Social Identities

Social Identities

In the past, applications owners would add a "new user registration" process to their site, and would issue userids and passwords to these "outsiders". This created a burden for both sides -- the user would have to remember yet another set of credentials, and the site would have to institute business processes to deal with forgotten passwords, etc.

A growing number of these applications, though, are looking to "outsource" the identity problem by leveraging the authentication and Web Single SignOn (SSO) functionality provided by the big internet identity providers (e.g., google, yahoo, facbook, etc). The outside users of these sites now authenticate at one of those sites, and those sites provide the local application with information about the browser user.

Since the mid-1990s commercial Internet-based Service Providers have allowed people visiting their sites to "sign up" and obtain an account. Almost always these accounts have the user supplying a userid (which must be unique within the site) and a password (which sometimes must meet certain strength requirements). Sometimes the userid is actually the user's email address at some other site. Oftentimes, the site asked the user to provide other information as part of their "profile". Several of these items would usually be classified as PII (eg name).

In the mid-90's, investors thought that attracting large numbers of people to create local accounts was a sign that a site was prospering and succeeding. Over time, though, users began to push back on creating so many accounts. In addition, protocols began to emerge to support Web Single SignOn across a multitude of commercial Service Provider sites. This reduced the number of places where a user would have to maintain an "account". In recent years, a handful of large sites have come to hold the vast majority of user accounts (ie google, yahoo, twitter, msoft?, other). Taken together, these sites are often described as providers of "social identities". These sites are currently using a variety of proprietary protocols (and variations of OpenID) to provide SSO functionality. The consensus is that it is extremely unlikely the social identity providers would agree to issue SAML Assertions to SAML SPs.

One significant difference between enterprise identities and social identities is that enterprise identities have been through a business process to ensure that the Credential is given to the physical person with whom the account is associated. Social Identities do not currently have an equivalent process. Users go to these sites and create accounts, and then self-assert profile information (eg a name). Consequently, social identities are not currently viewed as having a sufficiently high Level of Assurance to allow them to be used for business transactions where account information is linked to a person's name or real world identity. They can be used for business transactions when all the information needed to complete the transaction is entered by the person (eg a credit card number and validating information). They cannot be used for business transactions when a browser user is claiming to be a specific individual (eg accessing a government services site).

In the future, there may be processes provided by third parties to verify the real world identity of a person using a social identity.

See TN - Protocols Used by Social Identities for detailed information about the protocols used by Social Identity sites.