블루투스를 이용한 이중인증방식의 전자지불 시스템의 개발

김성일O* 김용민* 김현익* 정창훈** 김응규***
(주)에스티* 고려대학교** 한밭대학교***
{sungillkO, yongmink}@stkorea.net* kimhyunik@hanmail.net* iqjump@stkorea.net** kimeung@hanbat.ac.kr***

Dual Authentication Electronic Payment System using Bluetooth

Sungill KimO* Yongmin Kim* Hyunik Kim* Changhoon Jung** Eungkyeu Kim***
ST co., ltd.* Korea University* Hanbat National University***

요 약

최근 전자상거래의 활성화와 더불어 기존의 유선인터넷에서 사용하고 있는 전자지갑(S/W) 등 전자상거래 방식에서 Smart Card나 이동통신 단말기와 같은 독립적인 유/무선 단말을 사용하는 전자지불 시스템에 대한 관심이 고조되고 있다. 본 연구에서는 전자지불 시스템에 Bluetooth를 이용하여 안전한 사용자 인증 및 종단간의 보안을 제공 전자화폐의 발행/지불이 가능한 전자지불 시스템의 모델을 제시하고자 한다. 각 단말의 서브셋(subset)으로 Bluetooth 컨트롤 시스템과 이를 이용하는 전자지불 시스템으로서 전자지갑 및 전자화폐 발행기/자동판매기를 구현하여 각각의 보안 통신과 전자화폐의 발행/지불이 가능함을 나타냈다. 구현 결과물은 실제 전자지불 시스템에 적용이 가능할 것으로 보인다.

1. 서 론

최근 구축된 IT 인프라를 바탕으로 사용자 편의성을 증대시킨 전자 지불 시스템이 주목을 받고 있으며, 이에 관련된 하드웨어 및 소프트웨어가 속속 개발·상용화되고 있다. 특히 기존의 유선 통신 기반(인터넷 등)의 전자지불 방식에서 휴대전화, PDA 등 무선 통신 단말기를 이용한 전자지불 관련 시스템 산업이 그 관심의 대상이 되고 있다.

본 연구에서는 무선 전송 기술의 하나인 Bluetooth를 전자 지갑에 적용하였다. 또한 전자 지갑을 이용해서 안전한 지불 메커니즘이 이루어질 수 있는 지불 시스템을 설계하고 테스트를 행하여 실제로 활용할 수 있는 기반을 마련하고자 한다.

2. 전자 지불 시스템의 설계

Bluetooth 전자지갑을 이용한 전자지불 시스템은 상품 구입시 전자화폐를 대금 결제에 이용할 수 있다. 전자지갑은 무선 네트워크를 통해 전자화폐 발행 및 결제가 가능하며 전자화폐의 지불을 사용자가 요청한 시점에 이루어지는 직불 시스템(pay-now payment system)을 통해서 사용자의 거래은행 계좌잔고에서 지불할 금액만큼의 인출이 이루어진다.

2.1 지불 시스템의 보안

Bluetooth를 각 무선 단말의 서브셋으로 적용하여 지불 시스템을 설계함으로써 사용자 편의성을 도모하였다.

Bluetooth는 공개된 규격으로 케이블 없이 고정 또는 휴대 기기간의 근거리 무선 링크가 가능하며 링크 단에서의 128비트 키까지 사용하는 SAFER+ 알고리즘을 이용함으로써 종단간의 보안을 제공한다. 또한 모듈 간 링크 수준에서 상호 인증을 수행함으로써 인가되지 않은 장치의 접근을 통제할 수 있으며 보안 수준에 따라 3가지 모드로 나눌 수 있다. 블루투스가 이러한 보안 레이어를 제공하지만 사용자 인증에 대한 부분 및 보안의 취약점이 존재한다[1].

블루투스를 전자지불 시스템에 사용하기 위해서는 단말 인증뿐만 아니라 공개키 기반의 사용자 인증 시스템의 도입이 필요하다.

본 연구에서 제시한 전자지불 시스템에서는 거래의 기밀성과 무결성을 보장하기 위해서 블루투스에 의한 무선 암호화 통신을 제공하며 거래당사자간의 상호 인증은 공인인증서를 통해 이루진다. 단말 수준의 기기인증 및 거래당사자간의 상호 인증을 통해 안전한 거래가 이루어지도록 시스템을 설계하였다[2,3].

2.2 시스템 구성요소

전자지불 시스템은 블루투스 모듈을 서브셋으로 하는 전자지갑과 전자지갑을 초기 등록하는 전자지갑 등록기 및 전자지갑을 이용하여 전자화폐를 발행할 수 있는 전자화폐 발행기 그리고, 전자화폐를 이용하여 상품을 구입할 수 있는 자동판매기로 구성된다.

2.3 동작 시나리오

2.3.1 전자지갑 등록

① 은행의 전자지갑 등록 시스템 즉, 전자지갑 등록기를 이용하여 새로운 전자지갑을 은행의 사용자계좌에 등록한다.

② 전자지갑의 시리얼 넘버 및 PIN 값을 은행의 사용자의 계좌 정보에 저장한다.

③ 인증서 및 개인키 그리고, 인증서 접근 암호를 생성 및 입력하여 사용자의 전자지갑으로 전송 저장한다.

2.3.2 전자화폐 발행

① 등록된 전자지갑은 은행의 전자화폐 발행기에서 Bluetooth 보안 접속 및 사용자 인증 후, 사용자가 원하는 금액만큼의 전자화폐를 사용자의 계좌로부터 인출하여 발행될 수 있다.

② 전자화폐 발행기와의 접속 및 통신을 위해 사용자는 PIN 및 인증서 암호를 직접 입력하여 보안 인증을 받는다.

③ 발행된 전자화폐는 은행의 사용자 계좌 이용 정보와 연계되어 저장된다.

④ 전자화폐 발행 후, 발행정보는 전자화폐 발행기를 통해 사용자의 전자지갑으로 전송, 저장된다.

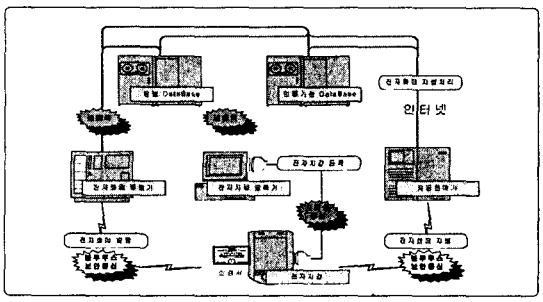
2.3.3 전자화폐 지불

① 자동 판매기에서 상품 선택 후, 전자화폐로 지불한다.

② 자동판매기와의 접속 및 통신을 위해 사용자는 PIN 및 인증서 암호를 직접 입력하여 인증을 받는다. 자동판매기는 전자화폐 발행기와 마찬가지로 은행 및 인증기관과 연동이 가능하다.

③ 전자지갑의 Bluetooth 보안 접속 및 사용자 인증을 거친 후, 사용자의 전자화폐로 결제한다. 결제는 지불 금액 만큼 사용자의 전자화폐 계좌에서 자동판매기 소유주 계좌로 이체된다.

④ 전자화폐 지불 후, 지불정보는 자동판매기를 통해 사용자의 전자지갑으로 전송/저장된다.

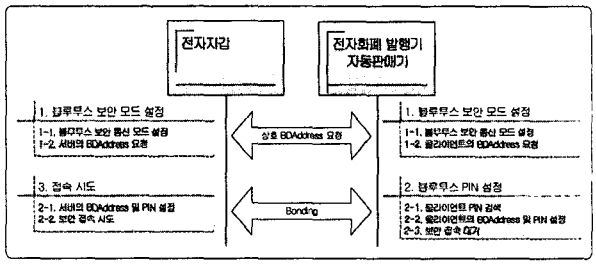


[그림 1] 전자 지불 시스템 구성도

2.4 전자 지불 프로토콜

2.4.1 Bluetooth 보안 접속

전자지갑과 전자화폐 발행기 및 자동판매기와의 통신시 쌍방의 Bluetooth 시스템은 보안통신을 위해 다음과 같은 프로토콜을 수행한다. 이 때, 접속을 시도하는 쪽은 Bluetooth 클라이언트(전자지갑)에 해당되며, 접속을 대기하는 쪽은 Bluetooth 서버(전자화폐 발행기 및 자동판매기)에 해당한다.

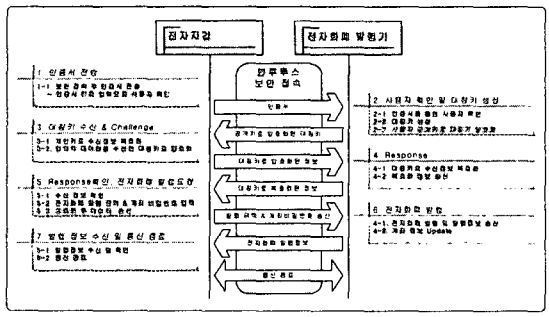


[그림 2] Bluetooth 보안 통신 설정 프로토콜

전자지갑은 전자화폐 발행기 및 자동판매기의 Bluetooth Device Address와 사용자 입력의 PIN을 이용하여 보안 접속을 시도한다. 만약 PIN값이 불일치할 경우는 통신 자체가 성립되지 않는다.

2.4.2 전자화폐 발행 및 인증

전자 화폐는 사용자의 요구로 사용자 은행 계좌에 있는 잔고 중 요구금액만큼 전자화폐 발행기를 통해서 발행된다. 이 때 전자화폐발행기는 Bluetooth에 보안 접속된 후 동작되며, 사용자의 인증 및 Session Key(일회용 대칭키)와 교환된다. 발행요청 및 발행정보의 암호화는 Session Key를 이용하며, 모든 발행 절차가 종료되면 Session Key는 소멸된다.

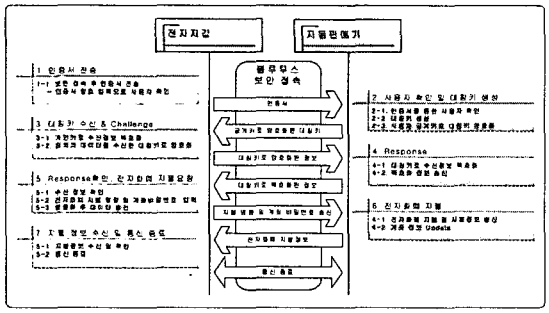


[그림 3] 전자 지갑 발행 프로토콜

2.4.3 전자화폐 지불 및 인증

사용자가 전자화폐로 거래가 가능한 자동판매기의 상품을 구입할 경우, 상품의 대금 지불 및 사용자 인증을 위한

프로토콜이 수행된다. 자동판매기는 사용자가 상품을 선택한 후, 전자화폐를 지불 수단으로 선택하면 인증기관 및 은행에 사용자 인증 및 대금 지불을 요청한다. 은행은 상품 대금을 사용자의 전자화폐에서 자동판매기 소유주의 계좌로 지불한다. 자동판매기는 구입하려고 하는 상품을 사용자가 선택 후, 지불방법을 사용자에게 선택하게 하며, 사용자가 전자지갑의 전자화폐로 결제를 선택할 경우에 작동하고, Bluetooth에 보안 접속된 후 동작한다.

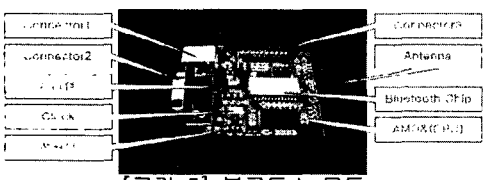


[그림 4] 전자 지갑 지불 프로토콜

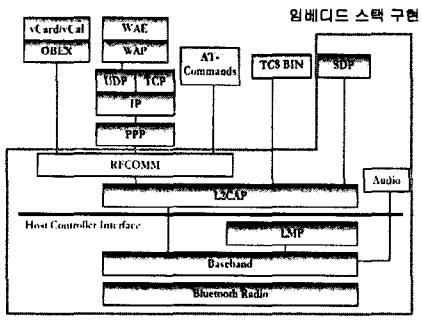
3. 개발 환경 및 구현

3.1 Bluetooth 시스템(BT_PC)

이 시스템은 전자지갑, 전자화폐 발행기 및 자동판매기의 Bluetooth 컨트롤 시스템이며, 이하 BT_PC 라 한다. BT_PC는 상위의 단말과 시리얼 통신으로 데이터를 송수신하며, Bluetooth의 보안접속 및 Bluetooth 자체 암호화 통신을 담당한다. 블루투스 모듈의 구현은 다음과 같다[4].



[그림 5] 블루투스 모듈



[그림 6] 블루투스 프로토콜 스택

3.2 전자지갑

전자지갑 등록기와 Serial 통신, 전자화폐 발행기 및 자동판매기와 BT_PC를 통한 Bluetooth 무선 통신을 사용한다. Window 계열의 MFC 개발 환경에서 구현한다.

3.3 전자지갑 등록기, 전자화폐 발행기 및 자동판매기

인증기관 및 은행 관련 기능은 전자화폐 발행기에 관련 데이터베이스 파일을 설치하여 데이터베이스 접근 표준인 ODBC를 사용하여 시험하였으며, 전자지갑 등록기 및 자동판매기도 같은 데이터베이스 파일을 사용하여 시험하였다.

4. 결론

Bluetooth를 이용한 무선 전자지갑은 Bluetooth 무선 통신 보안과 사용자의 인증 및 공개키를 이용한 세션키의 분배를 행함으로써 전자화폐의 발행 및 지불에 안전성을 높일 수 있도록 하였다. 실제 전자화폐가 발행되어 지불에 사용되는 것이 아니라 별도의 계좌를 통하여 지불이 이루어지므로 데이터의 복사 및 이중 사용의 문제를 해결코자 하였다. 이에 대한 안전성 문제는 향후 해결해야할 과제로 남아있다.

본 연구의 결과물은 소액의 지불이 가능한 상점이나 공공기관에 설치되어 있는 자동판매기 등에 적용 가능할 것이며 이로 인해 사용자 편리성이 증대된 안전한 지불 시스템의 구축이 가능할 것으로 보인다.

참 고 문 헌

[1] 서대희 외 3명, "Bluetooth Security에 관한 고찰", 정보보호학회지, 11권, 4호, pp.82~84, 2001. 8

[2] H.X.Mel and Doris Baker, Cryptography Decrypted, Addison Wesley, 2001

[3] 이문구 외2명, "Bluetooth 보안 모델의 설계", 전자상거래학회 창간호, pp.147~162, 2000.4

[4] Jennifer Bray and Charles F. Sturman, Bluetooth Connect without Cables, PRENTICE HALL, 2001