전자 ID 지갑에서 데이터 전송

노종혁, 진승헌
ETRI 정보보호연구본부
e-mail : jhroh@etri.re.kr

Data Sharing in the Digital Identity Wallet

Jong-Hyuk Roh and Seung-hun Jin
ETRI, Information Security Research Institute

요 약

사용자 중심의 Identity 관리 기술은 기존에 사이트에서 관리하던 사용자 Identity 를 사용자가 직접 제어할 수 있도록 해주는 기술이다. 본 논문에서는 사용자 중심의 Identity 관리 기술 중 하나인 전자 ID 지갑을 소개하고 전자 ID 지갑의 주요 서비스인 Identity 공유 및 동기화 기술을 설명한다. 그리고 Identity 공유 시 필요한 링크 계약을 설명한다.

1. 서론

인터넷은 우리 삶의 큰 부분을 차지하고 있다. 오프라인에서 해오던 만남, 쇼핑, 학습, 오락 등의 행위를 인터넷 상에서 경험하는 것이 전혀 어색하지 않을 정도이다. 그러나, 이와 더불어 프라이버시에 대한 불안감이 증가되고 있다. 인터넷 상에서 주민등록 번호 도용은 당연한 일인 듯 우리 주변에서 자주 발생하고 있으며, 사용자의 정보를 캐내기 위한 피싱 공격 또한 어렵지 않게 맞닥뜨리고 있다. 이러한 문제점들을 해결하기 위해 많은 연구가 이루어지고 관련 기술이 소개되고 있다. 우리가 자주 사용하는 웹브라우저에는 개인정보를 보호하기 위한 P3P 기능[3], 피싱 사이트를 방지하기 위한 피싱 필터 기능 등이 탑재되어 있다. 그리고, 국내에서는 사용자의 주민등록번호를 노출하지 않기 위해 i-Pin 기술을 도입하여 여러 웹사이트에 보급하고 있다[1,2,10].

수년 전부터 사용자의 여러 정보, 즉 Identity 를 종합적으로 안전하게 관리하기 위한 기술인 Identity 관리 기술이 많은 연구소 및 기업들에서 지속적으로 연구 개발되고 있다. Identity 관리 기술에는 Identity 를 관리하는 기술, 공유하는 기술, Identity 를 보호하는 기술 등이 주된 서비스이다. 지금까지 등장한 Identity 관리 기술은 주로 서버 기반의 기술로써, 사용자 정보를 Identity 서버에서 대신 관리하는 방식이다. 그러나 최근에는 사용자 중심의 Identity 관리 기술이 대두되고 있다. 사용자 중심의 Identity 관리 기술은 사용자가 직접 자신의 정보를 관리하고 흐름을 제어할 수 있게 해주므로, 사용자 정보의 오남용 문제를 줄일 수 있고 자신의 정보를 최신 상태로 유지할 수 있도록 도와 준다[2].

본 논문에서는 사용자 중심의 Identity 관리 기술 중 하나인 전자 ID 지갑 기술을 소개한다. 그리고 전자 ID 지갑을 이용한 Identity 공유 및 동기화 기술을 설명하고, 공유 시 발생할 수 있는 프라이버시 문제를 제시하고 이를 해결할 수 있는 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 관련 연구로서 프라이버시, Identity 관리 기술, 전자 ID 지갑 기술을 살펴보고, 3 장에서는 전자 ID 지갑 기술에서 사용되는 Identity 공유 기술을 설명한다. 4 장에서는 Identity 공유 기술의 프라이버시 문제를 해결하기 위한 링크 계약 프라이버시 정책과 사용자 프라이버시 정책을 기술한 후, 5 장에서 결론을 맺는다.

2. 관련 연구

본 장에서는 Identity 관리 기술에 대해서 설명한다. 그리고 본 논문의 아이디어가 적용되는 시스템인 전자 ID 지갑을 살펴본다.

2.1 Identity 관리 기술

Identity 관리 기술은 일반적으로 인터넷 사용자의 Identity 관리 및 개인정보 침해 문제 해결을 목적으로 한다. 주로 아래와 같은 서비스를 제공한다.

- Identity 관리 서비스

사용자의 Identity 를 관리하는 서비스이다. 사용자의 Identity 를 신뢰 기관에 위탁하여 관리하거나, Identity 관리를 사용자 중심으로 처리하는 방법이 있다. 관리 대상으로는 Identifier, 크리덴셜, 사용자의 신원 정보 등 인터넷 또는 실생활에 관계된 사용자의 모든 정보가 포함된다.

- Identity 공유 서비스

사용자가 특정 서비스를 제공 받기 위하여 또는 특수한 자신만의 목적으로 Identity 를 다른 개체와 공유를 하고자 할 때, 안전하고 간편하게 공유할 수 있도

록 지원해주는 서비스이다.

- SSO(Single Sign-On) 서비스

한번의 인증 후, 추가적인 인증 절차 없이 여러 서비스 제공자를 자유롭게 이용할 수 있게 해주는 서비스이다. SSO 서비스는 Identity 관리 기술 이전에 독립적인 형태로 존재하던 서비스였으나, Identity 관리 기술이 등장하며 Identity 관리 기술의 중요한 서비스 중 하나로 인식되고 있다.

- 개인정보 보호 서비스

사용자의 Identity 를 자신이 아닌 타 개체가 사용고자 할 때, 사용자의 명시적인 동의를 요구하거나, 사용자 또는 개체간에 약속한 규칙 및 정책 등에 의하여 Identity 접근 또는 사용을 제어하는 서비스이다. 사용자 개인정보의 오남용을 방지하기 위한 서비스이다.

이외에 Identity 로밍 서비스, 권한 위임 서비스, 프로비저닝 서비스 등이 있다. 인터넷 Identity 관리 기술은 수년 전부터 많은 연구 단체 및 기업들이 연구해 오고 있다. 관련 표준으로는 Liberty Alliance 의 ID-FF(IDentity Federation Framework), ID-WSF(IDentity Web Service Framework), ID-SIS(IDentity Service Interface Specification)[5,6,7], OASIS 그룹의 SAML 및 XACML[8,9] 그리고 마이크로소프트, IBM 의 WS-Security, WS-Federation, WS-Trust, WS-Policy 등이 있다.

2.2 전자 ID 지갑

지금까지 Identity 관리 기술은 서버 기반의 기술로써 기업 내 전사 시스템에 적용되거나, 인터넷 환경에서 일부 사이트들 간에 연계를 통한 기술 형태로 제공되고 있다. 그러나 최근에 사용자가 자신의 정보를 직접 제어할 수 있는 사용자 중심의 Identity 관리 기술에 관심이 집중되고 있다[10,11].

사용자 중심 Identity 관리 기술은 사용자가 인터넷을 사용함에 있어 가입, 인증, 정보 공유 등의 서비스에 대해 서비스 제공자가 제공하는 환경을 이용하지 않고 사용자가 보유하고 있는 시스템을 이용하는 방법이다. 이 방법은 사용자에게 일관적인 인터페이스를 제공하여 편리함을 극대화할 수 있고 사용자가 서비스 제공에 주도적으로 관여할 수 있는 기회를 제공한다. 그림 1 은 사용자 중심의 Identity 관리 기술의 기반 환경을 도식화한 것이다.

한국전자통신연구원에서는 사용자 중심 Identity 관리 기술을 실현하기 위해 전자 ID 지갑 시스템을 개발하였다. 이 시스템은 사용자가 Identity 를 관리하는 형태를 실생활의 지갑에 비유하고 있다. 사용자가 가입한 사이트 목록, 사용자의 크리덴셜 정보, 개인 프로파일 정보 등을 카드 형태의 메타포를 차용하여, 사용자가 보다 직관적으로 Identity 를 관리할 수 있게 한다. 아래 표는 전자 ID 지갑 시스템의 기능을 보여준다 [11].

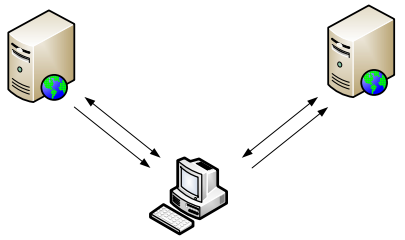

그림 1. 사용자 중심의 Identity 관리

표 1. 전자 ID 지갑 시스템 기술

기술	설명
사이트 가입 기술	전자ID지갑을 이용하여 일관된 방식으로 웹사이트에 가입하는 기술
사이트 관리 기술	전자ID지갑을 이용하여 가입한 웹사이트 목록 및 제공한 ID, 패스워드, 프로파일 정보 등을 관리하는 기술
범용 인증 기술	웹사이트가 제공하는 여러 인증 방식을 지원하기 위한 전자ID지갑의 인증 기술
통합 크리덴셜 관리 기술	사이트 인증 시 제출되는 패스워드, PKI, 바이오 정보 등을 관리하는 기술
Identity 공유 기술	사용자의 Identity 공유를 사용자가 직접 제어하는 기술
Link Contract 관리 기술	Identity 공유에 관련된 계약 정보를 관리하는 기술
Identity 동기화 기술	사용자의 Identity가 변경되었을 때 이를 최신 상태로 갱신하는 기술

3. 전자 ID 지갑의 Identity 공유

서버 기반의 Identity 공유 기술에서는 Identity 공유를 원하는 서버와 Identity 를 관리하는 서버 간에 계약을 체결하고 서로 합의에 의해 공유 항목을 결정하고 특정 공유 메커니즘을 지정한 후, 공유가 이루어진다. 그러므로, Identity 공유에서 사용자의 개인정보는 서버 간에 전송된다. 사용자가 자신의 정보를 제어하기 위해서는 프리퍼런스(preference) 또는 프라이버시 정책(policy)을 사용하여야 한다. 그러나, 이러한 프리퍼런스, 프라이버시 정책은 Identity 공유 도메인마다 고유한 특성을 갖고 있으므로, 사용자는 자신의 정보 공유를 제어함에 있어 각각의 도메인의 규칙을 따라야 하는 불편함을 갖는다.

이에 반해 사용자 중심의 Identity 관리 시스템에서는 정보의 흐름이 사용자 시스템을 통해서 이루어진다. 그러므로, 사용자가 자신이 모르는 사이에 정보가 전송되거나 하는 일은 발생하지 않고, 자신이 정해 놓은 프라이버시 규칙에 따라 Identity 공유를 제어할 수 있다.

3.1 Identity 공유 및 Identity 동기화

전자 ID 지갑의 Identity 공유가 이루어지기 위해서는 우선 사용자와 사이트 간에 공유 링크(Link)를 설정하고 링크를 따라 전송되는 데이터에 대한 계약을 체결하여야 한다. 공유 링크는 사용자와 사이트 간에 데이터가 이동하는 통로로써, 두 개체 간에 링크가 한 번 설정되면 링크를 재사용할 수 있게 되며, Identity 정보 변경에 따른 동기화 채널에서도 사용된다. 링크 계약(Link Contract)은 공유할 Identity 항목과 Identity의 이용 범위와 같은 프라이버시 관련 항목, 그리고 공유 채널을 위한 인증 방법 등을 포함한다. 공유 계약이 완료되면 사이트는 사용자에게 Identity 정보를 요청할 수 있다. 이때, 사전에 설정한 링크 계약에 따라 정보가 공유되고 사용자가 직접 공유에 대한 허가 유무를 제어할 수 있다[11].

그림 1 에서 보면 왼쪽 서버는 Identity 공급 주체(IDP. Identity Provider)이고 오른쪽 서버는 Identity 소비 주체(IDC. Identity Consumer)이다. Identity 공유를 나타내는 화살표는 공급 주체에서 사용자, 사용자에서 소비 주체로 되어 있다. 이는 Identity 공유의 특정한 상황을 표현한 화살표이다. 예를 들어 왼쪽 서버가 항공사 사이트이고 오른쪽 서버는 호텔 사이트이다. 사용자는 항공사에서 항공편을 예약하고 예약 정보를 공유하기 위해 공유 링크를 맺고 링크 계약을 설정하였다. 전자 ID 지갑을 이용하면 이러한 과정은 몇 번의 마우스 클릭만으로 처리된다. 그 후, 사용자는 호텔 사이트에서 호텔을 예약하려고 한다. 호텔 사이트에서는 사용자의 항공 일정 정보를 알려 주면, 항공사와 연계가 되어 있어 특정 서비스를 제공해 주는 호텔을 알려주는 기능이 있다. 이때, 사용자는 항공 예약 정보를 직접 입력할 수 있지만, 사용자 중심의 Identity 기술인 전자 ID 지갑을 이용하여 간단히 처리할 수 있다. 즉, 사용자는 전자 ID 지갑에 이미 생성되어 있는 항공사 사이트와 전자 ID 지갑의 링크를 호텔 사이트까지 연결하면 되는 것이다. 사용자는 전자 ID 지갑을 이용하여 사용자와 호텔 사이트 간에 항공 예약 정보에 대한 링크를 설정하고 계약을 맺는다. 그러면, 사용자의 항공 예약 정보는 그 정보를 보관하고 있는 항공사 사이트에서 사용자의 전자 ID 지갑을 거쳐서 호텔 사이트로 전송된다.

그 후, 사용자는 업무상 항공 예약 정보를 변경이 필요하게 되었다. 사용자는 항공사 홈페이지에 방문하여 항공 예약 정보를 수정하였다. 이때, 전자 ID 지갑은 변경된 예약 정보를 호텔 사이트에 자동으로 전송한다. 호텔 사이트는 수신된 예약 정보를 이용하여 예약된 호텔을 취소하고 일정에 맞는 다른 호텔 정보를 수집하여 전자우편 또는 휴대폰 SMS(Short Message Service) 등을 이용하여 그 정보를 사용자에게 알린다. 이러한 서비스를 Identity 동기화라고 하며 한 사이트에서 이루어지는 간단한 작업이 연관된 다른 사이트들의 부가적인 서비스들을 제공 받을 수 있게 해준다. Identity 공유 시 맺어 놓은 공유 링크 및 공유 계약 등이 이러한 서비스가 가능하도록 해준다.

3.2 링크 계약

링크 계약은 IDP, IDC 와 사용자 간에 Identity 공유를 위해 준수해야 하는 규칙 및 방법 또는 공유 대상에 대한 약속 등을 표기한 데이터이다. 공유 개체인 IDP, IDC, 사용자는 계약 항목을 준수해야 할 의무가 있다. IDP, IDC 사이트는 사용자 약관에 링크 계약 항목 준수를 명시하여야 한다. 링크 계약에는 포함되는 정보는 아래와 같다.

표 2. 링크 계약 정보

항목	설명
계약 번호	링크 계약을 관리하기 위한 계약 번호
개체 식별 정보	Identity 공유 개체들에 대한 식별 정보
공유 데이터 항목	Identity 공유 대상이 되는 데이터
유효 기간	링크 계약의 유효 기간
동기화 지원 여부	Identity 동기화 대상인지를 표현
인증 방법	Identity 공유 시 공유 개체를 인증하기 위한 메커니즘
프라이버시 정책	공유되는 정보에 대한 프라이버시 정책
전자 서명	공유 개체들의 링크 계약에 대한 서명 정보

3.2 링크 계약 프라이버시 정책

링크 계약에는 프라이버시 정책을 포함할 수 있는 공간이 있다. 이곳에 포함되는 프라이버시 정책은 Identity 공유 개체인 웹사이트와 사용자 간에 지켜야 할 사항이다. 프라이버시 정책의 내용은 공유되는 정보의 사용 목적, 정보 사용자, 정보 보유 기간 등이다.

3.1 절에서 설명하였듯이, 전자 ID 지갑에서는 IDP 와 사용자 간에 공유하는 정보가 사용자와 IDC 간에 공유되는 경우가 있다. 이때, 공유되는 정보에 대하여 두 개의 링크 계약이 생성된다. 하나는 IDP 와 사용자 간에 생성되는 계약이고 다른 하나는 IDC 와 사용자 간에 생성되는 계약이다.

4. 결론

사용자 프라이버시 문제는 인터넷 환경뿐만 아니라 앞으로 다가올 유비쿼터스 환경에서도 지속적으로 해결해야 할 이슈이다. 사용자의 정보가 필요한 곳에서는 언제나 프라이버시 문제가 발생하고 그 환경이 너무나 다양하여 몇 개의 시스템만으로는 해결하기 어렵다. 본 논문은 사용자 중심 Identity 관리 시스템인 전자 ID 지갑을 소개하였다. 전자 ID 지갑의 기술 중 하나인 Identity 공유 및 동기화 기술을 소개하고, 링크 계약, 프라이버시 정책 등을 설명하였다. Identity 정보를 사용자의 직접적인 제어와 프라이버시 정책을 이용하여 보다 안전하게 데이터를 전송할 수 있다.

참고 문헌

[1] Pete Bramhall, Marit Hansen, Kai Rannenberg, and Thomas Roessler, “User-Centric Identity Management: New Trends in Standardization and Regulation,” IEEE Security & Privacy, Vol. 5, Issue 4, 2007.
[2] Rafiy Saleh, Dawn Jutla, and Peter Bodorik, “Management of Users' Privacy Preferences in Context Information Reuse and Integration,” IEEE Information Reuse and Integration, 2007
[3] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C 2002.
[4] Liberty Alliance Project, Privacy and Security Best Practices, Nov. 2003.
[5] Liberty Alliance Project, Liberty ID-FF Architecture Overview, Nov. 2003.
[6] Liberty Alliance Project, Liberty ID-WSF Web Services Framework Overview, 2003.
[7] Liberty Alliance Project, Liberty ID-SIS Personal Profile Service Specification, 2003.
[8] OASIS, Assertion and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, 2005.
[9] OASIS, eXtensible Access Control Markup Language (XACML) Version 2.0, Committee draft 04, 2004.
[10] 노종혁, 진승헌, “인터넷 Identity 관리 시스템 환경에서 XACML 을 이용한 프라이버시 컨트롤러,” 한국통신학회논문지, 제 32 권 제 7 호, 2007.
[11] ETRI 디지털 ID 보안연구팀, Digital Identity Management 2007 년 기술 백서, 2007