신원 선택기를 이용한 주민번호대체수단 확장 서비스

김승현*, 최대선*, 진승헌*
*한국전자통신연구원 SW 콘텐츠연구부문
e-mail : ayo@etri.re.kr

i-PIN(internet Personal Identification Number) extension services using the Identity Selector

Seung-Hyun Kim*, DaeSeon Choi*, Seung-Hun Jin*
*S/W Contents Research Division, Electronics and Telecommunication Research Institute

요 약

주민번호대체수단은 주민번호를 대체하기 위한 본인확인정보로서, 5 개의 민간기업이 운영하는 민간 i-PIN 과 행정안전부가 운영하는 공공 i-PIN 이 서비스를 제공하고 있다. 하지만 주민번호대체수단이 더욱 활성화되기 위해서는 기존에 제시된 보안성, 편의성 문제를 해결해야 한다. 본 논문은 신원 선택기를 추가하여 i-PIN 의 프로토콜을 변경하지 않는 범위 이내에서 i-PIN 의 단점으로 지적되는 로그인 번거로움, i-PIN 사이트 기억 문제, 피싱을 비롯한 보안 문제를 해결하는 방안을 제시하였다. 제안하는 방법은 사용자가 가입한 i-PIN 제공자에 접근하는 단계, i-PIN 제공자에 id 와 비밀번호를 입력하는 단계를 없애고, 신원 선택기를 통해 사용할 신원 정보를 선택하는 것만으로 처리되도록 하였다. 본 기술은 ETRI 에서 개발중인 전자 ID 지갑 솔루션을 통해 구현되었으며, 해당 서비스는 2009 년 중에 민간 i-PIN 제공자를 통해 시범 도입될 예정이다.

1. 서론

주민등록번호는 국가가 국민에게 부여하는 고유 번호로서, 오프라인뿐만 아니라 온라인 환경에서도 개인을 식별하는 과정에 사용된다. 대부분의 웹사이트는 사용자를 등록하는 과정에서 주민등록번호를 필수적으로 입력하도록 요구하고 있다. 하지만 사용자의 주민등록번호가 여러 웹사이트의 데이터베이스에서 관리됨에 따라, 주민등록번호가 유출되거나 불법적으로 사용되는 등의 다양한 문제가 발생하고 있는 실정이다.

인터넷상에 개인의 주민등록번호와 이름이 유포돼 오남용 문제가 심각해짐에 따라, 가상의 주민등록번호와 같은 대체수단을 통해 인터넷을 이용할 수 있게 하여 개인정보를 보호하려는 취지로 i-PIN 서비스가 민간 및 정부 기관에 의해 시행되고 있다. 주민등록번호가 개인을 식별할 수 있도록 영구적으로 지정된 고유 식별 번호인 반면, i-PIN 은 일시적으로 개인을 식별하기 위해 제 3 의 신뢰기관이 부여하는 사용자 식별번호이다. 최근에 발생한 대규모 개인정보 유출 사고 등으로 주민번호대체수단의 의무도입이 고려되고 있는 시점이지만, 보안성, 편의성, 연동 문제 등이 우선적으로 해결되어야만 한다.

본 논문에서는 주민번호대체수단의 보안성과 편의성을 제고하는 방안을 제시한다. 신원 선택기를 적용하여 i-PIN 시스템의 단점으로 지적되는 id 와 비밀번호 입력의 번거로움, 가입한 i-PIN 사이트를 기억하지 못하는 문제, 피싱(Phishing) 및 파밍(Pharming) 등의 보안 문제를 해결한다.

본 논문의 구성은 다음과 같다. 2 장에서 주민번호대체수단을 소개하고, 기존에 제시된 단점인 보안성과 편의성 문제를 소개한다. 3 장에서는 신원 선택기를 이용한 방안을 제시하고, 동작 방식을 설명한다. 마지막으로 4 장에서는 결론 및 적용 상황을 보인다.

2. 주민번호대체수단

주민번호대체수단은 주민번호를 대체하기 위한 본인확인정보로서 출생연월일, 성별 등의 개인정보를 전혀 포함하지 않고 있으며, 가입자가 언제든지 갱신, 폐지를 할 수 있으며, 본인확인 정보는 가입자와 한정적인 시간 내에서만 유일성을 보장하고, 사용자가 신뢰하는 본인확인기관에 의하여 발급되는 난수이다.[1] 주민번호대체수단은 5 개의 일반 기업(한국신용평가정보, 한국신용정보, 서울신용평가정보, 한국정보인증, 한국전자인증)의 민간 i-PIN 과 행정안전부의 공공 i-PIN 에서 각기 다른 방식으로 제공되고 있다. 민간 i-PIN 의 경우 2008 년 2 월 기준으로 99 개 사이트에 도입되어 전체 114,112 건이 발급되었으며 [2], 공공 i-PIN 은 2009 년까지 전 공공기관에 도입 예정이다[3].

주민번호대체수단을 통해 개인의 신원을 안전하게 확인하며, 개인정보에 대한 자기 통제권을 확보하게 된다. 그러나 주민번호대체수단이 더욱 활성화되기 위해서는 기존에 제시된 보안성, 편의성, 연동 문제를 해결해야 한다. 따라서 본 논문에서는 그 중, 주민번

호대체수단의 보안성, 편의성 문제를 해결하는 방안을 제시한다.

i-PIN 서비스는 사용자 편의성과 보안에 관련된 문제가 있다. 먼저 사용자 편의성과 관련하여 i-PIN 사이트의 선택 및 로그인 과정에서의 번거로움이 존재한다. 현재 i-PIN 서비스를 제공하는 사이트는 6 개에 달하며, 유사한 인터페이스를 제공하지만 실제로 구동하는 내부 방식은 사이트마다 다르다. i-PIN 서비스가 주민번호대체수단으로 사용되기 때문에 사용자는 주로 웹사이트에 가입할 때만 해당 서비스를 사용하게 된다. 하지만 각 웹사이트는 각자 선호하는 i-PIN 서비스를 사용자에게 먼저 제시하고, 사용자가 타 i-PIN 사이트를 사용하고 싶은 경우 이를 직접 선택하도록 요구한다. 이는 사용자가 자신이 가입한 i-PIN 사이트를 기억해야 하며 직접 해당 i-PIN 사이트로 이동해야 한다는 불편함을 초래한다. 표 1 에서 알 수 있듯이, 민간 i-PIN 기관의 이름은 서로 유사하기 때문에 일반인들이 구분하기 어렵다. 또한 i-PIN 사이트는 일반 웹사이트와는 달리 높은 수준의 보안을 요구하기 때문에 표 1 에서 보이는 것처럼 복잡한 id 와 비밀번호를 사용해야 한다. 따라서 사용자가 i-PIN 사이트에 사용하는 로그인 정보를 기억하는 것 또한 불편함을 초래할 수 있다.

본인확인기관	Id 자리수	Pw 자리수
행정안전부	7-15	7-20
한국신용정보	6 이상	6-20
한국신용평가	6-16	8-20
서울신용평가	5-8	6-8
한국정보인증	공인인증서 사용	
한국전자인증	현재 서비스 잠정중단	

(표 1) 주민번호대체수단 제공자들의 보안정책

보안성 측면에서 i-PIN 서비스는 피싱(Phishing)이나 파밍(Pharming), 키보드 해킹 문제가 우려된다. 즉, 악의적인 사이트가 임의의 i-PIN 로그인 페이지를 만들어 사용자에게 로그인 정보를 입력하도록 속일 수 있다. 현재의 i-PIN 서비스는 팝업 페이지로 구동되어 사용자가 로그인 정보를 입력하도록 되어 있다. 그러나 사용자가 팝업 페이지에서 확인하는 정보만으로는 해당 i-PIN 서비스가 올바른지 판단하기 어렵다. 따라서 사용자가 가입한 i-PIN 서비스 사이트 정보와 로그인 정보를 도용 당하는 문제가 우려된다. 또한 i-PIN 사이트에 id 와 패스워드를 입력하는 과정에서 키보드 해킹이 발생하여 로그인 정보가 노출 당할 수도 있다. 각 i-PIN 제공자는 별도의 보안 솔루션을 설치하도록 권고하지만, 특정 브라우저에서만 동작 가능하고 사용자가 임의로 실행을 제한할 수 있다.

3. 제안하는 방법

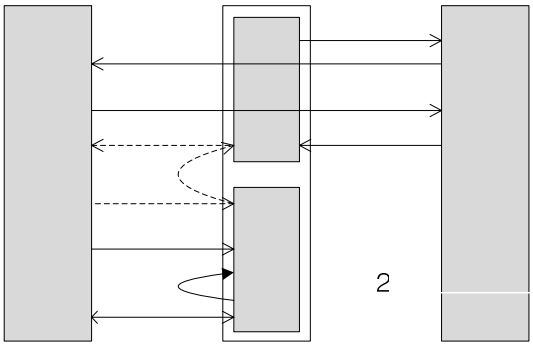
본 논문에서는 신원 선택기를 추가하여 i-PIN 의 프로토콜을 변경하지 않는 범위 이내에서 i-PIN 의 단점으로 지적되는 i-PIN 로그인 번거로움, i-PIN 사이트 기억 문제, 피싱 및 파밍 문제를 해결한다. 제안하는 방법은 사용자가 가입한 i-PIN 서비스 공급자에 접근하는 단계, i-PIN 서비스 공급자에 접근하여 id 와 비밀번호를 입력하는 단계를 없애고, 신원 선택기를 통해 사용할 신원 정보를 선택하는 것만으로 처리되도록 하였다. 또한 제안하는 방법은 사이트에 최소한의 수정만을 요구하여 i-PIN 서비스 제공자에게만 변경을 가하는 것만으로 동작할 수 있도록 한다.

신원 선택기는 사용자의 온라인 신원정보를 통합 관리하는 툴이다. 해외에는 Microsoft 사의 CardSpace[4], Eclipse 재단의 Higgins[5] 등이 있으며, 국내는 ETRI 의 전자 ID 지갑[6]이 신원 선택기와 관련된 프로젝트를 진행하고 있다. 신원 선택기는 주로 가입한 사이트 목록과 제출한 개인정보 등을 보관하고 있으며, 사용자가 간편하게 로그인 및 정보 제출 내역을 확인하고 제어할 수 있는 기능을 제공한다.

신원 선택기에서 사용자의 신원정보는 카드 타입으로 보관되며, 카드를 선택하는 것으로 해당 정보가 제출된다. 사용자와 사이트가 통신하는 방법은 각 솔루션마다 다르다. 전자 ID 지갑인 경우, 패스워드에 해당하는 SS(Shared Secret)를 사이트와 신원 선택기만 공유하고 있으며 PAKE(Password-Authenticated Key Exchange) 방식으로 공유키를 생성한 뒤에 프로토콜 메시지를 송수신한다. SS 는 사이트 가입시 랜덤으로 생성하기 때문에 사이트의 보안수준을 만족하기 쉬워지며, 사이트별로 유일하게 생성되기 때문에 해킹과 같은 공격으로 개인정보가 노출된 경우에도 피해가 한정된다.

신원 선택기를 i-PIN 서비스에 적용할 경우, 카드에는 사용자가 가입한 i-PIN 사이트 정보가 포함된다. 카드를 선택하는 것으로 로그인 절차가 수행되기 때문에 i-PIN 가입 및 사용이 간편해진다. 사용자는 어느 사이트에 가입했는지, id/pw 가 무엇인지 기억할 필요 없이, 생성된 i-PIN 카드 중에 하나만 선택하면 된다. 또한 사이트 로그인 및 개인정보 제출 시, 별도로 입력하는 정보가 없기 때문에 키로거와 같은 공격에 대처할 수 있다. 또한 카드에 저장된 사이트 주소, SS 정보를 이용하여 사이트와 상호인증을 수행하기 때문에 피싱 및 파밍 공격을 회피할 수 있다.

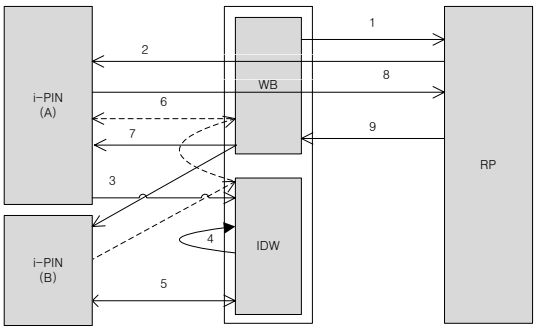
그림 1 은 신원 선택기를 통해 i-PIN 서비스를 제공받는 절차를 보여준다. 사용자가 웹브라우저(WB)를 통해 가입 등의 서비스를 요청하면, 사이트는 사용자를 i-PIN 제공자로 이동시켜 본인확인을 받도록 한다.(step 1,2) 이 단계에서 사이트(RP)는 i-PIN 제공자에게 i-PIN 요청 메시지를 전달한다. I-PIN 제공자는 사용자의 신원을 확인해야 하는데, 사용자가 신원 선택기를 이용한 방식을 선택한 경우(step3), 신원 선택기(IDW)가 구동하여 사전에 i-PIN 제공자로부터 발급받은 카드를 출력하고 사용자가 선택하도록 한다.(step4) 그림 1 에서는 신원 선택기를 구동한 i-PIN 제공자와 사용자가 선택한 i-PIN 카드의 발급자가 동일하기 때문에, 해당 i-PIN 제공자와 로그인 절차를 수행하는 것을 볼 수 있다.(step5) 로그인이 완료된 이후, i-PIN 제공자는 인증 세션을 설정하고 신원 선택기에게 자



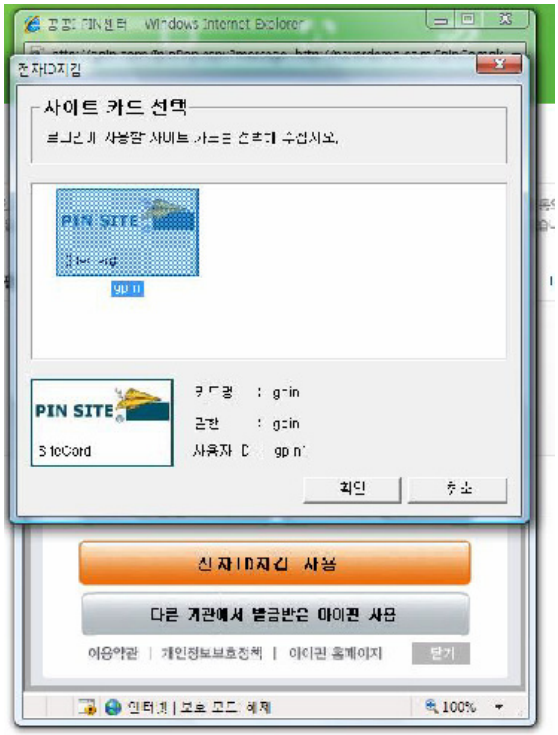
(그림 1) 주민번호대체수단 확장서비스 시나리오 – 하나의 i-PIN 제공자를 사용하는 경우

신의 i-PIN 제공자 식별자를 전달한다. 신원 선택기는 해당 식별자를 웹브라우저에게 전달하여 i-PIN 제공자의 i-PIN 응답 메시지를 제공하는 엔드포인트에 i-PIN 응답 메시지를 요청하도록 한다.(step6) i-PIN 제공자는 인증 세션을 확인한 뒤 i-PIN 응답 메시지를 작성하여 i-PIN 요청 메시지를 보낸 사이트로 사용자를 돌려보낸다(step7). 사이트는 해당 메시지를 검증한 뒤에 사용자가 요청한 서비스를 계속 진행한다.(step 8)

그림 2 는 신원 선택기를 통해 i-PIN 서비스를 제공받는 과정에서 사이트가 가입한 i-PIN 제공자 A 와 사용자가 가입한 i-PIN 제공자 B 가 다른 경우의 구동절차를 보여준다. Step1-3 은 그림 1 의 절차와 동일하나, 사용자가 선택한 카드의 발급자 B 와 신원 선택기를 구동한 i-PIN 제공자 A 가 다르기 때문에 다음 절차가 달라진다.(step4) 신원 선택기는 카드의 발급자인 i-PIN 제공자 B 와 로그인 절차를 수행한다.(step5) 로그인 후, i-PIN 제공자 B 는 인증 세션을 설정하고 신원 선택기에게 자신의 i-PIN 제공자 식별자 B 를 전달한다. 신원 선택기는 해당 식별자 B 를 웹브라우저를 통해 i-PIN 제공자 A 에게 전달하여 응답 메시지를 요청하도록 한다.(step6) i-PIN 제공자 A 는 식별자 B 를 확인하고 i-PIN 연동 메시지를 생성하여 i-PIN 제공자 B 에게 사용자의 i-PIN 응답 메시지를 요청한다. i-PIN 제공자 B 는 인증 세션을 확인한 뒤 i-PIN 응답 메시지를 작성하여 i-PIN 연동 메시지를 보낸 i-PIN 제공



(그림 2) 주민번호대체수단 확장서비스 시나리오 – 두 개의 i-PIN 제공자를 사용하는 경우



(그림 3) 주민번호대체수단 확장서비스의 구동화면

자 A 로 사용자를 돌려보낸다(step7). i-PIN 제공자 A 는 i-PIN 연동 메시지를 해석한 뒤, i-PIN 요청 메시지를 보낸 사이트(RP)에게 i-PIN 응답 메시지를 전달한다.(step 8). 사이트는 해당 메시지를 검증한 뒤에 사용자가 요청한 서비스를 계속 진행한다.(step 9)

그림 3 은 현재 구현된 주민번호대체수단 확장서비스의 구동화면을 보인다. 기존의 i-PIN 로그인 화면에 '전자 ID 지갑 사용' 버튼이 추가되어 있으며, 해당 버튼을 클릭하면 전자 ID 지갑이 구동한다. 전자 ID 지갑은 i-PIN 사이트에서 발급받은 카드를 조회하여 사용자에게 보여준다. 그림 3 에서 사용자가 발급받은 공공 i-PIN 카드 1 개가 보이지만, 만일 사용자가 타 i-PIN 제공자에서도 카드를 발급받은 경우, 해당 카드 또한 함께 조회된다. 사용자가 특정 카드를 선택하면, 전자 ID 지갑은 카드에 포함된 id 와 SS 를 비롯한 가입 정보를 이용하여 해당 i-PIN 제공자와 상호인증 절차를 수행한다. 상호인증 절차가 성공적으로 이루어지면, 인증 세션이 맺어지고 그림 1 또는 그림 2 의 절차를 거쳐 i-PIN 메시지를 주고받는다. 전자 ID 지갑을 통해, 사용자는 자신이 가입한 i-PIN 사이트를 기억해서 선택하는 단계와 해당 사이트에 등록한 id, pw 를 입력하는 단계를 생략하게 된다.

4. 결론

본 논문은 신원 선택기를 추가하여 i-PIN 의 프로토콜을 변경하지 않는 범위 이내에서 i-PIN 의 단점으로

지적되는 i-PIN 로그인 번거로움, i-PIN 사이트 기억 문제, 피싱 및 파밍 등의 보안 문제를 해결하는 방안을 제시하였다. 제안하는 방법은 사용자가 가입한 i-PIN 서비스 공급자에 접근하는 단계, i-PIN 서비스 공급자에 접근하여 id 와 비밀번호를 입력하는 단계를 없애고, 신원 선택기를 통해 사용할 신원 정보를 하나 선택하는 것만으로 내부에서 모두 처리되도록 하였다. 또한 제안하는 방법은 사이트에 최소한의 수정만을 요구하여 i-PIN 서비스 제공자에게만 변경을 가하는 것만으로 동작할 수 있도록 구성하였다. 본 내용은 ETRI 에서 개발중인 전자 ID 지갑 솔루션을 통해 구현되었으며, 해당 서비스는 2009 년 중에 민간 i-PIN 제공자를 통해 시범 도입될 예정이다.

5. Acknowledgement

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

참고문헌

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

[2] 인터넷상 개인정보 침해방지 대책, 방송통신위원회, 2008/4/24

[3] 공공기관 홈페이지 개인정보 노출 방지 대책, 행정안전부, 2008/8/26

[4] Microsoft, Introducing Windows CardSpace, http://msdn.microsoft.com/

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

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