Federated Identity Management

Mohammad Jabed Morshed Chowdhury

Today, we see federated identity everywhere, most noticeably in what we call 'single sign on.' With single sign on, you can log into your GMail and then open up YouTube in a different tab, for instance, and you'll stay logged in. The underneath mechanism that makes this possible is called Federated Identity Management (FIM).

Federated Identity Management is a model that enables companies with several different technologies, standards and use-cases to share their applications by allowing individuals to use the same login credentials or other personal identification information across security domains. The main purpose of federated identity management is to allow registered users of a certain domain to access information from other domains in a smooth way without having to provide any extra administrative user information.

The growth in identity management challenges, specifically cross-company, cross-domain issues, has led to the evolution of a new approach to identity known as federated identity management. As a system, FIM allows individuals to sign on to the networks of different enterprises using their personal identification information or login credentials to access data. The partners in an FIM system are responsible for authenticating their respective users and for vouching for their access to the networks. Federation is achieved using open industry standards or openly published specifications in order to enable multiple users to access common use cases.

A company must always trust its partners to vouch for their users, in this situation, Security Assertion Markup Language (SAML) may be used. SAML instantly recognizes whether a prospective user is a machine or a person and also defines the access that a particular machine or person can have. Federated identity management allows companies to share applications, regardless of the need to adopt the same technologies for authentication, directory services and security. One the biggest advantage of FIM is that it allows companies to have their own directories and also safely exchange data. The use of identity federation standards can help to minimize costs by eliminating the need to develop proprietary solutions. Organizations need to identify and authenticate users only once, which increases security and lower the risks associated with authentication of identity information several different times. The FIM also contributes toward improving privacy compliance by effectively controlling user access to information sharing. The end-user experience can also be improved by eliminating the need for new account registration.

Different between Federation and Single Sign-on

Single Sign-on (SSO) allows users to access multiple services with a single login. The term is actually a little ambiguous. Sometimes it's used to mean that (1) the user only has to provide credentials a single time per session, and then gains access to multiple services without having to sign in again during that session. But sometimes it's used to mean (2) merely that the same credentials are used for multiple services; the user might have to login multiple times, but it's always the same credentials. So beware, all SSO's are not the same in that regard. Many people (me included) only consider the first case to be "true" SSO.

Federated Identity (FID) refers to where the user stores their credentials. Alternatively, FID can be viewed as a way to connect Identity Management systems together. In FID, a user's credentials are always stored with the 'home' organization (the 'identity provider'). When the user logs into a service, instead of providing credentials to the service provider, the service provider trusts the identity provider to validate the credentials. So the user never provides credentials directly to anybody but the identity provider.

FID and SSO are different, but are very often used together. Most FID systems provide some kind of SSO. And many SSO systems are implemented under-the-hood as FID. But they don't have to be done that way; FID and SSO can be completely separate too.

Technologies of Federated Identity

Technologies used for federated identity include SAML (Security Assertion Markup Language), OAuth, OpenID, Security Tokens (Simple Web Tokens, JSON Web Tokens, and SAML assertions), Web Service Specifications, Microsoft Azure Cloud Services, and Windows Identity Foundation.

Digital identity platforms that allow users to log onto third-party websites, applications, mobile devices and gaming systems with their existing identity, i.e. enable social login, include:

Microsoft account – Formerly Windows Live ID

- Google Account
- Yahoo!
- Twitter
- LinkedIn
- PayPal
- Foursquare
- My Space

Conclusion

Use of identity federation standards can reduce cost by eliminating the need to scale one-off or proprietary solutions. It can increase security and lower risk by enabling an organization to identify and authenticate a user once, and then use that identity information across multiple systems, including external partner websites. It can improve privacy compliance by allowing the user to control what information is shared, or by limiting the amount of information shared. And lastly, it can drastically improve the end-user experience by eliminating the need for new account registration through automatic "federated provisioning" or the need to redundantly login through cross-domain single sign-on.

Federation among different universities in Bangladesh may lead to the information and research work sharing. Different universities should take the lead to come together so that everybody can be benefited by the resource of other partner universities ■