M-Commerce를 위한 자바 모바일 플랫폼 기반의 전자지불 구현 방안

박남제*, 신균호*, 최영진*, 송유진**
*(주)뉴레카 부설 정보통신연구소
**동국대학교 정보산업학과
e-mail:njpark@newreka.com

An Implementation strategy of mobile electronic payment based on java mobile platform for M-Commerce

Nam-Je Park*, Kyun-Ho Shin*, Young-Jin Choi*, You-Jin Song**
*Institute of Information & Communication
**Dept. of Information Industry, Dongguk University

요 약

본 논문에서는 자바 모바일 플랫폼을 기반으로 하는 M-Commerce 보안 플랫폼을 검토하고, J2ME 기반 CLDC와 MIDP를 이용해서 M-Commerce 전자지불을 위한 휴대용 전자지갑 구현방안을 제시한다. 본 논문에서 제안한 방안은 무선 인터넷 환경에서 신용카드 결제 방식으로 지불할 경우 관련 중요 정보를 안전하게 전송하고, 대금 결제를 할 수 있도록 한다. 그리고, 무선인터넷 응용프로토콜 WAP 방식의 보안을 고려한 WTLS 보안 메커니즘을 이용하고, J2ME 기술을 기반으로 하기 때문에 향후 IMT2000에서도 사용 가능하다.

1. 서론

무선 인터넷을 기반으로 하는 M-Commerce는 기존 E-Commerce에서 제공하기 힘들었던 이동성(Mobility), 편재성(Ubiquity), 그리고 이로부터 발생하는 위치 기반 서비스(Location based service) 제공이 가능하므로 여러 가지 이점이 있다. 이와 함께 안전한 무선인터넷 서비스를 제공하기 위해서는 상호운영성(interoperability), 확장성(scalability), 효율성(efficiency), 신뢰성(reliability) 및 보안성(security)을 고려하여야 한다. 특히 무선인터넷에서의 정보보호는 전송계층 및 응용계층에서 접근이 이루어져야 하고 무선 환경의 제약사항을 고려하여야 한다. WAP 방식인 경우, 무선 게이트웨이로 인해 단대단 보안(End-to-End Security)을 제공하기가 어렵다는 문제가 있으며 이를 해결할 수 있도록 해야 한다. 또한 M-Commerce 환경에서 다양한 응용서비스를 제공하기 위해 플랫폼 독립적인 어플리케이션 운영기능을 제공해야 한다.

보안상 매우 취약한 신용카드를 대체할 수 있는 휴대폰을 이용해 오프라인의 지급 결제를 수행하는 전자지갑 모델은 기존 신용카드의 안전을 극복하는 편리한 방법을 제공한다. 이러한 관점에서 본 논문에서는 자바 모바일 플랫폼 기반의 전자지불 기능을 구현할 수 있는 방안을 검토한다. 즉, 무선 인터넷 응용 프로토콜인 WAP을 중심으로 J2ME (Java 2 Micro Edition) 자바 플랫폼과 연결한 단말기의 브라우저를 탑재하여 M-Commerce 전자지불을 위한 휴대용 전자지갑의 구현방안을 제안한다. 또한 WTLS를 고려한 M-Commerce의 보안 플랫폼을 제시함으로써 기존 지불 방식보다 안전성이 향상되고 서비스 제공의 효율성을 높일 수 있을 것으로 기대된다.

2. M-Commerce의 개요

M-Commerce는 무선인터넷서비스나 이동컴퓨팅서비스 양방향에서 제공될 수 있고, 휴대형 단말기 및 통신 네트워크를 통해 인터넷 혹은 인터넷 유사서비스를 제공받으며 이루어지는 정보, 서비스, 재화에 대한 금전적인 거래로서 정의할 수 있다[1]. 따라서, M-Commerce는 무선 단말기와 무선망을 통한 상품(Goods), 용역(Service) 및 정보(Information)의 상업적 거래를 의미한다. M-Commerce의 구성도는 그림 1과 같이 나타낼 수 있으며, M-Commerce의 일반적인 구분은 표 1로서 설명된다[5].

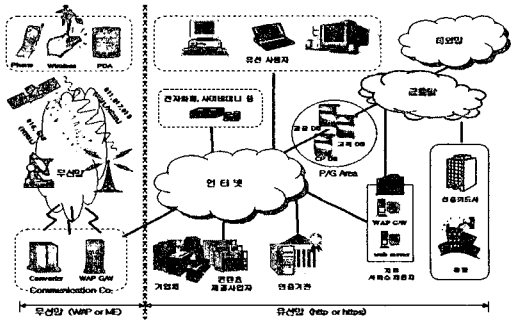

그림 1. M-Commerce의 구성도

표 1. M-Commerce의 구분

구 분	의 미
B2C	모바일 뱅킹, 쇼핑, 티켓팅, 경매 및 광고 등
B2B	모바일 공급관리, 사업관리 등
M2M (Machine to Machine)	향후 Bluetooth 등의 기술을 이용하여 이동 통신 네트워크를 통하지 않고 단말기를 신용 카드화하여 소액물품 구매 등에 사용하는 것

현재 국내에서 제공되는 M-Commerce는 이동통신사를 중심으로 M-Commerce와 관련 다양한 서비스를 제공하고 있지만 대부분 간단한 B2C형태로 벨소리 다운로드(건당 100원), 캐릭터 다운로드, 게임 등이 주류를 이루고 있는 상황이다. [표 2 참조]

표 2. 국내 M-Commerce 서비스 현황 및 동향

구분		SK텔레콤	신세기통신	한국통신 프리텔	한통엠닷컴	LG 텔레콤
브랜드명		Ntop	itouch017	Personet	M-Life	eZ web
접속방식		WAP	WAP	ME	ME	WAP
상용시기		2000.2.	1999. 12.	1999. 9.	2000. 1.	1999. 5.
브라우저	제공업체	에릭슨	Phone.com	MS	MS	Phone.com
	변형여부	자체변형	그대로 사용	자체변형	그대로 사용	그대로 사용
사용언어	Script 언어	WML	HDML/WML	m-HTML	m-HTML	HDML/WML
	버전	AUR 3.0	UP 3.2 / UP 4.0	ME 1.1 / ME 1.2	ME 1.1 / ME 1.2	UP 3.2 / AUR 3.0
이미지 규격		wBMP, SIS	wBMP, SIS	nBMP, SIS, TOY,GIF	TOY	wBMP, SIS
컨텐츠수	무료	2,771	582	410	973	1,005
	유료	500	없음	없음	11	없음
	계	3,721	582	410	984	1,005
보안솔루션		128 비트	Phone.com (48비트)	소프트포럼 (128비트)	소프트포럼 (128비트)	Phone.com (48비트)
주요서비스		전자상거래, 전자복권, 항공권예약, CNN뉴스, 위치정보 등	신용카드조회, 주식정보, 원격구매 등	인터넷쇼핑, 교통정보, 예약·예매, 주식정보, 위치정보 등	이동 쇼핑, 티켓팅, 뱅킹, 카드결제 등	교통돈(버스 등), 주식정보, 전자메일, 교량탐지, 경매, 게임 등
요금체계	정액요금제	90분 (5500원)	100분 (5500원)	120분 (4500원)	120분 (4500원)	150분 (5000원)
		180분 (9900원)	200분 (9900원)	240분 (8400원)	240분 (8500원)	300분 (9900원)
	일반요금제	일반 17원	일반 16원	평상 17원	평상 16원	오전 12원
		할인 12원	할인 12원	할인 12원	할인 12원	오후 16원
		심야 8원	심야 8원	심야 8원	심야 8원	새벽 8원

3. 자바 모바일 플랫폼과 M-Commerce 보안 플랫폼의 구성

3.1 자바 모바일 플랫폼의 구성

무선 인터넷의 대표적인 무선 응용프로토콜 표준방식에는 WAP(Wireless Application Protocol), ME(Mobile Explorer) 및 i-Mode 방식이 있다. 그림 2는 각 방식의 프로토콜 스택을 나타내고[2], 표 3에서 각 방식의 장·단점을 비교한다.

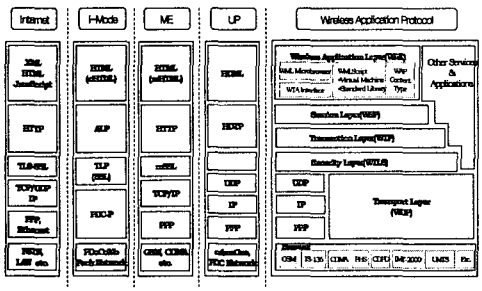

그림 2. 무선 응용프로토콜 방식의 비교

표 3. 무선 응용프로토콜 방식의 장·단점 비교

구분	WAP	ME	i-MODE	AnyWeb
제공업체	WAP포럼	MS, 퀄컴	NTT DoCoMo	삼성전자, AI-net
컨텐츠 기술언어	WML/WMLScript	Mobile-Html	Compact-html	s-HTML
단말기 브라우저	WAP 브라우저	Mobile Explorer	Compact Netfront	AnyWeb
전송 프로토콜	WSP/WTP/WDP	HTTP	HTTP	HTTP
보안계층	WTLS / SSL	SSL (mSSL)	SSL	MMS
단대단 보안	WAP Gateway와 기존 웹서버와 통합추진	무선단말이 기존 HTML 포맷 수용	무선단말이 기존 HTML 포맷 수용	서버에 MMS설치
인증서 형식	무선용 인증서	X.509 v3 인증서	X.509 v3 인증서	
PKI	WAP PKI			

자바의 무선환경 분야에서의 진화는 매우 빠르게 움직이고 있다. 주요 무선망 사업자와 단말기 제조업체들이 자바를 선택하는 이유로는 대체로 다음의 요소로 정리할 수 있는데, 무선 인터넷 환경에서 자바 모바일 플랫폼의 필요성은 다음과 같다[10].

- 동적 어플리케이션의 다운로드 서비스 기능 제공
- 플랫폼간의 호환성 제공
- 향상된 인터페이스의 표현
- 네트워크 환경과의 비연결성 고려
- 무선환경의 종단간 보안문제 해결책

WAP, ME, i-Mode의 종단간 보안 문제를 해결하지 못하는 상황에서 자바는 이미 훌륭한 보안 모델을 갖고 있으며, 무선 네트워크에서의 보안문제를 해결할 수 방안을 제시할 수 있다는 점이 자바의 모바일 환경의 필요성이라고 할 수 있다.

자바 모바일 플랫폼은 J2ME 기반의 CLDC(Connecte Limited Device Configuration)와 MIDP(Mobile Information Device Profile)로 나타내어질 수 있는데, CLDC는 128~512K의 메모리 여유공간과 16~32비트 프로세서, 저전력 소모, 네트워크 연결성을 가진 디바이스를 목표로 하고 있다. 보안 문제에 있어서는 보안 모듈 자체가 CLDC 구현보다 크기 때문에 저 수준의 가상머신 보안과 애플리케이션 레벨의 보안을 제공한다. 그리고, MIDP는 Java API의 한 묶음으로, CLDC와 함께 셀룰러 폰, 양방향 삐삐와 같은 이동 정보 단말기를 위한 J2ME 어플리케이션 운영 환경을 제공한다. MIDP는 사용자 인터페이스, 비휘발성 저장장치, 네트워킹, 그리고 어플리케이션 모델에 대한 정의를 제공한다. 또한, MIDP는 최종 사용자가 동적으로 자신의 디바이스에 어플리케이션을 설치하는 방법을 기본으로 제공한다. JAM(Java Application Manager)은 CLDC /MIDP 플랫폼의 새로운 어플리케이션 모델을 지원하기 위한 어플리케이션 관리 소프트웨어이고, 그 역할은 MIDP 어플리케이션인 MIDlet을 다운로드하여 설치, 업그레이드, 실행, 삭제하는 것이다.

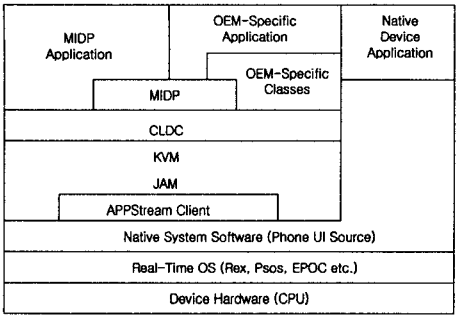

그림 3. J2ME 기반의 CLDC/MIDP 구조

3.2 M-commerce 보안 플랫폼의 구성

본 논문에서 제안한 M-Commerce 보안 플랫폼의 구성은 그림 4와 같다.

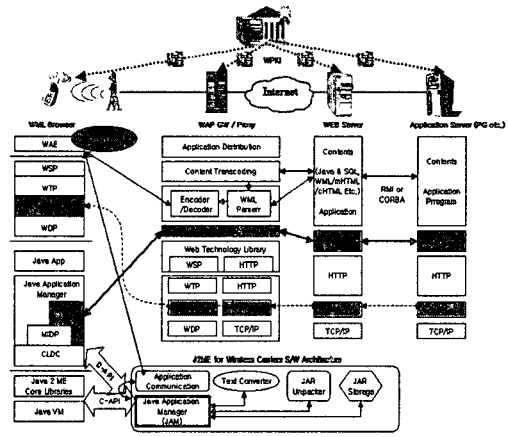

그림 4. M-commerce 보안 플랫폼 구성

M-Commerce 보안 플랫폼의 무선 응용프로토콜 부분에서의 보안은 WAP 보안모델을 기반으로 WTLS를 적용한다. 현재 적용된 WTLS Client/Server API의 모델을 보면 그림 5와 같다.

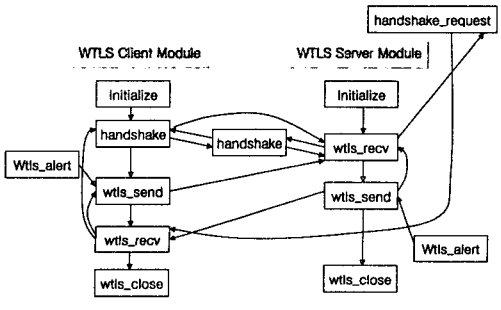

그림 5. WTLS Client/Server API 모델

한편, M-Commerce 보안 플랫폼 상에서 안전한 지불처리를 하기 위해 필요한 암·복호화 과정을 살펴보면 그림 6과 같다.

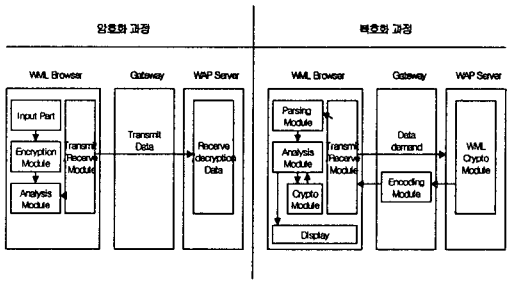

그림 6. 단말기 부분에서의 암/복호화 과정

4. 자바 모바일 플랫폼 기반의 전자지갑 구현방안

4.1 M-Commerce 환경의 전자지불 처리 흐름

본 장에서는 본 논문에서 제안한 휴대용 전자지갑을 이용한 무선환경에서의 지불처리 흐름의 개략적인 구성을 그림 7과 같이 나타낸다.

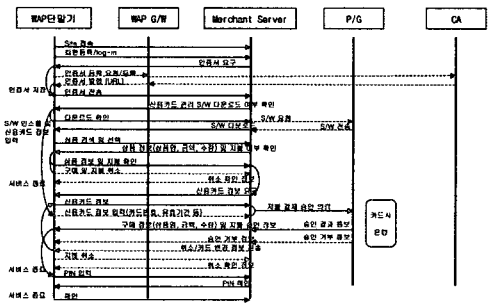

그림 7. 전자 지불 처리 흐름도

M-Commerce 보안 플랫폼을 기반으로 하는 안전한 전자지불을 위한 상호 키 처리절차에 따른 구매 및 지불처리 흐름도는 그림 8과 같다.

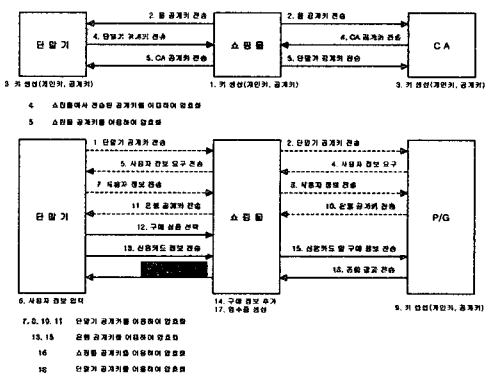

그림 8. 키 교환 처리절차에 따른 구매 및 지불 처리 흐름도

4.2 전자지갑 기능 및 화면 구성

M-Commerce를 위한 휴대용 전자지갑의 기능구성은 그림 9와 같으며, 기능에 대한 개략 설명은 다음과 같다.

- 지불처리 : 신용카드 정보, 사용자정보를 암호화하여 Payment Gateway에 전송
- ID, Password 관리 : 전자지갑에 사용자의 ID 및 패스워드를 등록
- 사용자 정보관리 : 사용자의 인적사항에 대한 정보를 관리
- 키 관리 : 사용자의 공개키/비밀키를 생성 관리
- 인증서 관리 : 인증서 요청 및 URL 저장
- RSA/ECC 암호화 알고리즘 : 특정 데이터 암호

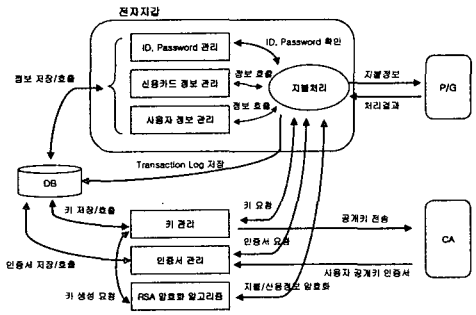

그림 9. 전자지갑 기능 구성도

그림 10과 11은 실제 J2ME 시뮬레이터 상에서 구현된 휴대용 전자지갑 화면을 나타내고 있다.

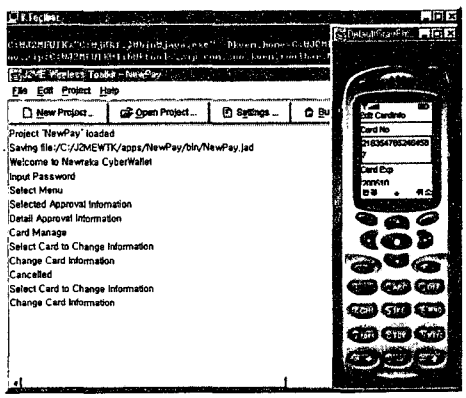

그림 10. 전자지갑 화면 구성 (1)

그림 10은 시뮬레이터는 Sun사의 Java™ 2 Platform Micro Edition, Wireless Toolkit[10]을 사용한 것으로 전자지갑에서 사용자 신용카드 번호를 등록하는 화면이다.

그림 11은 시뮬레이터 상에서 구현되어진 전자지갑의 기능을 나타내고 있다.

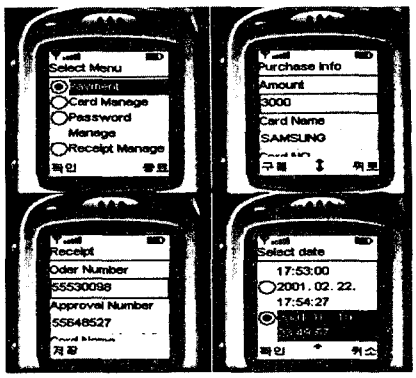

그림 11. 전자지갑 화면 구성 (2)

5. 결론

본 논문에서는 M-Commerce에 대한 개요와 자바 모바일 플랫폼인 J2ME를 분석하고, M-Commerce 보안 플랫폼을 구성하였다. M-Commerce를 안전하게 하기 위한 WTLS 및 자바 보안의 주요 기능에 대해 살펴보았고, 전자지갑에 대한 구현방안으로 모바일 환경상의 지불처리 방안을 제안했다.

현재 무선 인터넷 서비스를 지원하기 위하여 WAP포럼, W3C 및 MS사 등에서 독자적인 표준을 제안하고 있고, 썬과 오픈웨이브의 제휴로 자바 모바일 폰에 대한 활성화에 기여할 것으로 보인다. 따라서, 향후 자바 모바일 플랫폼 환경의 무선 인터넷 서비스가 일반화될 것에 대비하여야 할 것이다.

앞으로 WPKI과 연동할 수 있는 모듈 추가와 실제 단말기 상에 ECC알고리즘을 적용하여 구현하는 개발단계가 남아 있다

참고문헌

[1] J Davision, "Mobile E-commerce:Market Strategies", Ovum, 2000

[2] www.wapforum.org

[3] Katrina Bond, "Danny Willians, Mobile Ecommerce Analysis", Analysis Publication, 2000

[4] www.baltimore.com, "Baltimore telepathy-Making Mobile Commerce Secure", 2000

[5] 정보통신부, "무선기반의 M-commerce 활성화 정책방향", 2001. 1.

[6] 정보통신정책국, "무선인터넷 표준화 정책방안", 2001. 2.

[7] WAP Forum "Wireless Application Protocol spec 1.2", 1999. 12.

[9] WAP Frum, "Wireless Transaction Protocol Spec., Ver. 1.2", Jun. 1999

[10] Sun, http://java.sun.com/products/j2mewtoolkit/