Return to Advance CAMP wiki

Advance CAMP Monday, Oct. 5, 2015

1:10pm-2:00pm

Room 24

User-centric Identity; Identity Store(s) - One or Many?

CONVENER: Tom Jordan, University of Wisconsin-Madison; Subhasish Mitra (Utah)

MAIN SCRIBE: Jon Miner, University of Wisconsin-Madison

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES:

DISCUSSION:

Age of processes and procedures for joining/linking people without user intervention are unsupportable.

- Number of identity data providers increasing
- based on objectionable or sensitive/restricted data like SSN/Gender/DOB
- Formatting issues, consistency issues

Want to provide people an identity that they can assert themselves and to which role data can be attached.

UW-Madison is constructing machinery to allow people to “self-link” data. Working with data custodians to get buy-in, while HR is using it for student employees.

Q: Anything published on your website regarding this?
A: Not much. But we do have a self-link utility that’s documented somewhat.

End user: https://kb.wisc.edu/helpdesk/page.php?id=44831
HR officer: https://kb.wisc.edu/helpdesk/page.php?id=46865

Q: How are we handling source system data?
A: Will still be able to push out data from custodians if it is needed for business process.

Pushing name out to applications from preferred name as a step toward user-centric.

What attributes fall in to scope for this?

- Names, someday gender, pronouns
- Contact method

Handling for how people want that data disseminated? Not tackled yet.

Utah is looking at similar things, as are others.

Titles have been a problem, people want to assemble their title the way they want. Faculty profiles in web directory: CV, titles, area of interest.

Which job(s) do you list for someone when they have 20 different jobs?

“Get best” functionality to understand the “priority” of the various identity/demo sources.

Recredentialing issue for people who formerly attended/etc. Punting for now because of a lack of ability to validate identity.

Simultaneously working to push people to create credentials as early as possible and from the user so that future connecting.

What’s driving the project?

- User experience
- Supportability/Cost
- Decentralized system

Todd: Centralized systems aren’t better, just different, just authoritatively wrong.

How many people are working on it?

- Not a whole lot of people directly, it hasn't been a huge change for the existing system.

How do we flow data downstream?

- For a long time have asserted "best" demo from IdP, based on linking that has happened in identity system.
- Data projected out is always the conglomerate "best" which is inconvenient when it's wrong and the only data available.

Q. Where in the process does the account get created?
A. People create an identity, link credentials to it, and attach role (HR, Student, etc) to it.

Q. How to solve the problem of people who change their name inappropriately?
A. It's been perceived as a problem but hasn't been as much as it was thought to be. Currently limiting changes to first/middle and case/spacing for last. Has surfaced the problem of "professional name" in HR world and searchability.

Q. How are parents and payers being handled?
A. External ID project is creating a system to manage relationships. External relationships are being attached to people registered with the external.

Q. LOA?
A. We are not attaching the external identity to the internal identity, and could assert LOA1 if needed, but aren't currently. People who are physically present and get cards are proofed by ID Card.

Subhasish - Multiple identity stores at Utah, problems with people from different stores not being authorized well. Compromised account handling, multiple backend directories.

UW-Madison preferred name: https://kb.wisc.edu/helpdesk/page.php?id=25540 also http://registrar.wisc.edu/preferred_name.htm

ACTIVITIES GOING FORWARD / NEXT STEPS:

If slides are used in the session, please ask presenters to convert their slides to PDF and email them to acamp-info@incommon.org