GenericUseCases

This page is being used to collect GENERIC Use Cases. Per the usual policy on this wiki, any authenticated user should be able to edit this page.

A set of use cases has been submitted that describe campus central IT adding "social identity people" to the central person registry (and perhaps associating multiple sets of credentials with an individual); a separate set of use cases has been submitted which include no role for central IT or for "remembering" anything about the person using social credentials. Both models seem to have significant numbers of people interested in them. Consequently, both models are likely to be deployed, with campuses choosing a model appropriate to the problem they are trying to solve.

Link to contributed use cases page

Basic Use Case -- short term guest access. Jane Doe attempts to access Service X at campus Y, because she is working on a project with John Smith (a faculty member at campus Y). The service requires that she authenticate; she navigates through the Discovery Service and uses her google/yahoo /facebook account to authenticate, and is returned to Service X. Jane now has the baseline set of permissions at Service X. Later, John gives Jane access to the document they are working on together.

Variant one -- **short term guest access, email invite, pre-provisioned with certain specific rights**. (CMU) Student Jane logs into the local student system, and navigates to area X. She decides to give her parents access to this area. She enters one parent's email address. The system sends an email to that address; it contains a url with a token. The parent reads the email, clicks the url, is taken to a service on the campus. Because there is no existing session, the parent is redirected to a Discovery Service. They select their social service as their IDP, are redirected there, authenticate, and are redirected back to the campus. This time,they have a session, and consequently are granted access to Jane's instance of area X.

Variant Two (extending variant one); after authentication the user is taken to a central point of some sort (eg a Gateway); the first time there the user is taken to a Registration App and the user self asserts profile info. (need some sort of person registry. The GW constructs an EPPN value...)

Variant Three -- (extending variant two); some attributes are populated using values asserted by authentication service. (I'm not sure this is really any different than self-asserted...)

Basic Use Case 2 -- short term guest access. John Smith (a faculty member at campus Y) is working on a project with Jane Doe; they are using a wiki service to support their collaborative work. John goes to the wiki space, and grants Jane's OpenID value R/W access to the space. Later, Jane accesses the wiki, authenticates using her OpenID associated account, and gains access to their shared work space.

Basic Use Case 3 -- (web finger) John Smith is working with a group of 50 other researchers. He has email addresses for all of them; most of the email addresses are based at gmail and yahoo. He maps the email addresses to their associated OpenID values, and then grants all these OpenID values R/W access to the wiki space supporting their work.

Account linking 1-- built on variant two with the Person Registry. The Registry remembers all of the accounts that a person can use (eg OpenID, institution issued credentials, etc). The user's history and permissions are associated with all of the login accounts. (Perhaps some privileges require higher LoA authN?)

Account linking 2-- Sara has been accessing the public portions of SonnetBlast, a Bamboo workspace, based on an authentication to her FaceBook account. Six months later Sara starts a research plan that requires advanced features of SonnetBlast only accessible via federated login using her Wattsamatta U. userid. When Sara logs into SonnetBlast via the federated login for the first time, Bamboo, seeing this as a new user, prompts Sara to create a new account or to use an existing account. If she indicates that she has an existing account, she is prompted to login via an IdP she has used to access that account. The action identifies the existing account and her new login is then associated with that account.

Account linking 3-- Assistant Professor Kohlrabi has a Bamboo identity created under his Garden State College issued userid. Budget cuts to the university threaten to snowball into layoffs in the assistant professoriate. Based on Bamboo FAQ advice, He decides to link his Google account to his Bamboo identity as a precaution against losing his Bamboo portfolio in the event his university credentials are yanked as part of a termination of appointment.

He authenticates to the Bamboo account linking site with his institutional identity. He is invited to chose a social identity provider, clicks on a link that takes him to a Google login popup. After successfully authenticating, he is informed that his Bamboo account is now accessible via his google account credentials, regardless of the status of his Garden State ID. However, because the rights to access certain online journals and Bamboo data files depend on faculty status, he will not have access to those resources when logged in with his Google account. If he leaves GSU and takes an appointment at Trenton State, he will regain access to the data files and resources once he links his Trenton State identity via Account Linking Scenario 2.

Account linking 4-- Professor Jessica Postlethwaite holds joint appointments at Harvard and MIT in nanosemiotics. She is a senior partner in The Semiotics of Nanotechnology Bamboo Workspace. To bring together her data files from both MIT and Harvard, she uses the account linking service to link her Harvard and MIT identities, thereby consolidating them under a single Bamboo Person ID. Note that specific access rights are associated with particular identities, so there are some MIT materials that she cannot access when logged in via Harvard credentials.

sweden -- specific example of account linking. Person transitions through several stages: applicant (OpenID, social), student (institution issued credentials), alum (back to external credentials). All of these accounts are linked to a single individual.

n-tier case 1 -- (delegation used to access backend service)

n-tier case 2 -- (impersonation used to access backend service)

Alumni -- another specific example of account linking. (Carleton College) When alumni password recovery or account claiming can be managed through the email address on record, so can linking of alumni internal accounts with OpenID credentials. Alumni tend to access services rarely (reunion registration every five years, occasional alumni directory lookup); it makes so much sense for them to use credentials they use on a daily basis (like their Gmail account) instead of maintaining and/or recovering local credentials.

(n-tier) Jane Doe attempts to access Service X at campus Y, because she is working on a project with John Smith (a faculty member at campus Y). The service requires that she authenticate; she navigates through the Discovery Service and uses her google/yahoo/facebook account to authenticate, and is returned to Service X. Jane now has the baseline set of permissions at Service X. Jane clicks a button at Service X, which sends a query to a backend service; Service X authenticates to the backend service as Jane.