Identity 정보 공유를 위한 Web Service Framework

조영섭*, 진승헌**
한국전자통신연구원 디지털 ID 보안연구팀

Web Service Framework for Identity Information Sharing

Yeongsub Cho*, Seunghun Jin**
Digital ID Research Team, ETRI
E-mail : *yscho@etri.re.kr, **jinsh@etri.re.kr

Abstract

일반적으로 사용자가 인터넷 서비스를 제공받기 위해서는 자신의 정보를 먼저 등록해야 한다. 그러나 인터넷 서비스의 활용이 많아질수록 이와 같이 선 등록되어야 하는 정보의 양도 많아지며 또한 이들 정보가 불일치하는 문제가 발생한다. 본 논문은 이와 같은 문제를 해결하기 위해 사용자 Identity 정보를 웹 상에서 공유하는 기술인 Liberty Alliance 의 ID-WSF(Identity Web Service Framework)에 대하여 기술한다.

I. 서론

사용자는 인터넷 서비스를 제공받기 위해서는 인터넷 서비스 제공자에게 자신의 신상정보인 Identity 정보를 등록하는 것이 일반적이다. 그러나 이와 같이 서비스 제공자마다 매번 사용자 정보를 등록하는 것은 사용자의 편의성을 저하시키고 사용자 Identity 정보의 불일치 문제를 발생시킨다. 또한 서비스 제공자의 신뢰도가 낮은 곳에서 사용자 정보가 등록되기 때문에 사용자 프라이버시 침해 가능성이 높아지는 문제가 발생한다. 최근 이와 같은 문제를 해결하기 위해 사용자 Identity 정보를 웹 서비스 형태로 공유하는 방식에 대한 연구가 진행되고 있다. 본 논문은 사용자의 Identity 정보를 표준화된 웹 서비스로 제공하는 Liberty Alliance 의 ID-WSF(Identity Web Service Framework)에 대하여 고찰한다.

II. ID-WSF

사용자의 Identity 정보를 웹 상에서 공유할 수 있도록 하는 대표적인 표준이 Liberty Alliance 에서 제정한 Liberty Module 들이다. 다음 그림 1 은 Liberty Alliance 의 표준 모듈을 도식화 한 것이다.

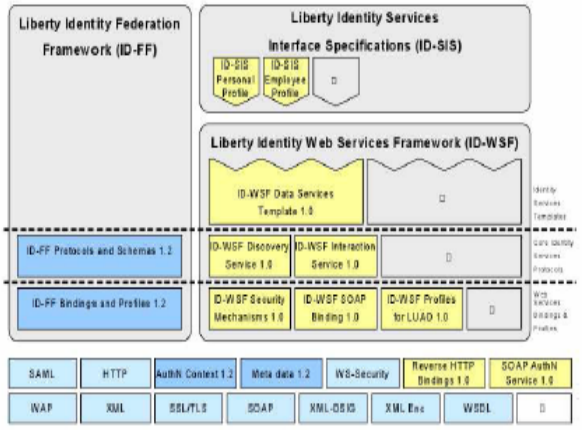

그림 1 Liberty Modules

그림에서 ID-FF 는 Federated Identity 관리와 인터넷 SSO 에 대한 표준을 규정하고 있으며 현재 SAML v2.0 으로 통합되었다. ID-SIS 는 Identity Service 의 표준 규격을 정의하고 있는 것으로 사용자 개인 프로파일 정보와 조직내의 프로파일 정보를 나타내는 Personal Profile 와 Employ Profile 이 규정되어 있으며, 현재 위치 정보인 Geolocation 등이 지속적으로 표준으로 제공되고 있다.

ID-WSF 는 다음과 같은 스펙들로 구성된다. DS(Discovery Service)는 사용자 정보를 공유하려는 WSP 가 자신이 어떠한 사용자에 대하여 어떠한 서비스를 제공할 것인지에 대한 정보를 discovery server 에 등록할 수 있도록 한다. 또한 WSC 가 사용자에 대한 정보를

제공하는 WSP 를 discovery server 에서 검색할 수 있도록 하는 기능을 제공한다. IS(Interaction Service)는 WSP 가 WSC 에서 요청한 사용자 정보를 제공할 때, 사용자의 동의가 필요한 경우, 사용자 동의를 얻을 수 있도록 하는 기능을 제공한다. Security Mechanism 은 ID-WSF 메시지를 교환하는 WSP, WSC, discovery server, interaction server 사이에 보안 기능을 제공한다. 보안 기능은 메시지 수준의 보안과 통신 레이어 수준의 보안 두 가지가 제공된다. SB(SOAP Binding)는 ID-WSF 메시지를 SOAP 으로 바인딩하여 웹 서비스가 제공될 수 있도록 하는 기능을 제공한다. SOAP 메시지를 구성할 때, SOAP 의 헤더에 ID-WSF 메시지간의 상호 연관성을 나타내는 <Correlation> 헤더 블록은 필수적이며 ID-WSF 메시지를 송신하는 송신자를 나타내는 <ProviderID> 헤더 블록을 가능하면 제공한다.

DST 는 ID-SIS 에서 공통적으로 요구되는 Query, QueryResponse, Modify, ModifyResponse 등의 메시지의 스키마와 프로토콜을 규정한다. ID-SIS 는 DST 스키마를 포함하여 기본적인 질의, 변경, 응답 메시지를 구성한다

Profiles for LUAD 프로파일은 서버 형태가 아닌 mobile device, personal computer 등에서 ID-WSF 메시지를 송신하고 수신할 수 있도록 하는 프로파일이다. 이외에도 웹 서버를 운용할 수 없는 곳을 위한 Reverse HTTP Binding 1.0 이 있으며, mobile device 에 인증 기능을 제공하기 위한 SOAP AuthN Service 가 제공된다.

Ⅲ. ID-WSF 스키마

본 장은 ID-WSF 스펙의 여러 메시지 중에서 가장 기본이 되는 메시지인 DS Modify 메시지 스키마에 대하여 기술한다.

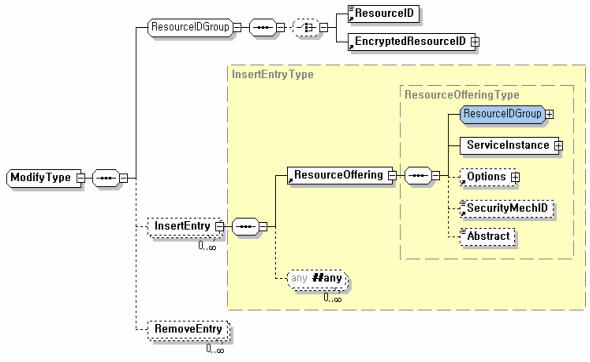

그림 2 DS Modify 메시지 스키마

<ResourceIDGroup>은 WSC 가 얻고자 하는 정보의 대상, 즉 사용자 또는 자원의 ID 를 나타낸다. 이것은 Plain Text 로 전달되거나 또는 암호화하여 전달될 수 있다.

<InsertEntry>는 WSP 가 공유하려는 사용자의 Identity 정보와 서비스 위치를 나타낸다. ResourceOffering 내의 ResourceIDGroup 은 서비스 대상이 되는 사용자 ID 를 나타내며, ServiceInstance 는 WSP 의 서비스 위치를 나타낸다. Options 는 서비스 대상의 제약 등 선택적인 사항을 나타내며, SecurityMechID 는 WSP 가 서비스 수행시 요구하는 보안 메커니즘을 나타낸다. Abstract 는 ResourceOffering 에 대한 설명문이다.

<RemoveEntry>는 DS 에 등록된 ResourceOffering 을 삭제할 때 사용하는 요소이다.

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 사용자 Identity 정보를 표준화된 웹 서비스로 제공하여 서로 공유할 수 있도록 하는 Web Service Framework 기술에 대하여 고찰하였다. 이 기술은 Identity 정보의 공유가 더욱 중요해짐에 따라 많이 활용되리라 예상된다. 현재 Liberty ID-WSF 는 하나의 도메인에 최적화되어 있는 기술로, 향후 여러 도메인에서 효율적으로 이 기술이 적용될 수 있도록 하는 연구가 필요하다.

참고문헌

[1] Liberty ID-WSF Data Services Template Specification v2.0-06, Liberty Alliance, http://projectliberty.org,

[2] Liberty ID-WSF Discovery Service Specification v2.0-02, Liberty Alliance, http://projectliberty.org,

[3] Liberty ID-WSF Implementation Guide v2.0-01, Liberty Alliance, http://projectliberty.org,

[4] Liberty ID-WSF SOAP Binding Specification v2.0-01, Liberty Alliance, http://projectliberty.org,

[5] Liberty ID-WSF Web Service Framework Overview, Liberty Alliance, http://projectliberty.org,

[6] 한국전자통신연구원, "인터넷 ID 관리 서비스 기술백서 v2.0", 2005