마이크로 소프트의 WFSC(Windows for Smart Card), 마스터 카드의 MULTOS와 같은 칩 카드 운영 시스템이 등장하면서, 독자적으로 카드 어플리케이션을 개발할 수 있게 되었다. 본 논문에서는 차세대 COS라 불리는 Java Card에 기반을 두고 IMT2000 단말기 상에서 USIM 카드를 이용한 통합 쇼핑몰 마일리지 관리 어플리케이션의 개발을 제안한다. 본 시스템은 국제 표준인 ISO 7816 표준과 GSM(Global System for Mobile communication), EMV 지불 스펙, 그리고 Java Card를 참조하여 시스템을 제안하였다.

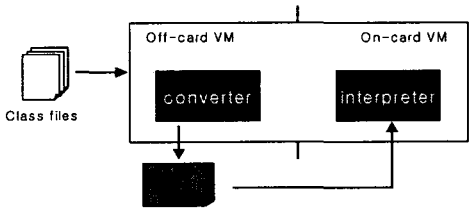
2. 관련기술

2.1 Java Card

Java Card는 스마트 카드의 장애 요소를 보안하기 위한 기술로서, 자바언어로 작성된 어플리케이션을 실행한다. 자바언어를 사용하여 작성하기 때문에 자바언어가 지니는 특성을 Java Card 에 적용시킬 수 있다. Java Card는 상위 레벨의 어플리케이션 개

발의 용이하며, 암호화 알고리즘에 의한 안정성이 뛰어나다. 또한 하드웨어적으로 독립성을 지니며, 다중어플리케이션을 지원하여 사용자의 편리성을 제공한다. Java Card는 소량의 프로그램과 데이터를 저장할 수 있는 RAM, EPROM, ROM이 탑재되어 있으며 JCVM, JCRE, APIs로 구성되어 있다.

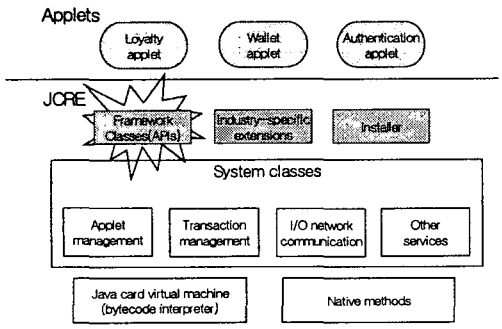
2.1.1 JCVM(Java Card Virtual Machine)



<그림 1> Java Card Virtual Machine

JCVM은 Off-card VM과 On-card VM으로 구성된다. 자바언어로 작성하여 생성된 Class 파일은 Off-card VM의 converter를 이용하여, CAP 파일로 변형된다. CAP 파일은 Class 파일을 보다 더 압축한 형태의 파일로서, Java Card에 로드되어 On-card VM의 interpreter를 통하여 실행한다.

2.1.2 JCRE(Java Card Runtime Environment)



<그림 2> JCRE의 구성 요소

JCRE는 Java Card 하드웨어의 상부에 위치한다. JCRE는 Java Card vendor로부터 Applet을 분리하는 역할을 하며, 표준화 시스템과 API 인터페이스를 제공한다. 로드되어 인스톨된 애플릿이나 데이터는 EEPROM에 저장되기 때문에, 전원의 공급이 끊어지는 경우라도, VM은 단지 보류되는 상태이며, JCRE의 상태와 모든 데이터 값은 보호된다.

2.1.3 APIs(Applicaton Programming Interface)

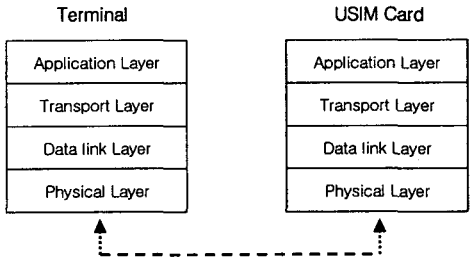
API는 Java Card의 어플리케이션을 위한 Java 패키지와 클래스를 정의한다. Java.lang Package는 기본적으로 자바언어에 지원되는 사항을 제공하는 것으로 자바 클래스 계층의 Root 에 해당하며, 모든 예외처리를 위한 상위 Class가 존재한다. Javacard.framework Package는 Framework class와 interface를 제공하며, 전송프로토콜을 지원한다. 또한, Applet 실행과 Applet들의 상호작용을 위한 Applet class를 정의하며, APDU class를 제공한다. Javacard.security Package는 암호화 알고리즘을 위한 framework를 제공하며, Javacardx.crypto Package는 암호화와 복호화 함수를 지원하기 위한 Cipher class를 정의한다.

2.2 USIM 카드

USIM 카드는 스마트카드의 일종으로 IMT2000 서비스 상용화시 단말기 내에 내장되는 장비로서, 마이크로프로세서와 메모리를 탑재하고 있으며, 전기적 신호에 의해 정보를 저장하며 처리한다. USIM 카드는 기본적으로 비밀 인증 데이터를 지니며, 사용자의 개인 데이터를 저장할 수 있는 기능이 있다. USIM 카드는 외부의 자원에 의존하지 않기 때문에 공격성에 대한 저항력이 크며, 암호화 알고리즘을 사용하므로 데이터의 보안성이 높으며 개인 휴대성과 간섭에 대한 안정성이 높은 특징을 지닌다.

2.2.1 전송 프로토콜

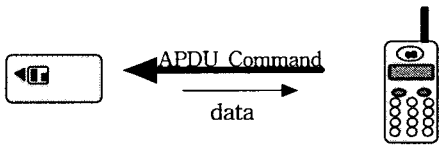
프로토콜이란 각각의 상이한 장비간에 오류 없이 데이터를 전송하기 위한 규약을 의미한다. 전송 프로토콜은 USIM 카드와 각 터미널 즉, 모바일 장비 사이에서의 데이터 변환에 관련된 프로토콜을 의미하는 것으로서 비동기식 반이중 통신 프로토콜을 사용한다.



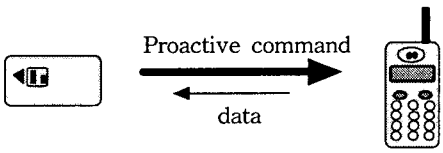
<그림 3> USIM 카드에서의 전송 프로토콜

2.2.2 단말기와 USIM 카드 사이의 통신

기존의 스마트 카드와 단말기간의 통신은 ISO 7816의 스펙을 기준으로 하여 Command와 Response를 주고받는 형식의 APDU를 사용한다. 그러나 이 형식은 스마트 카드가 단지 단말기의 명령에 응답하는 수준으로서 단말기 측의 부담이 크다는 것을 알 수 있다. USIM 카드는 이러한 부담을 최소화하기 위해 USAT(USIM Application Toolkit)를 사용한다. USAT는 카드에 어플리케이션을 저장하고 실행할 수 있는 기능을 제공함으로서 USIM 카드가 주축이 되어 통신이 이루어지도록 한다. 사용자가 어플리케이션을 선택하게 되면 Proactive Command를 통해 USIM 카드가 단말기로 통신의 시작을 요청하고, 단말기로부터 데이터를 받는다. 즉 USAT를 사용함으로서 USIM 카드는 과거의 종속적인 개념에서 벗어나 사용자, 모바일, 네트워크 명령어의 시작이 되는 것이다.

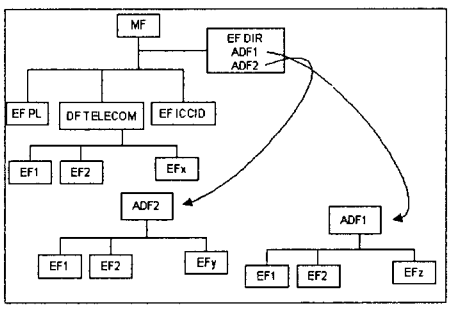


<그림 4> 기존의 APDU 명령어



<그림 5> USAT 명령어

2.2.3 USIM Card OS의 File 시스템 구조



<그림 6> USIM Card File 시스템 구조

USIM 카드는 계층적 구조를 지닌다. MF는 Master file로서 루트파일이 되며, 단 하나만 존재한다. DF는 Dedicated File로서, 다른 DF나 EF를 포함할 수 있다. EF는 Elementary File로서 가장 하위 계층의 디렉토리로 DF를 각각의 어플리케이션이라 볼 때, EF는 한 어플리케이션에 포함되는 함수들이라 볼 수 있다.

3. 쇼핑몰 마일리지 통합 관리 시스템

본 연구는, USIM 카드의 유효성을 입증하기 위하여, USIM 카드에 저장되는 어플리케이션의 개발을 목적으로 한다. 본 연구에서 제안한 시스템은 전자 지갑의 확장 시스템으로서, 서로 제휴되어 있는 각 쇼핑몰에서 축적한 마일리지를 USIM 카드내의 마일리지 통합 관리 어플리케이션을 통해 관리하는 것이다. 기존의 쇼핑몰 관리 서비스는 인터넷 상에서의 관리로서 사용자의 아이디와 패스워드만으로 보안을 하는 수준이므로, 개인 정보 유출의 문제가 발생할 가능성이 높다. 그러나 USIM 카드는 보다 더 강력한 보안 수단으로서 안전성을 높일 수 있다. 본 시스템의 가장 큰 특징은 소정의 프로그램을 카드내에 저장하여, 카드 자체의 연산을 통하여 마일리지를 관리한다는 점이다.

3.1 쇼핑몰 마일리지 통합 관리 시스템의 개발

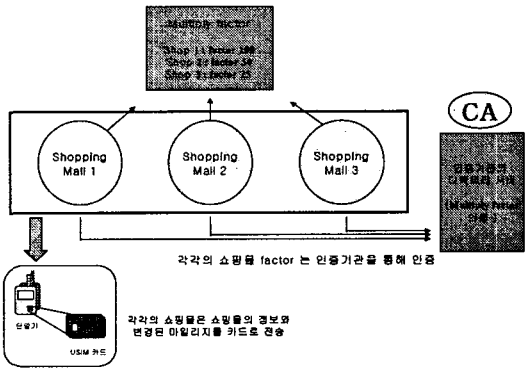
마일리지 통합 관리 시스템은 USIM 카드의 EEPROM에 저장되며, CPU를 통하여 연산작업을 수행한다. 쇼핑몰 통합 관리 서비스 어플리케이션은 서로 제휴되어 있는 쇼핑몰에서 마일리지를 받아서 USIM 카드내에 저장되어 있는 어플리케이션을 이용하여 마일리지를 통합하고 축적한다. USIM 카드에는 각 쇼핑몰의 ID와 쇼핑몰에서 축적한 마일리지, 통합적으로 적용된 마일리지를 저장하기 때문에, 오프라인 상에서도 저장 내역을 확인할 수 있다.

각 쇼핑몰에서의 마일리지는 Multiply를 이용하여 적용한다. Multiply factor는 각 쇼핑몰의 마일리지에 대한 가중치 값을 의미하는 것으로, 인증기관을 통해 인증을 받고, 인증기관의 디렉토리 서버에 저장이 된다. 사용자는 쇼핑몰을 통해 마일리지를 축적하고, 변경된 마일리지와 쇼핑몰의 정보를 카드로 전송한다. 카드내의 마일리지 통합 관리 어플리케이션을 통해, 각 쇼핑몰의 공인 인증된 Multiply factor를 적용하는 단계를 수행한다.

Java Card에 저장된 마일리지는 현금화가 가능해야 한다. 즉, Java Card에 저장되어 있는 또 다른 전자지갑과 같은 어플리케이션과의 공유를 통하여 현금화할 수 있도록 한다. 어플리케이션 구현 시, 쇼핑몰의 적용률이 변동할 경우를 고려하여, 적용률의

변동이 발생하는 경우, 쇼핑몰에서 쉽게 USIM 카드에 변동된 사항이 저장될 수 있도록 구현해야 한다.

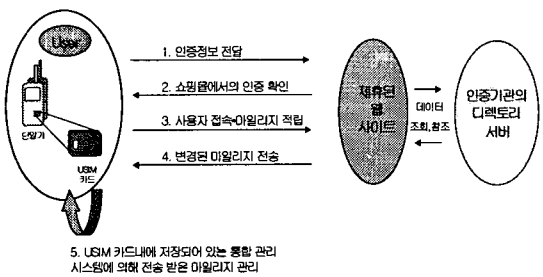
본 시스템은, Java Card를 기반으로 하여 자바언어로 구현되므로 Java Card와 Java 언어의 특징을 모두 적용시킬 수 있다. 자바언어로 생성된 class 파일은 USIM 카드에 탑재하기 위하여 Cap 파일로 변형한다. Cap 파일은 필요한 정보만을 압축한 파일로서 작은 용량을 지니기 때문에 USIM 카드내의 메모리에 저장하는 것이 가능하게 된다. 한 어플리케이션의 용량은 2k로 정도로 예상할 수 있으며, USIM 카드에는 여러 개의 어플리케이션을 탑재할 수 있다.



<그림 7> 쇼핑몰 마일리지 통합 관리 시스템

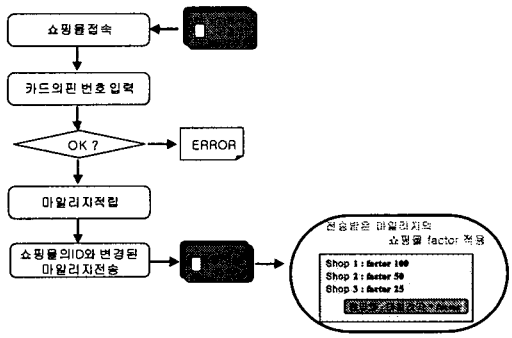
3.2 통합 쇼핑몰 마일리지 관리 시스템의 운영

사용자가 웹사이트를 접속하기 위해서는 인증정보의 교환이 필요하다. 쇼핑몰에 접속한 후 USIM 카드에 저장되어 있는 인증정보를 전송한다. 웹사이트는 인증정보를 확인한 후, 사용자에게 접속을 허용한다. 사용자는 쇼핑몰에서 마일리지를 적립한 후, 적립된 내용을 USIM 카드로 전송한다. 전송받은 마일리지는 USIM 카드내에 저장되어 있는 마일리지 통합 관리 시스템을 통해 마일리지를 관리되며, 일정량의 마일리지가 축적되면 현금화하여 사용할 수 있도록 한다.



<그림 8 >쇼핑몰 마일리지 통합 관리 시스템의 프로토콜

웹사이트를 접속하기 위해서 PIN Number를 입력하여야 한다. PIN Number는 유효숫자로 지정할 수 있으며, 유효숫자 이상의 입력을 받을 경우에는 에러 메시지를 전송하고, 접속을 거부한다. PIN Number를 입력하는 것은 인증서를 교환하기 이전 단계로서 보다 더 높은 안전성을 제공한다.



<그림 9> 쇼핑몰 마일리지 통합 관리 시스템 흐름도

4. 결론 및 향후과제

본 논문은, USIM 카드를 이용한 어플리케이션의 개발을 제안하였다. Java Card가 제공하는 어플리케이션의 개발의 용이성과, 뛰어난 독립성을 바탕으로 USIM 카드에 적합한 효율적인 어플리케이션을 제안하였다. 본 논문에서 제안된 마일리지 통합 관리 시스템은 USIM 카드의 메모리에 저장되는 어플리케이션으로서 한 개인의 독립적인 프로그램으로 작동된다. USIM 카드의 CPU를 통한 연산작용을 이용하여 마일리지를 직접 계산하고, 적립할 수 있는 프로그램으로서 적립된 마일리지의 현금화를 가능하게 한다. 아직 IMT2000 시장이 초기화 단계이기 때문에 USIM 카드를 이용한 다양한 어플리케이션의 개발이 뒷받침되어야 할 것으로 생각된다.

참고문헌

[1] Hansmann, Uwe (Edt) / Nicklous, Martin S. / Schack, Thomas / Seliger, Frank / Hansmann, Uwe / Springer Verlag "Smart Card Application Development Using Java" Springer Verlag 1999

[2] T. Trans and R. Cohen "Hybrid Recommender Systems for Electronic Commerce"

[3] Ivor Horton "Begining Java2" WROX 1999

[4] Chen "Java Card Technology for Smart Cards" Addison Wesley 2000

[5] 지식정보센터 "IMT 2000" 한국전자통신연구원 2001