사용자 중심 ID 관리 기능을 제공하는 전자 ID 지갑 시스템

Electronic Identity Wallet System to Provide User-Centric ID Management Facilities

21세기를 대비하는 정보보호 특집

조영섭 (Y.S. Cho) 디지털ID보안연구팀 선임연구원
진승헌 (S.H. Jin) 디지털ID보안연구팀 팀장

목 차

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

본 고에서는 사용자의 자기 정보 통제권을 강화시키는 전자 ID 지갑 시스템을 기술한다. 전자 ID 지갑 시스템은 ID 정보 제공자로부터 ID 정보 소비자로 유통되는 사용자의 정보를 사용자가 직접 제어할 수 있는 기능을 제공한다. 또한 전자 ID 지갑 시스템은 사용자가 가입한 사이트, 사용자의 크리덴셜 및 사용자의 데이터 공유 정보 등을 사용자에게 모두 카드-기반의 인터페이스로 제공하여 사용자에게 편리함과 일관성을 제공한다. 전자 ID 지갑 시스템은 현재의 웹 환경뿐만 아니라 사용자의 참여와 공유가 더욱 더 중요해지는 웹 2.0 환경에 적합한 사용자 중심 ID 관리 시스템이다.

Ⅰ. 서론

인터넷의 확산에 따라 온라인 뱅킹, 온라인 경매, 메신저 등과 같이 이전에는 상상할 수 없었던 사이버스페이스상의 서비스가 활성화되고 있다. 더욱이 최근 참여와 공유라는 비전을 가진 웹 2.0의 등장은 사용자를 이전의 수동적인 정보 소비자에서 능동적인 정보 제공자로 변모시키고 있다.

이와 같이 변화된 환경에서 서비스를 받기 위해 사용자들은 개인 신원정보인 ID(Identity)를 등록해야 한다. 그러나 이와 같이 등록된 ID 정보는 관리부재, 오남용 등으로 많은 문제가 발생하고 있다. 2005년 전 세계적으로 7억 1,400만 달러에 이르는 개인정보 도용 피해가 발생하고 있을 정도로 개인정보 보호는 사이버스페이스의 지속적인 발전을 위해 필수적으로 해결해야 될 요소가 되고 있다[1].

ID 관리 기술은 사용자의 ID 정보를 생성, 등록, 저장, 갱신, 폐기하는 등의 모든 관리 기능을 제공하는 기술로 개인정보의 보호를 위해 필수적인 기반 기술이다. ID 관리 기술은 초기에 사이트 독자적인 관리 기능을 제공하는 사일로(silo) 모델에서, Passport와 같이 중앙집중형 모델, 연합된 사이트에서의 ID 관리 기능을 제공하는 연합(federated) ID 모델로 발전해오다가 최근에는 사용자를 중심으로 ID를 관리하는 사용자 중심(user-centric) ID 모델로 발전해오고 있다.

본 고에서는 사용자의 자기 정보 통제 권한을 강화한 전자 ID 지갑 시스템을 기술한다. 전자 ID 지갑 시스템은 현재의 웹 환경뿐만 아니라 사용자의 참여와 정보 공유가 더욱 중요해지는 웹 2.0 환경에 적합하도록 개발되고 있는 사용자 중심 ID 관리 시스템(IdMS)이다. 전자 ID 지갑 시스템은 ID 제공자(IdP)에서 ID 소비자(IdC)로 유통되는 사용자의 Identity 정보 흐름에서 사용자가 직접적인 통제를 수행할 수 있는 기능을 제공한다. 또한 전자 ID 지갑 시스템은 사용자의 Identity 정보와 사용자가 가입한 사이트 정보, 크리덴셜(credential), 정보 제공자와 정보 소비자를 모두 카드 형태로 표현하고 이를 선택하여 정보 공유, 인증 기능 등을 수행할 수 있도록 하여 사용자에게 일관성 있고 편리한 인터페이스를 제공한다.

본 고의 구성은 다음과 같다. Ⅱ장에서 ID 관리 기술에 대하여 기술한다. Ⅲ장에서 Ⅴ장까지는 전자 ID 지갑 시스템에 대하여 기술한다. Ⅲ장에서는 전자 ID 지갑 시스템의 요구사항을 기술하고, Ⅳ장에서는 전자 ID 지갑 시스템의 구조에 대하여 기술한다. Ⅴ장에서는 전자 ID 지갑 시스템을 구현한 전자 ID 지갑 프로토타입과 그것이 제공하는 기능을 기술한다. 마지막으로 Ⅵ장에서 결론을 맺는다.

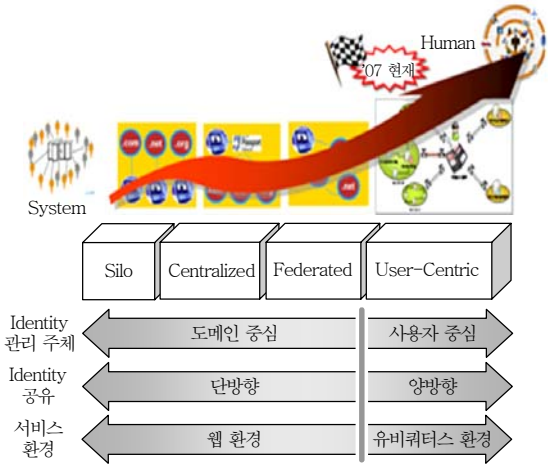
● 용 어 해 설 ●

IdMS: ID 관리 기능으로써 사용자 Identity의 생성, 등록, 변경 및 폐기의 전 과정을 수행하는 ID 관리 시스템이다. IdMS는 또한 사용자의 인증, 인가, 감사 기능을 제공한다.

Ⅱ. ID 관리 기술

1. ID 관리 모델

ID 관리 모델은 네 가지 모델로 분류할 수 있다. 첫번째는 사일로 ID 관리 모델로서 서비스와 ID 관리를 사이트 독자적으로 수행하는 모델이다. 두번째는 중앙집중형 ID 관리 모델로서 Microsoft의 Passport와 같이 특정 사이트에 등록된 ID 정보를 특정 사이트와 연합된 사이트들이 함께 이용하는 모델이다. 세번째는 연합 ID 관리 모델로서 연합된 사이트들 간에 ID 정보를 필요에 따라 공유하는 모델이다. 네번째는 사용자 중심 ID 관리 모델로서, 사용자를 중심으로 연결된 다수의 사이트들에 ID 정보가 제공되며 이러한 정보 제공은 사용자의 통제 하에 이루어지는 특징을 갖는 모델이다. 사용자 중심의 ID 모델은 ID 관리 주체가 사용자라는 특징 이외에도 공유되는 정보가 양방향 흐름을 가지며 공통 식별체계에 의해 관리되는 특징 등을 제공한다.



(그림 1) ID 관리 모델 분류

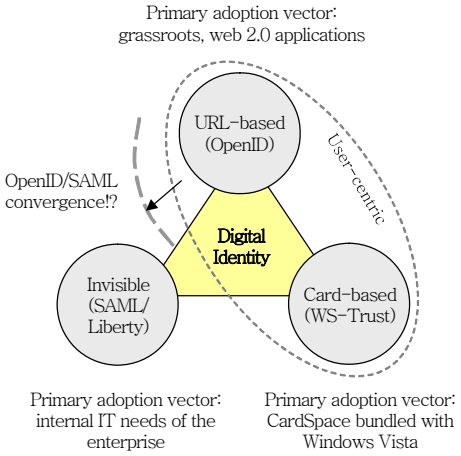
(그림 1)은 ID 관리 주체, ID 공유 흐름, 서비스 환경에 따라 변화해오고 있는 ID 관리 모델을 설명한다.

2. Identity Landscape

NetMesh의 CEO이자 YADIS 프로젝트를 운영하고 있는 Johannes Ernest는 2006년 IdM 시스템들을 세 가지 유형으로 분류하였다[2].

첫번째 Invisible 시스템은 사용자 ID 정보의 흐름이 사용자에게 인지되지 않는다는 특징을 가지고 있으며, 기업이 개인에게 ID를 부여하고 관리하며 개인은 어떤 ID를 공유할 것인가를 결정한다. Liberty Alliance[3] 표준에 기반한 IdM 시스템이 대표적이며, 2007년 현재 Liberty Alliance 표준에 기반한 ID와 장치들이 정부, 교육, 의료 등의 다양한 분야에 10억 개가 넘게 적용되고 있다.

Card-based 시스템은 ID 정보, 사용자 인증에 대한 정보를 사용자에게 카드 형태로 제공함으로써 사용자에게 편리하고 일관성 있는 인터페이스를 제공한다. 대표적인 것으로는 WS-* 표준을 기반으로 Kim Cameron이 Law of Identity를 통해 주장한 ID 메타시스템을 구현한 MS의 CardSpace[4]가 있다. CardSpace는 OASIS 표준인 WS-Security를 기반으로 X.509, Kerberos, SAML과 같은 보안



<자료>: http://netmesh.info/jernst/

(그림 2) The Identity Landscape 2006 Updated

토큰 포맷을 모두 사용할 수 있으며, Windows Vista를 통해 광범위하게 적용될 것으로 예상된다. CardSpace는 MS의 Vista 운영체제와 함께 제공되며 최근에는 Bandit 프로젝트[5]에서 비 MS 환경에서 카드 형태의 인터페이스를 제공하려는 연구가 진행되고 있다.

URL-based 시스템은 사용자에 대한 식별자를 URL로 표현하여 기존 시스템보다 사용자에게 친숙함을 제공하는 ID 시스템으로 OpenID[6]가 대표적이다. URL-based 시스템은 사용자와 사이트간에 신뢰 관리가 중요한 요인으로 작동하지 않는 영역인 블로그 등과 같은 웹 2.0 응용 영역에서 활용된다.

(그림 2)에서 보이듯이 이들 세 영역의 ID 시스템은 독자적인 기능을 제공할 뿐만 아니라 서로 융합되어 발전하고 있는 상황이다. URL-based와 Invisible의 경우, OpenID와 SAML이 통합되고 있다. 또한 Card-based 시스템인 CardSpace와 URL-based인 OpenID 시스템의 경우 CardSpace에서 OpenID를 지원하는 움직임이 일고 있는 상황이다.

3. ID 관리 요소 기술

본 절에서는 사용자 중심 ID 관리 분야의 요소 기술에 대한 동향을 고찰한다.

• 식별체계

식별체계는 사용자나 시스템을 식별하는 식별자 시스템을 나타낸다.

OpenID는 URL을 기반으로 하는 식별체계로 생성과 관리가 매우 간단하다. 2007년 7월, 약 4,500여 개의 사이트에서 사용되고 있으며 발급된 ID의 개수는 1억 2천여 개에 달한다. 현재 2.0 버전의 인증 스펙은 12번째 초안(draft) 버전이 공개되어 있다. 주로 블로그, 댓글 달기 등에서의 사용자 식별자로 활용된다.

XRI[7]는 OASIS에서 XRI TC에서 정의하고 있는 추상 식별자이다. XRI는 지칭하는 엔티티의 물리적인 위치, 응용, 전송 방식과 무관하게 추상적으로 엔티티를 식별할 수 있다. XRI는 현재의 웹 환경뿐만 아니라 차세대 환경에서 활용될 수 있을 것으로 기대되고 있다.

• 보안토큰 생성 분배

보안 토큰은 사용자에 대한 인증 정보, 사용자 속성 정보, 신뢰 관계, 시스템 정책 등과 같은 다양한 보안 정보를 토큰으로 생성하고 전달하는 기술이다.

SAML[8]은 OASIS에서 정의하는 것으로 보안 토큰의 구조, 전송, 프로파일 등을 포함하고 있다. 현재 대부분의 IdM 시스템은 기본적으로 SAML을 지원하고 있다.

WS-*[9]는 웹 서비스 환경에서 보안을 지원하기 위해 Microsoft와 IBM에서 정의한 규격으로 Security, Reliable Messaging, Transaction, Messaging, XML, Metadata에 대한 규격이 정의되어 있다.

• 정보공유

ID 정보의 공유는 일반적으로 IdP에서 ID 정보를 토큰형식으로 생성하여 IdC에게 제공함으로써 이루어진다.

XDI[10]는 인터넷 상의 데이터 공유, 연결, 동기화를 제공하는 범용성 있는 확장 서비스를 정의하는 것을 목표로 하며 OASIS에서 정의하는 규격이다. 공유되는 데이터의 식별자로 OASIS XRI TC에서 정의한 XRI를 사용한다. XDI는 매우 간단하고 일반적인 방식으로 구성되어 있으며, HTTP나 SMTP 같은 기본 프로토콜을 사용한다.

Higgins[11]는 이종 시스템 간의 ID 정보를 통합 사용할 수 있는 API를 공개 소스로 제공하려는 프로젝트로, IBM과 Novell의 주도 하에 Eclipse 프로젝트로 관리되고 있다.

OpenID는 속성 교환 스펙을 작성하고 있다. 속성 교환은 종단(endpoint) 간에 ID 정보를 교환하기 위한 OpenID의 확장 서비스로, ID 정보의 인출(fetch)과 저장(storage) 메시지를 제공한다.

Liberty Alliance의 People 서비스는 기업과 서비스 제공자 간에 사용자의 사회적 네트워크(social network) 정보를 일관성 있게 사용할 수 있는 기술로 다양한 종류의 사회적 응용에 활용할 수 있다. 사용자는 공개된 연계 환경에 분산되어 있는 친구, 동료, 가족과 같은 자신의 온라인 사회적 관계를 한 장소에서 관리할 수 있다.

• 상호운용

현재 다양한 IdM 시스템의 연구 개발이 이루어지고 있고, 이들 간의 이질성은 사용자의 불편을 가중시키고 있으며 시스템 확장의 걸림돌이 되고 있다. 이에 따라, IdM 시스템간의 상호운용성(interoperability)을 해결하려는 연구가 진행되고 있다.

OSIS[12]는 InfoCard를 이용한 상호운용 문서를 공개하고 2007년 5월 14일부터 16일까지 열린 IIW에서 information card selector의 호환성에 대한 작업을 수행하였다.

Concordia[13]는 Liberty Alliance의 융합 분야를 담당하는 프로젝트 명으로, 다양한 ID 관련 표준들과 어떻게 효과적으로 상호운용 할 수 있을지에 대한 연구를 수행한다.

이외에도 CardSpace, OpenID, SAML 사이의 상호운용에 대한 연구가 진행되고 있다.

Ⅲ. 전자 ID 지갑 시스템 요구사항

전자 ID 지갑 시스템은 안전하고 편리한 개인정보 공유를 위하여 사용자 자기정보 통제 및 인증을 강화하는 것을 목표로 한다. 전자 ID 지갑 시스템에 대한 세부적인 요구사항은 다음과 같다.

• 범용 인증

인터넷 사이트들은 각자 고유한 인증 체계를 가지고 있다. 인증 수단으로 Id(Identifier)와 패스워드를 사용하는 사이트, 사용자에게 공인 인증서를 요구하는 사이트 등이 있다. 따라서 사용자가 접근하려는 사이트들의 인증 방식이 상이하더라도 가능하면 사용자가 최소한의 인증만을 수행하도록 하여 사용자의 편의성을 높이는 범용 인증 기술이 필요하다.

• 통합 크리덴셜 관리

사용자 인증에 필요한 Id와 패스워드, 공인 인증서, 생체 정보 등의 인증 크리덴셜과 사용자가 가입한 사이트들의 목록, ID 데이터 정보 등을 사용자가 쉽게 인지할 수 있고, 안전하게 관리할 수 있는 서비스가 필요하다.

• 전자 ID 지갑을 이용한 사이트 가입

사용자가 인터넷 서비스를 제공받기 위해서는 일반적으로 사이트에 회원 가입을 해야 한다. 이와 같은 경우, 사이트들이 요구하는 ID 정보를 제공하고 관리할 때 사용자에게 편리하고 일관된 인터페이스를 통해 사이트 가입을 지원하는 서비스가 필요하다. 이 서비스를 통해 사용자는 사이트 가입에 필요한 ID를 안전하게 제공할 수 있다.

• ID 공유

사용자가 서비스를 제공받기 위해 사이트가 필요로 하는 ID 정보를 제공하는 기능이 필요하다. 또한 한 사이트에서 사용자 ID 정보가 변경된 경우, 변경된 내용이 동일한 ID 정보를 가지고 있는 다른 사이트에도 갱신될 수 있도록 하는 기능이 필요하다. ID 정보가 사이트에 전달될 때, 사용자의 직접적인 통제가 가능한 메커니즘의 지원이 필요하다.

• Link Contract 생성

전자 ID 지갑 시스템에서 ID 공유시 사용자가 IdP 또는 IdC와 공유 계약(LC)을 맺을 수 있도록 한다. LC는 ID 정보 공유시 공유 당사자들 간에 인증, 인가, 프라이버시 보호 정책 등을 협의하여 기술하고, 당사자들이 전자서명을 할 수 있다. LC는 상대방에게 실제 공유되는 ID 정보를 전달하기 전에 상대방이 LC에 기술된 방식으로 인증하였는지, 데이터 사용 목적이 적절한지 등을 평가하고 난 후, ID 정보를 제공하기 때문에 정당한 사이트에 서비스에 꼭 필요한 정보만을 제공할 수 있다. 이를 통해 사용자 프라이버시 보호를 강화할 수 있다.

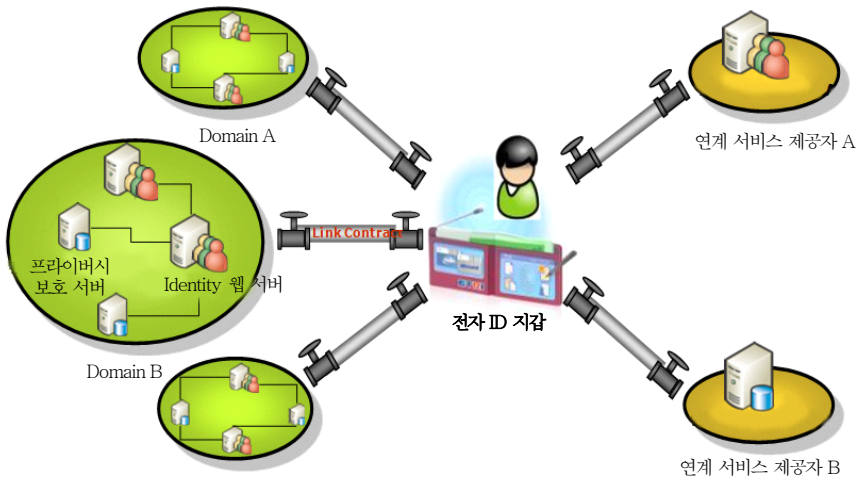
Ⅳ. 전자 ID 지갑 시스템

전자 ID 지갑 시스템은 사용자를 중심으로 사용자의 ID 정보가 ID 제공자에서 ID 소비자로 유통될 수 있도록 해주는 사용자 중심 IdM이다.

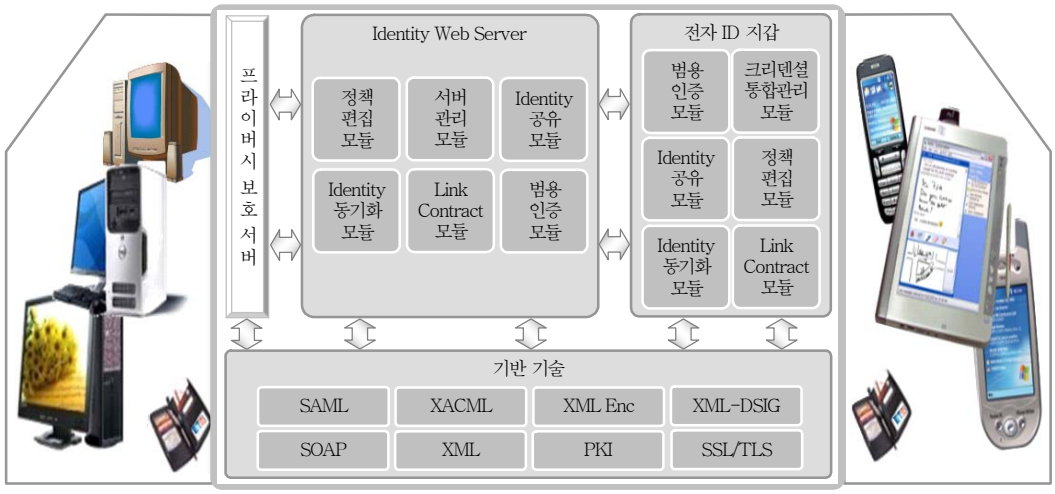
(그림 3)은 전자 ID 지갑의 개념도이다.

그림에서 보이듯이 전자 ID 지갑은 사용자의 ID 정보 흐름, 즉 ID 공유의 중간에 위치한다. 전자 ID 지갑을 통해 사용자는 자신의 ID 정보 흐름을 LC을 통해 통제할 수 있다. 따라서, 어떠한 연계 서비스가 사용자 정보를 필요로 할 때, 전자 ID 지갑은 적절한 IdP를 선택하고, IdP와 사용자가 맺은 link contract 그리고 사용자와 IdC의 역할을 하는 해당 연계 서비스가 맺은 link contract을 통해 ID 공유가 적절한지 판단할 수 있다. 전자 ID 지갑은 이와 같은 판단을 사용자가 쉽게 할 수 있도록 함으로써 사용자의 자기 정보에 대한 통제권을 강화해 준다. 일반적인 사용자 데이터와 달리 사용자의 이름, 주소, 이메일 등과 같은 사용자 프로파일에 해당하는 데이터의 경우에는 전자 ID 지갑에서 사용자가 데이터를 생성하여 다른 사이트에 제공할 수 있다. 즉, 이 경우에는 전자 ID 지갑이 IdP의 역할을 수행하게 된다.

(그림 4)는 전자 ID 지갑의 구성도이다.



(그림 3) 전자 ID 지갑의 개념도



(그림 4) 전자 ID 지갑의 구성도

전자 ID 지갑 시스템은 사용자 클라이언트 단에서 ID 관리 기능을 제공하는 전자 ID 지갑과 IdP와 IdC의 역할을 수행하는 사이트 단에서 ID 관리 기능을 제공하는 ID 웹 서버로 구성된다.

전자 ID 지갑은 다양한 사이트에 사용자가 쉽게 인증을 할 수 있도록 하는 범용 인증 모듈, 사용자의 패스워드, 지문, PKC 등과 같은 인증 크리덴셜과 사용자의 ID 정보를 관리하는 데이터 크리덴셜을 통합적으로 관리해주는 통합 크리덴셜 관리 모듈로 구성된다. 또한 다른 사이트와 사용자 ID 정보를 공유하는 데 사용되는 Identity 공유 모듈, ID 정보의 변경 시 이를 다른 사이트에 반영할 수 있도록 해주는 Identity 동기화 모듈을 포함한다. 또한 전자 ID 지갑에 대한 사용자 관리 정책 등을 제공하는 정책 편집 모듈, ID 공유시 사용자와 사이트간에 맺는 계약인 link contract을 쉽게 편집할 수 있도록 해주는 link contract 모듈로 구성된다.

ID 웹 서버는 전자 ID 지갑과 같이 Identity 공유 모듈, 범용 인증 모듈, link contract 모듈, 정책 편집 모듈을 가지고 있다. 또한 ID 웹 서버를 관리해 주는 서버 관리 모듈을 포함한다.

프라이버시 보호 서버의 경우에는 전자 ID 지갑

을 통해 생성되고 관리되는 사용자 데이터, 사용자 정책, 사용자 크리덴셜 등을 안정적으로 백업 및 관리함으로써 전자 ID 지갑의 분실시 전자 ID 지갑을 복구할 수 있는 기능을 제공한다.

V. 전자 ID 지갑 시스템 프로토타입

본 장에서는 전자 ID 지갑 시스템 기능을 구현한 전자 ID 지갑 시스템 프로토타입에 대하여 기술한다.

전자 ID 지갑 시스템 프로토타입은 ID 제공자의 역할을 수행하는 학교, 동사무소, 영어평가원 사이트를 구축하고 있으며, 이들 정보를 이용하여 사용자에게 취업을 알선하는 Recruit 사이트와 취업사이트인 IDCom 사이트를 구축하였다. 각각의 서버 사이트에는 ID 공유 기능을 위한 Identity 웹 서버 프로토타입이 구축되어 사이트 가입, 범용 인증, ID 공유, ID 동기화 기능을 제공한다. 사용자 단에서는 전자 ID 지갑 프로토타입이 구축되어 사이트 가입, 범용 인증, ID 공유, ID 동기화 기능을 제공한다. 이들 프로토타입들은 모두 SOAP, XML 전자서명, PKI 등을 기반 기술로 활용한다. 사용자 단에서 사용하는 전자 ID 지갑 프로토타입은 일반적인 웹 브라우저인 IE, Firefox와 연동하여 동작하도록 구현되었으며, Identity 웹 서버 프로토타입은 .NET 버전과 Java 버전으로 구현되었다.

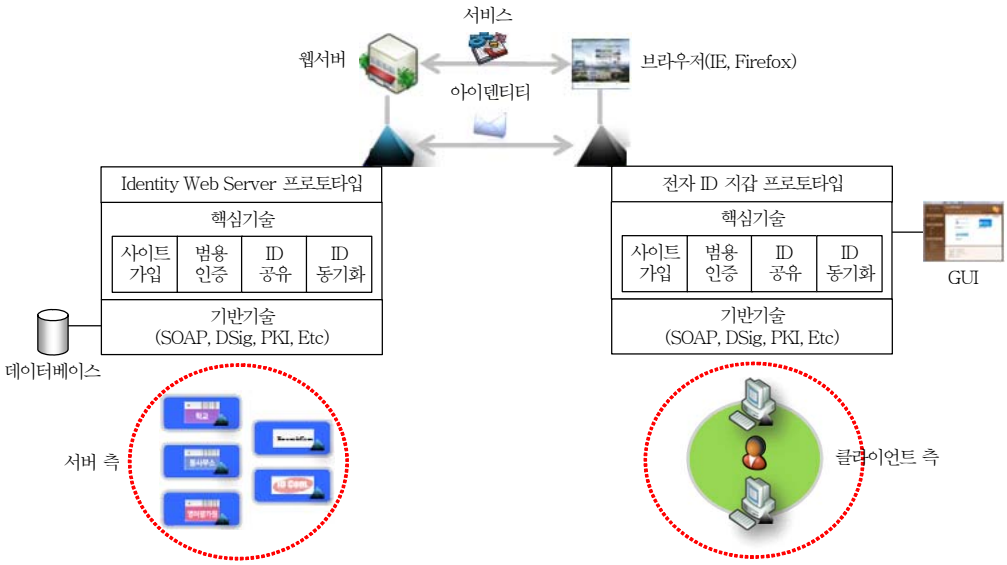
(그림 5)는 전자 ID 지갑 프로토타입의 구성을 보인다.

• 전자 ID 지갑을 이용한 사이트 가입

전자 ID 지갑에서 제공하는 사이트 가입 기능은 사용자가 가입하려는 사이트에 대한 정보를 카드 형태로 제공함으로써 사용자에게 편리한 인터페이스를 제공하며, 가입하려는 사이트에 대한 신뢰성을 검사하는 기능이 있어 사용자를 피싱으로부터 보호하는 기능을 제공한다.

(그림 6)은 전자 ID 지갑을 통해 Recruit 사이트에 가입할 때, 사용자에게 제공되는 사이트 가입 기능을 보인다.

(그림 6)에서 보이듯이 사이트 가입 기능은 사용자가 가입하려는 Recruit 사이트의 인증서를 검증하여 가입하려는 사이트가 안전한 사이트인 경우에는 “안전한 사이트입니다”라는 메시지를 제공하여 가입 사이트가 피싱 사이트가 아님을 사용자에게 확인시켜 준다.



(그림 5) 전자 ID 지갑 프로토타입 구성도

(그림 6) 전자 ID 지갑 사이트 가입

(그림 8) 통합 크리덴셜 관리

• 범용 인증

범용 인증 기능은 사이트마다 상이하게 제공하는 인증 방식을 전자 ID 지갑에서 범용적으로 제공하는 기능이다.

(그림 7)은 사용자가 전자 ID 지갑을 통해 사이트에 인증할 때, 사이트가 지원하는 인증 방식을 전자 ID 지갑에서 해석하여 사용자에게 적절한 인증 방식을 선택할 수 있도록 해주는 범용 인증 기능을 보인다.

(그림 7) 전자 ID 지갑 범용 인증

• 통합 크리덴셜 관리

통합 크리덴셜 관리 기능은 사용자가 인증시 사용하는 패스워드, 지문, PKC 등의 인증 크리덴셜 관리 기능과 사용자의 ID 정보에 대한 정보를 나타내는 데이터 크리덴셜 관리 기능을 제공한다.

(그림 8)은 통합 크리덴셜 관리 기능을 보인다.

(그림 8)에서 전자 ID 지갑은 사용자의 패스워드, 인증서, 지문 크리덴셜을 관리하고 있음을 알 수 있다.

• ID 공유

전자 ID 지갑은 IdP로부터 IdC로 정보의 전달이 필요할 때마다 사용자에게 정보 전달에 대한 동의를 얻도록 한다. 만약 사용자가 정보 전달에 동의하지 않는 경우에는 ID 공유는 실패하게 된다.

(그림 9)는 Recruit 사이트가 사용자의 학력 정보를 요청할 때, 전자 ID 지갑에서 사용자에게 제공하는 ID 공유 확인 기능이다.

(그림 9)에서 Recruit 사이트는 사용자에게 취업 관련 서비스를 제공하기 위해 사용자의 학력 정보를 요청하고 있으며, 이 정보의 이용 범위는 취업정보 조회에 활용될 것임을 보인다. 이 정보는 사용자와 취업사이트 간에 맺은 ID 공유 계약인 link contract

(그림 9) ID 공유 확인

을 사용자가 읽기 쉽게 표현한 정보이다. 실제 link contract은 그림에서 나타내는 XML 문으로 구성되어 있다.

• ID 동기화

전자 ID 지갑은 한 사이트에서 사용자의 ID 정보가 변경될 경우, 사용자에 대해 동일한 ID 정보를 보유하고 있는 모든 사이트의 ID 정보를 동기화하는 기능을 제공한다. ID 동기화 기능은 사이트와 사용자가 ID 공유 계약을 맺을 때, ID 동기화를 허용할 것인지 여부를 포함하도록 하여 ID 동기화를 원하는 사이트만 ID 동기화가 이루어지도록 하는 기능을 제공한다.

Ⅵ. 결론

본 고에서는 사용자의 자기 정보 통제 권한을 강화한 전자 ID 지갑 시스템을 기술하였다. 전자 ID 지갑은 ID 정보 제공자에서 ID 정보 소비자로 유통되는 사용자의 Identity 정보 흐름에서 사용자가 직접적인 통제를 수행할 수 있도록 하여 사용자의 자기 정보 통제 권한을 강화한 사용자 중심 IdM 시스템이다. 또한 전자 ID 지갑은 사용자의 Identity 정보와 사용자가 가입한 사이트 정보, 정보 제공자와 정보 소비자를 모두 카드 형태로 표현하고 이를 선택하여 정보 공유, 인증 등을 수행할 수 있도록 하여 사용자에게 일관성 있고 편리한 인터페이스를 제공한다.

전자 ID 지갑은 현재의 웹 환경뿐만 아니라 사용자의 참여와 정보 공유가 더욱 중요해지는 웹 2.0 환경에 적합한 사용자 중심 ID 관리 기능을 제공함으로써 인터넷 환경의 안전성을 제고시킬 것으로 기대된다.

● 용 어 해 설 ●

User-Centric IdM: 사용자가 중심이 되는 IdM으로, 사용자가 자신의 ID 정보를 직접 생성하여 IdC에게 제공할 수 있으며, IdP와 IdC 사이에 유통되는 자신의 ID 정보 흐름에 직접 개입할 수 있는 기능을 제공한다.

약 어 정 리

Id	Identifier
ID	Identity
IdC	Identity Consumer
IdM	Identity Management
IdMS	Identity Management System
IdP	Identity Provider
IIW	Internet Identity Workshop
LC	Link Contract
OSIS	Open Source Identity System
SAML	Security Assertion Markup Language
URI	Uniform Resource Identifier
XRI	eXtensible Resource Identifier
YADIS	Yet Another Decentralized Identity Interoperability System

참 고 문 헌

[1] IDC, Worldwide Identity Theft Black Market 2006-2010 Forecast, 2006.

[2] Johannes Ernst, Updating The Identity Landscape of 2006, http://netmesh.info/jernst/Digital_Identity/updating-three-standards.html

[3] Liberty Alliance Project, http://www.projectliberty.org/

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

[5] Bandit Project, http://www.banditproject.org/

[6] OpenID, http://openid.net/

[7] OASIS Extensible Resource Identifier(XRI) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xri

[8] Security Assertion Markup Language(SAML) OASIS Standard specification, Version 2.0, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[9] Web Service Security Standards, http://www.ibm.com/developerworks/webservices/standards/#security

[10] OASIS XRI Data Interchange(XDI) TC, http://www.oasis-open.org/committees/xdi

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

[12] OSIS Project, http://osis.netmesh.org/

[13] Concordia Project, http://projectconcordia.org/