모바일 전자 ID 지갑 시스템

김수형, 김승현, 김덕진, 정관수, 진승헌
한국전자통신연구원 정보보호연구본부
e-mail : {lifewsky,ayo,kdj,ksjung,jinsh}@etri.re.kr

Mobile Digital Identity Wallet

Soo-Hyung Kim, Seung-Hyun Kim, Deok-Jin Kim, Kawn-Soo Jung, Seung-Hun Jin
Information Security Research Division
Electronics and Telecommunications Research Institute

요 약

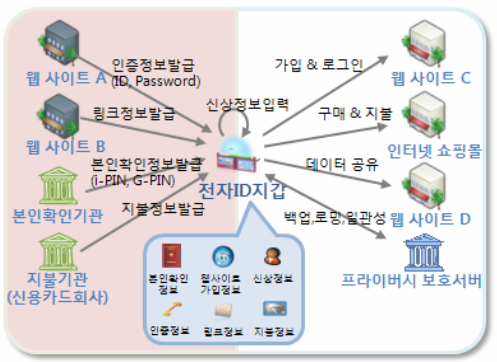
전자 ID 지갑은 일상생활에서 사용하는 지갑처럼 인터넷 상에서 사용되는 사이버 지갑으로, 사용자의 개인정보(주소, 전화번호 등), 인증정보, 지불정보 등과 같은 사용자의 Identity 정보를 보관하고 있다가 필요한 시점에 저장된 정보를 사용자의 통제 하에 자유롭게 이용할 수 있는 서비스 시스템이다. 모바일 전자 ID 지갑 시스템은 전자 ID 지갑 시스템의 구성 요소 중 하나로 개인의 모바일 단말장치에서 운영될 수 있는 소프트웨어로 구현되었으며, 사용자 인터페이스가 빈약한 모바일 단말장치에서도 사용자의 불편 없이 모바일 인터넷을 보다 안전하게 이용할 수 있는 방법들을 제공한다. 본 논문에서는 안전하고 신뢰할 수 있는 인터넷 환경 구축을 위해 개발된 기술들 중 하나인 모바일 전자 ID 지갑 시스템을 소개하고자 한다.

1. 서론

최근 인터넷 비즈니스의 주요 화두는 SNS(Social Networking Service)와 모바일인 것으로 보여진다. 특히 모바일 인터넷 분야에서는 HSDPA/HSUPA 와 같은 초고속 무선 통신기술과 Full Browsing 폰 및 무선 인터넷 응용에 적합한 스마트폰들이 대거 등장하고, 모바일 SNS 사이트들이 소개되기 시작하면서부터 일반 사용자들에게까지 관심의 대상이 되고 있는 실정이다. 모바일 인터넷을 활성화하기 위해 시급히 해결해야 하는 문제 중 하나는 보안이다. 현재의 핸드폰이 예전보다 좋은 프로세싱 파워를 가지고 있는 것이 사실이지만 아직까지 공개키 쌍을 생성하거나 PKI 기반 기술을 수행하는데 어려움이 있다. 그리고 ActiveX 와 같은 웹 기술이 활성화된 국내 인터넷 환경에서 모바일 단말의 브라우저를 통해 지불이나 인증서를 처리하는 것은 현재로선 불가능하다. 또한 대부분의 모바일 단말이 빈약한 사용자 입력 인터페이스를 제공하여, 사이트 가입에 필요한 개인 정보 입력은 논외로 하더라도 사이트에 로그인하기 위해 필요한 Id 와 패스워드를 입력하는 것조차 사용자들의 모바일 이용을 크게 제약하는 요인이 되고 있다. 따라서 위와 같은 문제를 해결하기 위한 방법들이 많이 연구되고 있으며, 본 논문에서 소개되는 모바일 전자 ID 지갑 또한 앞서의 문제들을 해결하는 종합 솔루션이 될 것으로 예상하고 있다.

2. 전자 ID 지갑 시스템 개요

전자 ID 지갑 시스템은 일상생활에서 사용하는 지갑처럼 인터넷 상에서 사용되는 사이버지갑으로, 사용자의 개인정보(주소, 전화번호 등), 인증정보, 지불정보 등과 같은 사용자의 Identity 정보를 보관하고 있다가 필요한 시점에 저장된 정보를 사용자의 통제 하에 자유롭게 이용할 수 있는 시스템이다. 그림 1 과 같이 전자 ID 지갑이 관리하는 데이터는 본인확인 정보, 사이트 가입정보, 신상정보, 인증정보, 지불 정보 등이며, 특별히 웹 사이트에서 저장되고 있는 자기 Identity 에 대한 메타정보를 포함한다. 전자 ID 지갑은 메타정보를 이용하여 사용자의 개인정보가 어디에 저장되어 있고 어떠한 내용인지를 사용자가 사이트를 방문하지 않아도 확인할 수 있도록 하며, 메타정보로 링크된 데이터를 사이트에 전달하는 기능을 제공한다.

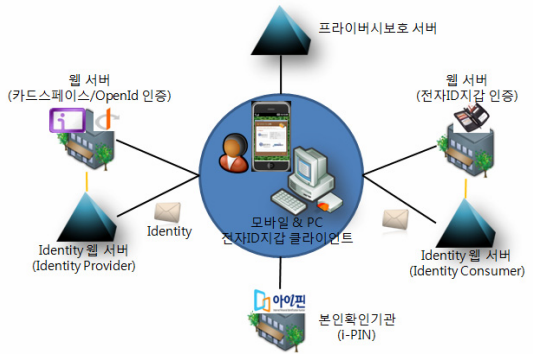


(그림 1) 전자 ID 지갑 시스템 개요

전자 ID 지갑 시스템은 IDM(Identity Management) 기술[1] 분류에 속하는 시스템이며, 특히 사용자 중심의(user-centric) ID 관리 모델[6][7][8]이 적용된 시스템이다[2]. 사용자 중심이란 모든 정보가 사용자를 통하여 흘러간다는 것이며, 이 말은 정보의 흐름을 사용자가 직접 통제할 수 있다는 의미를 내포하고 있다. 즉, 전자 ID 지갑은 정보의 흐름을 사용자가 직접 통제할 수 있도록 하여, 사용자가 의식하지 못하고 자기 정보가 노출되거나 불특정 서버 간에 공유되는 것을 방지할 수 있도록 한다. 또한 전자 ID 지갑은 Phishing/Pharming 사이트에 사용자가 개인 정보를 노출하는 것을 차단할 수 있어, 최근 인터넷에서 크게 이슈화되고 있는 인터넷 상에서 일어나는 프라이버시 문제를 다양한 측면에서 해결할 수 있다.

3. 전자 ID 지갑 시스템 구성

전자 ID 지갑 시스템은 그림 2 와 같이 크게 서버 시스템과 클라이언트 시스템으로 구성된다. 서버 시스템은 전자 ID 지갑 클라이언트와 가입/인증 프로토콜을 수행하는 인증서버와 공유 프로토콜을 수행하는 ID 공유 서버로 구성되며, 그 외 프라이버시 기능을 강화하기 위한 프라이버시 보호 서버, 본인확인 기능 수행을 위한 본인확인 서버, 기타 웹 서버가 포함된다. 클라이언트 시스템은 PC 용 전자 ID 지갑과 모바일용 전자 ID 지갑으로 구성되는데, 전자 ID 지갑 클라이언트 간 데이터의 이동 기능을 제공하여 사용자는 언제 어느 단말을 통해서나 동일한 인터넷 서비스를 이용할 수 있도록 한다.



(그림 2) 전자 ID 지갑 시스템 구성

4. 모바일 전자 ID 지갑 시스템 서비스

모바일 전자 ID 지갑 시스템은 아래 그림 3 과 같이 크게 가입 서비스와 인증 서비스를 제공한다. 모바일 전자 ID 지갑을 통한 사이트 가입은 기존의 방식과는 달리, 사용자의 입력을 최소화하기 위해, 자동 생성된 비밀정보와 이미 관리되고 있는 사용자 개인신상정보를 사용하여 가입 절차를 수행하며, 사용자는 모바일 단말에서 확인버튼을 누르는 것 만으로 가입을 완료할 수 있다. 그리고 모바일 전자 ID 지갑을 통한 사이트 인증은 가입 시에 저장된 사이트 정보를 이용하여 인증절차를 수행하여, 사용자는 ID 와 패스워드를 입력하지 않아도 사이트에 로그인할 수 있다. 이러한 가입/인증 서비스는 모두 안전한 프로토콜을 통해 수행되며, 기존의 SSL 을 통한 가입/인증 절차 이상의 안전을 보장하면서도 사용자에게 편리성을 제공하는 장점을 갖는다.

(그림 3) 전자 ID 지갑 시스템 기능

아래는 위와 같은 서비스를 제공하기 위해 필요한 세부 기능들을 좀 더 자세히 설명한다.

4.1 사이트 가입 및 탈퇴

모바일 전자 ID 지갑은 웹사이트에 가입하거나 탈퇴하기 위한 새로운 방법을 제시한다. 예를 들어 설명하면, 모바일 전자 ID 지갑을 통한 가입 흐름은 다음과 같다. 사용자가 브라우저를 통해 사이트에 접속한 후 가입 버튼을 클릭하면, 가입 웹 페이지는 브라우저를 통해 사용자의 단말장치에 설치된 전자 ID 지갑 클라이언트를 호출한다. 호출된 클라이언트는 해당 웹 사이트가 전달하는 가입 파라미터를 분석하고, UI 를 통해 사용자의 가입 동의를 받은 이 후, 웹 사이트의 인증 서버와 가입 프로토콜을 수행한다. 위에서의 가입 파라미터는 가입 프로토콜 수행에 필요한 서비스 URL, 사이트 기본 정보, 보안 정보 등이 포함된다. 모바일 전자 ID 지갑의 가입 프로토콜은 패스워드 기반의 키 교환(Password-Based Key Exchange) 프로토콜[3] [4]을 변형하여 설계되었다. 가입 프로토콜이 정상적으로 수행 완료되면, 모바일 전자 ID 지갑은 가입된 사이트의 정보를 사용자 단말의 암호화된 저장소에 저장하게 된다. 이렇게 저장된 사이트 정보를 우리는 사이트카드로 명하고 있다.

통상의 사이트들은 대부분 가입절차 상에서 가입을 원하는 사용자들의 신상정보를 입력 받는데, 모바일 단말을 사용하는 사용자가 이러한 정보를 입력하는 것은 매우 힘든 과정이다. 따라서 모바일 전자 ID 지갑은 미리 등록되어 관리하고 있는 개인신상정보를 앞서의 가입 프로토콜 후에 생성되는 세션 키를 사용하여 암호화 한 후, 인증 서버에 전달하는 기능을 제공한다. 우리는 위의 개인신상정보가 저장된 하나의 인스턴스(instance)를 프로파일 카드라고 하며, 개인의 용도와 취향에 따라 사용할 수 있도록 다수개의 프로파일 카드가 생성되고 저장되는 것을 허용하고 있다. 대부분의 인터넷 사용자들은 다수의 사이트에 등록되어 있는 상태이기 때문에, 이미 가입된 사이트에서 가입 절차를 재 수행하는 것은 사이트의 사용자 관리

측면에서 어려움이 있다. 따라서 전자 ID 지갑은 이미 사이트에 가입된 사용자들이 사이트카드를 발급 받을 수 있도록 전환가입이라는 기능을 제공한다. 즉, Id 와 패스워드로 인증정보를 등록한 사용자들이라 하더라도 전환가입 기능을 통해 사이트 카드를 발급받고 모바일 전자 ID 지갑이 제공하는 여러 기능들을 제공 받을 수 있도록 한다.

4.2 상호 인증

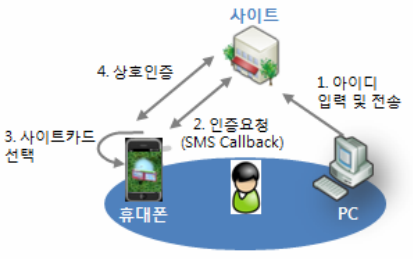
모바일 전자 ID 지갑을 통해 사이트에 가입한 사용자는 기존의 Id 와 패스워드와 같은 인증정보를 기억하고 있다가 입력해야 하는 수고 없이도, 모바일 전자 ID 지갑을 통해 사이트 카드를 선택하는 것만으로 로그인을 수행할 수 있다.

사용자가 직접 인증정보를 관리하지 않아도 된다는 것은 여러 측면에서 장점을 갖는다. 일반적인 사용자라 하더라도 보통 수십 개의 사이트에 가입되어 있기 때문에, 대부분의 사용자는 동일한 Id 와 패스워드를 사용하여 사이트에 등록하는 습관을 가지고 있다. 이러한 사용자의 습관으로 인해 특정 사이트가 해킹되어 가입자 인증정보 목록이 노출되었을 때, 전체 인터넷 시스템의 신뢰가 저하되는 문제를 야기한다. 그리고 자주 사용하는 Id 과 이미 다른 사용자에 의해 등록되어 있거나, 사이트마다 패스워드 보안 강도가 달라 다르게 입력한 패스워드로 인하여 Id 및 패스워드를 저장 미디어에 등록해 두게 되어 분실·노출되는 경우가 있으며, 패스워드를 재 등록하는 절차를 수행하는 등의 어려움이 실존하고 있다. 위와 같은 문제는 모두 모바일 전자 ID 지갑을 통해 해결된다. 모바일 전자 ID 지갑은 가입 프로토콜 수행 시에 랜덤하게 생성된 공유 키를 저장하고 있다가 이 공유 키를 이용하여 인증 프로토콜을 수행하므로 사용자는 패스워드를 기억할 필요가 없으며, 생성된 공유키는 사이트마다 다르게 등록되어 특정 사이트가 해킹되어 공유키가 노출되더라도 다른 사이트에서는 이용할 수 없는 구조를 갖는다. 그리고 모바일 전자 ID 지갑의 인증 프로토콜은 서버와 클라이언트 간의 상호인증에 기반한 프로토콜로 설계되었기 때문에 사용자는 Phishing/Pharming 에 대한 두려움을 덜 수 있다.

모바일 전자 ID 지갑은 인터넷 실명제 수단의 하나로 이용되는 본인확인 서비스의 고도화를 위해 기존의 주민번호대체수단인 i-PIN 또는 g-PIN 시스템과 연동하는 수단을 마련하고 있다. 모바일 전자 ID 지갑에 등록된 사이트카드 중에 본인확인기관이 발급한 사이트카드를 우리는 PIN 카드라고 하는데, PIN 카드는 특정 웹 사이트가 사용자에게 본인확인 정보를 요청할 때 사용되는 카드이며, 사용자가 PIN 카드를 선택하면 본인확인기관의 서버와 모바일 전자 ID 지갑은 상호인증을 거쳐 내부 프로세스에 의해 본인확인 프로토콜이 수행된다. 따라서 기존과 같이 사용자가 본인확인기관 사이트에 방문하여 자기가 가입한 본인확인기관을 선택하고 인증정보를 입력하는 하는 수고를 경험하지 않아도 된다[5].

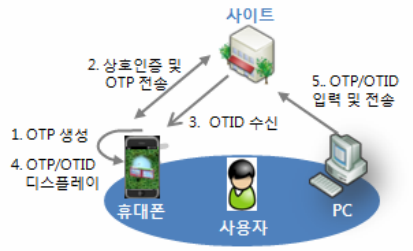
4.3 강화 인증

공공장소에서 높은 컴퓨팅 파워와 고해상도 디스플레이가 필요한 경우에 종종 공용 PC 를 사용하기도 하는데, 공용 PC 에 설치된 Malware 등을 통해 사용자의 로그인 정보가 노출되는 경우, 개인에게 치명적인 문제를 야기할 수 있다. 이러한 문제를 해결하기 위해, 모바일 전자 ID 지갑은 두 가지 방식의 강화인증(strong authentication) 기능을 제공한다. 첫 번째 방법은 그림 4 와 같이 SMS 을 통해 모바일 전자 ID 지갑이 PC 에서 입력해야 하는 인증정보를 대신 제공해주는 형태이며, 두 번째 방법은 그림 5 와 같이 기존의 OTP(One-Time Password)를 응용한 형태로 제공된다.



(그림 4) 강화인증 흐름(SMS)

그림 4 와 같이, SMS 을 이용한 강화인증 방법은 절차는 다음과 같다. 사용자가 PC 의 브라우저를 통해 사용자 Id 를 입력하여 전송하면 사이트는 이미 등록된 사용자 핸드폰 번호로 SMS 메시지를 전송한다. 해당 SMS 메시지에는 모바일 전자 ID 지갑 AppId, 사이트의 인증 서비스 URL, 임시 세션 Id 등이 포함된다. 모바일 전자 ID 지갑은 SMS 로 전달된 파라미터를 분석하고, 사용자로부터 사이트 인증을 수행할지 묻는다. 만약 모바일 전자 ID 지갑이 사전에 활성화된 상태가 아니라면 모바일전자 ID 지갑의 사용자 인증 코드를 사용자로부터 입력 받아 검증하는 절차를 먼저 수행한다. 이 후 모바일 전자 ID 지갑과 사이트는 상호인증을 수행하며, 인증 프로토콜이 완료하면 해당 사이트는 PC 브라우저를 인증 결과 페이지로 리다이렉션(redirect) 한다.



(그림 5) 강화인증 흐름(OTP/OTID)

위의 그림 4 에서 소개하는 방법은 사이트가 SMS 비용을 부담해야 한다는 것과 사용자의 Id 가 공용 PC 에 노출될 수 있다는 문제가 있는데, 프라이버시에 민감한 사용자는 이러한 정보도 노출하는 것을 꺼릴 수 있다. 따라서 우리는 이러한 문제를 해결하기 위하여 다른 방안을 함께 준비하였다.

일반적인 OTP 기법은 OTP 단말(전용기기 또는 핸드폰 소프트웨어)을 통해 생성된 OTP 와 사용자 Id 그리고 패스워드를 함께 입력하여 강화인증을 수행하는 목적으로 사용된다. 그러나 모바일 전자 ID 지갑은 그림 5 에서 설명하는 것과 같이, 상호인증 프로토콜을 수행하여 생성된 세션 키를 사용하여 서버에서 생성한 임시 ID 와 모바일 전자 ID 지갑에서 생성한 OTP 를 안전하게 교환하고, 이렇게 교환된 정보를 사용자가 임시 인증정보로 사용하는데 차이가 있다. 사용자가 Id 와 패스워드를 전혀 노출하지 않으므로 공용 PC 라는 환경에 적합하면서도, 이전의 OTP 기법들보다 효율적이면서고 안전한 장점을 갖는다.

5. 결론 및 향후 연구

지금까지 모바일 전자 ID 지갑의 개념과 구성요소들 및 제공하는 서비스들에 대해 간략히 소개하였다. 모바일 전자 ID 지갑은 모바일 인터넷 환경이라는 특성을 이해하여 설계 · 구현되었으며, 모바일 사용자에게 기존의 PC 환경보다 더 안전하면서도 편리한 인터넷 환경을 제공할 것으로 기대하고 있다. 또한 앞으로 사용자들로부터의 피드백을 받아 계속 발전시켜 나갈 계획을 가지고 있다.

이 논문에서는 현재까지 개발 완료된 모바일 전자 ID 지갑의 가입과 인증 등의 보안 서비스 위주로 설명되었지만, 우리는 전자 ID 지갑의 핵심 기능 중 하나인 Identity 정보의 공유 및 동기화 서비스를 통해 웹 사이트 간 서비스 매쉬업, 개인화 서비스가 가능한 기술들을 개발 중에 있다. 또한 전자 ID 지갑의 개념을 유비쿼터스 환경 또는 물리 환경까지를 고려하여 확장시키기 위한 연구를 준비하고 있다.

6. Acknowledgment

본 연구는 정보통신부 및 정보통신연구진흥원의 IT 신성장동력핵심기술개발사업의 일환으로 수행하였음. [IITA-2007-S-601-02, 자기통제 강화형 전자 ID 지갑 시스템 개발]

참고문헌

[1] 진승헌 외, “Digital Identity Management 기술백서”, 2007

[2] 조영섭, 진승헌, “사용자 중심 ID 관리 기능을 제공하는 전자 ID 지갑 시스템”, 전자통신동향분석 제 23 권 제 4 호, 2008/8

[3] Y. Oiwa 외. “Mutual Authentication Protocol for HTTP”, 2008

[4] International Organization for Standardization, “Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets,” ISO Standard 11770-4, May 2006

[5] 염흥열, 이석래, “인터넷 상에서 주민등록번호 대체수단 발전방향”, 전자공학회지 제 32 권 제 11 호, pp. 61-73, 2005/11

[6] Microsoft, “Introducing Windows CardSpace”, http://msdn.microosft.com/

[7] Higgins Project, http://www.eclipse.org/higgins

[8] OpenId, http://www.openid.net