M-Commerce 상에서의 안전한 지불 시스템에 대한 연구

백장미, 홍인식
순천향대학교 정보기술공학부

A Study on about secure Payment System on M-Commerce

Jang-Mi Baek, In-Sik Hong
Division of Information Technology Engineering, Soonchunhyang Univ.
E-mail : bjm1453@hanmail.net, ishong@sch.ac.kr

요 약

모바일 통신의 수요가 증가하면서 유선상에서의 상거래 형태가 무선으로 변화하고 있다. 무선 매체를 통한 지불 형태가 다양화되고 있으며 무선 거래의 이용률도 증가하고 있는 추세이다. 그러나 무선 통신은 유선 통신에 비하여 보안적 측면에서 공격의 대상이 되기 쉽다. 따라서 본 논문에서는 무선 통신 상에서의 안전한 전자상거래를 위하여 USIM을 이용한 지불 솔루션을 제안한다. USIM은 모바일 기기에 내장되는 스마트 카드 형태의 개인 인증 정보를 저장할 수 있는 모듈로서, 추가적으로 전자화폐의 기능을 담당한다. 제안한 솔루션의 유용성을 증명하기 위하여 Java 기반의 USIM을 이용하여 J2ME 환경상에서 전자화폐 시스템을 구현하였다.

1. 서론

모바일 기기의 수요가 증가하면서 모바일 기기를 통한 인터넷 서비스와 전자 상거래를 위한 서비스가 증가하고 있다. 무선 통신이 활성화되고 있는 이유는 이동성고 개인 휴대성을 제공하기 때문이다. 그러나 유선 통신에 비하여 보안적 측면에서 공격의 대상이 되기 쉽다. 1세대나 2세대 통신 시스템은 강력한 보안 시스템을 제공하지 못하였기 때문에 인가되지 않은 것들의 공격에 대한 해결책이 미흡했다. 그러나, 제 3 세대 통신으로 서비스가 제공될 예정인 IMT-2000 (International Mobile Telecommunication-2000)은 보안적인 측면을 강화하기 위하여 USIM(Universal Subscriber Identity Module)을 내장한다. USIM은 개인의 인증 정보를 저장할 수 있는 모듈로서 스마트 카드의 형태의 시스템이다. 즉, 모바일 기기만으로 강력한 보안성을 제공하기에는 부족하기 때문에 스마트 카드와의 연계를 통하여 높은 보안성을 제공할 수 있으며 더불어 모바일 기기가 지니는 이동성과 개인 휴대성 등의 장점을 살릴 수 있다. 본 논문은, IMT-2000 서비스 상에서 USIM을 이용하여 보다 안전하고 편리하게 지불을 할 수 있는 솔루션을 제안한다. 특히 Java 기반의 USIM을 이용하여 개인의 인증 정보를 내장하고 보호하며, 전자화폐 기능을 추가함으로서 안전한 지불 시스템을 구현한다. 2장은 USIM의 기능과 특징에 대하여 설명하고, 3장은 모바일 상에서의 지불 솔루션을 설명한다. 4장은 제안한 시스템의 구현을 위한 메소드와 시나리오를 설명하고 5장에서 결론으로 논문을 마친다.

본 연구는 정보통신부의 지원을 받아 연구되었음

2. USIM(Universal Subscriber Identity Module)

USIM은 개인의 인증 정보를 저장하기 위한 모듈이다. 모바일 기기에 내장되는 핵심 요소로서 공개키 기반 구조의 암호화 시스템을 적용하여 보안성을 제공한다. 초기의 통신 시스템은 제한적인 용량과 계산능력으로 공개키 방식과 같은 사이즈가 큰 암호화 알고리즘의 적용이 어려웠다. 그러나 USIM은 확장된 메모리와 CPU를 통해 공개키 암호화 방식을 수행하기에 적당한 시스템이다.

3. 모바일 상에서의 지불 솔루션

본 논문은 Java 기반의 USIM을 이용한 지불에 관련된 지불 솔루션을 제안하고 설계한다. 즉, 모바일 기기를 통하여 물품을 구매하고 결재와 지불을 위한 시스템을 제안한다. 결재를 위한 지불방법은 다양하게 적용될 수 있으나 본 논문은 USIM에 내장되는 전자화폐를 이용하며 결재를 수행하며, Online 상에서의 결재와 Offline 상에서의 결재를 모두 수행할 수 있는 솔루션을 제안한다. Java 기반의 USIM을 적용함으로 멀티어플리케이션의 개발과 탑재가 가능하며, 개발된 어플리케이션은 업그레이드가 가능하다. Java 기반의 USIM을 사용함으로 자체적인 보안기술과 Java 언어 상에서 제공하는 보안기술을 통해 보안성을 높였으며 인증서의 구조는 WPKI 방식을 적용하였다.

3.1 USIM 의 내장 데이터

UISM은 모바일 상에서 사용되는 인증시스템으로, 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 의 EEPROM에 저장된다. 표 1은 USIM은 결재 시스템을 위하여 필요한 필수적인 데이터를 보여준다.

표 1. USIM에 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 Date	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 현재 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 dentification 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 완료 거래 기록 저장	var.
Remote Wallet Server IP Address	전자 지불 서버의 주소	4

3.2 WPKI를 통하여 인증서를 받는 과정

모바일 기기로 인증서를 전송 받는 것은 WPKI 구조를 통해서 받는다. 그림 1은 인증서를 모바일 기기를 통해서 받는 과정을 보여주는 그림이다.

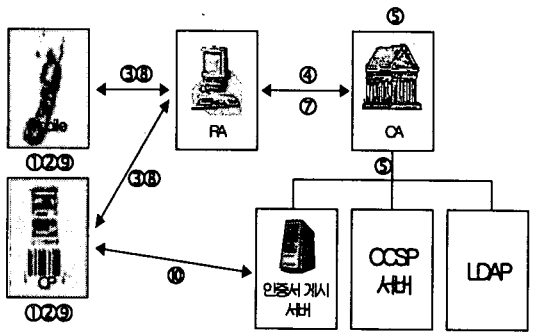

그림 1. 모바일 기기를 통한 인증서 발급 과정

우선 인증서의 WPKI 참조번호와 인가 코드를 입력한 후 키를 생성한다. 생성된 키로 인증서 요청 양식 생성하고 RA와 SSL을 통해 인증서 요청 양식 전송한다. 전송 받은 인증서 요청양식을 CA에 전송한 후, 전송된 데이터의 이상 유무 및 인증서 발급 가능 여부 등을 검증하고 검증이 확인되면 인증서 발급한다. 발급된 인증서를 LDAP 및 인증서 게시 서버에 저장한 후, 인증서를 게시한다. 게시된 인증서는 해당 URL을 RA에 재전송 해주고, CA가 되돌려준 URL을 모바일 기기에도 역시 재전송 해준다. 모바일 기기는 전송 받은 URL을 저장하고 메일 인증서 게시 서버로부터 갱신된 인증서를 수신 받는다.

3.2 장바구니 결재 시스템의 흐름도

그림 1은 쇼핑몰에서 구매하고자 하는 물품을 모바일 기기의 장바구니에 담고 통합적으로 결재하는 과정이다. 물품의 구매는 USIM의 전자화폐를 통하여 결재되며, 모든 계산 과정은 USIM에 내장되어 있는 CPU를 통해 이루어진다. 본 시스템은 기존에 제공되고 있는 시스템을 확장한 시스템으로 결재만을 위한 기능을 제공하는 것이 아니라, 모바일 기기를 통해 직접 물건을 선택하고 구매할 수 있는 시스템이다. 즉 모바일 기기의 제약적인 조건을 가만하여 쇼핑을 위한 가상몰이 존재한다. 쇼핑몰은 각각의 상품 번호가 존재하며 각각의 물품의 상품 번호를 모바일 기기에 입력하면 상품 번호에 해당하는 물품의 이름과 가격 등의 정보를 볼 수 있다. 구매하고자 하는 물품을 장바구니에 담은 후 USIM의 전자화폐를 통하여 결재를

한다. 각각의 상품에 대한 구매는 마일리지로 적립되어 USIM에 내장된다. 개인인증서와 상점의 인증서는 인증기관을 통해 관리된다.

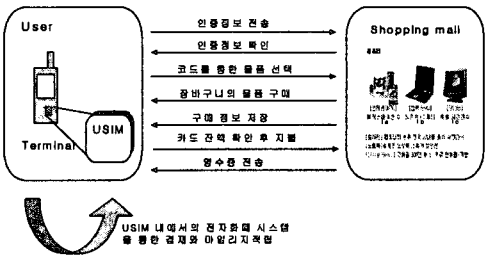

그림 2. 제안한 시스템의 흐름도

4. 시스템 구현

본 논문의 목적은 단말기 상에서 USIM을 이용하여 개인의 인증 정보를 저장함과 동시에 전자화폐 기능을 수행한다는 점이다. 즉 하나의 USIM 안에 다양한 어플리케이션을 개발할 수 있다는 것을 의미한다. 시스템 구현은 Java 기반의 USIM을 제공하는 Gemplus 211을 이용하였으며, 단말기와의 통신을 위하여 command와 response 명령을 서로 주고 받는 APDU (Application Protocol Data Unit)을 사용하였다. USIM 상에서의 모든 데이터는 기본적으로 방화벽과 암호화 알고리즘을 통해 보호되며, 서로 다른 애플릿 간의 데이터 공유가 필요할 경우 데이터의 공유메커니즘을 통하여 데이터를 주고받을 수 있다. 본 논문에서의 시스템은 ISO 7816 스펙을 기준으로 개발하였다.

4.1 어플리케이션의 install

Java Card의 off-card 상에 있는 컨버터를 통하여 생성된 CAP파일은 USIM 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 과정으로 로드될 때의 크기와 시간을 보여준다. 생성되는 어플리케이션의 크기는 대략 1-2K의 크기로 생성이 된다.

4.2 어플리케이션의 select

install된 프로그램은 select 메소드를 통하여 선택된다. 한번에 여러 개의 어플리케이션을 실행할 수 없으므로, 사용할 어플리케이션을 select 해주어야 한다. USIM의 어플리케이션은 각각의 AID(Application Identifier)를 지닌다. select 명령을 보내면, JCRE를 통하여 USIM에 내장되어 있는 각각의 AID와 비교한다. 즉 AID의 비교를 통하여 해당 프로그램의 사용권한을 줄 수 있다. 만약 USIM에 저장되어 있는 AID와 일치하지 않거나 select된 상태일 경우에는 재 select 명령을 실행하거나 deselect 명령을 실행한다. 그림 3은 USIM 상에서 select 명령을 수행하는 과정이다.

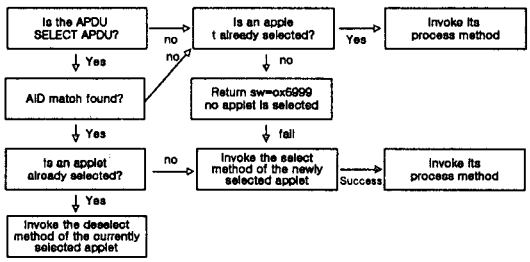

그림 3. USIM 상에서의 어플리케이션 select 과정

4.3 시나리오

본 시나리오는 Java 기반의 USIM 상에서 모바일 기기를 통한 결재 시나리오이다. Gemplus 사에서 제공하는 Gemxpress 211을 이용하여 구현할 수 있으며, Java Card의 특성을 이용하여 구현할 수 있다.

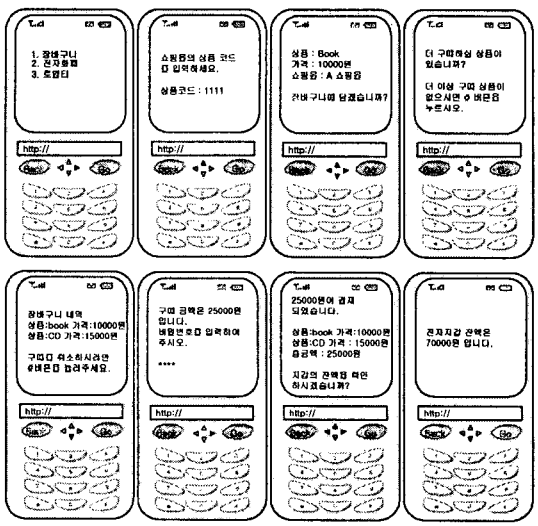

그림 4. 모바일 기기를 통한 결재 시나리오

Step1 : 모바일 기기를 통하여 장바구니 시스템을 선택한다.

Step2 : 장바구니에 물품을 담을 수 있는 화면이 디스플레이 되면 쇼핑몰에서 제공되는 각각의 물품 코드를 입력한다. 코드를 입력한 후 go 버튼을 클릭 한다.

Step3 : 상품 코드를 입력하면 해당 상품의 상품명과 가격 등의 정보를 모바일 기기로 전송한다. 데이터를 확인한 후 장바구니에 담기를 위하여 go 버튼을 클릭 한다.

Step4 : 장바구니에 담고자 하는 상품이 한 개 이상일 경우를 위하여 장바구니에 물품을 담는 단계를 반복한다. 더 이상의 구매 물품이 없으면 다음 단계를 수행한다.

Step5 : Step2-Step4의 과정을 반복한 후 장바구니에 담겨 있는 내역을 확인 할 수 있다. 구매할 물품이 확정이 되면 구매를 위한 버튼을 클릭 한다.

Step6 : 물품의 대금을 지불하기 위하여 USIM에 저장되어 있는 전자화폐에 접속한다. 안정성을 필요로 하기 때문에 전자화폐를 사용하기 위한 비밀 번호를 입력한다. 번호가 확인되면 결재를 완료한다.

Step7 : 전자화폐를 통하여 물품의 금액을 결재한 후 결재된 내역을 화면으로 디스플레이 해준다. 즉 영수증을 보여 주는 단계이다. 확인이 된 후 전자화폐에 남아있는 금액을 확인할 수 있다.

Step8 : 전자화폐에 남아있는 잔액을 확인한다.

5. 결론

모바일 통신의 수요가 증가하면서 무선매체를 통한 지불 형태가 다양화되고 있으며 무선 거래의 이용률도 증가하고 있는 추세이다. 그러나 무선 통신은 유선 통신에 비하여 보안적 측면에서 공격의 대상이 되기 쉽다.

따라서 본 논문에서는 무선 통신 상에서의 안전한 전자상거래를 위하여 USIM을 이용한 지불 솔루션을 제안한다. 즉 단말기와 USIM의 연계를 통하여 보안성 측면을 강화하여 안전하게 전자상거래를 할 수 있다. USIM은 개인 인증 정보를 저장할 수 있는 모듈로서, 추가적으로 전자화폐의 기능을 담당한다. 제안한 솔루션의 유용성을 증명하기 위하여 Java 기반의 USIM을 이용하여 J2ME 환경상에서 전자화폐 시스템을 구현하였다. 아직, IMT-2000 서비스는 준비중에 있으며 USIM을 연계하여 사용할 수 있는 다양한 어플리케이션의 개발이 미흡한 실정이다. 특히, 보안적인 측면을 강조하는 다양한 지불 시스템의 개발과 연구가 필요하다고 사료된다.

[참고문헌]

[1] 3GPP, http://www.3gpp.org/

[2] UMTS 23.01, "UMTS Network Architecture"

[3] Ramasami, "Security, Authentication And Access Control For Mobile Communications"

[4] G.Horn, B.Preneel, "Authentication and payment in future mobile systems", LNCS, Vol.1485, 1998

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

[6] Ivor Horton, "Beginning Java2", WROX

[7] W.Rankl and W.Effing, "Smart Card Handbook", John Wiley, 1997

[8] Java Card Forum, http://www.javacardforum.org/

[9] Gemplus, http://www.gemplus.com/

[10] 백장미, 강병모, 홍인식, "Java Card를 이용한 인터넷 쇼핑몰 마일리지 통합 관리 시스템에 관한 연구", 정보과학회, 제28권 제2호, pp. 214-216, 2001

[11] 하남수, 홍인식, "IMT-2000에서의 USIM을 위한 구조 설계 및 응용 프로그램 구축에 관한 연구", 정보처리학회, 제 8권 제 1호, pp. 627-630, 2001