情 報 保 護 學 會 誌
第 11 券 第 4 號, 2001. 8

모바일 서비스 플랫폼 기반의 무선 전자상거래 보안기술

박 남 제*, 송 유 진**

요 약

최근 인터넷 시장의 가장 큰 이슈는 무선환경과 컨텐츠의 유료화 움직임이다. 다양한 모바일 컨텐츠들이 무선인터넷을 지원하는 단말기의 보급과 더불어 빠른 성장세를 보이고 있다. 이에, 본 논문에서는 무선 인터넷 환경에 적합한 각 무선 응용프로토콜의 보안을 고려한 보안 메커니즘을 설계하며, WAP, ME 및 i-Mode방식에 대한 보안 요구사항을 분석한다. 또한, 향후 IMT2000에서도 사용 가능한 상업용 모바일 서비스 플랫폼을 검토하고, 표준화가 진행중인 자바 모바일 서비스 플랫폼을 기반으로 하는 J2ME 기술인 CLDC와 MIDP를 이용해서 M-Commerce 환경에서 사용되어질 보안 플랫폼을 제시한다. 본 논문의 결과는 향후 활성화될 M-Commerce의 안전한 응용서비스 제공을 위한 보안 플랫폼 구현의 기반이 될 것으로 기대된다.

Ⅰ. 서 론

인터넷과 무선통신 시스템이 급속히 성장하고 있다. 이들 성장의 한가운데 무선 인터넷이 있다. 무선 인터넷이란 브라우저가 내장된 휴대폰을 이용하여 인터넷주소(URL)로 접속하는 방식을 의미한다. 무선 인터넷에서 가장 매력적인 사업중의 하나로 무선 인터넷 전자상거래를 들 수 있다. 이제 디지털 경제 시대에서 무선 인터넷 전자상거래를 통해 고객은 언제, 어디서나 안전한 서비스를 제공받을 수 있을 것이다. 초기에는 무선 인터넷 전자상거래 서비스가 기존 인터넷 서비스에서 휴대폰으로 확대, 적용되는 형태가 되겠지만 이후에는 무선 사용자들만을 위한 새로운 서비스가 생겨날 것이다.

무선통신 환경은 유선상의 전자상거래에 비해 휴대 단말의 크기의 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. 여기서, 무선 인터넷에서의 정보 보호는 무선 환경의 제약사항을 고려하면서 전송계층 및 응용계층에서 제공되어야 하고, 특히 WAP 방식인 경우, 무선 게이트웨이로 인한 종단간 보안을 제공하기 어렵다는 문제가 있으며 이를 해결할 수 있도록 해야 한다. 이와 같이 이동통신의 응용서비스로서 무선 단말기를 이용한 무선 전자상거래 서비스를 안전하게 제공하기 위한 보안 대책이 필수적으로 요구된다. 여기서 무선 전자상거래에서의 보안 요구사항을 살펴보면 유선환경에서와 같이 기밀성(Confidentiality), 인증(Authentication), 무결성(Data Integrity), 부인 방지(Non-Repudiation) 등이 필요하다.

본 논문에서는 M-Commerce의 개요, 무선 인터넷 보안기술들을 살펴보고, 현재 상업용의 무선 플랫폼 서비스 기술들인 SK-VM, MobileTop, BREW 등을 분석하며, 이를 기반으로 안전한 M-Commerce 서비스를 제공할 수 있는 보안 플랫폼을 제시한다.

본 논문에서 제시한 보안 플랫폼은 무선 인터넷 프로토콜을 중심으로 자바 플랫폼과 연결한 단말기 브라우저를 탑재한 것으로 썬마이크로시스템즈에서 개발한 소형 디지털 디바이스를 위한 J2ME(Java 2 Micro Edition)을 기반으로 설계되었으며, 향후 WPKI와의 연동을 고려하고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 M-Commerce의 정의 및 구성도, 국내·외 현황 및

* 성균관대학교 정보통신대학원 정보보호학과 (njpark@mail.skku.ac.kr)
** 동국대학교 정보산업학과 (song@mail.dongguk.ac.kr)

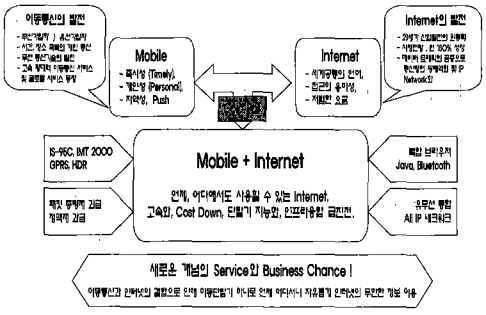
전망에 대해 살펴보고, 3장에서는 무선 응용프로토콜과 주요 상용 모바일 서비스 플랫폼에 대해 소개한다. 4장에서는 무선 인터넷방식에서의 보안기술과 자바 모바일 플랫폼상의 보안에 대해 분석하고, 5장에서 무선 전자상거래 보안 플랫폼을 제시하며, 무선 어플리케이션 상의 종단간 보안의 구성 방안을 살펴본다. 마지막으로 6장에서는 결론을 맺는다. 모바일 서비스 플랫폼의 구성에 있어 다양한 방안이 제기되고 있지만, 본 논문에서는 이들의 미세한 차이는 다루지 않으며, 자바 표준인 MIDP를 기준으로 한다.

II. M-Commerce의 개요

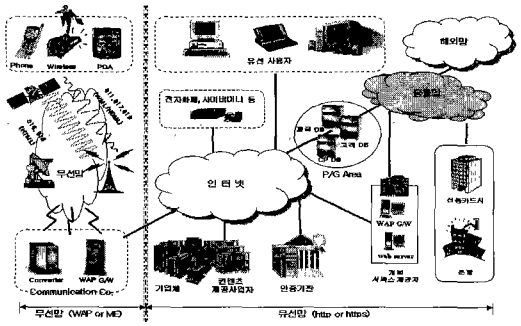
2.1 M-Commerce의 정의 및 구성도

Mobile E-Commerce 혹은 M-Commerce는 무선인터넷서비스나 이동컴퓨팅 서비스 양방향에서 제공될 수 있으며, 기존 E-Commerce에서처럼 정확한 정의를 내리기가 쉽지 않다. 다만 현재로선 휴대형 단말기 및 통신 네트워크를 통해 인터넷 혹은 인터넷 유사 서비스를 제공받으며 이루어지는 정보, 서비스, 재화에 대한 금전적인 거래의 뜻으로 정의할 수 있다[1]. E-Commerce가 PC Terminal을 이용한 전자적인 모든 거래 형태를 총칭한다면, M-Commerce는 PC Terminal을 대신하는, "거래가 가능하도록 지원되는 개인화된, 경량화된, 지역정보 제공이 가능한 개인용 Hand-held기기 (예를 들어, 핸드폰이나 PDA 등)를 이용한 전자적인 모든 거래 형태를 총칭"하는 것이다[1].

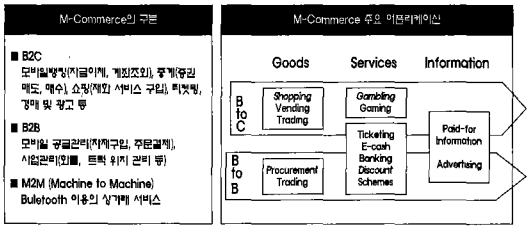
Mobile 환경과 인터넷이 M-Commerce라는 새로운 비즈니스 영역을 만들며, 보다 효율적인 상거래가 이루어는 M-Commerce 개념도를 그림 1과 같이 나타낼 수 있다.



〔그림 1〕 M-Commerce의 개념도



〔그림 2〕 M-Commerce의 구성도



〔그림 3〕 M-Commerce의 활용에 따른 구분

M-Commerce는 Mobile Commerce, Wireless E-Commerce 등으로 설명되기도 하며, B2B 영역일 경우에 Mobile B2B, Wireless B2B, Mobile B2B E-Commerce, B2B M-Commerce 등으로 설명된다. 결국 M-Commerce는 B2C M-Commerce와 B2B M-Commerce를 모두 포함한 개념이며, "Mobile Telecommunications Network를 이용한 전자상거래" 라고 이해하는 것이 정확하다. 따라서, M-Commerce는 무선 단말기와 무선망을 통한 상품, 용역 및 정보의 상업적 거래를 의미하며, M-Commerce의 구성도는 위의 그림 2와 같이 나타낼 수 있다. 그리고, 활용대상에 따라 그림 3과 같이 B2C(기업과 소비자), B2B(기업과 기업) 및 M2M(단말과 단말)으로 구분할 수 있다.

2.2 M-Commerce의 현황 및 전망

2.2.1 M-Commerce의 국내외 현황

국내 무선인터넷을 제공하는 서비스 사업자는 크게 이동전화 5개사와 (저속)무선데이터통신사업자로 구분될 수 있다. 앞으로 이동전화에 의한 무선인터넷이 국내 무선인터넷 시장을 주도해 나갈 것으로 보이며 기타 무선인터넷은 틈새시장을 형성할 가능성이 높다.

현재 국내 M-Commerce는 이동통신사를 중심으로 M-Commerce와 관련 다양한 서비스를 제공하고

있지만 대부분 간단한 B2C형태로 벨소리 및 캐릭터 다운로드, 게임 등이 주류를 이루고 있는 상황이다. 그러나 올해 들어서는 기업을 목표로 한 상품들을 앞다퉈 선보이는 등 보다 적극적인 모습을 보이고 있다.

SK텔레콤은 7개 은행 및 14개 증권사와 제휴, 뱅킹 서비스와 주식투자 관련 서비스를 제공하고 있다. 앞으로 IS-95C를 이용한 양방향 멀티미디어화로 거래 빈도를 높일 계획이다. 업체 중 가장 먼저 보안솔루션을 준비하였는데, 휴대폰에 내장된 암호화 모듈과 웹 서버쪽에 설치된 011 암호화 모듈이 직접 암/복호화를 수행하는 방식이다. 웹 서버단에 011에서 제공하는 암호화 모듈을 설치해야 한다.

KTF는 주식거래 및 신용카드 조회, 결제 서비스를 하고 있다. 최근에는 기업 대상으로 모바일 오피스를 구현해 주는 B2B 브랜드인 '비즈'를 발표하기도 했다. KTF는 MS, 소프트포럼과 협력하여 국내 금융권을 위한 국산 암호화 알고리즘인 SEED를 휴대폰에 탑재하였다. 앞으로 무선 PKI 서비스를 추가하고, 무선 지불수단 제공 및 금융정보의 고급화에 주력할 계획이다.

LG텔레콤은 교통 이용서비스인 019 이지패스 서비스와 여러 대형쇼핑몰과 일원화한 쇼핑 서비스를 제공하고 있다. LG텔레콤도 SK텔레콤의 경우와 동일하여 서버단에 작업을 해주어 종단간 보안을 해결하였다. 하지만 암호화가 적용된 휴대폰들은 HDML이 아닌 AU 시스템의 WML 브라우저를 탑재하고 있기 때문에 아직 보안 문제가 해결된 것은 아니다.

국내의 M-Commerce 서비스 현황을 살펴보면 표 1과 같다.

〔표 1〕 국내 M-Commerce 서비스 현황 및 동향

구분		SK텔레콤 011	신세기통신 017	한국통신 프리텔 016	한통엠닷컴 018	LG 019
브랜드명		N top	Itouch017	Peresnet	M-Life	eZweb(i)
접속방식		WAP	WAP	ME	ME	WAP
상용시기		1999.12 (1차) 2000.2.(2차)	1999. 12. 15.	1999. 9	1999.10(1차) 2000. 1 (2차)	1999. 5.
브라우저	제공업체	에릭슨	Phone.com	MS	MS	Phone.com
	변형여부	자체변형	그대로 사용	자체변형	그대로 사용	그대로 사용
사용언어	Script언어	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
컨텐츠 수	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)
포털사이트		www.n-Top.com	www.itouch017.com	www.magicn.com	www.magicn.com	www.ez-i.com
주요인기 컨텐츠		각종 게임 및 오락, 유머와 그림친구, 마이웹서비스, n-Top 게임, 친구찾기, 주식시세, 시황정보, 투자전략	멀티미디어, 게임, 미팅/결혼, 채팅	IRC 채팅, 미팅, 문자나라, 그림나라, 게임서비스, 증권 및 예약, 엔터테인먼트	이동 쇼핑, 티켓팅, 뱅킹, 카드결제 등	자바게임, 자바무선 네트워크 게임, 정보 커뮤니티, 교통방송, 교육
주요 CP		마리텔레콤, 거원, 텔미정보통신, 네모엔엠, 나스타, 웹캐슬 등	다날, 모비, 컴투스, 에어아이 등	지어소프트, 에어아이, 사이넷, 컴투스, 텔미 정보통신 등	지어소프트, 에어아이, 사이넷, 컴투스 등	컴투스, 보이소프트, 사이버경찰청 방송, 배움닷컴
무선인터넷 이용자 수	SMS	1,867,000	-	2,456,000	975,000	2,510,000
	WAP/ME	2,053,000	656	1,460,000	791,000	1,655,000
	합계	3,920,000	656,000	3,916,000	1,766,000	4,165,000
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

※ 한통엠닷컴은 향후 한통프리텔과 동일한 브라우저와 규격 사용 예정

국외 M-Commerce의 현황을 살펴보면, 지금까지 M-Commerce의 이용자와 시장규모 측면에서 유럽이 가장 중요한 지역으로서 북미지역을 훨씬 앞질러 시장을 선도해왔다. 현재 유럽지역 이동통신사업자들은 기존 무선인터넷 서비스의 한계를 극복하기 위해 이동통신망을 2.5G와 3G로 진화시키는데 많은 투자를 하고 있다.

북미지역은 유럽과 일본에 비해 무선인터넷과 M-Commerce 분야에 있어서는 기술개발면이나 서비스면에서 뒤쳐져 있다. 이와 같은 상대적 열세에도 불구하고 영어라고 하는 단일 언어를 사용한다는 장점이 있다. 그리고 인터넷 보급률이 높고 일반고객이나 기업고객이 온라인 전자상거래에 대한 선호도가 높다. 또한 낮은 이동전화 보급률과 국가표준의 부재에도 불구하고 북미시장은 절대치면에서 상당한 수의 가입자를 보유하고 있다.

2.2.2 M-Commerce의 전망

M-Commerce는 시간이 지나감에 따라 기능의 다양화와 비즈니스 활동에 부가가치를 창출해 주는 방향으로 전개된다. M-Commerce 시장은 오는 2003년을 분기점으로 PC를 통한 기존 인터넷 사용자를 능가할 것으로 전망되고 있다[1]. 전 세계적으로 볼 때 향후 2004년경에는 미국을 제외한 나머지 국가에서는 무선인터넷 서비스나 이동컴퓨팅 서비스의 이용자가 인터넷 이용자를 넘어설 것으로 보인다.

최근 Ovum이 발표한 보고서 "Mobile E-Commerce:

〔표 2〕 M-Commerce 분야별 국내시장 전망 (단위:억원)

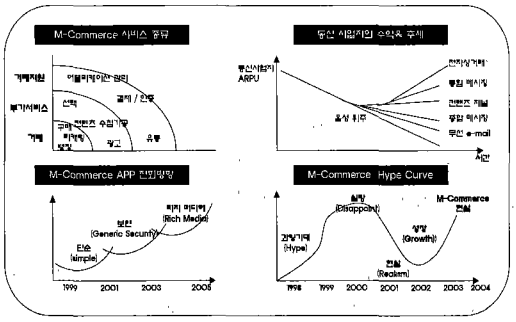
국내시장		2000	2001	2002	2003	2004
분야별	Commerce	0	42	366	1,134	2,434
	Entertainment	1,793	5,296	11,839	14,954	17,614
	Information	1,572	4,929	10,941	13,461	15,225
합계		3,365	10,267	23,146	29,549	35,273

출처 : 이비즈그룹 (2001. 3.)

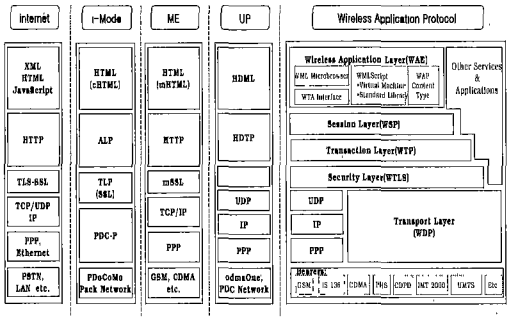
〔표 3〕 M-Commerce 분야별 세계 시장규모 전망 (단위:십억달러)

세계시장	2000	2001	2002	2003	2004	2005
Consumer	2,006	9,472	23,967	51,260	90,381	140,196
Business	1,547	5,691	13,907	31,323	49,877	70,587
합계	3,553	15,163	37,874	82,583	140,258	210,783
증감률		326.8%	149.8%	118.0%	69.8%	50.3%

출처 : Ovum (2000. 6.)



〔그림 4〕 M-Commerce의 진화모델



〔그림 5〕 무선응용프로토콜방식의 비교

Market Strategies"에 따르면, 2000년 M-Commerce의 매출액은 35억 달러로 매우 저조할 것으로 예측되지만, 2002년부터는 빠르게 성장하여 2003년에는 825억달러에 이르고, 2005년에는 2,100억 달러를 넘어설 것으로 전망하고 있다. 이에 각 분야별 매출액 전망을 살펴보면 국내시장은 표 2와 같으며, 세계 시장규모의 전망은 표 3과 같다.

그림 4는 M-Commerce의 진화모델을 단계적으로 분석한 자료로[1] 국내에서는 현재 1단계로, 이미 실현화 또는 구체화 단계에 이르고 있으며, 부분적으로 2단계에 진입하여 서비스를 제공하려는 시도를 하고 있다. 결국 2단계와 3단계에서 비로소 M-Commerce의 영역이 가장 구체화되고, 동시에 고객의 입장에서 가장 편리함을 추구하는 단계이다. M-Commerce 단계에서 가장 중요한 부분은 지금과 같은 1단계에서 서비스되는 이동통신의 특성과 기술적 분석을 벗어나, 진정한 고객 중심의 부가가치를 창출하는 3단계라고 할 수 있다.

Ⅲ. 무선인터넷과 모바일 서비스 플랫폼

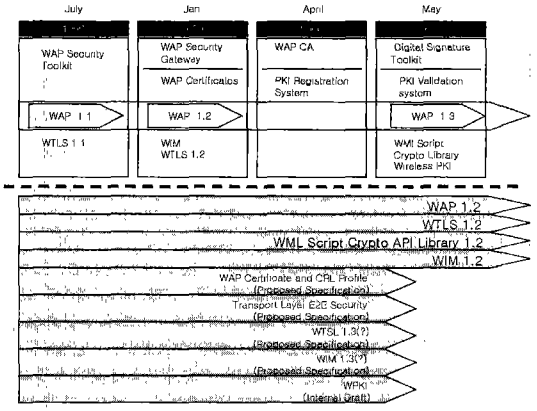
3.1 무선인터넷 응용프로토콜

무선 인터넷은 고정 무선망(무선 LAN, WLL, B-WLL, Bluetooth 등) 및 이동 무선망(IS-95, GSM 등)을 포함하여, 무선을 통해 인터넷 액세스 및 서비스를 받기 위한 환경 및 기술을 의미한다[3]. 실제적으로 이동 무선망, 특히 이동통신망을 이용하여 이동 중에 무선을 통해 인터넷 서비스를 받는 것을 의미한다. 이러한 무선 인터넷의 대표적인 무선 응용프로토콜 표준방식에는 WAP(Wireless Application Protocol)방식, 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 표준 방식이다. i-Mode는 일본의 NTT DoCoMo가 독자적으로 개발한 표준방식으로 자체 패킷망인 PDC를 기반으로 패킷 기반의 무선 인터넷 서비스를 제공한다. 각 무선응용프로토콜 방식의 구조에 대해 비교해 보면 그림 5와 같다.

3.1.1 무선인터넷 표준화 동향

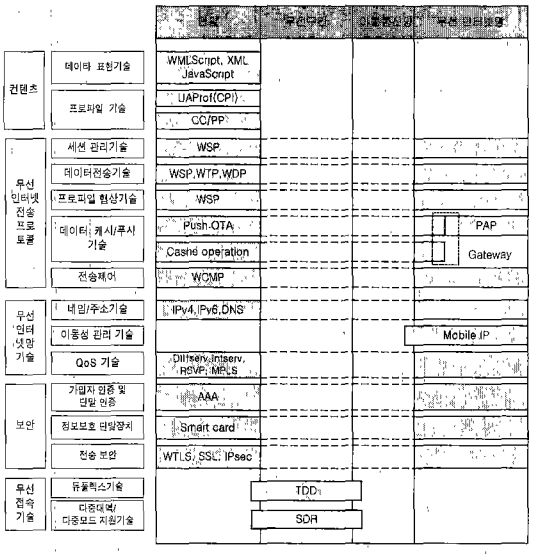
현재 무선인터넷 솔루션의 주류는 Ericsson, Motorola, Nokia, Phone.com(Unwired Planet)를 주축으로 약 300 여 개 업체가 주도하고 있는 WAP Forum과 Microsoft가 주도하는 Mobile Explorer (ME)이다.

WAP Forum에서는 새로운 WAP 프로토콜 표준을 제안하고 있는데 무선 환경에 맞는 프로토콜을 제정하고 고품질의 인터넷 및 전화 부가가치 서비스를 제공하고 이동통신 인프라 관련 표준화 단체에 대한 압력을 행사하는 등 현존하는 표준과의 호환성 (IP, XML기반)과 새로운 무선 데이터 서비스 표준 확립을 목적으로 하며 인터넷 중심의 데이터 서비스를 무선 환경(휴대폰, 호출기, PDA)에서 효율적으로 처리하기 위한 산업체 표준 제정을 목적으로 하고 있다. 지난 3월 말 노키아와 모토로라, 에릭슨, 지멘스를 포함하는 다수의 이동통신사업자들은 차세대 무선 서비스를 위한 표준 포맷으로 XHTML(Extensible Hyper Text Markup Language)의 지지를 공표함과 아울러 이를 기반으로 하는 제품과 컨텐츠, 서비스 개발에 본격적으로 착수할 계획이라고 밝혔다. 현재 WAP Forum에서 진행되고 있는 표준화 과정은 그림 6과 같다.



〔그림 6〕 WAP Protocol Stack의 표준화 동향

MS에서는 기존의 TCP/IP, HTTP 환경을 그대로 활용하는 방안을 내놓고 있다. 최근에는 차세대 통합 운영체계 개발을 발표하였는데 이는 유, 무선을 통합하여 접속하고 무선환경에서 기존의 Web 응용 프로그램을 이용할 수 있으며 .com을 뛰어넘는 .net의 환경을 추구할 것이라고 한다. 현재 시점에서 미래의 무선 인터넷 솔루션의 발전방향을 예측하기는 어려운 상황이다. 현재 무선인터넷 정보보호 시스템 개발 사업은 기본적으로 WAP을 기반으로 진행되고 있지만 ME의 솔루션을 간과하지는 않고 있다. 이러한 세계적인 표준화 동향에 맞춰 국내의 표준화동향 및 추진방향을 살펴보면 다음 그림 7과 같다.



(출처 : ETRI, 2000. 8.)

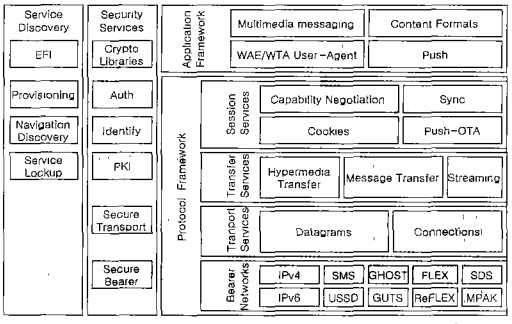
〔그림 7〕 국내 무선인터넷 표준화동향 및 추진방향

국내에서는 2000년 2월경 정보통신부를 중심으로 국가 차원의 검토작업에 들어간 바 있으며, 6월 중순경 "무선 인터넷 정책 전담반"을 구성하여, 정책/기술적인 측면과 더불어 표준체계 확립을 위한 연구에 착수하였으며, 올해 6월경 표준화 포럼을 발족하여 활동하고 있다.

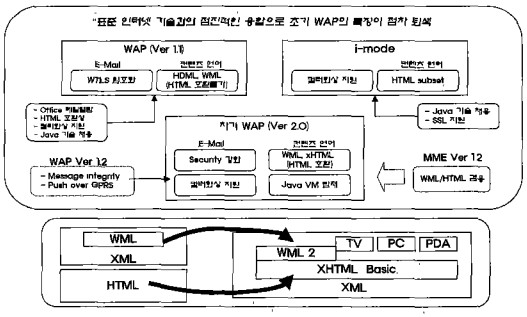
3.1.2 차세대 WAP의 발전방향

최근 조금씩 알려진 WAP 2.0의 골격을 보면 IP 기반의 통신 방식을 채용, TCP · TLS · HTTP 등의 프로토콜을 채택하고 있다. 즉, WAP의 응용 및 컨텐츠 환경만 남고 근간을 이루던 전송 프로토콜은 모두 사라져 버린 것이다. 작년에 발표된 새로운 WAP Spec의 구조를 살펴보면 그림 8과 같다. 따라서, 무선인터넷이든 유선인터넷이든 통신 프로토콜 및 서비스에서는 두드러진 차이가 나타나지 않는 환경이 되고 무선인터넷 단말기의 특수한 사용자 환경에 맞는 콘텐츠만이 차이점을 보이게 될 것으로 예상된다.

W3C가 XHTML을 개발하게 된 중요한 배경 중의 하나로 이식성(Portability)을 들 수 있다. 기존의 HTML 사용자는 PC 중심의 웹 브라우저만을 이용하였으나, XHTML을 사용하면 Mobile Phone, Palm, 셋톱박스 등을 지원할 수 있으며, 전자상거래 등에서 사용하는 특정양식을 XHTML의 새로운 양식 옵션을 통하여 지원할 수 있다. 특히, XHTML을 무선기기에 맞게 코드를 대폭 간소화시킨 XHTML Basic의 개발이 하드웨어적인 한계를 가지고 있는 이동기기에 매우 적합하도록 고안되어 Mobile Phone, PDA, TV에 이르기까지 폭 넓게 적용될 수 있게 되었다. 이와 같이 XHTML은 유무선 인터넷에서 동시에 사용할 수 있으며 유무선에 관계없이 인터넷 컨텐츠를 만들 수 있다는 특징을 지니고 있다.



〔그림 8〕 WAP 2.0 구조의 구성요소



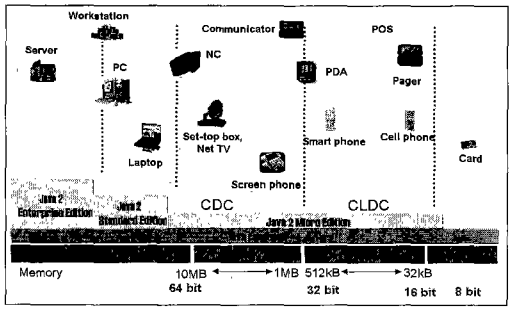
〔그림 9〕 WAP의 발전방향

3.2 모바일 서비스 플랫폼

3.2.1 자바 모바일 플랫폼

현재의 이동통신 단말기에 일반 PC와 같은 수준의 자바 플랫폼을 탑재하는 것은 불가능하다. 이에 썬 마이크로시스템즈사에서는 페이저, PDA, 셋톱박스, 이동통신 단말기들의 작은 디바이스들을 위한 솔루션으로 Java 2 Micro Edition(J2ME)을 제시하였다. 이에, 자바 플랫폼은 자바 2 플랫폼이라는 마케팅 개념이 가미된 새로운 플랫폼으로 진화하면서 J2EE (Java 2 Enterprise Edition), J2SE (Java 2 Standard Edition), J2ME(Java 2 Micro Edition)라는 세 가지 영역으로 분할되었다. 이것은 각각 엔터프라이즈 서버 시장, 데스크탑 시장, 소비자/임베디드 디바이스 시장을 목표로 한 역할 분담이었다. 그림 10은 이러한 자바 2 플랫폼의 분할을 설명하고 있다[7].

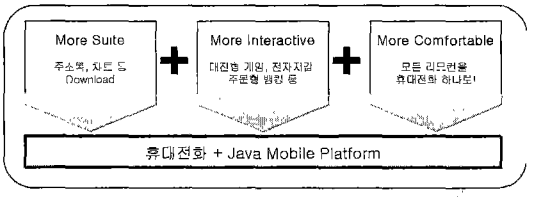
자바의 무선환경 분야에서의 진화는 매우 빠르게 움직이고 있다 무선 환경의 시장이 지금 현재의 가장 큰 시장이라는 공식은 변화의 가속도를 더욱 높이고 있다. 그리고 무선망 사업자와 단말기 제조업체를 중심으로 한 무선 시장의 주요 플레이어들의 자바 모바일 플랫폼 필요성을 살펴보면 동적 어플리



〔그림 10〕 Java 2 플랫폼의 구조

〔표 4〕 WAP과 JAVA 기술의 비교

	WAP	Java
개발회사	WAP Forum	SUN Microsystem
현 서비스 수준	Text 위주의 HTML 형태	프로그램 형태(Class File)의 다양한 형태 지원
서비스	통신사업자, 단말기에 의존적 서비스	H/W에 비의존적이므로 다양한 형태의 서비스
보안	WTLS는 보안의 취약성 내포	보안 Algorithm 및 전자서명 지원
Upgrade	하드웨어 Upgrade 및 교체	Software적으로 가능
이용방법	이용시마다 계속 접속	Download 후 계속 이용
Interface	Text위주, 작은 BMP 지원	다양한 그래픽 지원



〔그림 11〕 자바 모바일 플랫폼의 효과

케이션의 다운로드 서비스 기능 제공, 플랫폼간의 호환성 제공, 향상된 인터페이스의 표현, 네트워크 환경과의 비연결성 고려, 무선환경의 종단간 보안문제 해결책 등의 요소로 볼 수 있다. 현재의 무선 인터넷방식 WAP과 자바 환경의 서비스 플랫폼을 비교하면 위의 표 4와 같다.

향후의 무선 어플리케이션과 서비스는 실시간 동적으로, 그리고 안전하게 다운로드될 것이다. 자바는 이러한 실행코드의 네트워크 이동성을 보장하는 가장 우수한 솔루션이며, 차세대 모바일 솔루션의 기본적인 요소인 플랫폼간의 호환성을 제공한다. 동적으로 다운로드된 자바 어플리케이션은 근본적인 무선 환경의 유저 인터페이스를 탈피해 사용자들의 만족도를 높여 주며, 사용자의 전파 수신 불가능 환경에서의 상황을 고려한 동기화된 네트워크 연결성을 보장해 주어야 하는 측면에서 자바는 유리한 위치에 있다. 그리고, 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 환경으로의 필요성을 말할 수 있다.

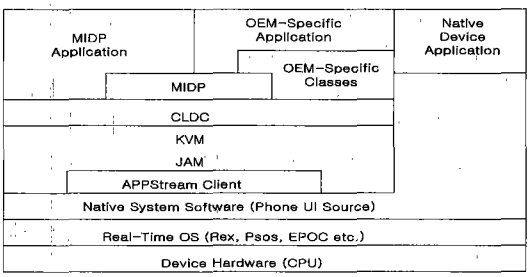
① CLDC (Connected Limited Device Configuration)

Java 2 Platform의 Micro Edition, J2ME 기술은 소비자 기기와 임베디드 기기 전반에 걸쳐 있다. 이동용 기기에서 사용 가능한 하드웨어 사양

과 네트워크 자원은 일반적인 전원(벽에 붙어있는)을 이용하는 기기보다 상대적으로 제한될 수 밖에 없다. CLDC는 128~512K의 메모리 여유공간과 16~32비트 프로세서, 저전력 소모, 네트워크 연결성을 가진 디바이스를 목표로 하고 있다[7].

CLDC의 특징은 부동 소수점을 지원하는 것은 오버헤드를 발생하기 때문에 지원하지 않고, Finalization과 가비지 컬렉션을 지원하지 않는다. 예외처리를 지원하지만 임베디드 환경에 의해 제한된 에러 처리만 하고, 네이티브 함수를 호출하는 JNI는 지원하지 않고, 또한 리플레션을 지원하지 않는다. 보안 문제에 있어서는 보안 모듈 자체가 CLDC 구현보다 크기 때문에 저수준의 가상머신 보안과 어플리케이션 레벨의 보안을 제공한다.

J2ME의 CLDC/MIDP 세부 구조는 다음의 그림 12와 같다.



〔그림 12〕 CLDC/MIDP Architecture

MID 부분은 Mobile Information Device의 하드웨어를 의미하며, 그 위의 Native System Software는 그 디바이스에서 사용되는 OS와 각종 라이브러리들을 의미한다. Native System Software 층 위에는 차례대로 CLDC와 MIDP, 그리고 OEM-Specific Classes라는 별도의 API가 탑재되는데, 이상과 같은 API를 기반으로 하여 휴대폰 단말기가 실행시킬 수 있는 프로그램들은 MIDP Applications, OEM-Specific Applications, Native Applications와 같이 세 가지로 분류된다.

② MIDP (Mobile Information Device Profile)

Java API의 한 묶음으로, CLDC와 함께 셀룰러 폰, 양방향 삐삐와 같은 이동 정보 단말기를 위한 J2ME 어플리케이션 운영 환경을 제공한다. MIDP는 사용자 인터페이스, 비휘발성 저장 장치, 네트워킹, 그리고 어플리케이션 모델에 대한 정의를 제공한다. 또한, MIDP는 최종 사용자가 동적으로 자신의 디바이스에 어플리케이션을 설치하는 방법을 기본으로 제공한다.

〔표 5〕 Java Application Manager의 기능

기 능	설 명
추출(Retreival)	서버로부터 MIDlet 추출
설치(Installation)	추출한 MIDlet을 디바이스에 설치
실행(Launching)	MIDlet 호출
버전관리	기존 MIDlet을 새 버전으로 Upgrade
삭제(Removal)	설치된 프로그램을 삭제

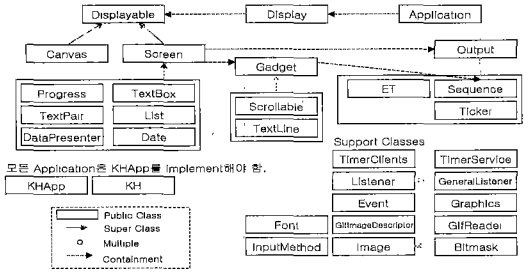
JAM(Java Application Manager)은 CLDC/MIDP 플랫폼의 새로운 어플리케이션 모델을 지원하기 위한 어플리케이션 관리 소프트웨어이고, 그 역할은 MIDP 어플리케이션인 MIDlet를 다운로드하여 설치, 업그레이드, 실행, 삭제하는 것이다. 다음 표 5는 JAM의 기본적인 기능이다.

3.2.2 상용 모바일 서비스 플랫폼

게임 등 멀티미디어 소프트웨어를 무선인터넷을 통해 내려 받아 실행시킬 수 있도록 해 주는 '소프트웨어 플랫폼' 시장이 빠르게 확대되고 있다. 현재 국내에서는 신지소프트의 스왑(SWAP), 썬마이크로시스템즈의 자바플랫폼에 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. 이들 플랫폼은 대부분 휴대폰에 '버추얼머신(VM)' 형태로 탑재돼 노래방, 게임, 모바일 북, 만화, DDR 등 다양한 콘텐츠를 이용할 수 있게 한다. 이 VM을 이용해 게임을 할 경우, 정지된 화면과 텍스트 위주의 WAP 게임에 비해 빠른 실행속도와 사운드 지원으로 다이나믹한 게임을 즐길 수 있다. 또 다운로드 방식으로 각종정보를 휴대폰에 저장하므로 접속 끊김이나 비싼 통화료 등 단점을 극복할 수 있다. 특히 VM의 경우, 모든 종류의 휴대폰에 적용할 수 있어 범용성 확보 및 새로운 상품개발에 용이하다.

① EZ-JAVA(KVM)

가장 먼저 상용화된 것으로 지난해 10월 국내에서 LG텔레콤은 SUN으로부터 자바 관련 기술을 이전 받아 'KVM'(Kilobite Virtual Machine)을 개발했다. 'Ez-java(kittyhawk)'라는 브랜드명으

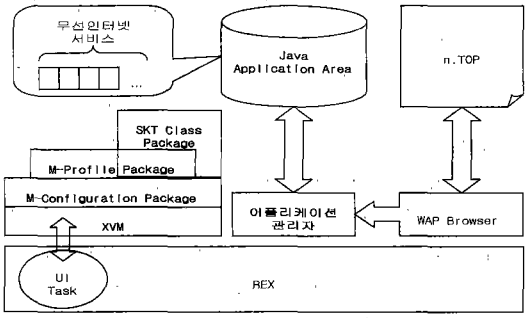


〔그림 13〕 KittyHawk Class Diagram

로 현재 20여개의 업체가 이 플랫폼을 이용해 60여개의 컨텐츠를 서비스하고 있다. KVM은 게임 용량이 30K로 정해져 있고 1폴리 사운드 칩을 사용해 게임에 적합한 사운드를 지원할 수 없다는 단점이 있다. 사운드 문제는 새로운 휴대폰이 나오면 해결될 전망이다.

② SK-VM

SK-VM은 SK텔레콤에서 Clean Room 기반으로 자체 개발한 J2ME 자바 실행 환경으로 가상머신 및 단말 확장 UI, 네트워크, IO를 포함하는 클래스 라이브러리로 구성되어 있고, 무선이동단말기에서 응용프로그램을 다운로드 및 실행시킬 수 있는 환경을 제공한다. 먼저 SK-VM 플랫폼에 대한 구조를 살펴보면 그림18과 같다.



〔그림 14〕 SK텔레콤 SK-VM 플랫폼의 구조

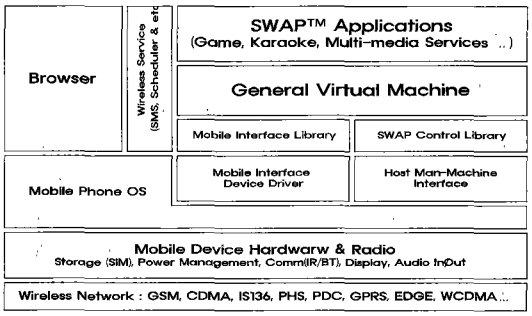
위 그림에서 오른쪽 요소들이 SK-VM 플랫폼의 구성요소로 단말기에 추가되어 탑재되는 부분으로, J2ME의 구성 요소들을 Clean Room Implementation 한 것이다. XVM은 KVM을 구현한 것이며, M-Configuration Package는 CLDC를, M-Profile Package는 MIDP를 구현한 것이다. 그리고 SKT Class Package는 SK텔레콤에서 무선인터넷 서비스에 필요한 API를 정의한 것으로 J2ME 구성요소 중에서 OEM-Specific Classes 부분에 해당된다.

M-Profile은 일반적인 UI의 생성에 기초를 하고 있기 때문에 M-Configuration과 M-Profile만을 사용해서 실시간 게임을 개발하는 데에는 한계가 있다. 이에, SK-VM 플랫폼에서는 게임과 같은 실시간 어플리케이션의 개발을 위해서 M-Profile과는 달리 속도와 성능을 고려하여 개발된 별도의 클래스를 제공하고 있다.

③ GVM (General Virtual Machine)

자바플랫폼에 이어 모습을 드러낸 것은 신지소프트의 SWAP(Sinji Wireless Application Plug In)으로, C언어를 기반으로 자체 개발한 휴대폰 단말기용 프로그램 스크립트 다운로드 솔루션이다. 주요 특징으로는 적은 메모리/CPU 사용으로 통화품질이 우수하며, 다양한 어플리케이션 개발에 편리함을 제공한다. TCP/IP에 직접 연결하여 사용하므로 Browser에 상관없이 서비스를 제공할 수 있고, 4폴리의 미디 사운드를 지원한다. 하지만, 현재 표준화의 가능이 낮고, 보안이 취약하다는 단점이 있다.

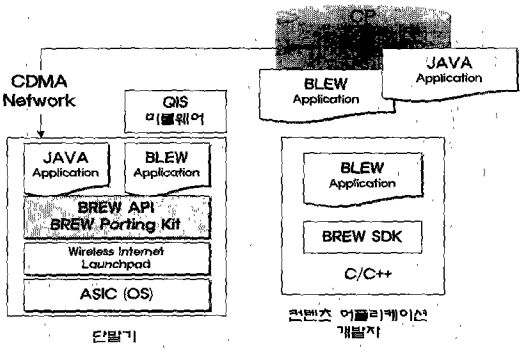
SK텔레콤이 GVM이란 이름으로 서비스하고 있으며 현재 10여개 업체가 노래방, DDR, 고스톱, 게임 등 30여 개의 다양한 콘텐츠를 제공하고 있다. 향후 야구게임, 만화 등 다양한 콘텐츠가 추가될 예정이다.



〔그림 15〕 GVM 플랫폼의 구조

④ BREW (Binary Runtime Environment for Wireless)

미국 퀄컴사가 개발한 CDMA기반 무선기기를 위하여 개발한 차세대 오픈 소프트웨어 플랫폼으로, 바이너리 다운로드 방식을 사용하는 플랫폼이다. BREW기술이 탑재된 이동통신사 네트워크를 통해 무선으로 원하는 데이터를 다운받고, 단말기의 S/W도 무선 업그레이드 받을 수 있다는 것과 라이센스



〔그림 16〕 BREW 플랫폼의 구조

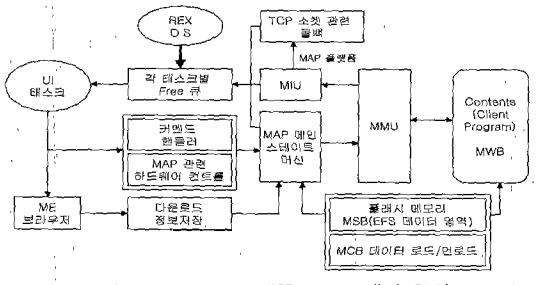
가 무료라는 장점이 있으나, BREW를 탑재한 단말기로만 사용 가능하다는 단점이 있다. 그러나, H/W와 직접 접속이 가능하기 때문에 속도가 빠르다. 아울러 BREW 플랫폼상에서 자바 VM을 탑재해 자바를 실행시키는 것도 가능하므로 단순한 자바 VM과는 크게 다르다. BREW는 아래 같이 Application(Wireless Launchpad Suite), API(Poting Kit), SDK(SW 개발도구), Middleware (QIS: 퀄컴인터넷서비스)의 4가지 모듈로 구성되어 있다.

퀄컴은 오는 2001년 하반기에 국내에서 기기 제조업체들에 라이센스 없이 무료로 제공할 계획에 있다.

⑤ MAP (Mobile Application S/W Plug-In)

국내 ㈜모빌탑이 C언어를 기반으로 자체 개발한 휴대폰 단말기용 프로그램 스크립트 다운로드 솔루션이다. C언어를 기반으로 제작된 컨텐츠를 서버에서 Binary 형태로 다운받아 단말기내에 탑재한 API (Application Program Interface)를 이용하여 실행되는 것이다.

C언어 VM을 휴대폰에 탑재한 것으로, 다양한 Application 개발에 편리하며, 1폴리의 미디사운드를 지원한다. 현재 플러그인 서비스를 한통프리텔과 한통엠닷컴의 매직ⓝ을 통해 서비스하고 있다.

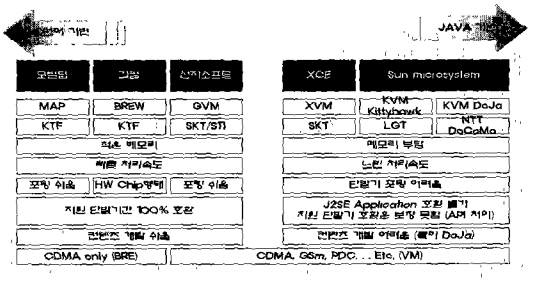


〔그림 17〕 MAP 플랫폼 소프트웨어 구성도

3.2.3 모바일 서비스 플랫폼의 비교

단말기 탑재용 Virtual Machine의 종류별 장단점을 비교해 보면, 무선 플랫폼 시장을 선점하고 있는 자바 플랫폼은 버추얼머신이 번역과정을 거쳐 실행파일을 생성한 후 어플리케이션을 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. 현재 국내에서는 LG텔레콤이 채택하였고, 보다폰, 도이치텔레폰, 스프린트, 모토롤라, 노키아 등과 같은 세계적인 업체들이 표준으로 채택할 예정으로 있다. 일본의 NTT DoCoMo i-Mode도 MIDP를 채택한 KVM을 탑재하였다.

이에 반해, C 기반의 무선서비스 플랫폼 방식은 자바 서비스 플랫폼에 비해 메모리 확장이나 HW의 개선없이 단말기에 소프트웨어만 수정하여 탑재 가능하다는 장점과 동적인 네트워크 게임 제공이 유리하다는 장점이 있다. 국내에서 신지소프트와 SK텔레콤에 의해 개발된 GVM이 있고, IS-95C를 필두로 작년 10월경부터 서비스를 개시하였다. 현재는 단말기가 한정되어 있지만, 향후 모든 단말기로 확대될 예정이다.



〔그림 18〕 상용 모바일 서비스 플랫폼의 비교

현재 국내이동통신사들은 각기 다른 플랫폼을 도입, 컨텐츠와 단말기 개발업체들에 미치는 악영향이 크다고 판단하여 앞으로 국내 모바일 서비스 플랫폼의 표준을 위한 작업을 2001년 7월부터 시작하였다. 이들의 구체적인 논의는 '한국 무선인터넷 표준화 포럼'과 '한국정보통신기술협회'가 될 전망이다.

3.2.4 J2ME 플랫폼 표준화 동향

JCP(Java Community Process)라는 조정 위원회에서 현재 작업중인 J2ME 플랫폼은 표 6과 같다.

〔표 6〕 J2ME 플랫폼 표준화 동향

명 칭	요구사항 정의	명세서 버전
CLDC	JSR-30	1.0 (Public Review)
MIDP	JSR-37	1.0 (Public Review)
CDC	JSR-36	0.5 (JCP Review)
Foundation Profile	JSR-46	·
Personal Profile	JSR-62	·
RMI Profile	JSR-66	·

(출처 : http://java.sun.com/jcp)

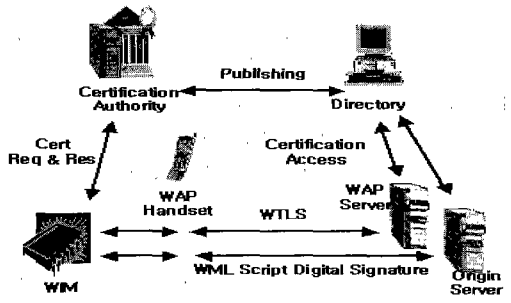
J2ME 플랫폼은 J2EE, J2SE와는 달리 다중 컨피규레이션을 수용하고 있으며, 특히 메모리의 요구사항에 따라 두 가지의 컨피규레이션이 정의되고 있다. 즉, 128K~512K의 메모리가 가용한 디바이스들은 CLDC로, 512K 이상(주로 2M 정도)의 메모리가 가용한 디바이스들은 CDC라는 컨피규레이션을 적용하려 하고 있다. CLDC는 KVM을 기본 가상머신으로 채택하고 있으며, CDC는 기존의 퍼스널 자바를 바탕으로 표준화 작업이 진행중이다. MIDP는 CLDC를 기반으로 양방향 페이저, 셀룰러폰, 무선 기능이 탑재된 PDA 등의 Mobile Information Device (MID)를 목표로 정의된 프로파일이다. Personal Profile, Foundation Profile, RMI Profile 등을 CDC를 기반으로 하는 프로파일이며, JCP에서 표준화를 진행중이다.

Ⅳ. 무선 전자상거래 보안

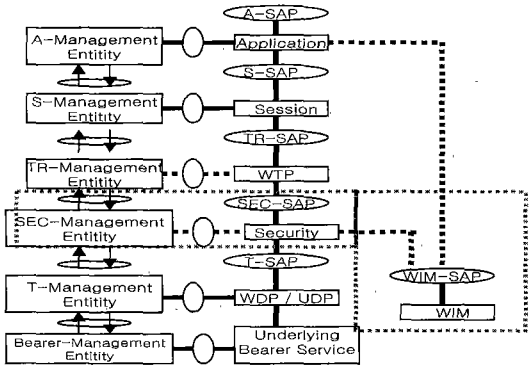
4.1 무선인터넷 방식에서의 보안기술

4.1.1 WAP 보안기술

현재 사실상 국제표준으로 자리 매김하고 있는 WAP 표준의 보안기술은 WAP 프로토콜 구조의 네번째 계층인 WTLS에서 이루어지며, 이는 유선



〔그림 19〕 WAP 보안 구성요소



〔그림 20〕 WAP 계층 보안 모델

인터넷 TLS를 근간으로 작성된 보안 프로토콜로서 무결성, 기밀성, 인증 등의 보안 서비스를 제공하게 된다. WAP 환경의 보안 구성요소와 WAP 계층별 보안 모델을 살펴보면 아래의 그림 19, 그림 20과 같다.

WAP 1.2에서 무선 인터넷 보안과 관련해서 WTLS, WPKI, WIM, WMLScript Crypto Library, Transport Layer End-to-End Security 등에 관한 표준규격에서 기술하고 있는데, 상세한 내역을 살펴보면 표 7과 같다.

〔표 7〕 WAP 관련 보안 표준규격 내용

표준 목록	주요 내용
Wireless Transport Layer Security (WTLS)Spec	산업표준인 TLS 프로토콜에 기반을 두며 협대역 통신에 적합하도록 최적화된 보안 프로토콜로서 단말기와 응용서버 사이에서 무결성, 기밀성, 인증 및 서비스 거부공격에 대응하는 기능을 제공
WMLScript Crypto Lib Spec	응용계층에서 사용자 메시지에 대한 전자 서명 기능을 제공하여 트랜잭션에 대하여 부인방지 서비스가 가능하도록 하는 응용계층의 보안 프로토콜의 스펙
WAP Identity Module Spec	WAP에서 사용되는 인증서에 대한 안전성을 높이기 위한 인증서의 보관 및 연산을 담당하는 모듈 스펙
Transport Layer E2E Security Spec	WAP의 종단간 보안문제를 해결하기 위해 전송계층에서 클라이언트와 서버를 WTLS 보안 세션으로 연결하는 방법을 제시하고 있는 스펙
WAP Public Key Infrastructure Definition	무선환경에 적합한 공개키 기반구조에 관해 사용자와 게이트웨이의 인증서 발급에 대한 정의를 하고 있는 스펙
WAP Certificate and CRL Profile Spec	WPKI에서 사용되어지는 WAP 인증서 및 인증서 취소목록에 관한 프로파일을 정의하고 있는 스펙

① WTLS (Wireless Transport Layer Security)

WTLS는 인터넷의 보안 메커니즘인 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security)에 기반해서 작성된 것으로, WTLS는 통신을 하는 두 응용 프로그램 사이에 안전한 채널을 형성하여 통신의 내용을 보장하는 방법이다. WTP와 WDP 사이에서 수행되며 WAP을 사용하는 모든 응용프로그램들을 지원한다. WTLS는 기밀성, 사용자 인증, 메시지 무결성 등의 보안 서비스를 제공하나, 부인방지는 제공하지 않는다. 두 응용간의 기밀성 서비스는 DES, IDEA 등과 같은 관용 암호방식을 사용하여 제공되는데 이때 사용되는 비밀키는 Handshake 프로토콜을 통해 생성되며, 기밀성을 필요로 하는 다수의 어플리케이션 각각에 대해 다양한 암호 알고리즘을 제공할 수 있다. 클라이언트와 서버의 상호 인증은 연결 설정과정에서 서로간에 신뢰할 수 있도록 클라이언트와 서버가 서로에 대해 인증할 수 있도록 하는데, 공개키 암호방식과 무선 X.509 인증서가 사용된다. 메시지 무결성 서비스는 MAC(Message Authentocation Code)기법을 함께 이용하여 데이터 변조 여부를 확인할 수 있다.

WTLS와 SSL/TLS와의 차이점을 살펴보면 첫째, SSL/TLS는 TCP/IP위의 Connection oriented transport protocol이지만 WTLS는 WDP(Wireless Datagram Protocol)위의 Datagram Transport Porotocol을 지원한다. 따라서 Datagram의 유실, 중복, 순서의 뒤바뀜 등을 체크할 수 있도록 Sequence Number를 Record Layer의 헤더에 Explicit Field로 사용한다. 둘째, 통신에 걸리는 시간이 유선환경과 다르다. 즉, 메시지 요청에 대한 응답 대기 시간이 10초 이상 매우 길수도 있음을 고려한다. 셋째, 통신 속도에 제한이 있으므로 가능한 통신 데이터량을 최소로 해야 한다. 따라서 TLS에 비해 많은 부분에서 데이터의 길이를 가능하면 줄이고 있다. 특히 인증서의 경우 무선전용 인증서 포맷을 사용토록 한다. 넷째, 무선 단말기의 메모리와 Processer의 Power가 제한되어 있으므로 사용할 수 있는 알고리즘에 제한이 있다. 연산이 많이 걸리는 암호 알고리즘이나 RAM을 많이 필요로 하는 알고리즘 등을 적용하기 어렵다. 다섯째, 아직 WTLS에 대한 세계적인 표준화가 안되어 있으므로 국가마다의 다른 알고리즘에 대한 정책도 고려해야 한다. 이 중 가장 큰 차이점은 SSL/TLS이 Connection-oriented 프로토콜인 TCP 상위에서 동작하는데 비해, WTLS는 Datagram Protocol인 UDP 또는 WDP 상위에서 동작한다는 점이다. 따라서 SSL/TLS가 재전송, 중복된 데이터 처리 등의 기능을 수행하지 않아도 되는 반면에 WTLS에서는 통신의 신뢰성을 보장할 수 있는 방법이 추가되어야 한다[14].

② WMLScript Crypto Library

WMLScript Crypto Library는 WTLS에서 지원하지 않는 전자서명 기능을 응용 계층에서 Crypto.signText() 함수를 이용해 부인방지 서비스를 제공한다. 부인방지 서비스는 전송되어지는 데이터에 대해서 전자서명을 수행함으로써 제공이 가능한데, 전송되는 모든 데이터에 대해서 전자서명을 수행하는 것은 많은 연산을 필요로 하기 때문에 비효율적이다. 이에, 어플리케이션 계층에서 제공하는 WML Script에서 제공되어지고 있다. Crypto.signText() 함수를 이용해 WML 문서 단위로 서명하기 때문에 사용자는 필요한 중요 문서에만 전자서명을 수행함으로써 실행에 대한 최소한의 부담을 줄일 수가 있으나, 현재 단말기의 성능 제한으로 인해 많은 시간이 소요된다. 그리고, 개별적인 무선 암호라이브러리에 의한 응용계층의 암호화없이는 Gateway에서의 보안상 헛점이 발생하기 때문에 보완적인 기능으로만 사용되어지고 있다.

③ WIM (WAP Identity Modules)

WTLS와 응용레벨에서 보안 함수를 수행하는데 필요한 암호 연산을 지원하기 위해 비밀키 및 인증서를 저장한다. 무선 단말기의 취약한 보안을 위해 사용되는 요소로 스마트카드로 구현된다.

WAP에서 WIM을 사용하는 목적은 보안 정보를 안전하게 저장하기 위한 목적과 보안 정보에 관한 연산을 WIM 내부적으로 처리하여 보안 정보의 노출을 방지하기 위함이다. WAP에서 WIM의 사용은 WTLS에서 핸드쉐이크 동안에 클라이언트 인증을 위한 암호 연산을 위하여 사용되며, 연결 지속시간이 긴 WTLS 세션을 보호하기 위하여 사용된다. 또한 WTLS에서 디지털 서명을 위한 경우로 나뉘어진다. 따라서 참조모델에서 WTLS, WALS, WIM의 관계를 나타내면 앞서 보았던 그림 20과 같이 나타낼 수 있다. 사용자는 WPKI에 따라서 인증서를 발급받으면 WIM에 보관하고, WIM은 안전한 통신을 필요로 하는 응용을 사용하는 경우에 WTLS

와 WALS의 요구에 따라서 인증서에 관련된 연산을 실행한다.

스마트카드로 구현할 때에 인터페이스 규격은 ISO7816 규격에 기반하며, WIM에 저장하는 정보의 구조는 PKCS#15를 준용한다. 스마트카드를 이용한 WIM의 구현은 가장 쉽게 적용할 수 있는 예에 불과하지만, 휴대전화에서 SIM(Subscriber Identity Module) 카드와 같은 여러 응용을 가진 다용도의 카드로서 구현되어, 보안 정보를 효율적으로 보관하고 여러 형태의 단말에 동시에 사용할 수 있기 때문에 향후 사용이 더욱 확대될 전망이다.

④ WPKI (WAP Public Key Infrastructure)

현재 WAP 포럼에서 제안하고 있는 무선 PKI 관련 표준 기술은 WAP Public Key Infrastructure와 WAP Certificate and CRL Profile Spec이다.

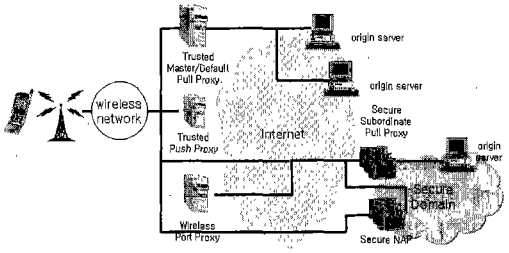
WAP에서 제안하고 있는 WPKI에서의 보안 시스템은 MS(Mobile Station), WAP Gateway, CP(Contents Provider), 인증시스템, 등록관리 및 포탈 시스템으로 구성된다. WPKI는 서버와 클라이언트간의 인증을 위해 무선 환경에 적합한 공개키 기반 구조를 제공한다. 유선 공개키 기반 구조와의 호환 등을 고려해서 일반적으로 서버는 WTLS에서 정의하는 인증서를 사용하고 클라이언트는 X.509v3 형식을 사용한다.

현재 WAP 포럼에서는 WAP 1.2에서 정의된 보안 기능을 관리하기 위해서 필요한 기능을 정리하여 WAP PKI 모델을 정립하고 있는 초기 단계로서, WTLS 2등급용 게이트웨이 인증서, WTLS 등급 3용 클라이언트 인증서, 디지털 서명을 위한 클라이언트 인증서 등에 대하여 작업이 진행되고 있다. 이 작업은 현재 인터넷에서 사실상의 표준으로 받아들여 지고 있는 IETF(Internet Engineering Task Force)의 PKIX(Public Key Infrastructure X.509) 작업반의 연구 결과에 기반하고 있지만, WAP 포럼의 다른 연구 영역에 비해서는 미진한 상태이다. 주요 특징적인 내용은 다음과 같다.

- MS에서는 자신의 인증서를 LDAP URL 형태로 수신한다.
- MS과 CP 사이의 전자서명 및 검증을 위해서는 WML Crypto Library인 SignText, Verify Text를 사용한다.
- WTLS 인증서는 유선망의 인증서 폐지 목록의 무선망 적용에 대한 오버 헤드로 인하여 24시간마다 갱신되는 형태를 취한다.
- WTLS 및 SSL을 통한 전송 계층 데이터 보안 서비스를 제공한다.
- WAP Gateway로 인한 종단간 데이터 보안 서비스 처리가 불가하다.

⑤ Transport Layer End-to-End Security

게이트웨이를 이용한 무선과 유선간의 프로토콜 변환으로 발생하는 WTLS 종단간 보안의 문제점은 Transport Layer에서 해결될 수 있다. Transport Layer 종단간 보안을 구성하는 요소들의 역할은 다음과 같다[15].

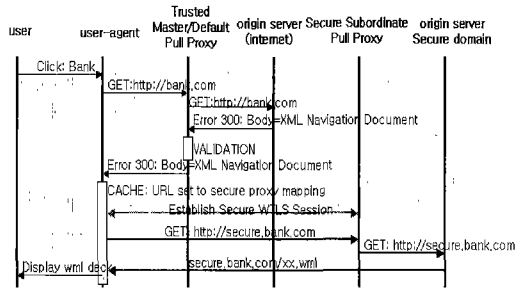


〔그림 21〕 Transport Layer E2E 구조의 구성요소

- Master Pull Proxy : Navigation Document 전송에 관련하는 신뢰된 개체
- Trusted Push Proxy : 서버와 클라이언트에 푸시 서비스 제공
- Wireless Port Proxy : WDP와 UDP 사이의 게이트웨이 제공
- Secure Domain : 서비스 제공자에 의해서 제공되는 안전한 네트워크 환경
- Subordinate Pull Proxy : 서비스 제공자의 영역에 있는 안전한 프락시
- Origin Server : WAP 서비스 제공

위의 보안 요소들을 바탕으로 Transport Layer 종단간 보안을 설정하는 과정은 서비스 제공자의 프락시, 즉, Secure Subordinate Pull Proxy를 통해 이루어진다. 종단간 보안 설정과정을 5개로 구분해서 설명하면 그림 22와 같다.

- 사용자가 Trusted Master Pull Proxy를 통해 원하는 응용서버(예:은행)에 http//bank.com으로 접속한다.



〔그림 22〕 Transport Layer End-to-End 구조의 순서도

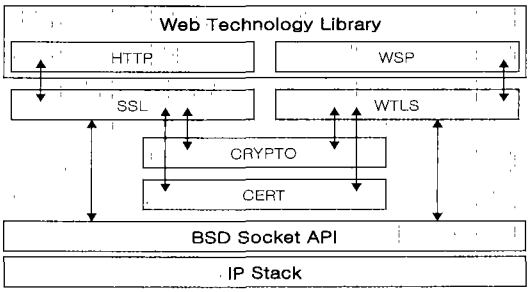
- 응용 서버는 HTTP 300 에러코드와 자신의 Secure Subordinate Pull Proxy까지 도달할 수 있는 정보를 포함하는 XML Navigation Document를 보낸다.
- Trusted Master Pull Proxy는 받은 정보에 대한 검증을 거쳐서 사용자에게 전달한다.
- 사용자는 관련 정보를 토대로 Secure Subordinate Pull Proxy에 접속해서 안전한 WTLS 세션을 설정하고 암호화된 통신(http://secure.bank.com)을 한다.
- 서버는 사용자에게 secure.bank.com/xx.wml 과 같은 WAP 응용 서비스를 제공한다.

이러한 WTLS를 이용한 메커니즘은 WAP 포럼에 제안된 상태로 아직 정식으로 승인된 규격은 아니다.

4.1.2 ME 보안기술

MS에서 개발한 ME 1.0에는 SSL이 포함되어 있지 않다. 따라서 증권, 뱅킹 거래 등에는 활용할 수 없는 제약이 있었으므로 보안이 요구되는 국내 환경을 위해 소프트포럼의 SSL 솔루션을 채택하였고 ME 1.0을 위한 SSL을 단말기에 포팅하였다. 소프트포럼의 SSL 솔루션은 SSL v.3 표준을 준수하고 있다. 따라서 일반 웹 서버와 SSL 통신을 할 수 있다. 향후 MME 2.0에서 제시하는 보안기술의 구조는 다음의 그림 23과 같다

MS ME용의 SSL 모듈에서는 사용자 인증 기능을 제공하지는 않는다. 이것은 현재 일반적인 보안 웹 서비스에서와 같이 익명 SSL 세션을 만들고 ID와 비밀번호로 인증을 수행한다는 의미이다. SSL의 인증 기능을 사용하기 위해서는 단말기에서 RSA 개인키 연산이 수행되어야 하는데 현재 단말기의 스펙에서 RSA 개인키 연산 시간만 약 10초 정도 소



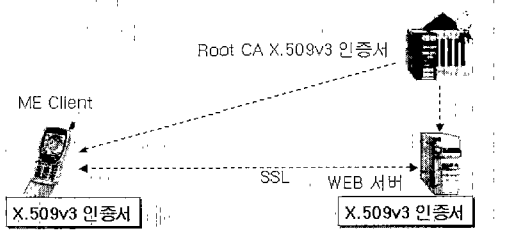
〔그림 23〕 MME 2.0의 보안기술 구조

요되며 실제 상황에서는 이보다 더 많은 시간이 소요될 것으로 추정되므로 현실적으로 불가능하다. 따라서 SSL에서 인증 기능을 제공하기 위해서는 스마트 카드를 사용하는 것이 필요하다.

국내의 ME를 채택한 단말기에 들어가는 소프트포럼의 mSSL의 특징은 다음과 같다[12].

- SSL 128비트 암호 서비스 제공
- 기존 SSL 40비트/128비트
- 암호서비스와의 연동 SSLv3 보안 프로토콜 적용
- 국자 표준 대칭키 알고리즘 SEED 적용
- 향후 WPKI과 연동하여 전자서명 인증 서비스 제공

mSSL은 현재 SSL v3.0에 정의된 3가지 암호와 SEED 블록 암호키를 이용한다. 지원하는 암호 알고리즘은 공개키 암호 알고리즘, 대칭키 암호 알고리즘, 해쉬 알고리즘이 있다. mSSL에서의 공개키 알고리즘으로 RSA만 지원하는데, 이 RSA 모듈은 최대 1024비트 키를 지원하며 공개키 연산만 수행한다. 대칭키 암호알고리즘에 관해서는 mSSL은 두 가지 비밀키(암호키)를 지원하는데, 하나는 스트림 단위로 메시지를 암호화하는 RC4 알고리즘으로서, mSSL은 키의 크기가 40비트인 RC4와 키의 크기가 128비트인 RC4 두 가지를 지원하며, 다른 하나는 블록 단위로 메시지를 암호화하는 SEED 암



〔그림 24〕 ME의 무선 PKI 구조

호알고리즘으로서 키의 크기가 128비트이고 한번에 처리하는 메시지의 블록의 크기 128비트이다. mSSL이 지원하는 해쉬 알고리즘은 MD5와 SHA-1이다.

ME 기반의 무선 PKI는 표준 기구에 의한 표준화 작업이 이루어지고 있지는 않으나 유선 망과 동일한 형태의 기술 동향을 갖는다. 다음은 SSL 기반의 무선 PKI 구조이다.

그림 24에서 나타나듯이 무선망에서의 PKI는 현재 제공되는 인터넷 PKI 구조와 동일한 구조를 갖는다. 이러한 구조는 무선 PKI의 궁극적인 구조이기는 하지만 현실적으로 무선 단말기에서의 X.509 인증서 처리, 인코딩 방식 처리, CRL 처리, 전자서명 키 쌍 생성 처리 등 다양한 제약사항을 어떻게 극복하는 것이 관건일 것이다. 따라서 이러한 문제를 해결하기 위한 방법으로 보안 서비스 부분을 스마트 카드 기반으로 개발하는 것에 대한 연구가 진행 중이다.

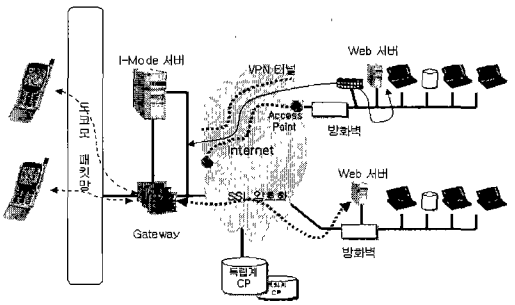
4.1.3 i-Mode 보안기술

도코모가 설치한 i-Mode 서버는 i-Mode 휴대전화에서 발신된 패킷 데이터를 TCP/IP HTTP로 프로토콜 변환을 해서 인터넷에 접속하는 게이트웨이다.

각 사이트는 도코모의 i-Mode 서버를 경유해서 IP로부터 제공된다. i-Mode 서버와 휴대전화는 도코모 패킷 통신망, i-Mode 서버와 IP는 인터넷 또는 전용선을 이용하고 있다. 또한 i-Mode 서버는 전자우편의 메일서버로서의 역할도 담당하고 있다.

i-Mode에서는 기본적으로 각 IP와의 보안은 IP가 독자적으로 결정한 사용자 번호와 암호번호를 입력함으로써 이루어진다. 이런 통신은 SSL(Secure Sockets Layer Protocol)등의 인터넷에서 많이 사용되고 있는 안전한 통신은 아니다. 도코모의 i-Mode 서버와 IP의 서버간에서는 SSL에 의한 통신을 이용하고 있는 경우도 있지만 휴대전화와 I-Mode 서버 사이는 암호화가 되어있지 않다. 물론 휴대전화의 무선프로토콜로서 암호화가 되어 있고 은행 등의 보안이 중시되는 IP와는 i-Mode 서버에서 전용선으로 연결되어 있지만 그 외의 IP와는 인터넷망을 경유하고 있기 때문에 보안에 문제가 있는 것이다.

i-Mode는 공식 Site들을 대상으로 SSL과 VPN을 이용해 인증 및 보안을 제공한다. 최근에는 무선 구간에도 SSL 기능 적용으로 종단간 보안이 가능하다. 그리고, 단말기 ID에 의한 세션관리 기능도 제공한다.



〔그림 25〕 i-Mode 인증/보안 Session 관리 구조

4.2 자바 모바일 플랫폼상의 보안

CLDC 환경에서는 J2SE 플랫폼의 정책기반 보안 모델을 적용하기 어렵다. 왜냐하면 CLDC 구현보다 보안 모듈에 대한 구현이 훨씬 더 크기 때문이다. CLDC에서 정의된 보안 관련사항은 다음과 같은 두 가지 수준의 보안에 대한 지원을 말할 수 있다. 즉, 다시 말해서 보안 문제에 있어서는 보안 모듈 자체가 CLDC 구현보다 크기 때문에 저 수준의 가상머신 보안과 어플리케이션 레벨의 보안을 제공하는 것이다.

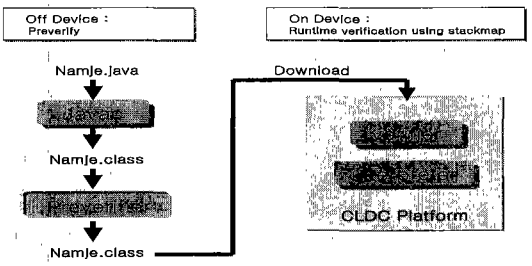
① 저 수준 가상머신 보안 :
- 어떤 방법으로든 가상머신 내부에서 동작하는 Application은 Device에 위해한 행위를 할 수 없다.
- 클래스 파일 검증기에 의해 검증되어야 한다.
- 응용 프로그램은 VM 상위에서 실행되고, Native Code Interface를 지원하지 않으므로 기기를 직접 접근 못한다.
- 사전검증(Preverify) + 실행검증(Runtime Verify)

② 어플리케이션 레벨 보안 (Sandbox Model)
- 모래상자 모델 (Sandbox) 형태의 보안모델 적용
- 응용프로그램은 오직 허용된 자바 API만 사용할 수 있는 닫힌 환경(=모래상자)에서만 수행 가능

보안에 관한 CLDC는 원시적인 자바의 모습으로 퇴화했는데 SandBox 보안모델은 다음과 같은 요구사항을 만족해야 한다.
- 자바 클래스 파일은 유효한 자바 어플리케이션임이 검증되고 보장되어야 한다.

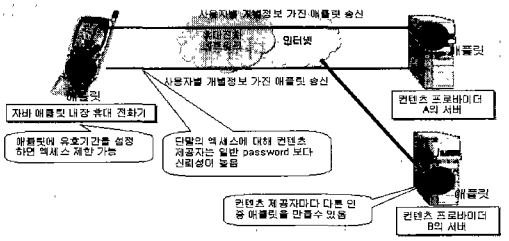
- 어플리케이션 프로그래머는 사전에 미리 정의된 자바 API만을 사용해야 한다.
- 자바 어플리케이션의 다운로드와 관리는 네이티브 코드 수준에서만 가능하다. 클래스 로딩 메커니즘과 가상머신의 시스템 클래스를 오버라이딩할 수 없다.
- 네이티브 함수를 호출하는 새로운 라이브러리를 사용해 어플리케이션을 작성할 수 없다.

클래스 검증과정은 사전검증과 실행시 검증이라는 새로운 방법을 도입해서 사용하는데, 이를 통해 오프 디바이스에서 공간 절약적인 처리와 검증시간을 줄일 수 있다. CLDC에서는 JAR 파일을 사전로딩과 사전링킹을 통한 로마이징을 구현한다. CLDC 라이브러리는 lang.util.io 패키지만을 사용한다[13].



〔그림 26〕 CLDC Security - Two Pass Verifier

위의 CLDC 보안모델의 방법으로 자바 애플릿을 이용한 보안강화 모델을 생각하면 그림 27과 같은 구성으로 이루어질 수 있다.

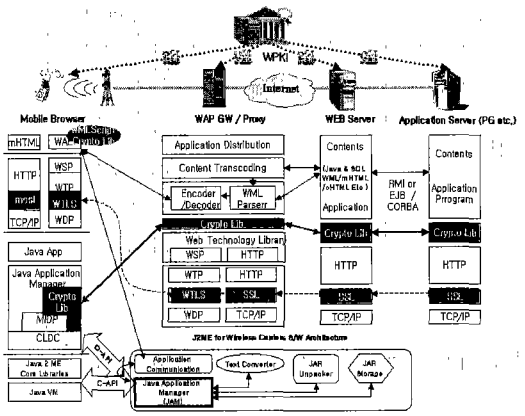


〔그림 27〕 자바 애플릿을 통한 보안강화 방안

V. 무선 전자상거래 보안 플랫폼

5.1 무선 전자상거래 보안 플랫폼 구성

지금까지의 무선환경에서의 각 응용 프로토콜에 대한 분석과 서비스 플랫폼에 대한 내용을 바탕으로



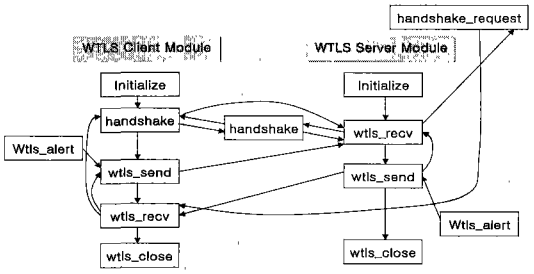
〔그림 28〕 M-Commerce 보안 플랫폼 구성

M- Commerce 보안 플랫폼의 구성을 살펴보면 그림 28과 같다. 본 보안 플랫폼 구성은 여러 상용 서비스 플랫폼 중의 자바 모바일 서비스 플랫폼을 기반으로 구성한 M-Commerce 플랫폼을 나타낸다.

먼저 위의 보안 플랫폼은 WAP 방식 기준의 ME 방식을 수용한 것으로 Mobile 브라우저상의 mSSL과 WTLS Client 암호화 모듈을 이용해 어플리케이션 서버까지 전송계층의 보안 방안을 지원하고, 전송 계층에서 제공하지 못하는 부인방지를 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.

단말기측에서의 MIDP 어플리케이션 프로그램은 CLDC 보안모델에 따르며, 어플리케이션 관리자는 실행 시에 인자로 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.

M-Commerce 보안 플랫폼의 무선 응용프로토콜 부분에서의 보안은 WAP 모델을 기반으로 WTLS를 적용한다. 현재 적용된 WTLS Client/Server API의 모델을 보면 그림 29와 같다.



〔그림 29〕 WTLS Client/Server API 모델

5.2 무선 전송계층 보안 프로토콜의 설계방안

WTLS의 구조는 Handshake Protocol, Alert Protocol, Application Protocol, Change Cipher Spec Protocol, Record Protocol 등으로 이루어져 있으며, Handshake Protocol, Alert Protocol, Change Cipher Spec Protocol은 WTLS의 동작에 관한 관리를 위해 사용되며, 실질적인 보안 서비스는 Record Protocol에서 제공된다. 클라이언트와 서버가 WTLS를 통해서 연결을 할 경우 먼저 Handshake Protocol을 수행하여 한 세션동안 보안서비스 제공에 사용되는 세션키, 암호 알고리즘, 인증서 등과 같은 암호 매개변수를 서로 공유하게 된다. 여기에서 생성된 세션정보는 Record Protocol에서 보안 서비스를 제공하는데 이용된다. WTLS 프로토콜은 크게 보안 서비스 제공에 필요한 세션을 생성하는 단계인 'Session State'와 이 세션정보를 이용해 클라이언트와 서버가 메시지를 주고받는 'Connection State'로 구분할 수 있다. WTLS가 구현된 클라이언트가 서버에 연결을 시도하는 시점에서 'Session State'가 시작되는데, 세션 정보는 Handshake Protocol이 진행중인 상태인 'Pending State'와 Handshake Protocol이 완성되는 시점에서 Change Cipher Spec Protocol을 통해 세션 생성이 이루어지는 'Current State' 단계를 거쳐 생성된다. 이러한 세션 정보는 세션 ID, 상대방 인증서, 압축방법, 암호 알고리즘 식별자, 키 길이 등의 정보가 포함된 Cipher Spec, 비밀정보인 Master Secret, 연결을 시작할 때 세션을 재사용할 것인지에 대한 플래그 정보 등으로 구성된다. 이러한 세션은 여러 개 생성될 수 있으며, 또한 세션을 재사용할 수 있도록 함으로써 Handshake Protocol에서 주고받는 메시지를 줄여 효율적으로 동작할 수 있도록 하고 있다. 세션정보는 클라이언트 정보와 서버가 메시지를 주고받는 'Connection State'에서 유지된다. 이때 연결이 종료되면 이러한 정보는 소멸된다. WTLS Alert Protocol은 Handshake Protocol, Change Cipher Spec Protocol, Record Protocol이 수행중일 때 발생하는 모든 오류메시지를 처리하는 프로토콜이다.

본 논문에서 설계한 무선 전송계층 보안프로토콜은 WAP Spec을 바탕으로 서비스 프리미티브를 고려한 Handshake 과정과 API 설계과정을 설명한다.

5.2.1 WTLS Handshake 설계방안

핸드쉐이크 프로토콜은 안전한 세션의 암호학적 매개변수들을 만들기 위한 절차로서 WTLS 레코드 프로토콜위에서 수행된다. 핸드쉐이크를 통하여 프로토콜의 버전과 암호학적 알고리즘을 일치시키고 선택적으로 상호간의 인증을 수행한다. 상호간 공유된 시크릿을 만들기 위하여 공개키 암호기법을 사용한다.

핸드쉐이크는 다음과 같은 단계의 목표를 추구한다 :

- 알고리즘의 일치를 위한 Hello 메시지 교환 및 난수의 교환
- 서로가 Pre-Master Secret에 대한 일치를 위해 필요한 암호 매개변수의 교환
- 상호 인증을 위한 인증서 및 암호 정보의 교환
- Pre-Master Secret으로부터 Master Secret의 생성 및 난수의 교환
- 레코드 계층을 위한 보안 매개변수의 제공
- 서로 같은 보안 매개변수의 계산과 핸드쉐이크 과정의 안전성에 대한 상호검증

핸드쉐이크 프로토콜 설계를 위한 서비스 프리미티브의 정의를 살펴보면 다음과 같다.

① WTLS 서비스 프리미티브 정의

- SEC-Unitdata

쌍방간에 사용자 데이터를 교환하기 위해서 사용되며 쌍방의 전송 주소(Transport Address) 사이에 안전한 연결이 존재할 때만 호출될 수 있다. 여기서 전송 주소는 이 프리미티브의 매개변수인 출발지주소, 출발지포트, 목적지주소, 목적지포트의 4쌍(4-tuple)로서 구분되는 주소를 말한다.

- SEC_Create

안전한 연결 설정을 시작(initiation)하기 위해서 사용되며, 상위계층에서 Source Address, Source

Port, Destination Address, Destination Port, Client Identities, Proposed Key Exchange Suites, Proposed Cipher Suites, Proposed Compression Methods 등을 제안하면서 안전한 연결 설정을 시도한다.

· SEC-Exchange
서버가 클라이언트와 키 교환을 하거나 공개키 인증을 하면서 안전한 연결을 설정하고자 할 때 사용된다.

· SEC-Commit
핸드쉐이크가 완전히 끝나고 쌍방 중 어느 한쪽이 새롭게 협상된 연결상태에 전환하기를 요청했을 때 시도되며 아무런 매개변수가 없다.

· SEC-Terminate
현재의 안전한 연결을 종료하기 위하여 사용된다.

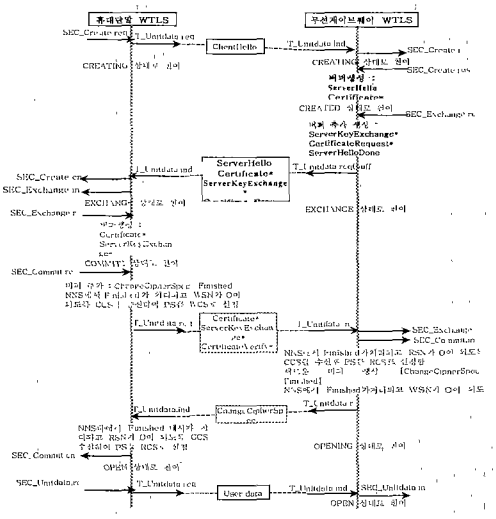
· SEC-Exception
경고성(warning) 경고를 상대방에게 알려주기 위해서 사용된다.

· SEC-Create-Request
새로운 Handshake를 시도하기를 서버가 클라이언트에게 요구할 때 사용되며 서버에 의해서만 사용된다.

② WTLS 완전 핸드쉐이크의 동작

클라이언트는 ClientHello 메시지를 서버에게 보낸다. 이때 서버는 ServerHello 메시지로 응답을 하거나 치명적인 경고로 인해 보안세션의 설립이 실패할 수 있다. ClientHello와 ServerHello가 설립하는 특성 값들은 다음과 같다. 프로토콜 버전, 키 교환 다발(키 교환 알고리즘), 암호 다발(암호 다발, 암호 및 MAC 알고리즘), 압축방법, 키 재생성 주기 및 순서번호 방식과 추가적으로 ClientHello.random과 Server Hello.random에 각각의 난수 값의 생성과 교환이다. 만약 인증이 필요하면, 서버는 서버의 인증서를 클라이언트에 보내도록 준비한다. 추가적으로, 만약 서버가 인증서를 가지고 있지 않거나 서버의 인증서가 단지 서명용이라면 ServerKeyExchange 메시지가 전송할 수도 있다. 이제 서버는 핸드쉐이크의 hello 메시지 단계가 완료되었음을 나타내는 ServerHelloDone 메시지를 보낸다. (위에서 설명한 핸드쉐이크 메시지들은 하나의 SDU로 결합되어 하위 계층으로 전달된다.) 그런 다음 서버는 클라이언트의 응답을 기다린다. 만약 서버가 인증서 요청 메시지인 Certificate Request를 보냈다면 인증서 메시지를 반드시 보내야 한다. 클라이언트 키 교환 메시지인 ClientKey Exchange 메시지는 만약 클라이언트 인증서가 전혀 보내지지 않았거나 클라이언트 인증서가 키 교환을 위해 충분한 데이터를 포함하지 않는다면 지금 보내진다. 이 시점에서 클라이언트에 의해서 암호규격변경(ChangeCipher Spec) 메시지가 보내지며 클라이언트는 이제까지 보류되어왔던 암호규격(Pending Cipher Spec)을 클라이언트의 현재 전송시점 암호규격(Current write Cipher Spec)으로 복사한다. 그런 다음 클라이언트는 즉시 새로운 알고리즘, 새로운 키, 새로운 시크릿을 적용하여 Finished 메시지를 보낸다. 이제부터는 암호규격 인식자(Cipher Spec indicator)를 1로 설정한다. 이것은 레코드 계층에서 레코드 타입을 규정하는 인자가 된다. 암호규격변경 메시지를 받았을 때, 서버는 또한 보류암호규격을 서버의 현재 읽는 시점 암호규격으로 복사한다. 클라이언트에 대응하여 서버는 자신의 Change CipherSpec 메시지를 보내며, 보류암호규격을 현재전송시점암호규격으로 설정하고 새로운 암호규격을 적용하여 Finished 메시지를 보낸다. 이 시점에서 핸드쉐이크는 완결이 되고 클라이언트와 서버는 응용계층의 데이터 교환을 시작할 수 있다.

그림 30은 완전 핸드쉐이크 프로토콜에서 클라이언트와 서버가 서로 동작하는 구체적인 예를 나타내고 있다.

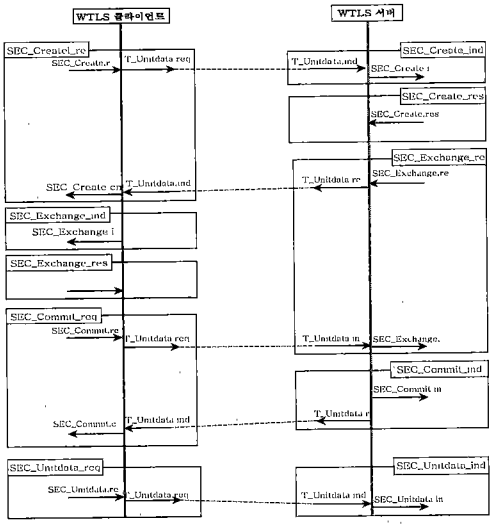


(그림 30) WTLS 완전 핸드쉐이크의 동작 예시

5.2.2 WTLS API 설계방안

① 응용 프로그래밍 인터페이스(API) 함수 설계 방안

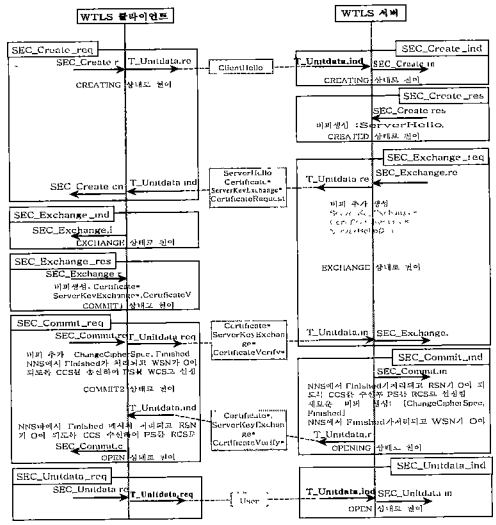
WTLS 클라이언트와 WTLS 서버의 상태 천이를 분석하면 완전 핸드쉐이크의 경우 그림 31과 같이 각각의 프리미티브를 API로 그룹화할 수 있다.



〔그림 31〕 WTLS API 함수 설계 방안

② 응용 프로그래밍 인터페이스 함수별 실행 내용

다음은 WTLS의 완전 핸드쉐이크 시, WTLS 클라이언트와 WTLS서버의 각 인터페이스 함수에서 수행해야 할 내용을 그림으로 정리한 것이다.

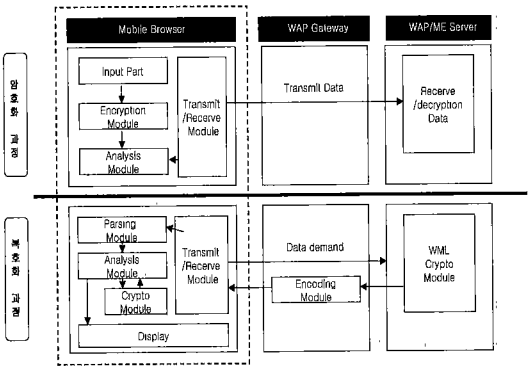


〔그림 32〕 WTLS API 함수별 실행 내용

5.3 어플리케이션상의 종단간 보안

무선 단말기의 브라우저와 서버간의 종단간 보안 통신은 앞서 말한 WAP 방식의 경우와 자바 모바일 환경의 경우에 맞춰서 크게 두 가지의 방식으로 나누어진다. 설명한 두가지 방식은 향후 WPKI의 연동을 고려한 종단간 보안방식으로서, 하나는 단말기 브라우저가 데이터를 요청할 경우 암호화된 데이터를 전송하는 경우이며, 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 무선 환경에 최적화된 ECC 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 33〕 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 WWW 상에서의 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.
- 파싱모듈은 트리구조의 API형태로 구조화한다.
- 해석모듈은 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.

V. 결 론

WWW의 등장과 함께 혁명적인 전환을 맞았던 인터넷은 이제 무선 인터넷이라는 또 다른 전환기를 맞고 있다. 무선 인터넷은 사용자에게나 서비스 공급자에게나 여러 가지 면에서 매우 매력적인 매체이다. 그러나 무선통신의 단점인 느린 전송속도, 낮은 전송률, 부족한 자원을 물려받고 있고, 또한 유선 인터넷과 마찬가지로 중요한 데이터를 주고받기에는 보안상 취약한 점이 있다.

무선인터넷 전자상거래가 활성화되기 위해서는 유선 인터넷 수준의 보안기능 구현이 우선돼야 하며 이를 위한 각종 기술표준 정립이 시급한 것으로 보인다. 무선 전자상거래를 위해 필요한 보안 요구사항으로 첫째, 고객과 서비스 업체간에 전송되는 정보를 암호화하는 기밀성 유지, 둘째, 전송되는 데이터가 무선 채널상에서 변환되지 않도록 하는 데이터 무결성, 셋째, 인증서를 통한 고객과 서비스 업체간 상호 확인을 위한 인증, 넷째, 상호 거래 내역에 대한 부인을 방지하기 위한 거래부인 방지 등이 필요하다고 본다. 그러나 이런 현안 문제점에도 불구하고 IMT-2000의 도래와 함께 M-Commerce는 전 세계적으로 이동통신 사업자들에게는 반드시 필요한 서비스임에는 틀림이 없다.

본 논문에서는 이러한 M-Commerce 환경의 보안 문제를 해결하기 위해서 WAP에서 사용하는 여러 가지 대안들을 분석해 보았다. 또한, 향후 IMT 2000에서도 사용 가능한 상업용 무선 서비스 플랫폼을 검토하고, 표준화가 진행중인 자바 모바일 서비스 플랫폼을 기반으로 하는 J2ME 기술인 CLDC와 MIDP를 이용해서 M-Commerce 환경에서 사용되어질 보안 플랫폼을 구성하였으며, WAP 방식에서의 WTLS에 대한 설계방안을 제시하고, 응용계층의 종단간 보안을 위한 방안을 논하였다.

현재의 시점에서 완벽한 보안을 제공하는 메커니즘을 제공하는 것은 무리이지만, 무선 환경에 대한 여러 단점들을 해결한다면 계속적인 발전이 있을 것으로 예상된다. 이를 지원하기 위한 관련 기술들의 연구와 서비스 제공방안에 대한 좀 더 다양한 연구들이 요구되고 있으며, 이를 관련기술들의 다각적인 고려를 통한 서비스 제공방안에 대한 또 다른 측면의 연구가 요구되고 있다. 더불어 이를 기반으로 무선환경의 전자상거래 서비스도 더욱 활성화가 될 것으로 전망한다.

본 논문에서 제시한 모바일 서비스 플랫폼 기반의 무선 전자상거래 보안 플랫폼을 통해 향후 여러 응용 서비스를 안전하게 제공할 수 있으므로 무선 전자상거래를 보다 활성화시키는데 기여할 것으로 기대된다.

참 고 문 헌

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

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

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

[4] "Wireless Application Environment Over-

view", *WAP Forum*, April 30, 1998
[5] "Wireless Application Protocol Architecture Specification", *WAP Forum*, November 8, 1999.
[6] "WAP WTLS ver. 18-Feb-2000", *WAP Forum*, http://www.wapforum.org
[7] CLDC/MIDP, http://java.sun.com/
[8] "무선기반의 M-Commerce 활성화 정책방향", 정보통신부, 2001
[9] "무선인터넷 표준화 정책방안", 정보통신정책국 2001. 2.
[10] 김용운, "WAP의 한계와 문제점", ETRI, 2001. 1.
[11] 박정서, 김정유, "Mobile Commerce", 2001
[12] 김재홍, "무선인터넷 기술동향", 2000. 7.
[13] 최원호 외 3명, "자바플랫폼 기반으로 하는 마이크로브라우저 설계", 경남대, 2000. 9.
[14] 이동훈, 임채훈, "WTLS 안전성 분석", 퓨처시스템, pp.1-2, 2000
[15] "Wireless Application Protocol Architecture Specification", WAP-210-WAPArch, WAP Forum, 2000
[16] KVM WhitePaper, http://java.sun.com/products/kvm
[17] 송유진 외 5명, "전자상거래 보안기술", 생능출판사, 1999.
[18] 강본용명, 산본박자 저, 송유진 번역, "현대암호", 생능출판사, 1999.
[19] 박남제, 신균호, 최영진, 송유진, "M-Commerce를 위한 자바 모바일 플랫폼 기반의 전자지불 구현방안", 2001년 한국정보처리학회 춘계학술발표논문집, PP.817-820, 2001.
[20] 박남제, 송유진, "M-Commerce Security Platform based on WTLS and J2ME" 2001 IEEE International Symposium on Industrial Electronics, FrM5-06, 2001.

〈著者紹介〉

박 남 제 (Nam-Je Park) 학생회원

2000년 8월 : 동국대학교 정보산업학과 졸업
2001년 3월~현재 : 성균관대학교 정보통신대학원 정보보호학과 석사과정
2000년 5월~현재 : (주)뉴레카 정보통신연구소 전임연구원
관심분야 : 전자상거래 보안, 무선인터넷 보안, 전자지불시스템

송 유 진 (You-Jin Song) 정회원

1982년 2월 : 한국항공대학교 전자공학과 졸업
1986년 2월 : 경북대학교 정보시스템 전공 (석사)
1995년 2월 : 일본 동경공업대학 정보보호 전공 (박사)
1988년 2월~1996년 2월 : 한국전자통신연구원 선임연구원
1996년 3월~현재 : 동국대학교 정보산업학과 교수
관심분야 : 암호이론, 전자상거래 보안, 무선인터넷 보안, 스마트카드 보안, 전자화폐