People Service – federated social identity

Liberty Alliance Webinar

Paul Madsen, NTT
Co-Chair, Liberty Technical Expert Group
People,
people who need
people
are the luckiest
people
in the world ...

Babs Streisand
(but not if they rely on the Web to find each other)
Evolution of identity
No identity in early Web, e.g. search engines, maps
Single identity web applications were next, e.g. online banking, personalized portals
Many web apps now derive some or all of their value by enabling interactions between multiple identities.
YASNs, photo sharing, blog rolls, file sharing, music playlists, etc
But
User's social networks
Fragmented & Duplicated
Duplicate views of same social network
Connection mechanisms
Single provider and/or address sharing
Send an invite to join Flickr

We'll send each person you list below an email with a link to Flickr. If they are not interested, they can safely ignore the invitation.

See past invites on your invite history page.

First, enter your friends' info

Email Address

Name (required)

Then, customize your invitation and send it

This invitation will be coming from you. But we don't know your full name and that is a bit weird for the recipient. You can go and add it to your profile first or you can just enter it in this box and we will use it for this invitation but won't save it on your profile.

Your Name: paulmadsen

This person is a friend.
Scenario
Bob wants to share his vacation photos with Tony
1) Bob provides photo provider Tony's account name or email
2) Photo provider sends Tony an email with link
3) Tony responds & creates account
4) Tony questions his decision after viewing 40 unfocussed sunset shots
What if?
1) Bob doesn't want to repeat this every time he wants to interact with Tony
2) Tony doesn't have or want an account at photo provider
3) Tony doesn't want his email given out so indiscriminately
Current model won't fly
What do we need?
1) Work across identity providers
2) Leverage existing identities rather than creating new
3) Reusable common social layer
Common Social Layer

Application

Application

Application

Application
4) Minimum disclosure
ID-WSF
People Service
Cross-principal connections made and maintained in privacy-++ manner
Components
1) API

2) Invitations

3) Identity Tokens
API allows PS to act as the clearing house for user's social federations
- manage user-user connections
- manage social structure (groups)
- mediate identity mapping
- Create new user.
- Add user to group.
- List group members.
- Is user a member of this group?
Invitation mechanisms support initial establishment of identifiers for users between providers
Identity tokens allow providers to refer to users in other than the context of an authentication statement.
Connections between users manifested as exchange of identity tokens between corresponding providers.
Scenario revisited ... this time with a PS in the mix
PS facilitates cross-provider and persistent user-user connections
Notify

Add

Invite

AuthnRequest

Query

Response

SP

PS

IDP

People
Service
Dance
1) While visiting his photo provider, Bob indicates he wants to share his vacation photos.
2) Photo provider discovers & then queries Bob's PS in order to display existing members
Photos'R'Us

Share Photos

Who do you want to share photos with?

Existing friends?

Mary
Fred
JoJo the Elephant Man
Al
Poopsy

Specify a new friend?

Submit
3) Bob sees that Tony isn't in the list and so asks that he be added (and that he then be allowed to see photos)
Photos'R'Us

Share Photos

Who do you want to share photos with?

Existing friends?

Mary
Fred
JoJo the Elephant Man
Al
Poopy

Specify a new friend?

Tony

Submit
4) Photo provider sends 'Add Tony' request to Bob's People Service
5) PS & Photo provider work together to create an invitation URL for Bob to send to Tony (or sent directly from Photo provider)
6) Tony chooses to respond. After giving informed consent, he gets added to Bob's PS.
7) Tony gets federated between his IDP and other providers
8) Photo provider assigns appropriate privileges to new identifier (not 'account') for Tony
9) Tony sees the Grand Canyon from 23 different angles
What's different?
Bob manages his social network in cohesive manner.
Connection between Bob & Tony persists to be used again in different social contexts (until either chooses to discard)
Tony uses his existing IDP account rather than creating yet another at photo provider.
Privacy of both users respected
Model also supports sharing SOAP-based resources.
Conclusions
People,
people who need
people
are
the
luckiest
people
in the world ...  

Babs Streisand
(if they can take advantage of an ...)
ID-WSF
People
Service
Thanks

(let's stay in touch)

https://www.projectliberty.org/resources/whitepapers/Liberty_Federated_Social_Identity.pdf