Contribution ID: **50** Type: **not specified**

Design and Implementation of Portal System for Subscribed Cloud Services in Identity Federation

Tuesday, March 7, 2017 4:30 PM (30 minutes)

With growing number of online services, identity federation is rapidly spreading, especially in the academic world. Identity federations have been established in many countries. In Japan, an academic identity federation called “GakuNin” is operated since 2010.
In identity federation, IdP can provide information about a user as attributes in addition to the authentication-related information. An SP can request attributes about a user from an IdP and then utilize those attributes to authorize users and provide services. In general, an IdP releases attributes they derived from authoritative source systems within the organization. Although academic society affiliations or research community membership across universities are user data that would often be interesting for academic services, a typical campus identity management system is not designed to manage such data, and the IdP is thus unable to provide it to services. Some of the advanced academic federations are beginning to make available attributes like this, especially related to the membership of a group that spans multiple organizations, by means of the Attribute Provider (AP). The SP is typically responsible for aggregation of additional attributes from APs after the initial exchange with the IdP. A unique user identifier is supplied by the IdP to the SP and is shared with APs in order to look up additional attributes of that user.
An IdP usually joins one federation and is connected to some services such as organization-specific services provided by the organization. If users in the IdP could use all the services joining the federation, they could easily recognize usable services through their credentials of the IdP. But the reality is not the case, for example, because the organization does not subscribe a service, or the IdP is not configured to send attributes to the service correctly, and so on. Users must access each service that joins the federation in order to make sure that they can use the service. It is not realistic especially if the federation has a lot of services.
Furthermore, adding AP makes this problem more complex. The AP must know user identifiers in advance to identify themselves, usually by means of attributes from IdPs. Some SPs must also receive specific attribute values from an AP for authorization, which is uncertain for ordinary users.
We propose a portal system for each stake holder to register some information. With this information it displays his / her usable services for any accessing user. For example, IdP operators register SPs configured on their IdPs, and SP operators register their strategies for authorization. APs provides membership information of the user.
We do an elementary evaluation about our system, which calculates availability of some complicated SPs by some conditioned users.
We will present a demo of this system working in our production federation.

Primary author: Mr NISHIMURA, Takeshi (Project Researcher)

Co-authors: Dr SAKANE, Eisaku (National Institute of Informatics); Dr AIDA, Kento (National Institute of Informatics)

Presenter: Mr NISHIMURA, Takeshi (Project Researcher)

Session Classification: VRE

Track Classification: Virtual Research Environment (including Middleware, tools, services, workflow, … etc.)