GOVP1200515391

최 종
연구보고서

무선 인터넷 기반에서 농산물 특화된 M-Commerce 시스템의 구축
Implementation of a M-Commerce System for Agricultural Products on Wireless Internet

연구기관
조 선 대 학 교

농 림 부

제 출 문

농림부 장관 귀하

본 보고서를 “무선 인터넷 기반에서 농산물 특화된 m-commerce 시스템의 구축” 과제의 최종보고서로 제출합니다.

2003 년 8 월 13 일

주관연구기관명 : 조선대학교
총괄연구책임자 : 정 일 용
세부연구책임자 : 정 일 용
연 구 원 : 이 대 용
연 구 원 : 강 창 기
연 구 원 : 탁 동 길
연 구 원 : 유 성 진
연 구 원 : 오 명 옥
연 구 원 : 이 여 진

요 약 문

Ⅰ. 제 목

무선인터넷 기반에서 농산물 특화된 m-commerce 시스템의 구축

Ⅱ. 연구개발의 목적 및 필요성

■ 연구의 목적

이동 환경에서도 인터넷 컨텐츠 이용이 가능한 무선 단말기를 사용하여 농산물의 구매 및 판매등을 제공하는 무선인터넷 기반의 안전한 전자상거래 시스템의 개발을 수행한다. m-commerce 시스템을 구축하기 위해서 정보보호기술, 전자상거래 시스템 기술, 그리고 이동통신 환경에서의 무선인터넷 기술들을 연구한다.

■ 연구의 필요성

인터넷이라는 전세계를 연결할 수 있는 네트워크 인프라의 형성을 통해 인간의 기본적인 생활 패턴은 급격하게 변화되고 있다. 최근 인터넷 비즈니스는 기존의 상품들의 수요를 촉발시키는 역할과 더불어 전 세계적인 규모로 창출하고 있다. 인터넷을 이용한 상거래의 형태는 무선인터넷이라는 부분으로 이동하고 있다. 무선 망 기술의 기술적인 발전과 더불어 다양한 무선 인터넷 서비스가 활성화되어지고 있다. 다양한 정보를 시간과 장소의 제약을 벗어나 빠르고 쉽게 접근하는 것은 디지털 사회의 궁극적인 목적이고 변화되는 삶의 패턴이 된다. 이러한 사회적인 변화와 기술의 발전으로 무선 인터넷은 광범위하게 적용될 것이다. 다양한 무선 인터넷 활용 분야에서 가장 생산적인 분야가 m-commerce 분야이다. 모바일 비즈니스가 갖는 편리성 즉, 언제 어디서나 편리하게 자신이 필요로 하는 재화와 서비스를 제공받을 수 있는 특징은 유선에서 수행하고 있는 제한된 상거래 행위를 뛰어 넘을 수 있다는 것이다. m-commerce는 무선 단말기를 통하여 쇼핑, 구매 및

결제 등 인터넷 분야에서도 활발하게 이루어지고 있는 확장된 형태의 전자상거래로 발전할 수 있다. 이와 더불어 국내 상용화가 예정된 IMT-2000 서비스는 기존의 유선망 중심의 전자상거래 기반을 무선망으로 전환하는 계기가 될 것이며, 데이터 전송 속도나 이동성의 보장으로 전자상거래의 영역을 더욱 확대시킬 것이다. 또한 무선망에서의 이동성을 실현하는 PDA와 같은 단말기에 대한 꾸준한 발전은 무선망에서의 전자상거래 영역을 확대시킬 것이다. 이러한 현실을 고려할 때 우리의 농산물 유통구조에 PDA와 무선 인터넷을 이용한 농산물 전자상거래를 도입하여 도매시장의 정보화 및 농산물 유통에 있어서 정보화의 기초를 확립할 수 있을 것이다.

Ⅲ. 연구개발 내용 및 범위

이동 환경에서도 인터넷 컨텐츠 이용이 가능한 무선 단말기를 사용하여 농산물의 구매 및 판매, 상황정보 등을 제공하는 무선인터넷 기반의 안전한 m-commerce를 구축한다. 이 시스템은 전자상거래 구현 기술 및 보안기술, PDA 응용프로그램 개발 기술등을 이용하여 안전하고 효율적으로 설계 및 구축한다.

- ■ 농산물 유통 전자상거래 시스템 기본 설계
  - · 국내·외 전자상거래 관련 솔루션 연구
  - · 전자상거래 시스템 구현 기술 및 동향 연구
  - · 사용자 인증, 결재 및 지불 시스템 등의 전자상거래 보안 기술 연구
- ■ 무선인터넷 기술 분석
  - · 무선인터넷 프로토콜 및 마이크로 브라우저 구현 기술 연구
  - · 유·무선 연동 기술 연구
  - · 무선인터넷 보안 기술 연구
- ■ 농산물 거래를 위한 안전한 전자상거래 시스템 구축
  - · 농산물 거래에 관련한 컨텐츠 개발
  - · 보안을 고려한 전자상거래 시스템의 구성
  - · 웹 상에서 농산물 거래를 위한 어플리케이션 개발
- ■ m-commerce 구현을 위한 모바일 전자상거래 시스템 개발

· 이동성 및 단말기 성능을 고려한 무선인터넷 환경에 최적화된 컨텐츠 설계
· 무선망 보안 기술을 적용한 시스템 설계
· 효과적인 유·무선 연동을 위한 시스템 개발 방법론 적용

■ PDA에 적합한 응용프로그램 개발
· 모바일 단말기에 적합한 응용프로그램 개발을 위한 기술 연구 및 개발
· PDA를 이용한 무선인터넷 접속을 통한 전자상거래 시스템 설계 및 구현

Ⅳ. 연구개발 결과

본 연구에서는 안전한 m-commerce 시스템이 PDA기반에서 설계되고 구현되었다. 이동환경에서 무선 인터넷/웹을 통하여 전자상거래 시스템의 접근이 가능하도록 하며 안전한 시스템 구축을 위해 암호화 과정 및 인증서등을 통해 인증 및 보안서비스를 제공한다. 개인 단말기로 사용되는 PDA의 특징을 고려하여 Server와 PDA간의 신뢰성있는 테이타 전송을 위해 인터페이스 프로그램을 개발한다. 제안된 시스템은 프로세서 실행을 최소화하면서 효율적이고 사용이 용이하도록 하고, PDA를 위한 응용 프로그램 개발의 기술적 접근을 통해 보다 발전적인 개발환경을 마련하였다.

Ⅴ. 활용에 대한 건의

■ 무선 인터넷상에서 정보서비스를 제공하기 위해서 확장을 원하는 기존의 유선 인터넷 기반의 e-commerce 업체에게 낮은 가격으로 Upgrade를 제공
■ PDA를 사용하여 안전하고 신뢰성 있는 실시간 경매 시스템 설계와 농산물 가격에 대한 상황정보 등을 제공
■ 무선 인터넷기반에서 안전한 m-commerce 시스템의 설계 및 구현
■ 모바일 환경에서 서버와 PDA를 위한 인터페이스 기술의 구현

SUMMARY

(영 문 요 약 문)

Ⅰ. Title

Implementation of a m-commerce system for agricultural products on wireless internet

Ⅱ. Objective and Importance of The Research

■ Objective

In this project, a secure m-commerce system based on wireless internet is designed and implemented. It provides services that purchases and sells agricultural products by utilizing wireless DTE(data terminal equipment) enable to connect internet contents. In order to construct a m-commerce system, technologies for information security, a e-commerce system and wireless internet on mobile communication environment are researched.

■ Importance

Using internet, worldwide communication network, life patterns of people have been changed drastically. Recently internet business creates new demands for purchasing existing products and comes to enlarge market place to the world. Internet-based e-commerce system now move to wireless internet environment. With technical advance of wireless network, various services offered on wireless internet have been activated. Access to lots of information securely and easily without limitation of time and space is an ultimate goal to digital society and helps to change life patterns. Due to these social changes and technical advances, wireless network will be applied to many areas of industry practically. Among these applications, one of productive areas is

m-commerce. Mobile business provides convenience, that is a characteristic obtaining products and services he/she requests at anytime and anyplace. It is totally different from current e-commerce systems performed on internet. With wireless DTE, m-commerce can accomplish services for shopping, purchasing and selling as an extended form of conventional systems. On these social circumstance IMT-2000 service offered in a near future can be an opportunity to change to e-commerce systems on wireless network from internet-based systems. Also areas of e-commerce can be extended relatively owing to high speed of data transmission and assurance of mobility. Considering these factors, e-commerce on wireless internet for agricultural products is applied to agricultural distribution structure and then infrastructure of information on market place and distribution structure can be established.

Ⅲ. Contents and Scopes

In this project, a secure m-commerce system based on wireless internet is designed and implemented. It provides transactions of agricultural products and information on situation by wireless DTE enable to utilize internet contents. It is designed effectively by employing e-commerce technology, security technology and implementation technology of application program on PDA

- Design of e-commerce system for agricultural distribution
  - Analysis of solutions related to e-commerce systems
  - Analyses of Implementation and trend for e-commerce system
  - Secure e-commerce systems with user authentication, repudiation, and secure transaction systems
- Analysis of wireless internet technology
  - Protocol for wireless internet and technology for implementation of micro browse
  - Secure technology for wireless internet

- Interaction of wireless network and internet.

■ Construction of a secure e-commerce system for agricultural products
  - Development of contents related to agricultural transactions
  - Design of a secure e-commerce system
  - Development of application for agricultural transactions on Web

■ Development of a m-commerce system on wireless internet
  - Design of optimized contents on wireless internet by considering mobility and performance of DTE
  - Design of a secure system applied on wireless network
  - Implementation of methodology for an efficient interaction of wireless network and internet

■ Implementation of application program appropriate for PDA
  - Researches on implementation of application program appropriate for mobile DTEs
  - Design and Implementation of e-commerce systems connected to wireless internet by using PDA

Ⅳ. Results

A secure m-commerce system is designed and implemented on PDA. It can access to wireless internet/web and provides authentication and secure transactions by employing electronic signature and certificate. Considering the characteristic of PDA as an personal DTE, interface program between server and PDA is implementation in order to transmit data reliably. The proposed system being user-friendly and effectively minimizes performance of processer. Implementation of application program for PDA provides an improved environment for system developer utilizing PDA on wireless internet.

Ⅴ. Suggestions for applications

- If a e-commerce system on internet would like to extend to provide services on wireless network, we can upgrade it with lower cost.
- Using PDA, realtime auction results and situation information on prices of agricultural products can be provided.
- Design and Implementation of a secure m-commerce system on wireless internet
- Implementation of Interface technology between PDA and server

CONTENTS
(영 문 목 차)

목 차

제 1 장 연구개발과제의 개요

제 1 절 연구개발의 필요성

1. 기술적 측면

인터넷의 등장과 더불어 사회 생활 및 경제 패턴의 변화를 이루게 되었으며 좀더 쉽고 빠른 정보 교류는 곧 사회 구성원 및 조직의 경쟁력이 되어지고 있다. 이러한 변화에 한층 힘을 주게 되는 부분이 무선 인터넷이다. 다양한 정보를 시간과 장소의 제약을 벗어나 빠르고 쉽게 접근하는 것은 디지털 사회의 궁극적인 목적이고 변화되는 삶의 패턴이 되어지고 있다. 최근에 발전되고 있는 무선 망 기술은 무선 인터넷을 위한 인프라 구축의 의미를 갖고 있으며 이는 인터넷 서비스의 다양화를 가져오게 되었다.

무선 인터넷은 이동통신과 인터넷이라는 두 가지 기술을 필요로 하며 두 망 사이에 연동을 위한 방식이 연구, 개발되어 표준화를 추진 중에 있다. 또한 무선 인터넷을 위한 단말기에 대한 꾸준한 연구가 진행하고 있다. 이러한 단말기 중 PDA의 경우 컴퓨터의 기본이 되는 CPU, 메모리와 운영체제를 갖추고 있고, 각각의 운영체제를 기반으로 하는 다양한 응용 프로그램과 주변 기기를 갖추고 있어 노트북으로 가능한 대부분의 작업이 가능한 작은 초소형 컴퓨터라고 할 수 있다. 이와 같은 특징을 가진 PDA는 '언제, 어디서나 인터넷 접속이 가능하다(Anytime, Anywhere On the Net)'는 장점을 지니게 되어 인터넷 접속과 함께 별도의 응용프로그램 개발을 통한 시스템 구축에 보다 효율적이다. PDA는 메모리나 운영체제등의 한계성이 존재하므로, PDA를 이용한 시스템 구축시 이러한 한계성을 고려하여야 하며, 관련 업체들은 한계성을 극복하기 위한 연구를 꾸준하게 수행하고 있다.

인터넷을 기반으로 하는 사회적인 변화와 정보기술의 발전으로 무선 인터넷의 이용 범위는 광범위하게 적용될 것이다. 다양한 무선 인터넷 활용 분야에서 가장 생산적인 분야는 m-commerce 분야이다. m-commerce는 무선 단말기를 통하여 쇼핑, 구매 및 결제 등 인터넷 분야에서도 활발하게 이루어지고 있는 현재의 전자상거래 확장 부분이다.

최근 무선 인터넷 사용이 보편화되고 있으며, 이제는 언제 어디서나 근무가 가능한 인터넷 비즈니스 및 전자상거래에 의한 물품 구매가 일상적으로 전개되고 있다. 이러한 사회적 환경에서 국내 상용화가 예정된 IMT-2000 서비스는 기존의 유선망 중심의 전자상거래 기반을 무선망으로 전환하는 계기가 될 것이며, 데이터 전송 속도나 이동성의 보장으로 전자상거래의 영역을 더욱 확대시킬 것이다. PDA와 같이 이동성을 실현하는 단말기에 대한 꾸준한 연구 역시 무선망에서의 전자상거래 영역을 확대시킬 것이다. 이러한 현실을 고려할 때 우리의 농산물 유통구조에 PDA와 무선 인터넷을 이용한 농산물 전자상거래를 도입한다면 도매시장의 정보화 및 농산물 유통에 있어서 무선 정보화의 기초를 확립할 수 있을 것이다.

2. 경제·산업적 측면

인터넷이라는 전 세계를 연결시킬 수 있는 네트워크 인프라가 형성되면서 인간의 기본적인 생활 패턴은 급격하게 변화되고 있다. 필요한 정보를 수집하기 위해 도서관의 출판된 서적을 뒤지거나, 관련 분야의 전문가들에게 전화나 팩스를 통하는 방식으로부터 관련 분야의 웹사이트 접속을 통하거나 E-메일을 이용한 신속한 정보 취합 등의 방식으로 변화되어지고 있다. 이와 같이 정보를 수집하는 방식뿐 아니라 우리의 전통적인 거래의 방식에서도 큰 변화를 가져왔다. 전통적인 거래의 방식에서도 전화나 팩스를 통해서 직접 만나지 않고도 일정한 과정들을 진행시킬 수 있었다. 그러나 이런 방법들은 거래를 성사시키는데 주요한 역할을 하는 것이 아니라 부수적인 과정으로만 여겨졌다.

그러나 인터넷상에서 이루어지는 상거래에서는 오히려 대면접촉의 방식이 부수적인 과정으로 변모하면서 과거의 거래방식과는 명확하게 다른 모습을 보여주고 있다. 이런 인터넷에서 이루어지는 거래는 단순히 거래방식의 변화 그 이상의 의미를 우리에게 가져오고 있다. 다시 말한다면 최근 인터넷 비즈니스는 기존의 상품들의 수요를 촉발시키는 역할과 더불어 새로운 시작을 전 세계적 규모로 창출하고 있다는 점에서 주목하지 않을 수 없다.

인터넷 비즈니스는 첫째, 범세계적인 시장(Global Market), 저렴한 거래비용(Transaction Cost) 등을 제공하면서 경제적인 이점을 구매자와 판매자에게 제공하고 있다. 즉 인터넷 비즈니스는 인터넷이 보급되어 있는 세계 구석구석까지 판매자가 구매자에게 원하는 재화나 서비스를 공급할 수 있는 방식이다. 또한 전통적인 실물 시

장에서 재화나 서비스를 제공하기 위해서는 상품의 제조원가 이외에도 임대료, 종업원 인건비 등과 같은 거래 비용(Transaction Cost)을 지불해야 한다. 그러나 인터넷 비즈니스는 이런 비용을 추가적으로 지불할 필요가 없다. 이것은 바로 공급자에게 보다 저렴한 가격으로 수요자에게 접근할 수 있게 해준다. 자신의 수익률을 유지하면서도 수요를 더욱 창출할 수 있는 인터넷상의 비즈니스에 대부분의 기업이 관심을 갖는 것은 당연한 결과이다.

또 하나 인터넷과 관련된 여러 가지 기술이 발전하게 되면서 기존에는 거래가 불가능했던 상품이 이제는 인터넷 비즈니스를 통하여 거래가 가능해졌다. 예를 들어, 이전에는 컴퓨터 게임, 영화, 신문 등 각기 다른 미디어를 통하여 전달되어야만 했던 것들이 이제는 인터넷이라는 매체를 통하여 포괄적으로 제공될 수 있다는 것이다. 신문이나 영화, 게임 등이 각기 나누어져 거래되는 것이 아니라 인터넷을 통해 통합적으로 제공될 수 있다는 기술적인 가능성을 많은 기업들에게 인터넷 비즈니스로 뛰어들 수 있는 계기를 제공하고 있다.

인터넷의 급속한 보급과 인터넷 비즈니스가 갖고 있는 이점은 인터넷 비즈니스에 대해 국내외적으로 낙관적인 전망을 갖게 했다. 1999년 7월 IDC(International Data Corporation)에서 발표한 자료에 따르면 1998년에 인터넷 비즈니스로 상품을 구매한 고객의 수가 3100만 명이었으나, 2003년에는 1억 8천만 명으로 급증할 것으로 예상하고 있다. 이 수치는 인터넷 이용자의 36%를 차지할 것으로 예상되고 있다. 이를 통해서 인터넷 비즈니스의 총 규모는 1998년 말의 45억 달러에서 매년 100% 이상의 고성장을 거쳐 2003년 말에는 1조 달러에 달할 것으로 예상되고 있다.

인터넷을 이용한 상거래의 형태는 2000년 초에 무선 인터넷이라는 또 다른 부분으로 이동하고 있다. 물론 모바일 비즈니스가 일반 상거래에서 주요한 상행위로 자리를 잡은 것은 아니지만 발전의 과정을 예측해 본다면 어렵지 않게 m-commerce가 다가오는 21세기에는 일반적인 거래방식으로 자리를 잡을 것을 예측할 수 있다. 모바일 비즈니스가 갖고 있는 편리성 즉, 언제 어디서나 편리하게 자신이 필요로 하는 재화와 서비스를 제공받을 수 있는 특징은 m-commerce를 유선상에 매여있는 상거래 행위와는 커다란 차별성을 제공하고 있다.

본 연구에서는 이러한 무선인터넷의 이점을 농산물 유통에 적용하고자 한다. 현재 농산물 유통이 점차적으로 전문화, 대형화, 선진화되고 물류센터, 직거래가 확산되는 등 다양한 유통경로 증가 추세에 따라 농산물 판매경로가 다양하게 분산됨으로 기존에 농산물 생산과 소비의 최대 접점인 공영도매시장을 경유하여 수탁·판매의 거래

주체였던 도매법인의 판매량 감소는 명약관화한 현실이다. 또한, 도매시장 내에서도 법인과의 판매량 경쟁 또한 치열한 상태임으로 예전의 판매 영업활동만으로 도매법인이 농산물 유통의 농산물 유통의 선도적인 위치를 유지·발전시킨다는 것은 시대적으로 불가능한 실정이다. 그러므로 그 동안 농산물 유통분야에서 도매법인이 보유한 강점과 비교우위를 최대한 활용하여 최신 정보통신 기술인 무선인터넷을 이용한 전자상거래 시스템을 개발함으로써 국내 농산물 유통의 선도적인 역할을 할 수 있을 것이다.

3. 사회·문화적 측면

IT 산업을 기반으로 한 신 경제(New Economy)의 거대한 두 축은 인터넷과 이동통신이다. 인터넷이 각광을 받기 시작한 것은 최근의 일이지만, 인터넷은 이미 사회, 경제, 정치적인 측면에서 인류의 삶에 깊숙이 스며들어 새로운 패러다임의 변화를 촉진하며 우리 주변의 모든 것을 바꾸어 놓고 있다. 일반적인 유선인터넷은 가정이나 사무실에서 모뎀이나 LAN으로 연결된 PC에서 접속하는 환경으로, 실내 공간을 벗어나 업무를 보는 인구가 늘어나고 있는 추세에서는 인터넷을 이용하는 데 여러 가지 제약이 따른다. 한편 이동통신은 전 국민의 절반 가량이 소지할 정도로 급격하게 확산되었다. 무선인터넷은 이러한 두 개의 거대한 축의 통합 과정을 통해 탄생했다. 무선인터넷은 인터넷이라는 네트워크의 탈중심적, 개방적, 양방향성 등의 특성과 이동통신의 이동성, 양방향성, 개인화(Personalization)의 특성을 그대로 물려받고 있다.

이렇듯 사회·경제·문화 모든 면에 변화를 가하고 있는 인터넷과 이동통신이 결합된 무선인터넷, 그리고 전자상거래 등의 기술을 국내의 농산물 유통 환경에 도입한다면 각 기관에 산재되어 제공되고 있는 유통정보를 생산자가 출하의사 결정에 유용한 정보로 가공하여 제공하고, 또한 도매시장 유통정보를 전자경매가 실시되고 있는 도매법인부터 실 시간대에 생산자에게 제공함으로써 농산물 유통에 대한 불신풍조를 해소할 수 있을 것이다.

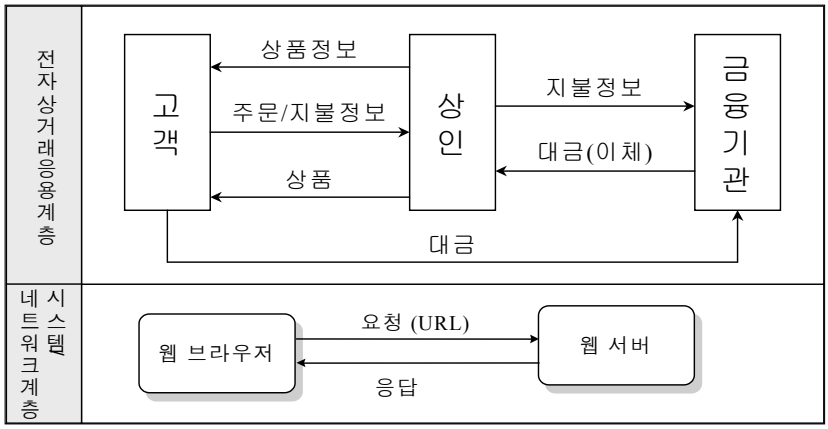
제 2 절　목표 및 내용

이동 환경에서도 인터넷 컨텐츠 이용이 가능한 무선 단말기를 사용하여 농산물의 구매 및 판매, 실시간 경매결과, 상황정보 등을 제공하는 무선인터넷 기반의 안전한 전자상거래 시스템의 개발을 목표로 한다. 구체적으로 유선망에서의 안전한 전자상거래 시스템 구현을 위한 전자상거래 구현 기술, 그리고 무선 이동통신 환경에서의 m-commerce 구현을 위한 무선인터넷 기술 개발을 최종 목표로 한다. 크게 두 분야로 나누어 추진되는 본 과제의 주요 연구 내용은 다음과 같다.

1. 안전한 전자상거래 시스템의 설계 및 구축

전자상거래 시스템 구현시에는 시스템의 개발능력 및 상호운영 그리고 변화에 대한 능동성을 반드시 고려해야만 한다. 즉, 전자상거래 플랫폼은 정보 기술 환경의 변화에 유연하게 대처할 수 있는 구조가 필요하며, 미래의 기술 변화에 능동적으로 대응하기 위한 기술의 표준화를 추구해야 하며 시장 추세 등을 고려한 구현 기술이 요구된다.

기존에 구축된 전자상거래 시스템들은 구현 아키텍처에 따라 3가지로 분류할 수 있다. 먼저 Client/Server 아키텍처는 데이터베이스 서버와 조작 데이터를 처리하고 표현하는 응용 한정적인 큰 규모 클라이언트 프로그램이 요구된다. 따라서 데이터베이스 부하 증가에 대한 확장의 어려움이 따르며 클라이언트에 내장된 로직의 유지보수가 어렵다. 두 번째로 N-Tier 아키텍처는 클라이언트 소프트웨어와 데이터베이스 서버 사이에 응용 서버가 존재하는 구조를 가진다. 응용 서버는 비즈니스 로직을 구현하고 클라이언트는 이를 표현하는 메커니즘을 가지고 있다. 하지만, 일반적으로 하나의 응용 서버를 보유함으로써 신뢰성에 대한 문제를 야기한다. 마지막으로 웹 기반의 아키텍처에서는 오직 웹 브라우저만을 클라이언트에 배치하고 비즈니스 로직 구현을 위한 계층은 시스템 독립적인 모듈의 조립으로 구성한다. 따라서 클라이언트에 대한 부하를 줄여주고 이질적인 환경들의 통합을 위한 단일 인터페이스 제공 및 개별 로직의 구현이 가능하다. 본 과제에서는 웹 기반의 EC 시스템의 구조를 바탕으로 효율적인 EC 시스템 구축을 위한 보편화된 구조를 제시한다.



[그림 1] 상거래 절차 및 보안

또한 안전한 전자상거래가 되기 위해서는 정보보호 기반 서비스가 인터넷과 웹 서비스에 대한 보호 기능과 상거래 행위를 위한 개체 및 절차에 대한 보호 기능 제공이 필요하다. 다시 말하면 안전한 전자상거래를 위해서는 정보보호 기반서비스를 기초로 인터넷/웹 보안과 상거래 보안이 이루어져야 한다.

전자상거래는 기존의 다른 응용 시스템과는 보안 요구사항의 핵심이 현저히 다르다. 기존의 응용 시스템은 데이터와 시스템 자원에 대한 사용자의 접근 통제 및 시스템 이용에 대한 이력 자료의 관리를 근간으로 하는데 반해서, 전자상거래에서는 데이터에 대한 접근 통제 이외에도 사용자의 실체에 대한 증명과 데이터 내용에 대한 사후 검증 수단의 확보에 중점을 둔다. 이러한 전자상거래 특유의 보안 요구사항을 충족시킬 수 있는 수단이 전자서명이다. 또한 전자상거래는 시스템의 관련범위가 특정한 조직이나 응용 시스템에 국한되지 않고 다양한 이질적인 구성요소를 포괄적으로 수용해야 한다는 특이점이 있다. 이와 같은 다양한 요소들에 일관된 보안 정책을 수립하여 적용하고 구현하기 위해서는 전자서명 시스템의 기반구조(infrastructure) 구축에 대한 면밀한 검토가 필요하다.

또한 전자상거래는 사용자에 대한 강력한 인증뿐만 아니라 전자상거래에 관련된 많은 응용 시스템간의 높은 상호 운용성을 요구한다. 이에 따라 보안 기능도 상호 운용성을 지원할 수 있도록 구현되어야 하며, 이는 지금까지는 정보보안 구현에서 중요하게 고려하지 못한 점이다. 호환성과 이식성을 고려한 보안 체계의 구현을 위해서는 보안 체계의 표준화가 필수적이며, 국제 표준 기구나 여러 나라의 정부 및 업체들이 전 세계적인 차원에서 노력을 하고 있다.

안전한 전자상거래 시스템을 구축하기 위해서는 아래와 같은 보안 사항을 고려하여 시스템을 설계 및 구축한다.

- 신원 인증(secure authentication)
  - 구매자와 판매자의 상호 인증 구조가 필요하다.
  - 사용자 인증 등을 통하여 거짓 위장 발주를 회피하는 구조가 필요하다.
  - 수표발행자와 인수자의 신원에 대한 인증이 필요하다.
- 전송 데이터 보안(secure communication)
  - 사용자의 신용정보(이름, 주소등), 신용카드 정보(신용카드 번호. 사용자 이름. 사용기한등)의 안전성 확보가 강구되어야 한다.
  - 전자 공증 제도와 같이 지불 데이터의 법적, 제도적 증거 능력을 높임으로써 전자 지불 내용에 대한 증명 수단이 강구되어야 한다.
- 안전한 지불 시스템(secure payment)
  - 다양하고 안전한 전자지불 방식이 제공되어야 한다.
  - 전자현금의 이중사용, 즉 불법적인 현금복사에 대한 방지대책이 있어야 한다.
  - 사기, 탈세 등의 대응 방법이 있어야 한다.
- 프라이버시 보호(privacy, anonymity)
  - 전자거래에 대한 익명성을 보장하여 프라이버시의 보장이 이루어져야 한다.

2. m-commerce 구현을 위한 무선인터넷 기술 연구

짧은 시간 동안에 급속도로 발전해온 무선 인터넷 기술은 현재에도 제반 환경과 더불어 빠르게 변화하고 있다. 서비스의 속도를 올리기 위하여 무선망과 관련된 기술들이 개발, 연구, 구현되고 있으며 사용자의 변화하는 요구를 충족시키기 위하여 각종 단말기들이 개발되고 있다. 무선망과 인터넷 망의 연동을 위한 표준도 통일되지 않은 상태에서 서비스가 시작되고 있으며 국제 표준을 획득하기 위하여 더 나은 기능을 제공하기 위한 노력이 계속되고 있는 것이다.

무선 인터넷 관련 업체들은 주도권을 쥐고 있는 이동통신 업체와 단말기업체 뿐만 아니라 무선망 관련 장비업체, 무선 인터넷 핵심 기술 개발 업체, 무선 인터넷 서비스 업체 등으로 나눌 수 있다. 무선 인터넷 관련 기술 업체들은 표준 프로토콜과 사이트 구축 및 서비스를 위하여 해법을 제시하고 있으며 대개의 서비스 업체들은 컨텐츠 제

공업체로 볼 수가 있다.

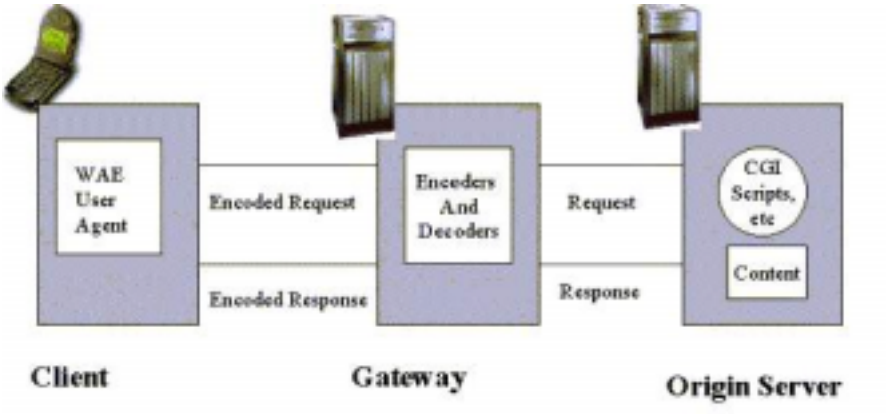
그러나 이동통신사가 제공하는 환경에서 유선 인터넷에서 제공되던 서비스를 그대로 제공하려면 문자와 이진 그림만이 제공되는 환경에서는 제약점이 많으며 이를 해결하기 위해서는 브라우저나 WAP 프로토콜 나아가 단말기에까지 수정을 가해야 할 필요가 있게 된다. 따라서 무선 인터넷 서비스의 개발은 무선망, 단말기의 환경 등의 기술적인 측면과 시장상황 등을 잘 고려하여 기획하여야 한다. 기술적으로는 WAP 프로토콜이나 각 통신사에서 사용하는 언어, 브라우저에 대한 정보가 필요하다. 예를 들어 PIM(Personal Information Management) 서비스를 개발하고자 한다면 WAP에서 제공하는 vCard 나 vCalendar에 대하여 알아야 한다. 전자상거래 사이트등의 무선 인터넷 사이트의 구축을 위해서는 기존의 유선 인터넷 기술과 더불어 WML, HDML, m-HTML등의 무선 인터넷 언어들을 알아야 하며 WAP에서 정의되지 않는 서비스를 제공하려면 WAP 프로토콜을 변형할 수도 있다.

WAP 방식은 전 세계적으로 사용자 면에서 가장 많은 수를 차지하고 있다. 또한 공개된 표준이라는 점에서 많은 연구가 이루어지고 있으며 수많은 어플리케이션이 개발 중이다. 따라서 세계적인 표준으로 자리잡기에 가장 유망한 프로토콜이다. 그러나 기존의 HTTP를 지원하지 않는다는 점과 WAP 게이트웨이에 비용이 많이 든다는 점 때문에 MS의 ME 방식과 i-mode 방식에 표준을 내 줄 가능성도 있다. 기술적으로는 HTTP와 별도의 WAP 프로토콜이 기존의 기술과의 호환성을 제공하고 어플리케이션의 개발이 가능하기 때문에 다른 방식에 비하여 많은 유연성을 가지고 있고 기존의 서비스와 차별화 된 서비스를 개발하기에는 가장 유리하다. 즉, WAP에서 표준으로 정의되지 않는 포맷의 파일에 기반한 서비스나 제공되지 않는 서비스일지라도 단말기나 무선망의 성능이 보장되는 한 제공되는 프로토콜을 이용하여 구현이 가능한 장점이 있다.

WAP forum에서 제공하는 Spec은 계층적이고 확장 가능한 특성상 정확하게 정의되어 있지 않고 개발자에게 맡겨 버리는 경우도 많으며 현재에도 표준을 제정중인 부분도 있다. WAP 방식은 사용자의 모든 요구를 수용할 수 있을 정도는 아니지만 사용자의 편의와 단말기의 기능을 고려한 표준들이 많이 연구되고 있다. WAP에서 규정된 멀티미디어는 현재 압축이 안된 WBMP파일만이 있다. 이를 개선하기 위하여 음악과 동영상의 표준화 노력이 계속되고 있으며 (WAP multimedia expert group) 단말기 Spec등의 개선도 논의되고 있다. 또한 무선 인터넷의 보안 문제(WAP Security 워킹 그룹), 기존의 기술과의 호환 (WAP Interoperability Group), 메시지 통합 관리

시스템의 구현에 관한 표준 연구되고 있다.

궁극적인 WAP 게이트웨이의 목적은 무선환경을 위하여 따로 사이트를 만드는 것이 아니기 때문에 기존의 HTML 사이트를 자동변환 하기 위한 노력이 계속되고 있다.



[그림 2] WAP 구성도

HTML을 기반으로 한 기술은 WAP의 경우와는 달리 컨텐츠 개발이 용이하다는 장점이 있다. 언뜻 보기에는 이러한 장점이 그다지 중요한 사항이 아닌 것처럼 보일 수 있으나 컨텐츠의 양적, 질적 성장이 무선인터넷 시장의 성패를 좌우할 것이라는 현실을 볼 때 큰 장점이 될 수도 있다. 그러한 장점을 파악하고 사업적으로 성과를 거둔 대표적인 이동통신사업자로 NTTdocomo가 있다. NTTdocomo는 기존의 HTML의 서브셋(c-HTML)을 통해 무선인터넷 사이트 구축을 가능케 함으로써 컨텐츠 제공자에게는 개발의 용이성을 제공하였고 무선인터넷 단말기의 제한된 메모리 및 데이터 통신 속도문제등 기술적 문제에 적절히 대처할 수 있었다.

MS의 경우에는 ME 1.0버전을 내놓고 WAP과 힘겨루기를 계속하고 있다. 현재 ME 1.0의 경우는 mHTML이라는 개발언어를 채택하고 있다. ME 1.0의 경우에는 무선단말기까지의 End-to-End 보안문제 등의 미해결과제가 있으며, 이는 WAP 1.2도 해결책을 제시하지 못하고 있다. ME 2.0버전에서는 이에 대한 해결책을 내놓을 것이라 한다. ME의 방식을 따를 경우에는 MS의 운영체제 및 어플리케이션의 토탈 솔루션을 향후에 제공받을 수 있을 것이라는 장점이 있다. 이러한 ME 방식을 국내에서는 한국통신프리텔과 한솔엠닷컴이 채택하고 있다. 이에 대응해 삼성전자는 단말기 업체로서 또 하나의 다른 방식을 제공하고 있는데 그것이 바로 s-HTML이다. s-HTML

도 syntax는 c-HTML이나 m-HTML과 비슷한 점이 많다. Any-Web이라는 브라우저 및 보안 모듈인 MMS 2.0, 보안 Gateway Server인 MProxy Server 2.0을 개발하였다. 이러한 많은 무선 인터넷 방식이 난립하는 가운데 어떠한 방식이 표준으로 자리잡게 될 지는 알 수 없다. 그러나 현재 사용되고 적용되는 방식을 기초로 새로운 표준이 생길 것임에는 틀림이 없다.

따라서 본 과제에서는 무선인터넷을 구현하기 위해 현재 사용되고 있는 다양한 기술들을 다방면으로 보다 자세히 연구·분석하여 위와 같은 구현 방식을 모두 수용한 범용적인 무선인터넷 시스템을 설계 및 구축하고자 한다.

제 2 장 m-commerce 시스템 기술 개발의 현황

제 1 절 m-commerce를 위한 기반기술

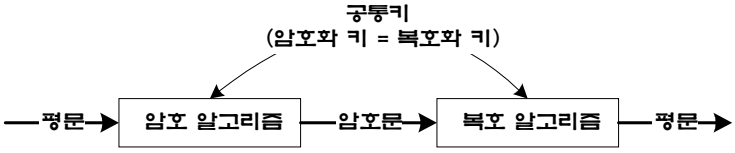
1. 보안 기술

가. 암호화 기술

암호화 기술은 평문을 허가받은 사람만이 해독 가능한 형태의 암호문으로 변환하는 기술이다. 이 기술은 공개된 전산망에서의 불법적인 도청을 방지하기 위하여 사용되는 것으로, 제 3자가 정보를 훔쳐내더라도 그 의미를 알 수 없게된다. 이러한 암호화, 복호화 과정에서 이용되는 알고리즘을 암호 알고리즘이라 하고 암호 알고리즘에서 암호문 변환의 주체가 되는 것을 키(Key)라고 한다. 이 때 사용되는 키의 종류에 따라 암호키와 복호키가 같은 관용키 암호알고리즘과 이들 두 키가 다른 공개키 알고리즘으로 구분된다.

1) 대칭형 암호화

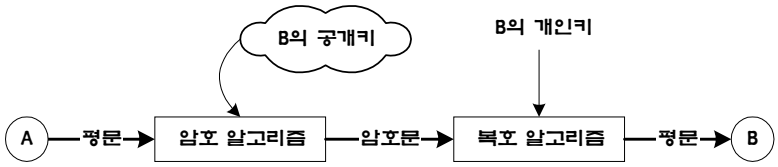
공통키 암호화 방식(Symmetric Algorithm)은 암호키로부터 복호키를 계산해 낼 수 있거나, 복호키로부터 암호키를 계산해 낼 수 있는 방식을 말한다. 이 방법의 장점은 암호화와 복호화가 빠르다는 점과, 다양한 암호화 기법이 개발되어 있다는 것이며 단점은 복수의 사용자가 관련되어 있을 때 키의 공유문제가 발생한다는 것이다. 또한 키 자체를 상대방에게 안전하게 보내는 것이 문제가 될 수 있다. 공통키 암호화 방식에서는 암호키와 복호키가 동일하며 이 키를 Key라고 했을 때 암호화와 복호화 과정은 [그림 3]과 같다.



[그림 3] 대칭키(비밀키) 암호 시스템

2) 공개키 암호화

공개키 암호화 방식(Asymmetric Algorithm)은 암호키와 복호키가 다른 형태이고, 이 방식은 알고리즘 수행 속도측면에서는 다소 느리기는 하지만 다수의 사용자가 이용시에는 키관리가 편리하다는 강점을 가지고 있다. 그러므로 인터넷 전자상거래와 같이 수백만명의 사용자가 있는 경우에 널리 활용되고 있으며 암호화와 복호화 과정은 [그림 4]와 같다.



[그림 4] 공개키 암호 시스템

3) 해쉬 함수

암호학적 해쉬 함수는 현대 암호학에서 중요한 역할을 수행하고 있다. 특히 무결성과 메시지 인증을 위한 사용에 관심을 가질 수 있다. 해쉬 함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해쉬값 또는 해쉬 코드라 불리우는 값을 출력한다. 보다 엄밀하게 말하면, 해쉬 함수는 임의의 길이의 문자열을 고정된 길이를 갖는 n비트 문자열로 대응시킨다. 정의역을 D, 치역을 R이라 할 때 해쉬 함수 h:D->R (|D|>|R|)는 다대일 대응 함수이다. 이것은 충돌이 반드시 존재함을 의미한다.

해쉬 함수는 현재 전자서명(Digital Signature)과 메시지 인증(Message Authentication) 등과 같은 응용분야에서 매우 중요한 도구로 사용되고 있다. 처음에는 주로 DES같은 블록 암호알고리즘에 기초하여 해쉬 함수를 설계하였으나, 블록 암호알고리즘 자체의 속도문제로 말미암아 전용 해쉬 함수 개발의 필요성이 대

두되었다. 현재 가장 널리 사용되고 있는 해쉬 함수는 전용 해쉬 함수로써. 1990년 Rivest가 제안한 MD계열 해쉬 함수가 주를 이루고 있다.

나. 인증 및 서명

1) 인증

인증(authentication)이란 정보의 교류 속에서 전송 받는 정보의 내용이 변조 또는 삭제 여부와 주체가 되는 송/수신자가 정당한지를 확인하는 방법을 말한다. 보통 인증이라 하면 사용자 인증과 메시지 인증으로 구분한다.

가) 네트워크 통신상의 위협 요소

네트워크를 통해 메시지를 주고받을 경우 다음과 같은 위협 요소들이 존재할 수 있다.

- 위장 : 마치 자신이 정당한 송·수신자인 것처럼 행동하거나, 불법적 메시지를 정당한 사용자로부터 온 것처럼 위장할 수 있다.
- 내용 변조 및 수정 : 내용의 일부 또는 전체를 삽입, 삭제, 변경, 수정하는 일련의 행위
- 순서 및 시간 변경 : 통신 쌍방간의 메시지를 삭제하거나 재 정렬하는 경우 송신자의 의도와는 다른 결과를 얻을 수 있다. 또한 메시지를 지연시키거나 같은 내용을 반복해 보낼 경우 수신자는 혼란을 일으킬 수 있다.
- 트래픽 분석 : 사용자들 사이의 트래픽 형태를 예측함으로서 연결의 주기와 기간등을 결정해 주요 정보가 전송되는 시간대에 메시지를 가로챌 수 있다.
- 부인 : 메시지의 송신 또는 수신 사실을 부인함으로서 신뢰성을 떨어뜨릴 수 있다.

나) 사용자 인증

사용자 인증이란 메시지의 생성, 전송, 수신, 이용, 저장 등의 일련의 과정에 관련되어 있는 송/수신자, 전송자, 이용자, 관리자들이 제 3자에게 자신이 진정한 사용자라는 것을 증명할 수 있도록 하는 기능을 말한다. 그런, 제 3자가 위장을 통해 자신이 진정한 사용자임을 증명하려 할 경우 불가능해야 한다.

다) 메시지 인증

메시지 인증이란 전송되는 메시지의 내용이 변경이나 수정이 되지 않고 본래의 정보를 그대로 가지고 있다는 것을 확인하는 과정을 말한다. 즉, 수신된 메시지가 정당한 사용자로부터 전송되었고, 변경되지 않았음을 확인하기 위해 인증을 수행하게 된다.

2) 전자 서명

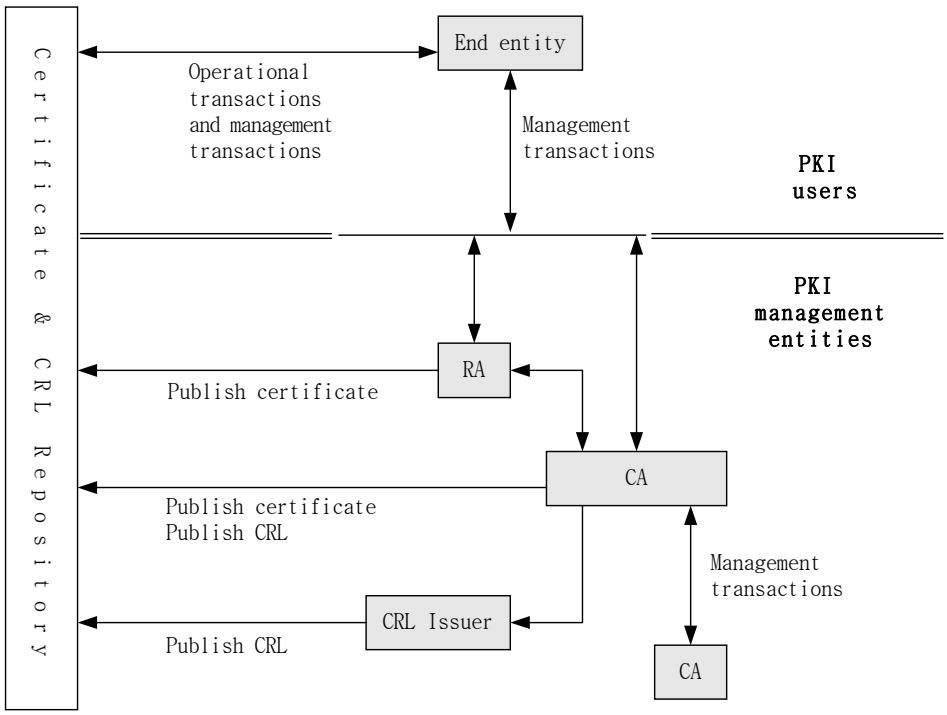
전자 서명이란 전자화된 문서의 메시지 내용이 수정 및 변조되지 않았음을 보장하는 동시에 메시지의 주체인 사용자들이 진짜라는 것을 제 3자가 확인할 수 있게끔 하는 인증 방식을 말한다. 전자서명으로 이용될 수 있는 암호 시스템은 크게 대칭형 암호 방식, 중재자 방식 그리고 공개키 암호 방식 등이 있다.

다. 공개키 기반구조(PKI)

1) PKI 개요

인증 서비스를 제공하는데 있어서 기반기술로 작용하는 공개키 기반구조는 공개키 암호방식에서 공개키의 인증 문제를 해결하기 위한 것으로, 신뢰할 수 있고 효율적인 키 관리 및 인증서 관리 기능을 제공함으로써 사용자 인증, 부인방지, 기밀성 제공등 보안 서비스의 사용을 가능하게 하는 것이 목적이다. 즉 공개키 기반구조는 보안 서비스 및 인증 서비스 제공을 위한 제반 구조를 제공한다.

PKI시스템을 구성하는 요소로는 인증서를 발행하고 취소하는 인증기관, 인증서 등록 및 사용자 신원확인을 대행하는 등록기관, 인증서 및 인증서 취소 목록을 저장하고 사용자에게 서비스하는 디렉토리, 그리고 인증서를 신청하고 인증서를 사용하는 사용자로 분류될 수 있다. [그림 5]는 PKI 시스템 구성 요소간의 관계를 나타낸 것이다.



[그림 5] 공개키 기반구조

가) 인증기관 (CA : Certification Authority)

인증기관은 일반적으로 계층구조를 이루며, 다음과 같은 기능을 수행한다.

- 사용자의 공개키 인증서를 발행 또는 취소한다.
- 사용자에게 자신의 공개키와 상위기관의 공개키를 전달한다.
- 등록기관의 요청에 의해 인증서를 발행한다.
- 상호 인증서를 발행한다.
- 인증서와 그 소유주 정보를 관리한다.
- 인증서, 인증서취소목록, 감사파일을 관리한다.

나) 등록기관 (RA : Registration Authority)

인증기관이 사용자에게 인증서를 발행해주기 위해서는 먼저 사용자의 신원을 확인해야 하는데 이와 같은 사용자 인증 문제가 중요해지면서 사용자 신원 확인과 인증서 발급 과정을 분리하는 것이 보편적인 추세이다. 조직등록기관(Organization Registration Authority) 이라고도 하며 등록기관의 기능은 다음과 같다.

· 인증기관을 대신해 사용자들의 인증서 신청시 그들의 신원과 소속을 확인하는 기능을 수행한다.
· 사용자의 신원을 확인한 등록기관은 사용자의 인증서 요청서에 서명하여 이를 인증기관에 전달한다.
· 디렉토리로부터 인증서와 인증서 취소 목록을 검색한다.
· 인증서 취소를 요청한다.

다) 저장소(Repository)

인증서와 사용자 관련정보, 상호인증서 및 인증서 취소목록을 저장 및 검색하는 장소로서, 응용에 따라 이를 위한 서버를 따로 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버는 DAP(Directory Access Protocol)이나 LDAP(Lightweight Directory Access Protocol)를 이용하여 X.500 디렉토리 서비스를 제공한다.

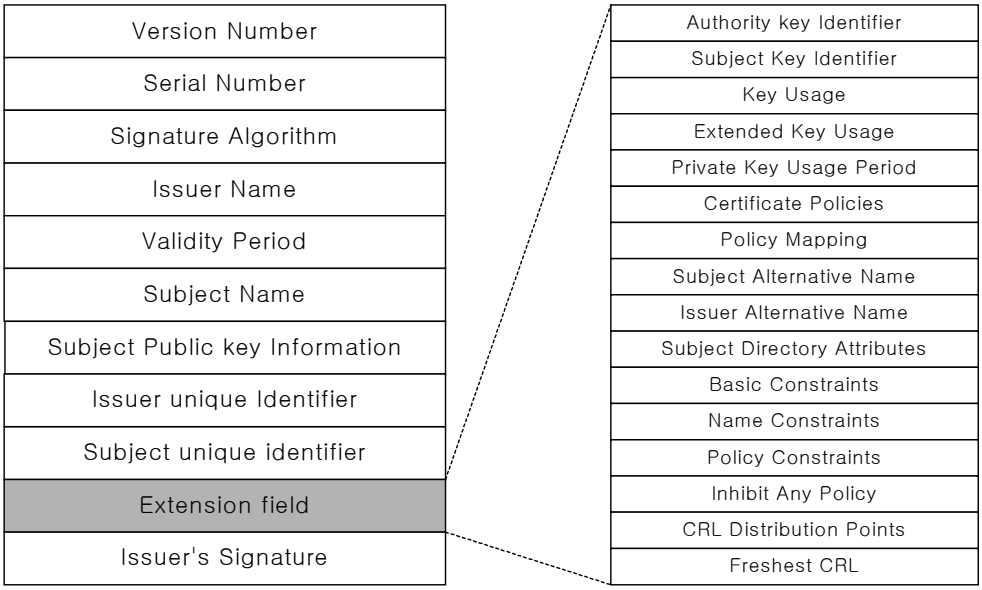
라) 사용자(Client)

PKI내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미하며, 다음의 기능을 수행한다.
· 자신의 비밀키/공개키 쌍을 생성한다.
· 인증기관에 공개키 인증서를 요청하고 인증서를 받는다.
· 전자서명을 생성 검증한다.
· 특정 사용자의 인증서를 획득하고 인증서 취소목록을 이용하여 인증서 상태 검증을 한다.
· 인증경로를 해석한다.
· 비밀키의 손상 및 분실로 인한 긴급상황 발생시 인증기관에 인증서를 취소하고 새로운 인증서를 발급 받아야 한다.

2) X.509 인증서

인증기관인 CA는 사용자의 공개키를 자신이 서명한 인증서로써 신뢰할 수 있음을 증명한다. CA가 제공하는 인증서는 ITU-TX.509 표준을 따른다. 인증서의 구성은 인증서 버전, Serial Number, 알고리즘 식별자, 발행자, 유효기간, 등록자의

ID와 CA의 개인키로 암호화된 서명으로 구성되어 신뢰할 수 있는 공개키를 제공받을 수 있다.



[그림 6] X.509 인증서 구조

X.509 인증서의 구성항목과 내용은 [표 1]에 표기하였다. 사용자는 인증기관에 의해 공개키의 무결성을 보장받을 수 있다. 그러나 사용자의 개인키의 노출이나, 도난, 분실된 경우 키를 획득한 악의의 사용자가 정당한 사용자로 가장할 수 있다. 그러므로 개인키의 누출에 따른 키의 손상의 경우 인증기관에 등록된 해당 개인키를 즉시 폐지하고 이를 다른 사용자들에게 알려야 한다. 이렇게 폐지된 인증서들에 대한 목록을 인증서 폐지목록(CRL : Certificate Revocation List)이라 하고 인증서를 요청하는 사용자에게 이 목록도 검색할 수 있도록 하여야 한다.

[표 1] X.509 구성 항목과 세부 내용

항 목	내 용
Version	인증서 형식의 연속된 버전의 구분, (0,1,2)
Serial Number	발행자가 생성한 각각의 인증서에 대한 유일 식별자
Algorithm Identifier	인증서를 서명하기 위해 사용된 알고리즘
Issuer	인증서를 발행하고 서명한 CA
Period of Validity	인증서가 유효한 시간
Subject	공개키 소유자 ID
Subject Public Key Information	사용자의 공개키와 이 키가 사용될 알고리즘 식별자
Issuer unique identifier	발행자의 부가적인 정보포함
Subject unique identifier	공개키 소유자의 부가적인 정보포함
Extensions	인증정책, 인증서 취소목록관련 등 여러 기타 사항
Signature of CA	CA의 개인키로 암호화된 CA서명 값

인증서 폐지목록에는 인증서 폐지목록의 버전, 서명, 알고리즘 및 발급기관의 이름, 인증서 발급일, 다음 갱신일, 취소된 인증서의 정보(인증서 일련번호, 폐지일자 및 사유)등이 포함되어 있다. 또한 인증서의 유효기간에 따라 인증서 효력이 만료되기도 하는데, 장기간 동안 같은 키를 사용할 경우 노출의 위험이 늘어나므로 정해진 기간이 초과되면 인증서의 기능을 상실하게 된다.

2. 전자상거래

전자상거래와 관련된 표준으로는 CALS와 관련된 표준인 STEP, ITEM, CITIS 등을 비롯하여 실제 상품 정보의 검색, 교환, 거래에 활용되는 전자카탈로그, 상품 분류체계 및 코드, 새로이 주목받고 있는 XML 계통의 정보교환 표준, 전자지불, 보안, 인증과 관련된 내용 등 기술적 범위가 매우 광범위한 것이 특징이다. 이중 전자상거래에 특화된 기술의 표준화 동향은 다음과 같다.

가. 전자상거래 프레임워크

전자상거래의 실제적인 시스템 구현을 위하여 체계적인 호환성 확보를 위한 프레임워크를 구성하는 작업이 국제적으로 활발히 진행되고 있다. 대표적인 예로는 XML을 기반으로 하는 CommerceNet의 eCo와 마이크로소프트사가 활동하는 BizTalk 등을 들 수 있다.

eCo 프레임워크는 인터넷 전자상거래의 각종 서비스, 보안, 응용 프로그램상의 문제를 해결하기 위해 CommerceNet에서 제안한 전자상거래 프레임워크로서 인터넷 전자상거래에서의 객체지향 아키텍처를 통합 어플리케이션과 서비스 재활용성을 증진하는 것을 목적으로 한다. BizTalk는 플랫폼에 상관없는 전자상거래 프레임워크를 구성하는 것으로 EAI(Enterprise Application Integration)이나 전자상거래를 위하여 구성되었다. 이 외에도 XML을 이용하여 전자상거래의 공통된 기반이나 프레임워크를 구성하고자 하는 표준화 활동으로는 xCBL, ResettaNet, cXML, ebXML 등이 있다.

나. 전자카탈로그, 상품분류체계 및 코드

전자카탈로그란 전자상거래를 위하여 상품 및 서비스에 대한 정보를 전자적인 형태로 저장하여 교환하기 위한 전자문서를 말하며 상품에 대한 간략한 소개, 동화상, 정지화상, 제작업체 URL, 연락처, 주문서 및 기업에 대한 기타 안내 등 기존의 인쇄물 형태의 카탈로그에 비하여 많은 내용으로 구성된다.

전자카탈로그의 구축 및 교환을 위한 기술적 구성요소는 다음 표와 같다.

[표 2] 전자카탈로그의 필요한 기술적 구성요소

분류	내용
포맷관련	상품정보의 전자적 문서 저장방법(포맷) 예 - 텍스트, HTML, XML, SGML, PDF, RTF 등
표현관련	전송된 상품정보를 사용자가 볼 수 있는 형태로 나타내기 위한 스타일시트 예 - CSS, XSL, DSSSL 등
전송관련	상품정보를 전송하기 위한 전송 프로토콜 예 - HTTP, X.400, X.435, FTP, SMTP 등

이외에도 전자카탈로그의 관련된 표준으로 디렉토리서비스 표준이 있다. 디렉토리 서비스 표준으로는 현재 X.500과 LDAP가 많이 사용되고 있다.

다. 전자지불

전자지불시스템이란 기존의 화폐 개념을 네트워크 상으로 옮겨 디지털화한 무형의 화폐 또는 지불 수단을 말한다. 전자화폐는 크게 가치저장형(Mondex, K-cash 등), 지불지시형(CyberCash, First Virtual), 네트워크형(Ecash, Netcash)으로 구분할 수 있으며 전자화폐와 관련된 표준으로는 Smart Card나 IC Card에 관련된 표준, 보안 프로토콜에 관련된 표준, 플랫폼이나 운영체계에 관련된 표준, 인터넷 뱅킹에 관련된 표준 등을 들 수 있다. 다음은 전자지불과 관련된 표준 기술이다.

- o SET(Secure Electronic Transaction)
- o SSL(Secure Socket Layer)
- o JEPI(Joint Electronic Payment Initiative)
- o MULTOS(Multi-application Operating System)
- o Java Card
- o EMV(Europay, Mastercard and Visa)
- o OFX(Open Financial Exchange)

라. 전자문서/XML

1999년 2월 제정된 전자서명법에 따르면 전자문서란 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 작성, 송·수신 또는 저장된 정보를 말한다. 또한 전자문서교환(Electronic Data Interchange)란 거래상대방과의 업무 처리에 있어 종래의 종이서류 대신에 서로 합의한 표준화된 전자문서를 컴퓨터간에 교환하는 방식을 말한다.

관련 기술로는 Open-EDI, OO(Object-Oriented)-EDI, Interactive EDI, 인터넷 EDI, XML/EDI, Simple-EDI, BSI(Business System Interoperation)등을 들 수 있다.

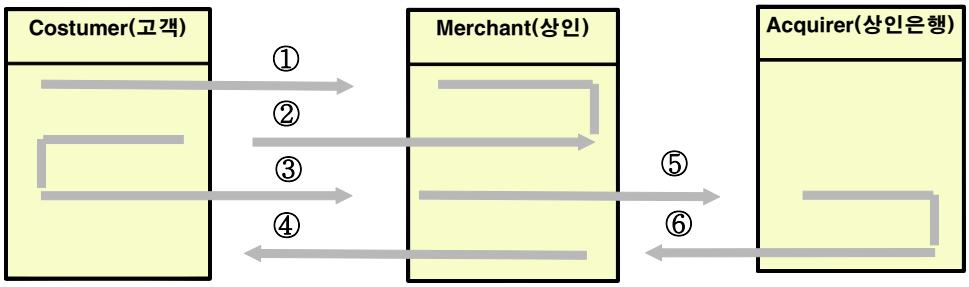
마. CALS

CALS는 제품의 설계, 획득, 운영지원과정에서 발생하는 자료와 정보를 디지털화하여 자동화된 환경을 제공함으로써 업무의 과학적, 효율적 수행과 정확하고 신속한 정보공유 및 유통체계를 통해 제품 획득, 운영지원 비용 절감, 시간 단축, 종합적인 품질경영 능력을 향상시키고자 하는 전략이라 정의할 수 있다. CALS와 관련된 기술들은 다음과 같다.

- o STEP(STandards for the Exchange of Product model data)
- o IGES(Initial Graphic Exchange Specification)
- o CGM(Computer Graphic Metafile)
- o Raster Graphic
- o IETM(Interactive Electronic Technical Manual : 대화형전자식기술교범)
- o CITIS(Contractor Integrated Technical Information System)

바. SET(Secure Electronic Transaction)

SET은 현실세계의 신용카드 거래를 기반으로 모델링되어 기존의 금융 시스템과 연동이 쉬운 구조로써 고객(Cardholder), 상인(Merchant), 상인은행(Acquirer), 카드발행처(Issuer:은행 또는 카드회사), 인증국(CA), 지불 게이트웨이(Payment gateway)로 구성된다. [그림 7]는 SET의 구성요소간 전자지불 정보의 트랜잭션 단계로 1,2 단계는 고객과 상인사이에 확인서와 인증정보를 주고 받음으로써 전자지불 절차를 수행하기 위해 준비하는 단계이고. 제 3단계에서는 고객의 상품선택 후 지불요청을 하고, 상인은 고객의 지불정보에 따라 은행에게 확인 요청을 제 4단계에서 실행한다. 또 제5단계에서는 은행이 이에 대한 조회결과를 알려주고 끝으로 제 6단계에서는 고객이 요구한 상품 및 서비스를 상인이 고객에게 제공한다.



[그림 7] SET기반 트랜잭션 단계

1) SET의 기본 기능

전자지불 프로토콜로서 SET은 보안 문제점이 금융기관, 상인, 고객 모두의 이익에 어떤 문제도 끼쳐서는 안된다는 원칙을 기본으로 다음과 같은 기능적 요구사항을 만족하도록 설계되었다.

■ 정보의 기밀성 제공

인터넷을 통한 개인의 신용카드 번호등의 지불 정보와 함께 전송되는 구매정보등 상거래 정보의 유출을 막기 위해 메시지 암호화를 통해 정보의 기밀성을 유지한다.

■ 정보의 무결성 제공

지불 정보가 전송중에 변조되지 않았다는 것을 증명하기 위해 전자 서명을 사용하여 보낸 메시지와 받은 메시지가 정확히 일치함을 보여줌으로써 정보의 무결성을 제공한다.

■ 고객에 대한 인증

카드를 가지고 거래를 하는 고객에 대한 인증은 고객이 인증기관에서 발급받은 인증서와 전자 서명을 사용하여 해당 고객이 유효한 신용카드 사용자임을 확인한다.

■ 상인에 대한 인증

고객의 입장에서 볼 때 자신이 거래하는 상인이 해당 브랜드의 카드를 수용할 수 있는 권한을 지니고 있는지 확인하기 위해 전자 서명과 함께 상인이 인증기관에서 발급받은 인증서를 사용한다.

■ 최상의 보안성 제공

전자상거래의 모든 정당한 구성원을 보호하기 위해 효율적이면서도 강력한 보안성을 제공하기 위해 공개키 암호화 알고리즘과 전자 서명, 전자 봉투(digital envelope), 이중 서명등의 보안 기술을 사용한다.

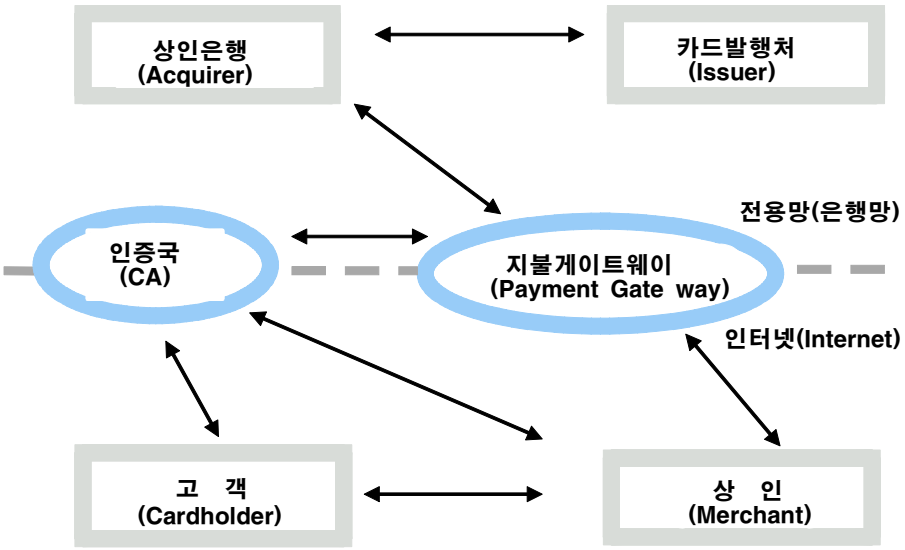
■ 벤더(vendor) 독립성

기존 전자 지불 처리 기술과 달리 특정 벤더에 영향을 받지 않고 다양한 하드웨어와 소프트웨어에서 적용이 가능한 구조로 설계되어 다양한 응용 소프트웨어의 개발이 가능하게 하였다.

2) SET 프로토콜의 구성 및 처리 절차

SET프로토콜이 정의하는 영역은 전송되는 메시지에 대한 암호화 알고리즘의 적용 방법과 인증에 사용되는 메시지와 그 형식, 구매에 사용되는 메시지와 그 형식, 인가에 사용되는 메시지와 그 형식, 대금 결재에 사용되는 메시지와 형식 그리고 구성 요소들간에 주고받는 메시지 등이다. [그림 8] 은 SET을 기반으로 한 전자지불 시스템이 인터넷 상에 구현되었을 때의 구조를 보인 것이다.

SET에서 참여자는 상인은행, 카드발행처, 지불게이트웨이, 인증국 그리고 고객이며 쇼핑 시나리오는 다음과 같다. 고객이 상인의 웹 홈페이지에서 구매할 상품을 검색하고 선택하면 선택된 상품에 대한 구매 요구가 상인 서버로 전송된다. 이에 상인서버는 접수된 구매 요구에서 고객이 선택한 물품에 대한 가격, 선적 요금 등을 포함한 구매 형식을 고객에게 전송한다.

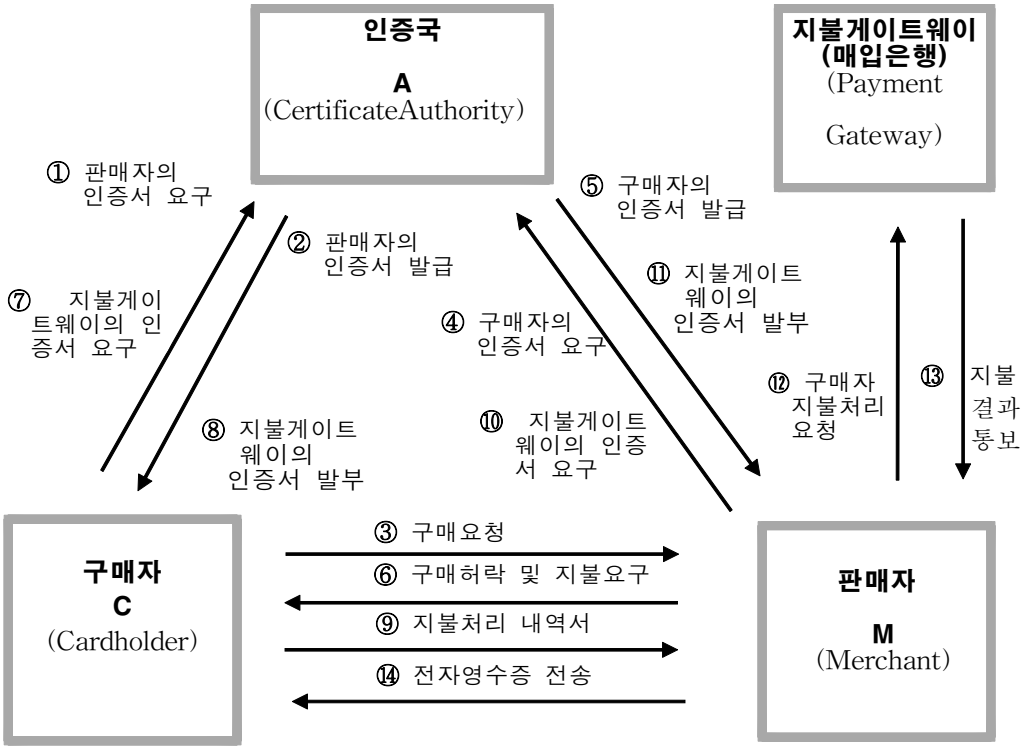


[그림 8] SET기반의 전자상거래 구조

고객은 구매 요구형식을 확인하고 지불에 사용할 신용카드의 정보와 함께 암호화하여 최종 구매 요구를 상인 서버로 전송하게 되는데 상인 서버는 고객이 전송한 최종 구매요구에 포함된 지불 정보를 지불 게이트웨이로 전송하여 지불인가 요청한다. 지불 게이트웨이(payment gateway)는 지불 정보를 은행 망과 연동하여 지불인가(authorization)를 요구하고 그 결과를 상인 서버로 전송하면 상인 서버는

지불인가 결과에 따라 거래가 성립되었다면 지불인가 정보를 포함한 전자 영수증에 해당하는 구매 확인서 전송하여 주고 상인 서버는 성립된 거래에 대한 서비스를 수행 또는 배달 대행 서비스에 상품 배달 의뢰하면 접수된 상품 배달 요구에 따라 해당 고객에게 상품 배달된다. 그리고 상인서버는 지불인가와 동시에 또는 일괄처리에 의해 정기적으로 인가받은 지불에 대한 결재 요구를 지불 게이트웨이로 전송하게 된다. 마지막으로 지불 게이트웨이는 상인 서버로부터 전송된 결재 요구를 금융망과 연동하여 수행하게 된다.

이와 같은 수행절차[그림 9]을 단계별로 자세히 살펴보면 다음과 같다.



[그림 9] SET기반 전자상거래 수행절차

[1 단계] 고객이 상인의 웹 홈페이지에서 구매할 상품을 검색하고 선택한 후 상인의 인증서를 인증기관에 의뢰한다.

[2 단계] 인증기관은 고객인 정당한 인증국에 등록된 여부와 함께 고객이 원하는 거래상대자인 상인이 인증기관에 등록되어 있고 정당한 거래자인경우 전

자인증서를 고객에게 발급하여 준다.

[3 단계] 고객은 상인의 인증서를 통해 얻은 공개키로 정보를 암호화한 후 상인에게 선택된 상품에 대한 구매 요구를 한다.

[4 단계] 상인은 접속 요청자인 고객이 정당한 거래자인지를 알기 위하여 인증국에 고객의 인증서를 확인 및 발부요청을 한다.

[5 단계] 인증기관은 상인의 거래 상대자인 고객의 인증서를 상인에게 발부하여 준다.

[6 단계] 상인은 인증서를 통해 정당한 카드거래자임을 알고 접수된 구매요구에서 고객이 선택한 물품에 대한 가격, 선적 요금등을 포함한 구매 형식을 고객의 인증서에서 획득한 고객의 공개키로 암호화하여 고객에게 전송한다.

[7 단계] 고객은 상인이 보내온 구매허락 및 구매형식에 대하여 상품내역과 카드결제를 위한 정보 즉, 자신의 카드번호, 비밀번호, 자신의 신분등을 암호화하여 상인에게 보내게 되는데 여기에서 고객은 상인과 지불게이트웨이에게 보낼 정보를 각각 암호화하여 보낸다. 먼저 고객은 인증기관에게 지불게이트웨이의 인증서를 요구한다.

[8 단계] 인증기관에서는 지불게이트웨이를 인증하는 전자인증서를 고객에게 전송한다.

[9 단계] 고객은 지불게이트웨이의 전자인증서를 통해서 공개키를 획득하고 자신이 상인에게 보낼 정보중에 지불정보(신용카드정보)를 지불게이트웨이의 공개키로 암호화하고 상인에게 보낼 주문정보는 상인의 공개키로 각각 암호화하여 최종 구매 요구를 상인에게 전송한다.

[10 단계] 상인 서버는 고객이 전송한 최종 구매요구에 포함되어 있는 구매정보를 확인하고 지불 정보를 지불게이트웨이로 전송하여 지불인가를 요청하기 위하여 먼저 지불게이트웨이의 인증서를 인증기관에 의뢰한다.

[11 단계] 인증기관은 지불게이트웨이의 인증서를 상인에게 전송한다.

[12 단계] 상인은 지불게이트웨이의 인증서를 통해 지불게이트웨이를 인증함과 동시에 공개키를 얻어 자신의 인증서 와 고객의 인증서 그리고 고객이 보내온 정보중의 지불정보를 보낸다.

[13 단계] 지불게이트웨이는 상인으로부터 전송된 지불 정보에 대한 결과를 상인 서버로 전송한다.

[14 단계] 상인 서버는 지불인가 결과에 따라 거래가 성립되었다면 지불인가

정보를 포함한 전자 영수증에 해당하는 구매 확인서를 고객에게 전송한다.

[15 단계] 상인 서버는 성립된 거래에 대한 서비스를 수행 또는 배달 대행 서비스에 상품 배달 의뢰하면 접수된 상품 배달 요구에 따라 해당 고객에게 상품 배달된다.

[16 단계] 상인서버는 지불인가와 동시에 또는 일괄처리에 의해 정기적으로 인가받은 지불에 대한 결재 요구를 지불 게이트웨이로 전송하게되고 지불 게이트웨이는 상인 서버로부터 전송된 결재 요구를 금융망과 연동하여 수행하게 된다.

공개키 암호화 방식과 비밀키 암호화 방식을 결합하여 신뢰성 있는 정보만을 제공하는 SET프로토콜이 실질적으로 서비스되기 위해서는 다음과 같은 문제들이 해결되어야 한다. 먼저 판매자와 구매자 모두가 신용카드 결제에 앞서 디지탈 ID를 확보해야한다. 둘째, 신용카드 기반 전자지불 시스템이 한번의 지불 트랜잭션에 카드신용조회, 키인증, 네트워크 비용 등을 감안하여 처리절차를 최소한 단축시킴으로 지불 트랜잭션의 비용을 감축시켜야 한다. 셋째, 신용카드 결제로 인한 개인정보 유출 등의 후유증이 해결되고 마지막으로 전자상거래 시스템을 이용하는 구매자들이 찾고자하는 물건들을 쉽게 발견할 수 있도록 전체 시스템과 결제시스템을 조율하여야 한다.

3) SET 프로토콜의 범위와 구성

SET 프로토콜이 정의하는 영역은 전송되는 메시지에 대한 암호화 알고리즘의 적용 방법과 인증에 사용되는 메시지와 그 형식, 구매에 사용되는 메시지와 그 형식, 인가에 사용되는 메시지와 그 형식, 대금 결재에 사용되는 메시지와 그 형식 그리고 구성 요소들간에 주고받는 메시지등이다. SET에서는 상품 검색이나 상품 배달, 상품 정보의 제공에 사용되는 메시지, 고객 및 상인의 신용도 관리나 상인에 의해 구성되는 웹 홈페이지의 구성과 신용카드 이외의 수단 및 고객, 상인, 지불 게이트웨이 시스템 자체에서의 방화벽등에 의한 시스템 보안에 대해서는 정의하지 않았다.

SET은 OSI layer의 응용 계층에서 운영되는 프로토콜로 크게 고객(Cardholser), 상인(Merchant), 상인 은행(Acquirer), 카드 발행처(Issuer : 은행 또

는 카드회사), 인증국(CA)지불 게이트웨이(Payment gateway)로 구성된다. [그림 8]은 SET을 기반으로 한 전자 지불 시스템이 인터넷상에 구현되었을 때의 구조를 보인 것으로 그림에서 화살표는 정보의 흐름을 나타낸 것이다. 고객은 카드 발행사로부터 발급받은 신용카드를 소지하고 컴퓨터를 이용하여 인터넷에 있는 상인의 홈페이지에서 상품을 선택하고 구매하는 당사자를 의미한다. 상인의 인터넷 상에 홈페이지를 개설하고 상품을 판매하거나 서비스를 제공하는 역할을 하며 신용카드를 취급하기 위해 은행과 관계를 맺어야 한다. 지불 게이트웨이는 상인으로부터 전송된 지불 정보를 은행망 쪽에 있는 상인 은행으로 전송하여 처리하는 일종의 대리인 역할을 한다. 고객, 상인, 지불 게이트웨이는 SET을 이용한 거래를 하기 위해 인증국에 등록하고 인증서를 발부 받는다. 서로 메시지를 주고 받는 당사자들은 상대방에게 보낼 메시지를 암호화하는데 공개키가 실제로 상대방의 공개키가 확실한지 확인할 방법을 필요로 한다. 인증국은 공개키의 안전한 배포를 위해 믿을 수 있는 기관에 설치되며 등록자들의 공개키가 들어있는 인증서를 전자 서명하여 인증한다. 카드 발행처와 상인 은행은 지불 게이트웨이로부터 전송된 신용카드 지불 정보를 기존의 신용카드 거래에서 수행되는 방식과 동일한 방법으로 처리하고 그 결과를 지불 게이트웨이로 전송한다.

3. 무선인터넷

무선인터넷 기술의 핵심은 무선망과 유선망의 효율적인 결합이다. 다시 말해서 CDMA/GSM 기반의 무선망과 TCP/IP를 사용하는 인터넷 망을 효율적으로 연동하여, 무선단말기로부터 무선망을 통해 유선망에 위치한 컨텐츠에 효율적으로 접근할 수 있는 통신 프로토콜을 정의하는 것이 무선인터넷 기술이 해결해야 하는 핵심과제인 것이다. 그러므로, 이러한 무선인터넷 표준을 주도하기 위한 치열한 경쟁이 벌어지고 있는데, 국내에서는 WAP 진영과 MS 진영의 양분화가 진행되고 있으며, 일본의 NTT 도코모는 아이모드라는 독자적인 행보를 걷고 있다.

WAP(Wireless Application Protocol)은 모토로라, 노키아, 에릭슨, Phone.Com 등이 주축이 되어 결성하고, 현재 AT&T, 벨사우스 와이어리스 데이터, IBM, 삼성전자, LG IC 등을 포함하여 전 세계의 200여 개 업체가 회원으로 참여하고 있는 WAP 포럼이 무선인터넷을 위하여 정의한 프로토콜이다. WAP의 특징은 기존

의 인터넷 기술을 그대로 수용하되, 무선환경에 최적화 된 프로토콜을 정의하는 것이며, 단말기에 탑재된 WAP 브라우저가 WAP 게이트웨이를 통해 WML/WMLScript로 구성된 컨텐츠에 접근하는 것으로 정의되어 있다.

WAP의 가장 큰 장점은 현재 전 세계적으로 표준에 가장 가까이 다가서 있고, 무선 부분에 관해 고효율의 이용이 가능하다는 것이다. 반면 HTTP, TCP 등 기존 인터넷 표준의 프로토콜을 사용하고 있지 않아 HTML과의 상호 호환성이 떨어진다는 단점이 있다. WAP을 통한 무선인터넷 서비스 제공에는 WML로 변환하기 위한 게이트웨이가 반드시 필요하다. 이 때문에 WAP 서비스를 직접 제공하려면 그 투자 비용이 상당하다. 국내 사업자 중 SK텔레콤과 신세기통신, LG텔레콤에서는 WML에 기반한 WAP 서비스를 시행중이다.

마이크로소프트는 기존의 HTML과 HTTP를 그대로 사용하여 모바일 익스플로러가 탑재된 단말기를 통해 HTML 문서에 접근하는 방식을 사용하고 있으며, 도코모의 아이모드 역시, Compact Netfront라는 HTTP 기반의 웹 브라우저가 탑재된 단말기를 통해 HTML로 작성된 문서에 접근하는 방식을 채택하고 있다. 물론 기존의 HTML을 그대로 사용할 수 없으므로 마이크로소프트와 아이모드는 각각 mHTML, C-HTML이라는 HTML의 서브셋을 재정의 하였다.

모바일 익스플로러는 게이트웨이를 이용하지 않기 때문에 투자비를 절감할 수 있으며 기존의 HTML 컨텐츠를 그대로 이용할 수 있다는 장점을 제공한다. 동시에 브라우저의 오버헤드가 크다는 단점이 있으며 공개되지 않는다는 점에서 브라우저에서 지원하지 않는 파일을 이용한 서비스를 제공하지 못하는 단점도 가진다. 현재 국내 시장에서는 한국통신엠닷컴과 한국통신프리텔이 마이크로소프트의 투자를 받아서 M-HTML 기반의 ME 방식 무선인터넷 서비스를 제공하고 있다.

무선인터넷 프로토콜을 정의할 때 고려해야 할 사항은 무선망과 무선단말기의 열악한 환경으로 인한 제약이다. 무선망은 유선망보다 상대적으로 열악한 통신환경을 가지고 있다. 특히, 유선망에 비해 대역폭이 제한적이므로, 대역폭의 효율적인 사용이 관건이다. 그리고 무선단말기는 PC와는 달리, 디스플레이 크기가 작고, 입력장치가 발달되어 있지 않으며, 전력소모량이 적어야 한다는 제한이 있다. 그러므로, 이러한 무선환경의 제약사항을 충분히 고려하고 있으며, 또 오픈된 표준을 선택하고 있는 WAP 프로토콜이 앞으로 세계적인 표준을 장악할 전망이다. 마이크로소프트는 WAP 포럼의 회원으로 참여하였고, 워킹 그룹에서 활동하고 있음을 내세우며, WAP을 지원할 것임을 공식적으로 표명하였다. NTT 도코모도

WAP 방식을 채택할 것임을 밝히는 등, 현재로서는 WAP이 무선인터넷 표준경쟁에서 상대적인 우위를 차지하고 있다.

제 2 절 무선 인터넷 기술 및 표준화 동향

1. 무선인터넷 기술 현황

가. 무선 네트워크 기술

1) 모바일 IP

가) 기술 개요

IP 서브넷과 매체간의 이동성을 제공하기 위해서 IETP 모바일 IP WG에서 모바일 IP가 제안되었다. 이동통신 단말의 경우 일정한 기지국에서 다른 기지국으로 이동할 수 경우 인터넷 접속을 계속 유지, 사용할 수 없게 된다. 그 이유는 기존의 인터넷라우팅 프로토콜은 일종의 PPP(Point to Point Protocol)이기 때문에 호스트가 다른 네트워크로 바뀔 경우 호스트의 새로운 위치로 데이터를 계속 전달할 수 없기 때문이다. 따라서 이와 같은 문제를 해결하기 위한 것이 모바일 IP의 개념이다. 현재 제공되고 있는 무선인터넷 서비스는 교환기가 IP를 가지고 있는데 비하여 모바일 IP의 경우, 기지국과 단말기가 IP를 가지게 된다.

이처럼 모바일 IP는 네트워크 주소 기반의 IP 경로 설정에서 기인하는 호스트의 서브넷간 이동 제한을 극복하기 위하여 고안되었다. 기존의 IPv4는 네트워크 주소 기반의 Longest Prefix Match 방식의 라우팅 알고리즘을 사용한다. 실제로 이러한 Longest Prefix Match 방식은 라우팅 테이블의 효율과 간결함을 유지하지만 최종 목적지는 서브넷의 라우터로 제한하게 되므로 노드가 서브넷을 이동할 경우 기존의 라우팅 메커니즘은 이동성을 제공하지 못하게 된다. 모바일 IP는 3계층에서 서브넷간의 이동성을 제공하는 메커니즘으로 실제 그 자체는 완전한 이동성을 제공하는 무선환경의 3계층 프로토콜로는 큰 의미가 없다.

그러나 무선인터넷이라는 것은 기지국과 라우터로 이루어진 유선 코어 망의 절

대적인 지원을 받게 되며 특히 이러한 유선 코어 망에서 3계층 프로토콜로서 모바일 IP 이동성의 의미는 절대적이다. 실제로 3GPP2의 무선 IP 네트워크는 3계층 프로토콜로 모바일 IP를 수용하고 있고, UMTS의 경우 GPRS 내에서 글로벌한 IP 이동성을 지원하기 위해서 모바일 IP를 수용하는 표준을 정하고 있는 현실이다.

- 이동 호스트(MN)
  - 자신의 IP주소를 바꾸지 않고 접속점(Point of Attachment)을 바꾸는 호스트 혹은 라우터
- 이동성 에이전트(Mobile Agent)
  - 홈 에이전트(Home Agent : HA) : 이동 호스트의 홈 네트워크에 존재하는 라우터 혹은 호스트, 이동 호스트가 홈 네트워크를 벗어나 있을 경우 홈 에이전트는 이동 호스트에게 데이터 그램을 터널링(Tunneling). 이동 호스트의 현재 위치를 계속적으로 유지
  - 외부 에이전트(Foreign Agent : FA) : 이동 호스트의 방문 네트워크(Visited Network)에 존재하는 라우터 혹은 호스트. 홈 에이전트에 의해 전송된 데이터그램을 디-터릴링(de-Tunneling)하고 등록된 이동 호스트에 전송. 등록된 이동 호스트에게 FA 외부 에이전트는 기본 라우터로 작동됨
- 의탁주소(Care-of Address)
  - 이동 호스트에 현재 접속점을 의미(FA)하는 것으로 홈 에이전트에 의해 터널링되는 패킷의 목적지

나) IPv6 기술

(1) IPv6(IP version 6)의 개요

현재 Internet 프로토콜의 기본이 되고 있는 IPv4의 IP 주소는 32비트로 표시하기 때문에 인터넷 접속 호스트의 증가로 2005~2011 안에 이용 가능한 IP 주소가 그의 없을 것으로 전망된다. IPv4에서는 통신망간을 연결하기 위한 라우터정보 테이블의 정보량이 지나치게 커지게 되는 문제점을 가지고 있음에도 불구하고 차세대 인터넷의 활성화에 크게 기여할 것이다. IPv6는 ISTF, IETF, IAB 등에서 1993년부터 개발하였으며, 1995년 1월에 Internet Protocol 표준 권고안인 RFC 1883 (IPv6)를 발표하였다. IPv4의 후계자인 IPv6가 IPv5로 명명되지 못한 것은 ST라는 인터넷 프로토콜이 IPv5로 정해졌기 때문이다.

21세기는 인터넷이라는 통신망에 의해서 세계의 정보공유 및 전자무역이 활발하게 전개될 것이다. 이렇게 전세계적인 무역을 위한 인터넷 가입자 주소 할당을 위하여 IPv6을 폴란드의 노키아 연구소에 근무하는 찰스퍼킨스씨가 제안하여 현재 상용서비스를 위하여 세계의 연구기관에서 추진 중에 있다. 2005년경 정도면 세계이동전화의 30% 정도는 모바일 IP가 부여될 것으로 예상된다.

IPv6의 강력한 힘은 다음과 같이 표현할 수 있다.

- 주소(Addressing)의 무한대 수용
- 관리(Management)의 편리성
- 보안(Security)성의 탁월함
- 품질보증(Qos)을 보장

또한, IPv6는 특유의 이동성으로 인하여 보다 진보된 모바일 IP를 지원함으로서 무선인터넷 기술에도 많은 영향을 미칠 것으로 전망된다. IPv6와 IPv4를 비교하여 보면 [표 3]과 같다.

[표 3] IPv4와 IPv6 비교

구 분	IPv4	IPv6
주소체계	32bit (예:143.248.142.172)	128bit (예:FEDC:0098:7654:3210:EDFC:BA98:9820:82A3)
주소개수	4.2*109	3.4*1038
할당방법	A,B,C,D 및 CIDR	CIDR
보 안 성	Ipsec 별도 설치	Ipsec 탑재
Header Field수	10	6
QoS	Not Used	Flow label, Traffic class
주소유형	Unicast Multicast Broadcast	Unicast Multicast Anycast
라우팅 기능	수동	자동

IPv4에서의 주요 개수는 32bit 인 42억개이며, 할당방법으로는 Class A, B, C로 나누어 배정함으로써 주요할당의 고갈이 예상되고 있다. IPv6는 128bit로서 거의 무한대로 주소를 할당할 수 있다. 보안성에 있어서 IPv4는 IPsec별도

로 설치를 하여야 만이 보안성 확보되는 반면에 IPv6는 프로그램이 탑재되어 있다. 특히 IPv6에서는 Header Field수를 IPv4의 10개에 비하여 6개로 단순화 시킴으로써 정보이외의 불필요한 Header를 줄였다. 또한, 주소 유형에 있어서 IPv6는 어떤 주소방법에도 관계가 없는 Any Cast를 도입하였으며, 구성방법에 있어서 자동적으로 실현되도록 하였다.

(2) IPv6의 특징

IPv6는 IPv4와 비교시 다음과 같은 특징을 가지고 있으므로 IPv6와 IPv4는 상당기간 네트워크상에서 서로 공존하면서 사용되어질 것으로 보인다.

(가) IP Address 확장

IPv6는 IPv4에서 32bit를 사용하던 것에 비해 대폭적으로 확장하여 128bit를 사용한다. IPv4는 A, B, C Class로 분류하여 관리하였던 관계로 Address 낭비가 심했던 점을 보완하였다.

IPv6 Address 유형은 다음과 같다.

- Uni-cast : 개인 Internet 사용자들이 이용
- Any-cast : 기업 전산망에 이용
- Multi-cast : ISP(Internet Serve Provider) 등에서 이용

(나) 이동 서비스 기능 지원

IPv4에서는 Transparency의 제약을 받아 매질의 변화가 생기면 서비스에 제약을 받는다. Mobile Internet 서비스에서 파일다운 로드시 셀 핸드오버가 생기면 IP 주소가 바뀌면 곧 연결이 끊어진다는 의미를 가진다. 이를 해결하기 위해서 IPv4 규격에서는 불가능하여 모바일 IP라는 새로운 개념을 도입하였으며 IPv6에서는 프로토콜 내에서 모바일 IP를 지원한다.

(다) 실시간 멀티 미디어 처리 기능

영상 데이터를 전송할 수 있는 광대역폭을 확보하였다. 고속 전송로와 저속 모뎀사이에도 두 어드레스간에 전송되는 패킷을 특수 처리하여 화상 회의나 인터넷폰 등을 사용할 때 무리없이 사용이 가능토록 지원한다. IPv4는 10개의 Field로 되어있던 Header 부분을 전체 길이는 그대로 두고 6으로 줄어들게 하여 효율성 향상하였다.

(라) IP 자체의 보안성 확대

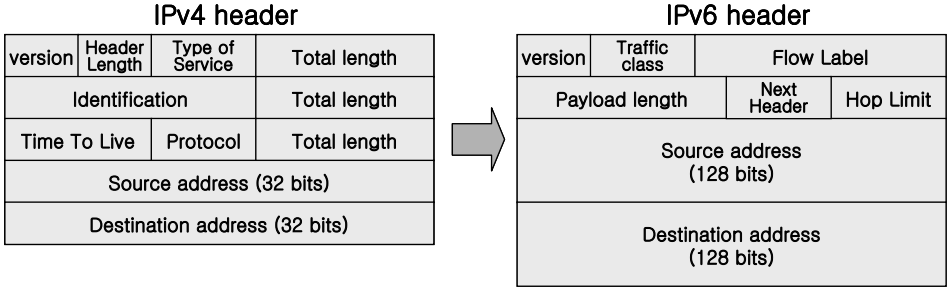
IPv4에서 보안기능을 첨가해 주는 IPsec(IP Security)이라는 프로토콜을 별도로 설치하였으나 IPv6에서는 프로토콜 내에 IPsec을 탑재해 보안 기능을 수행한다. 메시지 발신지 확인 인증 기능 및 수신자 외에는 메시지를 읽을 수 없게 하는 암호화기능을 지원한다.

(마) 라우팅 기능

ISP가 변경되는 경우 그 네트웍에 속한 모든 호스트들의 IP주소를 자동적으로 바꾸어 주는 서비스를 지원한다.

(3) Pv6 주소 할당

IPv4는 주소 할당 공간의 부족 및 주소 설정의 어려움이 있으며, ISP 변경시 사이트 주소 재할당의 문제가 발생되어 Network Layer 수준의 Security 대책이 미비한 설정이다. 이러한 문제점을 보안하여 적용한 IPv6과 기존의 IPv4 헤더는 [그림 10]과 같은 구조를 가진다.



[그림 10] IPv4와 IPv6의 헤더 구조

IPv4의 헤더에서 사용되는 Header Length, Identification, Flag & Flag offset, Header Checksum을 IPv6의 헤더 주요기능은 다음과 같다.

- Version : 4bit로서 6버전을 뜻한다.
- Traffic Class : 4bit로서 IPv4에는 없는 새로운 기능으로 VOD와 멀티미디어 정보의 실시간 전송에 이용되고 있다.

- Flow Label(흐름 레벨) : 24bit로서 IPv4에는 없는 새로운 기능으로 VOD와 멀티미디어 정보의 실시간 전송에 이용되고 있다.
- Pay Load Length : 16bit로서 IPv6 머리부를 제외한 패킷(사용자 데이터)의 길이를 나타낸다.
- Next Header : 8bit로서 IPv6 머리부에 이어 Header Type(머리형식)을 나타낸다. IPv4의 경우와 같은 값으로 되어있다.
- Hop Limit : 8bit로서 패킷의 라우터 중계기 수의 한계를 나타낸다. 1회 중계 될 때마다 1을 빼고, 0이 되면 그 패킷은 파기된다.

2) 패킷 교환망 기술

현재 무선인터넷을 지원하는 패킷 교환 망 기술로는 북미를 중심으로 하는 3GPP2의 3G Wireless Packet Network와 유럽의 3GPP를 중심으로 하는 GPRS(General Packet Radio System)로 나눌 수 있다. 현재 프로토콜상의 이동성 지원을 보면 3G Wireless Packet Network의 경우 모바일 IP를 이용하여 이동성을 제공하고, GPRS의 경우 일종의 이동성 지원 노드인 SGSN, GGSN 상에서 GTP를 이용하여 이동성 지원을 하고 있다.

3) 블루투스

가) 개요

블루투스(Bluetooth) 단거리 무선통신을 위한 기술 규격이다. 그러나, 단거리 무선통신 기술은 블루투스 외에도 몇 가지가 더 있기 때문에 간결하게 정의하면 이해하기 힘들 것이다. 좀더 구체적으로 설명하자면 블루투스는 작고(0.5 평방인치), 저렴한 가격(5달러), 그리고 적은 전력 소모(100Mw)로 휴대폰, 휴대폰의 PC 등과 같은 휴대장치들, 네트워크 액세스 포인트들, 기타 주변장치들 사이의 좁은 구역(10m～100m)내 무선 연결(Radio Link, 2.4GHz ISM Open Band)을 위한 하나의 기술적인 규격 사양이다.

블루투스가 탑재된 휴대용 PC를 사용자가 갖고 있다면 주변 10m～100m이내에 유선 망(POTS, ISDN, xDSL)이나 유선 LAN(10BaseT, 100BaseT, Wireline), 무선망(Cellular, PCS, Paging, Satellite)이나 무선 LAN(802.11, SWAP)등의 외부 통로만 있으면 언제든지 인터넷 접속이 가능하다. 물론 이메일도 가능하며, 자체 보안

기능(Key운영, Authentication, Encryption 등)을 가지고 있어 전자상거래와 같은 보안이 필요한 통신 매체로도 활용할 수 있다.

또한 휴대전화 사용의 경우 무선 귀걸이형 전화만 있으면 전화가 어디 있든 언제든지 통화할 수 있으며, 전화기 한 대로 사무실과 가정에서 부가적인 전화비용을 지불할 필요없이 무선 인터넷폰으로 전화를 사용할 수 있다. 일반전화(PSTN), 휴대전화(Cellular, PCS)까지 사용할 수 있어 전화 하나로 3가지 방법을 통해 전화를 쓰는 효과가 된다. 응용분야는 무궁무진하며 그동안 우리가 상상하지 못했던 아이디어도 블루투스를 통해 실현 가능해졌다.

이렇게 일반적인 인터페이스(UART, USB, PCM, PCMCIA등)를 제공하고 ISM Open Band로 연결시키는 저가, 소형, 저전력 소모의 블루투스가 모든 전자/전산 분야 개발자들의 관심을 받고 있는 것은 당연한 일이다.

나) 기능 및 특징

(1) 전송속도, 거리, 주파수

최대 데이터 전송 속도 1Mbps에 최대 전송 거리를 10m를 목표로 하고 있다. 1Mbps는 사용자가 라이센스없이 이용할 수 있는 2.4GHz의 ISM(Industrial Scientific Medical : 산업 및 의료용 주파수)주파수를 사용해 손쉽고 저렴한 비용으로 실현할 수 있는 전송 속도다. 옵션으로 출력 엠프가 있으면 100m까지 가능하다. 주파수 호핑 방식의 스펙트럼 확산 기술을 사용하는데 1MHz 폭의 채널을 79개 사용하여 초당 최대 1,600회까지 채널을 바꿀 수 있고 이와 같은 고속의 채널 스위칭은 다른 무선통신에 대한 간섭을 막는다.

또한 홉핑을 고속으로 처리하므로 캐리어 센스를 할 필요가 없다. 같은 주파수 대역으로 작동하는 다른 시스템들과 비교해 볼 때 블루투스는 더 빨리 호핑하며 더 짧은 패킷을 사용함으로써 다른 시스템보다 더 안정적으로 통신한다. 전송 거리 10m는 사무실 내에서 사용자가 휴대하고 있는 기기와 책상에 설치해 둔 PC간 전송 거리로 충분하다는 판단에 따른 결정이다.

(2) 전파의 송신 출력

블루투스의 동작 영역은 송수신 감도를 높이면 (+20dBm) 약 100m 정도까지 가능하지만 외부 전력 증폭기가 필요하기 때문에 일반적으로는 0dBm, 약 10m 정도이다. 즉, 10m 이내의 블루투스 송수신장치들은 별도의 케이블 연결

없이도 자동으로 연결되고, 데이터를 주고받을 수 있는 것이다. 또한 동작 거리에 맞게 자동으로 출력을 조절해 절전하는 기능도 있다.

(3) 피코넷, 스캐터넷

네트워크 토폴로지는 1:1과 1:n 연결을 지원한다. 블루투스를 통해 임의로 연결되는 장치들의 모임인 몇 개의 피코넷(Piconet)을 설정할 수 있고, 피코넷 사이를 연결할 수 있다. 각 피코넷은 다른 피코넷에 속하는 모든 사용자들은 이 호핑 시퀀스에 동기화 된다. 피코넷은 휴대용 PC와 이동전화처럼 두 개의 연결된 장치들로 시작되고 8개의 장치까지 확장할 수 있다. 피코넷은 주파수 호핑 패턴을 결정하는 마스터기와 최대 7개까지의 종속기들로 나뉘어진다. 피코넷 안의 어떠한 기기든 마스터기가 될 수 있다. 마스터기는 동시에 다른 피코넷의 종속기가 될 수 있다. 피코넷을 연결한 네트워크 형태를 스캐터넷(Scatternet)이라 한다. 스캐터넷은 2개 이상의 피코넷으로 구성되며 100개까지의 피코넷을 연결할 수 있다. 피코넷과 스캐터넷은 통신 관리 및 기기 상태를 제어하기 위해 8bit의 MAC(Media Access Control : 무선 LAN용 전용 기술) 어드레스를 사용한다.

현재 스마트 스캐터넷 등의 신기술이 개발되고 있다.

(4) 데이터 채널, 음성 채널

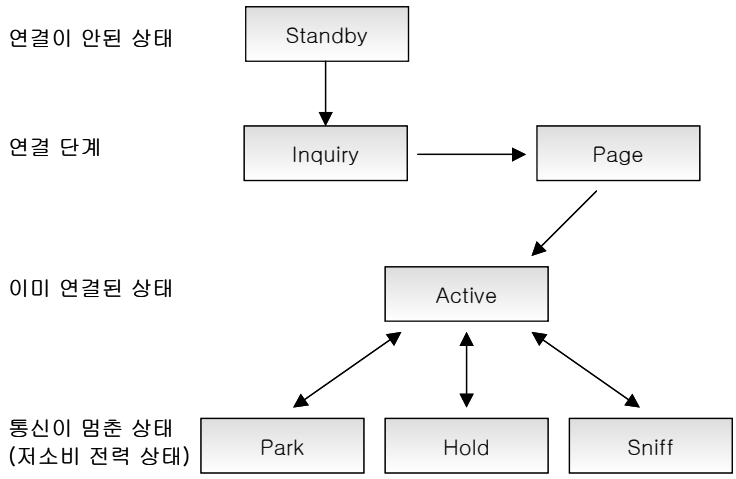
블루투스 시스템의 비동기적인 데이터 채널을 제공하거나 동시에 3개의 동기화 음성 채널을 제공하거나 또는 동시에 비동기적인 데이터와 동기적인 음성을 지원하는 1개의 채널을 제공할 수 있다. 각 음성 채널은 64Kbps의 동기화 링크를 지원하며 3개까지 동시에 확보할 수 있다. 비동기식 채널에서는 다운링크는 최대 721Kbps, 업링크는 57Kbps의 비동기식 링크를 제공하거나 대칭 전송시 432.6Kbps의 동기식 링크를 제공한다.

패킷 다중화 방식은 TDD(Time Division Duplex : 시분할 양방향 통신 방식)이다. 이 표준안은 회선 교환과 패킷 교환 방식을 모두 지원하고 비동기 전송을 하면서 64Kbps의 음성 채널을 최대 3개까지 동시에 확보할 수 있다.

(5) 전력 모드

블루투스 기기는 여러 통신 방식을 위한 전력 모드를 지원하고 있다. 모드

의 종류는 모두 7가지이다. 연결되지 않은 상태의 스탠바이(Standby) 모드, 조사(Inquiry) 모드, 페이지(Page) 모드, 활성(Active) 모드, 대기(Hold) 모드, 탐지(Sniff) 모드로 설정된다. 이러한 모드들은 소비 전력을 최소화하도록 구성되어 있다. 스탠바이 모드에서의 각 기기는 1초 정도마다 새로운 메시지를 체크한다. 기기가 서비스를 요청하기 시작하면 그 기기는 마스터가 되어 주변기기의 인식 작업을 시작한다.



[그림 11] 블루투스 소비전력 상태

(6) 데이터 교환 기능

블루투스 데이터 교환을 기본적인 기능으로 지원한다. 데이터 교환은 휴대폰에서 PDA로 명함을 전송하는 것처럼 간단할 수도 있고 동시에 PDA와 PC간 개인정보를 동기화시키는 것처럼 복잡할 수도 있다.

이러한 응용 분야뿐만 아니라 다른 데이터 교환까지도 규정하고 있다. 이 애플리케이션을 지원하기 위해 같은 상위 계층 프로토콜, 즉 OBEC(Object Exchange) 프로토콜을 사용한다. 장치 사이에 장애물이 있는 경우를 보면 전파의 특성상 어느 정도의 장애물을 관통하기 때문에 적외선에 비해 유리하다.

(7) 인증과 암호화

사용자 보호와 정보 보안을 위해 시스템은 쌍방환경에 적당한 보안 기능을 제공해야 한다. 즉, 블루투스에서 각 유닛은 인증과 보안 알고리즘을 같은 방식

으로 구현해야 한다. 기본적 수준의 보안이 정의되어 칩 구현에 적당하도록 될 것이고, 인증 알고리즘은 처리 기능에 있어서 장치에 무리가 가지 않는 수준에서 제공될 것이다. 암호화 알고리즘에 대한 앞으로의 지원 계획은 후방향 호환성(Backward Compatibility)을 지원할 것이다.

주요 보안 기능은 다음과 같다.

- Challenge response routine for authentication
- Stream cipher for encryption
- Session key generation-session keys can be changed at any time during connection

보안 알고리즘에서는 공용 개체인 블루투스 유닛 주소(Address), 비밀 개체인 개인 사용자 키(Private User Key), 불규칙 번호(Random Number)와 같은 세 개의 개체가 사용된다. 위에서 설명한 대로 블루투스 유닛 주소는 질의 절차를 통해 얻을 수 있다. 개인 사용자 키는 초기화 중에 유도되며 결코 공개되지 않는다. 그리고, 불규칙 번호는 블루투스 유닛의 의사 임의 처리(Pseudo-Random Process)를 통해 유도된다.

다) 블루투스 활용분야

(1) 활용분야

블루투스가 먼저 적용될 분야는 휴대폰 단말기, 휴대용 컴퓨터, 전자수첩 그리고 귀걸이형 폰, 네트워크 엑세스 포인트 등과 같은 주변 장치들이 될 것이다. 2002년까지 1억 개의 휴대폰에 내장 또는 장착될 것으로 예상되는 한편, 수백만 이상의 휴대용 컴퓨터, 휴대장치, 기타 다른 전자제품에 사용될 것으로 보인다. 향후에 블루투스가 탑재될 것으로 기대되는 장치는 이동전화, PDA, 휴대용 PC, 노트북, 디지털 카메라, 가정용 무선 전화기, 전화용 헤드폰 등 다양한데, 다음은 이들 장치들이 블루투스를 탑재함으로써 가능하게 되는 서비스에 대한 예상 분야이다.

- 인터넷 브리지로 쓸 수 있다.

  블루투스가 탑재된 노트북으로 이동시에는 가방 속의 이동전화에 연결해서, 사무실에서는 모뎀이나 LAN에 연결해 인터넷에 접근할 수 있다.

• 궁극적인 헤드셋(Headset)이 된다.

블루투스가 탑재된 헤드셋 착용시 선이 연결돼 있을 경우 생길 수 있는 행동의 제약이나 이동의 제약을 극복할 수 있다.

• 노트북을 가방에 넣어둔 채로 메일 착신 신호를 받거나 검색이 가능하다.

블루투스는 금속이 아닌 물체를 통과해 사용할 수 있으므로 노트북이 가방에 있는 상태에서 이동전화를 사용해 이메일을 수신할 수 있고, 착신 신호를 이동전화에 알릴 수 있으며, 이동전화를 통해 이메일을 검색할 수 있다.

• 자동 싱크로나이저

이동전화나 PDA가 PC와 근접하면 자동으로 자료의 동기화가 이뤄진다.

• 선 없는 PC

전원을 공급하는 선만 제외하고 현재 사용중인 PC에 있는 모든 선이 블루투스를 사용해 대체될 수 있다. PC에 키보드, 마우스, 프린터 등 주변 장치를 연결하기 위한 모든 선이 사라질 수 있다.

위와 같은 많은 응용 분야들에 대해 업체의 동향을 보면 많은 제조업체들이 블루투스를 지지하는 이유를 크게 세 그룹으로 나눌 수 있다. 첫 그룹은 웹브라우저 데이터와 이메일 데이터 등을 포함한 응용 분야에 대한 기존의 유선 인터페이스 대신에 무선 연결을 사용하려는 그룹이다. 두 번째 그룹은 MP3 플레이어와 PC간 또는 헤드셋과 휴대전화기간의 음성 및 영상 파일 데이터 비즈니스 관련 회사들이다. 세 번째 그룹은 제어 데이터와 암호화 키 등을 취급하는 그룹이다. 이 세 그룹 모두 데이터 통신량이 증가할 것이다. 따라서 휴대전화 서비스 사업자의 수익이 늘어날 것으로 기대된다.

블루투스 특징
FCC의 면허가 필요없이 무료로 사용할 수 있는 2.4GHz대 ISM(Industrial Scientific Medical) 대역의 주파수 사용
1Mbps 속도(실제 효과 속도 712Kbps)로 최대 10m내에서 각종 단말기들을 무선 접속해 사용할 수 있음
2.4GHz 대역에서 대역폭 1MHz의 채널을 79개 설정, 1초간에 1,600회 채널을 바꾸는 주파수 호핑 방식의 스펙트럼 확산 기술로 전파를 송수신
초당 1,600회의 매우 빠른 주파수 호핑 방식을 통해 잡음이 많은 무선 주파수에서도 성능이 고르게 유지될 수 있는 장점
사용되는 고성능 집적 회로 라디오 수신기가 극소형(9×9mm 마이크로 칩에 장착 가능)
소비 전력이 매우 적음 (대기 상태에서 0.3mA, 데이터 교환시 최대 30mA)
짧은 데이터 패킷을 사용할 뿐만 아니라 유연성이 좋은 패킷을 사용하기 때문에 접속시 접속률이 극대화될 수 있음

[그림 12] 블루투스 특징

(2) 블루투스의 문제점

가트너 그룹 산하 데이터퀘스트의 애널리스트들은 최근 “PC와 무선 관련 업계는 블루투스에 대해 보다 관심을 쓸 것”을 주장하고 나서 업계에 경종을 울리고 있다. 블루투스는 최고 기업들이 다수 참여해 개발 및 마케팅에 전력하고 있지만, 그 만큼 몇 가지 우려가 제기되고 있다. 분석가들은 업계에서 블루투스를 만병통치약으로 받아들일 수 있다는 점을 걱정하고 있다. 즉, 블루투스를 무선 인터넷 접속에서부터 LAN에 이르기까지 모든 것을 아우르는 솔루션으로 여길 수도 있다는 것이다.

애널리스트 데일 포드는 “업계가 극복해야할 중요한 문제 중 하나는 블루투스에 대해 균형감을 유지하고, 이를 모든 분야에 적용할 수 있는 솔루션으로 파악하지 않는 것”이라고 주장했다. PC 기술 연구자인 마틴 레이놀즈는 블루투스에 관해 언급하며 “보안상 심각한 약점이 있다”고 시사했다. 레이놀즈는 “블루투스 사양에 보안 사항이 포함돼 있긴 하지만 요구 사항은 아니며, 개발자들은 분명한 요구 사항이 아닌 경우 개발 작업에서 그것을 생략해버리는 경향이

있다"고 설명했다. 데이터퀘스트는 보안상의 결함만 제외하면 상이한 장비간에 동기화 기능을 제공하는 블루투스의 전망은 낙관적이라고 평가하고 있다.

업계 전문가들은 2001년경 블루투스 가능 장비는 휴대폰, 노트북, PDA 등 1억 대에 달할 것이며 성장 잠재력은 8억대에 이를 것으로 내다보고 있다. 또한 데이터퀘스트는 2004년이면 10억 대의 블루투스 장비들이 시장으로 쏟아져 나올 것이라 전망하고 있다.

라) 향후 전망

블루투스는 핸드폰에 탑재되는 것을 시작으로 사무용, 가정용 정보기기와 가전제품에 채택될 것으로 예상되며, 그 적용 속도가 행후 1~2년 안에 가속화될 전망이다. 특히 블루투스 인프라 구축에 가장 큰 영향을 주는 가격이 5달러 정도까지 낮아진다면 그 파급 효과를 더욱 클 것으로 기대를 모으고 있다. 이제 급속히 성장하기 시작한 블루투스를 이용한 사업 분야에 눈을 돌려야 할 때가 된 것이다.

무선인터넷과 IMT-2000과 함께 서비스되어 우리가 상상하는 많은 부분을 현실화 시켜줄 것으로 기대된다.

나. 브라우저 기술

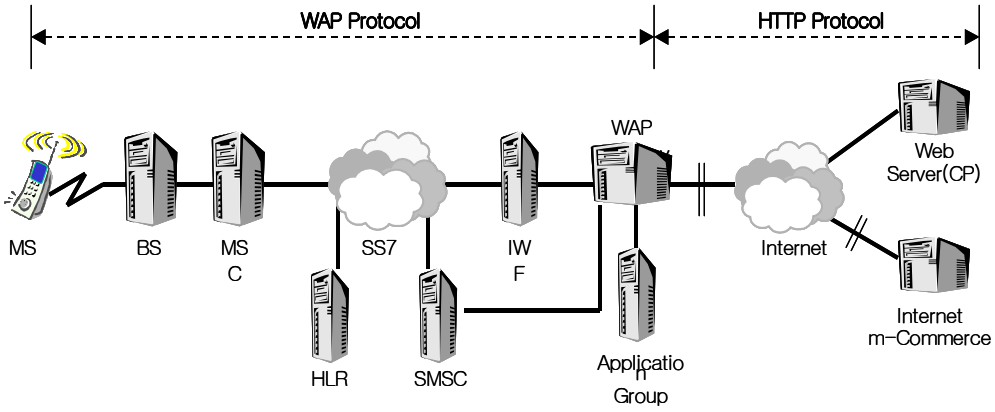
1) WAP

가) 개요

기존의 유선 인터넷에서는 많은 양의 데이터를 빠른 시간에 전송할 수 있지만, 무선 환경에서는 이러한 서비스가 어렵다. 특히 이미지나 동영상과 같은 경우에는 상당히 많은 양의 데이터 처리가 필요한데, 무선 환경에서는 이러한 대량 데이터 위주의 서비스를 제공하는데 무리가 있다. 또한 기존의 무선 데이터 서비스는 별도의 PC나 PDA 등을 이용해야 접속해야하는 불편한 점이 있다. WAP은 이와 같이 기존의 인터넷 프로토콜을 사용할 경우에 발생하는 문제들을 해결하고, 기존 인터넷 중심의 데이터 서비스를 무선환경에서 효율적으로 처리하기 위해 제안된 프로토콜이다. 국제적으로 WAP 정의를 위해 표준화 기구인 WAP포럼이 설립되어 표준화 작업이 진행되고 있다. WAP 포럼은 1997년에 Nokia, Motorola, Ericsson, Unwired Planet(현재의 Phone.com) 등 4개의 단말기 업체를 중심으로 구성되었으며, 현재 약 200여 개의 업체가 참여 중이다.

나) WAP 기술 분석

무선인터넷 단말기에 게이트웨이에 이르는 부분과 게이트웨이에서 CP(Content Provider)나 m-commerce 부분 등 여러 가지 인터넷 관련 서비스를 하는 웹서버 부분으로 나눌 수 있다. [그림 13]은 무선망에 대한 전체 구성도이다.



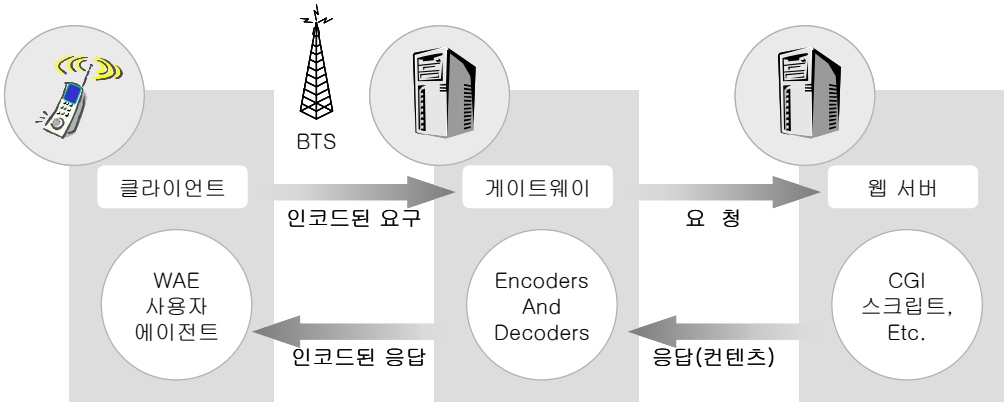
[그림 13] 무선 망 구성도

- MS(Mobile Station) : 단말기
- BS(Base Station) : 기지국/관리 장비
- MSC(Mobile Switching Center) : 교환기
- SS7(Signaling System 7) : 유/무선 망 프로토콜
- HLR(Home Location Register) : 홈 위치 등록기
- SMSC(Short Message Service Center) : 문자 메시지 시스템
- IWF(InterWorking Function) : 데이터 전송 장치
- WAP G/W(GateWay) : WAP 게이트웨이 서버
- Application Group : Billing, UMS(unified messaging system), PIM(Personal Interface Management)등 응용 소프트웨어
- Web Server (CP) : 외부 인터넷 컨텐츠 프로바이더
- m-Commerce : 방화벽 내에 있는 전자상거래 서버

(1) WAP의 구조

(가) WAP 프로그래밍 모델

WAP 프로그래밍 모델은 WWW 프로그래밍 모델과 유사하다. WAP 컨텐츠와 애플리케이션은 WWW 포맷을 기반으로 하여 이미 정의된 컨텐츠를 이용한다. 컨텐츠는 WWW 통신 프로토콜을 기반으로 하는 표준 통신 프로토콜을 사용해서 전송한다.



[그림 14] WAP 프로그래밍 모델

• WAP의 표준 콤포넌트

- Standard Naming Model : WWW 표준 URL은 Origin 서버에서 WAP 컨텐츠를 확인하기 위해서 사용한다.
- Content Typing : 모든 WAP 컨텐츠는 WWW 타입과 함께 특정한 컨텐츠 타입을 준다.
- Standard Content Formats : WAP 내용 형식들은 WWW 기술에 의거하고, Display Markup, Calendar Information, Electronic Business Card Objects, 그리고 이미지들과 스크립트 언어를 포함한다.
- Standard Communication Protocol : WAP 통신 프로토콜들은 네트워크 웹서버에 모바일 터미널 브라우저가 요청한 통신을 가능하게 한다.

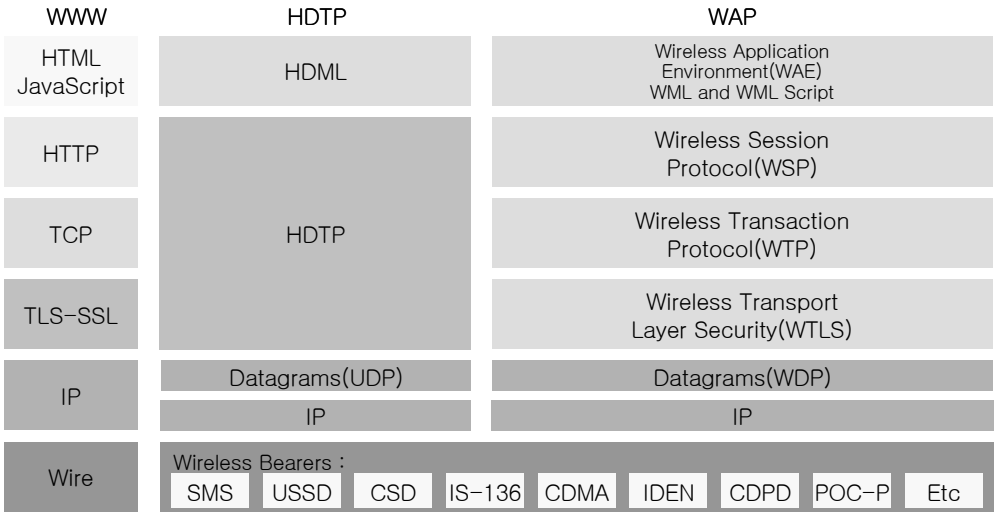
• WAP 프록시 기능

- 프로토콜 게이트웨이 : 프로토콜 게이트웨이는 WAP 프로토콜 스택(WSP, WTP, WTLS, WDP)을 WWW 프로토콜 스택(HTTP and TCP/IP)으로 변환한다.
- Content Encoders and Decoders : 컨텐츠 인코더는 네트워크에 맞게 자료를 줄인 WAP 컨텐츠를 변환한다. 이러한 구조는 이동 터미널을 통해 다양한 WAP 컨텐츠와 애플리케이션 개발자가 모바일 터미널에서 운영되는 컨텐츠 서비스와 애플리케이션을 만들 수 있게 해준다는 것을 의미한다. WAP 프록시는 컨텐츠와 애플리케이션으로 하여금 표준 WWW

서버에서 호스트의 역할을 할 수 있도록 해주며 또한, CGI 스크립팅과 같은 WWW 기술을 이용해서 개발할 수 있도록 해준다.

(나) WAP 구조와 콤포넌트(WAP Layer)

[그림 15]는 유선인터넷인 WWW과 폰닷컴에서 개발한 HDTP(Handheld Device Transport Protocol)와 WAP를 비교해 놓은 것이다.



[그림 15] WWW, HDTP, WAP 스택 비교

• WAE(Wireless Application Environment)

WAE는 WWW과 이동통신 기술의 조합을 기반으로 하는 애플리케이션 환경을 가진다. WAE 연구와 주요 목적은 오퍼레이터와 서비스 제공자로 하여금, 효과적이고 유용한 방법으로 다양한 다른 무선 플랫폼에 접근할 수 있게 해주는 애플리케이션과 서비스를 만들 수 있게 함으로서, 상호 운영 가능한 환경을 구축하는 것이다.

• WSP(Wireless Session Protocol)

HTTP 1.1에 상응하는 기능을 정의하고, 장시간 활용하는 세션을 정의하며, 세션 관리를 위한 Suspend/Resume 기능도 제공하고, 프로토콜 기능에 대한 협

상도 가능하게 한다. WSP는 WAP 프록시가 WSP클라이언트를 표준 HTTP 서버에 연결할 수 있도록 디자인되었다.

• WTP(Wireless Transaction Protocol)

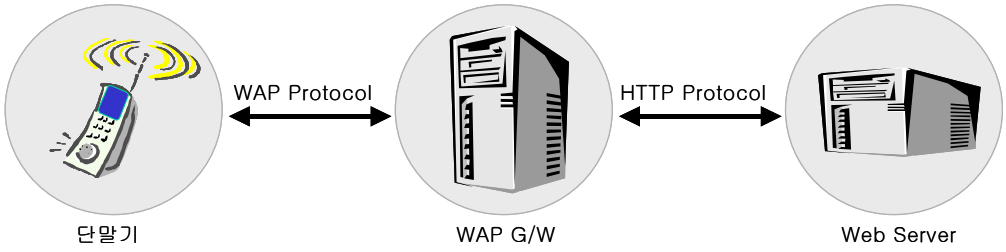
WTP는 데이터그램 서비스의 상위에서 동작하며 모바일 Station과 같은 Thin 클라이언트에서 실행하기에 적합한 작은 트랜잭션 형태의 데이터 전송 기능을 제공한다. 신뢰성 및 비신뢰성 전송 기능을 제공하고 오류 복구를 위한 재전송 기능도 담당한다.

• WTLS(Wireless Transport Layer Security)

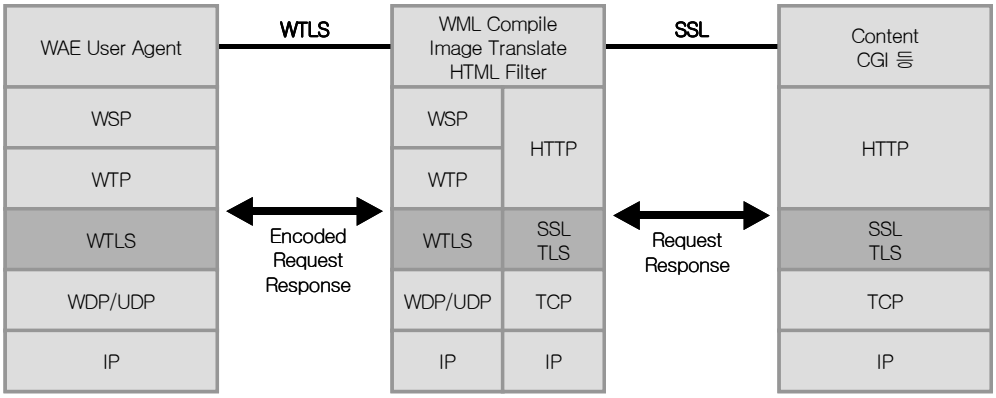
WTLS는 산업 표준인 TLS(Transport Layer Security) 프로토콜이며, SSL(Secure Socket Layer)로 알려진 프로토콜에 기반하는 보안 프로토콜이다. WTLS는 WAP 전송 프로토콜을 사용하며 좁은 통신 채널폭에 사용하도록 최적화되어 있다. 이것은 데이터의 기밀성, 무결성, 인증, 부인봉쇄 등의 보안 서비스를 제공한다.

• WDP(Wireless Datagram Protocol)

WDP는 WAP 구조에서 Transport Layer 프로토콜이다. WDP Layer는 다양한 네트워크 타입에 의해 지원되는 Data-Capable Bearer서비스로서 동작한다. 일반적인 전송 서비스로서 WDP는 WAP 상위 계층 프로토콜에 일관된 서비스를 제공하며, 이용 가능한 Bearer 서비스 중의 하나와 통신한다. End-to-End 전송을 위해 포트 어드레싱을 제공하고 인터넷의 UDF와 같은 전송 기능을 담당한다.



[그림 16] 단말기와 웹서버 사이의 프로토콜 변환



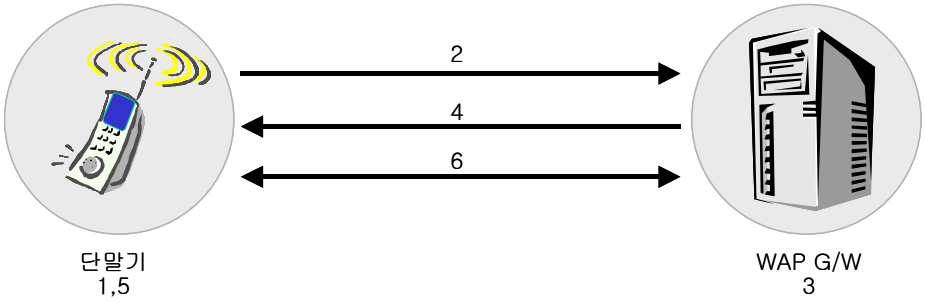
[그림 17] Communication between a Phone and The Internet

[표 4] SSL Component

Component	Domestic	Exportable
Key-exchange suites	RSA(up to 1024 bits)	RSA(up to 512 bits)
Bulk-encryption algorithms	3 DES(up to 192 bits) RC4(up to 128 bits) DES(up to 64 bits)	DES(up to 56 bits) RC4(up to 56 bits)
Message authentication Code(MAC) algorithms	MD 5 SHA-1	MD 5 SHA-1

(다) 보안

WAP은 WAP 클라이언트와 서버 사이에서의 연결 보안에 초점을 맞춘 유연한 보안 구조를 제공한다. WAP은 WAP 프로토콜 끝점 사이에서 End-to-End 보안을 제공할 수 있다. 만약 브라우저와 Origin 서버 사이에서 End-to-End 보안을 요구한다면 WAP 프로토콜을 사용해서 직접 통신해야 한다.



[그림 18] Key Exchange

• WAP 게이트웨이와 인터넷 사이의 통신

게이트웨이와 인터넷 사이의 통신은 Secure Port에서 보호된다. 클라이언트는 http:// 로 시작하는 URL 브라우징에 의해서 Secure Port에 접근하고, Secure Port는 넷스케이프에서 만든 산업 표준인 Secure Sockets Layer를 사용한다.

• WAP 게이트웨이와 단말기 사이의 통신

WAP 단말기는 대역폭의 제한 때문에 SSL을 사용할 수가 없다. 그 대신에 좀더 작고 경제적인 WAP이나 HDTP를 사용한다. 다음은, 단말기와 WAP 게이트웨이 사이에서 KEY exchange가 일어나는 과정을 순서대로 설명한 것이다.

- 단말기는 Diffie-Hellman 알고리즘을 써서 Public Key와 Private Key를 생성한다.
- 단말기는 Public Key를 게이트웨이로 보낸다.
- 게이트웨이는 단말기가 보내온 Public Key와 게이트웨이 자신의 Private Key를 이용하여 SSK를 만든다.
- 만들어진 자신의 Public Key를 단말기에 보낸다.
- 단말기는 게이트웨이의 Public Key와 단말기 자신의 Private Key를 이용하여 SSK를 만든다.
- 세션이 성립되어 단말기와 게이트웨이 사이의 통신은 보호된다. 만일 단말기의 SSK와 게이트웨이의 SSK가 같지 않다면 세션은 성립되지 않는다.
- SSK(Shared Secret Key)는 최초의 인증을 위한 것이며, 세션 생성을 위

한 Secret Key이다. 이것은 Diffie-Hellman(or RSA) 알고리즘을 이용하여 만든다.

• WAP 커뮤니케이션

WAP은 정보와 서비스를 무선 장치들에 전송하기 위한 규정이며, WAP Security의 한 부분인 WTLS 커뮤니케이션을 써서 통신한다. WAP WTLS는 게이트웨이 서버와 WAP 단말기 사이의 커뮤니케이션이 보호되는 방법을 정의한다. WTLS에 대한 내용은 WAP 포럼 웹사이트(http://www.wapforum.org)에서 볼 수 있다.

• HDTP 커뮤니케이션

HDTP는 WAP과 유사한 폰닷컴의 규정이다. 전화기와 게이트웨이 서버는 새로운 세션을 확립하기 위해 SSK를 사용한다. 세션 키는 세션을 맺고 있는 동안 암호화하고, 모든 커뮤니케이션을 해독하기 위해 사용된다.

(2) 게이트웨이

WAP 게이트웨이는 웹서버의 요청에 의해서 단말로 정보를 전송하는 기능과 이메일 도착, 주식 변경정보 등 자신의 취향에 맞는 정보를 등록하고, 그 데이터의 비밀 유지, 무결정성, 인증을 위한 기능을 한다. 또한 웹서버와 WAP 간의 프로토콜 변환을 위한 PPG(Push Proxy Gateway)의 역할을 하며 HTML을 단말기가 해독할 수 있는 HDML이나 WML로 변환하는 기능을 한다.

(3) WAP 응용 시스템

WAP에 대한 수요가 많아지고 그 서비스를 지원하는 업체가 많아지면서 게이트웨이의 기본 기능 이외에 여러 가지 부가적인 서비스들이 나타나기 시작했다. 그런 서비스들은 게이트웨이 이외에 특수한 기능을 하는 시스템을 더하여 다양한 서비스를 제공하게 된다.

지금 언급하고자 하는 서비스 및 시스템들은 폰닷컴에서 개발한 가입자 관리 및 자동 등록 시스템인 MMS, 무선인터넷 서비스와 전화통신 서비스를 결합한 WTA Service/server 및 게이트웨이의 E2E 보안 문제를 해결해줄 보안 WAP 게이트웨이이다.

(가) MMS

MMS(Mobile Management Server)는 폰닷컴에서 개발한 관리 도구로서 WAP용 무선 단말기를 사용하여 등록 관리가 가능하게 할 뿐만 아니라 WAP 솔루션(Gateway, Application, Handset)의 등록 기능들을 중앙화한다. 다시 말해서 MMS를 사용하게 되면 사용자는 인터넷을 처음 사용할 때 혹은 핸드폰을 처음 구입해서 따로 등록을 대리점에 하지 않고 그 핸드폰을 가지고 사용자가 직접 등록이 가능할 수 있게 되는 것이다.

MMS의 특징들을 살펴보면 개방형 표준을 기반으로 하므로 WAP 솔루션을 지원하기 위한 간단한 솔루션을 망 사업자에게 제공하며 음성과 데이터 변수, 둘 다 등록된다. 또한 단말기 등록시의 복잡함과 비용을 줄일 수 있다. 그리고 유연한 접속 구조로 기존)의 망과의 통합이 쉽고 셀프 서비스를 사용하면 고객 지원 비용을 줄일 수 있다.

(나) WTA 서비스

WAT(Wireless Telephony Application)는 WAP과 전화통신 서비스를 위한 애플리케이션 구조이며, 이때 WTA 서버가 이동 망 (호처리 부분)과 접속해서 호출 처리를 하기 위한 기본적인 동작을 제공해준다.

(다) 보안 WAP 게이트웨이

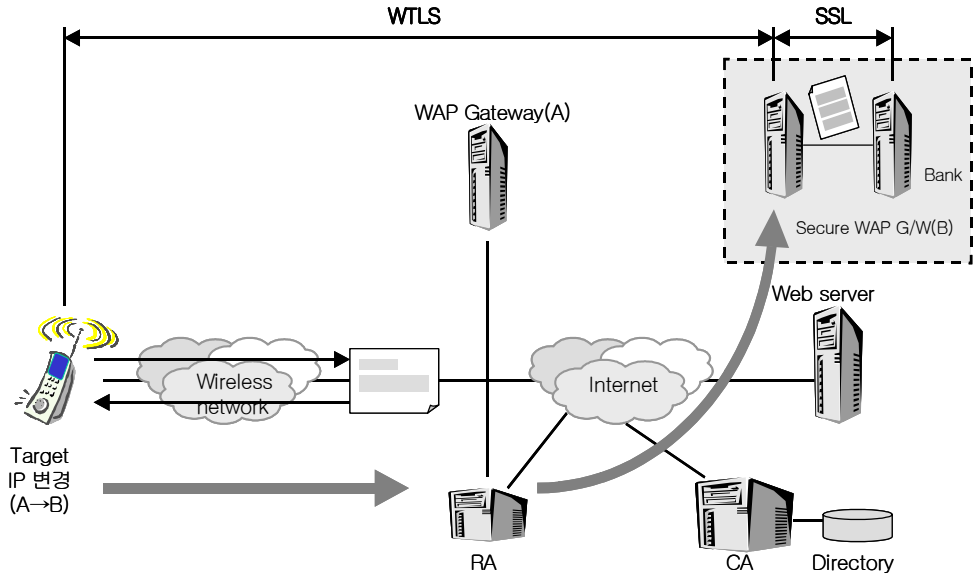
WAP 게이트웨이의 보안 측면의 단점(웹서버에서 휴대 단말기로 통신하는 경우 혹은 그 반대의 경우 게이트웨이에서 암호가 순간적으로 풀렸다가 다시 암호화한다)를 보완하기 위하여 특히 뱅킹 시스템 같은 극히 보안을 요구하는 시스템에서 사용하기 위하여 웹서버간의 설치하는 소규모의 게이트웨이를 말한다.

• CA(Certification Authority)

인증서가 아무리 안전한 장치라 하더라도 가명으로 인증서를 받는다면 아무 소용이 없다. 따라서 신뢰할만한 제3자 기관에서 인증서의 발급을 받아야한다. 이렇게 인증서 발급이 공인된 기관을 인증기관이라 하며 주업무는 인증서의 발행 및 폐기, 갱신, 대체 업무, 인증서의 폐기목록관리, 인증서 분배 및 디렉토리 서비스 등을 한다.

• RA(Registration Authority : 등록 대행 기관)

공인 인증서를 발급하기 위하여 인증기관을 대행하여 전자 서명법과 CA의 인증 업무 규칙에 따라 가입자 신원을 확인하고, 이에 수반되는 각종 인증 서비스를 대행하는 기관을 말한다. 고객에 대한 공인 인증서 신청, 접수, 본인 확인, 고객 관리 등의 인증기관의 업무를 대행하여 수행한다.



[그림 19] 보안 WAP 게이트웨이를 사용한 E2E security Network 구성도

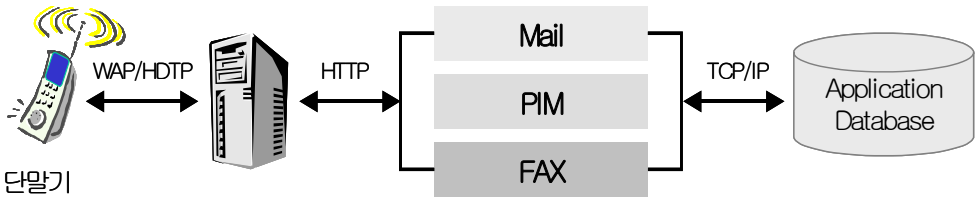
▪ 보안 WAP 게이트웨이 동작 원리

1. 가입자는 인터넷에 접속하기 위하여 게이트웨이에 접속한다. (WTLS를 사용한다.)
2. 게이트웨이는 URL을 검색하여 해당 웹서버로 전송한다.(SSL을 사용한다.)
3. 수신받은 보안 WAP 게이트웨이는 SSL 수신 거부와 새로운 주소로 송신하도록 요구한다.
4. 거부 요구를 받은 게이트웨이는 새로운 주소를 단말기로 전송한다.
5. 새로운 주소를 전송받은 단말기는 새로운 주소로 변경한다.
6. 새로운 주소로 WTLS통신을 한다.

(4) WAP 응용 서비스

WAP 응용 서비스의 분야는 기존의 유선 인터넷 분야와 마찬가지로 다양하다. 여러 응용프로그램과 솔루션 가운데, 단말기에서 제공하는 WAP 솔루션 중 기본적인 애플리케이션을 간단히 동작과 함께 소개한다. 이러한 서비스들은 일반적인 솔루션이기 때문에 망 사업자들은 기본적으로 선택하고 있는 응용 서비스이기도 하다.

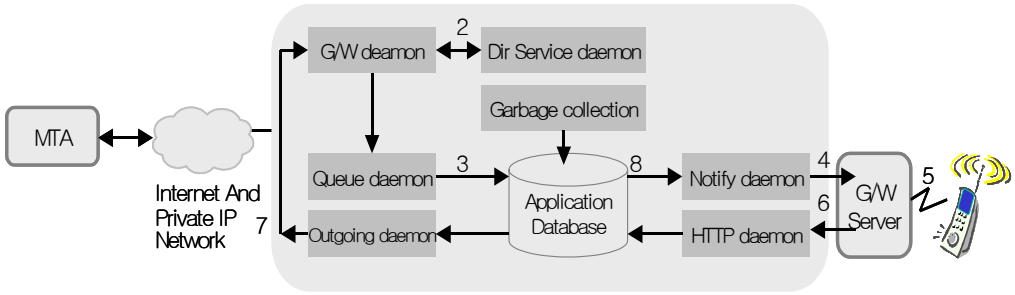
단말기는 WAP이나 HDTP를 이용하여 게이트웨이에 액세스하며 게이트웨이는 HTTP를 이용하여 애플리케이션에 요청하거나 재전송한다. 또한 애플리케이션은 TCP/IP를 이용하여 데이터베이스와 연락한다. 이때 게이트웨이는 단말기가 이해할 수 있는 WML이나 HDML로 변환하여 보낸다.



[그림 20] WAP 응용 서비스

(가) 메일 서비스

등록된 사용자는 메일 애플리케이션을 사용하여 자신의 단말기로 이메일 내용을 전송하고 받을 수 있다.

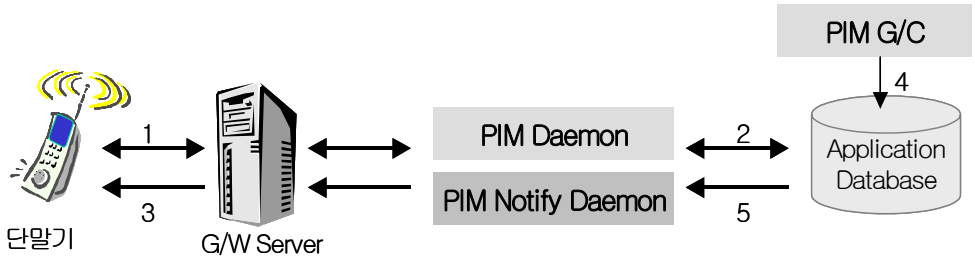


[그림 21] 메일 서비스 구성도

1. MAT(Mail Transfer Agent) 애플리케이션은 가입자를 가리키는 메시지를 받으며, 그 메시지를 Gateway Daemon으로 보낸다.
2. Gateway Daemon은 Directory Service Daemon으로 조회하여 가입자의 주소를 알아낸다.(만약, 찾지 못할 경우에도 메일은 송신자에게 메시지를 보낸다.) Directory Service Daemon은 이 메시지를 Query Daemon으로 보낸다.
3. Query Daemon은 애플리케이션 데이터베이스에 저장하고 송신자가 요구한 Delivery-time Processing을 실행한다.
4. Notification Daemon은 주기적으로 데이터베이스를 조회하며 새로운 메시지는 게이트웨이로 전송한다.
5. 게이트웨이는 가입자에게 새로운 메일을 전송한다. 만약 가입자가 회신을 한다면 단말기를 게이트웨이로 회신을 전송한다.
6. HTTP Daemon은 이 메시지를 수신하고 애플리케이션 데이터베이스에 저장한다.
7. Outgoing Daemon은 주기적으로 데이터베이스를 조회하고, 회신을 MTA 애플리케이션에 전송한다.
8. 만일, 가입자가 메시지 저장 유효 시간내에 메시지를 삭제하지 않았다면 Gabage-Collection Processor가 데이터베이스에서 메시지를 삭제한다.

(나) PIM 서비스

PIM(Personal Information Management)은 가입자가 단말기로 개인적인 주소록이나 달력, 스케줄링 등과 같은 서비스를 하게 해준다.

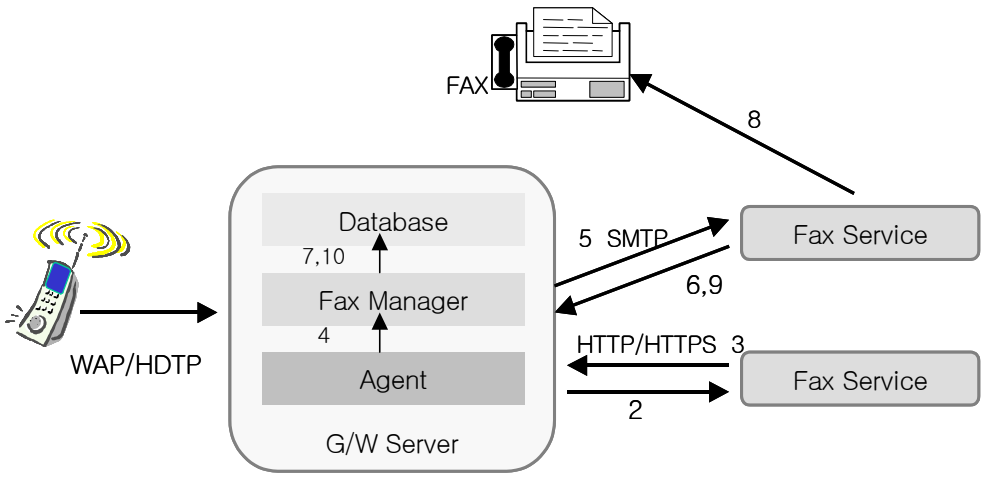


[그림 22] PIM 서비스 구성도

1. 단말기는 게이트웨이에 PIM 서비스를 요청한다.
2. Pim Daemon은 요청한 내용을 애플리케이션 데이터베이스에서 선택, 수정, 추가, 삭제한 후에 HDML/WML 데크를 생성해서 게이트웨이에 돌려보낸다.
3. 게이트웨이는 HDML/WML 데크를 컴파일해서 단말기에 돌려보낸다.
4. 만일 가입자가 정해진 시간 안에 데이터를 삭제하지 않으면 PIM G/C는 애플리케이션 데이터베이스에서 데이터를 삭제한다.
5. PIM Notify Daemon은 정기적으로 애플리케이션 데이터베이스에 질의하고 데이터베이스에 변화가 일어나면 가입자에게 통지한다.

(다) 팩스 서비스

팩스 매니저는 게이트웨이에 등록된 사용자를 대신하여 팩스를 전송한다. 팩스 매니저는 문서를 전송하고 팩스가 전송이 잘되었는지 감시하며 완료된 팩스의 정보를 수집한다.



[그림 23] 팩스 서비스 구성도

1. 단말기는 HDML이나 WML 애플리케이션을 동작시켜 팩스 요구를 생성시키며 생성된 요구는 WAP이나 HDTP를 사용하여 Agent로 전송한다(가입자는 팩스 번호를 미리 기입해두거나 화면에 표시되는 대로 입력한다.)
2. Agent는 HDML 또는 WML 애플리케이션으로 팩스 서버에게 팩스 내용을 요구한다.
3. 서버는 팩스 내용이 포함된 응답을 생성해 HTTP/HTTPS의 형태로 전송한다.
4. Agent는 팩스 내용을 팩스 매니저로 보낸다.
5. 팩스 매니저는 내용을 이메일 형식으로(SMTP) 팩스 서비스로 보낸다.
6. 팩스 서비스는 내용을 Queue에 저장하고 그 저장된 Queue를 가리키는 정보를 마찬가지인 이메일 형태로 팩스 매니저로 돌려보낸다.
7. 팩스 매니저는 게이트웨이 데이터베이스에 있는 팩스의 상태를 업데이트시킨다.
8. 팩스 서비스는 팩스를 송출한다. 만일 팩스 번호가 통화중이라면 정기적으로 재연결을 시도한다. 만약, 팩스를 전달하지 못했다면 실패 보고를 한다. 이 실패 보고에는 회선이 끊어졌거나 응답이 없거나 혹은 음성 회선이라는 등의 실패 정보가 들어가 있다.
9. 팩스 서비스는 팩스가 성공적으로 전송되었는지 아닌지를 알려주는 정보를 이메일의 형태로 전송한다.
10. 팩스 매니저는 게이트웨이 데이터베이스에 있는 팩스 상태를 갱신시킨다.

(5) WAP 및 무선인터넷 동향 및 발전 방향

(가) 국외 동향

각국의 WAP 동향을 [표 5]에 정리해 두었다.

[표 5] 국가별 WAP 동향

국가	동 향
유럽	• 2000년 초 대부분의 주요업체들이 WAP 지원 단말기 개발 • WAP은 WAP 포럼에서 개발되고 현재 텍스트 기반인 WAP 1.1에서 향후 멀티미디어 WAP 기술 개발 예정
미국	• 모토로라의 i1000 단말기 판매중 • WAP 기반의 무선 인터넷 서비스가 벨에틱모빌, 스프린트 PCS 사에서 99년 말부터 서비스 중 • 마이크로 소프트가 ME와 스팅거로 구성된 무선 인터넷 솔루션 제공
일본	• NTT-Docomo의 i-Mode의 독자 모델로 600만 가입자 확보

(나) 국내 동향

이동통신 5개 사업자의 무선 인터넷 프로토콜을 보면 SK텔레콤, 신세기통신, LG텔레콤은 WAP 솔루션을 사용하고 있고, 한국통신프리텔, 한국통신엠닷컴은 마이크로소프트 ME 솔루션을 사용한다. 독자 모델로는 국내 에이아이넷의 s-HTML(삼성의 애니웹 적용) 솔루션이 있다. [표 6]에서 국내의 망 사업자별 무선인터넷 서비스 현황을 확인할 수 있다.

[표 6] 망 사업자별 무선인터넷 서비스 현황

업체명	서비스명	웹브라우저 표준 방식	업체명
SK텔레콤	서비스명	서비스명	-이동전자상거래 개념 도입 -신세대를 위한 TTL 서비스를 강화 -m-Commerce를 위한 보안 솔루션을 개발중 중장년층이 많은 것을 고려 -전자상거래 초점
신세기통신	i-touch 017	WML	-데이터 서비스 전담하는 il사업단 신설 -이동형 포털 서비스 개념 도입 -폰닷컴으로부터 WAP 게이트웨이 구매 -무선커뮤니티 서비스 및 검색 기능 강화 모바일 포털 서비스에 초점
한국통신프리텔	i-touch 017	WML, 기타 수용	-모든 브라우저 표준 수용 가능한 솔루션 도입 (오라클 파나마서버) 정보서비스센터 설립 -우무선 통합 컨텐츠 500여종 확보
LG텔리콤	EZ-web	HDML	-100개 사이트 기반 서비스 제공중 폰닷컴으로부터 HDML 게이트웨이구입 WWML과 호환 가능 -모바일 전자상거래의 사용화
한국통신엠닷컴	Click018	WML,HTML	-삼성전자 단말기로 애니웹 서비스 실시 -WML, HTML 수용할 수 있는 별도 웹 서버 설치 -7개 메뉴와 24개의 서브 메뉴로 구성된 엔테인먼트 컨텐츠 중심 서비스

(다) WAP 발전 방향과 IMT-2000

① 주요 회사 동향

1999년 12월 마이크로소프트사는 에릭슨과 제휴하여 언제 어디서나 인터넷 접속이 가능한 이동전화 개발을 천명하였고, 폰닷컴은 한국 지사를 설립하여 국내에 진출하였다. SK텔레콤은 Wireless Data 게이트웨이를 개발하였고, 기존 HTML 문서 형식을 무선인터넷에 적합한 WML로 변환, 인터넷 정보를 이동전화로도 검색 가능하다.

② WAP 관련 사업자간 상호 협력 강화

제1회 WAP 2000 행사가 개최되어, WAP 표준화 강화, 인터넷 프로토콜, 기술 사항 표준화의 목적으로 SK텔레콤, LG텔레콤, STI 공동 운영 사무국 설치를 합의하였다. 이를 토대로 표준 경쟁시 주도권 확보와 CP에 대한 협상력을 강화할 수 있게 되었다.

③ 기술 진화 방향

기술의 진화 방향은 무선 데이터 전송 시스템 개발, 단말기의 컬러화, WAP의 버전 업으로 가고 있다. 웹과 MP3 기능을 간신 이동전화 단말기의 출시 및 업그레이드가 지속되고 있고, m-Contents, m-commerce 등 이동성이 보장된 통신 기반의 벤처 기술이 크게 확대될 전망이다. WAP의 경우 버전 향상과 국제 표준으로 지위가 한층 강화될 전망이고, 각 국가나 개발업체들의 채택 및 확산이 본격화 될 것이다. IMT-2000은 향후 서비스 차별성 부각에 힘이 모아질 것으로 보이고, 국내 이동통신 사업자들의 무선인터넷 사업은 향후 IMT-2000 사업의 연장선에서 판단되어야 한다.

(라) WAP의 미래

WAP 포럼이 제시하고 있는 표준안이 짧은 시간에 폭넓은 지지를 받아 사실상의 시장 표준으로 대두되고 있는 이유는 An Open Industry Established World Standard이고 XML과 IP를 포함한 인터넷 산업을 기반에 두고 있기 때문이다. 뿐만 아니라 기술 전반에 걸쳐 90%가 넘는 세계 시장을 대표하는 단말기 제조업체에 수용되었고, 100만 가입자를 대표하는 망 사업자들에 의해 적극적 지원이 존재하기 때문이다. WAP의 시장 지배력은 광범위하다. 그 후원 그룹으로 97년 에릭슨, 노키아, 모토로라, 폰닷컴 등이 주축이 되어 결성한 WAP 포럼의 멤버인 AT&T, 벨사우스 와이어리스데이터, IBM 등을 포함하여 전세계 200여 개가 넘는 업체들이 WAP 규격을 지원한다.

이와 같이 WAP 포럼에 참여하는 업체들이 세계 이동전화 가입자의 90%를 차지하고 있다는 점, 표준화 활동 및 관련 애플리케이션 개발이 가장 활발하게 이루어지고 있다는 점 등을 고려할 때 사실상 표준으로 자리잡았다고 할 수 있다. 현재 많은 무선 산업이 WAP 표준을 선택하고 있다. 그러나 WAP은 데이터량이 많지 않은 애플리케이션에 적합한 프로토콜로 폭넓은 무선 서비스 구축에 제약이 많고 HTTP등 기존의 인터넷 표준의 프로토콜을 사용하고 있지 않아 HTML과의 상호 교환성 및 화상 표시 지원 등의 문제점 및 다른 무선 프로토콜을 사용할 수 있

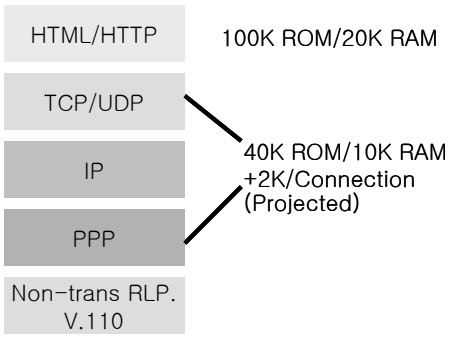
도록 개방형 아키택처도 수용해 확장성을 넓히는 유연성을 보완해야 할 점도 지적되고 있다.

2) ME

가) 마이크로소프트 모바일 익스플로러(MME) 1.0

마이크로소프트는 1999년 CDMA의 기반 기술을 소유하고 있는 퀄컴과 무선인터넷을 위해 Wireless Knowledge라는 조인트벤처를 만들었다. 이어 CDMA 환경에 적합한 무선인터넷 브라우저인 모바일 익스플로러 1.0을 WPAK(Wireless Product Adaptation Kit)이라는 이름으로 발표하고 한국통신엠닷컴, 한국통신프리텔과 기술 제휴를 통해 이를 국내 무선 단말기 제조업체가 수용하도록 하는데 성공하였다. 이들 통신 사업자들은 ME 사용자들을 위한 무선 통신 서비스를 제공하기 위해 마이크로소프트사의 유무선 인터넷 서비스 복합 포털 플랫폼인 MCIS/W를 채택 국내에서 처음으로 HTTP/HTML을 기반으로 한 무선인터넷 서비스를 시작했다. WPAK은 MME 1.0의 full source code를 포함하여 API Tools, Integration Tools, Phone Emulator, Documentation을 포함하고 있다.

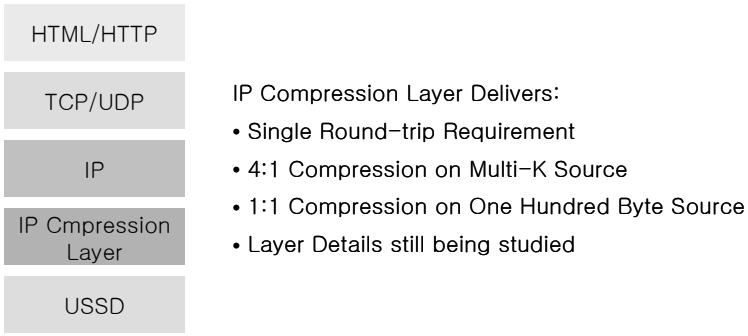
[그림 24]처럼 MME 1.0은 기본 HTML/HTTP를 이용하여 기존에 제작되어 있는 유선인터넷 컨텐츠를 쉽게 무선으로 쓸 수 있는 환경을 제공하였다. 이와 더불어 북마크, 쿠키, vCard, TelURL, Alerting 그리고 Forum를 유선 인터넷에서 사용하고 있는 것과 같은 방식으로 구현했다. MME 1.0에서는 구체적으로 다음과 같은 tag를 지원한다.



[그림 24] MME Stack for Version 1.0

(Circuit Switched)

이와 더불어 SMS와 같은 저속의 Connectionless를 위해 [그림 25]와 같은 IP Compression Layer를 개발하고 있다.



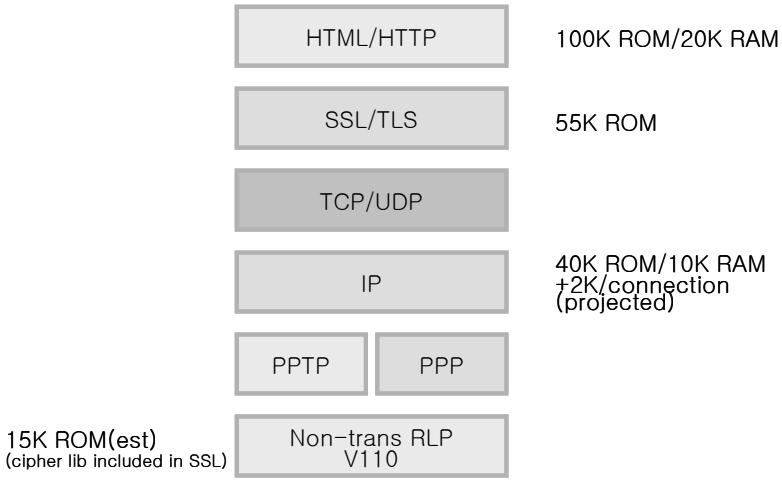
[그림 25] IP Compression Layer

나) 서비스 구축 및 데이터 센터

MME 1.0 사용자들은 자신의 무선 단말을 이용하여 인터넷 서비스를 받을 수 있을 뿐만 아니라 가정에 있는 자신의 컴퓨터를 통해 유선서비스를 이용할 수 있다. 유선과 무선에서 만들어지는 컨텐츠가 상호 경계 없이 구축되고 유선의 장점인 입력의 용이성과 서비스의 다양성이 무선 사용자들에게 컨텐츠의 풍부함을 가져다준다. 또한, 무선의 장점인 유동성과 즉시성 유선 사용자들에게 더 향상된 서비스를 제공할 수 있는 무선인터넷을 손쉽게 구축할 수 있다는 것이다.

다) MME의 발전 방향

MME의 다음 버전인 MME 2.0DMS 듀얼 모드를 지원한다. 따라서 사용자는 자신이 필요로 하는 애플리케이션이나 컨텐츠에 따라 HTML 브라우저나 WAP 브라우저를 선택해서 구동할 수 있다. 따라서 ME를 지원하는 단말 혹은 WAP를 지원하는 단말이라는 분류는 더 이상 의미가 없을 것 같다. [그림 26]은 MME 2.0에 들어가는 HTML/HTTP 부분을 설명한다.



[그림 26] Microbrowser Stack for Version 2.0(Circuit Switched)

MME 2.0은 SSL, XML/XSL, HTTP-NG, JPG/GIF, 2way SMS/USSD, HTML4.0(including image), Jscript, Binary Compression, HTTP-DAV, XML based PIM Contact Data, iCal mime을 지원함으로서 무선 단말과 유선인터넷 서비스 사이에 동기화를 보장한다.

기업 고객을 대상으로 하는 Wireless Knowledge 서비스와 윈도 2000에서 새롭게 선보인 Active Sync, 그리고 Exchange2000을 기반으로 다양한 무선 서비스를 제공하는 AirStream이 2000년에 발표될 예정이다. 유럽에서 각광 받고 있는 Sendit사를 인수하여 그 기본 플랫폼 위에 MCIS의 장점을 추가한 MICSA가 매우 중요한 차세대 플랫폼으로 주목받고 있다. 이들의 모든 장점을 취합하여 기업과 일반 고객과의 구분없이 구축될 MSN 모바일 서비스와 Exchange2000의 다음 버전인 Mercury가 매우 중요한 모바일 서비스 플랫폼으로 구축될 것이다.

다. 모바일 미들웨어 기술

1) JAVA 관련기술

무선인터넷 기술이 계속해서 발전함에 따라 WML, HTML 등의 마크업 언어 기반의 서비스를 벗어나 좀더 다채로운 서비스에 대한 요구가 늘어나기 시작했다. 그러기 위해서는 무선 단말기가 단순한 브라우저 이상의 기능을 수행할 수 있어야

만 한다. 또한, 컬러 액정의 등장, 멀티미디어 기능의 강화 등을 통해서 단순한 음성 통화를 위한 도구의 수준에서 벗어나 손위의 컴퓨터라고 할 수 있을 정도로 다양한 기능과 용도로 발전해 나가고 있는 무선 단말기들 보다 편리하고 통합된 애플리케이션 개발 환경을 요구하게 되었다.

자바는 이러한 무선 단말기의 개발 환경을 진일보하게 할 수 있는 최적의 기수이다. 플랫폼 독립성, 객체지향적이면서도 간결한 언어 구조 등의 장점으로 인해 이미 가장 경쟁력 있는 인터넷 기술로 인정받고 있는 자바는 차세대 무선인터넷을 위한 핵심 기술로서도 각광을 받고 있다. 그 이유는 자바 플랫폼이 무선 단말기에 탑재된다면 자바 애플리케이션을 무선망을 통해 동적으로 다운로드하여 설치하고 이를 통해 보다 역동적이고 향상된 무선인터넷 서비스가 가능해지기 때문이다.

자바는 프로그래밍 언어로서의 의미와 플랫폼 아키텍처로써의 두 가지 의미를 지니고 있으며 플랫폼 독립성이나 아키텍처 중립성이 뛰어나고 어떤 운영체제(Operating System)에도 이식이 가능하다. 다시 말해서 한번 작성되면 어떤 플랫폼이나 운영체제에서든 다시 작성하지 않고도 즉시 실행할 수 있는 WORA(Write Once, Run Anywhere)를 지원한다.

이런 특징이 가능한 이유는 자바 플랫폼(자바 가상 머신)이 어떤 플랫폼이나 운영체제에서도 실행할 수 있게 설계되었기 때문에 자바 가상 기계를 수행할 수 있는 플랫폼이면 어디서든 수행이 가능하다. 물론 썬마이크로시스템즈 사에서는 각각 다른 플랫폼에 맞는 자바 가상 머신을 개발하여 플랫폼에 딸 제공하고 있다. 언어라는 측면에서 자바는 C나 C++와 같은 문법적인 요소를 가지고 있다. 이는 자바가 하드웨어를 제어하려는 자바 개발 성격에 알맞은 언어인 C언어를 기반으로 만들어졌기 때문이다.

자바의 처음 개발 목적은 전자 제품이 업그레이드될 때마다 새로운 CPU, 새로운 아키텍처로 바뀌기 때문에 그 소프트웨어 업그레이드 비용을 절약하고 새롭게 재작성하는 번거로움을 없애기 위한 독립적이고 아키텍처 중립적인 언어와 플랫폼이 필요했기 때문이다. 그 이유로 자바는 태어나게 되었고 그러한 독립적이고 중립적인 성격이 웹의 성격과 맞아 떨어졌기 때문에 썬마이크로시스템즈에서 자바를 발표하자마자 엄청난 속도로 발전하게 되었다. 그 결과, 현재 어디서나 자바의 위력을 볼 수 있다. 그 당시의 웹 개발자들은 텍스트나 이미지 위주의 웹 문서에 자바 언어를 이용한 다양한 형태의 다이나믹한 웹 문서를 개발할 수 있다는 것만으로도 자바는 대단한 것이었다.

그러나 지금의 자바는 웹 문서나 애플리케이션 개발 이외에도 기업 환경에 맞는 EJB(Enterprise Java Beans)와 같은 컴포넌트를 비롯하여, 동영상 처리, 메일 기능, RMI(Remote Method Invocation)나 CORBA(Common Object Request Broker Architecture)을 이용한 분산 객체의 이용, Servlet이나 JSP(Java Server Page)을 이용한 웹 문서 개발, JDBC을 이용한 데이터 베이스 연동 등의 모든 분야에서 다양하게 사용되고 있다.

가) 자바 기반 무선 단말의 필요성

자바는 브라우저 기반의 무선인터넷 서비스에 새로운 활력소를 제공할 차세대 솔루션으로 주목받고 있다. 망 사업자와 단말기 제조업체를 중심으로 한 무선 시장의 주요 플레이어들이 자바를 선택하는 이유는 다음과 같다.

- 동적인 애플리케이션의 다운로드

  향후의 무선 애플리케이션과 서비스는 실시간으로, 동적으로, 그리고 안전하게 다운로드될 것이다. 자바는 실행 코드의 네트워크 이동성을 보장하는 가장 우수한 솔루션이다. 사용자는 자신의 단말기에 필요한 애플리케이션을 스스로 선택하고 설치할 수 있다.

- 크로스-플랫폼 호환성

  플랫폼간의 호환성은 차세대 모바일 솔루션의 기본 덕목이다. PDA, 셀룰러폰, 페이저 등의 단말기에 상관없이 사용자들은 동일한 애플리케이션을 원할 것이고, 만약, 각각의 플랫폼에 맞추어 애플리케이션을 재개발해야 한다면 이미 경쟁력을 상실한 것이다. 자바는 플랫폼 호환성에 관해서는 이미 충분한 강력한 경쟁력을 가지고 있다.

- 향상된 사용자 경험과 역동성

  기존의 브라우저 기반의 서비스는 유저 인터페이스에 근본적인 한계가 있다. 동적으로 다운로드된 자바 애플리케이션은 보다 향상된 그래픽과 더욱 빠른 응답 속도를 통해 사용자들의 만족도를 높여줄 것이다.

- 비연결성

  항상 네트워크에 연결되어 있을 수는 없다. 사용자는 지하 5층에서 장시간 머무를 수도 있다. 자바 애플리케이션을 사용함으로써 네트워크에 연결되지 않았을 때 작업한 내용을 네트워크에 연결이 가능한 상태에서 동기화하는 것이 가능해질 것이다.

• 보안 문제의 해결

아직 무선인터넷에서의 보안 문제는 완전히 해결되지 않고 있다. WAP과 MME, 그리고, i-Mode는 종단간 보안에 관한 완벽한 솔루션을 제시하지 못하고 있다. 그에 비해 자바는 이미 훌륭한 보안 모델을 가지고 있으며 무선 네트워크에서의 보안 문제도 해결할 수 있을 것이다.

나) 무선단말의 현황과 향후 전망

(1) 국내외 현황

CDLC/MDIP 전문가 그룹에는 에릭슨, 모토로라, NTT-Docomo, 팜 컴퓨팅, 샤프, 소니, 노키아, 삼성전자, 썬마이크로시스템즈, 심비안 등의 세계적인 무선 사업자 및 단말기 제조업체들이 멤버로 참가하고 있다. 그리고, 2000년 자바원 컨퍼런스에서는 모토로라의 iDEN, RIM의 블랙베리 등의 다양한 단말기에 CLDC/MDIP가 탑재되어 선을 보였다. 현재 자바 기반의 무선 단말 기술에서는 썬마이크로시스템즈와 함께 NTT-Docomo는 자사의 i-Mode 서비스를 위한 자바 기반 단말을 올 하반기에 상용화할 예정임을 발표한 바 있다. 그리고 모토로라의 경우, 향후 자사의 모든 단말기에 자바 플랫폼을 탑재할 것을 선언하였다.

국내의 경우 LG텔레콤이 이미 EZJava라는 이름의 CDMA 단말을 위한 자바 플랫폼의 개발을 완료한 상태이고, 올 하반기에 세계 최초로 상용화할 예정이다. LG텔레콤은 EZJava를 국내뿐만 아니라 영국의 브리티쉬 텔레콤에도 공급할 계획을 발표한 바 있다. SK텔레콤 역시 하반기에 자바 기반의 무선 단말을 상용화할 예정에 있고, 대부분의 단말기업체들도 자사 단말기에 자바를 탑재할 준비를 하고 있다. 비아이컨설팅, XCE, 대상정보기술, 이엑스이모바일 등의 국내의 벤처기업들도 자바 기반의 무선 단말 솔루션을 공급할 준비를 갖추고 있다.

(2) 향후 전망

무선인터넷 시장은 급격하게 성장하고 있다. 자바는 브라우저를 중심으로 한 마크업 언어 기반의 무선인터넷 서비스의 큰 발전에 기여하게 될 것이다.

2) 임베디드 시스템(Embedded Systems)

썬마이크로시스템즈의 2000년 5월의 자료를 보면 현재 셀룰러폰을 사용하는 사람은 약 3억 5천만 명에 달하며 2002년 말이나 2003년 초에는 약 10억 명에 도달할 것으로 보고 있다. 2000년 초 PC의 사용 인구가 3억 1천만 명 정도임을 미루어 볼 때 놀라운 수치라고 할 수 있다. 2002년도 하반기에는 대부분의 핸드폰 유저가 무선인터넷에 접속할 것으로 예상할 수 있으므로 엄청난 시장이 태동되고 있는 것이다.

임베디드 시스템으로는 무선통신 기술(Wireless Technology)의 중심에 서 있는 썬마이크로시스템즈의 KVM 기술과 여기에 비견되어지는 심비안(symbian)의 EPOC, 마이크로소프트의 Windows CE, 우리가 눈여겨 보아야 할 또 다른 세상인 JINI등을 말할 수 있다.

가) KVM

지난 2년 동안 썬마이크로시스템즈는 consumer and embedded 시장에서의 제품들을 지원하기 위해 자바 가상 머신(Java Virtual Machine) 기술을 소개하고 발전시켜 왔다. 스크린폰(Screen Phone), PDA 그리고 셋톱박스 등을 목표로 한 퍼스널자바와 스마트카드를 목표로 한 자바 카드가 그것이다. 그리고, 썬마이크로시스템즈는 이러한 기술들을 계속 발전시켜 나갔으며 디바이스의 가용 메모리 분류에 따라 Java VM의 종류를 구분을 하였으며, 가용 메모리가 128K 정도인 제품들을 겨냥한 새로운 기술이 K Virtual Machine(KVM)이다(여기서 K는 kilobyte를 나타낸다). Consumer and embedded 디바이스에서 휴대용, 동적인 다운로드, 그리고 보안 애플리케이션의 개발과 적절한 발전을 위해 modular, scalable한 아키텍처를 제공하기 위한 노력으로서 KVM은 발전되어 왔다.

제한된 자원을 가진 제품들을 위해 KVM은 다른 형태의 디바이스간의 기본적인 기능들을 이끌어 낼 수 있는 최소한의 Java VM과 Java API 구성을 제공한다. KVM은 16비트 또는 32비트 프로세서에 전체 메모리가 256K정도인 디바이스를 대상으로 하지만 디바이스 자체의 메모리 크기와 디바이스에 필요한 기능들을 충족하기 위해 유동적으로 적용될 수 있다. KVM은 썬마이크로시스템즈의 버추얼 머신 제품들이 제공하는 중요한 규칙들을 모두 포함하고 있으므로 기존의 Java VM의 장점들을 모두 가지고 있으며 메모리 자원에 제한이 있는 connected 디바이스(Cellular phones, Pagers, PDAs, Settop boxes, and Point Of Sale terminals)에 최적화되어 있으며, 다음과 같은 점에 중점을 두고 개발이 되었다.

- 작은 크기를 위해 최적화된다.
- 다른 플랫폼에 쉽게 포팅(porting)할 쉬 있어야 한다.
- 모듈과 확장성은 풋프린트의 증가 없이 가능한 '완전'하고 '빨라야' 한다.

나) 윈도 CE

윈도 CE는 새로운 32비트 디바이스를 가진 modular embedded 운영체제이다. 윈도 CE는 실시간 프로세싱(processing)을 지원할 뿐만 아니라, 이동하는 등 장소에 제약을 받는 장치에 내장하기 위한 목적으로 설계되었다. 'CE'가 무슨 뜻인지에 대해 마이크로소프트에서는 명확히 설명하고 있지 않지만 대게 'Consumer Electronics'의 약자라고 알려져 있다.

윈도 CE가 제공하는 대표적인 것은 다음과 같다.

- 윈도우 CE 기반 디바이스로부터 웹 데이터(Web data)를 핸들링 할 수 있는 경량의 HTTP 서버
- Windows Media technologies의 동화상 stream 및 DirectX 지원
- 개선된 실시간의 granular control of the scheduling of system 지원
- 진보된 실시가 애플리케이션 서비스(DCOM, COM, MSMQ, ActiveX, access SQL server)

윈도 CE는 여러 회사의 포켓용 컴퓨터에 사용되었으며, TCI를 위해 만들어진 케이블 TV셋톱박스의 한 일부로도 사용되었다. 마이크로소프트는 윈도를 사용하는 데스크탑 사용자들이 윈도 CE가 장착된 제품 등에서 익숙한 사용자 인터페이스를 발견하게 될 것이라고 주장한다. 포켓용 컴퓨터나 케이블 TV의 셋톱박스 외에도 윈도 CE는 운전 중에 사용하는 Auto PC의 운영체제로도 사용될 전망인데, 여기에는 마치 라디오 채널을 선택하는 것과 같은 마이크로소프트의 프로그램 제어 개념이 들어간다.

라. 무선 보안기술

무선 데이터 서비스, 즉 무선인터넷에 대한 수요가 증가하고 있는 가운데, 무선인터넷이 보다 활성화되기 위해서는 유선 인터넷에서 제공되는 것 같은 다양한 응용 서비스들이 개발되어야 할 것이다. 현재 인터넷에서 가장 주목받으며 활발하게 제공되고 있는 서비스는 전자상거래 서비스이며 이동통신 환경에서도 금융, 증권, 경매 등과

같은 전자상거래 관련 서비스가 주요 서비스 아이템으로 자리잡을 것으로 예상되고 있다.

그러나 무선인터넷에서 전자상거래를 비롯한 데이터 서비스가 성공적으로 제공되기 위해서는 반드시 해결해야 될 문제가 있는데, 보안 문제가 바로 그것이다. 보안 기술은 기존의 인터넷에서도 가장 중요한 요소 가운데 하나로 취급되고 있다. 특히 음성 위주의 이동통신에서는 도청만이 문제가 되었지만 증권이나 뱅킹같이 단순한 정보 서비스를 뛰어넘는 상거래 활동이 이루어지는 데이터 서비스에서는 사용자 인증, 데이터 무결성 보장 등 해결해야 할 문제가 많다. 이동통신에서의 보안은 무선 네트워크 환경을 충분히 고려하여 이루어져야 하며 또한 단순히 무선 네트워크에만 그치는 것이 아니라 유선인터넷과의 연동을 반드시 고려해야 한다.

1) 무선 보안의 종류

무선 데이터 서비스에 대한 중요성이 강조되고 있는 가운데, 여러 가지 다양한 무선인터넷 솔루션이 개발되고 있다. 이와 같은 무선인터넷 솔루션이 개발되고 있다. 이와 같은 무선인터넷 솔루션은 [표 7]과 같이 크게 2가지 부류로 구분할 수 있다.

첫째는 기존 유선 인터넷에서의 프로토콜인 HTTP에 기반해서 무선 데이터 서비스를 제공하는 경우이며, 다른 하나는 무선 네트워크 환경에 적합한 새로운 프로토콜을 개발하여 무선 데이터 서비스를 제공하는 방법이다. 현대 HTTP에 기반한 방식은 마이크로소프트사의 ME(Mobile Explorer)와 NTT-Docomo의 I-Mode 서비스가 대표적이며, 프로토콜을 새로 개발하는 방식으로는 WAP 포럼에서 개발을 주도하고 있는 WAP(Wireless Application Protocol)이 대표적이다.

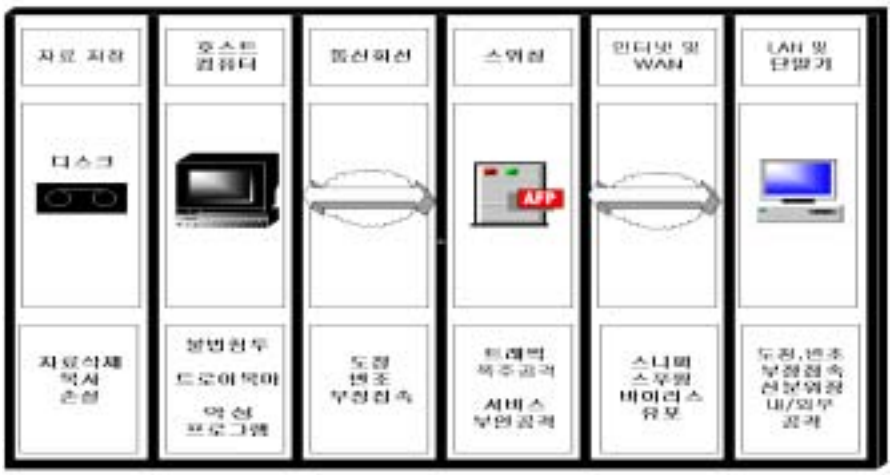
무선인터넷에서의 정보 보호 서비스는 무선인터넷이 어떤 프로토콜을 기반으로 해서 동작하는지에 따라 제공 형태가 달라진다. 즉 WAP과 같이 새로운 프로토콜을 정의하는 경우에는 이에 적합한 새로운 정보 보호 메커니즘이 개발되어야 하며, ME나 I-Mode와 같이 기존의 HTTP에 기반하는 경우에는 SSL(Secure Socket Layer)과 같은 유선인터넷에서 사용되고 있는 정보 보호 메커니즘의 수용이 가능하다.

[표 7] 주요 무선인터넷 솔루션

구분	WAP기반	HTTP기반	
		ME	i-Mode
개발 주도업체	WAP 포럼	Microsoft	NTT-Docomo
컨텐츠 기술 언어	WML	M-HTML	C-HTML
전송 프로토콜	WSP/WTP/WDP	HTTP	HTTP
단말기 브라우저	WAP 브라우저	Mobile Explorer	Compact NetFront
보안 매커니즘	WTLS	SSL	SSL

최근 들어 해킹, 바이러스 등의 사고가 급증하면서 일반인들의 보안 기술에 대한 관심도 증가하고 있다. 특히 인터넷을 통해서 쇼핑, 증권, 금융 업무 등 경제 문제와 직결되는 서비스의 제공이 늘어나면서 보안 기술의 중요성은 더욱 강조되고 있다.

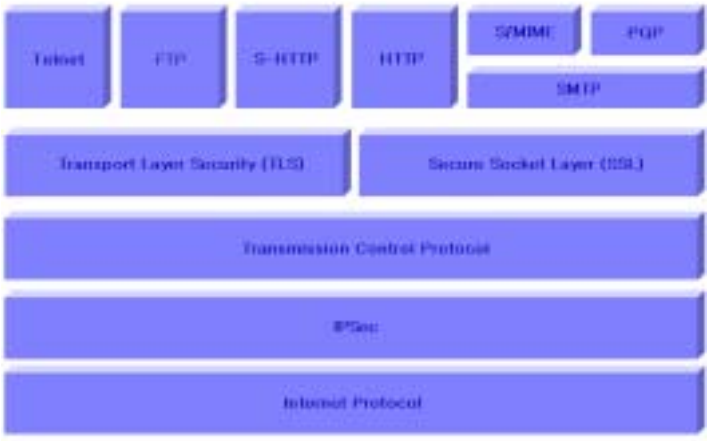
일반적으로 정보통신 시스템에 대한 위협 요소는 [그림 27]과 같이 분류할 수 있는데 이에 대응하는 보안 기술은 크게 2가지로 구분할 수 있다. 첫째는 시스템 보안이며, 다른 하나는 네트워크 보안이다. [그림 27]에서 호스트 컴퓨터나 단말기에 대한 불법 침투, 부정 접속, 신분 위장, 자료 삭제 및 손실 등의 공격에 대한 방어는 시스템 보안에 속한다. 즉 시스템 보안은 해킹, 바이러스와 같은 공격에 대해서 정보 보호 서비스를 제공하며, 주로 운영체제 보안과 관련이 있다. 또한 시스템 보안의 하나로 최근 많은 관심을 끌고 있는 침입 탐지 시스템(IDS; Intrusion Detection System)이 있다. 침입 탐지 시스템은 시스템이 네트워크에 대한 침입을 즉각적으로 탐지하고 대처할 수 있는 기술로 침입자에 대한 불법적인 사용을 탐지하고, 합법적인 사용자에 의한 오용이나 남용을 탐지하는 것이 목표이다. 시스템 보안에 대한 연구는 비교적 역사가 깊으며 다수의 시스템 보안 도구가 개발되어 있고, 정보 보호 시스템에 대한 평가 기준 및 평가 제도 또한 잘 정비되어 있다.



[그림 27] 정보통신 시스템에 대한 위협 요소

인터넷이 보편화되고 네트워크의 규모가 커짐에 따라 보다 강조되고 있는 네트워크 보안은 네트워크 상에서의 도청, 메시지 변조, 신분 위장 등의 공격에 대해서 정보 보호 서비스를 제공한다. 네트워크 보안을 통해 제공되는 정보 보호 서비스는 크게 다음과 같은 4가지가 있다.

- 기밀성(Confidentiality) : 네트워크를 통해 전송되는 데이터는 권한이 부여된 사람만이 내용을 볼 수 있어야 한다
- 사용자 인증(User Authentication) : 메시지를 작성한 사람의 신원을 확인할 수 있어야 한다
- 데이터 무결성(Data Integrity) : 전송된 데이터가 전송 도중에 변경되었는지 확인할 수 있어야 한다.
- 부인 봉쇄(Non-repudiation) : 송신자가 메시지를 송신한 사실을 부인하거나 수신자가 메시지 수신 사실을 부인할 수 없어야 한다.



[그림 28] 네트워크 보안 매커니즘

이러한 정보 보호 서비스는 하나의 메커니즘을 통해서 모두 제공될 수 없으며, 다양한 메커니즘에 의해서 제공되는 것이 일반적이다. [그림 28]은 인터넷의 기반인 TCP/IP에서 대표적인 네트워크 보안 메커니즘을 보여준다. 즉 IPsec은 IP 계층에서 정보 보호 서비스를 제공하며, TLS/SSL은 TCP 계층과 애플리케이션 계층 사이에 위치한다. S/MIME과 PGP는 이메일 보안 도구이며 S-HTTP는 애플리케이션 계층인 HTTP에 보안 서비스를 제공한다. 이밖에도 대표적인 네트워크 보안 메커니즘으로 침입 차단 시스템(Firewall)을 들 수 있다.

2) WAP에서의 보안

가) WAP 개요

WAP 방식은 사용자 및 참여 업체가 가장 많은 수를 차지하고 있다. 또한 공개된 표준이란 점에서 많은 연구와 응용이 개발 중에 있다. 따라서 세계적인 표준으로 자리잡기에 가장 유망한 프로토콜이다. 기술적으로 WAP 프로토콜은 기존의 기술과 호환성을 제공하고 응용 개발이 가능하기 때문에 많은 유연성을 갖는다. WAP 표준은 현재 2.0까지 발표되었으나, 현재 무선인터넷에 적용되고 있는 것은 WAP 1.x 기술이다. WAP 1.x는 무선망과 기존의 유선 인터넷망을 연동하기 위한 WAP 게이트웨이를 두고 있다. 사용자의 단말기와 게이트웨이는 WAP에서 정의된

프로토콜로 통신이 이루어지며, 게이트웨이와 기존 유선망과의 통신은 HTTP를 통하여 이루어진다.

나) WAP에서 제공하는 보안 표준 목록

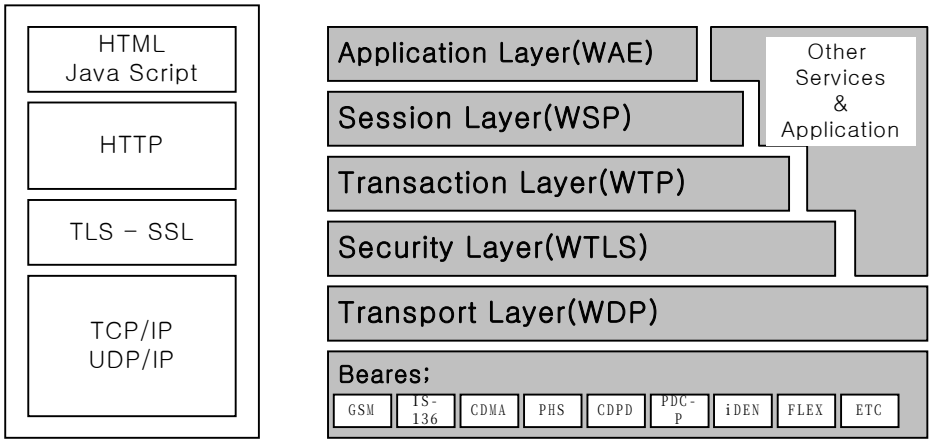
무선인터넷은 무선망과 인터넷 기술의 접목이다. 지금까지 무선망에서의 보안은 중요한 문제로 생각되어지지 않고 있다가 인터넷과의 접목에 따른 보안상의 취약점으로 인하여 다양한 보안 해결책을 WAP Spec에서도 제시되고 있다. WAP Spec에서 제시되고 있는 보안 관련 표준 목록은 [표 8]과 같다.

[표 8] WAP에서 제공하는 보안

표 준 목 록	주 요 내 용
Wireless Transport Layer Security (WTLS) Spec	클라이언트와 서버사이에 형성된채널의 안정성을 보장하는 전송계층 보안 프로토콜을 말하며, 유선 네트워크에서 SSL 또는 TLS와 같이 채널을 통과하는 정보에 대한 기밀성 및 무결성, 그리고 통신하는 클라이언트와 서버에 대한 상호 인증 기능을 제공.
WMLScript Crypto Lib Spec	사용자 메시지에 대한 전자서명 기능을 제공하여 트랜잭션에 대하여 부인방지 서비스가 가능하도록 하는 응용계층의 보안 프로토콜이며, 클라이언트와 서버의 메시지 교환에 의존하지 않고 전자 서명을 필요로 하는 응용인 경우에만 브라우저에 의하여 실행됨.
WAP Identity Module Spec	WAP에서 사용되는 인증서에 대한 안정성을 높이기 위하여 인증서를 보관하고 인증서에 대한 연산을 담당하는 모듈스펙.
Transport Layer E2E Security Spec	WAP이 가지고 있는 E2E 보안 서비스 부재의 문제점을 해결하기 위해 전송계층에서 클라이언트와 서버를 WTLS 보안 세션으로 연결하는 방법을 제시하고 있는 스펙.
WAP Public Key Infrastructure Definition	WAP에서 통신하는 개체의 인증을 위하여 사용자 인증서와 게이트웨이 인증서를 발급, 운영 및 관리하는 무선환경에 적합한 공개키 기반구조.
WAP Certificate and RL Profile Spec	무선 환경에 적합한 공개키 기반구조에서 사용되어지는 WAP인증서 및 인증서 취소목록에 관한 프로파일을 정의하고 있는 스펙.

다) WTLS (Wireless Transport Layer Security)

WAP포럼에서는 [그림 29]와 같이 TCP/IP 와는 별도의 무선환경에 적합한 프로토콜을 정의하였다. 이 가운데 보안 프로토콜이 WTLS(Wireless Transport Layer Security)이다. WTLS는 인터넷에서의 보안 메커니즘으로 잘 알려져 있는 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security)에 기반해서 작성되었다. WTLS는 통신을 하는 두 응용프로그램 사이에 안전한 채널을 형성하여 통신 내용의 보안을 보장하는 방법이다. WTP와 WDP사이에서 수행되기 때문에 특정 응용프로그램에 종속되지 않고, WAP을 사용하는 모든 응용프로그램을 지원한다. WTLS는 기밀성, 메시지 무결성, 사용자 인증의 보안서비스를 제공하지만 부인방지의 서비스는 제공하지 않는다.

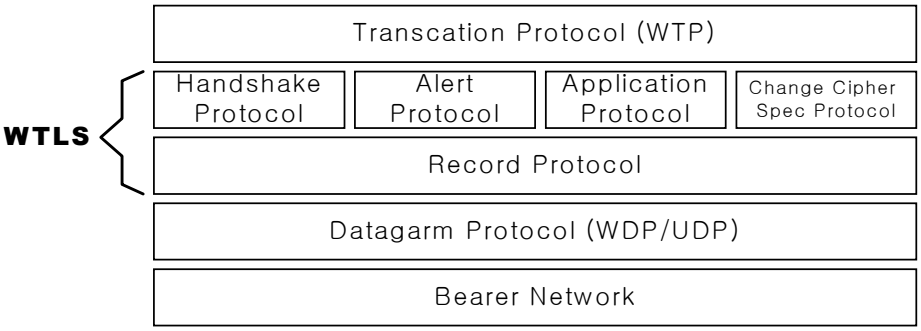


[그림 29] WAP 프로토콜 스택

라) WTLS의 구조

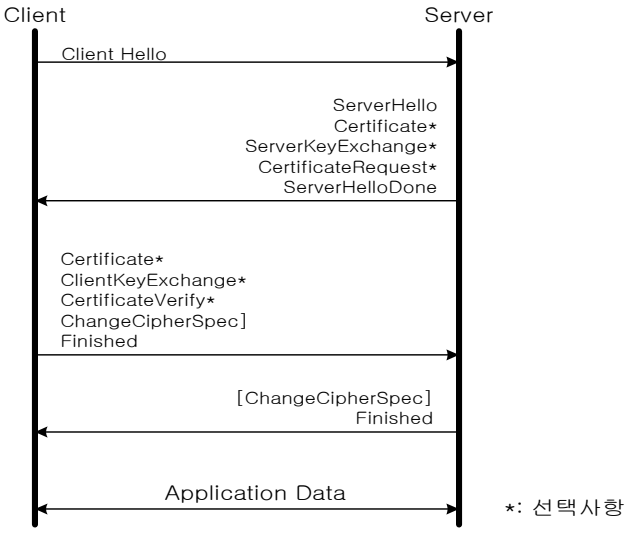
WTLS의 구조는 [그림 30]과 같다. Handshake 프로토콜, Alert 프로토콜, Cipher Spec 프로토콜은 WTLS의 동작에 대한 관리를 위해 사용되며 실질적인 보안 서비스는 Record 프로토콜에서 제공된다. 클라이언트와 서버가 WTLS를 통해서 연결을 할 경우 먼저 Handshake 프로토콜을 수행하여 한 세션 동안 보안 서비스 제공에 사용되는 키, 암호 알고리즘, 인증서 등과 같은 암호 매개변수를 서로 공유하게 된다. 여기에서 생성된 세션 정보는 Record 프로토콜에서 보안 서비스를 제공하는데 이용된다. Alert Protocol에서는 오류 메시지가 정의되며, 클라이언트나 서버에서 오류가 발생했을 때 오류 메시지를 보내서 오류가 발생한 사실을 상대방

에게 알리는 역할을 한다. Change Cipher Spec Protocol은 하나의 메시지로 구성되며, 이 메시지가 전송된 이후의 메시지는 새로운 보안 파라미터에 의해서 암호화되어 전송됨을 알리는 역할을 한다.



[그림 30] WTLS의 구조

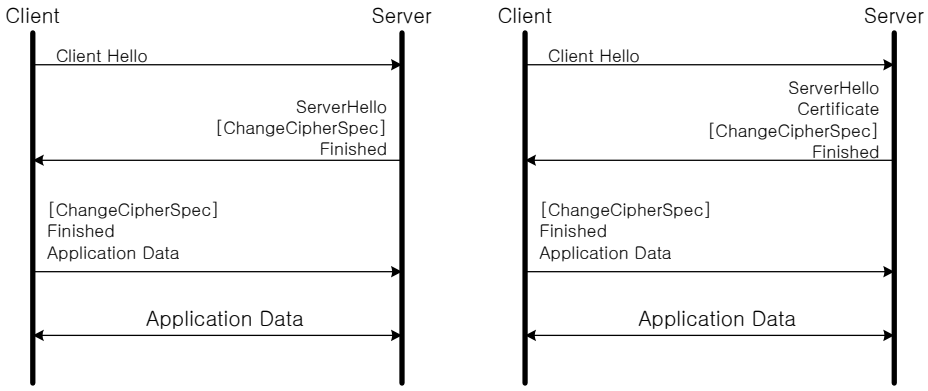
WAP의 WTLS의 Handshake 과정은 크게 Full Handshake, Abbreviated Handshake, Optimized Full Handshake등 3가지로 구분할 수 있다. 이 가운데 Full Handshake 와 Abbreviated Handshake는 SSL/TLS에서도 사용되는 방법으로 Full Handshake는 새로운 세션을 시작할 때 사용되는 것이며, Abbreviated Handshake는 기존의 세션을 재개해서 다시 이용할 경우에 사용된다. Full Handshake과정은 [그림 31]과 같다.



[그림 31] Full Handshake

Abbreviated Handshake에서는 [그림 32]와 같이 이전 세션 정보를 이용하여 세션을 시작하기 때문에 인증서 교환과 같은 서버와 클라이언트 인증을 위한 정보는 교환되지 않으며, 이전 세션에서 사용한 암호 매개변수로부터 새로운 세션에서 사용될 매개변수들을 생성한다.

끝으로 Optimized Full Handshake는 WTLS에서 새롭게 추가된 것으로 [그림 32]와 같이 서버는 클라이언트 인증을 위해 클라이언트의 인증서를 요청하지 않고, 서버 내에 보관하거나 저장소를 통해 제공되는 클라이언트 인증서를 통해 클라이언트 인증을 수행한다.



[그림 32] Abbreviated Handshake 및 Optimized Full Handshake

마) WTLS의 보안문제점

WTLS를 이용한 보안 솔루션이 가지고 갖고 있는 가장 커다란 문제는 종단간 보안(End-to-End)문제이다. 현재 WTLS를 이용한 보안 솔루션의 경우, [그림 33]과 같이 무선 네트워크에서는 WTLS를 이용해서 정보 보호 서비스를 제공하고, 유선 네트워크에서는 SSL/TLS를 통해서 정보 보호 서비스를 제공하게 되는데, 이때 종단간 보안 문제가 발생한다.

[그림 33] WAP 보안구조

이러한 보안서비스를 운영할 경우에 WAP 게이트웨이는 WTLS로 보호되는 데이터를 SSL에 적합하게 변환하거나 SSL로 보호되는 데이터를 WTLS에 적합하게 변환하는 역할을 수행한다. 이처럼 WAP 게이트웨이는 WTLS나 SSL로 보호되는 데이터를 복호화 하는 작업을 수행해야 하며 이 과정에서 본래의 데이터(평문)의 내용을 알 수 있다. 이러한 경우 WAP 게이트웨이 관리자가 불법적으로 사용자의 정보를 사용할 수 있기 때문에 큰 문제가 된다.

무선인터넷 서비스가 증권, 금융과 같은 전자상거래 응용 분야에 적용되기 위해서는 이와 같은 종단간 보안 문제가 반드시 해결되어야 한다. 현재 종단간 보안 서비스를 제공할 수 있는 방안은 SSL이용, Secure WAP 게이트이용, 응용프로그램 이용등의 3가지 방안이 있다.

3) ME에서의 보안

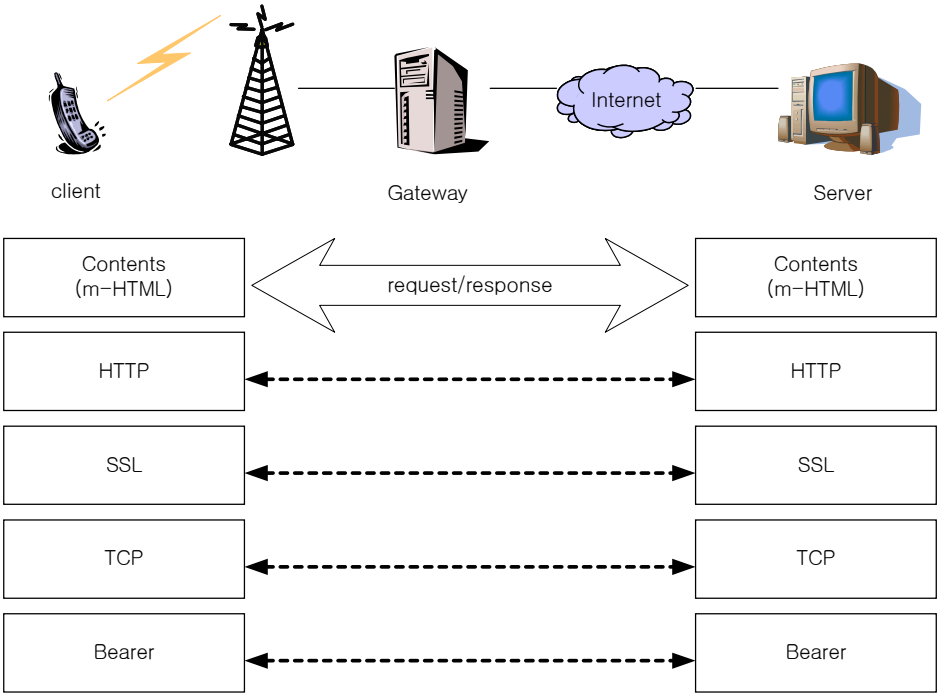
가) ME 개요

마이크로소프트는 WAP포럼에도 참여하고 있으면서 WAP 방식이 가지는 단점을 다른 차원에서 해결하기 위하여 ME 방식을 제안하고 BT(British Telecom), AT&T, 퀄컴 등과 연합하여 무선인터넷 시장을 장악하기 위하여 노력하고 있다. WAP과 W3C에 대응하여 마이크로소프트는 CDMA관련 원천 기술을 보유하고 있는 퀄컴과의 제휴를 통해 와이어리스날리지라는 합작회사를 설립하여 무선 인터넷 사업을 강화하였다.

와이어리스날리지는 휴대폰에서 인터넷을 검색할 수 있도록 윈도CE를 근간으로 한 이동통신용 웹브라우저인 ME(Mobile Explorer)를 개발하였다. ME에서는 WAP게이트웨이가 할 일을 무선 단말기 내의 브라우저가 하도록 하고 있다. 내부적으로 기존의 HTTP방식과 호환이 되도록 하고 있으며 HTML을 축약한 m-HTML(Mobile HTML)을 사용한다.

ME에서는 OS에 무관한 브라우저를 제공하고 게이트웨이를 이용하지 않으며 M-HTML을 기본언어로 하고 있으므로 이에 의하여 이동통신 사업자에게는 투자비 절감이라는 장점을 제공하면서 기존의 HTM 컨텐츠를 그대로 이용할 수 있다는 점에서 컨텐츠 제공업자에게 편의를 제공하고 있다. 동시에 브라우저의 오버헤드가 크다는 단점이 있으며 공개되지 않는다는 점에서 브라우저에서 지원하지 않는 파일을 이용한 서비스를 제공하지 못하는 단점도 가진다. ME는 게이트웨이의

구현이 필요없다는 점과 기존의 HTML 컨텐츠의 사용이 가능하다는 점에서 WAP의 단점을 극복하려 하고 있다. ME에서의 무선인터넷 접속방식은 [그림 34]와 같다.



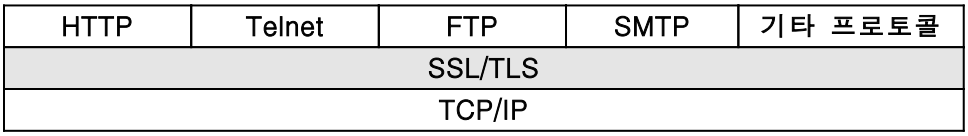
[그림 34] Mobile Explorer를 통한 무선인터넷 접속방식

나) SSL 프로토콜

WWW의 사용량이 증가하고, 이를 상업적으로 이용하려는 시도가 계속되면서 안전한 WWW 통신은 인터넷 정보보호 기술 가운데에서도 가장 중요한 부분의 하나로 받아들여진다. WWW 보안 메커니즘 가운데 가장 대표적인 것은 SSL 및 TLS이다. SSL/TLS는 WWW통신을 할 때, 서버와 클라이언트 사이에 암호화된 채널을 형성함으로써 통신 보안을 구축하는 방법이다.

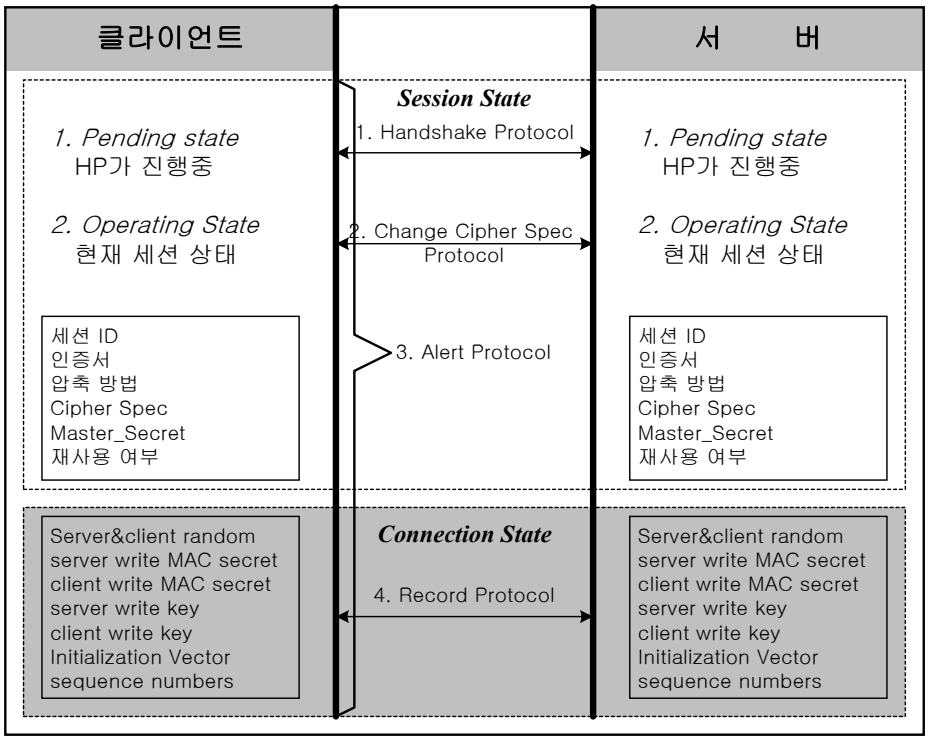
SSL은 웹 브라우저 개발로 이미 잘 알려져 있는 Netscape 사에서 1994년에 제안하였으며, 자사의 웹 어플리케이션에 처음으로 구현함으로써 현재 웹 보안의 대명사로 알려져 있는 보안 프로토콜이다. 현재 버전 3.0까지 개발되어 있는 상태이며, Netscape, Internet Explorer와 같은 브라우저에서 널리 사용되고 있다. TLS는

SSL 과 동일한 역할을 하는 보안 메커니즘으로 SSL 3.0에 기반하여 설계되었으며, 현재 인터넷 표준화 기구인 IETF(Internet Engineering Task Force)에서 이에 대한 표준화 작업을 진행 중이다.



[그림 35] SSL 보안 프로토콜

앞에서도 언급한 바와 같이 SSL/TLS은 네트웍(인터넷) 환경에서 통신을 하는 두 응용 프로그램 사이에 안전한 채널을 형성하여 통신 내용의 보안성을 지켜주는 방법이다. [그림 35]와 같이 응용 프로그램과 TCP 사이에서 수행되기 때문에 특정 응용 프로그램에 종속되지 않고, TCP/IP를 사용하는 모든 응용 프로그램들을 지원해 줄 수 있다. SSL은 다음과 같이 기밀성, 사용자 인증, 메시지 무결성 등의 보안 서비스를 제공하며, 부인 봉쇄는 제공하지 않는다.



[그림 36] SSL/TLS Handshake 과정

[그림 36]은 SSL 프로토콜의 전체적인 흐름을 나타내고 있다. 이것은 크게 보안 서비스 제공에 필요한 세션을 생성하는 단계인 “Session State″와 이 세션 정보를 이용해 클라이언트와 서버가 메시지를 주고받는 ”Connection State″로 구분할 수 있다.

SSL이 구현된 클라이언트가 서버에 연결을 시도하는 시점에서 “Session State″가 시작되는데, 세션 정보는 Handshake Protocol이 진행중인 상태인 ”Pending State″와 Handshake Protocol이 완료되는 시점에서 Change Cipher Spec Protocol을 통해 세션 생성이 이루어지는 “Operating State″ 단계를 거쳐 생성된다. 이러한 세션 정보는 세션 ID, 상대방의 인증서, 압축 방법, 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 클라이언트와 서버가 메시지를 주고받는 Record Protocol에서 보안 서비스를 제공하는데 이용된다. 즉. Cipher Spec에 정의된 암호 알고리즘을 이용해 메시지의 기밀성과 무결성을 제공하고, 이때 사용되는 키는 Master_Secret을 이용해 생성된다. 이렇게 생성된 키와 Server&Client Random, 주고받는 메시지의 순서번호 등은 세션 정보와는 별도로 클라이언트와 서버가 연결을 설정한 후 메시지를 주고받는 “Connection State″에서 유지된다. 이때 연결이 종료되면 이러한 정보는 소멸된다.

“SSL Alert Protocol″은 ″SSL Handshake Protocol″, ″SSL Change Cipher Spec Protocol″, ″SSL Record Protocol″등이 수행중일 때 발생하는 모든 오류 메시지를 처리하는 프로토콜이다.

다) ME 보안 프로토콜

ME나 i-mode와 같이 HTTP를 기반으로 하는 무선 인터넷 솔루션에서 정보보호 서비스를 제공하기 위해서 가장 간단한 방법은 [그림 37]과 같이 SSL을 이용하는 것이다.

[그림 37] 무선 인터넷에서의 SSL

이 경우, 게이트웨이는 무선 네트웍 구간과 유선 네트웍 구간의 중계 역할만을 담당하며, 클라이언트와 웹 서버의 통신에 개입하지 않는다. 따라서 클라이언트와 웹 서버간의 종단간 보안(End to End Security)이 가능하며, 클라이언트와 웹 서버는 기존 유선 인터넷에서의 경우와 동일하게 SSL을 통한 정보보호 서비스를 제공받을 수 있다.

또한 정보보호 서비스를 위해서 웹 서버의 특별한 수정이 필요하지 않기 때문에 기존에 구축되어 있는 시스템을 그대로 사용할 수 있다는 장점이 있다. 이와 같은 서비스를 제공하기 위해서는 클라이언트에서 SSL의 처리가 가능해야 하는데, 현재 단말기의 CPU나 메모리 용량으로는 유선환경의 PC에서와 같이 비교적 빠른 속도로 SSL을 처리하는 것은 불가능하다. 특히 많은 양의 연산을 필요로 하는 공개키쌍 생성이나 인증서 관리 등의 처리는 매우 곤란하다고 할 수 있다. 따라서 무선 인터넷에서 SSL을 원활하게 운영하기 위해서는 단말기에서 SSL을 효율적으로 처리할 수 있는 기술 개발이 선행되어야 한다.

4) 무선 PKI

가) 무선PKI 개요

현재 유선 PKI와 CA의 인증서(X.509)를 그대로 사용하는 것은 무선환경의 특성상 부적합하다. 그 이유는 무선 클라이언트 장비들은 유선 장비와 비교해 통신 대역폭, CPU와 메모리 리소스, Battery의 수명, 사용자 인터페이스 등에서 많은 차이가 있다. 따라서 이와 같은 특성을 고려하여 무선보안을 구현하여야 한다.

공개키 기반구조는 무선 인터넷에서도 정보보호 서비스를 제공하기 위한 기반 역할을 한다. 기존 인터넷과의 원활한 연동을 위해서는 무선 인터넷에서의 공개키

기반구조가 정의되어야 하며, 이는 유선 인터넷에서의 공개키 기반구조와 원활한 연동이 이루어져야 한다. 또한 무선통신 환경에서의 대역폭, 단말기 등의 제한을 고려한 인증서 프로파일, 암호 알고리즘, 키 크기, 인증서 취소여부 확인 메카니즘 등의 선택이 이루어져야 할 것이다. 이와 관련하여 WAP Forum에서는 X.509에 기반한 WTLS 인증서를 정의하는 작업이 진행중이며, ANSI에서는 X.509와는 별도의 인증서를 정의하는 작업이 진행중이다.

나) PKI와 무선 PKI

유·무선 공개키 기반 구조의 가장 확실한 차이점은 인증서 검증과정에 있다. 일반적으로 PKI기반의 공개키 암호 시스템 사용에 있어 클라이언트가 갖는 가장 큰 부담은 상대방의 인증서 검증 작업에 따른 시스템의 부하이다. 이러한 검증 단계는 사용자가 신뢰할 수 있는 인증기관이 서명한 것인지, 인증서에 포함된 인증기관 서명이 올바른지 검사하고, 인증서의 사용 용도가 현재 작업에 적합한 점과 인증서의 유효기간등을 검사해야만 한다. 이중 가장 문제가 되는 부분은 바로 인증서의 유효 기간의 검증작업이다. 일반적으로 인증기관으로부터 발급받은 사용자 인증서는 1년 정도의 유효기간을 갖는다. 그러나 사용자가 비밀키를 저장하고 있던 하드디스크가 포맷되거나 스마트카드/USB 키를 분실한 경우 등과 같이 인증서의 유효 기간이 만료되기 이전에 폐지된 인증서들의 목록, 즉 인증서 폐지 목록 리스트(CRL, Certificate Revocation List)를 유지해야만 하고 이를 주기적으로 갱신해야 한다. 인증서 검증 단계에서 앞서 설명한 모든 단계가 성공했다 하더라도 해당 인증서가 CRL에 등록되어 있는지를 검사하는 것은 필수적이다.

이러한 작업을 위해서는 클라이언트에 인증서 폐지목록을 포함한 인증서를 검증할 정보들이 필요하다. 유선 환경에서는 클라이언트가 디렉토리 서버로부터 인증서 폐지목록을 주기적으로 다운로드 하여 사용할 수 있지만 무선 인터넷 환경은 실제로 일반적으로 사용되는 PC환경이 아주 다르다. 즉 제한된 컴퓨팅 파워와 메모리를 가지고 있으며 주기적으로 CRL을 다운받기 위해 소용되는 시간과 비용으로 인해 사실상 적용이 불가능하다. 따라서 이러한 문제를 해결하기 위해서 제안된 방법인 SLC(Short Lived Certificate)를 이용하거나 실시간으로 인증서의 상태를 검증 요청(OCSP, Online Certificate Status Protocol)하는 인증서 검증방식을 사용해야 한다.

유,무선 PKI기술의 또 다른 차이는 무선 단말기의 제한된 성능으로 인해 사용

되는 암호화 알고리즘에 있다. 국내에서는 유선 환경의 서명용 알고리즘으로 보통 RSA 또는 국내 표준인 KCDSA가 주로 사용되었다. 그러나 무선상에서는 인증기관의 서명용 알고리즘은 유선과 같이 RSA를 사용하는데 반해 사용자의 전자서명용 인증서는 Elliptic Curve를 이용한 ECDSA가 주로 사용된다. 이는 RSA가 보안 측면에서 안전하기 위해서 필요한 키의 길이가 1024비트의 보안 강도를 가지면서 보다 빠른 연산이 가능하기 때문이다.

· SLC(Short Lived Certificate)방식

인증서의 유효 기간을 기존의 인증서 폐지목록 갱신 주기와 비슷하게 해서 클라이언트가 해당 인증서에 대한 인증서 폐지 목록 검증 작업을 하지 않도록 하는 방식이다. 일반적으로 인증서의 유효 기간은 1년 정도지만 이것을 24시간 또는 이보다 더 짧게 함으로써 단기간 동안 별도의 인증서 폐지 목록에 대한 검증을 하지 않아도 된다는 가정이다. 그러나 이 경우 인증기관에서는 매일 전체 사용자의 인증서를 재 발행해 주어야 하기 때문에 기관 측에 많은 부하가 발생하게 된다.

· OCSP(Online Certificate Status Protocol)방식

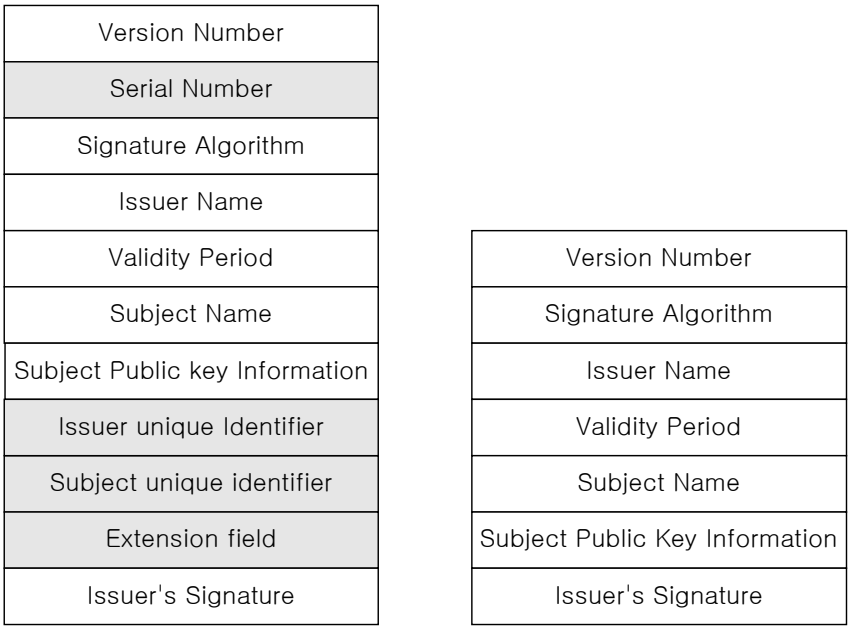
OCSP방식은 클라이언트가 인증서 검증 작업을 수행하기 어려우므로 별도의 장치 B, 즉 제3자에게 인증서 검증을 요청하고 그 결과를 클라이언트가 받아 작업을 수행하는 방식이다. 이 경우는 별도의 OCSP서버가 필요하게 되고 무선을 이용한 클라이언트는 수신한 인증서를 OCSP서버에게 보내서 그 인증서의 유효성 여부를 묻게 된다. 그러면 OCSP서버가 해당하는 인증서의 검증 작업을 통해 클라이언트에게 인증서의 유효성 여부를 알려준다. 이 경우는 일반적으로 유선에서 사용하는 X.509v3 인증서를 사용하게 된다.

다) 무선인증서

유선 PKI 인증서의 구성은 인증서 버전, Serial Number, 알고리즘 식별자, 발행자, 유효기간, 공개키 등록자의 ID와 그 외 기타 선택사항이나 확장필드로 정확한 사용자의 정보를 제공하고, CA의 개인키로 암호화된 서명으로 구성되어 신뢰할 수 있는 공개키를 제공 받을 수 있다.

무선인증서는 인증서 버전, 알고리즘 식별자, 발행자의 ID, 유효기간, 공개키

소유자의 ID, 공개키 정보, CA의 서명으로 구성되었으며 꼭 필요한 정보 이외의 항목은 줄였다. 무선 환경에서 사용하는 인증서는 확장필드를 지원하지 않거나 정의하지 않아서 전자서명 인증관리체계와 연계성이 부족하다. 그렇기 때문에, WAP/WTLS 인증서의 경우 인증서 규격이 유선과 다를 수 있고 변환과정을 게이트웨이에서 처리한다.



a. 유선 PKI 인증서 b. 무선 PKI 인증서

[그림 38] 유선 PKI와 무선 PKI 인증서

라) ECC를 통한 성능의 향상

타원 곡선 암호(ECC, Elliptic Curve Cryptography)는 타원 곡선상의 연상에서 정의되는 이산 대수 문제의 복잡성을 이용하는 암호 시스템으로 RSA/DSA와 같은 공개키 암호 보다 짧은 키 길이와 빠른 연산 속도로 동일한 수준의 보안 강도를 제공해 줄 수 있기 때문에 많은 관심을 받고 있다. ECC 163비트 길이는 RSA 1024비트 길이의 키와 동일한 보안 강도를 갖는다.

또한 기존 공개키 암호시스템에 비해 타원 곡선 암호는 키 길이의 증가에 따른 보안 강도가 월등하게 높기 때문에 향후 하드웨어의 발전 속도를 고려할 때도 여

러 장점을 갖는다. 실제로 ECC 512비트 길이의 키와 같은 보안강도를 제공하기 위해서는 RSA의 경우 대략 1만5000 비트 길이의 키를 사용해야 한다.

2. IMT-2000 기술

가. 정의 및 개요

1) 정의

1980년대 중반에 들어서 시스템마다 주파수 대역이 다르고 주파수 대역폭이 좁아 음성 서비스에 국한하여 서비스를 제공했던 아날로그 셀룰러 이동전화가 폭발적으로 보급되면서 국가별로 서로 다른 시스템의 운영으로 인한 이동성의 한계 및 기술 제약으로 발생하는 용량의 한계를 드러내게 되었다. 그래서 이에 대한 대안으로 '국제전기통신연합(ITU/ International Telecommunication Union)'을 중심으로 단일기술표준과 공통의 주파수 대역 사용 및 광대역화 및 디지털화된 이동통신을 검토하게 되었다.

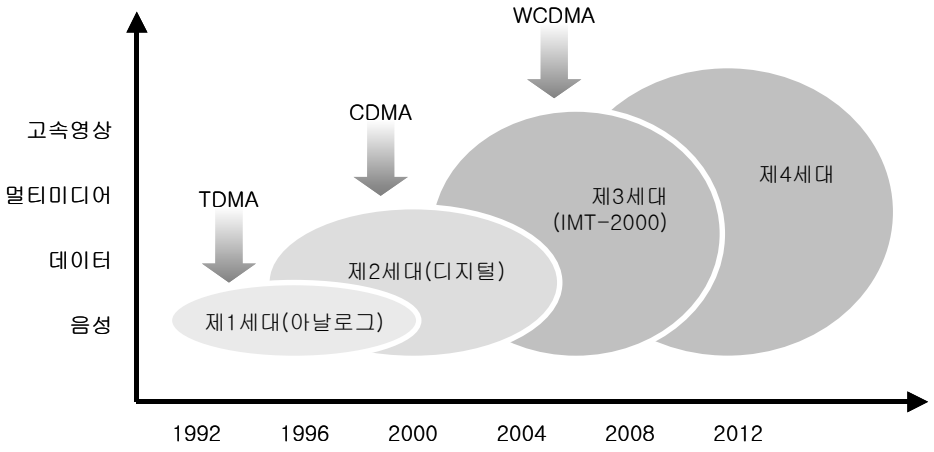
그리하여 1985년 ITU는 시스템 종류(위성, WLL 또는 이동통신)나 국경에 관계없이 어느 나라에서도 운용되는 하나의 보편적인 이동전화기술인 FPLMTS (미래공중육상이동통신 시스템)의 개발 가능성을 연구하는 그룹을 설립하여 본격적인 연구에 들어갔고, 이것이 본격적인 IMT-2000 개발의 시작이라 할 수 있다. 이후 1992년에 개최된 WRC(World Radio Conference)-92 회의에서 글로벌 로밍을 위해 1885~2025MHz / 2110~2200MHz 대역을 위성과 육상부분의 전세계 공통 주파수 대역으로 할당되었으며, 1997년에 WRC-97회의에서 어떤 언어로도 발음하기 어려운 이름인 FPLMTS 대신 2000년경에 2000MHz (2GHz) 대역을 사용하여 서비스를 하게 된다는 의미에서 IMT-2000으로 개칭하게 되었다.

이에 대응하여 국내에서는 '95. 12월 TTA 전파통신연구위원회 산하의 FPLMTS 작업반을 구성한 후 이를 '97년 7월에 IMT-2000 분과위원회로 확대 개편하였고, '99년 6월 ITU-R에 3가지의 IMT-2000 RSPC (무선규격)을 무선전송 후보 기술규격으로 제안하였으며, 이를 국제표준으로 적극 반영하기 위해 3GPP와 3GPP2 양 진영에 모두 참여하여 국제적인 협력체계를 구축하는 등 국내우수기술

의 IRP(지적재산권) 확보 등 적극적인 활동을 벌이고 있다.

이러한 IMT-2000 서비스는 육상/위성 환경에서 무선단말기로 음성, 고속 데이터, 영상 등의 멀티미디어 서비스 및 글로벌 로밍을 제공하는 차세대 이동통신 서비스로서, 21세기를 주도할 대표적인 정보통신서비스로 부각되고 있어, 세계 각 국에서는 기술개발과 표준화 활동에 전력을 다하고 있다.

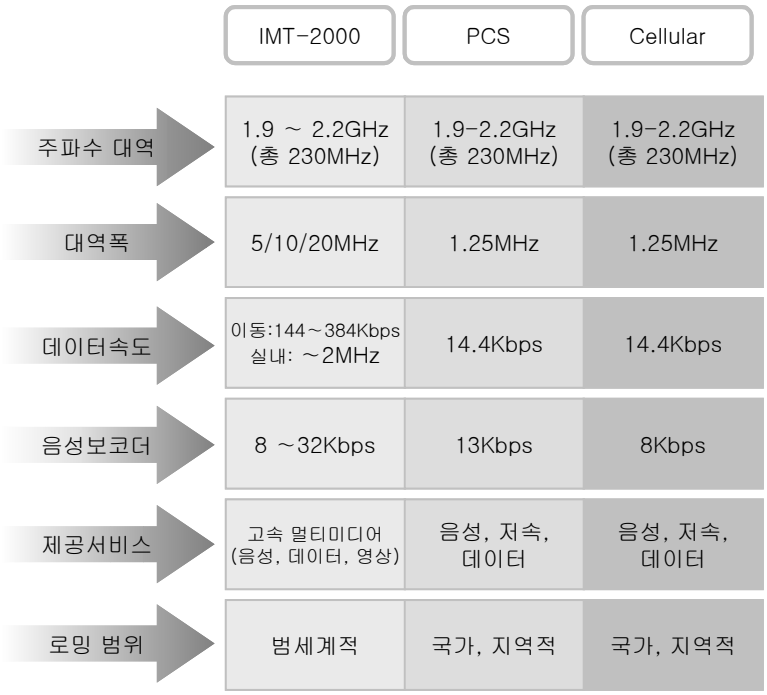
IMT2000은 International Mobile Telecommunication 2000의 약어로 국제적 이동 통신이란 의미로 해석된다. IMT-2000은 사용하려는 주파수 대역 (2000Mhz)과 도입 시기 (2000년경)를 고려, IMT-2000이라는 이름을 고안하였다. IMT-2000은 하나의 단말기로 유무선 환경에서 음성, 데이터, 영상 등을 고속으로 주고받을 수 있는 유무선 통합 개념의 글로벌 멀티미디어 이동통신서비스이다. IMT-200이 도입되면 사용자는 세계 어디서든 자신의 단말기를 사용하여 통화하는 '국제 로밍' 서비스를 받을 수 있으며, 동영상을 포함한 멀티미디어 서비스를 이동중에 이용할 수 있다. 세계 어느 곳에서도 하나의 단말기 또는 사용자 접속카드로 서비스를 이용할 수 있도록 하는 개인화된 신개념 3세대(3G) 서비스이다. 그래서 IMT2000이 3세대(3G)서비스라고도 불리우고 있다. IMT2000은 전 세계적 표준화 및 동일 주파수를 활용하여 세계적인 로밍(global roaming)이 되고 고품질의 음성, 인터넷, 영상 등 멀티미디어 통신이 가능하다.



[그림 39] IMT-2000 발전 방향

2) 개요

셀룰러 이동통신은 1세대인 아날로그 방식(FDMA)을 거쳐 2세대 이동통신인 디지털 방식으로 발전했다. 2세대 이동통신은 유럽에서는 TDMA방식, 미국에서는 TDMA/CDMA 방식, 한국 및 아시아권에서는 CDMA 방식으로 상용화되어 있다. 2.5세대에 해당하는 PCS(Personal Communication Services)는 기존의 디지털 셀룰러 이동통신과 기술적인 유사성 때문에 서비스 면에서 차별성을 보이지 못하고 있다.



[그림 40] IMT-2000과 이동전화 시스템의 비교

IMT-2000 통신 서비스는 PCS가 지역 또는 국가 간의 서로 다른 무선 접속 규격으로 인해서 한 지역에서 사용되고 있는 이동 단말기가 다른 지역에서는 쓸 수 없는 로밍 문제와 데이터 전송률이 8~13Kbps 정도에 불과해 영상 같은 대용량의 데이터를 전송할 수 없다는 문제점을 극복하고자 대두되었다. IMT-2000은 공통 주파수 사용과 단일 기술 표준으로 이용자가 세계 어느 곳으로 이동하더라도 하나

의 단말기로 이동전화 서비스를 이용할 수 있도록 한다는 목표로 연구 및 추진되어 왔다. 3세대 IMT-2000에서는 고속 데이터 네트워크로 발전하여 유선 망과 같이 무선에서도 고속 멀티미디어 서비스를 실현하고, 보다 확대된 글로벌 로밍 서비스를 제공하는 것이다.

나. IMT-2000의 표준화 동향

1) 개요

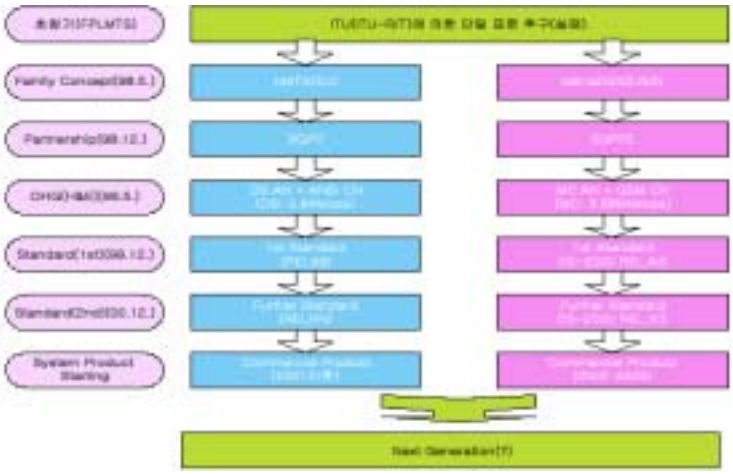
1980년대 중반에 들어서 시스템마다 주파수 대역이 다르고 주파수대역폭이 좁아 음성서비스에 국한하여 서비스를 제공했던 아날로그 셀룰러 이동전화가 폭발적으로 보급되면서 국가별로 서로 다른 시스템의 운영으로 인한 이동성의 한계 및 기술 제약으로 발생하는 용량의 한계를 드러내게 되었다. 그래서 이에 대한 대안으로 '국제전기통신연합(ITU/ International Telecommunication Union)'을 중심으로 단일기술표준과 공통의 주파수 대역 사용 및 광대역화 및 디지털화된 미래이동통신을 검토하게 되었다. 그리하여 1985년 ITU는 시스템 종류(위성, WLL 또는 이동통신)나 국경에 관계없이 어느 나라에서도 운용되는 하나의 보편적인 이동전화 기술인 FPLMTS (미래공중육상이동통신 시스템)의 개발 가능성을 연구하는 그룹을 설립하여 본격적인 연구에 들어갔고, 이것이 본격적인 IMT-2000 개발의 시작이라 할 수 있다. 이후 1992년에 개최된 WRC(World Radio Conference)-92 회의에서 글로벌 로밍을 위해 1885~2025MHz / 2110~2200MHz 대역을 위성과 육상부분의 전 세계 공통 주파수대역으로 할당되었으며, 1997년에 WRC-97회의에서 어떤 언어로도 발음하기 어려운 이름인 FPLMTS 대신 2000년경에 2000MHz (2GHz) 대역을 사용하여 서비스를 하게 된다는 의미에서 IMT-2000으로 개칭하게 됩니다. 이에 대응하여 국내에서는 '95. 12월 TTA 전파통신연구위원회 산하의 FPLMTS 작업반을 구성한 후 이를 '97년 7월에 IMT-2000 분과위원회로 확대 개편하였고, '99년 7월 IMT-2000 프로젝트그룹으로 변경하여 유/무선, 위성 및 주파수분야의 국내/외 표준화활동을 담당하고 있습니다. IMT-2000 프로젝트그룹은 '98년 6월 ITU-R에 3가지의 IMT-2000 RSPC (무선규격)를 무선전송 후보기술규격으로 제안하였으며, 이를 국제표준으로 적극 반영하기 위해 3GPP와 3GPP2 양 진영에 모두 참여하여 국제적인 협력체계를 구축하는 등 국내우수기술의 IPR(지적재

산권) 확보 등 적극적인 활동을 벌이고 있습니다. 이러한 IMT-2000 서비스는 육상/위성 환경에서 무선단말기로 음성, 고속 데이터, 영상 등의 멀티미디어 서비스 및 글로벌 로밍을 제공하는 차세대 이동통신 서비스로서, 21세기를 주도할 대표적인 정보통신서비스로 부각되고 있어, 세계 각국에서는 기술개발과 표준화 활동에 전력을 다하고 있다.

2) 표준화 동향

국제적인 IMT-2000 기술표준화는 북미(cdma2000)와 유럽/일본(W-CDMA)을 중심으로 개발되어 온 기술방식을 단일화하기 위해 3GPP와 3GPP2를 중심으로 진행되고 있으나 규격의 통합은 사실상 어렵게 되었다고 말할 수 있다. 지금까지의 기술표준화는 과거의 시스템 기술 개발력을 보유하고 있는 Ericsson, Lucent Technology, Motorola, Nokia 등 제조업체의 이해관계에 의해 진행되어 왔으나, IMT-2000 기술표준화에 있어서는 표준의 최종소비자인 전 세계 이동통신사업자의 의견을 반영하기 위해 '99년 5월 OHG(Operator's Harmonization Group)를 결성하여 복수표준을 통합할 수 있는 체계를 ITU, 3GPP, 3GPP2에 제안하여 요구사항을 반영하였고, 사업자의 망진화와 연계하여 자율적인 표준 선택권을 확보하게 되었다. 그 중, ITU는 UN 산하기구로서 전기통신 부분의 표준화는 ITU-T에서, 전파통신에 관한 표준화는 ITU-R에서 담당한다. IMT-2000 표준화와 관련된 중추적인 역할은 ITU-T의 SG 11에서 망구조, 신호방식 등을 다루고, ITU-R의 SG 8(Study Group 8)내의 TG 8/1(Task Group 8/1)에서는 시스템 요구조건과 무선전송방식 등에 관한 검토가 이루어지고 있다.

IMT-2000 연구는 일반, 서비스, 과금과 정산, 교환과 신호방식, 망 운용과 관리, 무선 시스템 등 6개 분야로 분류하여, 각 분야별 권고작성부문 /연구위원회(SG)명, 연구과제번호, 권고명, 작성시기, 관련 SG 등을 정리했다. 이 내용은 기본적인 것으로 향후 각 SG/TG에서 재검토되어 정도를 높여가기로 하였다.



[그림 41] IMT-2000 표준화 과정

IMT-2000 시스템의 국제 표준화를 위해 우리나라의 표준화 기구인 TTA를 포함해 북미의 TIA, T1P1, ANSI, 유럽의 ETSI, 일본의 ARIB, TTC, 중국의 CWT 등이 적극적으로 참여하고 있으며, 여기서 연구 개발한 후보 무선전송 기술을 ITU에 제출한 이후 한국, 일본 및 유럽의 WCDMA(일본의 W-CDMA와 유럽의 UTRA 포함) 기술인 3GPP라는 조직을 구성하여 단일 표준화 안을 작정하기 시작했으며 cdma2000방식(약칭: W-cdmaOne)은 3GPP2를 중심으로 상세 표준화 작업을 수행하고 있다.

IMT-2000과 관련하여 현재 가장 영향력이 있고 관심을 끌고 있는 시스템은 광대역 전송과 CDMA 기술을 채택하고 있는 유럽의 W-CDMA와 미국 cdma2000이다. W-CDMA는 유럽과 일본에서 시작되어 현재 RTT의 표준화가 주요 쟁점으로 다루어지고 있다. RTT 표준으로 제출된 5가지의 UMTS/IMT2000 방식 중에서 에릭슨에서 제출한 W-CDMA방식과 지멘스에서 제출한 TD-CDMA방식이 비교적 높은 평가를 받고 있다. 에릭슨의 W-CDMA방식은 일본의 W-CDMA방식과 비슷하여 이미 하나의 방식으로 통합된 상태이다. 또한, W-CDMA와 TD-CDMA도 협의를 거쳐 W-CDMA와 TD-CDMA기술을 겸한 UTRA로 확정되었다. UTRA는 대칭 주파수대(FDD모델)에서 W-CDMA기술을, 비대칭 주파수대(TDD모델)에서 TD-CDMA기술을 사용하게 된다. W-CDMA의 핵심기술은 GSM-MAP을 기반으로 하며, 네트워크 확장방식을 통해 ANSI-41에서도 운영이 가능하다. 한편 퀄컴에서 제안한 cdma2000은 IS-95와 IS-41에서 발전된 것으로, 루슨트, 모토롤라, 노텔

과 퀄컴에서 연합으로 제출한 Wideband cdmaOne기술을 기반으로 한다. cdma2000의 주요 특징은 기존의 TIA/EIA-95B표준과 겸용하여 IS-95B 주파수대역에서 공동 운영이 가능하다는 점이다. 그 밖에 cdma2000은 기존의 IS-634A표준도 효과적으로 지원할 수 있다. cdma2000은 ANSI-41을 기반으로 하며, 네트워크 확장방식을 통해 GSM-MAP에서의 운영이 가능하다.

cdma2000은 MC-CDMA방식을 채택하여 음성, 패킷 데이터 등의 업무를 지원할 수 있다. cdma-2000에는 1X와 3X 두 부분이 포함되며, 6X, 9X, 12X까지 확장될 수 있다. 대역폭이 N*1.25MHz인 cdma2000시스템에 대해서는 여러 개의 반송 주파수를 전체 주파수 대역에 이용할 수 있다. 하나의 반송 주파수를 지원하는 cdma2000표준인 IS2000은 이미 1999년 6월에 통과되었다.

현재 제3세대 이동통신 시스템의 이동통신표준 제정을 위한 각 국의 경쟁이 매우 치열해지고 있다. 이중 일본과 유럽의 W-CDMA와 퀄컴의 cdma2000이 가장 치열한 경쟁을 보이고 있으나 현재까지의 상황으로 볼 때 W-CDMA가 우위를 보이고 있다. 그러나 퀄컴은 중국 대륙의 방대한 이동통신시장 진출을 통해 cdma2000을 제3세대 이동통신시스템의 세계 표준으로 채택하려는 노력을 경주하고 있다. 이와 함께 2000년 6월 유럽 GSM방식으로 통신 서비스를 제공하는 중국 제2 통신사업자인 차이나 유니콤에서도 cdma2000을 채택하기로 발표하였다.

현재 전세계적으로 퀄컴이 추천하는 cdma2000을 채택하고자 하는 통신사업자들이 증가하고 있는 이유는 W-CDMA와 비교할 때 설비투자가 1/2에 불과하기 때문이다. 국제 로밍면에서도 퀄컴의 기술은 W-CDMA보다 앞서가고 있다. DDI-IDO연합은 현재 한국과 홍콩에서 cdmaOne 단말기 로밍 서비스를 진행하고 있으며, 2000년 하반기에 미국으로 확대하고 9월에는 호주로 확대할 계획이다. 그 밖에 퀄컴에서는 cdmaOne방식과 유럽 및 대부분의 아시아 국가들에 보급되어 있는 GSM방식을 동시에 이용하는 단말기를 개발하고 있다. 이에 따라 W-CDMA와 cdma2000의 제3세대 이동통신시스템 표준 쟁탈전은 갈수록 치열해질 것으로 예상된다. 1999년 전세계 통신 사업자들로 구성된 OHG에서는 3GPP와 3GPP2의 기술을 통합한 단일 IMT-2000 표준안을 권고하게 되었고 WCDMA를 기반으로 한 유럽식 UTRA FDD(UMTS Terrestrial Access Frequency Division Duplex)방식, UTRA TDD(Time Division Duplex)와 미국식 cdma2000방식이 ITU의 8/1에서 권고한 IMT-2000 무선접속 표준화 방식으로 권고되어졌다. 이에 따라 3GPP의 Chip Rate는 3.84Mcps로 바꾸었고, 프레임 당 슬롯 수도 16개에서 15개로 변경되었으

며, 순방향 링크에서 Common Pilot Channel을 도입하였다. 이를 바탕으로 무선 접속 분야인 경우 ITU-R(TG8/1)과 네트워크 분야인 경우 ITU-T(SG11)에서는 위의 3가지 방식 외에 TDMA 방식을 포함한 5개의 표준화 안을 권고하게 되었다.

다. 서비스

제3세대 이동전화 MIT-2000은 휴대전화 하나로 다양하고 편리한 멀티미디어 서비스 및 무선인터넷 서비스를 제공하게 될 것이다. MIT-2000은 점점 늘어가는 멀티미디어 요구에 부합하는 음성, 데이터는 물론 동화상까지 전송이 가능하게 되는 고속화 및 광대역화라는 이동전화 기술이다. 이를 위해 IMT-2000에서는 고속 이동 환경에서 144Kbps, 저속 이동 환경에서 384Kbps, 정지 및 실내 환경에서 2Mbps 정도까지도 데이터 전송 속도가 실현될 것이다. 2005년경에는 최고 2Mbps로서 차원 높은 무선 멀티미디어 커뮤니케이션이 가능하게 될 것이다. IMT-2000에서 구현 가능한 서비스로는 인터넷 접속, 영상 컨텐츠, 대용량 데이터/자료 전송 및 소프트웨어 다운로드 등 다양한 멀티미디어 컨텐츠를 수용할 수 있는 형태의 서비스가 제공될 것이다.

IMT-2000 서비스의 큰 특징은 하나의 단말기로 로밍을 지원하는 것이다. 국제 로밍에 관해서는 ITU(International Telecommunication Union)표준안에서 보듯이 처음에는 북미(3GPP2; 3rd Generation Partnership Project Ⅱ)의 CDMA2000(동기식)과 유럽/일본(3GPP; 3rd Generation Partnership Project)의 W-CDMA(Wideband CDMA, 비동기식)의 복수 표준으로 자리 잡았다. 그러나 통신 사업자들이 주축이 된 OHG(Operator Harmonizing Group)에서 동기식 및 비동기식 모두 상호 연동이 가능하도록 합의했기 때문에 ITU 역시 W-CDMA 기반의 DS(Direct Spread)방식, 기존의 CDMA2000으로부터 진화가 유리한 MC(Multi-Carrier) 모드, 데이터 전송과 같은 특정 목적으로 사용 가능한 TDD 모드 등의 유럽의 GSM과 북미의 ANSI41에서 모두 수용할 수 있도록 했다. 그 결과 앞으로 단말기가 어떤 망에 접근하더라도 서비스가 가능한 글로벌 로밍이 실현 가능하게 되었다.

1) 베어러 서비스

베어러 서비스는 액세스 지점간의 정보 전달을 가능케 해주는 것으로, 이동통신 시스템이 사용자가 아닌 이동 단말기에 제공하는 서비스라고 말할 수 있다.

베어러 서비스는 통시 시스템의 계층적 기능 구조에서 낮은 계층의 기능을 수

행하며 PSTN, N-ISDN, IP 망과 상호 연동이 가능해야 한다. 베어러 정보 전달은 연결형 및 비연결형 서비스가 가능해야 하는 요구 사항을 모두 지원한다. 또한 보장/불변 비트율 (a Nonguaranteed/Dynamically Variable Bit Rate)을 제공하며 실시간과 비실시간 응용 서비스도 지원한다. 지원 비트율은 시골같이 도심과 멀리 떨어진 실외 무선 환경에서는 144Kbps, 도시나 도시 인근 교외의 실외 무선 환경에서는 적어도 384Kbps 까지 지원한다.

2) Tele Service

IMT-2000 Tele service는 사용자 관점에서 구분되는 통신 서비스라고 할 수 있다. 3GPP 22.003/3GPP TS 22.100/22.105 규격에 언급되었거나 또는 현재 논의가 진행중인 3G-324/M에 기반을 둔 멀티미디어 서비스 등으로 다음과 같은 Tele 서비스들이 지원되고 있다.

(1) 음성 및 전화 서비스

PSTN/ISDN의 음성 정보와 오디오 전송을 제공한다. 고정회선 사용자간, IMT-2000 시스템 사용자간에 양방향, 대칭 채널을 경유한 음성 통신을 지원한다.

(2) 인터넷 접속

IMT-2000 시스템은 외부 데이터 망과 상호 동작할 방법을 제공한다. 이러한 상호 동작은 이동 무선 환경 하에서 상호 동작 망의 QoS 베어러 기능으로 대처할 수 있다. 다중화된 H.324 비트 스트림 내에서 개별화된 Qos 파라미터를 허용함으로써 IMT-2000 시스템 베어러 서비스 상에서 각 미디어 스트림을 위한 FEC(Forward Error Correction) 기법 또는 재전송 기법(ARQ) 등을 허용한다.

3) 부가 서비스

W-CDMA 기반의 IMT-2000 시스템에서 제공하는 부가 서비스는 다음 항목과 같다.

- 발신번호 표시 (Calling Line Identification Presentation)
- 발신번호 표시 금지 (Calling Line Identification Restriction)
- 무조건 착신통화 전환 (Call Forwarding Unconditional)
- 통화중 착신통화 전환 (Call Forwarding on Mobile Subscriber Busy)

- 무 응답시 착신통화 전환 (Call Forwarding on No Reply)
- 접근 불가시 착신통화 전환 (Call Forwarding on Mobile Subscriber Not Reachable)
- 모든 발신 통화 차단 (Barring of Outgoing International Calls)
- 국제전화 발신통화 차단 (Barring of All Incoming Calls)
- 모든 착신통화 차단 (Barring of All Incoming Calls)
- 통화 전환 (Call Deflection)
- 착신번호 표시 (Connected Line Identification Presentation)
- 착신번호 표시금지 (Connected Line Identification Restriction)
- 과금정보 제공 (Advice of Charge - Information)

3. 국내·외 무선인터넷 시장

가. 해외 무선인터넷 시장 현황

1) 유럽

가) 개요

1990년대에 유선 인터넷에서 미국에 주도권을 내어 준 유럽은 일찌감치 무선분야로 관심을 돌렸다. 그 결과 오늘날 세계 이동전화 시장 상위 5개국에 핀란드, 노르웨이, 스웨덴, 덴마크등 스칸디나비아 4국이 포함되었고, 유럽은 무선인터넷의 강자로 부상되었다. 이는 국가에서 정책적으로 추진한 이유도 있지만 험준한 산악이 무선에 더 적합한 환경 조건을 제공했기 때문이라 할 수 있다. 2000년 5월 유럽이 최대 IT 행사인 <TIME 이벤트>가 열린 스웨덴의 수도이자 유럽 IT의 중심도시인 스톡홀름의 모습은 유럽이 무선인터넷의 선두 주자임을 분명하게 보여주었다.

유럽인에게 휴대폰은 생활의 주요 수단이 되어 있는 예로 유럽은 휴대폰을 이용해서 자판기의 음료수를 빼먹는다거나, 주차료나 세차비를 지불하는 등의 서비스가 이미 생활화되어 있는 대표적인 예이다.

나) 무선인터넷시장

(1) 시장동향

최근 유럽은 이동통신 시장의 폭발적인 성장과 업체간의 대규모 M&A로 인한 거대 기업의 탄생으로 세계이동통신시장에 새로운 강자로 급부상하고 있다. 또한 무선 인터넷 시장의 발전은 크게 휴대통신기기의 보급과 인터넷 사용 인구에 비례하여 그 규모를 예측할 수 있는데, 유럽의 경우는 이 두 가지 조건이 모두 충족되어 있어 인해 향후 무선인터넷 시장에서 앞서 갈 모든 준비를 갖춘 셈이다. 휴대 통신기기의 보급면에서 살펴보면 세계의 어느 지역보다 높은 보급률을 자랑하고 있는데 이러한 유럽의 고도 성장의 배경은 여러 가지 면에서 그 이유를 발견할 수 있다.

첫째, 통신을 위한 인프라의 구축이 국가적 차원에서 선행되었다는 것을 들 수 있다.

둘째, 세계 유수의 통신장비 및 통신 회사들이 많이 위치하여 활발한 기술개발 및 인수합병이 진행되었다는 것을 들 수 있다.

셋째, 유럽의 이동통신 시장이 발전할 수밖에 없는 지리적인 조건을 들 수 있다. 지형적으로 타국과 국경을 바다로 하고 있는 우리나라와는 달리 국경을 맞대고 있는 수많은 유럽국가들 사이에서 글로벌 로밍을 필수적 요소라는 것이 대표적인 예라 할 수 있다.

(2) 유럽시장의 특징

유럽의 이동통신 시장은 미국과의 다른 특징을 지니고 있다. 그래서 미국의 무선 비즈니스 모델을 유럽 쪽에서 도입하거나 혹은 반대로 유럽 쪽의 모델을 미국 쪽으로 가져가기에는 많은 문제점이 있다. 세계 무선 시장의 두 축 을 형성하고 있는 유럽과 미국 사이에 이러한 차이점이 발생하는 사회, 문화적인 이유는 다음과 같다.

첫째, 언어문화적임을 생각해 볼 수 있다. 유럽시장은 하나의 단일 시장이 아닌 서로 다른 언어와 문화를 가지고 있는 여러 개별 국가들에 의해 이루어진 복합시장이라고 할 수 있다. 반면 미국의 경우 하나의 거대한 단일 시장을 형성하고 있다. 즉 유럽의 경우 어느 하나의 웹사이트가 개별이용자에게 좀더 효율적인 접근을 하기 위해서는 각 개별 이용자가 사용하고 있는 언어로 표현되

어야 함은 물론이고, 더 나아가서 서로 다른 문화적 측면도 고려되어야 한다.

둘째로는 세계화전략을 고려해 볼 수 있는데, 유럽의 경우 서로 다른 크기의 여러 개의 분화된 개별국가 시장을 형성하고 있다. 즉 유럽국가의 대부분 기업들은 기본적으로 제한적인 내수 시장을 극복하기 위한 세계화 전략을 고려하고 있다는 것이다.

셋째, 통신회사의 경우를 분석할 필요가 있다. 통신시장 선점한 몇몇의 유럽 회사들은 미국의 중상위 규모 정도의 통신 사업자 이상의 고객을 확보하고 있다. 즉 미국 시장에서 망 사업자들이 필요로 하고 있는 것과 비슷한 규모의 장비나 서비스들의 수요가 발생한다는 것이다.

다) 무선인터넷 단말기

(1) 단말기 시장

GSM Association의 2000년 7월 자료에 의하면 전 세계적으로 GSM(Global System for Mobile communication)을 사용하는 인구는 최근 6개월간 22%가 증가하여 3억 3,100만명이 되었다. 이중 65%에 이른 2억 1,500만명이 유럽에 집중되어 있으며 27% 정도인 9천만명 정도가 아시아 지역에 위치하고 있다.

2005년 전세계 무선인터넷 브라우저가 탑재된 단말기 분포를 보면 서유럽과 동유럽을 합쳐서 36% 정도로 유럽이 가장 큰 시장을 형성하고 있으며, 아시아가 31%으로 두 번째, 미국과 캐나다를 포함 북미가 20% 정도로 세 번째 큰 시장규모를 형성하고 있다. 또한 WAP에 관한 관심 여부를 알아본 결과 독일 인터넷 사용자의 약56%, 프랑스36% 정도가 이미 WAP에 관해서 알고 있었다. 이러한 조사 결과 인터넷에 익숙한 사용자들이 무선인터넷폰에 더 많은 관심이 있다 것을 말해주고 있다.

라) 무선인터넷 서비스

(1) 서비스 동향

유럽에서 사용되고 있는 무선인터넷 서비스는 일본 i-Mode 서비스보다 빈약한 컨텐츠를 가지고 있지만 사용 면에서 많은 활용빈도를 가지고 있다. 서비스 영역으로는 업무적인 부분과 그의 엔터테인먼트부분 그리고 단문 메시지 서

비스(SMS : Short Message Service) 부분으로 크게 구분할 수 있다. 무선 인터넷의 사용요구는 유선 응용프로그램의 무선으로 확장하는 것 외에, 무선만을 위해 새로이 등장한 서비스들을 생각해 보면 '맞춤서비스'라는 의미에 더 가까울 수 있다. 여기서 '맞춤'이라는 말은 무선 네트워크 환경에 맞도록 축소 또는 요약한다는 의미이거나, 사용자 각각이 원하는 개별화된 정보를 제한다는 뜻이기도 하다.

국내에서도 무선인터넷에 관심 있는 사람이라면 누구나 당연히 생각할 수 있는 일반적인 부가가치 서비스가 유럽에서 일정 부분 수익이 창출되고 있음 역시 눈 여겨 볼 필요가 있다.

(2) 무선전자상거래

유럽의 시장조사 회사인 듈라체에 따르면 유럽의 이동전화를 이용한 EC 시장 규모는 지난해 약 3억 2,800만 달러에서 오는 2003년 230억 달러를 기록, 불과 5년 동안 60~70배나 확대될 전망이다. 이 같은 전망은 이동전화 가입자가 현재 전세계적 약 3억 7,500만명에 달해 약 1억 6천만명으로 추산되는 인터넷 사용자보다 두 배 이상 많은 사용자가 기반을 마련했다는 점에 근거하고 있다.

무선전자상거래 초기 시장에서의 서비스 유형이 모바일 뱅킹과 간단한 티켓 예매, 정보 서비스 등을 나타내고 있으며, 중간 단계를 상품 구매와 복잡한 티켓 예매, 그리고 마지막 단계의 서비스는 미디어 다운로드나 스트리밍 서비스 등을 나타내고 있다. 무선전자상거래의 실용화에 대한 근거로 현재 유선 컨텐츠가 WAP을 통하여 쉽게 무선으로 전환될 수 있으며, 예산 면에서도 연간 유선 전자상거래 사이트 유지비용의 10%정도 수준으로 유지 가능하다는 현실성 있는 가능성을 유럽의 e-commerce의 경영자들의 조사결과를 실은 "Europe's Mobile Internet Opens up"에서 시사되고 있다. 또한 Forrester 사의 분석에 의하면 1/3 정도의 유럽 무선인터넷에 대한 종량제 요금 체계를 제공할 것으로 보여 더욱더 무선 인터넷 전자상거래의 확산을 부추길 것으로 예상하고 있다. 그리고 세계 최대 온라인 경매업체인 미국 이베이가 유럽에서 무선경매서비스를 실시할 예정이며, 이는 WAP을 지원하는 이동전화를 통해 제공된다.

(3) 무선 뱅킹 서비스

무선 뱅킹 서비스는 무선전자상거래와 더불어 또 하나의 독립된 서비스 영

역을 구축하고 이다 특히 이용자 측에서 가장 관심을 가지고 또 실제로 이용하고 있는 서비스 중의 하나이다. 따라서 각종 은행과 망 사업자들은 이러한 사용자의 요구에 부흥하기 위해 다양한 방법으로 무선 뱅킹 서비스를 지원하려는 노력을 보이고 있다. 특히 타 지역보다 유럽에서 무선전자상거래 서비스와 무선 뱅킹 서비스 시장이 가장 크게 형성하고 있다. 예를 들어 스웨덴의 망사업자중 하나인 Telia의 WAP 포탈서비스인 MyDOF은 1999년 말부터 서비스를 시작한 초기 무선 포털 서비스가 있다. 또 1999년 5월에 영국의 BT Cellnet과 UK Bank First Direct에서 시작한 무선 폰뱅킹 서비스가 있다. 이외에도 2000년 2월 Vodafone과 The Woolwich, UK bank는 노키아와 손잡고 Open Plan이라는 서비스를 내놓았는데 은행간의 통합 서비스를 고객에게 제공하는데, 잔액 조회와 거래 서비스는 물론 영수증 지불 처리 및 계좌간 이체 등의 서비스도 제공한다고 밝혔다.

이처럼 다양한 시도가 각종은행, 통신사업자, 그리고 단말기 제조업체들과의 제휴를 통해서 이루어지고 있는 것을 볼 때 휴대폰을 이용한 부가 서비스가 초기 시장 수용과 성공 가능성 면에서 가장 유력한 후보라 할 수 있다. 그래서 모바일 뱅킹 서비스가 현실적으로 수입을 올리기 위해서 고려되어야 하는 점은 네트워크 사용량의 증가와 충성스런 단골 고객을 확보한다는 측면에서 즉각적인 효과를 기대할 수 있을 것이다.

현재 유럽에서 행해지고 있는 무선 뱅킹 서비스를 보면 뱅킹 서비스를 독자적으로 서비스하기보다는 비슷한 유형의 여러 가지 부가정보 서비스와 병행해서 진행하고 있는 것을 알 수 있다.

마) 결론

유럽은 새로운 IT 산업, 즉 이동통신 산업의 새로운 중심지로 입지를 굳혀가고 있다. 우리나라 또한 인구 대비 50% 이상이 휴대폰 보급률과 20% 이상의 인터넷 사용 인구를 가지고 있고, 다른 산업보다 이동통신 산업의 전망이 밝다고 본다. 하지만 이렇게 좋은 내수 환경에서 개발된 서비스나 솔루션, 비즈니스 모델들이 국내 시장에서 한정된다면 그 또한 반쪽짜리 성공밖에 되지 않는 것 같다.

비록 서로 다른 통신 환경을 갖고 있지만, 우리 보다 앞서 무선 데이터 서비스를 실현했고, 여러 가지 면에서 앞서 가고 있는 유럽 시장을 분석해 보고 그들의 좋은 점을 새롭게 구성하고, 단점을 보완하는 응용들을 개발한다면 국내 시장

은 물론 국제 시장에서 경쟁력도 충분히 확보살수 있으리라 확신한다. 더욱이 제한된 내수 시장을 극복하고 일지 감치 유럽 전역을 하나의 시장으로 보고 글로벌화를 추진한 유럽 각국의 서비스. 솔루션들은 우리나라 제품들의 국제화에 좋은 연구 자료가 될 것이다.

2) 일본

가) 시장 동향

(1) 통신시장

일본의 이동전화 서비스는 휴대전화와 고속으로 이동을 하지 않는 보행자를 대상으로 한 이동전화 서비스인 PHS(Personal Handy System)로 나누어진다.

(2) 모바일 인터넷 시장

최근 PC와 접속이 없이 자체적으로 데이터 통신과 부가서비스에 접속이 가능해졌는데 그 용도를 보면 다음과 같다.

- 단문 메시지(Short Message, 인터넷 메일)
- 홈페이지 열람
- 멀티미디어 송수신
- m-commerce

■ 모바일 인터넷 사업자

NTT-Docomo의 i-Mode, IDO그룹의 EZWeb, J폰 그룹의 J-스카이 등 모두 3 가지가 있다.

■ 모바일 인터넷 시장전개

1999년 2월 NTT-Docomo는 i-Mode 서비스를 개시하였는데 휴대전화기의 액정표시 창으로 인터넷 정보를 열람할 수 있는 기능을 가지고 있어 은행거래나 뉴스열람, 티켓 예약등이 가능한 서비스이다. i-Mode 단말이 휴대전화와 같은 형상의 일체화된 단말이기 때문에 부피가 크다든지, 조작이 귀찮다는 문제를 간단히 해결했으면 통신요금문제 또한 시간에 관계없이 주고받은 데이터 양으로만 요금이 부과되는 정액 요금제이기 때문에 조작에 다소 시간이 걸려도 안심하고 사용할 수 있게되었다.

1999년 4월 IDO와 DDI셀룰러가 i-Mode를 대항해 WAP(Wireless

Application Protocol) 방식 서비스를 시작한 것이다. WAP은 i-Mode 처럼 휴대전화만 정보서비스를 제공하였지만 컨텐츠 기술언어로 HDML(정식으로 WML)로 표현된다는 점에서 다르다. i-Mode 보다 뛰어난 User Interface를 만드는 것이 가능하다는 장점이 있다. 즉 WAP의 갖고 있는 휴대전화용 컨텐츠 서비스가 세계적인 표준이 될 가능성이 있다는 것이다.

나) 컨텐츠

(1) 모바일 인터넷과 컨텐츠

모바일 인터넷에서는 유선인터넷과는 달리 제한된 주파수 대역을 사용하기 때문에 컨텐츠를 최적화시킬 필요가 있다. i-Mode와 IDO-DDI그룹의 EZ시리즈는 서로 다른 방식을 이용하고 있다.

- 컴팩트 HTML

  i-Mode 에서는 종래의 웹서버에서 사용하던지 HTML 언어를 채용하고 있다. 아직까지 HTML로 웹서버를 구축한 인력이 많으므로 비교적 용이하게 상용할 수 있다는 특징이 있다.

- WAP(Wireless Application Protocol)

  IDO와 DDI의 EZ 시리즈에서는 WAP이라고 불리는 모바일 환경에 특화된 프로토콜을 채용하고 있다. WAP에는 전용의 WML(Wireless Markup Language)로 서버를 구축해야 하므로 아직 불편함이 있으나 최근에 HTML 필터라고 불리는 WML 변환 서버가 개발되어 기존자원의 효율적 이용이 가능해질 전망이다.

- 컨텐츠의 중요성

  스마트폰 환경에서는 제공되는 컨텐츠가 좋을수록 이용하기 편하고 그 편리성이 사용을 결정하게 만든다. 이런 의미에서 기존 인프라를 활용해서 손쉽게 새로운 서비스를 전개한 i-Mode는 높은 평가를 받는다. WAP 서비스의 시장 침투도 이런 컨텐츠를 어떻게 조기에 확보하는가에 달려 있다.

- 주목받는 컨텐츠 서비스

  최근에 주목받는 컨텐츠 서비스로 GPS와 PHS의 위치정보 연동 서비스가 있다.

다) 애플리케이션

지속적으로 확대되는 모바일 인터넷 시장에서 가장 유망한 기기는 스마트폰이 될 것으로 보인다.

(1) 스마트폰의 발전

초기 스마트폰 서비스가 제1기라면 지금 보급되고 있는 컬러 디스플레이를 장착한 스마트폰은 제2기라고 말할 수 있다. 제3기는 사용자 고유의 응용프로그램이 사용되는 시기가 될 것이다. 아마도 자바(JAVA)로 대표되는 애플릿들이 실행될 가능성이 많다.

(2) 음성인식 기술 보이스 XML

모토로라와 IBM에서는 음성정보를 데이터로 변환한 후에 인터넷상의 액세스하는 기술을 개발중인데 이를 Voice XML이라 한다. 사용자는 인터넷에 브라우저를 사용할 필요가 없이 보통의 음성을 사용해서 접속한다. 홈페이지도 음성으로 안내가 나오고 요구하는 내용을 음성으로 전달해준다.

(3) IC 카드를 내장한 차세대 휴대전화

현재의 휴대전화에는 ID-ROM이라 불리는 기기에 전화 번호 정보를 묻어두고 있다. 따라서 기종 변경 시 등록이 가능한 대리점에서 해야한다. 하지만 유럽의 휴대전화 GSM에서는 SIM칩이라 불리는 발신자번호 등록 칩이 내장되어 있어 사용자가 자유로이 장착할 수 있다. 일본은 UIM이라 불리는 IC칩에는 발신자 번호, 무선네트워크 접속정보 등이 들어 있다. UIM 칩 자체도 연산능력, 기억 용량 등에 따라 정보 처리를 할 가능성도 있다.

(4) 휴대전화가 전자지갑이 된다

일본의 차세대 휴대전화에 탑재될 IC 카드를 이용하여 휴대전화 전자지갑에 가치를 저장할 수 있다.

라) 모바일 인터넷 서비스

(1) 개요

휴대전화와 PHS는 전화기라고 하는 누구나 알고 있는 기능을 바탕으로 문

자 메시지, 인터넷으로 확대하면서 진화를 계속하고 있다. 휴대전화 이용자는 이런 새로운 기능을 이용하는데 서서히 적응하고 있다.

(2) 인터넷 이용 공간의 변화

인터넷캐주얼 이용자는 고정 망 인터넷 이용자와 달리 PC와 무관한 고교생을 시작으로 일반인등 PC 비사용자들이 '언제든지, 어디에서건, 간편하게'를 모토로 가정이나 일상생활 공간을 사용 공간으로 한다. 사용목적 또한 생활 속에서 정보탐색이나 오락을 즐기기 위함에 있다. 그러면서 이제는 항상 가지고 다니는 휴대전화나 정보 단말기의 사용으로 공간이 확대되어 왔다. 이것은 종래의 이용환경에 새로운 이용환경을 융합한 비즈니스 시장의 발생을 의미한다.

우선, 새롭게 인터넷 서비스를 제공하는 사업자는 새로운 환경에서 필요로 하는 서비스를 추구한다. 다음으로는 종래의 고정적 장소에서 이용되는 PC와 새로운 환경에서 사용되는 휴대전화나 정보 단말을 결합하여 양자의 환경의 차를 메우는 접속 서비스가 발생한다.

(3) 메일

일본의 모바일 인터넷에서 가장 쉽게 받아들여진 서비스가 메일이다. 메일은 아직 본격적인 쌍방향 정보의 흐름은 아니지만 문자 메시지에 익숙한 젊은 세대들에게 빠른 시간 내에 모바일 인터넷을 보급하는데는 크게 기여하고 있다.

종래의 휴대전화나 PHS에서 사용된 단문 메시지는 인터넷과 연결이 되지 않아 단지 휴대전화 사이의 메일 교환만 가능했다. 그러던 것이 인터넷과 연결이 되면서 메일의 이용 용도가 비약적으로 늘어났다. 또한 개인적인 용도에서 동일한 휴대전화나 PHS에 한정된 커뮤니케이션이 인터넷을 통하여 세계의 이용자 모두를 상대로 한 서비스로 확산되었다.

(4) 웹브라우징

웹브라우징은 모바일 인터넷이 휴대전화기에 의존하고 있다는 점에서 문자 커뮤니케이션에서 정보 액세스로 발전한 것이다. 이렇게 함으로써 적극적인 정보 탐색과 쌍방향 통신이 가능해진다.

인터넷은 HTML을 사용하기 때문에 표시되는 방식에 따라 따르게 나타난

다. 한편 휴대전화 등에서 표시 화면이 2바이트 문자로 10 ×10 행에 불과하기 때문에 컴팩트 HTML(i-Mode)이나 HDML(WAP)이라고 불리는 이동전화에 한정된 기능을 가진 표시 기술 언어가 사용되고 있다.

(5) 위치정보서비스

대표적인 모바일 인터넷의 새로운 서비스로 이동기기의 장점을 살린 GPS(Global Positioning System) 기술을 응용한 서비스를 들 수 있다. 고객의 위치에 따라 개별화되어 제공되는 쌍방향 정보의 제공은 분명 모바일 인터넷이 개척하고 있는 새로운 분야이다.

위치 정보는 서비스는 이동하는 지역에 따라 고유한 정보를 제공하는 서비스이다. 또한 I-point 네트워크에서는 자신이 메모를 붙인 지도나 위치 정보를 첨부하여 메일로 보낼 수 있고 위치정보를 다양한 서비스로 취급할 수 있다. 그리고 위치정보는 GPS 기능을 사용하거나 대상이 되는 단말기가 어느 기지국에서 전파를 받는가에 의해 측정할 수 있다.

(6) 기존 인터넷 컨텐츠 이식

모바일 인터넷 특성에 맞게 새로 개발된 정보들과 인터넷상에서 제공되고 있는 기존 다양한 정보를 이식하려는 시도도 이루어지고 있다. 이것은 모바일 상에서 정보 흐름도 일방적인 정보 전송이라는 형식에서 이용자의 능동적인 정보 검색이라는 쌍방향성을 획득해 나가고 있다는 것을 의미한다.

이러한 인터넷 정보의 본격적인 이식과정에서 다양한 서비스가 등장한다. 우선 이동 단말기로 정보검색을 하기에 불편하다는 현실을 반영하여 이용 편의성을 제공하는 서비스가 개발되고 있다.

(7) m-commerce

모바일, 인터넷, 물류, 결제 기능을 연결한 전자상거래도 활발하게 시도되고 있다. PC를 통한 인터넷과 가장 차별되고 있는 것은 컨텐츠의 유통이다. 모바일 인터넷을 통한 컨텐츠 유통이 활발한 것은 저작권문제가 자연적으로 해결되기 때문이다. 즉 휴대폰은 컨텐츠를 다른 곳으로 옮길 방법이 없기 때문에 불법복제에 따른 비용을 제외한 가격으로 컨텐츠 비즈니스를 할 수 있다. 또 모바일 인터넷을 통해 전자상거래가 활발한 것은 모바일 인터넷이 제공하는 과금

구조도 큰 기여를 하고 있다.

마) 모바일 인터넷 서비스 제공자

(1) i-Mode

일본의 최대 휴대전화 업체인 NTT-Docomo에 의해 1992년 2월에 시작된 서비스이다. 처음에는 주로 휴대전화를 이용한 문자 메시지 서비스에서 시작했으나 이후 본격적인 인터넷 접속 서비스를 제공함으로써 히트 상품으로 자리잡았다. 이 서비스는 가벼운 휴대전화에서 이메일을 송수신할 수 있고 홈페이지를 열람할 수 있게 되면서 폭발적인 인기를 모았다. 이용 가능한 정보의 종류와 수가 풍부한 것이 보급 속도에 박차를 가하고 있고, 뉴스 전달이나 온라인 뱅킹, 항공권 예약/판매 서비스가 잇따라 등장하고 있다.

- 가입자 추이

  니케이정보스트레터지 2000년 6월호에 의하면 i-Mode는 매월 계약자 수가 증가, 2000년에만 매월 전월 대비 20%의 증가세를 유지하고 있다.

- i-Mode 서비스의 진화 과정

  i-Mode의 서비스 초기에는 뉴스전송이나 간단한 정보검색에서 출발하여 지금은 온라인 뱅킹, 항공권 예약/판매, 신규용어검색, 캐릭터구입, 야후 정보의 제공은 물론이고 리얼타임 앙케이트 조서와 배너 광고까지 이루어지고 있다. 또한 일본 텔레콤의 네트경매, 견적 서비스를 제공하는 등 i-Mode 전용 사이트를 노린 비즈니스 모델로 출현하고 있다. 이러한 비즈니스 모델은 일반적으로 PC통신이나 ISP 서비스와 같이 정보 게시료를 비즈니스로 하고 있는 것은 대부분이다.

- i-Mode의 경쟁우위

  우선 압축형 HTML이라고 하는 C-HTML(compact HTML)을 채택하여 HTML로 작성된 기존 인터넷의 풍부한 컨텐츠를 손쉽게 전환할 수 있었다. 두 번째로 패킷 서비스를 일찍 도입하여 저렴한 요금으로 서비스할 수 있었다는 점이다. 마지막으로 “i-Mode의 비즈니스 모델”로 이야기되는 독특한 결제 시스템을 들 수 있다.

(2) EZweb과 J-스카이

1999년 4월 IDO그룹인 모바일 인터넷이 EZweb이고, 1999년 12월 J폰그룹이

서비스를 개시한 것이 J-스카이이다. EZweb과 J-스카이가 이용하는 언어인 WAP은 WML로 서버를 구축해야 하므로 아직 불편함이 있다. 게다가 WAP는 i-Mode보다 응용력이 뛰어나 다양한 사용자 인터페이스를 만들 수 있지만 이미 HTML로 작성된 인터넷상의 컨텐츠를 보는 것은 불가능하다.

그러나 WAP이 가진 장점은 여전히 매력적이다. 휴대용 전화용 컨텐츠 서비스에 사용되는 세계적인 표준으로 성장한다면 전 세계의 이용자를 대상으로 휴대폰용 홈페이지를 운영할 수 있다.

바) IMT-2000

(1) 개요

IMT-2000(International Mobile Telecommunication 2000)은 차세대고속광역 이동통신으로 국제 로밍과 음성, 텍스트, 영상통신을 가능하게 하는 2Mbps의 고속 데이터 통신을 실현하며 사용 무선 주파수는 1.885~2.2GHz 대이다. 무선통신 방식은 일본과 유럽이 추구하는 W-CDMA(Wideband Code Division Multiple Access)방식과 미국등에서 제안하는 CDMA-2000(Wideband cdmaOne)방식이 유력하다.

(2) CDMA

CDMA 방식은 주파수 대역을 분할하는 개념을 떠나서 전체 이용자들이 주파수 대역을 공유하고 각 통신을 PN부호라 불리는 신호의 위상 차에 의해 인식하게 된다. 3KHz의 주파수 대역을 사용하므로 음성, 데이터, 화상등 정보신호를 고속으로 처리할 수 있다. 정보 신호를 스펙트럼 확산(SS: Spectrum Spread)을 광대역으로 분산하는 동시에 다중 층의 전송 코드를 통해 무선 단말을 식별한다. 코드를 특정하기가 극히 어려우므로 도청이 곤란하다는 점도 특징이다.

(3) W-CDMA

CDMA와 동일하나 전송특성이 대폭개선 되었다. W-CDMA는 기존의 TDMA 방식에 비해서 다음과 같은 점에서 장점이 있다.

- 멜티레이트 서비스

  넓은 주파수 대역을 사용하므로 정보의 전송로가 넓어 이용자들에게 저

속에서 고속까지 다양한 전송속도를 제공 가능하다.

- 전송품질의 향상
  주파수 대역이 넓어 기지국과 단말간에 도달하는 전파의 식별 정밀도가 높다. 기지국과 단말간에 직선으로 전달되는 전파가 구조물 등에 반사되면 시간차가 생기는데 기지국이나 단말의 수신부에서 신호의 합성이 가능해져 결과적으로 신호강도가 증가한다.
- 시스템의 효율화
  W-CDMA에서는 다수의 이용자들이 1개의 채널을 동시에 사용한다. 즉 다른 사용자로부터 전파 간섭이 완화되어 주파수 효율적 이용이 가능하다.

(4) 정부정책

일본에 IMT-2000을 도입한 때의 무선 설비의 기술적 조건에 관해서는 1999년 9월에 전기통신 기술심의회로부터 차세대 이동통신 방식의 기술적 조건중이 ITU의 권고안에 포함된 IMT-2000의 무선전송방식 중 DS-CDMA(Direct Spread-Code Division Multiple Access : W-CDMA)와 MC-CDMA (CDMA-2000)가 선정이 되었다.

우정성은 무선 설비 규칙등 관련 규칙의 개정을 하고 2000년 3월 공포, 4월 시행이 되었다. 또 IMT-2000의 원활한 도입을 위해 사업화 및 무선국 면허에 관한 방침을 2000년 3월에 공표했다. 이후 2000년 4월부터 신청접수를 시작하고 2001년 중 도입을 결정하고 사업자의 조기결정을 목표로 하고 있다. IMT-2000 서비스의 2000년부터 2010년 말까지 시장규모는 42조 200억 엔에 이를 것으로 예측하고 있다.

4. 무선인터넷 표준화 동향

가. 무선 접속 기술

1) 블루투스

블루투스의 특징을 들면 다음과 같다.

• 2.45GHz ISM(Industrial Scientific Medical) 주파수 영역을 사용
  - 2.45GHz의 주파수는 FCC(Federal Communications Commission)의 라이센스를 받지않아도 되는 무료 주파수이다.
• 10M 거리 이내에서 최대 1Mbps의 속도로 음성 및 데이터를 교환.
  - 블루투스는 10M 거리 이내에서 최대 1Mbps의 속도로 음성 및 데이터를 교환하여 출력앰프 존재시 100M까지 확대 가능하다.
• 이용되는 애플리케이션
  - 전화기(셀룰러, 무선 등), 헤드셋, 컴퓨터(랜탑, 데스크탑 등등), 컴퓨터 주변장치(키보드, 마우스 등등), LAN장치, PDA, 디지털 카메라 등이 있다.

블루투스는 다양한 층의 복합적인 무선 네트워크 기술로 그 요구만큼이나 많은 구성 요소를 필요로 한다. 불루투스는 최종 목적은 하나의 칩에 블루투스의 모든 기능을 통합시키는 것을 목적으로 삼고 있다. 다음은 블루투스의 칩 관점에서의 발전 단계를 나타낸다.

• 5Chip (1998 이전) - CPU, RAM, Flash, Baseband, Radio
• 3Chip - Flash, Link Controller(Baseband + CPU + RAM), Radio
• 2Chip - Link Controller(Baseband + CPU + RAM), Radio
• 1Chip(현재일부)

블루투스는 Volume 1, Core, and Volume 2, Profile 등으로 표준화 영역이 나뉜다. Core 파트는 라디오기술, 베이스밴드 기술, 링크 관리자, 서비스 발견 프로토콜, 전송 계층과 각기 다른 통신 프로토콜에서의 상호 운용성에 대해 명시한다. 프로파일 파트는 각기 다른 형식의 블루투스 응용에 필요한 프로토콜과 절차들을 명시한다.

2) HDR

HDR은 코드분할 다중접속(CDMA)방식에 기반을 두고 음성과 데이터를 빠른 속도로 전송하는 시스템으로 퀄컴에서 개발하였다. HDR은 1.5Mbps(최대 2.4Mbps)로 데이터를 전송할 수 있는 데이터 전송 기술로 56Kbps모뎀에 비해 25배 이상 빠른 속도로 데이터를 전송할 수 있어 통신 사업자들은 이 기술을 기반으로 이동전화 사용자에게 초고속의 데이터 전송 서비스를 제공할 수 있다. 또한

HDR은 패킷화한 데이터를 최적화해 전송함에 따라 인터넷 접속, 전송 기능이 강화됐고 오디오, 비디오 등 멀티미디어 파일 전송률도 향상 됐다. 이 기술은 기존 cdmaOne 인프라 및 장비, 단말기 등에서 활용할 수 있어 비용을 절감할 수 있고, 데이터 전송 폭이 향상돼 한정된 지역에서 많은 사용자등에게 데이터를 전송할 수 이는 점이 특징이다. 특히 본격적인 IMT-2000 시스템의 모든 인프라가 갖춰지기 전에 고속 패킷 전송이 가능하다는 점에서 매우 고무적인 기술이다.

HDR의 서비스 활용 분야를 보면 다음과 같다. HDR은 2.4Mbps의 고속 데이터 전송이 가능한 구조로 IMT-2000 서비스의 무선 멀티미디어를 위한 인터넷 기술로 활용이 적합하다. 물론 특정 응용에 제한되지 않고 다양한 서비스의 지원이 가능하다.

단말기의 동향을 3가지로 나눌 수 있다. HDR/IS-95 서비스의 동시 지원이 가능한 듀얼 서비스 단말기, 그리고 HDR PDA와 HDR 단말기로 나뉠 수 있다. 듀얼 서비스 단말기의 경우 IS-95서비스의 통화를 하고 HDR 서비스의 경우 데이터 통신을 위한 무선 모뎀의 역할을 수행하며 HDR PDA의 경우 브라우저 등을 탑재하여 그 자체가 컴퓨터의 역할을 한다. 마지막으로 HDR 단말기의 경우 PC등에 연결하여 무선으로 고속 데이터의 송수신이 가능한 장비라 할 수 있다.

HDR의 표준화 진행 상황을 보면 이미 상용화를 위한 1/2차 테스트를 성공리에 마친 바 있으며, 표준 규격에 있어서 2000년 말에 완료 예정인 CDMA2000 Release B와 함께 Phase I의 표준화를 완료할 예정이다. HDR의 경쟁 표준을 보면 1XTREME가 있다. 1XTREMED은 모토로라와 노키아가 발표한 새로운 무선 표준 기술로 하향 최대 5.2Mbps 전송 속도를 갖는 기술로 현재 CDMA2000 1X 시스템의 구조에 포함하여 표준화 대상에 넣으려고 하고 있다. 그러나 현재는 HDR이 전략적으로 많은 지원을 받고 있다.

나. 무선인터넷 라우팅 기술

1) Mobile IP

Mobile IP는 3계층에서 IP 데이터그램의 이동성을 지원하기 위한 프로토콜로서 이동경로를 FA와 HA가 유지하고, 고정망 기반의 라우팅 제약을 터널링으로 극복하는 원리를 채택하고 있다. Mobile IP의 원리가 제정된 지는 상당히 오랜 시간이 지났으나 현재 실제로 네트워크가 구현이 되어 상용적으로 활발히 사용되는 곳은

거의 없고 연구의 목적으로 구현된 정도이다. 그러나 앞으로 무선 인프라가 유선 인프라 못지 않게 활용도가 높아질 것이며, 특히 4세대 네트워크와 관련되어 이동망에서 패킷 이동성을 지원하기 위한 표준으로 채택되고 있다. Mobile IP는 현재 IETF에서 Mobile IP WG가 구성되어 표준화가 진행중이다. 위에서도 언급하였지만 현재 네트워크 구조와 연계되어 표준화가 활발히 진행중이다. 그 예를 보면 마이크로 이동성의 지원, 보안, 인증, 권한, 계정 등에 관한 AAA 서비스의 적용 등을 들 수 있다.

다음은 현재 워킹그룹의 장단기 연구에 대한 목표와 Mobile IP WG RFC와 Draft의 제목과 내용을 약식으로 기술하여 표준화 현황을 정리한 것이다.

- 단기적인 연구 목표
  - 현재 IPv4 이외에 앞으로 사용하게 될 IPv6에서도 이동성을 지원한다.
  - 이동 노드와 사용자를 확인하기 위한 NAI를 사용한다.
  - Inter-domain 및 Intra- domain 이동성을 지원하기 위하여 모바일 IP가 어떻게 AAA를 사용할 것인지를 구체화한다.
  - 이동 노드를 위한 security framework/-trust 모델을 개발한다.
  - IPv4의 사설 주소 공간에 대한 해결책을 개발한다.
  - 셀룰라/무선 네트워크를 지원하기 위한 모든 요구조건을 문서화한다.
- 장기적인 연구 목표
  - 서브넷 안에서의 이동성을 지원할 수 있는 마이크로 mobility를 위한 IP 기반의 해결책을 구한다.
  - Diff-sev, Int-serv, RSVP 등을 사용하여 mobile IP 환경에서 QoS를 지원한다.
  - 위치 프라이버시를 보장한다.

2) MANET

MANET(Mobile Ad Hoc Network)은 기존 IP처럼 유선을 기반으로 한 망이 존재해야만 하는 것이 아니라 임의의 형태를 갖는 이동 노드와 이동 라우터들만으로도 네트워크 라우팅의 하부구조(Infrastructure)구성이 가능하도록 하는 것이다.

예를 들어, 사막같이 사람들이 밀집되어 있지 않은 곳, 혹은 선박이나 비행기같이 유선 기반 망이 구축되어 있지 않은 곳, 특히 군용 응용과 같은 환경에서 손쉽

게 망을 구성할 수 있는 장점이 있다. 위와 같은 임의의 형태를 갖는 애드 혹 망의 경우 고정망의 하부구조가 없기 때문에 움직이는 호스트가 패킷을 전달하는 라우터의 기능을 수행하여야 한다. 이때 기존의 라우팅 프로토콜을 MANET에서 사용하면 고정된 경로상에서 주기적인 메시지 교환 때문에 상당량의 대역폭을 낭비할 뿐만 아니라 라우팅 기능을 가지고 있는 이동 단말이 이동할 때 이에 대한 변화에 빠르게 대처할 수도 없다. 이러한 문제로 인해 MANET은 다음과 같은 라우팅 프로토콜들을 표준화한다.

DSR은 주기적인 라우팅 메시지가 없으므로 네트워크 대역폭의 오버헤드를 줄이고 전력을 보호한다. 단말의 이동과 같은 변화에도 빠르게 적용하며 변화가 발생하지 않은 주기 동안에는 라우팅 프로토콜의 오버헤드가 없다. 또한 DSR은 단방향링크의 존재에 대해서도 올바른 경로를 계산하도록 설계되었다. DSR의 작업은 크게 라우트 발견(Route discovery), 라우트 유지(Route Maintenance), 라우트 캐쉬(Route Cache) 그리고 라우트 발견시 피기백킹(Piggybacking on Route Discovery)으로 나눌 수 있다.

현재 MANET은 IETF의 MANET WG에서 표준화되고 있다. 현재까지 나와있는 것은 라우팅 프로토콜이 대부분이다. MANET WG는 현재 위와 같이 무선상에서 임의의 형태를 가지는 네트워크상에서 운용될 수 있는 라우팅 프로토콜을 표준화하고, 시장에 적용하고, 이후에는 수백 개의 라우터를 지원할 수 있도록 확장할 계획이다. 또한 표준화에 있어 무선 환경이 갖는 특성을 반영한다. 이후 부가적인 기능을 갖는 라우팅 프로토콜을 표준화할 계획이다.

MANET의 특징들로는 다음과 같다.

- MANET을 구성하는 각 노드들은 그들의 이동성에 제한이 없으므로 임의의 노드에 대해 자주 발생하는 링크의 설정이나 해체 시에도 네트워크의 동작에 심각한 영향을 미쳐서는 안됨.
- 무선 링크들은 유선 링크보다 대역폭이 낮으므로 대역폭의 손실이 적은 라우팅 프로토콜이 필요.
- 대부분의 노드들은 전력 사용에 제한을 받으므로 시스템 디자인할 때 전력 보호를 고려하여야 함.
- 패킷 조각들이 네트워크를 계속해서 떠도는 것을 조직적으로 막기 위한 프로토콜이 요구됨.
- 무선 네트워크에서는 단방향 링크가 발생할 수도 있기 때문에 단방향 링

크의 존재도 수용할 수 있는 라우팅 알고리즘이 필요.

• 유선 링크에 비해 쉽게 공격을 당할 수 있기 때문에 보안에 특별히 신경을 써야 함.

다. 무선인터넷을 위한 패킷 코어 네트워크

IMT-2000 핵심 망 기술은 모바일 IP를 이용하는 북미의 3G 무선 패킷 네트워크와 GSM 망과 연계하는 유럽의 GPRS로 구분할 수 있다. 3세대 무선 패킷 네트워크는 제3세대 ANSI-41네트워크 및 이를 기초로 한 CDMA2000 무선 접속 기술 및 단말기 등 세부 규격 작성을 위한 1999년 1월 결성된 3GPP2에서 표준화가 진행중이다. 3세대 무선 패킷 네트워크는 CDMA2000의 핵심 망 구조로써 회선 교환 망 과 패킷 교환 망이 분리된 형태를 가지며 패킷 교환 망은 기본적으로 이동 에이전트(Mobile Agent)를 이용하여 패킷의 이동성을 지원하고 보안, 인증 서비스를 강화하여 사용자로 하여금 인터넷과 사설 망의 서비스까지도 이용 가능하도록 하는 구조를 목표로 표준화가 진행중에 있다.

GPRS는 GSM 네트워크와 이를 기초한 WCDMA 접속 기술 단말기 등의 세부 규격을 작성하기 위한 표준하 기구인 3GPP에서 표준화가 진행중이다. GPRS도 역시 회선 교환 망과 패킷 교환 망이 분리된 형태를 가지며 2세대의 GSM(Group Special Mobile)망에서 UMTS로의 진화를 위한 과도기적인 2.5세대 패킷 교환 망이다. 유럽은 이미 현재 GPRS 망을 서비스중인 곳도 있다. 그러나 GSM/GPRS 기반의 핵심 마을 벗어나면 로밍이 되지 않는 단점이 이쓰므로 이를 해결하기 위한 GPRS 망에서 Mobile IP를 수용하는 'Mobile IP in UMTS', 'All IP' 형태를 단계적으로 정의하고 있다.

라. 무선인터넷 기타 응용 기술

1) 기타 무선 응용 컨텐츠 기술

현재 무선인터넷을 위한 응용 기술은 표준 응용 프로토콜 기술과 컨텐츠 기술로 나누어 생각할 수 있다. 특히 응용 프로토콜 영역의 기술을 보면 응용 계층을 영역으로 포함하는 WAP을 들 수 있다. WAP 프로토콜은 무선 영역에서 마이크로

브라우저로 효율적인 웹서핑을 가능하게 되는 구조로 되어 있다. 그밖에 무선인터넷을 위한 응용 계층의 프로토콜은 우세한 다른 표준이 없다. 그러나 무선컨텐츠의 기술 영역을 보면 상황이 달라진다. WAP 구조에서 무선컨텐츠의 표준은 wml, wmlscript로 대표되는데, 경쟁력 있는 다른 표준들을 보면 마이크로소프트의 m-HTML 형식으로 일본의 NTT-Docomo가 i-Mode라는 이름으로 서비스하고 있는 c-HTML 컨텐츠가 있다.

가) 마이크로소프트 ME(Mobile Explorer)

마이크로소프트는 ME는 소형 전화 단말기, PDA 등의 소형기기 등에서 사용될 수 있는 마이크로 브라우저를 뜻한다. ME의 특징을 보면 표준 컨텐츠로 m-HTML을 사용하며 표준 웹 프로토콜로서 http를 사용하게 된다. 이는 인터넷 표준을 그대로 지원하여 개발자의 노력 비용을 줄이고 시장 선점을 빠르게 하려는 노력으로 보인다. m-HTML은 인터넷 표준인 HTML 3.2의 부분집합으로 ME에서 지원된다. ME의 또 다른 특징은 느린 CPU와 한정된 메모리를 고려하여 가벼운 API를 사용하고 있으며 다양한 OS를 구축하기 위한 툴킷을 제공하고 있다. 특히 마이크로소프트는 모바일 익스플로러의 기능에 m-HTML 뿐만 아니라 WAP의 컨텐츠 역시 파싱이 가능한 구조를 제시하고 있다.

나) W3C(c-HTML)

c-HTML은 1994년 미국의 MIT, 유럽의 INRIA, 일본의 게이오 대학 등이 중심이 되어 전세계의 300개 이상의 업체/학계가 참여하여 표준화한 결과이다. 현재 일본 최대 휴대전화 사업자인 NTT-Docomo의 휴대 정보서비스인 i-Mode 서비스는 표준 컨텐츠로 c-HTML을 사용하고 있는데 이를 WAP의 wml, ME의 m-HTML에 대응되는 기술로 인터넷 표준인 HTML 4.0을 일부분에서 일부 기능을 추가하거나 삭제한 특징을 가지고 있다.

특히 c-HTML을 파싱하는 마이크로 브라우저는 인터넷 애플리케이션 소프트웨어 개발업체인 액세스(Access)가 compact NetFront라는 이름으로 개발하였다. 세스는 후지쯔, 마쓰시타, 미쯔비시, NEC, 소니 등과 c-HTML을 HTML의 서브넷으로 공동 개발해 1998년 4월 인터넷 표준 기구인 W3C에 제안하였다. c-HTML의 특징을 잠깐 보면, 기존 HTML의 일부분으로 WAP과는 달리 게이트웨이의 필터 기능을 필요로 하여 컨텐츠를 변환할 필요가 없으며, 개발이 쉬워 개발자에게

부담이 적고 시장의 응용 확장이 용이하며, 서비스를 위한 초기 투자 비용이 적은 장점이 있다.

i-Mode는 패킷 망에서 i-Mode를 운영하고 있다. 따라서 과금은 패킷 전송으로 매겨지게 된다. 특히 유로 사이트의 서비스를 사용할 경우 과금 징수를 NTT-Docomo가 대행하여 서비스 수수료를 공제한 후 컨텐츠 제공자에게 나머지를 돌려준다. 컨텐츠 제공자는 컨텐츠 개발에만 집중할 수 있는 매력이 있다. 물론 사용자 역시 데이터 송수신에 해당되는 만큼만 지불할 수 있어 서비스 측면에서 효율적이다.

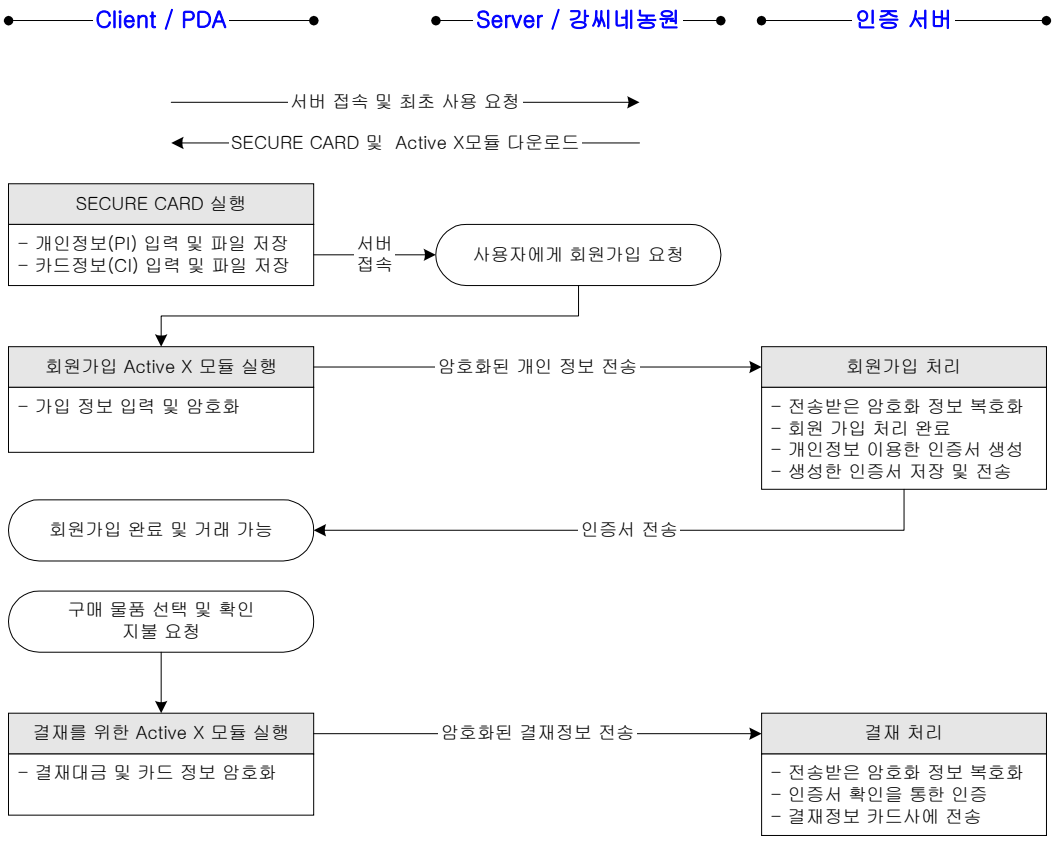
무선인터넷의 표준 컨텐츠는 크게 프로토콜의 측면에서는 HTTP와 WAP의 대결로 압축되고, 컨텐츠 역시 WAP의 wml, HTML 진영과 HTML 기반의 m-HTML, c-HTML로 압축된다.

제 3 장 연구개발수행 내용 및 결과

제 1 절 시스템 설계 개요

본 시스템은 무선 단말기 PDA를 이용하여 언제어디서나 농산물 구매가 가능하도록 전자상거래를 구축한다. 이 때 개인 단말기라는 특징을 고려하여 보다 안전하고 효율적인 거래가 이루어질 수 있도록 시스템을 구축하였다.

이 시스템은 m-commerce 실현을 위한 상거래용 웹사이트, 인증에 관한 기능을 담당하는 인증서버, 실제로 구매를 하는 개인 사용자의 PDA 단말기로 구성되어 있다. 다음 그림은 각 구성요소간의 관계와 수행절차에 대한 것이다.



[그림 42] 시스템 구성요소간 관계 및 시스템 개요

제 2 절 시스템 개발 환경

1. 전자상거래 서버

무선 환경에서 접속이 가능한 농산물 전자상거래 서버 역할을 하는 홈페이지를 구축한다. 회원가입 및 로그인, 상품 주문에서 구매결정에 이르기까지 일련의 기능을 포함하는 서버를 구축한다. 본 연구에서는 신용카드 기반 기반의 결재 처리를 기본 가정으로 한다.

1) 개발언어 및 프로그램

- 운영체제

  웹 서버의 운영체제로는 NT계열(Windows NT, Windows 2000), Unix계열(Unix, Linux)등을 들 수 있으나 클라이언트에서 사용되는 응용 프로그램등의 환경을 고려하여 Windows 2000으로 선택하였다.

- 웹 서버

  전자상거래용 홈페이지 제공을 위해 전 세계 웹 서버의 절반 이상을 차지할 만큼 뛰어난 성능을 갖춘 범용적인 프로그램으로 거의 모든 운영체제에서 사용할 수 있는 아파치(apache) 웹 서버를 이용했다.

- 데이터베이스

  홈페이지의 정보(예:물품정보)는 물론 가입되는 회원들에 대한 정보, 물품구매에 대한 관련정보(구매리스트 및 결재정보) 등을 저장하기 위한 데이터베이스로는 MySQL을 이용한다.

2. 인증 서버

개인 사용자가 PDA를 통해 상거래 페이지에 접속하여 거래를 할 경우, 회원가입은 물론 물품구매과 같은 동작을 수행하게 된다. 이때 사용자의 개인정보 및 신용정보등은 암호화되어 서버로 전송이 되는데 이때 클라이언트의 암호화한 정보 수신을 담당하는 서버로 인증서버라 하여 전자상거래 서버와는 별도로 동작하게 된다. 이는 암호화된 정보의 복호화 기능은 물론, 인증서 생성과 클라이언트로의 인증서 전송등

을 담당하여, 보안과 관련한 기능을 담당하게 된다.

1) 개발언어 및 프로그램

■ Visual C++ 6.0

- 인증을 담당하는 서버 개발에 사용하며, 소켓통신을 이용한다.

3. 클라이언트

개인 PDA 단말기를 이용하여 상거래 서버에서 관련 프로그램(SECURE CARD)와 거래를 진행시 필요한 Active X 컨트롤등을 다운받아 사용하게 된다.

1) PDA

PDA는 외형적으로 Computer의 기본이 되는 CPU, Memory, OS를 갖추고 있고, 각각의 OS를 기반으로 하는 다양한 Application과 주변 기기를 갖추고 있다. 입력방식은 Touch Screen을 통한 필기 인식을 사용하고 있다. 필기 인식이 가능하므로 주소록, 일정관리, 계산기 등의 개인정보관리 기능(PIMS)으로 쓸 수 있고, 노트북으로 가능한 대부분의 작업을 할 수 있다.

PDA는 보통 입력장치로 Pen을 사용하는 소형 컴퓨터(Small Computer)들을 의미하지만 제작 회사 또는 언론에 의해 다른 종류로 구분이 되기도 한다. 3Com Palm Computing사의 제품들은 파일럿(Pilot) 또는 팜(Palm)이라고 부르고, Microsoft사의 WinCE OS를 사용하는 제품들은 Keyboard를 사용하는 HPC(Handheld PC), Pen을 사용하는 PPC(Palm-Sized PC, WinCE 3.0버전 출시 이후로는 Pocket PC)로 구분하고, HP의 일부 제품들과 Psion사의 Psion 시리즈를 PalmTop이라고 부른다. 그리고 Nokia9000 시리즈와 같이 Mobile Phone과 PDA가 결합된 형태의 제품들을 Smart Phone 이라고 하는데, 이것이 가장 이상적인 결합체 같이 보이긴 하지만 Software가 부족하다는 단점이 있다. 일부 기종들은 독립적인 활동을 보장받지만 대부분의 PDA들은 PC Companion류의 제품들로 Cradle이라고 불리는 장치를 통해 Desktop에 Data를 보관하기 때문에 PC와 함께 사용할 수 없다면 다소 불편할 것이다. 물론, 기본 제공 Program외에도 새로운 Program을 설치하여 사용할 수도 있다.

본 연구에서는 PDA중 가장 많이 사용되고 있는 iPAQ Pocket PC를 이용하였다.

[표 9] iPAQ Pocket PC

iPAQ Pocket PC H5450		
	크기 및 무게	138.0 mm X 84.0 mm X 15.9 mm, 206g
	프로세서	Xsale PXA 250 400Mhz
	디스플레이	반투과성 TFT LCD, 3.8 Inch / 96 mm, 65,536 Color
	배터리	Li-ion 720mA
	운영체제	Microsoft PocketPC 2002
	메모리	ROM: 48M RAM: 64M

2) 개발언어 및 프로그램

- eMbedded C++ 3.0
  - Active X 컨트롤 개발에 사용한다.
  - 회원가입과 구매를 결정시 개인/신용 정보의 안전한 전송을 담당한다.
- Visual C++ 6.0
  - SECURE CARD 개발에 사용된다.
  - 단말기에 저장되는 개인정보 및 신용정보의 입력을 담당한다.

3) Active X

Active X는 Microsoft에서 제안한 컨트롤 기술이며 Visual Basic 및 Visual C++등의 개발 환경을 제공한다. ActiveX는 마이크로소프트사에서 COM, DCOM 기술에 인터넷 기술을 접목하여 개발한 개념으로 인터넷을 지원하는 프로그램이다. 요즈음 Application 프로그램의 개발은 ActiveX로 한번 프로그래밍하여 인터넷에서도 Local Application과 똑같이 동작하도록 하는 것이 추세이다. ActiveX 컨트롤의 확장자는 ocx이다. 이 파일은 한번 작성하여 일반 Application과 웹에서도 사

용이 가능하게 된다. ActiveX Control은 암호화 모듈을 포함하고 있으며, 회원가입이나 결재요청과 같은 과정을 수행할 경우 해당 Control을 사용 가능하도록 처음 접속시 사용자가 다운로드를 통해 PDA내에 설치가 되고 PDA Registry에 등록되게 된다.

EVC++을 이용한 PDA용 ActiveX control을 제작하기 위해서는 먼저 같은 이름을 가진 PC용 ActiveX Control이 PC의 Registry에 등록되어 있어야 한다. PC용 ActiveX Control이 등록된 상태에서 같은 이름의 PDA용 ActiveX Control을 제작하게 되면 같은 CLASSID를 갖는 PDA용 ActiveX Control을 만들 수 있다. 이와 같이 하는 이유는 EVC++을 이용하여 제작한 ActiveX Control은 Compile후 자동으로 PDA Registry에만 등록되어 Desktop에서 PDA Application 개발 시에 PDA Registry에 등록된 ActiveX Control을 PC에서 사용할 수 없기 때문이다. 그러므로 같은 ID를 갖는 PC용 ActiveX Control을 제작하여 PDA Application에 Embedded 될 수 있게끔 한다.

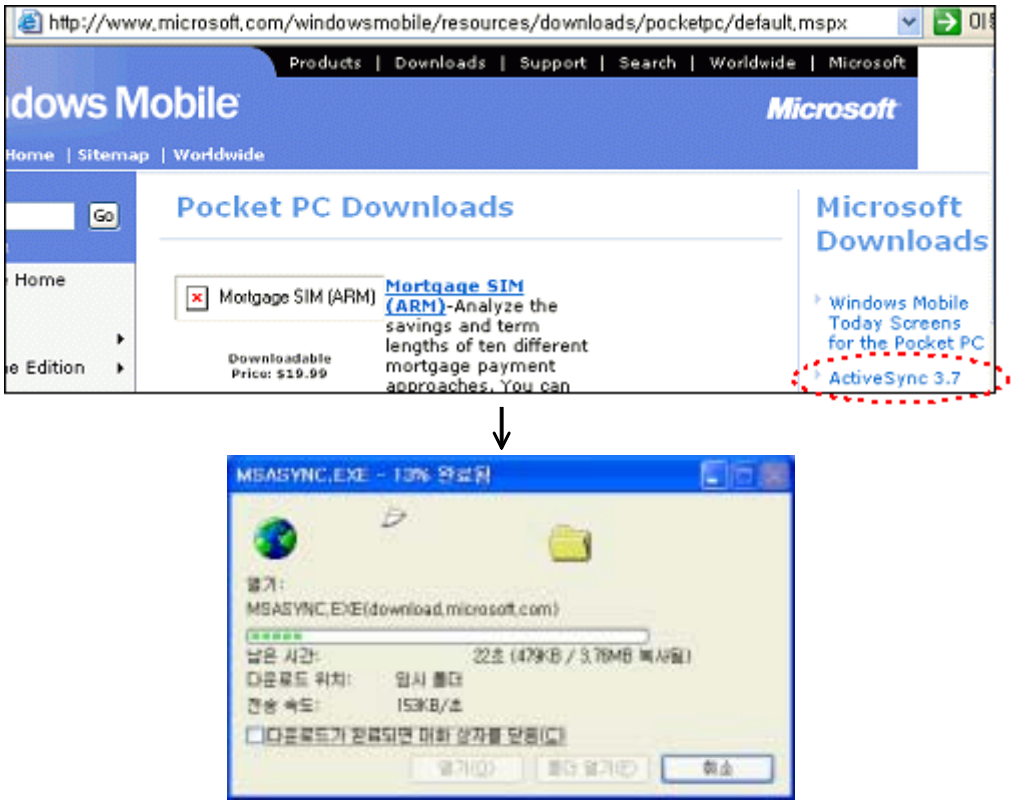
4. 개발용 프로그램 설정

가. Microsoft ActiveSync

데스크탑 컴퓨터와 PDA 단말기는 크래들이라는 별도의 장치를 이용하여 상호 통신이 가능하다. 예를 들어 PDA에 응용 프로그램 설치를 하고자 할 경우 일반적으로 CD등을 통해 배포를 하게 되는데, 데스크탑에서 응용프로그램 설치 프로그램을 실행하게 되면 크래들을 통해 설치 정보들이 PDA 단말기로 전송이 되게 된다. 이때 크래들은 물리적인 연결만을 담당하며, 데스크탑과 PDA에 대한 실제적으로 연결 설정을 담당하는 프로그램이 Microsoft사에서 제공하는 ActiveSync이다. 보고서 작성 기준으로 현재 버전은 3.7이 제공되며 본 연구 개발 진행시에는 버전 3.6을 이용하였다.

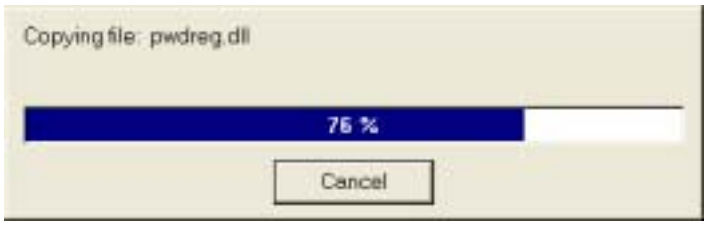
■ 프로그램 구하기

Microsoft사(http://www.microsoft.com)에서 무료로 제공해주는 프로그램을 다음 그림의 과정을 거쳐 다운로드를 받는다.



■ 설치과정

다운받은 프로그램은 다음 그림과 같은 단계를 거쳐 데스크탑에 설치된다.

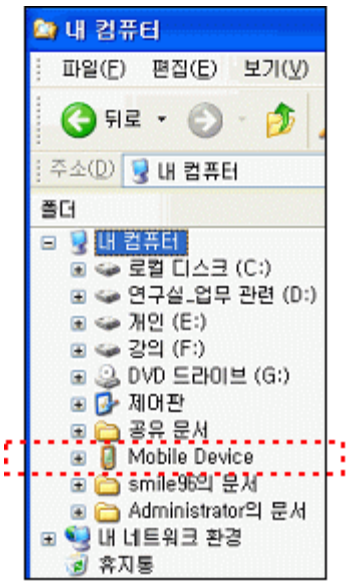


■ 기능 및 사용

설치가 완료되면서 ActiveSync는 COM 포트에 연결되어 있는 크래들을 통해 PDA를 인식하게 되며, 데스크탑은 PDA에 접근이 가능하게 된다. 또한 데스크탑에서 COM 포트를 통해 PDA로의 자료 전송이 가능하게 된다.

연결 설정이 완료된 후 다음 그림과 같이 데스크탑에 연결되어 있는 PDA를 탐

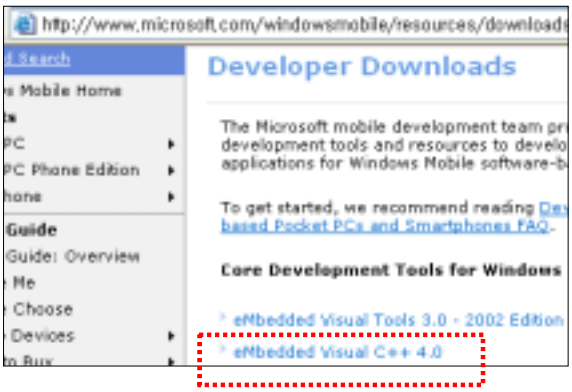
색기등을 통해 확인할 수 있다.



나. eMbedded VC++

PDA와 데스크탑는 서로 다른 CPU를 사용하고 있다. PDA에도 여러 종류의 CPU를 사용하고 있다. PDA 어플리케이션 개발을 위해서는 각각의 CPU에 맞는 SDK가 있어야 한다. 이를 위한 제작툴중 하나인 eMbedded VC++을 이용하여 본 시스템을 개발한다.

■ 프로그램 구하기



■ 설치과정

다운받은 프로그램은 다음 그림과 같은 단계를 거쳐 데스크탑에 설치된다.

제 3 절　시스템 설계 및 구현

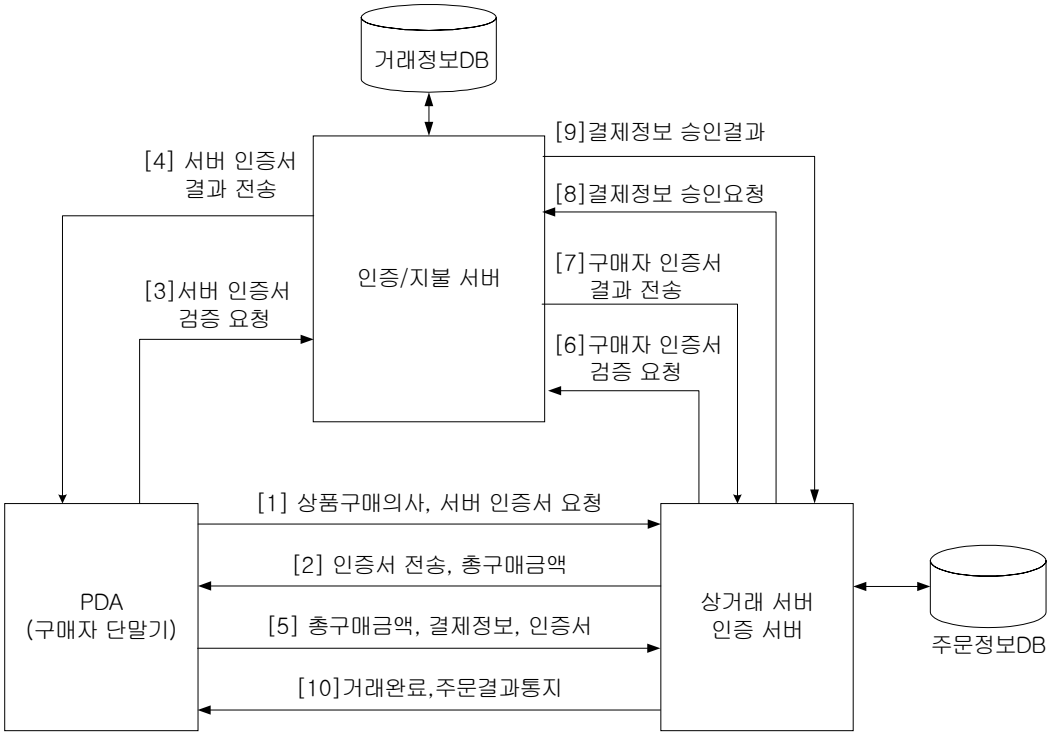
본 시스템은 무선 단말기 PDA를 이용하여 언제 어디서나 안전하게 농산물 구매가 가능하도록 전자상거래를 구축한다. 이때 개인 단말기라는 특징을 고려하여 보다 안전하고 효율적인 거래가 이루어질 수 있도록 시스템을 구축하였다. [그림 43]과 같이 본 시스템은 m-commerce 실현을 위한 상거래용 서버 역할을 하는 웹사이트, 인증에 관한 기능을 담당하는 인증서버, 실제로 구매를 하는 개인 사용자의 PDA 단말기로 구성되어 있다. 또한 본 시스템은 결재수단을 신용카드로 기본 가정한다. 이때 신용카드사의 지불게이트웨이와의 승인처리를 위한 통신에 대한 구현은 본 시스템에서는 이루어지지 않는다.

단말기를 이용하여 상거래 서버에 접속한 구매자는 회원가입 및 안전한 구매를 위해 SECURE CARD라는 별도의 프로그램을 다운로드를 받게 된다. SECURE CARD는 구매자에 대한 개인정보와 구매에 필요한 신용카드 정보등을 암호화하여 PDA에 저장함으로써, 개인 단말기라는 특수성을 고려한 시스템 구축이 이루어지게 한다.

SECURE CARD를 이용한 정보저장이 완료된 후 구매자는 원활한 전자상거래를 위해 회원가입을 한다. 회원가입시 단말기에 저장되어 있던 개인정보를 이용하여 인증서버에 암호화된 형태로 전송되게 되며, 인증서버는 회원가입 절차를 수행한 후 인증서를 생성하여 구매자 단말기로 전송하여 인증서를 이용한 전자상거래 시스템을 구축하게 된다.

구매자는 구매하고자 하는 물품 목록을 선택한 후 지불요청을 수행하게 된다. 구매정보(물품, 가격, 배송정보 등)등은 상거래 서버에 기록되며, 지불정보(금액, 카드정보)는 인증서버에 암호화된 형태로 전송되게 된다.

아래 그림은 본 연구에서 제안한 시스템의 전체 흐름도를 나타낸 것이다.



[그림 43] 전체 시스템 흐름도

[단계 1,2] 사용자는 상품 검색 및 선택을 하여 인증서와 구매정보등의 내용을 상거래 서버와 공유된 키로 SECURE CARD를 이용하여 암호화하여 전송한다. 상거래 서버는 상품 내역을 복호화하고 상품 내역을 확인한다.

[단계 3,4] 인증서 서버는 사용자의 인증서를 검증한다.

[단계 5,6,7] 인증이 검증되면 상거래 서버와 공유한 키로 SECURE CARD를 이용하여 암호화한 개인정보를 전송한다. 상거래 서버는 키를 이용하여 개인정보를 복호화하여 저장한다.

[단계 8,9] 상거래 서버는 사용자와 지불 게이트웨이와 공유된 비밀키로 암호화된 카드정보, 타임 스탬프를 상거래 서버와 지불 게이트웨이와 공유된 세션

키로 암호화하여 전송한다. 카드 정보는 상거래 서버는 알지 못하고 사용자와 지불 게이트웨이만 볼 수 있도록 하였다. 이 단계는 본 연구에서는 기본 가정으로 설정한다. 지불 게이트웨이는 신용카드 회사등을 생각할 수 있다.

1. 전자상거래 웹사이트

개인 무선 단말기를 통해 언제 어디서나 접근 가능한 농산물 전자상거래 구축을 한다. 즉, 유선환경과 무선환경의 조화와 함께 접근 용이성이 탁월한 m-commerce가 구축되게 된다. 이때 사용자 개인 단말기라는 특징을 고려하여 SECURE CARD라는 별도의 어플리케이션을 이용하여 개인 정보의 반복 입력의 불편함을 해소하며, 상거래 진행시 입력되거나 저장되어 있는 정보들은 별도의 암호화의 과정을 통해 상거래 서버와 통신을 하게 된다.

농산물 전자상거래를 위한 홈페이지를 구축함으로써, 무선 단말기를 이용해 언제 어디서나 접근이 가능하게 된다.

2. 인증 서버

회원가입의 경우 가입을 위한 개인정보는 암호화과정을 통해 암호화되어 인증서버로 전송되게 된다. 인증서버는 사용자가 보내준 암호화된 정보를 복호화하여 데이터베이스에 저장한 후 이 정보를 이용하여 인증서를 생성하여 사용자에게 재전송하게 된다. 또한, 추후 이 사용자가 구매를 하고자 할 경우 신용카드 및 구매정보 역시 암호화된 형태로 인증서버로 전송되게 된다.

이 시스템은 신용카드 결재를 기반으로 하기 때문에, 카드회사와의 연계가 필요하지만, 본 연구수행 중에는 카드회사와의 연계의 어려움이 있으므로, 인증서버에서 결재정보를 수신한 후 카드회사의 프로토콜 형식에 맞는 데이터 전송이 이루어져 결재에 대한 승인이 이루어짐을 가정으로 한다.

3. SECURE CARD

PDA는 이동성이 강한 정보기기로 기존 유선상의 정보기기에 비하여 정보입력 작업이 원활하지 않은 입력 구조를 가지고 있다. 따라서 PDA기반의 결제 솔루션을 제공하는데 거론될 수 있는 문제가 사용자와의 인터페이스이다. 이동기기의 정보입력에 대한 불편함을 해결하고 안전한 결제 솔루션을 제공하기 위하여 SECURE CARD를 설계하였다.

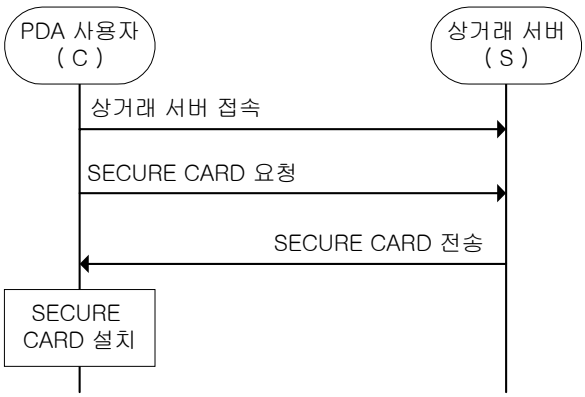
SECURE CARD는 사용자가 정보를 입력하면 그 정보를 PDA에 저장하여 모든 상거래 서버와 거래할 때 사용할 수 있도록 구성하였다. 또한 PDA 분실시 개인정보 보호를 위해 입력된 정보는 안전한 블록 암호 알고리즘(대칭키 암호 알고리즘)을 이용하여 암호화하여 저장된다. 일반적으로 인증을 위해 대칭키 암호 알고리즘과 공개키 암호 알고리즘을 사용한다. 대칭키 암호 방식은 비밀키가 공유되었다는 전제를 바탕으로 인증 및 보안 서비스를 제공하지만, 인터넷과 같은 공개 네트워크 상에서는 사전에 안전하게 키를 분배하는 것이 매우 어렵기 때문에 공개키 암호 방식을 이용하기도 한다. 공개키 암호의 경우 대칭키 방식에 비해 시간이 오래 소요되는 단점이 있다.

본 연구에서는 PDA와 같은 무선단말기의 CPU나 밧데리 등의 한계를 고려하여 대칭키 암호 알고리즘을 이용한 암호화 과정을 수행하며, 암호키의 보호와 안전한 인증을 위해 타임 스탬프를 이용한 인증 절차를 수행한다.

본 연구에서 제안하는 SECURE CARD는 설치 모듈, 거래정보 관리 모듈, 암·복호화 모듈로 구성된다.

가. SECURE CARD 설치 모듈

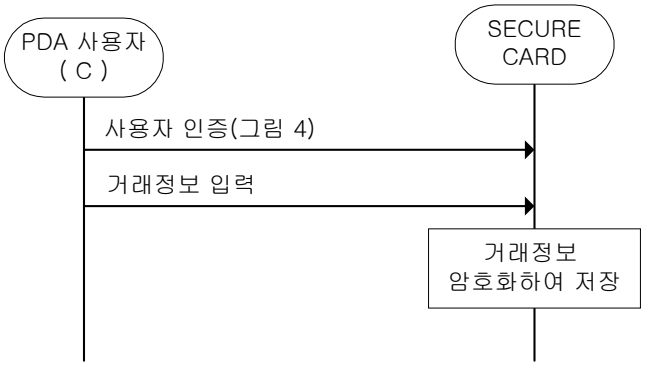
사용자는 안전한 거래를 위하여 m-commerce를 이용하고자 할 때 전자 상거래 서버로부터 SECURE CARD를 다운받아 설치하여야 한다. 한번 설치가 되면 SECURE CARD는 제휴된 모든 m-commerce 환경에서 사용이 가능하다. 설치 절차는 [그림 44]와 같이 설치된다.



[그림 44] SECURE CARD 설치

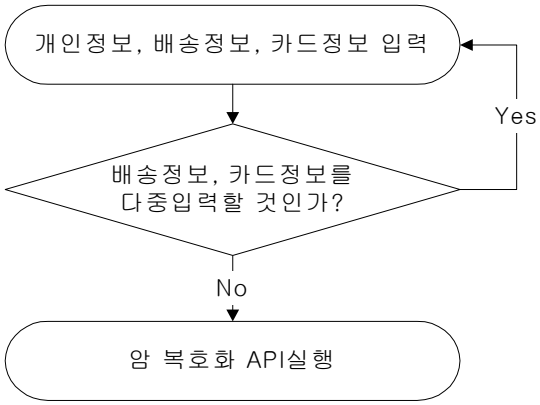
나. SECURE CARD 거래정보 관리 모듈

거래정보 관리는 온라인상에서 회원가입 또는 상거래 거래시 필요한 정보의 활용을 위해서 개인정보, 배송정보, 카드정보의 필수 항목을 관리한다. 개인정보에는 ID, 인증코드, 이름, 주민등록번호, E-mail 주소, 전화번호를 필수항목으로 하여 사전에 입력받는다. 사용자는 자신이 소유하고 있는 카드정보도 PDA에 미리 저장한다. 카드에 대한 필수 항목은 카드번호, 유효기간(년, 월)으로 설정하였다. [그림 45]는 거래정보 관리를 나타낸 것이다.



[그림 45] SECURE CARD 거래정보관리

SECURE CARD는 사용자로부터 입력받는 개인정보, 배송정보, 카드정보를 암호화하여 PDA에 저장하며 복호화 작업도 수행한다. 암·복호화 모듈은 다른 암·복호화 알고리즘을 추가적으로 확장할 수 있다. 암·복호화 모듈은 [그림 46]과 같이 입력받은 개인정보, 배송정보, 카드정보를 사용자가 초기에 입력한 인증코드를 이용하여 암·복호화 기능을 수행한다.



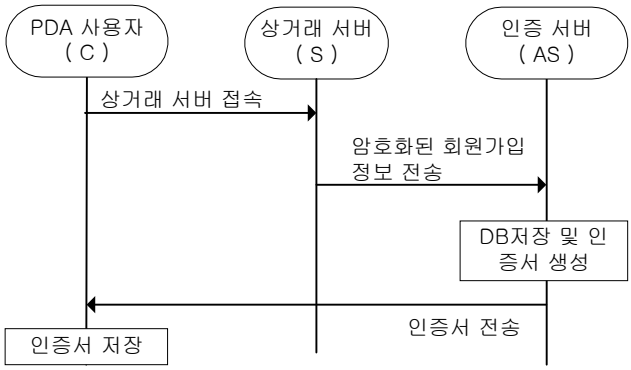
[그림 46] 암·복호화를 통한 정보의 저장모듈

4. Active X 모듈

홈페이지에 접속한 사용자는 원활한 물품구매를 위해 관련 모듈을 다운받아 개인 PDA에 등록하게 된다. 이때 등록한 Active X는 회원가입과 지불처리를 위한 모듈로 구성된다.

가. 회원가입 Active X 모듈

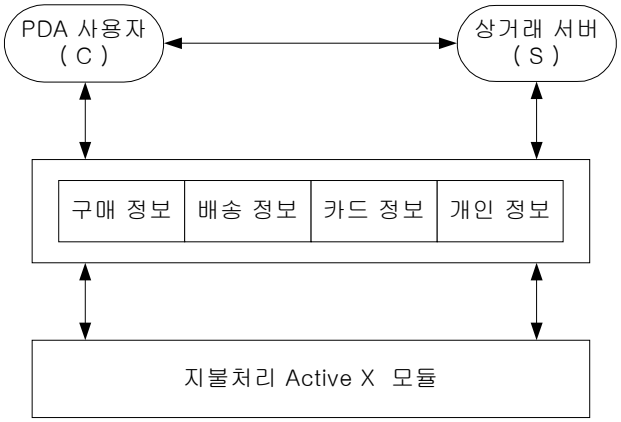
홈페이지에서 회원가입 메뉴를 선택할 경우 Active X 모듈이 실행되게 되는데, 회원가입시 필요한 사용자 정보들은 SECURE CARD를 통해 PDA에 이미 저장되어 있던 개인정보들을 이용하게 되므로, 별도의 중복입력이 필요없게 된다. 이 모듈은 인증서버에 접속하여 가입정보들을 암호화하여 전송하여 주고, 인증 서버를 통해 인증서 형식의 인증정보를 다운받게 된다. 추후 이 인증서는 지불처리시 이용되게 된다.



[그림 47] 회원가입 모듈

나. 지불처리 Active X 모듈

사용자가 상품을 구매 요청하는 경우 서비스 제공자는 구매정보를 Active X 컨트롤을 이용하여 PDA 사용자의 SECURE CARD로 전송한다. PDA 사용자는 구매정보를 확인한 다음 자신의 배송정보, 카드정보를 선택하여 Active X 컨트롤을 이용하여 서비스 제공자의 SECURE CARD로 전송한다. 배송정보와 카드정보는 암·복호화 모듈에 의해서 암호화되어 전송된다. 상거래서버도 사용자에게 전달할 데이터가 있을 경우 사용자처럼 Active X 모듈을 이용하여 암호화하여 전송한다. [그림 48]은 지불처리 Active X 모듈을 표현한 것이다.



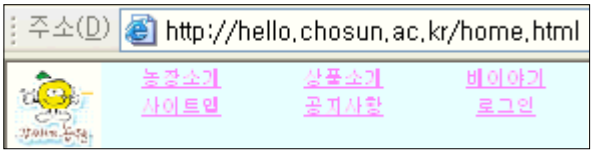
[그림 48] 지불처리 Active X 모듈

제 4 절 연구 결과

1. 전자상거래 웹사이트 구축

본 시스템은 현재 배를 재배하고 판매하고 있는 농장과의 직접 연결을 통해 보다 저렴한 가격과 신뢰성 있는 거래가 가능하도록 전자상거래 웹사이트를 구축하였다. 무선 단말기를 통한 입력의 불편성을 고려하여 홈페이지는 구매 위주의 상거래가 가능하도록 게시판과 같은 기능을 배제하였다.

다음은 홈페이지에 구성된 메뉴를 나타낸 것이다.



가. 농장소개

본 연구를 위해 연계되어 있는 농장에 대한 소개로, 구매자들에게 신뢰성을 제공해줄 수 있게 된다.

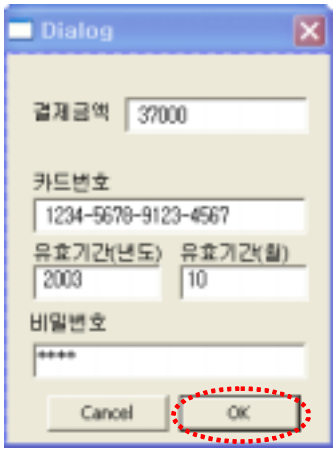
나. 상품소개

등록되어 있는 상품정보를 볼 수 있는 메뉴로, 상품보기/주문하기/ 주문내역 확인의 기능을 포함하고 있다. 실제로 구매자가 전자상거래를 할 경우 본 메뉴를 통해 물품 구매가 가능하게 될 것이다.

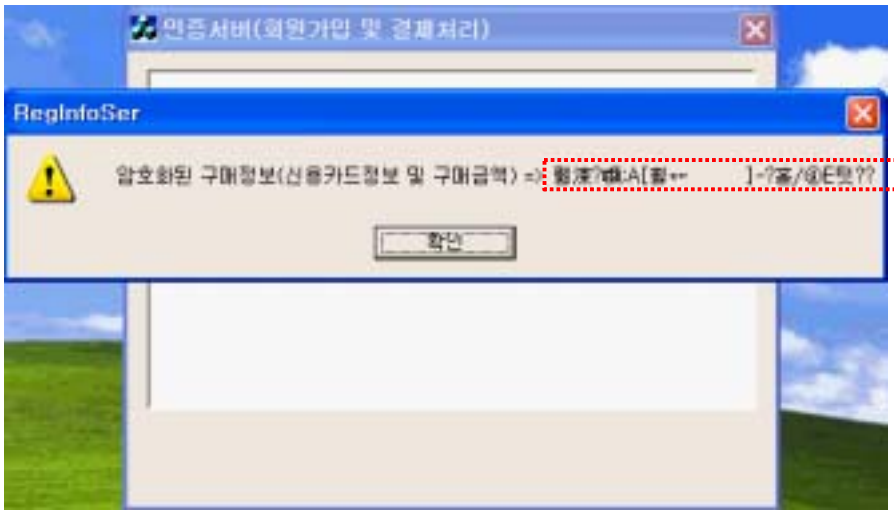
구매자가 원하는 물품을 선택한 후 주문요청을 하게된다. 구매자에 대한 정보와 배송정보등을 입력한 후 구매자는 신용카드 결재를 요청하게 된다. 본 연구에서는 신용카드 거래를 기반으로 하는데, 결재를 위한 신용카드 정보는 SECURE CARD를 통해 이미 PDA에 저장되어 있으므로, 거래시 별도의 입력이 필요가 없게 된다. 저장되어 있던 신용카드 정보를 읽어들인 후 결재정보는 인증서버로 암호화된 형태로 전송되게 된다.

구매하고자 하는 물품을 선택한 후 지불처리를 하는 전 과정을 설명한다.

<결제확인>을 선택할 경우 결재정보 전송을 위한 모듈이 수행되며, 이때 전송되는 정보는 암호화 과정을 통해 안전하게 전송되게 된다.



좌측 그림은 신용카드 결재를 위한 Active X 모듈 실행 화면이다.
<OK>버튼을 클릭함으로써 신용카드 정보와 결재금액정보는 암호화 과정을 거치게 되며, 이렇게 암호화된 정보는 인증서버로 전송되게 된다. 아래 그림은 인증서버가 수신한 암호화된 결재정보를 나타낸 것이다.
이때 신용카드정보는 SECURE CARD를 이용해 구매자가 이미 등록해놓은 정보로, 개인 단말기에 안전하게 저장되어 있는 정보들이므로 사용자가 직접 입력할 필요가 없다. 즉, 사용자의 편의성을 도모하게 된다.



결재정보는 고객의 카드정보의 보호를 위해 서버에 저장하지 않으며, 위의 그림과 같이 전송받은 정보는 카드회사의 프로토콜에 맞춰 데이터 형식을 갖추어 전송되게 된다.

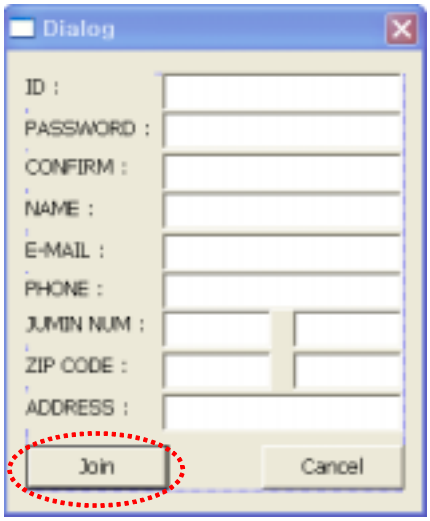
다. 배이야기

판매되는 농산물에 대한 일반적인 정보를 제공한다.

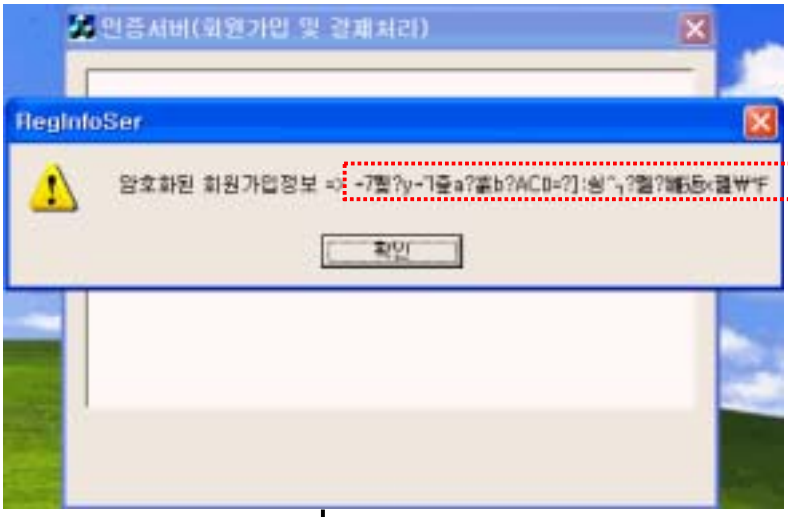
라. 회원가입

전자상거래의 원활한 이용을 위해 개인 사용자들은 개인정보를 입력한 후 서버와의 접속을 시도하며, 이때 사용자가 입력하는 개인정보들은 별도의 암호화 과정을 거쳐 안전하게 전송되게 된다.

회원가입을 담당하는 Active X 모듈이 아래와 같이 실행되며, 가입정보를 입력한다.



<join>버튼을 선택하면, 가입정보는 암호화 과정을 거쳐 서버로 전송된다. 아래그림은 수신된 암호화된 정보이다.



가입정보는 복호화 과정을 거쳐 데이터베이스에 저장되며, 서버는 타임스탬프 등을 이용하여 인증서 형태의 정보를 생성한다. 이렇게 생성된 인증서는 가입요청자에게 전송되어 가입자의 PDA 단말기에 저장되게 된다.

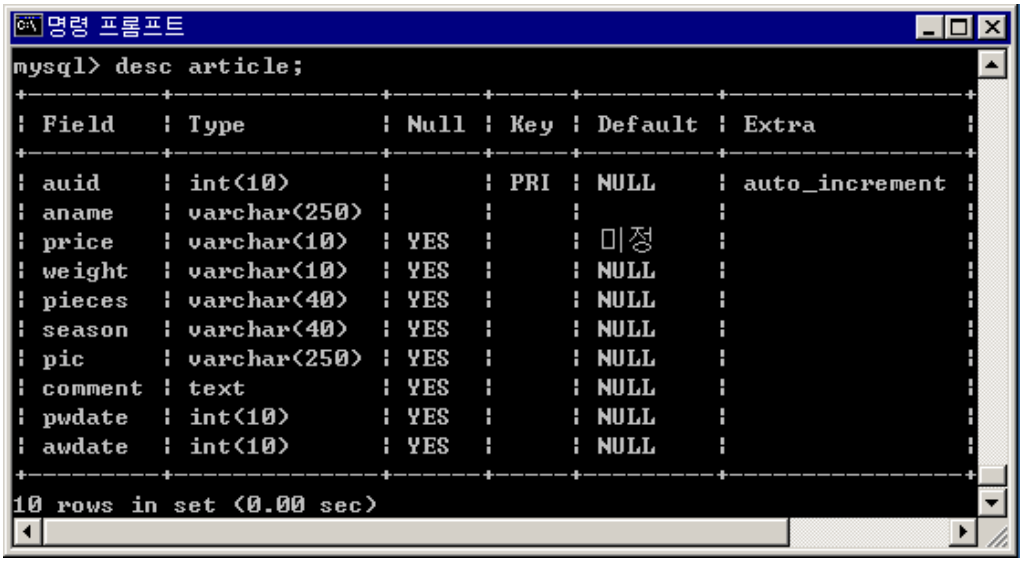
위에서 살펴본 바와 같이 전자상거래 시스템 구축의 한 과정인 회원가입 기능을 통해 고객의 원활한 접근이 가능하게 되며, 이 때 가입시 등록하는 정보는 암호화 모듈을 거침으로써 보다 안전하게 전송되게 된다.

2. 전자상거래 서버용 Database 구축

선택한 4가지의 테이블은 가장 기본적인 기능 구현을 위한 테이블 구성이다.

웹사이트 구축시 필요한 상품정보는 물론 회원정보를 포함한 각종 자료를 저장하기 위한 데이터베이스를 구축하였다. 위의 그림에서 선택한 4가지의 테이블을 제외한 나머지 테이블은 본 웹사이트에 대해 게시판의 기능을 추가할 경우 사용되는 테이블이며, 본 연구에서 가장 중요시되는 테이블은 등록물품 테이블, 회원정보 테이블, 구매정보 테이블등을 들 수 있다.

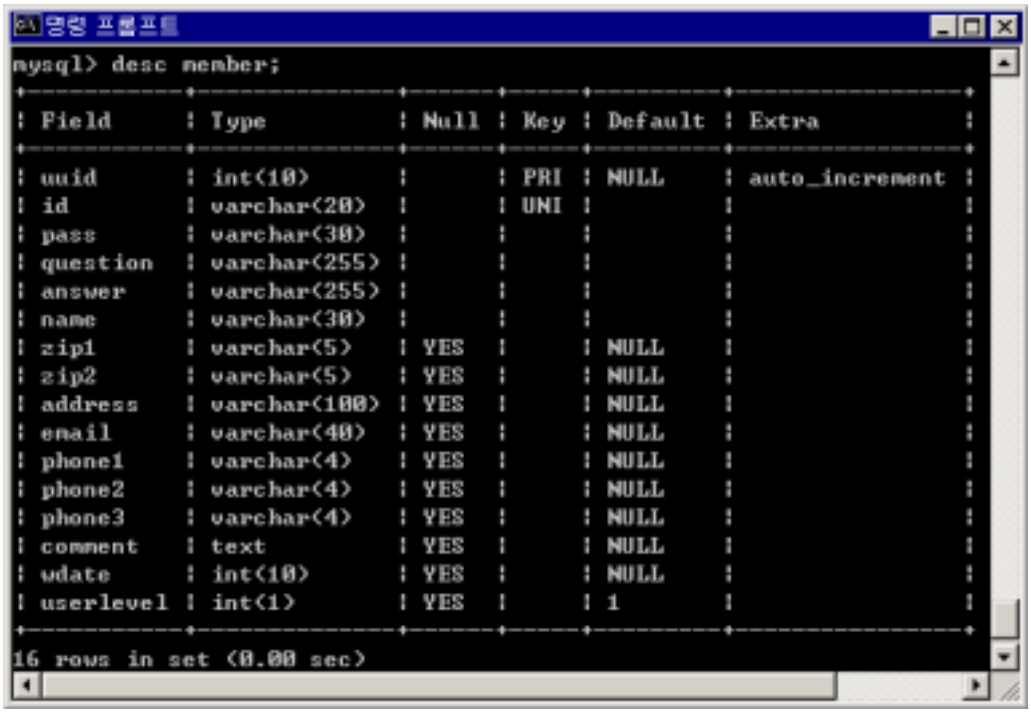
■ 등록 물품 테이블



명령 프롬프트

```
mysql> desc article;
+---------+--------------+------+-----+---------+----------------+
| Field   | Type         | Null | Key | Default | Extra          |
+---------+--------------+------+-----+---------+----------------+
| auid    | int(10)      |      | PRI | NULL    | auto_increment |
| aname   | varchar(250) |      |     |         |                |
| price   | varchar(10)  | YES  |     | 미정    |                |
| weight  | varchar(10)  | YES  |     | NULL    |                |
| pieces  | varchar(40)  | YES  |     | NULL    |                |
| season  | varchar(40)  | YES  |     | NULL    |                |
| pic     | varchar(250) | YES  |     | NULL    |                |
| comment | text         | YES  |     | NULL    |                |
| pwdate  | int(10)      | YES  |     | NULL    |                |
| awdate  | int(10)      | YES  |     | NULL    |                |
+---------+--------------+------+-----+---------+----------------+
10 rows in set (0.00 sec)
```

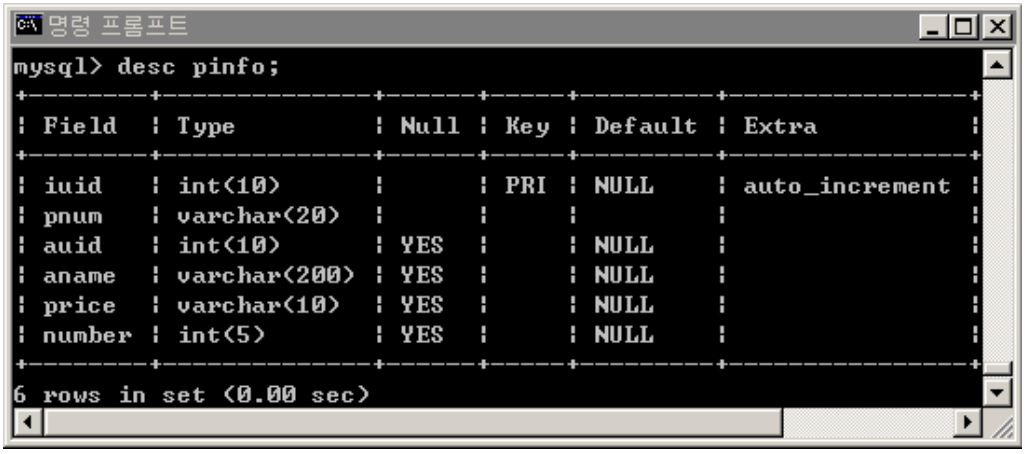
■ 회원 정보 테이블



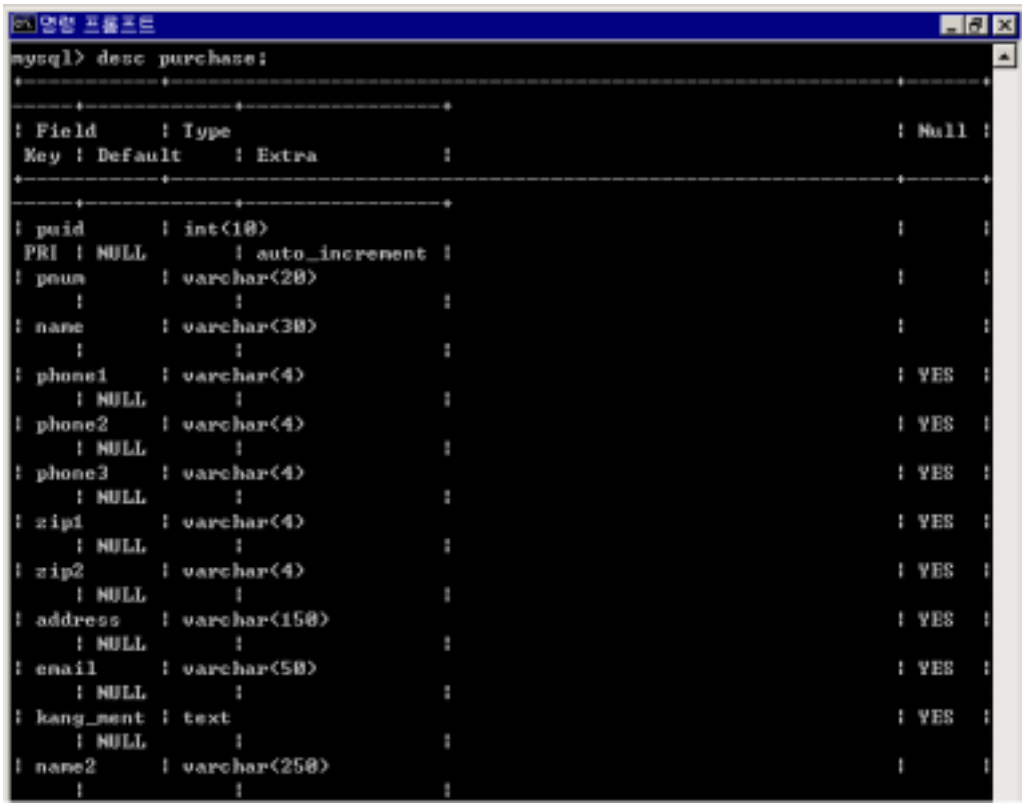
명령 프롬프트

```
mysql> desc member;
+-----------+--------------+------+-----+---------+----------------+
| Field     | Type         | Null | Key | Default | Extra          |
+-----------+--------------+------+-----+---------+----------------+
| uuid      | int(10)      |      | PRI | NULL    | auto_increment |
| id        | varchar(20)  |      | UNI |         |                |
| pass      | varchar(30)  |      |     |         |                |
| question  | varchar(255) |      |     |         |                |
| answer    | varchar(255) |      |     |         |                |
| name      | varchar(30)  |      |     |         |                |
| zip1      | varchar(5)   | YES  |     | NULL    |                |
| zip2      | varchar(5)   | YES  |     | NULL    |                |
| address   | varchar(100) | YES  |     | NULL    |                |
| email     | varchar(40)  | YES  |     | NULL    |                |
| phone1    | varchar(4)   | YES  |     | NULL    |                |
| phone2    | varchar(4)   | YES  |     | NULL    |                |
| phone3    | varchar(4)   | YES  |     | NULL    |                |
| comment   | text         | YES  |     | NULL    |                |
| wdate     | int(10)      | YES  |     | NULL    |                |
| userlevel | int(1)       | YES  |     | 1       |                |
+-----------+--------------+------+-----+---------+----------------+
16 rows in set (0.00 sec)
```

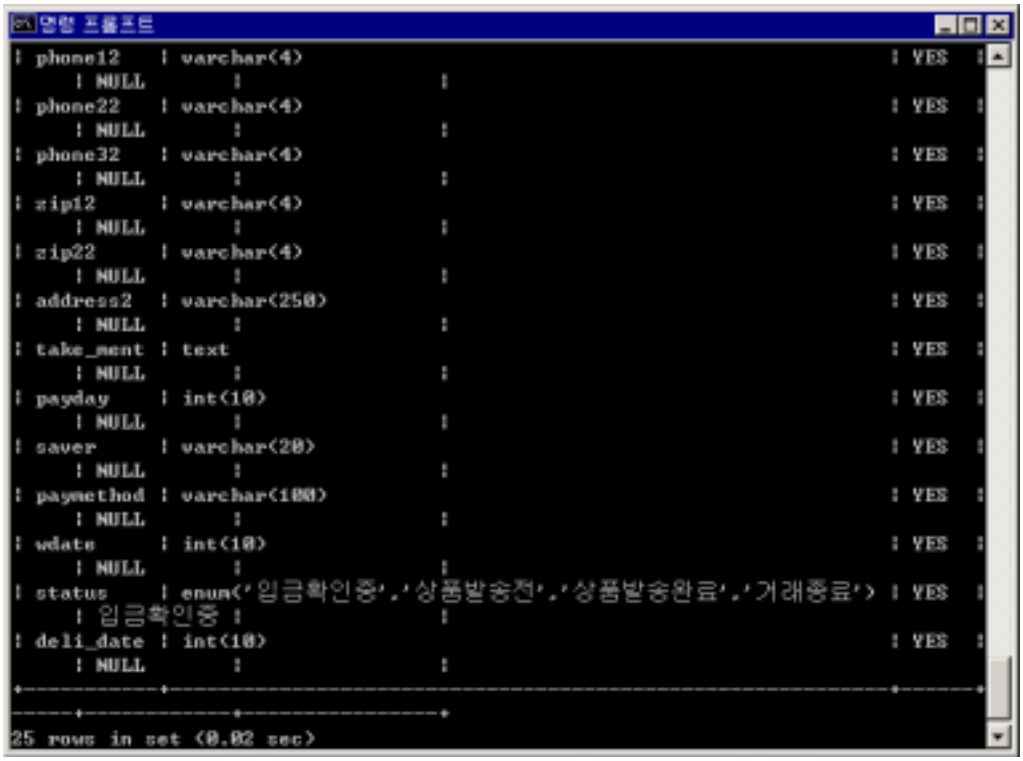
■ 구매 정보 테이블 - 전체 구매 리스트



■ 구매 정보 테이블(1) - 각 구매 물품 별 구매자 정보



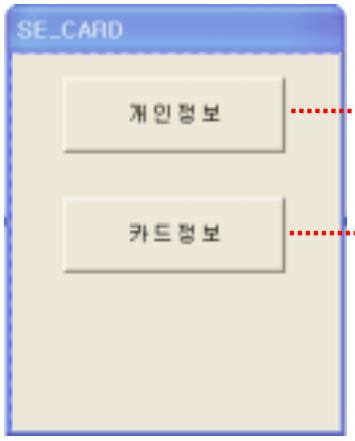
■ 구매 정보 테이블(2) - 각 구매 물품 별 구매자 정보



3. SECURE CARD

개인 단말기인 PDA를 이용하여 서비스 이용자가 최초 사용을 위해 회원가입을 할 경우 SECURE CARD라는 별도의 어플리케이션과 함께 암호화 모듈을 포함한 관련 파일들이 PDA로 다운받게 된다. 이때 사용되는 SECURE CARD는 사용자의 정보에 대한 안전한 저장이 가능하도록 한다.

다음은 SECURE CARD에 대해 나타낸 것이다.



회원가입과 상거래 진행시 필요한 <개인정보> 및 <카드정보>를 저장하기 위한 SECURE CARD가 실행된 모습이다.

<개인정보> 및 <카드정보>를 입력완료하게 되며, 사용자의 PDA 단말기에 입력한 정보는 암호화되어 저장되어, 추후 대금결재 및 회원가입시에 자동으로 읽어들여 사용되게 되며, 암호화된 형태로 저장되어 있으므로 타인에게의 정보노출을 막을 수 있다.

4. 주요 모듈

가. 회원가입

사용자가 회원가입을 수행하고자 할 경우 Active X 모듈이 호출되어, 이후의 모든 과정은 Active X 모듈에서 수행되게 된다. 아래는 웹 페이지에서 Active X 모듈을 호출하는 방법을 나타낸 것이다.

■ 모듈 위치 : 전자상거래 웹 사이트
■ 모듈 기능 : 회원가입 Active X 모듈 호출

```
<html>
<body>
   <object id='join' classid='CLSID:A57E81F5-08BA-474D-9AE1-3AA8DF903703'>
   </object>
</body>
</html>
```

이렇게 실행된 다이알로그에 개인정보를 입력한 후 가입 버튼을 클릭하면 아래의 OnJoin() 모듈이 호출되어, 개인정보는 암호화 과정등을 거쳐 인증서버로 전송된다.

■ 모듈 위치 : PDA에 등록되어 있는 Active X 모듈
■ 모듈 기능 : 사용자가 입력한 가입정보의 암호화 및 전송

```
void CJoinDlg::OnJoin()                    // 회원가입 요청시 수행되는 함수
{
    pSok = new CClientSock;     // 소켓 변수 생성
    pSok->Create();             // 소켓 생성

    SendReady();                // 암호화 및 전송
}
void CJoinDlg::SendReady()
{
        LPSTR lpBuff;
        lpBuff = U2A(dlg.m_strBuffer.GetBuffer(dlg.m_strBuffer.GetLength()));

        //--------------------------
        //      암호화 과정 수행
        //--------------------------

        SendPacket(cBuff);     // 암호화된 정보 전송(인자:암호화된 정보)
}
```

```
void CJoinDlg::SendPacket(const char *cData)  // 전송
{
        ..... 생 략 .....

        pSok->Send(Buff,strlen(cData));          // 암호화된 데이터 전송
}
```

인증서버로 전송된 암호화된 데이터는 복호화 과정을 거쳐 가입정보를 이용하여 회원등록을 한 후 인증서를 생성하여 사용자에게 전송해준다. 이때 인증서에 대한 정보는 추후 구매요청을 할 경우 구매자에 대한 인증을 위해 저장되게 된다. 인증서버에 대한 설명은 아래에서 다시 설명한다.

아래는 인증서버에서 인증서를 전송할 경우 회원가입 요청을 하였던 사용자의 PDA 단말기에 처음 SECURE CARD를 다운로그 할때 동시에 다운되어 등록한 Active X 모듈에 대한 설명이다. 즉, 인증서를 수신하고 저장하는 모듈을 나타낸 것이다.

■ 모듈 위치 : PDA에 등록되어 있는 Active X 모듈
■ 모듈 기능 : 인증서버에서 수신한 인증서 저장

```
void CClientSock::OnReceive(int nErrorCode)          // 인증서 수신
{
        char Buff[1024];
        memset(Buff, NULL, sizeof(Buff));

        Receive(Buff, 1024);                        // 소켓을 이용한 인증서 수신

        m_dlg->CertSave(Buff);                      // 인증서 저장 함수
}

void CJoinDlg::CertSave(const char * cCertData)     // 인증서 저장
{
        ..... 생략 .....
        //------------------------
        // 인증서 파일 형태로 저장
        //------------------------
}
```

나. 물품구매

사용자는 구매하고자 하는 물품을 선택한 후 결재요청을 하게된다. 이때 PDA에 저장되어 있던 Active X 모듈이 실행되게 되며, TotalPrint() 모듈이 실행되며 아래의 프로그램 절차에 의해 결재정보는 암호화 과정을 거쳐 인증서와 함께 서버로 전송되게 된다.

■ 모듈 위치 : PDA에 등록되어 있는 Active X 모듈
■ 모듈 기능 : 사용자가 구매요청한 물품에 대한 결재정보 암호화 및 전송

```
BOOL CPaymentCtrl::TotalPrint()
{
        CString Temp;
        Temp.Format(L"결제 금액이 %s 입니다 결제 하시겠습니까?", m_total);
        if(MessageBox(Temp, NULL, MB_OKCANCEL) == IDOK)    {
                ..... 생 략 .....
                if(total.DoModal()==IDOK)  {
                        ..... 생 략 .....
                        total.CreateSok(strTemp);       // 소켓 생성 모듈
                }
        }
}
void CTotalPay::CreateSok(CString Temp)
{
        pSok = new CClientSock;
        pSok->init(this);
        pSok->Create();

        SendReady(Temp);
}

void CJoinDlg::SendReady()
{
        // OS(WinCE, Win32)간 메모리 관리 차이에 따른 변환과정 수행
        LPSTR lpBuff;
        lpBuff = U2A(dlg.m_strBuffer.GetBuffer(dlg.m_strBuffer.GetLength()));

        //--------------------------
        //      암호화 과정 수행
        //--------------------------

        SendPacket(cBuff);              // 암호화된 정보 전송(인자:암호화된 정보)
}
```

■ 모듈 위치 : PDA에 등록되어 있는 Active X 모듈
■ 모듈 기능 : 사용자가 구매요청한 물품에 대한 결재정보 암호화 및 전송

```
void CJoinDlg::SendPacket(const char *cData)
{
        ..... 생 략 .....
         pSok->Send(Buff,strlen(cData));          // 전송
}
```

다. 인증 서버

인증서버는 위에서 설명한 회원가입 및 물품구매 기능 수행에 따른 정보 수신 및 관련기능 수행을 담당하는 서버이다. 이 서버는 암호화된 형태로 수신한 개인정보 및 카드정보를 복호화하거나, 회원가입시 요청되는 인증서를 생성/전송하는 기능을 수행하게 된다.

■ 모듈 위치 : 인증서버
■ 모듈 기능 : 회원가입 및 인증서 생성, 복호화 수행

```
void RealSock::OnReceive(int nErrorCode)     // 수신용 소켓 클래스
{
        char Buff[1024]="";
        Receive(Buff, 1024);          // 소켓을 통한 암호화 정보 수신
        CString imsi="";
        imsi = Buff;

        m_dlg->Print(this, imsi);    // 기능 수행
}

void CRegInfoSerDlg::Print(RealSock *pWnd, const char * cData)
{
        //---------------------------
        //      복호화 과정 수행
        //---------------------------

        szToken = strtok(result, szSeps);
        while(szToken != NULL) {
                strcpy(szArray[i++], szToken);
                szToken = strtok(NULL, szSeps);
        }
```

■ 모듈 위치 : 인증서버
■ 모듈 기능 : 회원가입 및 인증서 생성, 복호화 수행

```
        CString strSQL;
        if(CString(szArray[0])=="join")
        {
                // 회원가입시 전송되는 개인정보 처리
                CDatabase m_DBjoin;
                strSQL = "Insert into member(name,email,phone1,phone2
,                       phone3,zip1,zip2, address,id,pass) values
                        ('"+CString(szArray[1])+"','"+CString(szArray[2])
                        +"','"+CString(szArray[3])+"','"+CString(szArray[4])
                        +"','"+CString(szArray[5])+"','"+CString(szArray[6])
                        +"','"+CString(szArray[7])+"','"+CString(szArray[8])
                        +"','"+CString(szArray[9])+"','"+CString(szArray[10])+"')";
                Cert_Create(pWnd, szArray[9], szArray[10]);
        }
        else
        {
                // 물품구매시 전송되는 카드정보 처리
                strSQL="Insert into member(cardnum,cardvalid) values
                        ('"+CString(szArray[1])+"','"+CString(szArray[2])+"')";
        }
}

// 인증서 생성
void CRegInfoSerDlg::Cert_Create(RealSock *pWnd, char *szID, char *szPwd)
{
        //--------------------------
        //      인증서 생성
        //--------------------------

        ((RealSock *)pWnd)->Send(Buff, 1024);     // 소켓을 이용한 인증서 전송
}
```

제 4 장 목표달성도 및 관련분야에의 기여도

제 1 절 목표달성도

1. 연구 목표 및 내용의 연차적 계획

구 분	연구개발목표	연구개발 내용 및 범위
1차 년도 (2001년)	· 농산물 유통 전자상거래 시스템 기본 설계	· 국내 · 외 전자상거래 관련 솔루션 연구 · 전자상거래 시스템 구현 기술 및 동향 연구 · 사용자 인증, 결재 및 지불 시스템 등의 전자상거래 보안 기술 연구
	· 무선인터넷 기술 기초 분석	· 무선인터넷 기술 및 관련 기술 동향 파악 · 무선인터넷 프로토콜 및 마이크로 브라우저 구현 기술 연구 · 유 · 무선 연동 기술 연구 · 무선인터넷 보안 기술 연구
2차 년도 (2002년)	· 농산물 거래를 위한 안전한 전자상거래 시스템 구축	· 농산물 거래에 관련한 컨텐츠 개발 · 보안을 고려한 전자상거래 시스템의 구성 · 웹 상에서 농산물 거래를 위한 어플리케이션 개발
	· m-commerce 구현을 위한 모바일 전자상거래 시스템 개발	· 이동성 및 단말기 성능을 고려한 무선인터넷 환경에 최적화된 컨텐츠 설계 · 무선망 보안 기술을 적용한 시스템 설계 · 효과적인 유 · 무선 연동을 위한 시스템 개발 방법론 적용

2. 연구개발의 전략

가. 연구개발 세부내용

연도 / 세부과제 및 주요내용	2001년 (1차년도)	2002년 (2차년도)	가중치	비고
○ 농산물 유통 전자상거래 시스템 기본 설계 및 무선인터넷 기술 기초 분석				
- 국내·외 전자상거래 관련 솔루션 연구	→		5	
- 전자상거래 시스템 구현 기술 및 동향 연구	→		5	
- 사용자 인증, 결재 및 지불 시스템 등의 전자상거래 보안 기술 연구	→		10	
- 무선인터넷 기술 및 관련 기술 동향 파악	→		5	
- 무선인터넷 프로토콜 및 마이크로 브라우저 구현 기술 연구	→		5	
- 유·무선 연동 기술 연구	→		10	
- 무선인터넷 보안 기술 연구	→		10	
○ 농산물 거래를 위한 안전한 전자상거래 시스템 구축 및 m-commerce 구현을 위한 모바일 전자상거래 시스템 개발				
- 농산물 거래에 관련한 컨텐츠 개발		→	10	
- 보안을 고려한 전자상거래 시스템의 구성		→	5	
- 웹 상에서 농산물 거래를 위한 어플리케이션 개발		→	10	
- 이동성 및 단말기 성능을 고려한 무선인터넷 환경에 최적화된 컨텐츠 설계		→	10	
- 무선망 보안 기술을 적용한 시스템 설계		→	10	
- 효과적인 유·무선 연동을 위한 시스템 개발 방법론 적용		→	5	
주 요 연 구 결 과	전자상거래 시스템 기본 설계 및 무선인터넷 기술 기초 분석	전자상거래 시스템 구축 및 모바일 전자상거래 시스템 구현		

나. 연구개발 및 평가 착안점

구 분	평가의 착안점 및 척도	
	착 안 사 항	척 도 (점수)
1차년도 (2001)	○국내·외 전자상거래 관련 솔루션 연구	10
	○전자상거래 시스템 구현 기술 및 동향 연구	10
	○사용자 인증, 결재 및 지불 시스템 등의 전자상거래 보안 기술 연구	20
	○무선인터넷 기술 및 관련 기술 동향 파악	10
	○무선인터넷 프로토콜 및 마이크로 브라우저 구현기술 연구	10
	○유·무선 연동 기술 연구	20
	○무선인터넷 보안 기술 연구	20
2차년도 (2002)	○농산물 거래에 관련한 컨텐츠 개발	20
	○보안을 고려한 전자상거래 시스템의 구성	10
	○웹 상에서 농산물 거래를 위한 어플리케이션 개발	20
	○이동성 및 단말기 성능을 고려한 무선인터넷 환경에 최적화된 컨텐츠 설계	20
	○무선망 보안 기술을 적용한 시스템 설계	20
	○효과적인 유·무선 연동을 위한 시스템 개발 방법론 적용	10
최종 평가	○유선 환경에서의 안전한 거래를 위한 전자상거래 시스템 구현	40
	○효율적인 유·무선 컨텐츠 변환 기술을 통한 정확한 정보의 전송	20
	○무선 환경의 특성을 고려한 안전한 거래를 위한 시스템 구현	40

제 2 절 연구개발 기여도

본 연구를 통해 이동성이 강한 무선 단말기의 이용이 가능한 농산물 전자상거래 시스템을 구축하였다. 안전한 데이터 전송을 위해 암호화와 무결성을 고려한 보안기술을 이용하고 인증서의 개념을 도입하여 사용자에 대한 인증 기능을 제공함으로써 보다 안전한 전자상거래 시스템을 구축하였다. PDA를 무선 단말기로 활용하였으므로 서버와 무선단말간의 효율적인 연동을 위해서 PDA 인터페이스 기술개발을 수행하였다. 하지만 PDA는 메모리를 비롯한 시스템부분에서 근본적으로 취약한 점을 가지고 있어 이를 극복하기 위해서 상당시간의 자료조사, 사례분석 및 인터페이스 프로그램 개발을 수행하였다. 또한 신뢰성있고 안전한 전자결재시스템을 위해서 SECURE CARD라는 어플리케이션을 개발하였고 이는 결재과정에서 필요한 정보를 효율적으로 입력할 수 있는 형태로 설계되어 시스템의 편의성을 도모하였다.

위에서 살펴본 바와 같이 무선 인터넷 환경에서의 안전한 농산물 전자상거래 시스템을 구축하여 본 연구에 대한 결과를 보여줄 수 있다.

1. 기술적 측면

인터넷과 무선통신이 결합된 무선인터넷이 새로운 패러다임으로 부상하고 있는 현실에서 인터넷의 이용확산은 광범위한 새로운 시장을 형성할 것이다. 이동통신환경과 무선통신망의 연동, 단말기의 고도화는 이동통신, 즉 무선인터넷 서비스발전을 가져오고 이러한 서비스의 발전은 차세대 이동통신 서비스의 진화를 가속화시키는 역할을 할 것이다.

무선인터넷 시장은 유선인터넷과 같은 단순한 Architecture뿐만 아니라 단말기와 통신망간 접속, 단말기 및 Browser 기능, 데이터통신망 등 다양한 분야가 접목되어 복합적인 발전을 기반으로 해야하는 종합서비스로서 WAP과 m-HTML로 대변되는 표준화는 서비스의 고도화 및 네트워크 기술의 진화에 따라 상호 보완될 것이다.

안전한 m-commerce 시스템 구축을 위해서 데이터의 비밀성과 사용자의 인증을 비롯한 정보보안 기술을 본 시스템에 embedding 시켰으며, 소액 전자결재를 위해서 전자상거래 보안 및 SET 기술을 포함한 결재시스템에 대한 연구를 수행하였다. 특히 X.509기반의 인증서는 무선 단말기에서 사용이 가능하도록 재조정하였고, 향후에 타

기관의 공인 인증서와 연계하여 활용하도록 연구를 수행하였다. PDA를 무선 단말기로 활용하기 위해서 PDA 인터페이스 기술개발을 수행하였다. 하지만 PDA는 메모리와 운영체제를 비롯한 시스템부분에서 근본적으로 취약한 점을 가지고 있어 이를 극복하기 위해서 상당시간의 자료조사, 사례분석 및 인터페이스 프로그램 개발을 수행하였다.

본 연구에서는 전자상거래와 무선인터넷의 다양한 연구를 통하여 농산물 유통에 특화된 m-commerce 시스템을 PDA기반에서 개발함으로써 새로운 무선인터넷 비즈니스의 밑받침이 될 수 있을 것이다. 이는 기존의 유선에서 운영중인 e-commerce관련 업체에게 무선 인터넷 환경에서의 서비스를 제공하기 위한 웹사이트 구축과 관련하여 낮은 가격으로 실현 가능하도록 한다. 이렇게 구축된 웹사이트는 본 연구에서 개발된 응용프로그램 및 관련 모듈을 이용하여 m-commerce 시스템 사용을 가능하게 될 것이다.

효율적이고 안전한 PDA 인터페이스 기술개발, 다양한 컨텐츠의 제공, 망진화에 따른 멀티미디어 서비스, Mobility의 극대화를 통하여 향후 실시될 IMT-2000에 필요한 기술적 환경 구축기반을 마련할 수 있을 것이다.

2. 경제 · 산업적 측면

농산물은 가격에 비해 상대적으로 부피가 크고 무거워 소송·보관·하역 과정 등의 물류 표준화와 기계화가 어렵고, 소비자의 기호에 맞는 당도, 크기, 색깔, 형태별 품질 규격화가 어려워 규격화된 유통방식 도입이 곤란하다. 또한 농산물은 수집 및 분산 과정이 복잡하고, 부패 및 변질이 쉬워 유통 과정 중에 감소나 폐기가 많아 유통비용이 과다 발생하며, 생산과 출하는 계절적으로 집중되는데 비해 소비는 연중 일정하여 수급과 가격이 불안정하다.

이러한 농산물 유통 현실에 있어서 일반 농산물에 대한 전면적인 m-commerce의 구축을 추진할 수 있다면 현재 국내 인구의 절반 이상이 휴대폰 및 PDA를 비롯한 무선 단말기를 사용함으로써 별도의 큰 비용 없이 유통 마진 감소로 유통비용을 절감할 수 있을 것이다. 또한 현 도매시장의 유통구조를 개혁하여 고효율, 저비용 유통 시스템으로 바꿀 수 있을 것이며, 막대한 자본과 선진경영기법을 갖춘 외국산 유통업체의 국내진출과 국내 대기업 유통참여로 유통 업체간 경쟁이 심화되고 있는 현실에서 물

류비 절감의 효과를 볼 수 있을 것이다. 또 다른 m-commerce 도입의 효과로서는 농산물 유통구조의 혁신을 통해 농업경쟁력 재고를 할 수 있을 것이며, 농산물 유통시장의 전면 개방으로 인한 변화에 따른 능동적인 대처 방안이 될 것이다. 그리고 IT강국을 표방하고 있는 정부의 적극적인 지원하에서 농수산물 전자적 유통구조 개선에 핵심적으로 참여할 수 있고, 전문 농산물 유통 쇼핑몰로써 시장 우위를 확보할 수 있을 것이다.

제 5 장 연구개발결과의 활용계획

- 무선 네트워크 환경에서의 서비스를 제공하기 위해 시스템 확장을 원하는 인터넷 기반의 e-commerce 관련 업체에게 낮은 가격으로 시스템 변경을 지원하여 m-commerce를 위한 웹사이트 구축이 이루어질 수 있게 된다. 이렇게 구축된 웹사이트는 본 연구에서 개발된 응용프로그램 및 관련 모듈을 이용하여 m-commerce 시스템 사용을 가능하게 한다.
- PDA를 위한 인터페이스 기술의 구현을 달성함으로써, 서버와 무선 단말기간의 데이터가 편리하고 신뢰성 있게 전송되고, 농산물 구매를 위한 전자결재를 안전하게 수행한다.
- 본 연구결과를 확장하여 PDA를 이용한 실시간 경매 시스템과 농산물 가격에 대한 상황정보를 제공할 수 있다.
- 본 연구에서 구축한 m-commerce 시스템에서 사용한 무선 인터넷 기반의 X.509 인증서의 항목을 일부분 조정하여 무선기반에서 운영하는 다양한 보안 시스템 설계에서 적용이 가능하다.
- 본 연구에서 기본 개발 환경인 PDA를 비롯한 모든 단말기에서의 이용이 가능한 확장성을 위한 연구가 요구된다.

제 6 장 연구개발과정에서 수집한 해외과학기술정보

■ OpenSSL, http://www.openssl.org
- 보안관련 프로그램 연구를 위해 OpenSSL에서 제공되는 관련 소스를 분석

■ Microsoft, http://www.microsoft.com
- 프로그램 개발을 위한 관련 툴 제공 및 사용법 등을 제공
- eMbedded VC++ 개발과 관련하여 제공되는 소스를 이용
- Active X와 관련한 기술 참고

■ http://www.codeppc.com/evc
- eMbedded VC++을 이용한 Pocket PC기반의 개발용 프로그램 소스 분석

■ http://www.ietf.org/rfc
- PKI, Web security 기술에 대한 내용 및 표준 참고

제 7 장 참고문헌

[1] IETF RFC 2246, "The TLS Protocol Version 1.0," 1999.

[2] IETF RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile, Apr-2002.

[3] WapForum, "WAP Certificate and CRL Profiles : WAP-211-WAPCert," May-2001.

[4] A. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1996.

[5] 김범태, 김은, “전자상거래 표준화 동향 및 이슈”, 한국정보처리학회 논문지 Vol.6, No.1, 1999.1.

[6] 김기병외 2인, “전자상거래를 위한 지불 방법 및 보안”, 정보과학회지, 제16권 제5호, 1998.5.

[7] 박기준, “무선 PKI를 중심으로 한 무선 인터넷 보안 분석”, 정보처리학회지, 제9권 제2호, 2002.3.

[8] 최애라, “WAP기반 무선인터넷 전자상거래 시스템에서 신용카드 결재를 위한 보안 프로토콜”, 석사학위논문, 조선대학교, 2002.2.

[9] 유성진, 김성열, 정일용, “안전한 통신 서비스를 제공하는 향상된 SSL 기반 정보보호 시스템의 설계,” 한국통신학회논문지, 제25권, 제9호, 2000.9.

[10] 조성지, “M-Commerce에서 PDA환경에 적용한 안전한 결제 프로토콜”, 석사학위논문, 조선대학교, 2003.2.

[11] SK Telecom Technical Journal, “Wireless Application Protocol 서비스 개요”, Vol.6, No.4, 1999.10.

[12] S. Garfinkel, G. Spafford, Web Security & Commerce, O'Reilly & Associates, Inc., Tokyo, 1997.

[13] S. Shim, J. Gao, Y. Wang, "Multimedia Presentation Components in E-Commerce," International Workshop on E-Commerce and Web-Based Information Systems, WECWIS, pp. 158-167, 2000.

[14] A. Schade, C. Facciorusso, S. Field, Y. Hoffiner, "Advanced Dynamic Property Evauation for CORBA-based Electronic Markets," International Workshop on E-Commerce and Web-Based Information Systems, WECWIS, pp. 109-116, 2000.

[15] 이정대, 정권성, 채송화, 이재일, "무선인터넷 보안 기술 동향“, 한국정보보호센터.

[16] 이동훈, 임채훈, “타원 곡선 암호의 표준화 동향,” 퓨처시스템, 2001. 8.

[17] 이동훈, 임채훈, “타원 곡선 암호의 기초와 응용,” 퓨처시스템, 2001. 8.

[18] 이동훈, 임채훈, “SSL 3.0과 TLS 1.0의 비교분석,” 퓨처시스템, 2000. 7.

[19] 김혁만외 5인, “PDA 기반 TOC 동영상 Streaming Service & PDA 전용 Application" 프로젝트 결과보고서, 2002.

[20] 이만영외 5인, 『전자상거래 보안 기술』, 생능출판사, 1999.

[21] 이이표외 1인, 『ActiveX & OLE 실무 프로그래밍』, 삼양출판사, 2000.

[22] 무선인터넷 백서 편찬위원회, 『무선 인터넷 백서 2001』, 소프트뱅크 미디어, 2000.9.
[23] 고재관, 『Mobile PDA Programming』, 삼각형프레스, 2001.8.
[24] 강선명, 『Visual C++ 암호화 프로그래밍』, FREELEC, 2003.1.
[25] 손재기,양만석,이형수, “포켓리눅스를 이용한 개인 휴대용 정보 단말기 기술”, 정보과학회지, 제20권 제7호, pp. 22-26, 2002.7.
[26] 이동근외4인, “무선 응용 프로토콜 보안 기술”, 정보과학회지, 제20권 제4호, pp. 66-72, 2002.7.
[27] G. Me, "A Secure Mobile Local Payment Application Framework," International Conference on Security and management, CSREA Press, pp. 85-92, 2003.
[28] Y. Li et al, "The Framework Supporting Qos-enable Web Services," International Conference on Web Services, CSREA Press, pp. 256-263, 2003.
[29] Active X 강좌, http://jys92.com.ne.kr
[30] 한국정보보호진흥원, http://www.kisa.or.kr
[31] 전자신문, http://www.etnews.co.kr
[32] 디지털타임즈, http://www.digitaltimes.co.kr
[33] Microsoft, http://www.microsoft.com
[34] OpenSSL, http://www.openssl.org

주 의

1. 이 보고서는 농림부에서 시행한 농림기술개발사업의 연구보고서입니다.

2. 이 보고서 내용을 발표할 때에는 반드시 농림부에서 시행한 농림기술개발사업의 연구결과임을 밝혀야 합니다.

3. 국가과학기술 기밀유지에 필요한 내용은 대외적으로 발표 또는 공개하여서는 아니됩니다.