The Journal of Korean
Institute of CALS/EC
Vol. 7, No. 1, April 2002

M-Commerce 보안 플랫폼상의 무선 전자지불시스템 설계 및 구현

김성한*, 이강찬*, 민재홍**

Design and implementation of Mobile Electronic Payment Gateway System based on M-Commerce Security Platform

Sunghan Kim, Kangchan Lee, JaeHong Min

Abstract

Recently, payment method is one of the most hot issues for transaction of contents in mobile and internet markets. Many kinds of mobile contents services are rapidly growing with the combination of internet application services. Payment method algorithms are demanded for the stable transaction between producer and consumer. Security protocol algorithms are widely adapted for mobile platform terminals. In this paper, we described security mechanism for the current wireless internet services and compared with the performance result. There are security protocols that based on java machine platform or WAP protocols. The system is based on J2ME technology for the java mobile platform. Based on this technology, a security system is proposed for the service of mobile commerce electronic payment. The system is designed for the stability of transaction so that it enables to apply into many kinds of internet payment system.

Key Word : Security Platform, Mobile Payment, J2ME(Java 2 Micro Edition)

* 한국전자통신연구원 선임연구원
** 한국전자통신연구원 책임연구원

1. 서론

무선 정보통신망의 발달로 인터넷의 중심이 기존의 유선에서 무선으로 급격히 이동함에 따라 전자상거래도 무선화 되고 있다. 무선통신 환경은 유선상의 전자 상거래에 비해 휴대 단말의 크기 제약, 컴퓨팅 능력, 제한된 입·출력 장치로 인한 제약뿐만이 아니라 무선망의 낮은 대역폭, 데이터 전송 지연과 불안정한 접속 등 다양한 문제점들을 해결할 수 있어야 한다. 또한 무선인터넷 서비스를 제공하기 위해서는 상호운영성(interoperability), 확장성(scalability), 효율성(efficiency), 신뢰성(reliability) 및 보안성(security) 등을 고려하여야 한다. 무선인터넷에서의 정보보호는 무선 환경의 제약사항을 고려하면서 전송계층 및 응용계층에서 제공되어야 하고, 특히 WAP 방식인 경우, 무선 게이트웨이(WAP Gateway)로 인한 종단간 보안(End-to-End Security)을 제공하기 어렵다는 문제를 해결할 수 있도록 해야 한다. 이와 같이 이동통신의 응용서비스로서 무선 단말기를 이용한 무선 전자상거래(Mobile Commerce, M-Commerce) 서비스를 안전하게 제공하기 위한 보안 대책도 필수적으로 요구된다. 무선 전자상거래의 보안 요구사항을 살펴보면 유선 환경에서와 같이 기밀성(Confidentiality), 인증(Authentication), 무결성(Data Integrity), 부인방지(Non-Repudiation) 등이 필요하다.

또한 유선과 마찬가지로 무선에서도 완벽한 보안이 필요하며, M-Commerce 환경에서 다양한 응용서비스를 제공하기 위해 플랫폼 독립적인 어플리케이션 운영 기능을 제공해야 한다. 보안상 매우 취약한 신용카드를 대체할 수 있는 휴대폰을 이용해 오프라인의 지급 결제를 수행하는 전자지갑 모델은 기존 신용카드의 안전을 극복하는 편리한 방법이 제공 가능하다.

본 논문에서 사용자가 시간과 장소에 구애받지 않고 상품구매 및 대금 지불을 할 수 있는 전자지갑을 자바 모바일 플랫폼 기반으로 구현할 수 있는 방안을 제시한다. 즉, 무선인터넷 응용 프로토콜인 WAP(Wireless Application Protocol)을 중심으로 J2ME(Java 2 Micro Edition) 자바 플랫폼과 연결한 단말기의 브라우저를 탑재하여 M-Commerce 전자지불을 위한 휴대용 전자지갑의 구현방안을 제안한다. 그리고 자바 언어를 이용한 동적인 서버 사이드 스크립트 언어인 JSP(Java Server Pages)와 무선인터넷 언어(WML, HDML, mHTML, cHTML)를 사용하여 특정 웹서버나 플랫폼에 서로 독립적인 서비스를 제공할 수 있는 무선 전자지불시스템을 설계 및 구현한다. 또한 WTLS(Wireless Transport Layer Security)를 고려한 M-Commerce의 보안 플랫폼을 제시함으로서 기존 지불방식보다 안전성이 향상되고 서비스 제공의 효율성을 높일 수가 있다.

본 논문에서는 M-Commerce의 개요, 무선인터넷 보안기술들을 살펴보고, 안전한 M-Commerce 서비스를 제공할 수 있는 보안 플랫폼을 제시한다. 본 논문에서 제시한 보안 플랫폼은 무선인터넷 프로토콜을 중심으로 자바 플랫폼과 연결한 단말기 브라우저를 탑재한 것으로 선마이크로시스템사에서 개발한 소형 디지털 디바이스를 위한 J2ME를 기반으로 해서 설계되었으며, 향후 WPKI(WAP Public Key Infrastructure)와의 연동을 고려하고 있다.

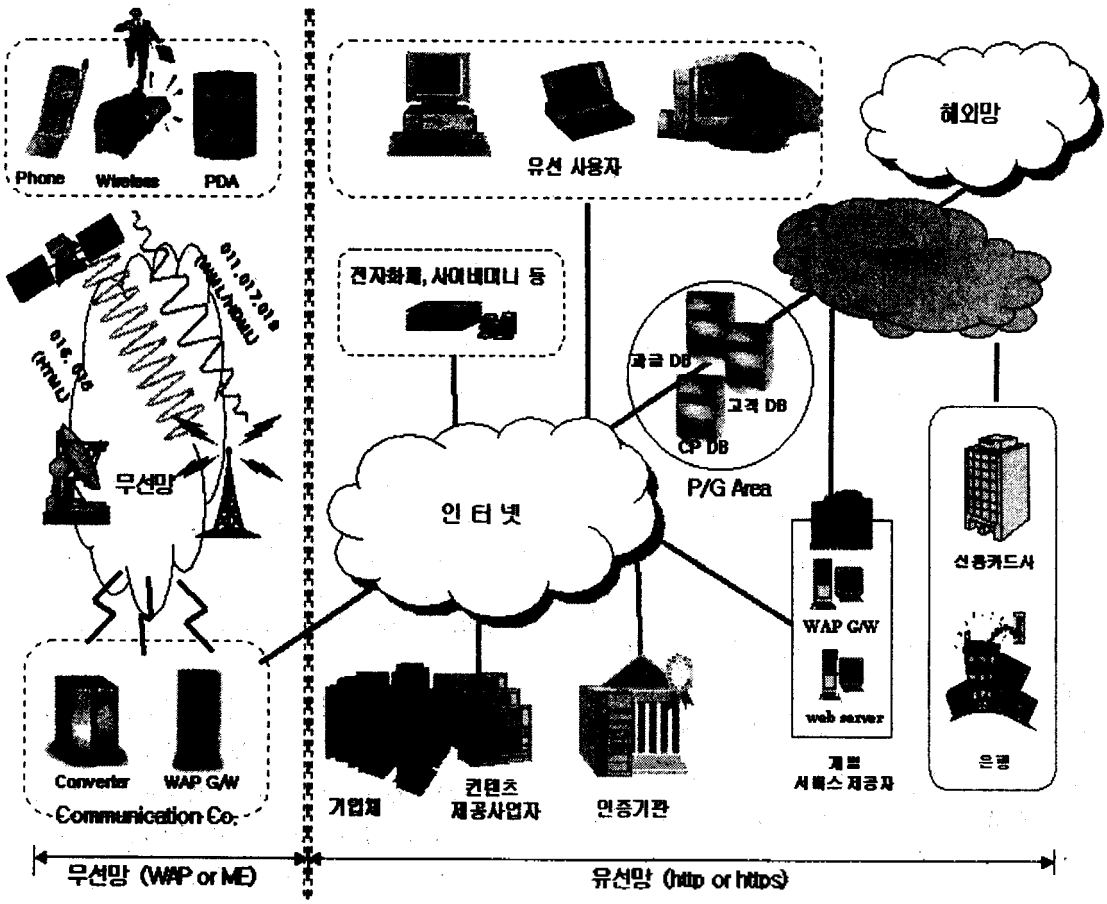
본 논문의 구성은 다음과 같다. 제 2장에

서는 무선인터넷방식에서의 보안기술과 자바 모바일 플랫폼상의 보안에 대해 분석하고, 제 3장에서는 무선 전자상거래 보안 플랫폼을 제시하며, 무선 어플리케이션 상의 종단간 보안의 구성 방안을 살펴본다. 마지막으로 제 4장에서는 결론을 맺는다. 모바일 서비스 플랫폼의 구성에 있어 다양한 방안이 제기되고 있지만, 본 논문에서는 이들의 미세한 차이는 다루지 않으며, 자바 표준인 MIDP(Mobile Information Device Profile)를 기준으로 한다.

2. 관련 기술 연구

2.1 무선 전자상거래 서비스 플랫폼

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,

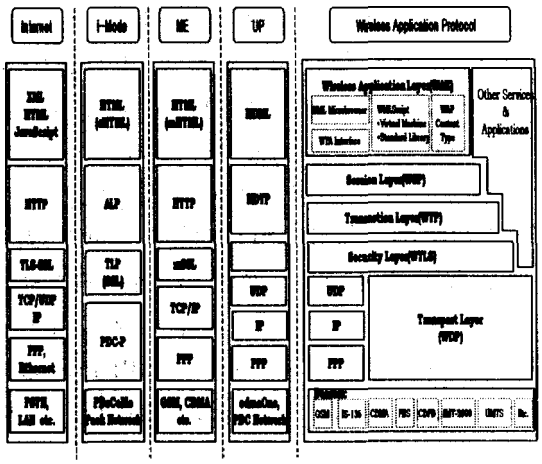


<그림 1> M-Commerce의 구성도

M-Commerce는 무선 단말기와 무선망을 통한 상품(Goods), 용역(Service) 및 정보(Information)의 상업적 거래를 의미한다. M-Commerce의 구성도는 <그림 1>과 같이 나타낼 수 있으며, 활용 대상에 따라 B2C(기업과 소비자), B2B(기업과 기업) 및 M2M(단말과 단말)으로 구분할 수 있다.

M-Commerce는 무선인터넷 응용프로토콜과 서비스 플랫폼을 기반으로 구성되어지는데, 무선인터넷의 대표적인 무선 응용프로토콜 표준방식에는 WAP방식, ME(Mobile Explorer) 방식 및 일본의 i-Mode가 있다. WAP 방식은 세계적으로 가장 많은 사업자가 채택하고 있는 무선응용프로토콜 표준으로 유럽의 에릭슨, 노키아 등이 중심이 된 WAP 포럼에서 작성되었다. ME방식은 미국 마이크로소프트사에서 개발된 방식으로 기존의 유선 인터넷기술 언어를 이동통신망에 맞게 수정하여 적용한 표준방식이다. i-Mode는 일본의 NTT DoCoMo가 독자적으로 개발한 표준방식으로 자체 패킷망인 PDC를 기반으로 패킷 기반의 무선인터넷 서비스를 제공한다. <그림 2>는 각 방식의 프로토콜 스택을 나타내고, <표 1>에서 각 무선 응용프로토콜 방식의 구조에 대해 비교한다.

무선 응용프로토콜의 제한된 속도와 비싼 서비스 요금, 불안한 안전성 등의 문제점을 해결하기 위한 대안으로 무선 서비스 플랫폼이 구성되어졌는데, 무선 서비스 플랫폼이란 Virtual Machine의 일종으로 어플리케이션 등이 실행될 수 있는 독립 환경을 의미한다. 서비스 플랫폼은 단순한 텍스트와 이미지 서비스에서 벗어나 게임, 동영상 같은 멀티미디어 통신을 가능하게 한다.



<그림 2> 무선응용프로토콜방식의 비교

<표 1> 무선 응용프로토콜 방식의 장·단점 비교

구분	WAP	ME	i-MODE	AnyWeb
제공업체	WAP포럼	MS, 퀄컴	NTT DoCoMo	삼성전자, Al-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			

현재 국내에서는 신지소프트의 SWAP, 썬마이크로시스템즈의 자바 플랫폼에 이어 최근 모빌탑과 XCE, 퀄컴 등이 새로운 플랫폼을 내놓고 있다. 또한 MS도 스팅거라는 코드명의 음성데이터 통합 단말 플랫폼을 개발중이고, 오픈웨이브도 WAP 브라우저에 플랫폼 기능

추가를 통해 경쟁에 동참해 무선 플랫폼 시장을 형성하고 있다. 이 서비스 플랫폼을 이용해 어플리케이션을 제작할 경우, 정지된 화면과 텍스트 위주의 WAP 환경에 비해 빠른 실행 속도와 사운드 지원으로 다이나믹한 환경을 즐길 수 있다. 또 다운로드 방식으로 각종 정보를 휴대폰에 저장하므로 접속 끊김이나 비싼 통화료 등 단점을 극복할 수 있다. 특히 VM의 경우, 모든 종류의 휴대폰에 적용할 수 있어 범용성 확보 및 새로운 어플리케이션 개발에 용이하다.

현재 국내외 서비스 중인 상용 무선 서비스 플랫폼을 비교하여 보면, 자바 플랫폼은 버추얼머신이 번역과정을 거쳐 실행파일을 생성한 후 애플리케이션을 실행하기 때문에 로딩 시간이 다소 느리지만 다양한 환경에서 사용할 수 있다는 것이 장점이다. 향상된 그래픽 환경과 편리해진 사용자 인터페이스 및 보안성 강화의 장점과 기존 인터넷 서버와 직접 연결하여 다운로드 받아 단말기에 이용 가능하다는 것도 장점이다. 이에 반해, C 기반의 무선서비스 플랫폼 방식은 자바 서비스 플랫폼에 비해 메모리 확장이나 HW의 개선 없이 단말기에 소프트웨어만 수정하여 탑재 가능하다는 장점과 동적인 네트워크 게임 제공이 유리하다는 장점이 있다.

2.2 무선 및 전자금융 보안 기준

WAP과 ME를 포괄하는 무선 보안/인증 관리체계에서 사용되어지는 전자서명 및 암호 알고리즘, WPKI 구성에 대한 인증서 규격, 전송방식 저장방식 등이 한국정보보호진흥원를 중심으로 연구되었다. 이 연구결과를 참고하여 전 세계 표준들을 중심으로 한 무선 환경 관련 보안/인증 표준들을 정리하여 보면 아래 <표 2>와 같다.

<표 2> 무선 보안/인증 관련 표준

항목		표준 내역
키생성	단말기	단말기 측 생성 RSA 알고리즘 (1024 bit)
	서버	단말기 측 생성 RSA 알고리즘 (1024 bit)
암호 알고리즘	단말기	SEED 알고리즘 (1024 bit)
	서버	SEED 알고리즘 (1024 bit)
해쉬 알고리즘	단말기	SHA1 알고리즘
	서버	SHA1 알고리즘
전자서명	단말기	RSA 알고리즘 (1024 bit)
	서버	RSA 알고리즘 (1024 bit)
인증서 규격	단말기	WTLS 인증서
	서버	WPKI
CRL 규격	단말기	Short-lived Cert (48시간)
	서버	Short-lived Cert (48시간)
코딩방법 / DN	단말기	DER/PEM/WTLS 인증서 코딩규격
	서버	DER/PEM/WTLS 인증서 코딩규격
인증 요청서	단말기	PKCS#10 / CMP
	서버	PKCS#10
인증서 전송방식	단말기	인증서의 URL 전송
	서버	인증서의 URL 전송 / 전체 인증서 전송
전자서명키 저장방식	단말기	PKCS#5로 암호화 PKCS#8로 저장
	서버	PKCS#5로 암호화 PKCS#8로 저장
인증서 및 CRL 획득방식	단말기	HTTP / LDAP
	서버	HTTP / LDAP

위에서 기술된 내용들은 국제 표준 및 단체 표준 등과 호환 가능하도록 정의하여 상호

연동성을 보장한다.

앞서 살펴본 무선/보안 인증관련 표준들을 기반으로 금융감독원에서 제시한 전자금융 안전대책 기준(안)을 분석하여 보면[3], 주요 안전 기준으로 인터넷 뱅킹, 사이버 트레이딩, 무선 전화를 이용한 금융거래, 전자지불 시스템, 거래 정보 기록 보관, 사용자 ID 및 비밀번호 등의 내용을 명시하고 있다.

<표 3>은 세부 업무별 보안 기준안 중 무선환경 전자지불과 관련된 내용을 간추려 분석한 내용이다.

<표 3> 전자지불 관련 세부 업무별 보안기준안

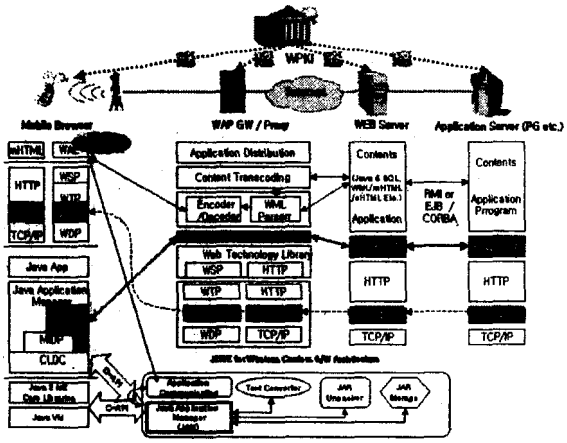
구분		암호화	인증	OTP	침입 차단	침입 탐지	로깅
은행	전자지불	○	○	○	○	○	○
	Phone 뱅킹	×	×	○	×	×	○
	Internet 뱅킹	○	○	○	○	○	○
	PC 뱅킹	×	×	○	×	×	○
증권	Mobile	○	○	○	○	○	○
	ARS	×	×	○	×	×	○
	Web Trading	○	○	○	○	○	○
	PC 통신	×	×	○	○	○	○
보험	CD/ATM	○	×	-	×	×	○
	인터넷폰	○	○	○	○	○	○

위의 표에 근거하여 본 논문에서 구현한 시스템의 전자지불 거래관련 보안 요구사항에 대한 주요 내용을 살펴보면 다음과 같다.

- 거래 내용에 대한 기밀성 보장 (Confidentiality) : 암호화
- 거래내용에 대한 무결성(Integrity) 보장 : 인증, 암호화
- 본인 인증(Authentication)
- 시스템 접근제어(Access Control) : 침입 차단 시스템
- 세션 제어(Session Control) : 침입 탐지 시스템
- 거래 및 접근 기록 : Logging

2.3 무선 전자상거래 보안 플랫폼 구성

무선환경에서의 각 응용 프로토콜에 대한 분석과 서비스 플랫폼에 대한 내용을 바탕으로 M-Commerce 보안 플랫폼의 구성을 살펴보면 <그림 3>과 같다. 본 보안 플랫폼 구성은 여러 상용 서비스 플랫폼 중 자바 모바일 서비스 플랫폼을 기반으로 구성한 M-Commerce 플랫폼을 나타낸다.



<그림 3> M-Commerce 보안 플랫폼 구성도

보안 플랫폼은 WAP 방식 기준의 ME 방식을 수용한 것으로 Mobile 브라우저상의 mSSL과 WTLS Client 암호화 모듈을 이용해 어플리케이션 서버까지 전송계층의 보안 을 지원하고, 전송 계층에서 제공하지 못하는 부

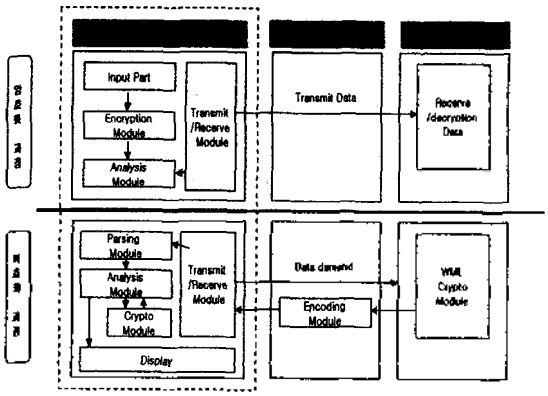
인방지를 위한 전자서명 기능은 WMLScript Crypto Library를 이용한다. 이를 바탕으로 응용계층의 암호화를 위해 J2ME 기반의 모바일 자바 암호 라이브러리를 사용하여 암호화하고, 각 응용계층별 서버모듈에서 대응되는 복호화 방안을 마련한다.

단말기 측에서의 MIDP 어플리케이션 프로그램은 CLDC 보안모델에 따르며, 어플리케이션 관리자는 실행 시에 URL(MSD 파일의 URL)을 전달받으면 즉시 다운로드 과정을 수행한다. MSD 파일을 다운로드 한 다음에 그 내용을 사용자에게 보여 주고 사용자가 다운로드를 원하면 실제 JAR 파일을 다운로드 한다. 그리고 MSD 파일과 JAR 파일을 저장하고 저장한 프로그램을 실행시키게 되는데, 저장하는 과정에서 만일 EFS 내의 어플리케이션 저장공간이 부족하다면 기존의 어플리케이션들 중에서 사용자가 선택하여 삭제할 수 있도록 하여야 한다.

2.4 어플리케이션상의 종단간 보안

무선 단말기의 브라우저와 서버간의 종단간 보안 통신은 앞서 말한 WAP 방식과 자바 모바일 환경에 맞춰서 크게 두 가지 방식으로 나누어진다. 두 가지 방식은 향후 WPKI의 연동을 고려한 종단간 보안방식으로서, 하나는 단말기 브라우저가 데이터를 요청할 경우 암호화된 데이터를 전송하는 것이고, 또 다른 하나는 수신된 WML Data 문서내의 입력 태그 및 자바 어플리케이션의 입력창을 이용해 서버로 전송하는 경우이다. 이 때, 암호화 및 복호화는 인증 과정 이후에 생성된 대칭키를 사용하며, 서버는 원하는 부분을 미리 혹은 동적으로 암호화하여 단말기로 전송할 수 있다. 보안 모듈에서의 기본적인 사항들은 아래와 같이 한다.

- 암호화엔진 모듈 : 암/복호화 모듈 및 인증 모듈의 동작의 기반이 되는 부분이며, 이 두 모듈에서 사용되는 암호 알고리즘은 SEED나 3-DES, 혹은 무선 환경에 최적화된 ECC (Elliptic Curve Cryptosystem) 알고리즘을 사용한다.
- 인증모듈 : 단말기와 서버간의 인증 프로토콜을 수행하여 상호 인증 및 암호화/복호화에 사용될 대칭키 교환기능을 동시에 수행한다. 인증은 한 세션 단위동안 유효하다.
- 암/복호화 모듈 : 앞의 인증 과정에서 얻은 대칭키로 상호간에 암호화/복호화를 수행하는 부분이다. 제안한 단말기의 브라우저에서는 해석 모듈에서의 요청이 있을 경우 해당 데이터를 복호화하여 전송하게 된다.



<그림 4> 어플리케이션 종단간 보안을 위한 암/복호화 과정

종단간 보안을 위한 암호화 과정과 복호화 과정은 다음 순서와 같다.

① 무선단말기의 브라우저가 데이터를 요청할 경우

무선 단말기와 서버와의 통신은 일반적인 WWW상에서의 HTTP 프로토콜과 유사하다. 즉, 단말기의 브라우저가 요청하고 서버가 응답하여 데이터를 전송하게 되며, 이 과정에서 암호화 및 복호화 과정이 추가된다. 그 순서를 보면 다음과 같다.

- 단말기의 브라우저는 서버에 데이터를 요청한다.
- 서버는 암호화된 데이터를 생성한다.
- 서버는 암호화된 데이터를 전송한다.
- 게이트웨이는 인코딩하여 단말기 측으로 전송한다.
- 단말기는 인코딩된 데이터를 수신한다.
- 파싱 모듈은 트리구조의 API형태로 구조화한다.
- 해석 모듈은 태그의 의미를 해석한다.
- 해당 내용을 복호화하여 전송한다.
- 내용을 디스플레이한다.

② 사용자가 입력한 내용을 암호화하여 전송하는 경우

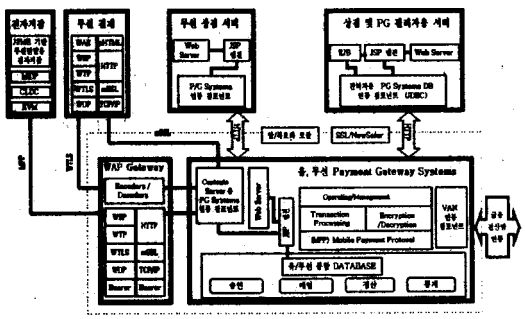
- 사용자는 데이터를 입력한다.
- 암호모듈은 이 데이터를 세션키로 암호화된다.
- 해석모듈은 암호화된 데이터에 추가하여 송수신 모듈로 보낸다.
- 서버로 전송한다. 이 때 게이트웨이는 일반 텍스트의 포맷으로 디코딩한다.
- WAP 서버는 이 데이터를 수신하여 복호화한다.

3. 무선 전자지불시스템 설계

이 장에서는 앞장에서 M-Commerce 환경을 고려해 구성한 보안 플랫폼을 기반으로 무선 전자지불시스템의 설계 및 기능분석에 대해서 기술한다.

3.1 전체 시스템 구성도

무선 전자지불시스템의 전체 구조는 <그림 5>와 같이 무선 지불서버, 무선인터넷 Form 결제방식 컴포넌트, 무선 단말용 전자지갑, 상점 서버용 지불서버 연동 컴포넌트, WTLS 연동 모듈 등으로 구성되어 있다. 구현된 주요 5가지 구조 중 중요한 기능인 무선 지불서버 및 Form 결제방식 모듈과 전자지갑 프로그램에 대한 보다 자세한 사항은 3.2에 걸쳐서 기술된다. <그림 5>는 무선인터넷상에서 전자지갑을 다운로드 받는 무선단말기를 이용한 전자지불시스템을 나타내는 세부 구성도 이다.



<그림 5> 무선 전자지불시스템 세부 구성도

무선 전자지불시스템을 구성하는 요소와 그 기능은 다음과 같다.

① 다중 결제처리를 위한 지불 서버
: 사용자로부터 받은 지불 정보의 유효성 여부 등을 판단하기 위하여 지불정보를 각 금융기관 서버에 보내고 지불 결과를 상점서버 및 사용자 단말로 전송하는 서버
- Transaction 처리기능 (Transaction의 복구, 조회, 기록 기능)
- 머천트 서버와의 연동기능
- 금융시스템과의 연동기능
- 안전한 지불정보 전송을 위한 암호화/복호화 기능
- 전자서명 생성/검증
- 운영관리 기능

② Form 결제방식 컴포넌트
: 사용자가 브라우저로 지불관련 인터페이스를 요청할 경우 응답하는 컴포넌트
- 지불결제 처리 의뢰 기능
- 지불결제 처리 결과 송수신 기능

③ J2ME 기반 무선 단말용 전자지갑
: 사용자가 무선단말기로 결제를 원할 경우 결제 관련 처리를 하는 프로그램
- 지불수단 정보(신용카드번호, 은행계좌 번호, 선불형 전자화폐번호) 저장기능
- 지불수단 정보 관리기능
- 전자지갑 접근 관리기능
- 지불시스템과의 연동기능
- 머천트 서버와의 연동기능
- 안전한 지불정보 전송을 위한 암호화/복호화 기능

④ 상점 서버용 지불서버 연동 컴포넌트
: 사용자의 처음 접속 점으로 지불서버와의 연결점을 제공하는 컴포넌트
- 지불서버와의 연동기능
- 유/무선 단말기와의 연동기능
- 안전한 지불정보 전송을 위한 암호화/복호화 기능
- 전자서명 생성/검증

⑤ MPP(Mobile Payment Protocol)
: 인터넷 상에서 제공 가능한 전자지불서비스를 무선망 환경으로 확장할 수 있도록 하는 전자지불 프로토콜
- J2ME기반 무선 단말용 전자지갑과 지불서버, 상점과의 지불정보 교환 프로토콜.
- WPKI가 제공하는 전자지불 처리 관련 기능(전자서명, 암호화/복호화) 제공.

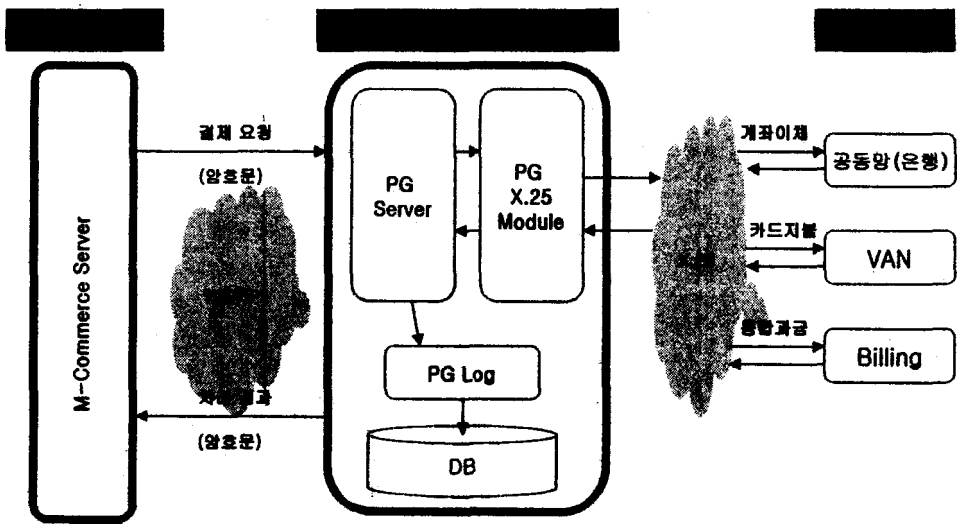
⑥ WTLS 인터페이스
: WAP 프로토콜 레이어에서 암/복호화를 처리하는 계층
- 암호화, 기밀성(HASH, HMAC), 인증(Symmetric and Public-Key)
- 동적 어드레싱, Multi-bearer Devices, 대역폭 자원 최적화

3.2 무선 전자지불 기능별 설계

본 절에서는 무선 전자지불시스템의 기능별 구성도를 나타내어 주요 기능을 정의하고 서비스 시나리오를 정립하여 기능별 세부 설계 내용을 기술한다.

3.2.1 무선 전자지불 서비스 설계

무선인터넷상에서의 단말기를 이용한 무선 전자지불 시스템은 전자지갑을 다운받을 무선 단말기와 물건 구매를 위한 무선인터넷 상점 서버, 전자지갑을 다운로드 받게하고 금융공동망과 인터넷망사이에서 지불처리를 하기 위한 전자 지불서버, 최종적인 지불에 대한 승인여부를 알려주는 금융기관(은행, 신용카드사, 선



<그림 6> 무선 전자지불 서비스 흐름도

불형 전자화폐 발행사)서버로 구성된다. <그림 6>은 무선 전자지불 서비스에서의 전체 서비스 흐름도를 나타낸 것이다.

본 논문에서 제안한 무선 응용프로토콜 및 무선 서비스 플랫폼의 휴대용 전자지갑을 이용한 무선환경에서의 지불처리 흐름의 구성은 <그림 7>에서와 같이 다음과 같다.

① 각 시스템은 인증기관으로부터 인증서를 발급 받는다.(WPKI 연동)

② 사용자는 지불을 위해 전자지갑을 무선 단말기로 다운로드한다.

③ 사용자는 전자지갑에 사용자 등록과정을 수행한다.

④ 사용자는 상점에 접속하여 구매과정을 마친다.

⑤ 사용자는 지불을 위해 전자지갑을 작동하거나 Form 인터페이스를 요청한다.

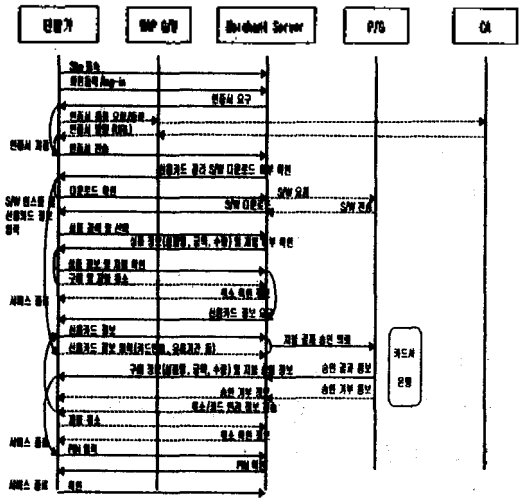
⑥ 사용자의 지불 및 주문 정보를 전자지갑에서 안전하게 상점으로 전달한다.

⑦ 상점측 PG 연동 컴포넌트는 사용자의 지불 정보를 PG로 전달한다.

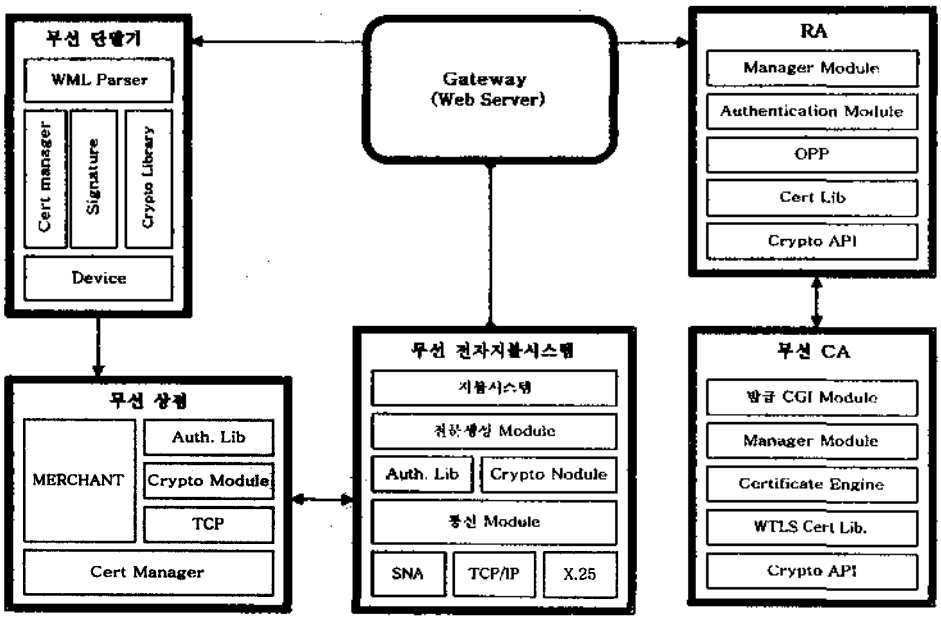
⑧ PG는 지불 정보를 각 금융기관에 전달하고, 승인 정보를 받는다.

⑨ PG는 승인 정보를 상점에게 전달한다.

⑩ 상점은 사용자에게 승인정보 전달과 상품 배달을 시행한다.



<그림 7> 무선 전자지불 처리 흐름도



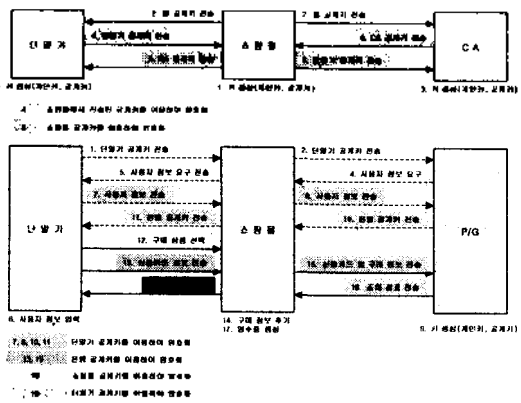
<그림 8> 무선 보안/인증 관련 전체 서비스 구성도

<그림 8>에서는 보안 서비스 구성도를 보이고 있다. 무선 응용프로토콜 방식을 수용한 Mobile 브라우저상의 mSSL과 WTLS Client 암호화 모듈을 이용해 어플리케이션 서버까지 전송계층의 보안과 단말기 환경의 암호 라이브러리를 이용해 응용계층에서 암호화를 하여 각 응용계층별 서버모듈에서 대응되는 복호화 방안을 마련한다. 차후 WPKI의 연동을 대비한 인증서 관련 관리 모듈들을 각 장치별로 설계한다.

앞의 무선 전자지불에서의 보안서비스 구성을 기반으로 하는 안전한 전자지불을 위한 상호 키 처리절차에 따른 구매 및 지불처리 흐름도는 <그림 9>와 같다.

3.2.2 무선 전자지불시스템 기능별 구성

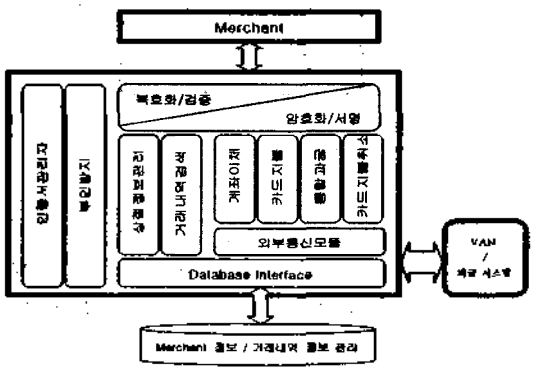
무선 전자지불시스템은 무선 지불서버, 결제 컴포넌트, 전자지갑, 상점서버 연동 컴포넌트, WTLS 모듈 등으로 구성되어 있는데, 이들 중 중요한 기능인 무선 지불서버 및 Form 결제방식 컴포넌트와 전자지갑 프로그램에 대한 보다 자세한 기능별 설계사항을 살펴보면 다음과 같다.



<그림 9> 키 교환 처리절차에 따른 구매 및 지불 처리 흐름도

• 무선 지불서버

<그림 10>은 주요 지불처리 기능 구성도로서 무선 전자지불시스템은 무선망과 인터넷망 그리고 VAN사 사이에 있는 시스템으로 독립적인 시스템으로도 존재할 수 있는 인터넷 연결부와 금융기관에 연결된 VAN사와의 데이터 송수신을 위한 VAN사 연동부인 외부통신모듈과 상점서버 연동부와 무선용 결제 단말기와의 데이터 송수신을 위한 무선인터넷 Form 연동부와 거래에 대한 데이터를 저장하는 거래내역 DB로 구성된다.

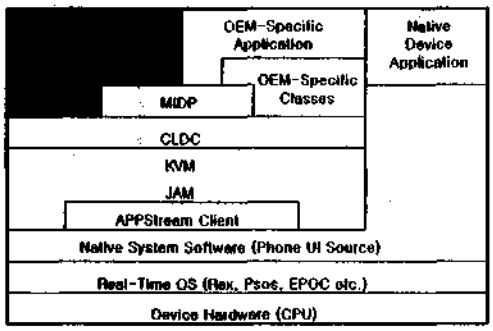


<그림 10> 무선 전자지불시스템 기능 구성도

• 전자지갑

<그림 11>은 전자지갑이 포함된 무선단말기의 소프트웨어 아키텍처를 나타내고 있다. 자바 모바일 서비스 플랫폼 기반의 MIDP 기능인 JAM(Java Application Manager)을 이용해 MIDP 어플리케이션인 MIDlet 형태의 전자지갑을 다운로드하여 설치, 업그레이드, 실행, 삭제한다.

전자지갑이 포함된 무선단말기는 다운로드된 전자지갑을 단말기상의 저장공간에 저장하는 저장기능부 무선단말기 소유자의 요청에 의해 전자지갑을 구동하는 구동기능부로 구성되고, 전자지갑은 무선단말기 소유자의 지불수단 정보를 기록하고 저장하는 저장부, 무선단말기 소유자가 전자지갑에 패스워드를 지정하여 다른 사용자가 무선단말기내의 전자지갑을 구동할 수 없게 제어하는 제어부, 지불 처리시 전자지갑에서 지불방법을 선택하고, 지불을 요청하는 지불요청부, 무선단말기 소유자가 선택한 지불수단정보를 전자지불서버에 전송할 때 지불수단정보 암호화를 위한 암호화부로 구성된다.

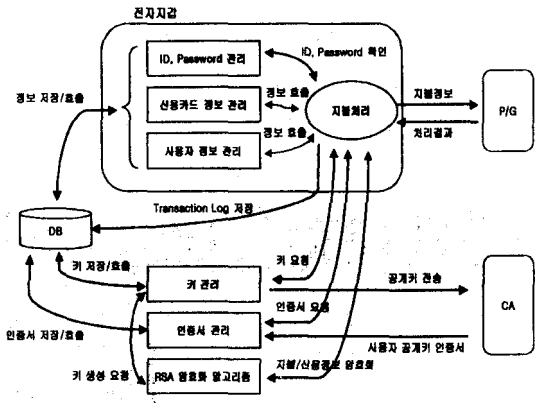


<그림 11> 무선 전자지갑 Level Architecture

무선 전자상거래를 위한 휴대용 전자지갑의 기능구성은 <그림 12>와 같으며, 기능에 대한 개략 설명은 다음과 같다.

- 지불처리 : 신용카드 정보, 사용자정보를 암호화하여 Payment Gateway에 전송
- ID, Password 관리 : 전자지갑에 사용자의 ID 및 패스 워드를 등록
- 사용자 정보관리 : 사용자의 인적사항에 대한 정보를 관리
- 키 관리 : 사용자의 공개키/비밀키를 생성관리
- 인증서 관리 : 인증서 요청 및 URL 저장

- RSA/SEED/3-DES/ECC 등의 고성능 암호화 알고리즘 : 특정 데이터 암호



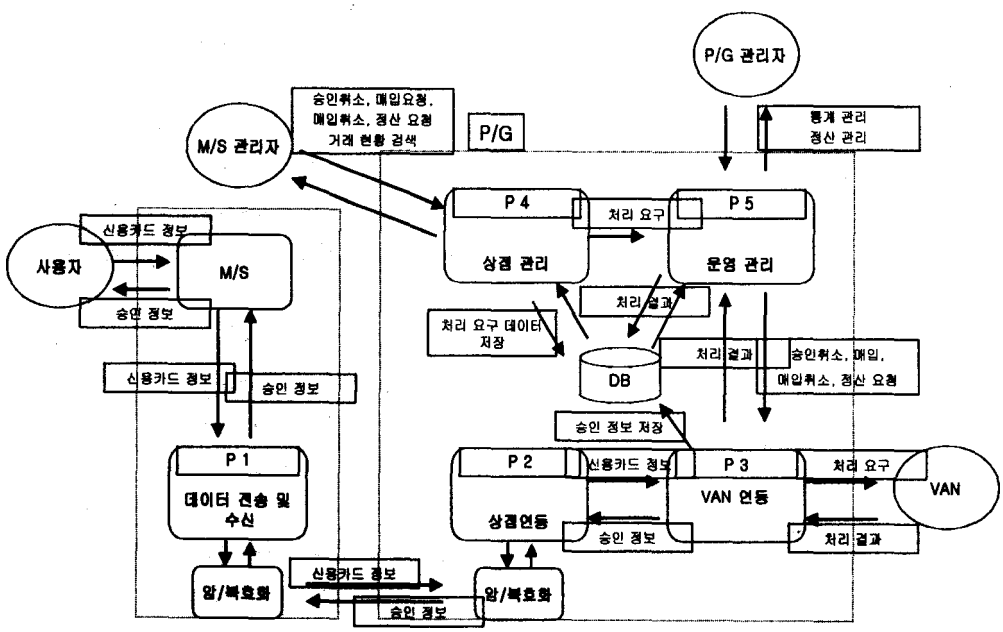
<그림 12> 전자지갑 기능 구성도

• 무선인터넷 Form 결제 컴포넌트

무선 전자지불시스템에서 무선 응용프로토콜을 기반으로 무선인터넷 Form 결제 컴포넌트를 구성하여 무선 지불서버와 연동을 통한 결제 정보를 처리한다. 그 주요 기능을 살펴보면, 상점에서 제공하는 주문화면(WML, ASP, PHP, JSP 등)에 사용자의 결제 정보를 입력하여 무선상의 지불을 처리하는 기능과 주문화면을 통해 입력된 사용자의 정보 중 금융정보(카드정보)는 P/G로 전송되어 카드 승인 등의 온라인 처리가 이루어지고 주문/배달 정보는 쇼핑몰에 저장하는 기능으로 나눌 수 있다. P/G로 전송되는 사용자 결제 정보는 WTLS/mSSL 암호화 방식을 적용한다.

• 데이터베이스 설계

무선 전자지불서버의 Form 연동 컴포넌트와의 처리내역과 VAN 등의 금융권의 결제 승인정보를 각 구성 테이블별로 설계하여 데이터베이스에 저장하도록 한다.



<그림 13> 무선 인터넷 Form 결제 컴포넌트의 기능흐름도

4. 무선 전자지불시스템 구현

4.1 구현환경

본 시스템은 리눅스환경에서 데이터베이스와 자바 언어를 이용하여 개발되었다. 사용자 인터페이스는 무선환경의 단말기에서 쇼핑 및 결제 결과를 받을 수 있도록 자바 언어를 이용한 동적인 서버 사이드 스크립트 언어인 JSP(Java Server Pages)와 무선인터넷 언어(WML, HDML, mHTML, cHTML)를 사용하여 특정 웹서버나 플랫폼에 서로 독립적인 서비스를 제공할 수 있도록 구현하였다.

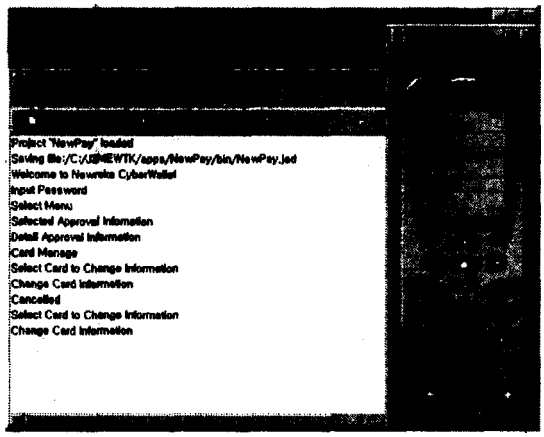
암호화 모듈을 사용하기 위해 SUN 규격을 따르는 NewSafer2001(Java Cryptography Library) 패키지를 사용하였다. 모바일 터미널의 클라이언트는 PentiumII PC의 Windows NT 운영체제에서 시험되었으며, 나머지 각 구성요소의 환경은 PentiumIII의 Linux 환경으로 구축되었다. 전송되는 정보를 암호화하기 위해서는 DES 및 RSA 암호화 알고리즘을 사용하였고, 키 교환은 Diffie-Hellman 키 교환 방식과 RSA를 사용하였다. 대부분의 경우 Diffie-Hellman 키 교환 방식을 사용한다. RSA를 사용할 때 공개키를 인증해 주는 인증 서버의 역할은 PG 서버가 그 기능을 담당하도록 하였다.

4.2 시스템 구성요소별 구현

본 절에서는 제 3장에서 살펴본 각 기능별 설계에 대한 구현을 기술한다. 전자지불처리의 화면 구성도에 대해 기술하고, 전자지갑, Form 결제 컴포넌트, 무선 지불서버의 기능 구현에 대하여 살펴본다.

4.2.1 전자지갑 구현

<그림 14>는 실제 J2ME 시뮬레이터 상에서 구현된 휴대용 전자지갑 화면을 나타내고 있으며, 시뮬레이터는 Sun사의 Java™ 2 Platform Micro Edition, Wireless Toolkit[10]을 사용한 것으로 전자지갑에서 사용자 신용카드 번호를 등록하는 화면이다.



<그림 14> 전자지갑 화면 구성

4.2.2 무선인터넷 Form 결제 컴포넌트 구현

<그림 15>와 <그림 16>은 실제 무선인터넷 시뮬레이터 상에서 구현된 무선인터넷 Form 결제 컴포넌트의 기능구현 화면을 나타내고 있다.

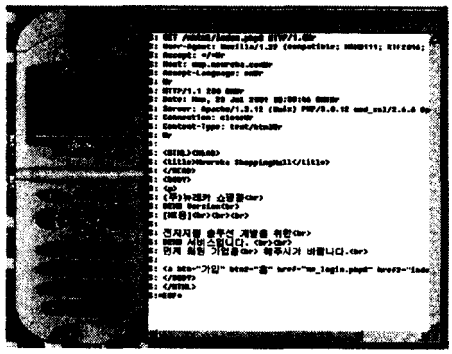
<그림 15>는 시뮬레이터는 Phone.com사의 UP Simularot를 사용한 것으로 무선 음반 쇼핑몰에서 28,000원에 대한 대금 결제를 신용카드 방식으로 하는 화면이다.

4.2.3 무선 지불서버 기능 구현

실제 무선인터넷 시뮬레이터 상에서 쇼핑을 하여 대금 결제를 한 뒤 온라인 상의 브라우저 접속을 통해 무선상의 대금 결제 내역을

유선 지불서버와 연동하여 조회할 수 있도록 구성되어진 기능의 접속화면이다.

<그림 15> 무선인터넷 Form 결제 WAP 방식



<그림 16> 무선인터넷 Form 결제 ME 방식-(2)

5. 결론

유선 인터넷에서 무선인터넷으로 사용자들의 이동이 예상됨과 동시에 무선인터넷상에서의 안전하고, 편리한 전자지갑방식의 지불인터페이스와 다양한 지불수단의 제공이 반드시 필요하게 된다.

본 논문의 시스템을 통해 무선 단말기 사용자들에게 편리하고, 안전한 지불을 위한 무선 단말기용 전자지갑을 제공하게 된다. 이는 많은 고객들이 무선인터넷 상점에서 상품을 쉽게 구매할 수 있는 계기를 제공하게 된다. 무선단말기를 이용한 전자상거래의 증가는 새로운 무선인터넷 시장의 성장을 촉진시키는 계기가 된다. 무선인터넷 시장의 성장은 무선인터넷 사업자에게는 무선인터넷 사용료라는 수익을 증가시키고, 무선인터넷 상점에게는 상품 판매에 따른 수익을 증가시키고, 전자지불 사업자에게는 시스템 사용수수료라는 수익을 증가시킨다. 또한 각 지불수단 제공자들에게도 새로운 무선인터넷 시장에 따른 수익을 발생시킬 수 있을 것으로 예상된다.

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 서비스 플랫폼 환경상의 무선 전자지불시스템을 설계 및 구현하였다.

현재 무선인터넷 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 무선인터넷 서비스가 일반화될 것에 대비하여야 할 것이다.

감사의 글

본 논문은 (주)뉴레카와 공동연구에 의한 논문 결과임을 밝혀 드립니다.

참고문헌

[1] J Davision 등 저, "Mobile E-commerce: Market Strategies", Ovum, 2000
[2] Katrina Bond, "Danny Willians, Mobile Ecommerce Analysis", Analysis Publication, 2000
[3] 금융감독원 정보기술검사국, "전자금융 안전대책 기준" 2000. 9.
[4] "Baltimore telepathy-Making Mobile Commerce Secure", Baltimore, www. baltimore. com, 2000
[5] WAP Forum "Wireless Application Protocol spec 1.2", 1999. 12.
[6] "Wireless Application Protocol Architecture Specification", WAP-210-WAPArch, WAP Forum, 2000
[7] "WAP WTLS ver. 18-Feb-2000", WAP Forum, http://www.wapforum.org
[8] KVM WhitePaper http://java.sun.com/products/kvm
[9] CLDC/MIDP, http://java.sun.com/
[10]Sun,http://java.sun.com/products/j2mewtoolkit/
[11] 박남제 외 3명,"M-Commerce를 위한 자바 모바일 플랫폼 기반의 전자지불 구현 방안", 2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호 2001. 4.

저자소개

김성한(e-mail : sh-kim@etri.re.kr)
광운대학교 전자계산기공학과 학사
광운대학교 전자계산기공학과 석사
현재, 한국전자통신연구원 표준연구센터 선임연구원
관심 분야 : XML, 무선인터넷서비스, 오디오 메타 프로세싱

이경찬(e-mail : chan@etri.re.kr)
충남대학교 컴퓨터공학과 학사
충남대학교 컴퓨터공학과 석사
충남대학교 컴퓨터공학과 박사
현재, 한국전자통신연구원 표준연구센터 선임연구원
관심 분야 : semantic web, ontology, RDF

민계홍(e-mail : jhmin@etri.re.kr)
고려대학교 산업공학과 학사
고려대학교 경영정보학과 석사
현재, 한국전자통신연구원 표준연구센터 책임연구원
관심 분야 : semantic web, 추론이론