공인 Web SSO 도입 방안에 대한 연구

최대선, 김태성, 진승헌
한국전자통신연구원
{sunchoi, taesung, jinsh}@etri.re.kr

Research for Implementation of Licensed Web SSO

Daeseon Choi, Taesung Kim, Seunghun Jin
Electronics and Telecommunications Research Institute

요 약

본 논문은 국내 인터넷 환경에 Web SSO를 도입하는 방안에 대한 연구를 담고 있다. ID관리의 문제점으로 인해 Web SSO가 필요한 실정을 분석하고 현존하는 Web SSO 기술 검토하여 이중 Liberty 방식을 채택한다. Liberty 방식의 Web SSO 구축 방안을 제안한 후 실제 사용되기 위해서 해결해야 할 기술적 검토사항을 분석하고 이에 대한 해결 방안으로 공인 IDP 체계를 제시한다. 실제 공인 Web SSO 구축을 위해 필요한 시스템 구성도 제안한다.

1. 서론

일반적인 인터넷 사용자는 웹사이트마다 반복되는 등록 절차를 매우 번거롭게 생각하고 있다. 여러 군데 등록해 두었기 때문에 주소 변경 등도 여러 군데에서 수행해야 한다. 또한 각 사이트의 ID와 패스워드를 암기하는 것도 매우 어렵기 때문에 보통 동일 ID와 패스워드를 사용하거나 패스워드를 메모해 두게 되는데 이는 보안상 큰 문제가 아닐 수 없다[1]. 본 논문에서는 이러한 문제를 해결하기 위한 Web SSO를 국내 인터넷 환경에 광범위 도입하는 방안에 대해 기술한다.

2. Web SSO

Web SSO란 한번의 등록 후, 하나의 ID와 PW로 한번의 로그인을 통해 모든 사이트의 서비스들을 이용할 수 있도록 해주는 서비스와 기술 방식을 말한다[6]. 일반적인 Web SSO는 SSO서버를 통해 인증한 다음, SSO 가입 웹사이트 접근 시, 별도의 인증 절차를 거치지 않는 방식으로 구성된다.

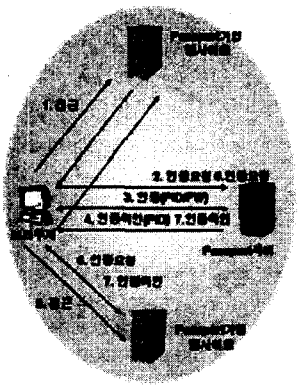
이러한 Web SSO가 대규모로 보급되어 이용되기 위해서는 다음과 같은 요구 사항을 충족시켜야 한다[7].

1. 다양한 인증 방법: Site의 요구에 따라 다른 인증 방법 사용 가능
2. 공인인증서를 사용한 인증 가능
3. 유무선 환경에 모두 적용 가능
4. Web SSO 서비스 제공자의 신뢰성 보장
5. 복수의 SSO서비스 제공자 가능
6. 사용자와 Web Site의 자유로운 SSO서비스 제공자 선택
7. SSO서비스 제공자간의 연동가능

3. 현존 Web SSO 기술

2장에서 나열한 요구사항을 염두에 두고 현존하는 Web SSO의 기술의 대표주자인 Microsoft의 Passport서비스와 Liberty Alliance의 Liberty 규격을 살펴보기로 한다.

[그림 1]는 Passport서비스의 동작 방식을 보여준다.

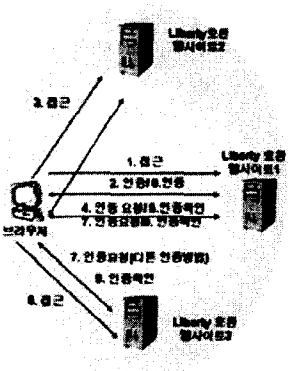


[그림 1] Passport 방식

Passport의 동작 순서는 다음과 같다[4].

1. 웹사이트 접근
2. Passport 서버로 Redirect 하여 인증 요청
3. Passport 서버에 PID(Passport ID)와 PW로 인증
4. Passport 서버에서 인증확인서 발급 후 웹사이트로 Redirect
5. 다른 웹사이트로 접근
6. Passport 서버로 Redirect 하여 인증 요청
7. 기 인증 되었으므로 인증확인서 발급 후 웹사이트로 Redirect

Passport 서버가 존재하고 실제 서비스를 제공하는 점과 달리 Liberty는 규격을 의미하며 현재 해당 서비스를 제공하고 있지 않다. [그림 2]은 Liberty방식의 WebSSO 동작 방식을 보여준다[2].



[그림 2] Liberty 방식

Liberty 방식의 동작흐름은 다음과 같다.

1. 웹사이트1(IDP, Identity provider)접근
2. 인증
3. 웹사이트2 접근
4. 최초 웹사이트1로 Redirect 하여 인증 요청
5. 인증 확인서 발급 후 웹사이트2로 Redirect
6. 웹사이트 3 접근
7. 웹사이트1로 Redirect 하여 인증 요청(다른 인증방법)
8. 다른 인증방법으로 인증
9. 인증확인서 발급 후 웹사이트 3으로 Redirect

[표 1]에서는 앞서 언급한 WebSSO의 요구 사항에 따른 두 방식의 비교가 기술된다. 공인인증 등 다양한 인증 방법과 여러 환경에서 사용 가능한 점, SSO 제공 기관을 다각화할 수 있다는 점 등을 고려해 볼 때 Liberty 방식이 적합한 것으로 판단된다.

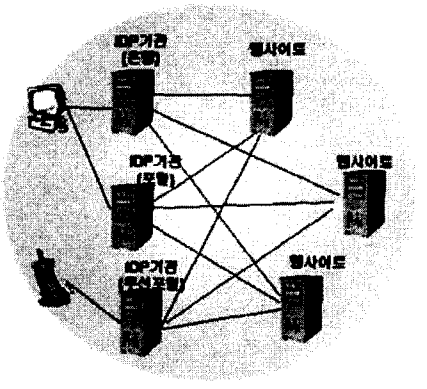
[표 1] Passport와 Liberty 비교

	Passport	Liberty
다양한 인증방법	패스워드	웹사이트에 요구에 따른 다양한 방법 (공인인증가능)
다양한 환경	유선 웹 환경	유선 웹 환경 무선 웹 환경(WML) 웹이외의 환경
SSO제공자	단일 제공자 Microsoft	1. 웹사이트 중 희망자 Ex)포털, 인증기관 등 2. 신설 가능
가입자	Microsoft Passport 서비스 가입	기 가입 웹사이트의 IDP화 신설 IDP에 가입

4. Liberty 방식 Web SSO 구축

4.1 기본구조

[그림 3]는 본 논문에서 제안하는 Liberty 방식의 Web SSO의 기본구조를 보여준다.



[그림 3] Liberty 방식의 Web SSO 기본 구조

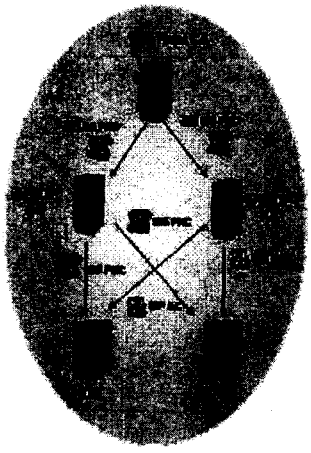
은행, 포털, SSO 전담 서비스 기관 등 복수의 SSO 제공기관이 존재하여 가입자들은 원하는 IDP 이용할 수 있다 . 모든 IDP와 모든 가입 웹사이트가 연동하는 Fully Connected 방식이 사용된다[3]. 이는 단일 Circle of Trust을 구성한다는 의미가 된다. 이러한 IDP에서 기존에 등록/존재하던 ID 사용하게 되며 IDP는 공인 인증을 포함한 다양한 인증 방법을 지원한다.

4.2 신뢰관리

이러한 구조의 WebSSO를 구성함에 있어 해결해야 할 문제 중 하나가 신뢰(혹은 서비스 관계)관리이다. 이는 IDP와 웹사이트 간의 관계 관리를 의미하며 웹사이트에서 신뢰할 IDP 목록 관리와 IDP에서(과금 등을 위해) 가

입 웹사이트 관리로 구분될 수 있다. 한편 상호 업무 규정, 메커니즘, 프로파일 등의 표준화 도 IDP와 웹사이트 간 규정되어야 하는 요소이다.

그런데 Fully connected IDP-웹사이트 구조에서는 관계의 수가 N^2 이므로 개별 사이트에서의 Static한 관계 관리가 현실적으로 불가능하다. 이러한 문제를 해결하기 위해 본 논문에서는 공인 IDP구조를 제안한다. [그림 4]는 공인 IDP구조를 보여준다.



[그림 4] 공인 IDP구조

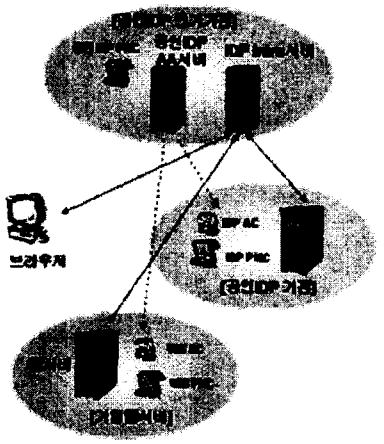
공인 IDP 구조에서는 IDP 기관을 인가하는 기관인 공인 IDP 인가 기관(Attribute Authority)이 IDP AC(Attribute Certificate)을 발행한다. 여기서 IDP AC는 IDP 자격을 공인하는 인증서로 사용된다. 또한 WS(Web site) 인가를 위해서 공인 IDP AA에서 IDP 이용을 위한 ticket을 발행하고 WS는 이를 구매해서 사용하게 된다.

공인 IDP 구조의 동작은 다음과 같은 방식으로 진행된다.

- IDP -> 웹사이트: IDP의 PKC와 AC를 이용해 인증 및 IDP 인가 여부 확인
- 웹사이트 -> IDP: WS AC를 제출해 사용권한 인가 및 과금, AC의 소유 증명은 PKC사용

4.3 시스템 구조

공인 IDP 구조를 사용한 WebSSO 시스템 전체 구조는 [그림 5]과 같다. 공인 IDP인가 기관은 별도 신설 기관이나 기존 공인 인증기관이 된다. 여기에는 Common Domain Service[3]를 제공하는 Intro 서버가 존재한다. 공인 IDP인가 기관에서 IDP AC를 발급받은 공인 IDP 기관은 포털, 은행 등 기존 고객 다수 보유 웹사이트이고 공인인증서 방식의 인증을 지원하며, 기존 웹 서비스에 IDP SDK추가하는 방식으로 구성된다. 가입 웹 서버는 기존 웹 서비스에 SP(Service Provider) SDK추가하여 구성되고 공인인증서 검증이 가능(신뢰)하여야 한다.



[그림 5] 공인 Web SSO시스템 구조

5. 결론

본 논문에서는 Web SSO 필요성, Passport, Liberty 기술 검토를 했고 Liberty 기반 Web SSO 체계 구축방안을 제시하였다. 이를 위해 신뢰관리라는 문제를 검토하여 해결방법으로 공인 IDP구조를 제안하였다. 이러한 공인 WebSSO가 사용되기 위해 필요한 정책은 IDP를 통한 SSO의 공인인증 법적 효력 인정이다.

참고문헌

[1] Daeseon Choi, Sangrae Cho, Seunghun Jin, Kyoil Chung, "An Information Security Model for the Next Generation Application Service", IWAP2002 , Taiwan, October 2002

[2] Liberty Alliance, "Liberty Architecture Overview", July 2002

[3] Liberty Alliance, "Liberty Architecture Implementation Guidelines", July 2002

[4] Microsoft, "Microsoft .Net Passport Security and Privacy Overview", October 2001

[5] Microsoft, " Security in a Web Services World: A Proposed Architecture and Roadmap", April 2002

[6] 최대선, 진승헌, 정교일, "통합 어플리케이션 정보보호 기반구조", 정보보호학회지, 2002 년 10 월

[7] 최대선, 김태성, 조상래, 진승헌, "차세대 어플리케이션 서비스를 위한 정보보호 모델", 정보보호학술 발표회 논문집, 2002 년 7 월