Return to Advance CAMP wiki

Advance CAMP Wednesday, Sept. 28, 2016

3:30pm-4:20pm

Gusman Room

User Centric Identity Federations

CONVENER: Maarten Kramers

MAIN SCRIBE: Mike Zawacki

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 15

DISCUSSION:

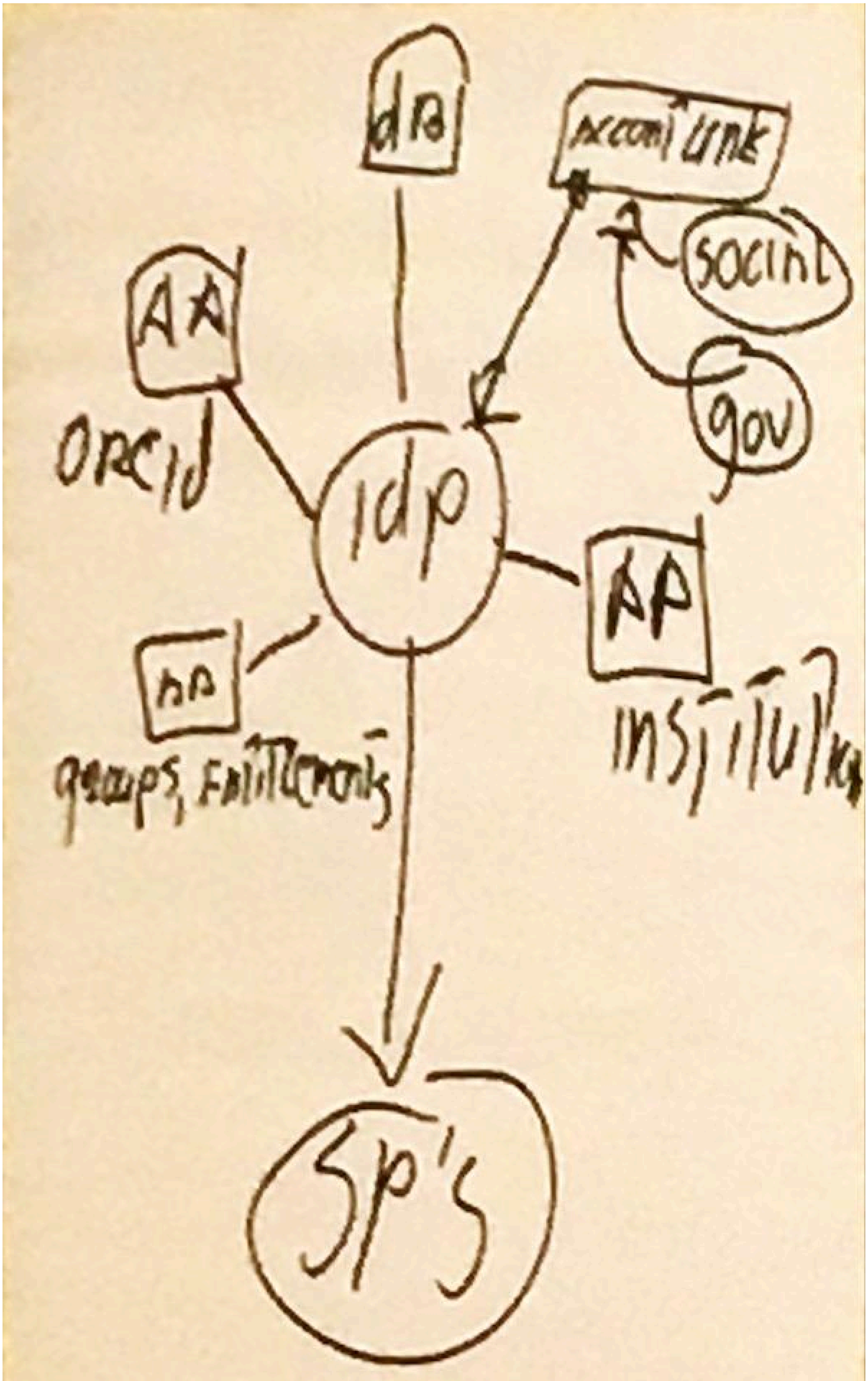
Current federations organized in an org-centric arrangement.

- Problem when a user leaves an organization - IDs can be destroyed, need to be rebuilt, access to resources can be lost
- Anyone outside of any organization can't have a federated identity (external collaborators, visiting SMEs, etc)

Initiatives in SWITCH, Italy to move toward more user-centric identity.

- Long lived/persistent
- Basic attributes set up by user
- Enrichment by AAs

(INSERT PHOTO OF DIAGRAM HERE)


AA
ORCid
idp
AP
social
gov
SP's

EU allows login by any EU users into any gov't system irrespective of nation of orign

IdP fed by numerous sources (institutions/schools, ORCID instances, etc) - user determines attribute release policy.

Question from Maarten: What's good about this? What's bad about it? What could be done differently?

Maarten: What's your experience with this approach?

- Thomas: SWITCH is work in progress. Haven't yet migrated an institution in. Still thin policy-wise. Multi-year project (probably lasting past 2020)
- Regarding diagram - slightly confusing to show only on IdP. Model relies on multiple, distributed IdPs. Plan is that when institution migrates into system their IdP is retained (helps with back compatibility w/SAML - key for eduGAIN)
- User choses institution for their "home" IdP. From there system verifies of user's connection with that institution. If found valid it then puts out that assertion.
- Increased SP complexity as it needs ts to pull attributes from multiple IdPs for groups of users. But can simplify/centralize changes which would then be propagated outward.
- Hybrid approach - elements of mesh and hub and spoke

Tom: What's the best way to add social IDs with institution's assertions?

- Maarten: Proxying perhaps. Need make it as easy as possible for SPs while preserving privacy.
- Thomas: Would like to create attribute query, add asserted attributes to IdP. Might implement some caching for performance issues, but don't want to centralize too much info.

Tom: What to do if an AA is unavailable?

- Maarten: Caching, possibly, but it does create a security risk. Some tuning would be needed to figure out what's reasonable and functional.
- Jon: How to handle "don't know' response?
- Tom: App can determine success/failure.
- Thomas: IdP must note which affiliations exist.
- Chris: Given SP limitations long term we dhouls be moving sources down toward SP (?)
- Jon: Concern that can force apps which don't need to assertions to end up receiving them
- Maarten: Update mechanism could be tricky - no way to ask for additional attributes.

Maarten: Authority issues - Institutions can assert some attributes, authenticate users. Maybe other possibilities?

Chris: Look at UW self service model. Attributes like prefered name should be owned by user, but if Google or other social portal is the source, how to add university asserted attributes? How to differentiate/advertise source of those attributes? Grand scheme, if user's attributes are decentralized into multiple sources we need to allow those associations to be mapped.

JonM: each interaction (data collection or assertion) happens where it needs to happen -- each source only asserts attributes needs to, and as close to the authority as possible.

- Tom: If we limit sources to assert only certain attributes it can result in info being hidden/issued
- Dedra: Do need to track some things at some times, minimal sets
- TomJ: What we've found is self asserted attributes generally cover the minimal set
- TomB: Issue with data discovery - need to think about completely different models/technologies.
- Mark: Don't want to store externally asserted attributes, so you need a way to know where to look up those attributes.
- Thomas: First attempt could be make proxy attempt from user's IdP. Eventually AAs could handle queries natively.
- Maarten: Possible that several claims could be directed by OP
- Gabriel: There are in fact aggregated and distributed claims in the OIDC spec, including provisions for OAuth-secured claim retrieval urls
- Chris: SP could keep track of required queries, make decision of where to go to resolve those.
- TomB: We never get rid of identity, even if attributes are changed/discarded.
- Maarten: in our university we take the opposite approach - identities can be purged.
- Jon: Our approach is that SPs/university department can continue offering services, no matter what.
- Chris: We require periodic logins
- Maarten: Sounds like for most institutions being able to log in is part of the process of maintaining identity
- TomJ: Challenging identity lifecycle issues. We have individual institutional IdPs but shared resources. Sometimes user is requesting access to resource using identity from another institution. System needs to create local identity to allow access.
- Jon: May need to fix some of those issues in person rather than via software. We may need to solve it some day, but not yet.

Maarten: Warren - How do you handle users "vanishing?

- Warren: We mainly worry about linking old IDs to new. Look for name collisions and if there's a fuzzy match we contact user and ask to confirm they're not this other user. Presents a problem if user's name changed (marriage, gender change) - we might miss them.

Gabriel: A lot of this discussion is around account linking. Relies on persistence of IDs, etc. What if there was a way to formalize the idea of credential portability. Some amount of recredentialing, same assurance/faith in accuracy of that data.

- TomJ: Interesting idea. What would be preserved in that process. You're effectively putting credential into new name space, with potential collisions, lack of portability would be an issue
- TomB: Where would credential be verified
- Gabrial: Not sure, just looking to treat this inband rather than out of band. If everyone had a persistent identifier then some of these issues would vanish.
    - Jon: Mentioned OOB fix we use - could be handled inband
- Albert: Question I have is whether this is needed or useful. One identifier we rely on is eppn. How do you carry eppn across institutional boundaries? How do you determine authority?
    - Maarten: Attribute based.
    - Gabriel: Much as we guard our attributes a user's previous identities are a record. If there were a distributed way to track previously known AKAs. Might be a way, but not ready to propose
    - Chris: ...but I will! SP-centered model. If we wanted to move to an SP-centered model question would be how the attribute authorities would be identified/remembered. If there were a mechanism to manage that you could use any of those attributes to create/resolve queries.
    - Dedra: If person's logging in, using linking attribute could be a compromise to avoid scoping issues.
    - TomJ: If we moved up a level, use model to associate multiple credentials (metadata query, something like that) could that work?
    - Gabriel: Distinct lack of continuity of programatic data flow. Everything dead ends somewhere.

ACTIVITIES GOING FORWARD / NEXT STEPS:

Continue discussing Maarten's proposed model