情 報 保 護 學 會 誌
第 12 券 第 3 號, 2002. 6

모바일 전자지갑 단말의 설계 및 구현

정 은 수*, 김 후 종*, 신 동 일**, 신 동 규**

요 약

무선인터넷의 활성화와 더불어 모바일 전자상거래에 대한 관심이 고조되고 있다. 모바일 전자상거래를 하기 위해서는 모바일 환경에 적합한 보안/인증 및 지불/결제 솔루션이 필요하며 이러한 기술은 기존 유선인터넷에서 사용하고 있는 방식을 그대로 사용하기에는 어려움이 따른다. 본 논문에선 무선인터넷을 이용한 전자상거래에 안전하고 편리한 지불/결제를 위해 모바일 전자지갑(Mobile Wallet) 모듈의 설계와 이동전화단말기에서의 전자지갑 모듈 구현함에 대하여 소개한다. 모바일 전자지갑을 설계함에 있어 무선인터넷을 이용한 전자지갑 모듈의 동작 프로세스에 대해 기술하였으며, 단말기에 저장된 전자지갑 정보를 읽어와서 지불 및 배송에 필요한 정보에 대해 암호화와 전자서명을 수행하기 위한 전자지갑 용 WML Script의 설계와 동작 프로세스에 대해 설명한다. 또한 이동전화 단말기에 전자지갑 모듈을 구현함에 있어 오프라인 전자지갑 모듈의 정보 입력과 모바일 전자지갑을 이용한 무선 전자상거래 서비스에 대해 단말 UI(User Interface) 기반으로 구현사례를 설명한다.

1. 서 론

무선인터넷은 시장을 넓혀가며 IT산업에 혁신을 가져오고 있다. 지난 80년대의 PC, 90년대의 인터넷에 이어 무선인터넷이 우리 사회·문화적 패러다임의 혁명적 변화를 재촉하고 있다.

무선 전자상거래란 무선 단말기를 이용한 전자상거래를 수행하는 것을 말하며 구체적으로는 무선 단말기, 즉 이동통신단말기, PDA, 노트북 등을 통해 인터넷에 접속하여 상거래를 수행하는 행위라고 정의할 수 있다.

이미 유선 인터넷을 이용한 전자상거래가 활성화되고 있으며 전자상거래의 활성화를 위한 전제조건으로 안전한 지불을 위한 보안/인증 기술과 다양한 지불수단의 제공을 뽑을 수 있다.

현재 유선에서 사용되고 있는 전자상거래를 살펴보면 인터넷 Shopping Mall에서 물품을 구입하고 지불정보와 배송정보를 전송하기 위해 보안채널을 생성하여 지불 정보를 전송하는 방식을 사용하고 있다.

이러한 유선인터넷에서 지불 방식을 무선인터넷 환경에서 동일하게 이용하기에는 무선통신의 좁은 대역폭, 이동통신 단말기의 중앙처리장치(CPU) 및 메모리의 제한 및 입력수단(화면,입력방법)의 불편으로 무선 전자상거래의 활성화에 한계가 있다[1].

무선인터넷은 금융업의 형태에 큰 영향을 미치고 있다. 이미 휴대폰은 소액전자결제의 대표적 수단으로 자리잡았으며 모바일뱅킹, 모바일증권거래, 모바일티켓팅, 모바일쿠폰, 모바일복권 등 다양한 종류의 모바일금융상품이 쏟아져 나오고 있다. 모바일 전자금융의 결정체는 무엇보다 모바일지갑(mobile wallet)이다. 무선망 및 금융전산망의 통합과 최첨단 IT기술에 힘입어 휴대폰은 현금 입출금은 물론, 마치 신용카드나 스마트카드와 같이 사용할 수 있는 전천후 지갑으로 변모하고 있다.

무선 전자상거래에 이용할 수 있는 지불수단으로는 신용카드, 전자화폐(Cyber Money 포함), 전자상품권, Point 등을 들 수 있으며 이러한 다양한 지불 수단을 무선 인터넷 환경에서 안전하고 편리하게 이용할 수 있는 방법이 필요하다.

본 연구에서는 다양한 지불 수단을 안전하고 편리하게 이용할 수 있는 모바일 전자지갑 단말을 구현함에 있어 전자지갑 모듈의 설계와 동작 프로세스에

* SK 텔레콤 Platform연구원
** 세종대학교 컴퓨터공학과 (shindk@sejong.ac.kr)

대해 설명하며, 모바일 전자지갑을 이용한 무선 전자상거래 서비스에 대해 이동전화 단말기의 UI(User Interface) 기반으로 구현 사례를 설명한다.

지불정보에 대한 암호화, 사용자에 대한 인증 및 상거래의 부인봉쇄를 위해WPKI(Wireless Public Key Infrastructure) 보안 방식을 사용한다[2],[3].

2. 모바일 전자자갑 설계

본 장에선 모바일 전자지갑의 설계 과정에 대해 오프라인 전자지갑 모듈의 기능과 유선 PKI와 무선 PKI의 차이점을 통하여 모바일 전자지갑에 적합한 무선환경에 최적화된 WPKI 기술 설계에 대해 설명한다. 그리고, 무선인터넷을 이용한 전자상거래 서비스에 대해 모바일 전자지갑의 지불 프로세스와 전자지갑 용 WML Script의 동작 프로세스에 대해 기술한다.

2.1 전자지갑모듈 설계

본 절에선 전자지갑 모듈의 오프라인 동작에 대한 기능적 설계에 대해 기술한다.

2.1.1 User Interface

전자지갑 모듈에 접근하기 위해서는 전자지갑 용 PIN(Personal Identification Number)을 입력받도록 하며 PIN 검증을 통해 인증된 사용자만이 전자지갑 정보를 접근하고 설정할 수 있는 인터페이스를 제공한다. PIN 정보는 사용자 인증과 전자지갑 정보의 암/복호화에 이용된다. 또한 정당하지 않는 사용자의 전자지갑 사용을 방지하기 위해 LOCK 기능을 제공한다.

2.1.2 전자지갑 정보 관리

전자지갑 정보는 크게 사용자 개인 신상정보(User Profile Information), 지불수단 정보(Financial Instrument Information) 및 인증서 정보(Certificate Information)로 나눌 수 있다.

■ User Profile Information

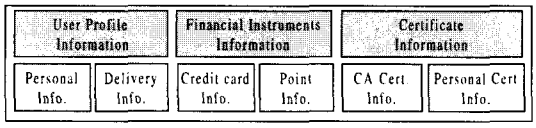
개인 신상 정보에는 사용자 이름과 이동전화번호와 같은 사용자 개인 정보(Person Information)와 구매 물품을 전달받기 위해 설정하는 배송지 정보(Delivery Information)가 있다.

■ Financial Instruments Information

지불 수단은 신용카드, Point(OK Cashbag) 결제 서비스를 지원하고 있으며 결제에 필요한 정보를 저장하고 있다.

■ Certificate Information

인증서 정보에는 CA 인증서와 개인 인증서가 저장되어 관리된다.



〔그림 1〕 전자지갑 정보 구성

그림 1은 전자지갑 정보 구성에 대해 Block 단위로 보여주고 있으며, 전자지갑 정보 저장 시에는 지불수단(Financial Instruments) 정보는 암호화 되어 저장된다. 각각의 전자지갑 정보는 필수 입력 항목과 선택 입력 항목이 존재하며 입력 항목이 필수 입력 항목일 경우 반드시 해당 항목을 입력하여야만 전자지갑 정보를 단말기에 저장할 수 있다.

2.1.3 PIN Verification

전자지갑에서는 사용자 확인을 위해 PIN(Personal Identification Number) 검증을 수행하는 흐름도이다. PIN 검증이 실패했을 경우에는 임의의 횟수(N) 동안만 재입력 시도를 허용하며 임의의 횟수 이상의 로그인 시도가 발생하면 부당한 사용자의 로그인을 방지하기 위해 PIN 정보 잠금 기능이 적용된다.

2.2 WPKI (Wireless Public Key Infrastructure) 기반 설계

공개키 기반의 암호화 및 전자서명을 구현하기 위한 유선환경의 PKI를 무선환경에 동일하게 적용하기에는 소용량 무선 단말기의 제약과 제한된 무선 대역폭 및 불안정한 네트워크 환경으로 어려움이 있다.

2.2.1 인증서(Certificate)

유선 PKI에서 사용하는 인증서 형식은 X.509을 사용하고 있으며 무선 환경에선 WAP Forum에서 제안하는 WTLS 인증서 또는 X.509 V3 인증서를

사용하고 있다. 이 부분은 이동통신 단말기의 Resource의 제약으로 유선에서 사용하는 X.509인증서를 그대로 사용하는 데는 어려움이 있기 때문이다. 모바일 전자지갑 단말의 경우 개인 인증서는 WTLS 또는 X.509 V3 Type의 인증서를 지원하며 서버 인증서는 WTLS 인증서를 사용하고 있다.

인증서 검증방법에 있어서도 기존 유선에서 주기적으로 1M Byte이상 되는 CRL(Certificate Revocation List) 정보를 다운 받아 관리하고 검증하는 데는 단말 Resource 및 무선 Network의 한계로 어려움이 있어 무선 환경에선 Short-Lived 인증서 또는 OCSP(Online Certificate State Protocol) 방식을 사용하여 인증서를 검증할 수 있다.

OCSP를 통하여 인증서의 Revocation Check가 가능하지만 OCSP를 통한 처리는 추가적 Round-trip 및 Validation Step을 필요로 하며 OCSP Responder에 대한 추가 Trust가 필요하다.

모바일 전자지갑의 경우 서버 인증서는 Long Term 인증서(1년)를 기반한 Short-Lived 인증서 형식(48시간)을 사용하고 있다. 실제 Short-Lived 인증서는 24시간마다 자동 발행이 되며 CA에서 서버의 인증서가 Revocation될 경우 CA에서 발행하지 않음으로써 처리된다.

또한 인증서의 저장정보Size 측면에서도 유선 PKI에서 사용하고 있는 X.509 인증서의 경우는 2K Byte정도의 Size이며 WTLS 인증서의 경우는 대략 1K Byte 정도의 Size가 된다. 이 부분은 서비스를 위해 여러 개의 CA인증서와 개인 인증서를 저장해야 하는 이동통신 단말기의 메모리에 큰 부하를 줄 수 있다.

모바일 전자지갑 단말의 경우는 최소 5개의 CA 인증서와 10개의 개인 인증서를 저장할 수 있는 메모리 저장영역을 유지한다. 또한 무선 Network을 통하여 인증서를 다운 받는 부하는 줄이기 위해 실제 인증서가 아닌 인증서 URL 정보를 전송하고 있다.

2.2.2 공개키 암호화 알고리즘

유선 PKI에서 키 생성 알고리즘으로 사용하는 RSA의 경우 보안적으로 안전하기 위해서 필요한 키의 길이가 1024 Bit인데 반해 무선 환경에서 이용되는 ECC의 경우는 약 160 Bit로 RSA 1024 Bit의 보안 강도를 가지면서 보다 빠른 연산이 가능하기에 무선 환경에선 ECC 알고리즘을 사용하고 있다.

실제 유선상에서는 RSA를 사용한 키 생성 및 전자서명에 큰 차이를 못 느끼지만 이동통신 단말의 제한된 Resource 환경에선 RSA 알고리즘을 이용한 서비스는 불가할 정도로 키 생성과 전자서명 연산속도가 느리다.

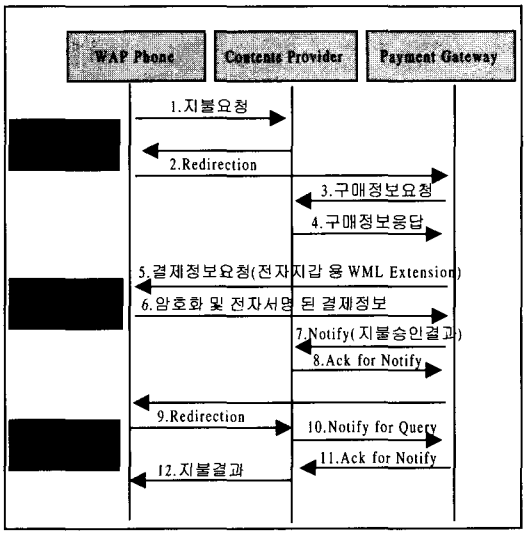
2.2.3 암호화 방식

암호화 방식에 있어 유선 PKI와 무선 PKI는 차이가 있다. 일반적으로 유선에선 Session Layer 기반의 암호화 방식인 SSL을 사용하고 있으며, 무선 환경에선 WAP Protocol에서 정의하고 있는 이동통신 단말과 WAP Gateway간 WTLS 보안 방식을 사용하고 Gateway와 Web기반의 CP(Contents provider)서버간 SSL을 이용할 수 있다.

WTLS의 경우 Gateway 단에서 암호화된 데이터가 풀려야 하는 치명적인 약점이 있어 실제 사용에는 한계가 있다. 이러한 문제를 해결하기 위해 무선 환경에선 Application Layer 단에서의 보안 방식을 많이 사용하고 있다.

모바일 전자지갑의 경우는 Application Layer 단에서 WML Crypto Script를 사용하여 암호화를 수행한다.

2.3 모바일 전자지갑 지불 프로세스



〔그림 2〕 모바일 전자지갑 지불 프로세스

무선인터넷을 이용한 상품 구매 절차를 단말기 프로세스를 중심으로 알아보면 다음과 같다. 단말기 프로세스는 대략적으로 on-line 쇼핑몰 접속, 상품

구매, 결제 요청, 결제 승인 결과 확인으로 이뤄지며 사용자는 구매할 상품을 선택한 후에 결제하기를 요청하는데 결제가 이뤄지기 위해서는 단말기에 저장된 전자지갑 정보를 읽어와서 결제 정보를 암호화하고 전자서명 하여 서버로 전달해야 한다.

그림 2는 사용자가 결제를 요청했을 경우 WAP 단말기, CP(Contents Provider), 그리고 PG (Payment Gateway)간 이뤄지는 프로세스를 순차적 흐름도로 나타낸 것이다.

각 프로세스의 상세 처리 내역은 다음과 같다.

① 지불요청
- 사용자가 물품 선택 후 결제하기를 선택한 경우
- 지불결제 Request를 CP로 전송

② Redirection
- CP에서 WAP Phone을 거쳐 Direct Link Page로 Redirection한다.
- 이때 CP에서 전송되는 Information은 CP ID,Transaction NO, Transaction Data & Time,물품정보를 얻어올 CP의 URL 등을 포함한다.

③ 구매정보요청, ④ 구매정보응답
- Direct Link Page에서 CP로부터 구매 정보와 전자지갑 접근 정보를 가져온다.
- 전자지갑 접근 정보라는 것은 CP에서 단말기의 전자지갑으로부터 배송지 정보를 가져올 것인지를 결정하는 전자지갑 접근에 관한 정보이다.

⑤ 결제정보요청, ⑥ 암호화 및 전자서명 된 결제정보
- 구매 및 지불 정보를 암호화하고 전자서명하기 위해 전자지갑용WML Script Extension이 실행된다
- 전자지갑용WML Script Extension실행은 전자지갑 비밀번호 확인, 전자지갑 정보 접근(off-line 전자지갑에 설정된 정보를 가져옴), 배송정보 및 결제 수단 선택, 전자서명 및 암호화 수행, Enveloped Data Return의 순서로 진행된다.

⑦ Notify, ⑧ ACK for Notify
- PG에서 지불 승인 요청 결과를 CP로 Notify하면 CP에서는 Notify에 대한 ACK를 보낸다.

⑨ Redirection
- Direct Link Page에서 WAP Phone을 거쳐 CP로 Redirection한다.
- Redirection URL로 접속하여 지불 승인 처리 결과를 전송

⑩ Notify for Query, ⑪ ACK for Notify
- CP에서 Direct Link Page로 최종 승인 결과 확인을 위한 Query를 던지면 Direct Link Page에서 ACK를 보낸다.

⑫ 지불결과
- 사용자에게 최종 지불 처리 결과 화면을 출력한다.
- 결과코드, 승인번호, 결제금액, Transaction NO & Time정보 등을 포함한다.

2.2 전자지갑 용 WML Script Extension

전자상거래에 사용될 개인정보, 결제정보 및 배송지정보는 모두 단말기 내의 전자지갑에 저장되게 된다. 단말기 사용자는 무선 CP에 접속하여 전자상거래를 할 경우 온라인 전자지갑 함수인 getMWData() 함수를 통하여 결제정보를 전달하게 된다[4].

getMWData() 함수는 다음과 같은 세가지 기능이 포함된 복합적인 함수이다.
- 전자지갑에 저장된 데이터를 읽어오는 기능
- 서버에서 요구한 데이터에 전자서명을 하는 기능
- 데이터를 암호화하는 기능

getMWData()를 통해 전자지갑을 사용하는 과정은 다음과 같다.

① 서버에서는 결제시 필요한 정보를 얻기 위해 getMWData() 함수가 포함된 WMLScript 문서를 전송한다.

② 단말기에선 getMWData()에 Argument로 주어진 서버 인증서를 통해 서버를 검증하고, 전자지갑의 각 필드에 대한 접근권한이 있는지 여부를 확인한다.

③ 접근권한이 확인되었을 경우 서버가 요청한 내용을 단말기NV에 저장된 전자지갑으로부터 가져온다.

④ 전자지갑에 접근하려는 정보가 암호화된 정보(결제정보)일 경우 사용자로부터 전자지갑 비밀번호를 입력 받는다.

⑤ 전자지갑 비밀번호 확인 후 단말기 NV영역에서 전자지갑 정보를 읽어와 사용자에게 확인하

며 사용자는 다양한 지불수단 및 다양한 배송지 정보를 선택할 수 있다.

⑥ getMWData() 함수 내부적으로 signTextEx() API를 사용하여 데이터에 대해 전자서명을 한다.

⑦ getMWData() 함수 내부적으로 encrypt TextEx() API를 사용하여 무선 PG서버의 공개키로 데이터를 암호화한다.

⑧ 무선 PG서버는 이 값을 자신의 개인키로 복호화한 다음 전자서명을 검증하고, 문제가 없을 경우 전자지갑으로부터 얻어낸 데이터를 가지고 결제하게 된다.

3. 단말기 구현 사례

본 장에선 실제 이동전화단말기에 전자지갑 모듈을 구현함에 있어 오프라인 전자지갑 모듈에 정보입력과 모바일 전자지갑을 이용한 무선 전자상거래 시나리오에 대해 단말기 UI기반으로 설명한다.

3.1 전자지갑 정보입력

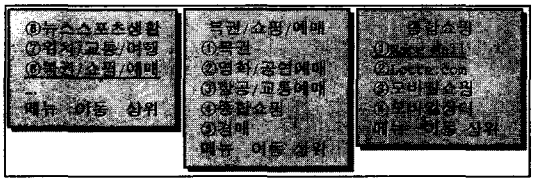
전자지갑 정보입력은 단말 메뉴에서 전자지갑을 선택하여 사용자정보, 결제정보, 배송지정보 등을 입력하는 것을 말하며 다음을 포함한다.

- 전자지갑 메뉴 선택
- 사용자 정보 입력
- 결제정보(신용카드) 입력
- 결제정보(OK Cashbag) 입력
- 배송지 정보 입력
- 비밀번호 변경
- 인증서 정보

3.2 무선 전자상거래 시나리오

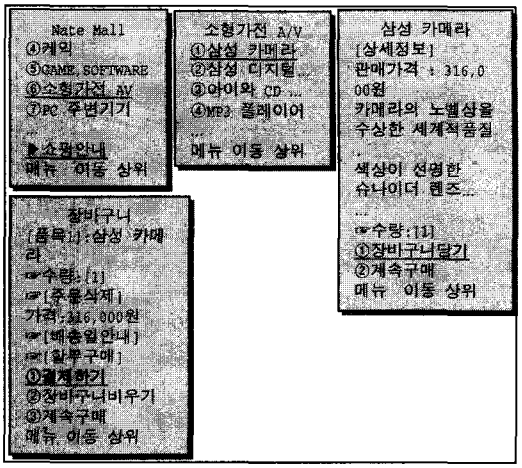
무선인터넷 단말을 이용한 신용카드 지불/결제에 대해 서비스 시나리오 별 단말 UI(User Interface)를 통해 구현사례를 설명한다.

- Marketplace 접속



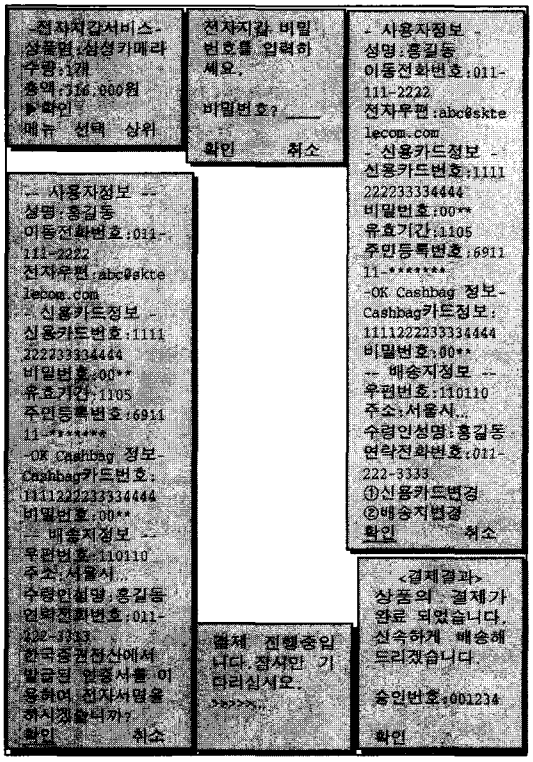
〔그림 3〕 Marketplace 접속

- 상품선택



〔그림 4〕 상품선택

- 전자지갑 열기 및 신용카드 결제



〔그림 5〕 전자지갑 열기 및 신용카드 결제

4. 결론 및 향후 개발방향

지금까지 무선 전자상거래에서 안전하고 편리한 지불/결제를 위한 모바일 전자지갑(Mobile Wallet)

모듈의 설계와 이동통신단말기에 모바일 전자지갑 모듈의 구현 결과에 대해 설명하였다.

오프라인 전자지갑 모듈의 정보 구성과 전자지갑 정보 접근방법을 통하여 오프라인 전자지갑의 안전성과 무선인터넷을 통하여 편리하게 전자지갑 정보를 이용할 수 있음을 알 수 있었다.

기존 유선환경의 PKI 기술을 동일하게 무선 환경에 적용하기에는 이동통신 단말기의 Resource의 제한 및 무선 Network의 한계로 어려움이 있었으며 본 연구를 통하여 무선 환경에 최적화된 WPKI 기술을 설계 할 수 있었다.

모바일 전자지갑 동작 프로세스에 대해 설명하면서 무선인터넷을 통한 지불/결제 시나리오을 이해할 수 있었으며 전자서명과 암호화를 위한 전자지갑 용 WML Script의 동작 프로세스와 WPKI 관련 시나리오에 대해 이해할 수 있었다.

마지막으로 이동통신 단말기에 모바일 전자지갑 모듈을 구현 결과를 단말기 UI를 통하여 적용 결과를 볼 수 있었으며, 보안 방식으로는 Session Layer 보다는 Application Layer기반의 WML Crypto Script를 사용해야 함을 알 수 있었다.

본 연구를 통해서 무선인터넷을 이용한 지불/결제의 가장 걸림돌이 되었던 보안/인증에 대해서는 무선환경에 최적화된 WPKI 기반의 전자서명과 암호화를 통해 안전한 상거래를 구현하였으며, 이동통신 단말기를 통한 상거래에 필요한 결제정보 및 배송지 정보의 입력을 매번 해야 하는 불편을 모바일 전자지갑 모듈을 통해 다양한 지불수단 선택과 편리한 지불을 사용자에게 제공함으로써 무선 전자상거래 활성화에 기여할 것으로 예상된다.

향후 연구계획으로는 현재까지 구현된 신용카드와 OK Cashbag 지불수단을 제공하는 전자지갑에서 좀 더 다양한 지불수단을 제공할 수 있는 전자지갑의 설계가 필요하며, 또한 Java 기반의 전자지갑 모듈 개발을 통해 유선과 무선에서 공통으로 사용할 수 있는 전자지갑 모듈의 연구와 개발이 필요할 것으로 보인다.

참 고 문 헌

[1] "무선인터넷 백서2001", 무선인터넷백서편찬위원회, 소프트뱅크미디어

[2] "SKT Security Service 규격(SKT SS Based on WPKI)", SK Telecom

[3] "전자상거래 보안기술", 이만영 외 5인 공저,생능출판사

[4] "WMLScript Language Specification," WAP Forum, 4th November-1999, URL: http://www.wapforum.org

〈著者紹介〉

정 은 수 (Chung Eun Su)

1995년 : 한양대학교 전자공학과 (공학사)

2000년 3월~2002년 8월 : 세종대학교 정보통신대학원 정보통신공학과 석사과정

1995년 2월~현재 : SK텔레콤 Platform연구원 Terminal개발팀

관심분야 : m-Commerce Terminal 솔루션무선 보안/인증 및 지불 솔루션, 근거리 결제기술

김 후 종 (Kim Who Jung)

1988년 : 서강대학교 전자공학과 (공학사)

1995년 : 서강대학교 전자공학과 (공학석사)

2000년 3월~현재 : 국민대학교 전자공학과 박사과정, SK텔레콤 Platform연구원 Terminal개발팀장

관심분야 : m-Commerce Terminal 솔루션무선 보안/인증 및 지불 솔루션, 근거리 결제기술

신 동 일 (Shin Dong Il)

1988년 : 연세대학교 전산과학과 (이학사)

1993년 : M.S. in Computer Science, Washington State University

1997년 : Ph.D in Computer Science, University of North Texas

1997년 9월~1998년 2월 : 시스템공학연구소 선임연구원

관심분야 : 이동통신, WAP, XML응용, CSCW, 지능형 에이전트

신 동 규 (Shin Dong Gyoo)
1986년 2월 : 서울대학교 계산통계학과 (이학사)
1992년 8월 : Illinois Institute of Technology 전산학과 (공학석사)
1997년 8월 : Texas A&M University 전산학과 (공학박사)
1986년 2월~1991년 1월 : 한국국방연구원 연구원
1997년 8월~1998년 2월 : 현대전자 멀티미디어연구소 책임연구원
1998년 3월~현재 : 세종대학교 컴퓨터공학과 조교수
관심분야 : 웹기반 멀티미디어, WAP, XML응용, 영상압축