2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

WPKI 기반 모바일 전자지갑 단말 설계 및 구현

정은수*, 신동규**
*SK 텔레콤 Platform연구원, **세종대학교 컴퓨터공학과
e-mail : *jes1248@sktelecom.com, **shindk@sejong.ac.kr

Design and Implementation of Mobile Wallet Cellular Phone Based on WPKI

Eun su Jung*, Dong-kyoo Shin**
* Platform R&D Center, SK Telecom
** Dept. of Computer Engineering, Sejong University

요 약

무선인터넷의 활성화와 더불어 무선 전자상거래에 대한 관심이 고조되고 있다. 무선 전자상거래를 하기 위해서는 무선 환경에 적합한 보안/인증 및 지불/결제 솔루션이 필요하며 이러한 기술은 기존 유선인터넷에서 사용하고 있는 방식을 그대로 사용하기에는 어려움이 따른다. 본 연구에선 무선인터넷을 이용한 전자상거래에 안전하고 편리한 지불/결제를 위해 모바일 전자지갑(Mobile Wallet) 모듈의 설계와 이동전화단말기에 전자지갑 모듈을 구현함으로써 안전하고 편리한 지불/결제 솔루션을 제공한다. 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 Script 의 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. 서론

무선 전자상거래 란 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 Mall 에서 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]

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 대해 설명하며, 모바일 전자지갑을 이용한 무선 전자상

거래 서비스에 대해 이동전화 단말기의 UI(User Interface) 기반으로 구현 사례를 설명한다.

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

2. 모바일 전자자갑 설계

본 장에선 무선인터넷을 이용한 전자상거래 서비스에 대해 모바일 전자지갑의 지불 프로세스와 전자지갑 용 WML Script 의 동작 프로세스에 대해 기술한다.

2.1 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 1 은 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 Request 를 CP 로 전송

② Redirection
- CP 에서 WAP Phone 을 거쳐 Direct Link Page 로 Redirection 한다.
- 이때 CP 에서 전송되는 Information 은 CP ID,Transaction NO, Transaction Data&Time,물품정보를 얻어올 CP 의 URL 등을 포함한다.

③ 구매정보요청, ④ 구매정보응답
- Direct Link Page 에서 CP 로부터 구매 정보와 전자지갑 접근 정보를 가져온다.
- 전자지갑 접근 정보라는 것은 CP 에서 단말기의 전자지갑으로부터 배송지 정보를 가져올 것인지를 결정하는 전자지갑 접근에 관한 정보이다.

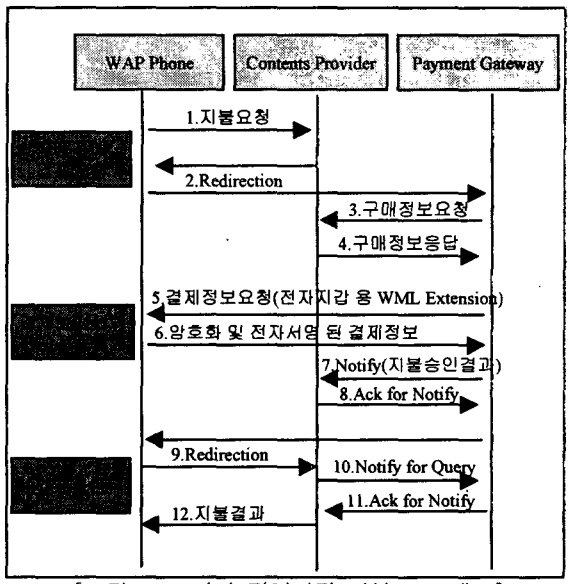
⑤ 결제정보요청, ⑥ 암호화 및 전자서명 된 결제정보
- 구매 및 지불 정보를 암호화하고 전자서명하기 위해 전자지갑용 WML Script Extension 이 실행된다
- 전자지갑용 WML Script Extension 실행은 전자지갑 비밀번호 확인, 전자지갑 정보 접근(off-line 전자지갑에 설정된 정보를 가져옴), 배송정보 및 결제 수단 선택, 전자서명 및 암호화 수행, Enveloped Data Return 의 순서로 진행된다.

⑦Notify, ⑧ ACK for Notify
- PG 에서 지불 승인 요청 결과를 CP 로 Notify 하면 CP 에서는 Notify 에 대한 ACK 를 보낸다.

⑨ Redirection
- Direct Link Page 에서 WAP Phone 을 거쳐 CP 로 Redirection 한다.
- Redirection URL 로 접속하여 지불 승인 처리 결과를 전송

⑩ Notify for Query, ⑪ ACK for Notify
- CP 에서 Direct Link Page 로 최종 승인 결과 확인을 위한 Query 를 던지면 Direct Link Page 에서 ACK 를 보낸다.

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



[그림 1. 모바일 전자지갑 지불 프로세스]

2.2 전자지갑 용 WML Script Extension[4]

전자상거래에 사용될 개인정보, 결제정보 및 배송지 정보는 모두 단말기 내의 전자지갑에 저장되게 된다. 단말기 사용자는 무선 CP 에 접속하여 전자상거래를 할 경우 온라인 전자지갑 함수인 getMWData() 함수를 통하여 결제정보를 전달하게 된다.

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 Argument 로 주어진 서버 인증서를 통해 서버를 검증하고, 전자지갑의 각 필드에 대한 접근권한이 있는지 여부를 확인한다.
③ 접근권한이 확인되었을 경우 서버가 요청한 내용을 단말기 NV 에 저장된 전자지갑으로부터 가져온다.
④ 전자지갑에 접근하려는 정보가 암호화된 정보(결제정보)일 경우 사용자로부터 전자지갑 비밀번호를 입력 받는다.
⑤ 전자지갑 비밀번호 확인 후 단말기 NV 영역에서 전자지갑 정보를 읽어와 사용자에게 확인하며 사용자는 다양한 지불수단 및 다양한 배송지 정보를 선택할 수 있다.
⑥ getMWData() 함수 내부적으로 signTextEx() API 를 사용하여 데이터에 대해 전자서명을 한다.
⑦ getMWData() 함수 내부적으로 encryptTextEx() API 를 사용하여 무선 PG 서버의 공개키로 데이터를 암호화한다.
⑧ 무선 PG 서버는 이 값을 자신의 개인키로 복호화한 다음 전자서명을 검증하고, 문제가 없을 경우 전자지갑으로부터 얻어낸 데이터를 가지고 결제하게 된다.

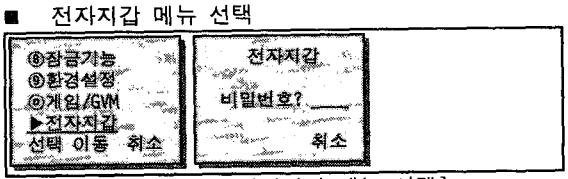
3. 단말기 구현 사례

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

3.1 전자지갑 정보입력

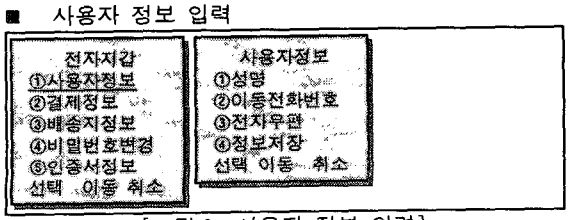
전자지갑 정보입력은 단말 메뉴에서 전자지갑을 선택하여 사용자정보, 결제정보, 배송지정보 등을 입력하는 것을 말한다.

■ 전자지갑 메뉴 선택



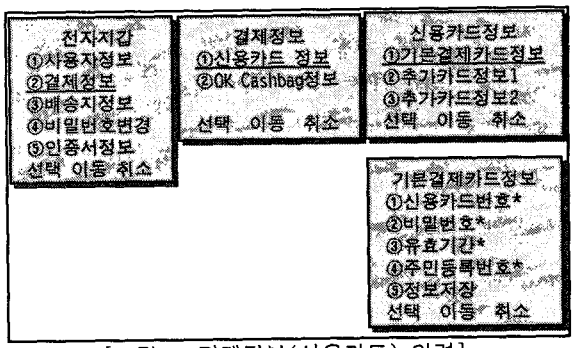
[그림 2. 전자지갑 메뉴 선택]

■ 사용자 정보 입력



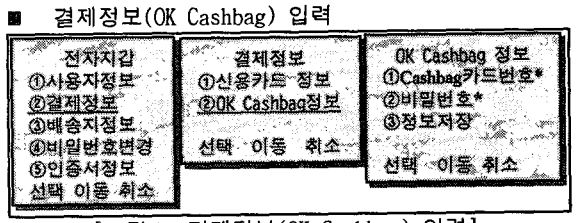
[그림 3. 사용자 정보 입력]

■ 결제정보(신용카드) 입력



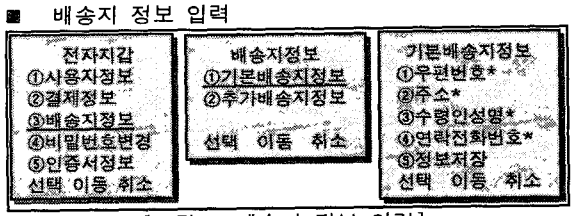
[그림 4. 결제정보(신용카드) 입력]

■ 결제정보(OK Cashbag) 입력



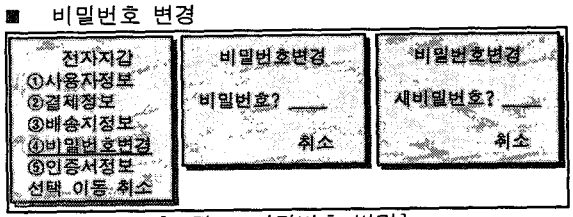
[그림 5. 결제정보(OK Cashbag) 입력]

■ 배송지 정보 입력



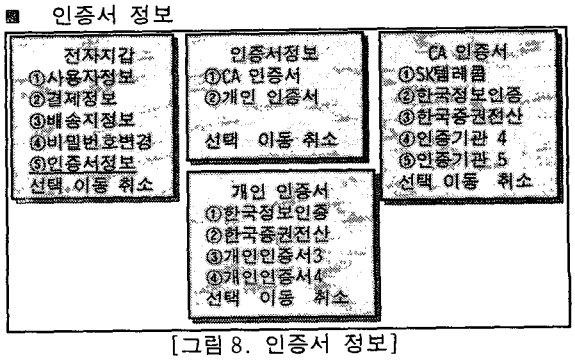
[그림 6. 배송지 정보 입력]

■ 비밀번호 변경



[그림 7. 비밀번호 변경]

■ 인증서 정보

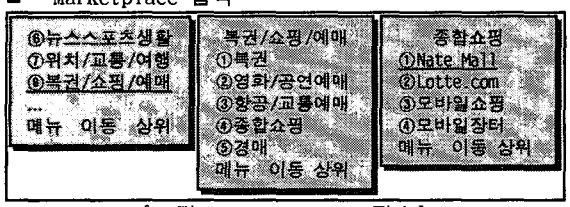


[그림 8. 인증서 정보]

3.2 무선 전자상거래 시나리오

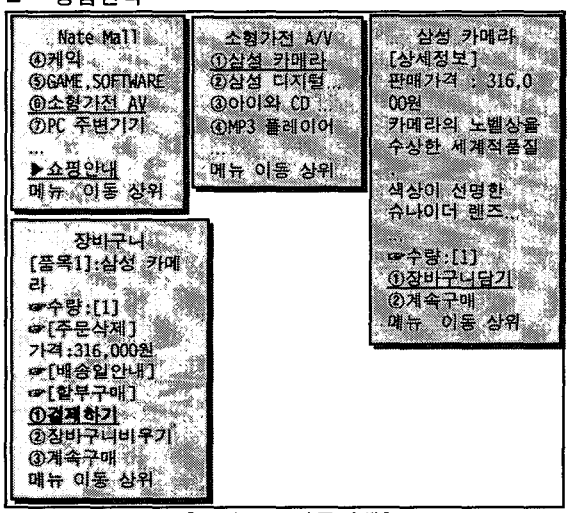
무선인터넷 단말을 이용한 신용카드 지불/결제에 대해 서비스 시나리오 별 단말 UI(User Interface)를 통해 구현사례를 설명한다.

■ Marketplace 접속



[그림 9. Marketplace 접속]

■ 상품선택



[그림 10. 상품선택]

4. 결론 및 향후 개발방향

지금까지 무선 전자상거래를 안전하고 편리하게 이용할 수 있는 모바일 전자지갑 모듈의 동작 프로세스와 이동전화 단말기에 구현사례에 대해 설명하였다.

본 연구를 통해서 무선인터넷을 이용한 지불/결제의 가장 걸림돌이 되었던 보안/인증에 대해서는 인증서 기반의 전자서명과 암호화를 통해 안전한 상거래를 구현하였으며, 이동전화단말기를 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.

■ 전자지갑 열기 및 신용카드 결제

[그림 11. 전자지갑 열기 및 신용카드 결제]

향후 개발방향으로는 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.

참고문헌

[1] " 무선인터넷 백서 2001" , 무선인터넷백서편찬위원회, 소프트뱅크미디어

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

[3] " 전자상거래 보안기술" , 이만영 외 5 인 공저, 생능출판사

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