

The Identity Web : 동향 및 보안 요구사항

조상래*, 진승헌**

한국전자통신연구원 디지털 ID 보안연구팀

The Identity Web : Trend and Security Requirement

Sangrae Cho*, Seunghun Jin**

Digital ID Research Team, ETRI

E-mail : *sangrae@etri.re.kr, **jinsh@etri.re.kr

Abstract

요구사항들이 필요한지 고려하여 본다.

실생활에서 나타나는 Social Network 을 웹에서 실현하기 위해서 Social Web 이 등장하고 그 전 단계로 Identity Web 이 현재 연구되고 있다. 그리고 웹의 확장으로 도메인간의 자유로운 데이터를 공유하기 위해서는 XML, XRI, XDI 가 제공되고 있다.. 본 논문은 Identity Web 을 실현하기 위한 기반 기술에 대하여 조사한 내용을 기술하고 이러한 인프라에서 자유로운 데이터의 공유를 하기 위해서는 어떠한 보안 요구사항들이 필요한지 고려하여 본다.

I. 서론

웹은 문서의 자유로운 공유를 위하여 개발되어 수많은 서비스를 인터넷에서 가능하게 하고 다양한 가치를 창조하고 있다. 하지만 실제 사람 또는 조직간의 원활한 네트워크를 지원하기 위해서는 웹 문서와 같이 데이터의 자유로운 공유가 필요하다. 'XRI/XDI 를 기반으로 하는 Identity Web 은 웹 아키텍처에 XML 문서의 연결을 사용하여 도메인간의 데이터 교환을 위한 새로운 추상적인 계층이다. 이러한 자유로운 데이터 공유는 향후 웹 응용 서비스에 굉장한 파급 효과를 가져올 것으로 예상되고 이에 대한 보안 요구사항도 아주 중요한 이슈로 충분한 검토가 필요하다.

본 논문은 Identity Web 을 실현하기 위한 기반 기술에 대하여 조사한 내용을 기술하고 이러한 인프라에서 자유로운 데이터의 공유를 하기 위해서는 어떠한 보안

II. Identity Web 동향

실생활에서 사회구성원들의 사회적 네트워크가 아주 다양한 형태로 구성되고 운영되듯이 웹에서 그러한 인간의 행동양식을 지원하기 위해서는 웹이 더욱더 진화하여 Social Web 이라는 형태로 발전되어야 하고 이러한 Social Web 을 이루기 위해서는 사용자들의 Identity - 즉 개인정보 - 가 자유롭게 공유될 수 있는 Identity Web 이 필요하다.

현재 웹에서 사용하고 있는 URI 는 지속성이나 재부여성은 결여가 되어서 자원이 이동하거나 내용이 변경되면 지속적인 식별성을 갖지 못하여 유지 관리가 쉽지 않다. 또한 다양한 Public Identifier 들의 사용은 이러한 식별자들이 사용자들을 바로 식별할 수 있을뿐더러 또 바로 연결도 가능하기 때문에 스팸과 같은 문제가 발생한다. 따라서 현재 OASIS 에서 추진하고 있는 XRI 라는 표준은 이러한 문제를 해결하고 지속적이고 재할당이 가능한 이름 식별체계를 지원한다.

웹이 문서의 자유로운 연결을 제공하기 위하여 HTML, URI, HTTP 를 제공하듯이 도메인간의 자유로운 데이터를 공유하기 위해서는 XML, XRI, XDI 가 제공되고 있다. 웹 문서가 HTTP Link 를 HTML 문서에 바로 사용하여 서로의 연결을 가능하게 하듯이 데이터 공유에서도 XDI Data Link 라는 기술을 이용하여 XML 문서에서 필요한 데이터를 다른 도메인의 XML 문서와 Link contract 을 맺어 공유할 수 있다.

¹ XRI - Extensible Resource Identifier
XDI - XRI Data Interchange

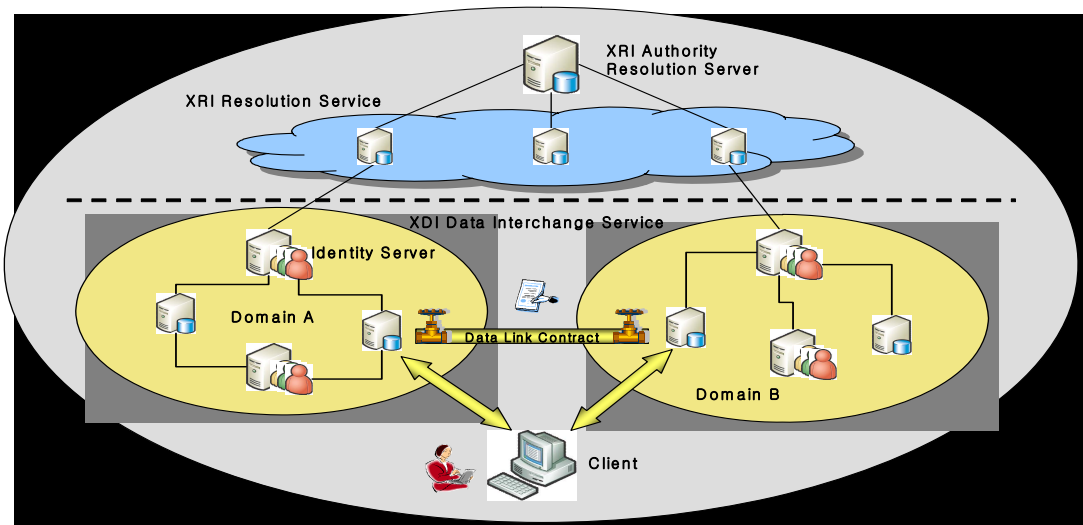


그림 1 The Identity Web 개념도

The Identity Web 은 1998 년 OneName 이라는 회사에서 XNS (Extensible Name Service)라는 프로젝트로 시작했다. 2000 년에 XNSORG 조직을 결성하고 2002 년에 XNSORG 는 XNS 를 OASIS 에 표준 상정하였다. OASIS 에서 XNS 는 XRI 와 XDI 로 나누어서 진행하고 있다.

III. Security Requirement

그림 1 의 Identity Web 에서는 사용자의 개인정보가 수많은 사이트와 교환되기 때문에 프라이버시와 보안 문제가 아주 심각하다. 현재 XDI 에는 Link Contract 이라고 하는 연결을 제공하여 쌍방의 합의하에 연결을 맺어 정보를 공유할 수 있다. 이때 계약을 맺기 전에 쌍방을 먼저 확인하는 인증이 수행되어야 한다. 인증은 Identity Web 에서 모든 프로세스의 시작이다. 인증과 더불어 SSO 서비스도 중요한 보안 요소 중 하나이다.

프라이버시 보호는 Identity Web 에서 가장 중요한 요소 기술로 XDI Link Contract 의 Permissions 부분에 기본적인 기능을 제공하고 있다. 실제 기능을 제공하기 위해서는 사용자가 편리하게 이해할 수 있는 프라이버시 정책 설정 기능이 필요하고 전체 프라이버시 정책을 관리할 수 있는 프레임워크도 중요하다. 또한 XRI 의 경우 식별자를 사용자의 실제 식별자(예: 이메일)로 전환하는 과정에서 프라이버시 기술을 이용하여 스팸을 방지할 수 있다.

각각의 XML 문서는 Identity 웹서버를 통하여 교환되는데 이때 인가는 누가 어떤 접근제어 권한을 가지고

데이터를 접근하지 통제할 수 있다. 인가 기술은 가장 기초적인 ACL 에서부터 RBAC 에 이르기 까지 다양한 접근제어 정책을 적용할 수 있다.

Identity Web 이 기존의 웹 기술을 그대로 사용하기 때문에 SSL 과 같은 채널 보안은 그대로 사용하며 XML 문서 자체의 기밀성과 무결성은 PKI 의 인증서를 사용하여 암호화 및 전자서명을 XML 문서에 적용하여 해결한다.

IV. 결론 및 향후 연구 방향

본 논문에서는 XRI/XDI 의 현재 동향에 대하여 고찰하여 보았고 향후에 실제 사용될 때 필요한 보안요구 사항들을 고려하여 보았다. 실제 XRI/XDI 가 인터넷에서 널리 쓰이기 위해서는 이러한 보안요구사항들을 만족하는 것이 중요한 조건이 될 것이다.

참고문헌

- [1] D. Reed, D. McAlpin, An Introduction to XRIs, <http://docs.oasis-open.org/xri/xri/V2.0/xri-intro-wd-04.pdf>, March 2005.
- [2] D. Reed, G. Strongin, The Dataweb: An Introduction to XDI, <http://www.oasis-open.org/committees/download.php/6434/wd-xdi-intro-white-paper-2004-04-12.pdf>, March 2005.