디지털 ID 관리 기술 동향 및 전망

조 영 섭* 진 승 헌**

◈ 목 차 ◈

1. 서 론

인터넷의 활용이 커져가면서 사용자는 수 많은 사이트에서 인터넷 서비스를 이용하게 되었다. 이러한 서비스를 제공받기 위해서 사용자는 사이트에서 자신을 식별할 수 있는 식별자(Identifier, id)와 자신의 개인 속성 정보(attribute)을 등록하여야 한다. 그러나 사용자가 식별자와 속성 정보로 이루어진 ID(Identity)를 관리하는 것이 점점 더 불편해졌을 뿐만 아니라 사이트에서 사용자 개인정보 오·남용으로 인한 피해가 증가하고 있는 상황이다[1]. 특히 국내 조사에 의하면 일반 인터넷 이용자들이 느끼는 개인정보에 대한 불안감이 매우 커 이를 비용으로 환산하면, 연간 개인정보보호에 대한 총 가치는 약 1조 2,982억 원에 달하고 있다고 한다[2]. 이와 같은 문제를 해결하기 위해서 최근 사용자의 ID 정보를 안전하게 관리하고 공유하는 ID 관리 기술에 대한 연구 개발이 활발히 진행되고 있다.

ID 관리 기술은 서비스와 ID 관리를 독자적인 사이트에서 수행하는 사일로(silo) ID 관리 모델로부터 진화하여, Microsoft의 .net Passport와 같이 특정 사이트에 등록된 ID 정보를 특정 사이트와 연합된 사이트들이 함께 이용하는 중앙집중형(centralized) ID 관리 모델과 Liberty Alliance와 같이 연합된 사이트들 간에 ID 정보를 필요에 따라 공유하는 연합 ID 관리 모델로 발전하였다. 최근에는 사용자의 참여와 공유가 중요시되는 웹 2.0과 같은 환경에서 사용자의 통제하에 ID 정보가 제공되는 사용자 중심 ID 관리 모델로 발전해오고 있다[3].

본 고에서는 이와 같은 ID 문제를 해결하기 위해 현재 진행되고 있는 디지털 ID 관리 기술의 동향과 전망에 대하여 살펴본다. 2장에서 디지털 ID 관리 기술의 최근 동향에 대하여 기술한다. 3장에서 국내외 ID 관련 표준화 동향에 대하여 기술하고 4장에서 국내외 ID 관리 시장 동향에 대하여 기술한다. 5장에서 최근 연구 개발이 활발히 진행되고 있는 사용자 중심 ID 관리 시스템 중에서 ETRI에서 개발 중인 전자ID 지갑 시스템에 대하여 기술하고 마지막으로 6장에서 결론을 맺는다.

2. 기술 동향

본 장에서는 ID 관리 기술의 Landscape와 국내외 기술 동향을 기술한다.

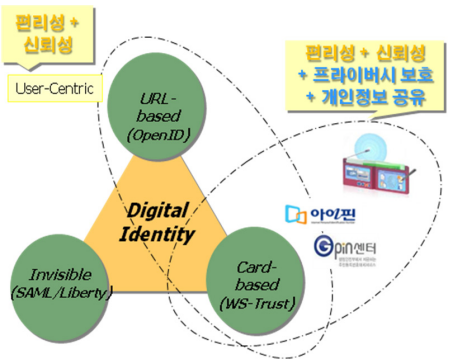
* 한국전자통신연구원 정보보호연구본부
** 한국전자통신연구원 정보보호연구본부, 팀장
본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심 기술개발사업의 일환으로 수행하였음.[2007-S-601-02, 자기통제 강화형 전자ID지갑 시스템 개발]

2.1 Identity Landscape

NetMesh의 CEO이자 YADIS(Yet Another Decentralized Identity Interoperability System) 프로젝트를 운영하고 있는 Johannes Ernest는 2006년 IdM(Identity Management) 시스템들을 세 가지 유형으로 분류하였다[4].

첫 번째 Invisible 시스템 유형은 시스템 간의 ID 정보 흐름이 사용자에게 인지되지 않는다는 특징을 가지고 있다. SAML과 Liberty Alliance 표준에 기반한 IdM 시스템들이 이 유형에 속한다. 두 번째 Card-based 시스템 유형은 인증 및 ID 정보가 요구될 때마다, 요구 조건을 만족시키는 ID 정보 제공자를 카드 형태로 사용자에게 제공하여 사용자가 선택할 수 있도록 한다는 특징을 가진다. WS-* 표준을 기반으로 MS Window 시스템에서 구현된 CardSpace가 대표적이며 최근에는 Bandit 프로젝트에서 비 MS 환경에서 Card 형태의 인터페이스를 제공하려는 연구가 진행되고 있다. 사용자에게 편리하고 일관성 있는 인터페이스를 제공한다는 장점이 있다.

세 번째 URL-based 시스템 유형은 인터넷 사용자에게 가장 일반적이며 친숙한 URL 형태로 사용자 식별자를 제공하여 인증 및 ID 정보 제공을 할 수 있도록 한다는 특징을 가진다. OpenID가 이 유형에 속하는 대표적인 ID 관리 시스템이며, 주로 사용자와 사이트간에 신뢰 관리가 중요한 요인으로 작동하지 않는 블로그 등과 같은 웹 2.0 응용 영역에서 활용된다.



(그림 1) The Identity Landscape

최근에는 기존 세 가지 유형의 IdM이 상호 융합하면서 상호간의 장점을 흡수하며 발전하고 있다. Card-based 시스템인 CardSpace와 URL-based인 OpenID 시스템의 경우 CardSpace에서 OpenID를 지원하는 움직임이 일고 있는 상황이다. 이를 통해 URL의 편리성과 Card-based의 신뢰성을 동시에 제공할 수 있다. 또한 국내의 경우 주민번호 대체 수단인 i-PIN과 개인정보 공유 기능을 융합하여 편리성, 신뢰성, 프라이버시 보호 및 개인정보 공유를 제공하려는 연구가 진행되고 있다[5]. 그림 1은 기존 IdM의 유형과 국내외 연구 동향에 따른 Identity Landscape을 보인다.

2.2 국내 기술 동향

2.2.1 i-PIN

인터넷 상에서 주민번호 대체 수단인 i-PIN(Internet Personal Identification Number)은 공공 i-PIN과 민간 i-PIN으로 구분할 수 있다. 민간 i-PIN은 민간 기관에서 운영되며 현재 5개 기관에서 서비스를 제공하고 있다. 공공 i-PIN은 OASIS의 SAML 2.0 표준에 기반하여 구현되었으며 2008년 7월 현재 행정안전부는 g-PIN 센터(http://g-pin.go.kr)를 구축하여 시범적용 테스트를 진행 중이다.

i-PIN 서비스가 시작된 이후로 각 서비스 제공기관별로 지원하는 개별 기술의 구체적인 내용과 추가 개발 내용은 알려지지 않고 있다. 그러나 각기 다른 기술들의 호환성을 제공하기 위해 KISA는 i-PIN 서비스 프레임워크[6]와 i-PIN 서비스 전달 메시지 형식[7]을 정의하였다.

2.2.2 전자ID지갑

ETRI는 Microsoft, KISA와 공동으로 2007년부터 2009년까지 '자기통제 강화형 전자ID지갑 시스템 기술개발' 과제를 진행하며 사용자 중심 IdM인 전자ID 지갑을 개발하고 있다. 전자ID지갑은 사용자 본인이 개인정보와 인증정보(id/pw, 인증서 등)를 안전하게 관리하고 있다가, 언제 어디서나 자신을 인증하고 개인정보를 자신의 통제 하에 선택하여 이용할 수 있는 시스템이다.

1차년도인 2007년에 개발된 프로토타입은 IETF 표준인 SASL(Simple Authentication Security Layer)을 변형한 범용인증 서비스, Identity 정보 공유 및 Link Contract, Identity 동기화 기능을 제공하는 Identity 공유 서비스, 전자ID지갑을 이용한 사이트 가입 및 인증 기능을 구현하였다.

2차년도인 2008년에는 1차년도의 프로토타입을 상용 수준으로 개발하고 i-PIN, OpenID, CardSpace 등의 관련 표준들과 호환되며, 오픈소스 환경뿐만 아니라 모바일 환경에서도 동작하도록 진행하고 있다.

2.2.3 기타

OAuth는 단순하고 표준화된 방식으로 안전한 API 인증이 가능하도록 하는 공개 인가 프로토콜이다. 현재 국내에서는 NC소프트의 자회사인 오픈마루가 OpenAPI 인증을 총괄하는 API 센터에서 스프링노트(http://www.springnote.com/)와 귓속말(http://blog.openmaru.com/216) 서비스의 OpenAPI를 사용하기 위한 인증 방식으로 OAuth를 지원한다고 발표하였다. 또한 2008년 6월 이후로는 OAuth 인증 방식을 사용하는 OpenAPI 서비스만 신규 지원하고 있다.

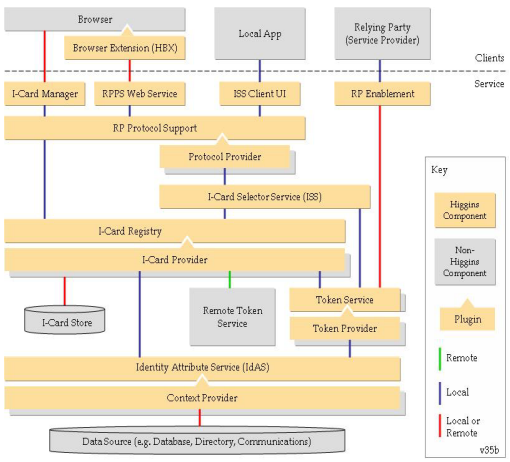
국내의 OpenID 프로바이더는 1.1 버전의 인증 체계를 사용하고 있다. 국내의 특수한 상황을 고려하여, NC소프트의 자회사인 오픈마루에서는 OpenID 프로바이더인 myID를 확장하여 제한적 본인확인제 사이트에 OpenID 로그인을 지원하였다. 사이트의 Id 인증과 회원 계정을 분리하여, OpenID를 로그인 방법으로 하나 더 지원하는 개념을 채택하였다. 따라서 OpenID 프로바이더 자체는 본인확인을 기본적으로 수행할 부담 없이, 본인확인제 사이트에 접근하는 OpenID 사용자에게만 한 번 실명확인을 거치게 된다.

2.3 국외 기술 동향

2.3.1 Higgins

Higgins 프로젝트[8]는 2004년 Eclipse 재단에서 'Eclipse Trust Framework'라는 이름으로 시작되었으며, 2006년부터 IBM, Novell, Google, Microsoft 등이 지원하는 프로젝트이다. Higgins는 다양한 사이트, 어플리케이션, 디바이스에 흩어져 있는 id/프로파일/소셜(social) 관계 정보를 통합 제공하는 인터넷 ID 프레임워크를 지향한다. 특정 프로토콜이 아닌 소프트웨어 아키텍처로서, 기존의 모든 ID 프로토콜을 지원하면서도 일관된 사용자 경험을 제공한다. 이를 통해 사용자가 웹사이트에 가입할 때 정보를 제공하는 작업, 커뮤니티 간에 데이터를 교환하는 작업, 소셜 네트워킹 프로그램들과 정보를 공유하는 작업, 자신만의 어플리케이션을 구축하는 작업 등을 쉽게 처리할 수 있다.

Higgins 아키텍처의 설계 철학은 모든 컴포넌트를 플러그인(plug-in) 방식으로 제공하는 것이다. 이에 따라 데이터 저장소, 보안 토큰 타입, 보안 프로토콜, 데이터 카드 타입, 토큰 서비스를 플러그인 방식으로 자유롭게 추가하고 제거하는 것이 가능하다. 그림 2는 Higgins 아키텍처를 보인다.



(그림 2) Higgins 아키텍처

2.3.2 Information Cards

Information Cards는 Microsoft의 ID Metasystem에 따라 CardSpace와 같은 IS(Identity Selector)의 상호운용성을 제공하기 위한 스펙 및 기술을 총칭한다. 관련 스펙은 2007년 1.0 버전에서 2008년 7월 1.5 버전으로 확장되었다[9]. Information Cards 관련 스펙으로 다음의 문서가 제공된다.

- Identity Selector Interoperability Profile V1.5, July 2008

- A Guide to Using the Identity Selector Interoperability Profile V1.5 within Web Applications and Browsers, July 2008
- An Implementer's Guide to the Identity Selector Interoperability Profile V1.5, July 2008
- Application Note: Web Services Addressing Endpoint References and Identity, July 2008

2.3.3 OpenID

OpenID는 2007년 12월, 인증 스펙 2.0 버전과 속성 교환(Attribute Exchange) 1.0 버전을 완성하였다. 이미 여러 번의 드래프트 작업으로 스펙은 완성되어 있었는데, OpenID 표준에 대한 지적재산권을 보유한 Sxip 사가 Non-Assertion Agreement에 서명하면서 18개월 간의 스펙 작업이 완료되었다.

현재 진행 중인 드래프트 문서로 Data Transport Protocol, Simple Registration Extension 1.1, Provider Authentication Policy Extension이 존재한다. 구체적인 내용은 표 1과 같다.

(표 1) OpenID 드래프트 문서

스펙	내용
Data Transport Protocol (DTP)	· XRD에 사용자의 PKI 공개키 넣는 방법 정의 · 송신자, 수신자의 식별자가 포함된 MIME 메시지를 생성하고 S/MIME으로 서명, 암호화 수행
Simple Registration Extension	· 경량화된 프로파일 전달 프로토콜 정의 · 사이트 가입에 필요한 8 종류의 정보를 전송할 수 있음 · 사이트는 해당 정보의 사용에 대한 정책을 명시함
Provider Authentication Policy Extension (PAPE)	· RP가 OP에게 사용자의 인증과 관련된 정책, 메커니즘을 요구하는 기능 정의 · 정책: 피싱 방지, 다중 인증, 물리적 다중 인증 · 메커니즘: PIN, 인증서, OTP, 보안 토큰 · OP는 응답으로 NIST 800-63을 준용하는 보증 레벨을 RP에게 전달할 수 있음

2.3.4 기타

Bandit 프로젝트[10]는 2006년 6월에 시작된 이후, ID 인프라를 구성할 수 있는 공개 시스템을 구성하기 위해 상호운용성과 통합 관점에서 관련 기술을 개발하고 공개적으로 표준화하였다. 따라서 Bandit 을 적용한 제품은 ID저장소의 위치에 무관하며, 다양한 인증 방법을 지원하고 쉽게 기존 시스템에 적용할 수 있다.

OAuth 토론그룹은 2007년 4월에 구성되었으며, OAuth의 드래프트 문서 작성과 실제 구현을 담당하였다. 2007년 7월에 초기 스펙이 완성되었으며, 2007년 10월에 OAuth Core 1.0 최종 드래프트 문서가 완성되었다. 스펙은 업데이트 되지 않았으나, 2008년 6월 26일에 개최된 OAuth Summit 2008에서는 OAuth 프로토콜, 확장성, OAuth 구현 사례를 공유하면서 특히 OAuth Core 1.0 스펙에 추가되는 여러 요구사항이 언급되었다.

3. 표준화 동향

본 장에서는 ID 관리 기술에 대한 국내외 표준화 동향을 기술한다.

3.1 국내 표준화 동향

국내에서 ID 관리 기술에 대한 표준화는 주로 디지털 ID관리 포럼과 TTA TC5(정보보호 기술위원회) PG502(개인정보보호 및 ID관리)에서 추진하고 있다. 디지털 ID관리 포럼에서 표준초안을 개발하고 TTA에서 정보통신 단체표준으로 개발하거나, TTA에서 직접 표준 초안이 개발하여 최종 표준을 확정하는 방법으로 표준안을 개발하고 있다.

TTA에서는 2006년 SAML 2.0 주장과 프로토콜, 바인딩, 프로파일에 대한 국내 표준화를 완료하였으며, 2007년 SAML 2.0 메타데이터와 인증 문맥에 대해 표준을 제정하였다.

2007년에 P3Pv1.1을 기반으로 국내 개인정보 관련 법규를 반영한 개인정보보호 정책 설정 및 협상 규격, 서비스 이용자의 개인정보 수집·저장·이용·파기

등의 생명주기를 고려한 개인정보 생명주기별 관리모델 등의 표준이 제정되었다.

2008년 현재 확장형 자원 식별자(XRI) 문법 V2.0, 공통 아이덴터티 데이터 모델과 상호운용성 및 신뢰를 위한 글로벌 ID 관리 시스템 요구사항, 자기통제 강화형 디지털 아이덴터티 공유 프레임워크, 본인확인 기술인 i-PIN 서비스 전달 메시지 형식과 서비스 중복가입 확인정보, 확장성 접근제어 생성언어 3.0, 프라이버시 강화형 역할기반 접근통제 정책언어 및 개인정보 DB 관리 기술의 보안요구사항 등에 대한 표준화가 진행되고 있다.

3.2 국외 표준화 동향

3.2.1 ITU-T

2006년 12월에 결성된 ITU-T SG17 FG IdM(Focus Group on Identity Management)에서는 포괄적인 IdM 프레임워크 개발을 촉진하고 분산환경에서 자율적인 Identity 발견, Identity 연계 및 구현 수단 개발을 진행하였다.

ITU-T SG17 내에서 ID 관리의 표준 개발을 직접적으로 담당하고 있는 곳은 Q6/17이다. FG IdM의 결과물 중 IdM 상호운용성 요구사항은 'X.1250: Requirements for global identity management trust and interoperability'라는 제목으로 표준화를 진행하고 있으며 IdM 시스템들간의 아이덴터티 정보의 표현을 위한 아이덴터티 데이터의 공통 데이터 모델을 개발하는 표준으로 'X.idm-dm: Common Identity Data Model'의 표준화 작업을 진행 중에 있다.

ITU-T SG17은 4년 회기를 마감하는 회의를 2008년 9월 개최하였으며, 이 회의에서 X.1250은 표준승인을 받지 못하고 다시 6개월 동안 검토를 받는 단계에 머물기로 결정(Re-determination)이 되었고 X.idif(X.1251)는 표준승인 절차에 들어가는 것으로 결정(Determination)이 되었다. 이번 회의에서 승인된 IdM 관련 신규 표준과제는 X.idmsg(Security Guidelines for Identity Management Systems), X.priva (Criteria for Assessing the Level of Protection for Personally Identifiable Information in the IdM), 그리고 X.idm-ifa (Framework architecture for interoperable identity management systems)이 있다.

3.2.2 ISO/IEC JTC1

ISO/IEC에서 ID 관리와 연관된 표준화 활동들로는 전자 거래(electronic transaction)에서 활용되는 전자 ID에 대한 명세 ISO/IEC 15944-1, 생체인식정보 교환 표준형식을 개발하는 ISO/IEC 19794 series 등이 있다.

ISO/IEC JTC1 SC27 WG5에서는 ID 개념, ID, 식별 및 식별자, ID 생명주기, ID 인증, 정보사회에서 ID 관리, 정보기술과 ID 관리, 정보보안과 ID 관리 등 포괄적인 ID 관리에 대한 표준 개발을 진행하고 있으며 다음 WD(Working Document)를 작성한 상태이다.

(표 2) ISO/IEC JTC1 SC27 WG5 WD

WD	Title
WD 24760	A Framework for Identity Management
WD 29100	A Privacy Framework
WD 29101	A Privacy reference architecture
WD 29115	Entity authentication assurance

3.2.3 OASIS

OASIS에서 제정한 ID 관련 표준들로는 SAML, XACML, SPML, XRI, WS-Security 등이 있다. SAML[12] 표준에서는 주체(subject)에 대해 발행된 assertion 구조 및 assertion 처리를 위한 관련 프로토콜들에 대해 정의하고 있으며 XACML[13]은 정보시스템에 의해 관리되는 자원에 대한 접근허용 여부를 정의하는 XML 언어 기반 보안정책 기술언어 표준이다. SPML은 사용자, 자원, 서비스 프로비저닝 정보교환을 위한 XML 기반 프레임워크를 정의하고 있으며 XRI[14]는 위치, 응용, 전송 프로토콜과 독립적인 URI와 호환성 있는 추상적 식별자와 해결(resolution) 프로토콜에 대한 표준을 정의하고 있다. WS-Security 표준에서는 웹 서비스 messaging에 적용되는 무결성 및 비밀성 지원을 위한 프로토콜을 정의하고 있다. 또한 XDI[15]는 XRI에 기반을 둔 데이터웹(dataweb) 구축을 목표로 인터넷 규모의 멀티 도메인들 간에 XRI와 XDI 기본 스키마에 기반을 둔 XML 문서를 상호간에

서로 공유하고 연결(linking), 동기화하는 표준화를 제안하고 있다.

3.2.4 기타

IETF에서 개발된 표준 중 ID 관리와 연관된 RFC들로는 자원이나 개체 식별을 위한 RFC 3986(Uniform Resource Identifier), URI를 포함하는 식별자에 대한 표준들인 RFC 3987(Internationalized Resource Identifier), RFC 2822(Internet Message Format), RFC 2141(Uniform Resource Name), RFC 4122(A Universally Unique IDentifier(UUID) URN Namespace), RFC 4474(Enhancements and Authenticated Identity Management in the Session Initiation Protocol), RFC 4484(Trait-Based Authorization Requirements for the Session Initiation Protocol) 등이 있다.

Liberty Alliance 프로젝트는 연합된(federated) ID 관리를 위한 가이드라인과 실례 그리고 공개 표준을 개발할 목적으로 2001년에 결성되었다. Liberty Alliance 프로젝트는 크게 세 개의 모듈로 구성되어 있다. 여러 사이트의 사용자 계정을 연결하는 ID의 연합(federation)을 다루는 ID-FF, ID 서비스의 생성, 검색, 사용을 위한 프레임워크를 제공하는 ID-WSF와 ID-WSF 위에서 일정, 주소록, 달력, 위치추적, 사용자 상태나 경고 등을 위한 ID 기반의 서비스를 다루는 ID-SIS로 구성되어 있다.

Liberty Alliance project는 기본적인 프레임워크인 ID-FF나 ID-WSF외에도 Identity 서비스를 평가하고 검증할 수 있는 Identity Assurance Framework를 개발하였고 엔티티들간의 Identity 정보의 원활한 교환과 프라이버시 제한을 정책으로 설정할 수 있는 Identity Governance Framework 표준안도 현재 개발되어 발표되었다.

4. 시장 동향

본 장에서는 ID 관리 기술에 대한 국내외 시장 동향을 기술한다.

4.1 국내 시장 동향

한국IDC의 2008년 조사에 따르면, 국내 ID관리 및 접근제어 시장이 2007년 308억 원 규모에서 연평균 11.5%의 성장을 보이며 2012년 531억 원 규모의 시장으로 성장할 것으로 전망하고 있다[16].

(표 3) ID관리 및 접근제어 국내 시장 규모

(단위:억원)

2007	2008	2009	2010	2011	2012	평균 성장률
30,804	34,229	38,267	42,587	47,485	53,088	11.5%

소프트포럼은 ID관리 솔루션으로 SafeIdentity를 출시하였다. SafeIdentity는 멀티도메인 간, 다양한 어플리케이션 간의 통합인증(SSO) 제공, 역할기반접근제어(RBAC, Role-based Access Control) 시스템 제공, 정책 기반의 관리 기능 제공, 고도의 사용자 개인화를 통해 자동 사용자 요청 및 승인 프로세스 지원, 감사 보고 기능을 제공한다.

이니텍은 INISAFE Nexess를 통해 기업의 분산된 자원과 사용자를 통합하고 일관된 체계를 구축하는 EAM 솔루션을 제공한다. id/PW, PKI, 지문인식, OTP, MOTP(Mobile One-Time Password), Smart Card 등 다양한 인증 방식뿐만 아니라 멀티도메인에서의 안전한 SSO도 제공한다. 또한 RBAC 기반의 권한 관리, 중앙 집중적 통합 관리와 관리자 위임 기능을 통한 분산적 관리 기능을 제공한다.

드림시큐리티는 다양한 인증방식(id/pw, 인증서, 생체인식, cd-key)을 지원하며 인증 단계에 따른 권한을 선택적으로 부여하는 SSO 솔루션인 Magic SSO & EAM v3.0 제품을 출시하였다. 이 제품은 사용자 인증 및 ACL 발급을 담당하는 인증서버(Policy Server)와 사용자 PC에 설치되고 사용자인증 후 세션을 관리하는 클라이언트 에이전트(Client Agent), 사용자 및 권한 관리가 필요한 어플리케이션을 등록하고 권한을 관리하는 인터페이스인 관리자 어드민(Policy Server Admin)으로 구성되어 있다.

국내의 OpenID 시장은 2007년부터 시작되었으며, 현재 NC소프트(http://myid.net), 안철수연구소

(http://idtail.com), Daum(http://openid.daum.net)이 OpenID 제공자로 동작하고 있다. OpenID 소비자로는 NC 소프트의 스프링노트(www.springnote.com), 미투데이(me2day.net), 라이프팟(www.lifepod.co.kr), 아이두(www.idoo.net)가 있다. 최근 대형 포털 및 인터넷 사업자들도 OpenID 적용에 관심을 보이고 있으며, Paran과 Egloos 등은 자사의 URL을 OpenID로 사용할 수 있는 기능을 제공한다.

4.2 국외 시장 동향

IDC의 2007년 7월 조사에 따르면, 전 세계적으로 ID관리 및 접근제어 시장 규모를 2005년 2,766백만 달러에서 연평균 10.7%의 성장을 보이며 2011년에 4,975백만 달러에 이를 것으로 전망하고 있다[17].

(표 4) ID관리 및 접근제어 세계 시장 규모

(단위:백만불)

2005	2006	2007	2008	2009	2010	2011
2,766	2,989	3,370	3,770	4,152	4,548	4,975

Sun은 ID 관리, 보호, 저장, 검증을 위해 Identity manager, Access manager, Directory server, Identity auditor를 포함한 Identity Management Suite를 출시하였다. 이 제품은 중앙집중 Identity 관리, 중앙집중 접근제어, 단일 인증(SSO), 기업용 감사 및 보고, 자동화, self-service, 관리자의 역할 위임, 연방(Federation) 기능을 제공한다.

IBM은 2006년, 기존의 Tivoli Federated Identity Manager, Tivoli Directory Integrator, Tivoli Access Manager를 갱신하고 소규모 조직을 위한 ID 관리 full suite인 Tivoli Identity Manager Express와 역시 소규모 조직의 federation을 위한 Tivoli Federated Identity Manager Business Gateway를 출시하였다.

Microsoft는 독점적인 중앙 관리에서 벗어나 여러 ID 제공자의 다양한 ID 기술들을 상호운용하는 ID 메타시스템 개념을 제안하고, 이 개념을 구현하여 윈도우 Vista에 CardSpace로 구현하였다.

일본 NTT Communication은 Liberty Alliance의 Federation 기술을 적용하여 400만 가입자들에게 MasterID라는 SSO 서비스를 제공하였다. 또한 2007년 7월 3일, NTT Communication은 NTT 레조난트 주식회사의 gooID와의 제휴를 통해 통합 서비스를 제공하기 시작하였다. 본 제휴는 NTT 소프트웨어 주식회사의 TrustBind/Federation Manager 기반 제품으로 가능하며, 이 제품은 Liberty의 상호운용성 시험을 통과한 것이다.

5. 사용자 중심 IdM: 전자ID지갑

본 장에서는 최근 연구 개발이 활발히 진행되고 있는 사용자 중심 IdM 중에서 ETRI, MS, KISA가 공동으로 개발하고 있는 전자ID지갑 시스템에 대하여 기술한다.

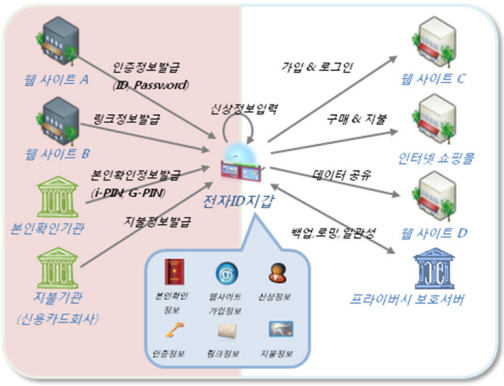
5.1 연구 배경

전자ID지갑은 사용자 본인이 개인정보와 인증정보(id/pw, 인증서 등)를 안전하게 관리하고 있다가, 언제 어디서나 자신을 인증하고 개인정보를 자신의 통제하에 선택하여 이용할 수 있는 시스템으로 다음과 같은 문제 해결을 목적으로 한다.

- 웹사이트 가입시마다 본인의 개인정보를 매번 입력하는 불편함
- 웹사이트 가입시 주민번호 입력에 대한 거부감
- 휴대폰으로 모바일 인터넷 로그인시 id/pw 입력이 매우 번거로움
- PC방과 같이 공용 PC에서 id/pw 입력에 대한 거부감
- 사용자가 접속하고 있는 사이트가 위장 사이트일지 모른다는 두려움
- 사용자가 어느 사이트에 가입되어 있는지 일일이 기억하기 어려움
- 이사, email 변경, 전화번호 변경 등과 같은 경우, 자신이 가입한 모든 사이트에 일일이 변경된 개인 정보를 갱신해야 하는 것이 불편함
- A 사이트에 저장된 나의 정보를 B 사이트에 새로 생긴 서비스로 가져가기 어려움

5.2 개념

전자ID지갑은 일상생활에서 사용하는 지갑처럼 인터넷 상에서 사용되는 사이버 지갑이다. 전자ID지갑은 사용자는 자신의 주소, 전화번호 등과 같은 개인정보, 로그인 아이디, 비밀번호 등과 같은 인증정보와 신용카드 등과 같은 지불정보들로 구성된 Identity 정보를 보관한다. 사용자가 인터넷 웹 사이트에서 서비스를 받으면서 웹 사이트가 사용자 인증, 개인정보, 결제 정보 등을 요구하면, 자신의 전자ID지갑에서 필요한 정보를 확인하여 웹 사이트에 제공하는 방식으로 운용된다. 그림 3은 전자ID지갑의 개념도이다.



(그림 3) 전자ID지갑 개념도

그림 3에서 보이듯이 전자ID지갑은 본인의 개인 신상 정보를 관리하고 있다. 그림 왼쪽에 있는 웹 사이트들은 사용자의 ID 정보를 제공하는 IdP(Identity Provider)들로, 전자ID지갑은 이들로부터 인증정보, 사용자 ID 정보, 본인확인 정보, 지불 정보 등을 발급받아 전자ID지갑에 저장한다. 이때 전자ID지갑에 저장되는 정보는 실제 사용자 ID 정보가 아니라 이들 정보를 발급받을 수 있는 연결(link) 정보이다. 이를 통해 전자ID지갑이 분실되더라도 실제 개인 정보가 노출될 위협이 제거된다. 그림 오른쪽에 있는 웹 사이트들은 사용자의 ID 정보를 소비하는 IdC(Identity Consumer)들로 사용자에게 서비스를 제공하는 웹 사이트들이다. 이들은 서비스를 제공하기 위해 사용자에게 가입 및 로그인, 지불 정보, ID 정보 등을 요청한다. 이들 요청 정보는 전자ID지갑에게 전달되고 전자ID지갑은 요청 정보를 만족하키는 IdP들을 Card 형태로 사용자에게 출력하여 사용자가 적절한 Card를 선택하도록 한다. 선택된 Card의 내용에 따라 전자ID지갑에서 직접 정보를 IdC에게 전달하기도 하고, IdP에 연결하여 ID 정보를 조회한 후, 해당 정보를 IdC에 전달하기도 한다.

그림 오른편에 있는 프라이버시 보호 서버는 전자ID지갑 분실을 대비한 백업 기능 및 자신이 사용하던 컴퓨터가 아닌 다른 컴퓨터에서도 전자ID지갑을 안전하게 사용할 수 있도록 해 주는 로밍 기능 등을 제공한다.

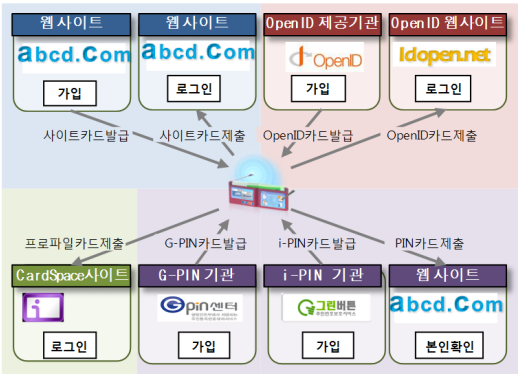
이와 같이 전자ID지갑은 사용자 ID 정보 흐름 중간에 위치하여, 사용자가 직접 ID 정보의 흐름을 통제할 수 있도록 하였으며, 모든 정보를 Card 형태로 표현하여 사용자에게 일관성있고 편리한 인터페이스를 제공하는 사용자 중심 ID 관리 시스템이다.

5.3 주요 기능

전자ID지갑이 제공하는 주요 기능은 다음과 같다.

5.3.1 웹사이트 가입 및 로그인 기능

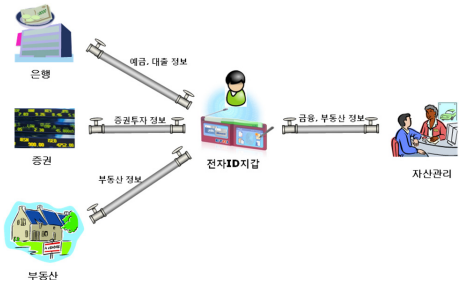
인터넷 웹사이트에 가입시 전자ID지갑에서 카드 형태의 프로파일 정보를 선택한 후 이를 제출하고, 사이트 카드 형태의 인증정보를 발급받은 뒤, 로그인 시 발급받은 사이트 카드를 선택하는 식으로 편리하게 가입 및 로그인을 수행할 수 있도록 해주는 기능이다. 웹사이트 가입시 본인확인을 수행하게 되는데, 이때 사용자는 i-PIN 발급 기관에서 카드 형태의 PIN 정보를 발급 받는다. 웹사이트 가입시 본인확인이 필요할 때 전자ID지갑에 보관 중인 PIN 카드를 선택하는 것만으로 본인 확인이 완료될 수 있도록 한다. OpenID 적용 웹사이트에서도 OpenID 제공기관에서 발급받은 OpenID 카드를 선택하여 로그인하는 기능을 포함한다. 그림 4는 전자ID지갑의 웹사이트 가입 및 로그인 기능을 보여준다.



(그림 4) 웹사이트 가입 및 로그인 기능

5.3.2 ID 공유 기능

사용자가 자신의 ID 정보를 웹사이트에 제공하거나, 다른 웹사이트에서 생성된 자신의 ID 정보를 타 웹사이트에 전달하는 기능으로 전자ID지갑에서는 몇 번의 클릭만으로 공유와 통제를 안전하게 수행하는 기능을 제공한다. 그림 5는 전자ID지갑의 ID 공유 기능의 활용 예를 도식화 한 것이다.



(그림 5) ID 공유 기능 활용 예

그림 5는 사용자의 금융 정보, 주식투자 정보, 부동산 정보가 전자ID지갑과 공유되고, 전자ID지갑은 공유된 개인 정보를 다시 자산관리 사이트와 공유함으로써 자산관리 사이트로부터 개인 자산관리 서비스를 받는 것을 나타낸다.

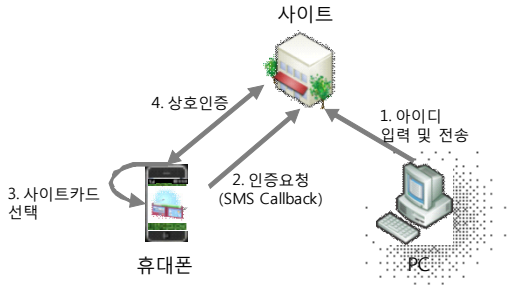
전자ID지갑은 ID 공유를 위해 전자ID지갑과 웹사이트 간에 공유 링크를 설정하는 기능을 제공한다. 공유링크는 실 세계의 계약서에 준하는 전자계약을 포함하고 있어, 공유하는 ID 정보와 ID 정보 공유시 필요한 인증, 인가, 보안 및 프라이버시 정책을 설정할 수 있다. 전자ID지갑을 통해 사용자 식별 및 데이터 검색이 이루어지므로 전자ID지갑에서 사용자는 프라이버시 통제만 행사하면 된다.

5.3.3 지불 결제 기능

사용자가 웹사이트에서 이용한 서비스 및 물품 구입 대금을 전자ID지갑에 저장된 지급결제 카드를 활용하여 안전하고 편리하게 결제하는 기능이다. 카드번호, 유효기간 등 복잡한 정보를 사용자가 직접 입력하지 않고 해당 카드 선택만으로 간단하게 지급결제가 수행된다. 신용카드, 휴대폰, 계좌이체 등의 수단이 제공되며, 사전에 사용자가 생성한 지불 카드를 지불시 선택하는 방식으로 지불결제가 이루어지게 된다.

5.3.4 모바일 보안 강화 로그인 기능

PC방 등 공개된 환경에 위치한 PC를 사용할 때 휴대폰을 이용하여 인증함으로써 사용자의 비밀번호 노출을 방지하는 기능이다. 전자ID지갑 소프트웨어가 설치되지 않은 PC에서도 휴대폰을 통해 안전하게 인증할 수 있는 수단을 제공한다. PC에서 id를 입력하여 웹사이트로 전송하면, 웹사이트는 사용자 id를 이용하여 사용자 휴대폰에 인증요청 SMS 메시지를 보낸다. 사용자는 휴대폰에 탑재된 모바일 전자ID지갑에서 사이트 카드를 선택한다. 휴대폰과 웹사이트 간의 상호인증이 이루어지고 이를 통해 웹사이트에 로그인한다. 그림 6은 모바일 보안 강화 로그인 기능의 흐름을 보인다.



(그림 6) 모바일 보안 강화 로그인 기능 흐름도

6. 결 론

본 고에서는 사용자의 ID 정보를 안전하게 관리하고 공유하는 ID 관리 기술에 대한 동향 및 전망을 기술하였다. ID 관리 기술은 국내외적으로 활발히 연구

가 진행되고 있으며 최근에는 웹 2.0 등에서 쉽게 사용할 수 있는 OpenID와 사용자 통제를 강화하고 일관성 있는 인터페이스를 제공하는 Card-Based IdM들이 활발히 연구 개발되고 있다. 국내외적으로 ID 관리 표준화가 활발히 진행되고 있으며, 국내 시장과 국외 시장에서도 ID 관리 시스템은 향후 꾸준히 성장할 것으로 예상된다. 본 고에서는 국내에서 연구개발이 진행되고 있는 사용자 중심 ID 관리 시스템인 전자ID지갑의 연구배경, 개념 및 주요 기능에 대하여 살펴보았다.

향후 ID 관리 기술은 현재의 웹 환경뿐만 아니라 사용자의 참여와 정보 공유가 더욱 중요해지는 웹 2.0 환경에 적합한 사용자 중심 ID 관리 기술이 더욱더 발전할 것으로 보이며, 서로 다른 영역의 ID 관리 기술들이 상호 융합을 통해 서로 간의 장점을 흡수하는 방향으로 ID 관리 기술이 발전할 것으로 보인다. 이를 통해 ID 관리 기술이 인터넷 환경의 안전성을 제고시킬 것으로 기대된다.

참 고 문 헌

[1] OECD WPISP, “Background paper on digital identity management,” 2006

[2] 한국정보보호진흥원, “개인정보의 경제적 가치 연간 약 1조 3천억원에 달해,” 2007.1

[3] 조영섭 외, 사용자 중심 ID 관리 기능을 제공하는 전자ID지갑 시스템, 전자통신동향분석, Vol. 23, No. 4, 2008

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

[5] 조영섭, 사용자 중심의 ID 관리 기술, FISCON 2008

[6] TTA, i-PIN 서비스 프레임워크, TTAS.KO-12.0054, 2007.12

[7] TTA, i-PIN 서비스 전달 메시지 형식, TTAS.KO-12.0055, 2007.12.26

[8] Higgins Open source Identity Framework, http://www.eclipse.org/higgins/

[9] Identity Woman, OASIS Identity Metasystem Interoperability TC - announced, 2008.7.24, http://www.identitywoman.net/?p=777

[10] Bandit Project, http://www.bandit-project.org/

[11] Liberty Alliance, http://projectliberty.org/

[12] OASIS Security Assertion Markup Language (SAML) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[13] OASIS eXtensible Access Control Markup Language(XACML), http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

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

[15] OASIS XRI Data Interchange(XDI) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xdi

[16] 한국IDC, “Korea Security Software 2008-2012 Forecast and Analysis,“ 2008.7

[17] IDC, “Worldwide Identity and Access Management 2007-2011 Forecast and 2006 Vendor Shares,” 2007.7

◐ 저 자 소 개 ◑

조 영 섭

1993년 인하대학교 전자계산공학과 학사
1995년 인하대학교 대학원 자자계산공학과 석사
1999년 인하대학교 대학원 전자계산공학과 박사
1998~현재: 한국전자통신연구원 정보보호연구본부 선임연구원
관심분야: Digital Identity Management, 인증인가, 정보보호

진 승 헌

1993년 숭실대학교 전자계산학과 학사
1995년 숭실대학교 대학원 전자계산학과 석사
2004년 충남대학교 대학원 컴퓨터과학과 박사
1999~현재: 한국전자통신연구원 정보보호연구본부 팀장/선임연구원
관심분야: Digital Identity Management, PKI, PMI, 인증인가, 개인정보보호