인터넷 환경의 사용자 중심 ID 관리시스템 연구동향†

원광대학교 이형효*
한국전자통신연구원 조상래 · 진승헌
전남대학교 노봉남**

1. 서 론

초고속인터넷 서비스의 빠른 보급으로 개인간 정보 교환은 물론 B2B, B2C 형태의 전자상거래 그리고 전자정부서비스가 일반화되고 있다. 그러나, 사용자들은 인터넷 사이트에서 제공하는 서비스를 이용하려면 각 사이트에서 요구하는 회원등록절차를 거쳐야 하며 회원등록과정에서 이름, 주민번호, 주소, 연락처 등 사용자 개인정보를 서비스 제공자에게 제공해야 한다. 경우에 따라 사용자는 각 사이트에서 설정한 아이디(identifier), 비밀번호 작성규칙에 따라 사이트마다 다른 아이디, 비밀번호를 발급받는 불편함도 발생하고, 각 사이트에서 제공되는 서비스를 이용하기 위해 사이트별로 각각 인증을 받아야 하는 불편함도 있다. 더욱 심각한 문제는 각 사이트에 제공된 개인정보의 관리절차, 개인정보 사용이력, 사용자가 가입한 사이트와 협력관계에 있는 타 사이트와의 개인정보 공유 등에 대한 정보를 개인정보 소유자가 손쉽게 파악하기 어려워 프라이버시 침해 및 개인정보 오남용 위험성이 높고 실제로 피해가 발생하고 있다는 점이다[19]. 따라서 개인의 프라이버시를 보호하면서도 개인정보를 안전하게 활용하도록 지원하는 관리체계에 대한 연구가 필요하게 되었다[1].

국내는 물론 미국, EU 등에서도 수년전부터 개인의 프라이버시를 보호하면서도 인터넷 환경에서 사용자가 정보서비스를 손쉽고 편리하게 이용할 수 있는 인프라에 대한 연구를 진행 중에 있다[2,3,4]. 본고에서는 위에서 언급된 문제점들을 해결하기 위해 국내외에서 진행 중인 인터넷 환경의 사용자 중심 ID 관리시스템들의 특성에 대해 정리, 분석한다.

† 본 연구는 한국전자통신연구원 연구과제(0801-2006-0006) 지원으로 수행되었습니다.
* 정 회 원
** 종신회원

2. ID 및 ID 관리시스템

2.1 디지털 Identity

디지털 Identity(이하 ID)란 온라인 환경에서 자신을 식별하기 위해 사용되는 속성(attribute) 정보의 집합으로 정의할 수 있다. ID를 구성하는 속성은 ID를 유일하게 식별하는 아이디 (identifier), ID 소유자임을 증명하는데 사용되는 패스워드나 인증서 등과 같은 신원증명(credential) 정보, 그리고 나이, 연락처 정보 등으로 매우 다양하다. ID는 사용자가 수행하는 거래의 종류나 역할에 따라 모든 ID 정보가 사용되지 않고 일부 ID만 이용된다(그림 1)[5].

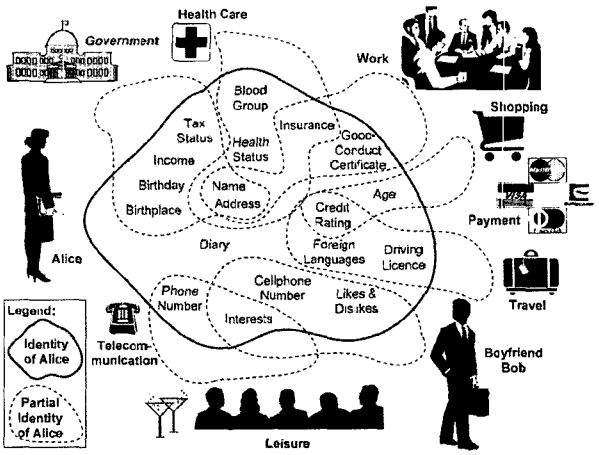

그림 1 디지털 ID 구성

일반적으로 사용자 ID는 정보화기기 및 인터넷의 여러 사이트에 분산, 중복 저장되어 있다. 따라서 정보시스템 이용이 활성화됨에 따라 사용자 ID를 구성하는 정보의 양도 증가하게 되어 관리의 불편함과 함께 개인정보 유출로 인한 프라이버시 문제가 이미 발생하고 있다. 그리고 유비쿼터스 사회로 발전함에 따라 ID에 대한 안전한 관리의 중요성은 더욱 커질 전망이다.

전자정부나 전자상거래 등을 통해 인터넷 사용이 일상화되고 있는 현실에서 신뢰할 수 있는 인터넷 환경

을 구축하는 것은 개인뿐만 아니라 사회, 국가적으로 매우 중요한 요소이다. 전자거래의 안정성을 보장하고 활성화를 유도하기 위해 ID 중복으로 발생되는 불편함을 해소하고 ID 도용 및 유출을 방지함과 함께 개인의 프라이버시 역시 보호되어야 한다.

2.2 ID 관리시스템

ID 관리시스템은 위에서 언급된 문제점들을 해결하기 위해 단일인증 서비스(SSO: Single Sign-On), 개인정보 소유자가 설정한 프라이버시 정책에 의한 개인정보 공유, 분산저장된 ID에 대한 일관성있는 관리기능을 수행하는 시스템으로 안전하고 신뢰성있는 개인간 정보교환이나 전자상거래, 전자정부서비스 구현을 위해 갖추어야 될 필수적인 ID 관련서비스를 제공한다.

초기 ID 관리시스템은 ID 관련 모든 정보를 단일 시스템에 저장하는 중앙집중형이 대부분을 차지했으며 대표적인 사례로는 Microsoft사의 .NET Passport가 있다. 그러나 사용자의 개인정보를 한 기업에서 통합관리하는 체계와 다른 ID 관리시스템과의 연동이 되지 않는 문제가 있다.

최근 이러한 문제점을 해결하기 위해 개인정보가 인터넷에 연결된 ID 관리시스템에 분산저장되어 있고 서로 연동할 수 있는 ID 관리체계에 대한 연구개발이 진행되고 있다. 이러한 ID 관리시스템의 대표적 예로는 IBM과 Microsoft 등이 주도하는 WS-I(Web Services Interoperability organization), Sun이 주도하여 2001년 결성되어 현재 150 여개 회원을 가진 Liberty Alliance[6]가 있다. 국제 표준화기구인 ISO/IEC JTC1/SC27은 ID 관리시스템 연구를 위한 WG5("Privacy, Identity and Biometric Security)를 새로 구성하였고[7], 경제협력개발기구(OECD: Organisation for Economic Co-operation and Development)에서도 정보보호작업반(WPISP: Working Party on Information and Security)을 구성, 전자정부서비스 및 전자상거래 활성화를 위해 ID 관리프레임워크에 대한 연구를 진행하고 있다[21].

한편 여러 프로토콜의 추가 설치가 요구되는 WS-I나 Liberty Alliance 외에 경량화된 ID 관리시스템들이 최근 개발되고 있는데, 이 시스템들은 인터넷 환경을 기반으로 하고 개인정보 이용 및 공유를 개인정보 소유자가 결정하는 사용자 중심의 ID 관리기능을 공통적으로 가지고 있다.

다음 장에서는 현재 개발이 진행 중인 인터넷 환경의 사용자 중심 ID 관리시스템들의 구조 및 특징에 대해 기술한다.

3. 사용자 중심 ID 관리시스템

3.1 XRI

XRI(eXtensible Resource Identifier)는 XML 관련 표준을 제정하는 OASIS에서 제정된 표준으로 위치, 응용, 프로토콜에 무관하게 추상화된 식별정보(identifier)에 대한 표준 구문과 변환 프로토콜(resolution protocol)을 정의하고 있다[8-11]. XRI 명세는 IETF(Internet Engineering Task Force)와 W3C(Word Wide Web Consortium)에서 표준으로 제정한 URI(Uniform Resource Identifier)와 IRI(Internationalized Resource Identifier)에 기반을 두고 있다. URI는 분산 네트워크 환경에서 자원을 효과적으로 식별하는 표준화된 방법이며, IRI는 URI가 ACSII 문자만 지원하는 단점을 보완하여 전체 UCS(Unicode Character Set)를 지원하는 특징이 있다.

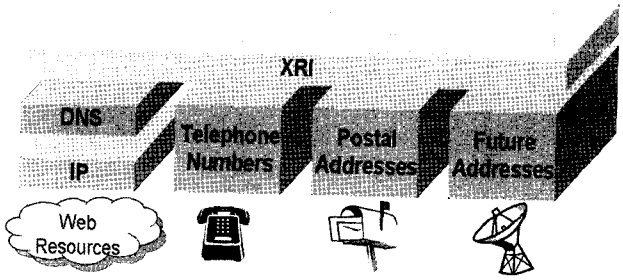

그림 2 XRI 동작계층

그림 2와 같이 XRI에 의해 표현된 자원은 특정 서비스나 응용, 저장된 위치, 접근 프로토콜에 무관하게 자원을 추상적으로 표현되고 있어 자원의 저장위치나 관리기관이 변경되어도 식별정보에 대한 자원을 투명하게 접근할 수 있는 장점이 있다.

XRI 식별정보[8]는 authority, path, query, fragment로 구성되는 점에서 URI와 IRI 식별정보 구조와 유사하나 각 구성요소가 URI, IRI의 구성요소에서 지원하지 않는 정보를 표현할 수 있으며 prefix로 "xri://"를 사용한다(그림 3).

xri:// *authority* / *path* ? *query* # *fragment*

그림 3 XRI 식별정보 구조

XRI authority 중 첫 서브세그먼트를 XRI 루트 authority라고 부르며, 루트 authority 중 특수한 authority를 표현하기 위해 사용되는 글로벌 컨텍스트 기호 (GCS: Global Context Symbol)와 의미, 사용 예를 정리하면 표 1과 같다.

3.2 XDI

XDI(XRI Data Interchange)는 OASIS의 XDI 기술위원회에서 개발 중인 XML 문서와 XRI를 사용하여 인터넷 및 다른 네트워크상에서 데이터를 공유, 연결 및 동기화하는 확장 가능한 서비스이다[12]. 이것은 사용자 수준에서 인식(human-readable) 가능한 현재의 웹이 다양한 사이트에 저장된 자원들을 HTML 문서를 이용하여 연결하는 방식과 같이, XDI도 XML 문서를 이용하여 다양한 자원들이 식별, 교환, 연결, 동기화될 수 있는 기계인식(machine-readable) 가능한 Dataweb을 구축하는 데 목적이 있다. 그러나 Dataweb에서는 공유 데이터에 대한 접근이나 사용에 대한 다양한 통제기능을 XDI 링크에 부여할 수 있어 신뢰된 데이터 교환 서비스를 제공할 수 있는 장점이 있다.

표 1 글로벌 컨텍스트 기호와 기능

글로벌 컨텍스트 기호	용 도	예 제
@	기관	xri://@sample*department/
=	사용자	xri://=john.smith
+	일반 용어	xri://+flower
$	표준화 기구에서 제안된 개념, 용어	xri://$contract
!	fully persistent	xri://!!1234

XDI 기술위원회에서 제안하는 Dataweb은 URI, HTML, HTTP 기술을 사용하고 있는 현재의 웹에 비해 정보 및 자원 위치, 소속 도메인, 응용, 프로토콜에 독립적(XRI)이며, 컴퓨터에 의해 자동처리가 가능(XML)하며 보다 정보를 포함한 문서 교환을 위해 다양한 프로토콜을 지원하는 특징을 가지고 있다. 그리고 Dataweb이 현재의 웹과 가장 큰 차이점은 XDI 링크에 대한 인증, 인가, 프라이버시 보호 등 다양한 통제기능을 제공하는 데 있다(표 2).

표 2 현재 웹과 Dataweb의 주소지정 방식 차이점

기능 요구사항	현재의 웹 (HTTP URI)	Dataweb 주소지정 (XRI)
지속성	정보나 자원의 위치이동, 이름 변경시 링크가 끊어지는 문제에 대한 표준화된 해결방법을 지원하지 않음	XRI authority나 path 세그먼트에서 재지정가능, 지속적인 식별정보 지원
위임 및 연계	도메인 이름에 한해 위임기능 지원	XRI authority나 path 세그먼트에서 제한없이 위임 기능
글로벌 컨텍스트	URI 중 top-level 도메인에 한하여 지원	4종류 (=, @, +, $)의 글로벌 컨텍스트 지원
교차 참조	다른 도메인의 URI 사용을 위해 URI 중첩사용 불가능	XRI 식별정보 내에 XRI나 URI가 제한없이 중첩사용 가능
국제화	부분적인 국제화기능 지원	완전한 IRI 지원
확장성	새로운 URI 스킴과 변환 프로토콜을 통해 확장가능	XRI 스킴과 변환 프로토콜에 따라 확장가능

Dataweb은 웹 서비스와 시멘틱 웹(Semantic Web)의 핵심 내용을 웹 구조의 중요 요소들과 결합함으로써 분산 데이터를 공유하기 위한 "복잡함의 이면에서 단순함"이 될 수 있는 해결책을 제시한다. Dataweb은 현재 웹의 연결(link)과 다른 점은 웹의 연결은 단지 연결된 자원을 가져올 수만 있지만, Dataweb의 연결은 쌍방향으로 데이터 교환할 수 있는 점이다. 또한 웹의 연결은 자원이 이동, 삭제된 경우 자원에 대한 연결불가능(broken link) 문제가 발생되나 Dataweb에서는의 대상 자원이 이동하거나, 이름의 변경, 소유자의 변경이 있을 경우에도 지속성있는 XRI를 이용하여 자원에 대한 연결서비스를 제공한다. 그리고 현재 웹 자원의 접근은 공개(public) 또는 비공개(private) 중에 하나인데, Dataweb의 연결은 XDI 연결 계약(link contracts)을 이용하여 모든 데이터의 흐름에 대하여 포괄적이면서도 세부 조절이 가능한 특징이 있다(그림 4).

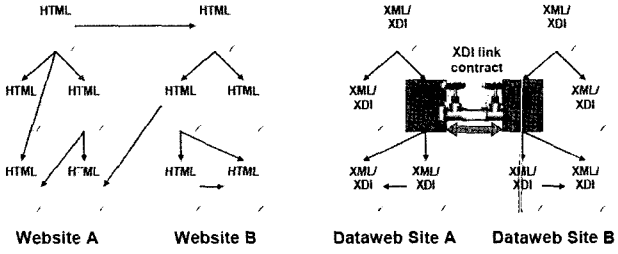

그림 4 현재 웹과 Dataweb 특징 비교

XRI와 XDI 표준을 기반으로 한 식별정보 서비스로는 2idi사[13]에서 제공하는 I-Names 서비스가 있다. I-Names 서비스는 식별대상인 가입자의 주거지 및 소속기관 변동으로 인한 가입자 정보의 변경에 관계없이 전자메일주소, 메시징서비스 주소, FAX번호, 이동전화번호 등 정보를 가입자가 제공 및 접근여부를 통제할 수 있는 서비스를 제공한다. 또한 가입자는 하나의 식별정보와 비밀번호만을 이용하여 Dataweb을 지원하는 사이트들간 SSO(Single Sing-On) 서비스를 지원받을 수 있다. 그리고 I-Names 서비스는 XRI가 UCS를 지원하고 있어 가입자는 자신이 사용하는 언어를 이용하여 식별정보를 지정할 수 있는 장점도 제공한다.

3.3 OpenID

OpenID는 Six Apart사에 의해 개발 중인 분산시스템 기반 사용자 중심의 ID 관리시스템으로 현재 OpenID 시스템에서 제공하는 주요 기능은 사용자가 자신이 이용하려는 각 사이트마다 계정을 갖지 않더라도 서비스를 사용할 수 있도록 하는데 있다[14]. 이를

위해 OpenID는 사용자가 자신의 계정이 개설되어 있지 않는 서비스 제공 사이트(Consumer)에 접속할 때 자신을 인증할 수 있는 사이트(Server)에서 인증과정을 수행하고 그 결과를 서비스 제공 사이트에게 전달하는 기능을 제공한다.

OpenID 시스템은 사용자 ID가 등록, 관리되고 있는 OpenID 서버를 이용해서 인증을 제공한다. 인증과정에서 OpenID 서버는 ID외에 추가적인 정보를 요구하지 않고 ID로 사용되는 URL 정보만을 이용하여 OpenID 서버에서 제공하는 증명 알고리즘을 이용하여 사용자를 인증한다. OpenID 시스템은 누구든지 추가로 소요되는 비용 없이 OpenID 관리 시스템이 될 수 있으며 OpenID식별자를 기반으로 인증을 제공하는 사이트들을 운용할 수 있다. 이 시스템들은 표준을 준수하기 때문에 모든 웹 브라우저를 지원한다.

OpenID는 일반적인 ID 관리 시스템과 비교해서 대략 3가지 장점을 갖는다. 첫째, OpenID는 사용자가 광범위한 인터넷 환경에서 자신의 ID를 완전한 분산시스템 구조하에서 관리할 수 있도록 지원한다. 둘째, 기존의 .NET Passport 시스템에서 SSO기능은 단일 COT(circle of trust)로 제한되었으나 OpenID는 OpenID가 가용한 모든 웹사이트에서 사용이 가능함으로써 단일한 로그 인으로 미칠 수 있는 영역의 범위가 확장된다. 셋째, OpenID는 OpenID의 서버의 이외에 응용의 설치와 부가적인 개인정보 요청 없이 온라인상에서 기존의 웹 브라우저만을 이용해 개인에 대한 인증기능을 수행한다.

OpenID 시스템은 User-Agent(*UA*), Identity(*I*), Consumer(*C*), Server(*S*) 등으로 구성된다. *UA*는 사용자가 인터넷 접속을 위해 이용하는 웹 브라우저를 의미한다. *I*는 사용자 ID를 의미하며 이는 URL로 표현된다. *C*는 사용자로부터 OpenID URL형태의 Identity를 제공받아 OpenID 서버에게 인증을 위임하는 웹사이트를 의미한다. *S*는 OpenID를 인증하는 OpenID 서버를 나타낸다.

그림 5는 OpenID의 인증절차를 보인다. *h*는 *S*로부터 생성된 세션 식별자이며, n과 t는 각각 nonce와 타임스탬프를 의미한다. k는 Consumer와 Server 사이에 전달되는 메시지의 무결성 점검을 위한 키를 의미한다. 먼저 단계 1에서 사용자가 Consumer 사이트에 자신의 Identity를 전달하고, 단계 2, 3에서 Consumer 사이트는 Identity에 의해 지정된 위치에서 Server 정보를 얻는다. 단계 4는 Consumer와 Server가 사용자의 인증을 위임하기 전에 인증 단계를 안전하게 수행하기 위해 안전한 통신을 위해 키를 협상하는 단계이다. 단계 5, 6에서 UA는 C가 전달한 S로 리다이렉트되며 이 때 *I*, *C*, *h*, *n*, *t* 값이 URL에 포함되어 전달된다. 단계 7과 8은 Server가 사용자에게 인증을 요구하고 ID/PW 방식과 같은 방식을 통해 인증을 수행하는 단계이다. 마지막으로 단계 9와 10에서 Server는 사용자에 대한 인증결과를 Consumer에게 중계한다. 이러한 인증과정을 통해 사용자는 계정이 없는 Consumer 사이트에 접속할 수 있게 된다.

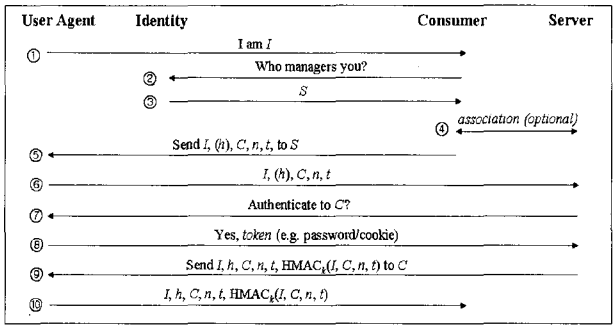

그림 5 OpenID 인증 절차

지금까지 구현된 OpenID 시스템은 인증기능 위주로 개발되었으나 구현 중인 OpenID 2.0에는 인증 외에 보다 포괄적인 ID 관리기능을 포함하고 있다.

3.4 LID

LID(Light-weight Identity) 프로젝트는 Netmesh사에 의해 개발된 ID 관리시스템으로 기존의 ID 관리시스템에서 추구하는 중앙집중식 구조에 의존하지 않고 인터넷 상에서 디지털 ID를 표현하고 사용하기 위한 프로토콜과 소프트웨어 구현을 목표로 하고 있다[15]. LID의 특징은 정보의 주체인 개인이 온라인상에서 자신의 모든 디지털 ID들을 관리하고 제어할 수 있다는 점이며 LID에서 식별정보는 URL 형태로 표현된다.

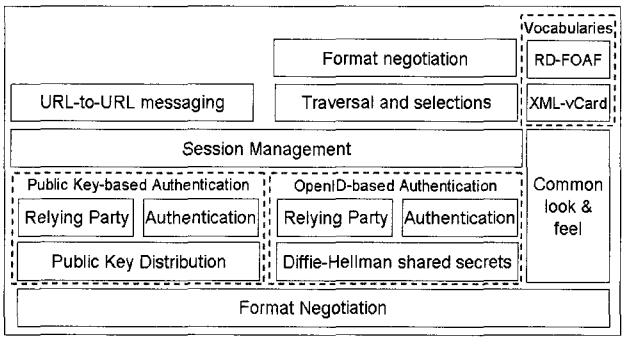

그림 6 LID 아키텍처

그림 6은 LID 아키텍처를 나타낸다. LID는 SSO, 개인 연락정보 관리, 개인정보 포맷 협상, XML 기반의 정보교환과 XPath를 이용한 정보선택 등과 같은

다양한 종류의 LID 서비스 프로파일들로 구성되어 있어서 ID관리의 다양한 서비스를 지원한다. LID는 SSO 서비스, 개인정보에 대한 통제 서비스 그리고 LID 구성요소간 전달되는 메시지에 대한 인증 서비스 외에도 사용자의 속성정보를 다른 사용자에게 안전하게 전달할 수 있는 다양한 기능들을 제공한다.

LID는 MS사의 .NET Passport와 같이 단일 회사가 개인의 디지털 ID를 중앙집중방식이 아닌 분산화된 ID 관리 서비스를 제공하며, OpenID 기반의 인증 프로토콜도 인증 프로토콜로 지원하고 있어 OpenID가 지원하는 URL을 이용한 인증 서비스를 지원한다. 또한 Liberty Alliance가 기업 관점에서 개인정보를 관리하는데 반해 LID는 사용자가 자신을 인증하는 시스템을 지정할 수 있고 자신의 디지털 ID 제공을 직접 통제할 수 있어 사용자 중심의 ID 관리 기능을 제공하는 특징이 있다.

3.5 SXIP

SXIP(Simple eXtensible Identity Protocol)[16]은 인터넷과 같은 대규모 네트워크 환경에 적합하고 디지털 ID 정보의 자동 교환을 위해 개발된 프로토콜이다.

그림 7과 같이 SXIP는 크게 User Client와 Homesite, Membersite로 구성된다. User Client는 사용자가 SXIP를 이용하기 위해 사용하는 웹 브라우저를 의미한다. Homesite는 사용자들이 ID 프로파일을 생성하고 ID 정보를 저장, 유지하는 사이트를 의미한다. 즉, Homesites는 웹사이트 또는 온라인상의 사용자 사이에 ID 교환이 쉽도록 하거나 다른 사이트에 제공한 그들의 데이터를 제공하는 기능을 수행하는 사이트들로서 의료, 금융, 회사 등 다양한 사이트가 될 수 있다. Homesite에는 사용자의 역할 또는 환경에 따라 서로 다른 ID 속성들로 구성된 집합인 Persona가 저장되어 있으며, SXIP 2.0에서 Persona 정보는 URI에 의해 표현된다.

그림 7의 단계 1에서는 사용자 Beth가 서비스 이용을 위해 membersite geeknews.com에 접속하고 geeknews.com 사이트는 사용자 인증과 인증된 사용자에 대한 정보를 저장, 관리하고 있는 homesite를 입력하도록 사용자에게 요청한다. 단계 2는 단계 1에서 사용자가 입력한 homesite인 ISP.com으로 사용자 브라우저가 리다이렉트되고 사용자 인증을 위한 ID와 비밀번호 입력을 요구하는 인증화면이 출력된다. 인증이 성공한 경우 Beth는 geeknews.com 사이트가 자신의 개인정보(전자메일 주소, 이름, 우편 주소 등)를 요청한 사실을 ISP.com을 통해 확인하고 개인정보의 제공여부 결정과 함께 최종 확인을 거쳐 개인정보 제공을 허가하게 된다. 단계 4, 5에서 Beth의 웹 브라우저는 geeknews.com으로 리다이렉트되고 geeknews.com이 제공하는 서비스를 정당하게 사용하게 된다.

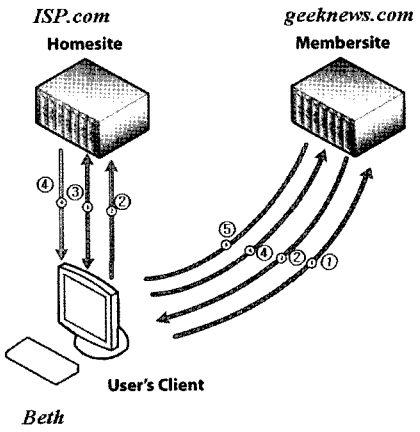

그림 7 SXIP 동작 구조

현재의 최신의 SXIP 프로토콜 버전은 SXIP 2.0이며, SXIP 2.0은 PKI를 필요로 하지 않는 URL기반 프로토콜인 Digital Identity eXchange(DIX)를 확장하여 개발되었다. SXIP 2.0 소스는 공개되어 배포되고 있으며 이것은 주요 클라이언트와 자료 교환 수단으로 웹 브라우저 등 다양한 기존의 기술들을 지원하고 있다. SXIP 2.0 프로토콜은 사용자의 디지털 ID를 구성하는 이름, 연락처, 근무처 정보 등 속성 정보에 대한 표준도 정의하고 있어 사이트간 정확한 디지털 ID 정보교환을 지원하는 특징을 제공하고 있다.

3.6 CardSpace

Microsoft가 SSO 서비스와 단일 ID로 여러 정보 시스템에 접근할 수 있도록 2000년에 발표된 .NET Passport[17]는 2억 명이 넘는 사용자를 확보했음에도 불구하고 단일 회사가 개인 ID를 중앙집중방식으로 관리하는 단일 ID 체계의 보안성과 프라이버시 보호에 대한 문제로 성공하지 못하였다. 이에 따라 Microsoft는 .NET Passport의 문제점을 보완하기 위해 WS-* 프로토콜과 XML 기반의 SOAP, SAML 등을 이용한 ID 메타시스템인 CardSpace(구 InfoCard)를 개발중에 있다[18]. CardSpace는 .NET Passport와는 달리 단일 ID 관리 대신 여러 ID를 관리할 수 있으며 CardSpace 소유자가 접속하는 사이트에 적합한 ID를 선택, 사용하는 기능을 제공한다. 다시 말하면, CardSpace는 card 선택기능을 수행하는 소프트웨어로 정의될 수 있고 card에는 사용자 ID, 유효기간, 발행자,

ID 정보를 표현하는 token 형식에 대한 정보를 저장하고 있는 있다.

그림 8은 CardSpace가 동작하는 예를 보이고 있다. 하나 이상의 ID를 소유하고 있는 사용자가 서비스 제공 사이트(RP: Relying Party)를 방문(①)하면 RP는 사용자 인증을 위해 필요한 ID 정보와 저장형식을 사용자에게 요청한다(②). CardSpace 소프트웨어는 RP 요구사항을 만족하는 ID card들을 선택하여 사용자에게 제시하게 되고(③) 사용자는 제시된 card 중 하나를 선택한다(④). 사용자에 의해 선택된 card는 card에 저장된 ID 서비스 제공자(Identity Provider)에게 사용자에 대한 token 생성을 요청하게 되고(⑤) ID 서비스 제공자에 의해 생성된 token은 CardSpace를 거쳐 RP로 전달되게 된다(⑥⑦).

CardSpace 시스템은 윈도우즈 Vista에 기본적으로 설치될 예정이며 윈도우즈 XP에도 설치가 가능하다.

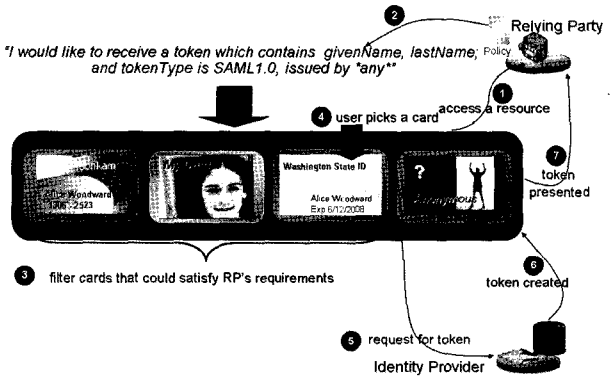

그림 8 CardSpace 동작 절차 예

4. 결 론

사용자들은 인터넷을 통한 온라인 서비스를 통해 일상 업무를 처리함으로써 편의성 제고와 함께 비용을 절감하는 혜택을 누리고 있다. 그러나, 이러한 온라인 서비스 이용을 위해 사용자들은 자신들이 사용하고자 하는 각 온라인 사이트에 이름, 주민번호, 주소, 연락처, 전자메일주소 등의 개인정보를 제공해야 하지만, 제공된 자기정보가 어떻게 사용, 관리되고 개인정보를 제공한 사이트와 제휴관계에 있는 다른 온라인 사이트에게 어떤 정보들이 공유되는지 알 수 없어 개인정보 유출 및 오남용으로 인한 피해에 노출될 수 있는 문제점을 안고 있다. 국내에서도 주민번호 등 타인 정보의 훼손, 침해, 도용 침해가 개인정보 침해 사례 중 가장 많은 비중을 차지하고 있다[19].

본 보고에서는 현재 국내외에서 연구, 개발되고 있는 인터넷 환경의 주요 ID 관리시스템에 대해 조사, 정리하였다. 조사된 대부분 ID 관리시스템들은 국제표준기술에 준거하고 있고 이전에 개발되었던 ID 관리시스템들에 비해 개인정보소유자의 자기정보통제권을 보호하기 위한 방법들을 제공하고 있다. 그리고 한 기관이나 기업이 개인정보를 중앙집중하는 구조 대신 분산된 시스템에 개인정보를 저장하고 활용하는 구조를 가지고 있다.

최근 ISO/IEC[7], EU[2,3,20], 경제협력개발기구[21]에서도 전자상거래 및 전자정부서비스 활성화를 촉진하기 위한 기반 환경으로 프라이버시를 보호하면서 개인정보 공유기능을 제공하는 ID 관리시스템에 대한 표준화 및 연구개발을 추진하고 있다. 국내에서도 외국의 연구 및 표준화 동향을 분석하면서 우리나라 환경에 적합한 ID 관리시스템을 개발하고 적용해 나가야 할 것으로 예측된다. 그리고 ID 관리시스템에 대한 기술측면 외에도 법제적 지원이 필수적으로 동반되어야 하므로 개인정보가 안전하게 보호되고 개인정보의 자기결정권에 의한 개인정보 공유를 가능하게 하는 법률 및 제도 제정 노력이 함께 진행되어야 할 것이다.

참고문헌

[1] 진승헌, 인터넷 서비스 환경의 고도화와 디지털 ID 관리 기술, 주간기술동향, 2006. 6.

[2] PRIME - Privacy and Identity Management for Europe, https://www.prime-project.eu/

[3] FIDIS(Future of Identity in the Information Society), http://www.fidis.net

[4] 인터넷 ID 관리 서비스, 한국전자통신연구원 디지털ID보안연구팀, 2006.

[5] HP, Federation - the enabler for electronic business, 2004.

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

[7] ISO/IEC JTC1/SC27 WG5 N4721, Information Technology - Security Techniques - A Framework for Identity Management, Oct., 2005.

[8] D. Reed, D. McAlpin, An Introduction to XRIs, Working Draft 04, http://docs.oasis-open.org/xri/xri/V2.0/xri-intro-V2.0.pdf, March 2005.

[9] G. Wachob, D. Reed, L. Chasen, W. Tan, S. Churchill, Extensible Resource Identifier (XRI) Resolution V2.0, http://docs.oasis-open.org/xri/xri/V2.0/

xri-resolution-V2.0-cd-01.pdf, March 2005.
[10] D. Reed, D. McAlpin, Extensible Resource Identifier (XRI) Syntax V2.0, http://docs.oasis-open.org/xri/xri/V2.0/xri-syntax-V2.0-cd-01.pdf, March 2005.
[11] D. Reed, Extensible Resource Identifier (XRI) Metadata V2.0, http://docs.oasis-open.org/xri/xri/V2.0/xri-metadata-V2.0-cd-01.pdf, March 2005.
[12] D. Reed, G. Strongin, The Dataweb: An Introdutction to XDI, April, 2004.
[13] http://www.2idi.com
[14] OpenID, http://openid.net/
[15] LID, http://lid.netmesh.org/
[16] SXIP, http://www.sxip.com/
[17] Microsoft, "Microsoft .NET Passport," http://www.microsoft.com/net/services/passport, 2004.
[18] Microsoft CardSpace, http://msdn2.microsoft.com/en-us/library/aa480189.aspx
[19] 박창열, "주민번호 대체수단 소개 및 진행현황," 정보보호 정책동향, 한국정보보호진흥원, 2006. 4.
[20] GUIDE, http://istrg.som.surrey.ac.uk/projects/guide
[21] OECD Working Party on Information Security and Privacy, Background Paper on Digital Identity Management, Sep., 2006.

이 형 효

1987. 2. 전남대학교 계산통계학과(학사)
1989. 2 KAIST 전산학과(석사)
2000. 2 전남대학교 대학원 전산학과(박사)
1990~1997 삼보컴퓨터 기술연구소, 한국통신 연구개발원
2001. 3~현재 원광대학교 정보·전자상거래학부 조교수
관심분야 : 프라이버시보호모델, ID관리시스템, 보안모델, 전자상거래보안
E-mail : hlee@wonkwang@ac.kr

조 상 래

1996 Imperial College of Science, Technology and Medicine, 전산과(학사)
1997 Royal Holloway, University of London, 정보보호(석사)
1997. 10~1999 7 LG 종합기술원 연구원
1999~현재 한국전자통신연구원 정보보호연구단 디지털ID보안연구팀 연구원
관심분야 : ID관리시스템, I&AM, 인증, 인가, 정보보호
E-mail : sangrae@etri.re.kr

진 승 헌

1993. 2. 숭실대학교 전자계산학과(학사)
1995. 2. 숭실대학교 전자계산학과(석사)
2004. 2. 충남대학교 컴퓨터과학과(박사)
1996. 4. (주)대우통신 종합연구소 연구원
1999. 5. (주)삼성전자 통신연구소 전임연구원
1999. 6~현재 한국전자통신연구원 정보보호연구단 디지털ID보안연구팀 팀장
관심분야 : ID관리시스템, I&AM, PKI, Network Security, EC
E-mail : jinsh@etri.re.kr

노 봉 남

1978 전남대학교 수학교육과(학사)
1982 KAIST 전산학과(석사)
1994 전북대학교 전산과(박사)
1983~현재 전남대학교 전자컴퓨터공학부 교수
2000~정보통신부지원 시스템보안연구센터 소장
관심분야 : 컴퓨터와 네트워크 보안, 정보보호시스템, 전자상거래 보안, 사이버사회와 윤리
E-mail : bongnam@chonmam.ac.kr