Issues for Management

Issues for Management

Campuses are seeing a growing number of situations where application owners want their site to be used by authenticated users who cannot be authenticated by the home campus. There is a broad range of use cases and requirements in these situations; GenericUseCases provides descriptions of many of these. Some of the key issues that must be considered when an application owner (and, the campus IT organization, if they are involved) include:

1. Will most of the usage be by campus members, or by people from outside the campus ?
2. How important is it that information about a person's "real identity" be available? If a person edits content at the site, how confident do others want to be about the real identity of the editor ?
3. Does the site want to grant more permissions to an identity that is thought to have a higher LoA ?
4. Does the campus want to "remember" social identities that are being used to access sites on the campus ? Or is the campus comfortable with delegating this decision to individual sites?

Often, at the outset, the answers to these questions are not clear or obvious. And, often, the answers will evolve over time. And, as campuses move toward outsourcing some of their core services (eg email to Google or Microsoft), depending on how the campus chose to handle identity and authentication, it may be easier to rely on SSO provided by the outsourced provider than on SSO provided by the campus infrastructure. Lastly, an application site based in an academic department may have different answers to these questions than the central IT organization at that same campus.

(These notes assume that a site needs to support access via local, Federated, and social identities. The target audience for these notes is management in the campus central IT department.)

Comparison of Enterprise and Social Identities

Campuses issue digital identities to members of their core communities (faculty, students, staff); recently, they are also issuing credentials to communities that have "some" relationship to the campus, but a weaker relationship than members of the core community. The business processes supporting credential issuance to members of the core community require the person to prove their legal identity, and then associate that identity with a digital identity (a process known as "identity proofing"). As a result, the campus trusts that when some authenticates to a system using Jane Doe's credentials that it MUST have been Jane that performed this action. If misuse occurs during a session that was initiated with Jane's credentials, then Jane is held responsible. However, because many of the people now receiving credentials are remote from the campus, these assumptions do not apply to them.

In recent years, campuses have begun to leverage Federated Identity, and the InCommon Federation, in order to allow people from other campuses to access local applications and collaboration sites. The Federated Identity approach allows a campus to leverage the identity proofing processes used at other campuses. Event though the user is authenticating at a different site, the local campus trusts that the other campus has done an effective job of identity proofing before issuing digital credentials to people.

More recently, more and more application owners want their sites used by people from outside of the Higher Education environment. This group of applications ranges from the expected submitting comments on a blog to participating in a wiki supporting a research project to real business applications (e.g., a student giving their parents access to the student bill). Many of these sites are looking to have these outside users authenticate at the big internet identity providers. This effectively offloads most of the burden of supporting these accounts to the identity provider. The cost of providing this support is often non-trivial, so this represents a big win for the application owner.

However, currently no organization provides any sort of identity proofing process for these accounts. Though many people use their name or nickname as their account name at these providers, there is no requirement that people follow this informal convention. Nor is there a process that prevents someone from using another person's name or nickname. Consequently, there is no way of automatically obtaining trust about the identity of a holder of a social account.

Some applications attempt to raise their confidence level about the true identity of the social account holder by using out-of-band approaches. Talking to the person and asking then to share their social identity is a popular approach. This has the obvious drawback that the application owner must know the outsider in order to ask this question. Other sites include a signup or apply page; the site owner reviews an application, perhaps contacts the applicant, and decides whether to grant admittance and which privileges to grant. In this case, the application owner has no recourse beyond revoking privileges if the applicant begins to behave badly. A third approach is to allow current members to use the application to send invitations to social identities; the social account holder clicks a url in the email message in order to join the site and gain privileges. This approach is useful when the current member is allowed to share access to specific information with other parties (e.g., a student giving their parents online access to a student bill). The campus does not care who the student shares the bill with; that is the student's responsibility. The campus does not need to know the real identity of the social account holder.

> ⚠ In our call of 28 March Dedre said she might draft some "language differentiating social loa 1 from campus loa 1" ... if memory serves, Heather was also interested in contributing to this. While the text above this note describes how the processes for proofing identity differs between social and campus identities, the way I recall this call suggested that Dedre had in mind something that was grounded in use cases – like the several enumerated in the prior paragraph, but perhaps more elaborately illustrated. If this draft is floating around somewhere, and its focus is what I'm imagining/recalling, might it be the bones of a section describing risks of using social identity providers? (~Steve Masover, 27 Aug 2011)

--- what are the risks of using social identities

Possible Deployment Models

Several possible deployment models are possible, depending on the level of use, the amount of risk that the application owner and site are willing to accept, and the need to maintain a longer term relationship with the social identity holder. This list is ordered from simplest to more complex.

> ⚠ Isn't it true that the ordering here -- "simplest to most complex" -- is from a campus central IT perspective? It is true that this is the declared audience of this page, but perhaps a more nuanced presentation would be helpful here. What's simplest for central IT (#1) is hands down most difficult for an application / site owner. (~Steve Masover, 27 Aug 2011)

1. The application owner deploys a Social to SAML gateway as part of their site. The site owner is responsible for all the work and configuration. There is no involvement by campus central IT.
2. The application owner uses a Social to SAML gateway operated by some other party, outside of the campus.
3. Campus central IT deploys a shared Social to SAML gateway. An application on the campus is allowed to leverage the gateway.
4. Campus central IT deploys a shared Social to SAML gateway, and elects to "remember" all of the social identities that cross the gateway.

Implementation Process

(for each option, guesstimate the level of effort and required skills)

-- existing open source implementations

-- existing commercial implementations

-- issues for the "build it locally" approach

-- comparison of enterprise and social identities
  -- pro's, con's and risks of the two approaches
  -- quick description of possible deployment models
  -- where to get the pieces (buy, open source, build)
  -- how much effort
  -- what are the risks of doing this ?

  -- other topics ?