IMT-2000 서비스 상에서의 Java Card를 이용한 M-commerce용 어플리케이션 개발

백장미[0] 홍인식
순천향대학교 정보기술공학부
bjm1453@hanmail.net, ishong@sch.ac.kr

Development of Application using Java Card in IMT-2000

Jang-Mi Baek[0] In-Sik Hong
Division of Information Technology Engineering, Soonchunhyang Univ.

요 약

이동형 무선 단말기의 사용이 급증함에 따라, M-commerce 시대로 바뀌고 있다. 특히 USIM 카드가 내장되어 있는 IMT-2000 서비스가 시작되면, 무선 인터넷 시장은 급속도로 발전할 것이다. 본 논문은 무선 인터넷 응용 프로그램의 개발을 위하여 USIM 카드 상에서의 Java Card를 활용한다. Java Card는 자바 언어를 사용하여 프로그램을 개발할 수 있으며, 다양한 어플리케이션의 개발이 가능하다. 본 연구는 Java Card의 유용성을 증명하기 위하여 실제 생활에 적용 가능한 지불 솔루션으로서 전자화폐 시스템과 마일리지 시스템을 개발한다. 즉, One 카드 개념으로서 USIM 카드 하나로 다양한 기능을 제공할 수 있다는 것을 증명한다.

1. 서 론

모바일 기기의 사용이 증가함에 따라, 상거래의 중심이 무선 인터넷으로 변하고 있다. 휴대폰이나 PDA와 같은 이동형 단말기를 이용하여 인터넷 서비스를 이용하며, 그에 따른 다양한 무선 인터넷 기술이 등장하고 있다. 특히 IMT-2000 (International Mobile Telecommunication-2000) 서비스에 사용되는 단말기에는 USIM(Universal Subscriber Identity Module) 카드를 내장함으로 인하여, 기존의 단말기보다 데이터의 저장기능과 프로세싱 기능이 확장된다. USIM 카드는 기본적으로 개인 인증 정보를 내장할 수 있으며, 스마트 카드의 OS인 Java Card을 사용으로 멀티 어플리케이션의 탑재가 가능하기 때문에 다양한 응용분야의 어플리케이션을 개발할 수 있다. 본 논문[1]에서는 Java Card의 특성을 활용하여, USIM 카드에 저장되는 어플리케이션의 개발을 목적으로 한다. 지불분야와 관련이 있는 전자화폐 시스템과 마일리지 시스템을 하나의 USIM 카드에 저장함으로써 Java Card의 유용성을 입증하고자 한다. 본 논문의 2장에서는 Java Card 기술의 특성과 구성에 대하여 설명하고, 3장에서는 모바일상에서의 지불 솔루션을 설명한다. 4장에서는 제안한 시스템의 시뮬레이션 수행 과정을 보여주며, 5장에서 결론으로 본 논문을 마친다.

2. Java Card 기술

USIM 카드 자체로는 응용 프로그램의 개발이 쉽지 않다. USIM 카드의 크기나 형태, 통신 프로토콜은 표준화 스펙이 있지만 내부 동작을 위한 작업은 제작사마다 다르다. 즉 제 3자가 독립적인 응용 프로그램을 개발하는 것은 거의 불가능하였으나 최근 USIM 카드를 위한 COS가 등장함으로써 어플리케이션의 개발이 용이해지고, 어플리케이션간의 이식성이 가능해졌다. 특히 Java Card는 모바일 인터넷 상에서 중심이 되고 있는 자바 언어를 사용하여 프로그램을 개발하기 때문에, 자바 언어의 특성을 최대한 활용할 수 있다[1][2][3].

2.1 Java Card 기술의 특징

(1) 어플리케이션 개발의 용이성

Java Card는 자바라는 고수준 언어를 사용함으로써 프로그램의 개발이 용이하다. Java Card는 표준 응용 프로그램 인터페이스와 공개적인 플랫폼을 제공하기 때문에, 어플리케이션의 개발자는 카드의 세부적인 차이에 관여하지 않아도 되며, 고수준의 프로그래밍 인터페이스를 이용하여 작업할 수 있다.

(2) 보안성

Java Card에 내장된 보안적인 특성들은 USIM 카드의 환경과 매치가 잘 이루어진다. USIM 카드는 개인 인증 정보나 전자화폐 기능을 담당하기 때문에 각각의 메소드와 변수들의 통제는 필수적이다. Java Card 의 플랫폼에서 동작되는 애플릿은 방화벽에 의하여 철저히 분리된다.

(3) 하드웨어의 독립성

Java Card 의 사용되는 하드웨어의 종류는 독립성을 지닌다. 즉, 어플리케이션의 개발은 CPU의 종류와 무관하다.

(4) 멀티 어플리케이션의 기능

Java Card는 전자지갑이나 인증, 로얄티, 의료 등의 다양한 응용 프로그램을 동시에 저장할 수 있으며, 애플릿 방화벽의 사용으로 응용 프로그램간의 데이터를 보호할 수 있다. 또한 전자지갑이나 로열티 등의 프로그램은 데이터의 공유가 필요하므로 공유 메커니즘을 통해 데이터를 공유할 수도 있다.

2.2 Java Card의 구조

Java Card는 JCVM(Java Card Virtual Machine)과 JCRE(Java Card Runtime Environment), APIs(Application Protocol Interfaces)로 구성되어 있다. JCVM은 컨버터와 인터프리터를 제공하며, JCRE는 애플릿을 관리한다. APIs는 Java Card의 어플리케이션을 위한 자바 패키지와 클래스를 정의한다.

2.3 Java Card 상에서의 어플리케이션 개발

Java Card는 매우 제한된 메모리를 가지고 있다. 제한된 메모리 상에서 어플리케이션을 개발하고 저장하기 위해서는 특수한 기법이 필요하다. Java Card는 자바 언어를 사용하여 프로

[1] 본 논문은 정보통신부의 지원을 받아 연구되었음

그램을 개발한다. 프로그래밍을 통해 생성된 class 파일은 Off-card상에서의 컨버터를 통하여 CAP 파일로 변환한다. CAP 파일은 Java Card의 제한된 메모리에 적합하게 압축된 형태의 파일로서, 대부분 2K 정도의 크기를 지닌다. 생성된 CAP 파일은 On-card 상에서 인터프리터를 통하여 실행된다.

3. 모바일 상에서의 지불 솔루션 제안

본 논문은 USIM 카드 상에서 Java Card를 이용한 지불에 관련된 어플리케이션을 설계한다. 즉, 모바일 기기를 통한 지불수단으로써의 전자화폐 시스템을 제안하였으며, 지불을 하였을 때 주어지는 마일리지를 관리하는 시스템을 제안하였다. Java Card 상에는 기본적으로 개인인증 정보가 내장되며, 개발된 어플리케이션은 업그레이드가 가능하다[4][5].

3.1 USIM 카드의 내장 데이터

UISM 카드는 모바일 상에서 사용되는 카드이므로, 개인 인증 정보가 필수적으로 내장된다. 상점과의 거래시 인증서의 교환을 통하여 상대방을 인증한다. 인증정보를 포함하여 지불에 관련된 금액 정보와 상점 정보 등을 내장해야 한다. 이 데이터는 USIM 카드의 EEPROM에 저장된다. 표 1은 USIM 카드가 전자화폐 기능과 마일리지 기능을 동시에 제공할 경우 USIM 카드에 내장되는 필수적인 데이터를 보여준다.

표 1. USIM 카드에 내장되는 데이터

이름	기술	바이트
Application Identifier (AID)	전자화폐와 마일리지 시스템의 AID	5-16
전자 지갑 ID	전자화폐와 마일리지 시스템의 ID	4
Application Expiration Date	어플리케이션 유효 날짜	3
Application Effective Data	어플리케이션 발효 날짜	3
Application File Locator (AFL)	Indicates the locationof the EFs related to a given application	252
Application Interchange Profile	Indicates the capabilities of the card to support specific functions in the application	2
Application Label	Mnemonic associated with the AID	1 - 16
Application Primary Account Number (PAN)	Valid cardholder account number	10
Application Primary Account Number (PAN) Sequence Number	Identifies and differentiates cards with the same PAN	1
Application Currency Code	Indicates the currency in which the account is managed according to ISO 4217	2
Application Transaction Counter (ATC)	Counter maintained by the application in the ICC (incrementing the ATC is managed by the ICC)	2
Current Balance	전자 화폐의 잔여 잔액	4
Maximum Balance	최대 잔액	4
Maximum Transaction Amount	1회 최대 거래액	4
Mileage Balance	마일리지 총액	4
Mileage of each shop	각각의 상점 마일리지	4
Certification Authority Public Key Index	Identifies the certification authority's public key in conjunction with the RID	1
Enciphered Master Personal Identification Number (PIN) Data	Transaction PIN enciphered at the PIN pad for online verification or for offline verification	8
Enciphered User Personal Identification Number (PIN) Data	Transaction PIN enciphered at the PIN pad for online verification or for offline verification	8
Issuer Public Key Certificate	Issuer public key certified by a certification authority	NCA
Customer Public Key Certificate	Customer public key certified by a certification authority	NCA
Customer Private Key	USIM 카드의 비밀키	32
Lower Consecutive Offline Limit	Issuer- specified preference for the maximum number of consecutive offline transactions for this ICC application allowed in a terminal with online capability	1
Personal Identification Number (PIN)	Try Counter Number of PIN tries remaining	1
Upper Consecutive Offline Limit	Issuer- specified preference for the maximum number of consecutive offline transactions for this ICC application allowed in a terminal without online capability	1
CAD ID Array	마일리지를 증가시켜야 할 상점 ID의 배열	var.
Transaction Log File	지불 관련 거래 기록 저장	var.
Remote Wallet Server IP Address	전자 지불 서버의 주소	4

3.2 전자화폐 시스템과 마일리지 시스템의 흐름도

그림 1은 쇼핑몰에서 물품을 구매한 후 USIM 카드상의 전자화폐 시스템을 통해 결재를 하는 과정이다. 쇼핑몰에서 구매한 금액에 대한 마일리지는 USIM 카드상에서 계산되어 적립된다. 개인인증서와 상점의 인증서는 인증기관을 통해 관리된다.

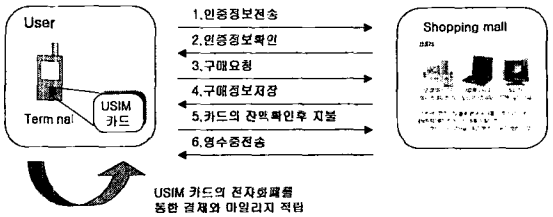

그림 1. 전자화폐와 마일리지 시스템의 흐름도

4. 시뮬레이션

본 논문은 단말기 상에서 USIM 카드를 이용하여 다양한 어플리케이션을 개발할 수 있다는 것을 보여주는 것이 목적이다. 즉, One 카드 개념으로서 하나의 카드로 여러 가지 기능을 통합하여 사용할 수 있다는 것을 보여준다. 본 시뮬레이션은 다양하게 개발할 수 있는 어플리케이션 중 전자화폐 시스템과 마일리지 시스템을 타겟으로 하였다. J 빌더를 이용하여 프로그램을 개발하였으며, 카드와 어플리케이션 사이의 통신은 *command*와 *response* 명령을 이용하였다. 상점에서 보내는 값은 임의로 정하여 TCP/IP 통신 프로토콜로서 전송하였으며, 전자화폐 시스템과 마일리지 시스템은 공유메커니즘을 통하여 서로의 데이터를 주고받을 수 있도록 하였다. 그 이외 인증 정보나 금액 정보 등의 중요 데이터는 방화벽에 의해서 보호된다. 본 시뮬레이션은 ISO 7816 스펙을 기준으로, Java Card를 지원하는 Gemplus의 Gemxpress 211을 사용하여 구현하였다.

4.1 어플리케이션의 install

Java Card의 off-card 상에 있는 컨버터를 통하여 생성된 CAP파일은 USIM 카드 상에서 사용하기 위하여 install 과정을 거쳐야 한다. install 과정을 위하여 install 메소드를 사용하였으며 install 메소드는 JCRE의 기본 애플릿 클래스로 정의되어 있다. install 과정은 한 번만 이루어지며, install된 프로그램은 select 메소드를 통하여 선택된 후, 실행된다. 그림 2에서는 전자화폐와 마일리지 시스템이 install되는 과정으로써 로드될 때의 크기와 시간을 보여준다. 전자화폐 시스템의 크기는 약 2K 정도이며 마일리지 시스템은 약 1K정도이다[6][7][8].

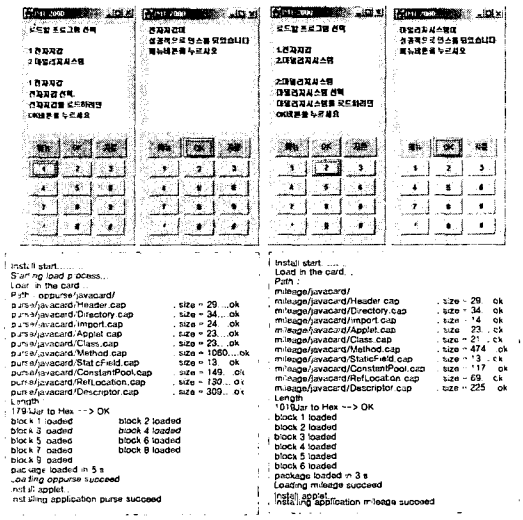

그림 2. 전자화폐 시스템과 마일리지 시스템의 install

4.2 어플리케이션의 select

install된 프로그램은 select 메소드를 통하여 선택된다. 한번에 여러 개의 어플리케이션을 실행할 수 없으므로, 사용할 어플리케이션을 select 해주어야 한다. USIM 카드는 각각의 어플리케이션의 AID(Application Identifier)를 지닌다. select 명령을 보내면, JCRE는 USIM 카드에 내장되어 있는 각각의 AID와 비교하여 해당 프로그램의 사용권한을 준다. 만약 USIM 카드에 저장되어 있는 AID와 일치하지 않거나 select된 상태일 경우에는 재 select 명령을 실행하거나 deselect 명령을 실행한다. 그림 3는 select 명령을 통한 어플리케이션 선택 과정을 보여준다. 본 시뮬레이션에서 사용한 전자화폐 시스템의 AID는 "A0 00 00 00 18 FF 00 00 00 00 00 00 00 00 01 02" 이며, 마일리지 시스템의 AID는 "A0 00 00 00 18 FF 00 00 00 00 00 00 00 00 00 02" 이다.

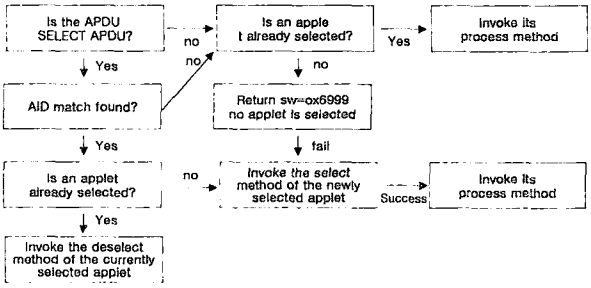

그림 3. USIM 카드의 어플리케이션 select 과정

4.3 전자화폐 시스템과 마일리지 시스템

본 시스템은 상품의 구매단계에서의 결재와 충전과정을 보여준다. 임의의 상점을 애플릿으로 구현하여 상품의 금액과 충전금액을 전송하며, 동시에 상품을 구매하였을 경우의 마일리지도 USIM 카드로 전송한다. USIM 카드의 자체적인 연산기능을 통하여 잔액을 확인할 수 있으며, 충전기능과 마일리지 저장기능을 수행할 수 있다. 그림 4에서와 같이, 상품의 구매와 충전과정에서는 PIN(Personal Identification Number)를 요구한다. 특히 충전 시에는 상호 인증 단계를 요구하므로, 사용자와 단말기 사이의 인증을 실행한다. 그림 5는 인증 단계상에서 생성되는 key값으로서 sessionkey는 매번 새로운 값을 생성한다.

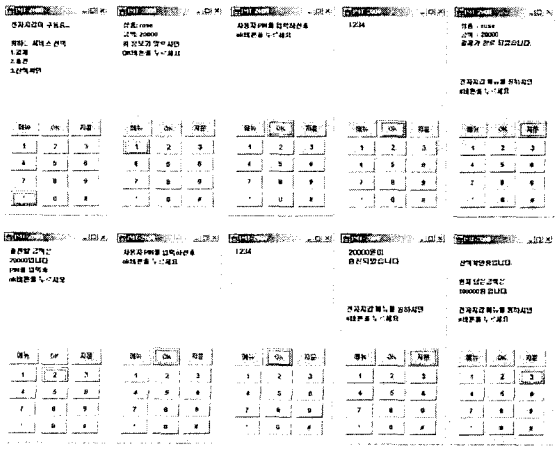

그림 4. 전자지갑의 구매와 충전 과정

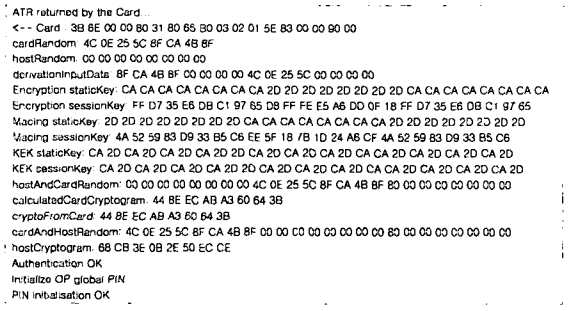

그림 5. USIM 카드와 단말기의 인증 과정

그림 6는 상품구매 시 마일리지를 적립하는 과정이다. 마일리지 펙터는 0.1로 가정하여 USIM 카드의 CPU를 통해 계산된다. 마일리지 펙터는 상점의 인증서에 포함되어 있으며 인증기관에 의해 관리되는 값이다.

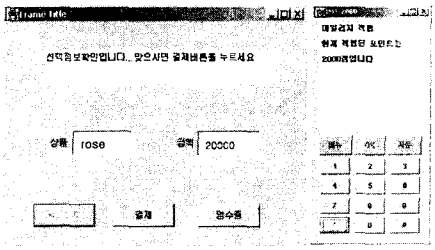

그림 6. 마일리지 적립 과정

5. 결론

본 논문은 무선 인터넷 응용 프로그램의 개발을 위하여, USIM 카드 상에서의 Java Card를 활용하였다. USIM 카드상에서의 모바일 기기를 사용하여 실제생활에서 서비스가 가능한 전자화폐 시스템과 마일리지 시스템을 개발함으로써 Java Card의 유용성을 증명하였다. 앞으로, IMT-2000서비스가 시행되면 USIM 카드를 이용한 다양한 서비스가 진행될 것이다. 그러나 아직은 미흡한 단계이므로 관련 기술의 연구가 필요하다고 사료되며, Java Card와 같은 USIM 카드의 COS를 이용하여 다양한 비즈니스 모델을 창출해야 할 것이다.

참고문헌

[1]Zhiqun Chen, "Java Card Technology for Smart Cards", Addison Wesley, 2000.
[2]W.Rankl and W.Effing, "Smart Card Handbook", John Wiley& Sons, 1997.
[3]Java Card Forum, http://www.javacardforum.org/
[4]백장미, 강병모, 홍인식, "Java Card를 이용한 인터넷 쇼핑몰 마일리지 통합 관리 시스템에 관한 연구", 정보과학회, 제28권 제2호, pp. 214-216, 2001.
[5]하남수, 홍인식, "IMT-2000에서의 USIM을 위한 구조 설계 및 응용 프로그램 구축에 관한 연구", 정보처리학회, 제8권 제 1호, pp. 627-630, 2001.
[6]Gemplus, http://www.gemplus.com/
[7]Ivor Horton, "Begining Java2", WROX, 1999.
[8]Ken Armold and James Gosling, "The Java Programming language", Addision Wesley, 1998.