Meeting 2022-05-12 T13:00 EDT

working whimsical group name “!=BE3”
attending: Rob Carter, Keith Wessel, Nicole Roy, Jon Miner, Albert Wu, David Bantz

Issues or threats to InC/TAP	possible mitigation strategies
Baseline Expectations model not readily extended to additional requirements to increase trust, assurance, interoperability	• ‘Optional requirements’: “If your entity does or wants X, then do it with technique Y” • Entity categories for cluster of behaviors • ‘Badges’ or other metadata decoration to indicate specific property or behavior
Enhanced trust and assurance for R&E perceived as unnecessary overhead or impediment for broad-use productivity SPs	• Operate 2 IdPs, optimized for respective R&E/productivity SPs (~Duke) • Bridge or adaptors to inter-operate 2 (or more?) IdPs
InCommon’s trust model and its enhancement of security poorly appreciated or understood	• Better articulation of benefits, potentially directly comparing with commercial non-federated alternatives • Rethink InC’s trust model; alternatives to full mesh?
Absence of clear “how to” guidance can make flexibility of TAP with InC seem unscalable and reliant on scarce expertise	Promulgate ingredients of Deployment Profile as expected behavior, with detailed recipes/cookbook (?)
InC and TAP incorporate requirements for enhanced trust & assurance for research that can seem ‘boutique’ to many institutions and thus not a requirement for institutional IAM	• Articulate a “both…and” value proposition to avoid seeming to directly compete with Okta, Azure, etc. • Re-emphasize enhanced security and privacy possible with InC/TAP as core academic values worth extra effort

Requirements of research and scholarship figured heavily in InC/TAP design, IdP operators more prominent now. Killer apps or demands from research (except NIH) important to drive advances	• Understand why • Beat the bushes…
from recent threads in Participants' email list:	
Maintenance & configuration of Shibboleth too difficult for many, driving institutions to hosted services with GUI or vendor-provided integrations	•Need for additional bridging / integration services with lower technical requirements to operate

2022-05-27 Notes:

Rob, Andy, Brett, Albert, KeithW, Jon, Chris, RickW, SaraJ, AnnW, DavidB

In smaller federations, some of these issues can be felt quicker.

More background/related stuff: InCommon internal brainstorming doc: https://docs.google.com/document/d/1gpMuNzSzNcJNWGvMBoCjFTrV-eoxYjsCkZPnhru6KW4/edit

Do we need a clear convincing description of how a commercial service can host multiple institutions with "automagic" integration, rather than spinning up new unique SP for every customer? Apart from any potential efficiency at the vendor end, R&E customers' costs to integrate are dramatically reduced for customers, and that in itself is a competitive advantage.

Examples of dysfunction or gaps:

- SP not supporting encrypted assertions (despite encryption key)
- uniquely named attributes
- requirements for user identifier in nameID
- relying on email address as unique identifier

Integration profiles specifically including details of use of entitlements for access control

CP: federation can support multi-tenant or proliferation of SPs for each customer, and still benefit everyone.

Is eduroam hub-spoke trust model a useful alternative to full mesh R&E federation model? Eduroam is some ways “easier”

AlbertWu: Much effort over past 20 years on getting IdPs to “do the right thing”; current need is to get SPs utilizing good practices to increase values of federation.

KW: What can we do as a federation that helps us think beyond SAML? Heather, Albert and I were talking about that yesterday. We seem to be stuck in a SAML box, and that box may be starting to become less useful to many.

AnnWest: We may be looking more at proxies to make it easier for sps to connect in. e.g. CI Logon but keep the center as SAML for security fit reasons.

AlbertWu: actual information resources may be behind a proxy; researchers interested in resources, not the supervening proxy (NIH, CILogin, …). A “service catalog” would be useful tool.

Let’s put out a call to SPs to name services available so we can promote them! [CP: Has Neils [van Dijk] at SURF been doing something on this already in the incubator space? (Service Catalog)]
• Tom Barton reminds us of prior REFEDS Service Catalog effort [c. 2019?]: https://docs.google.com/document/d/1P6bCZusitj3aOCtaKw7B1WwB96aSpr7ZtSqINrRjnac/edit#heading=h.414dt6rn0zdj
• eduGAIN wiki describes 2021 decision to stop work on a service catalog: https://wiki.geant.org/display/gn43wp5/eduGAIN+Service+Catalogue

Coordination will be a challenge:
https://www.nsf.gov/news/special_reports/announcements/042222-access.jsp

meeting week: June 27 ?

Meeting 2020-06-27

Attending: David Bantz, Andy Morgan, Rob Carter, Rick Wagner, Chris Phillips, Mike Grady, Keith Wessel, Sara Jeanes

Suggest we reward good behavior instead of punishing participants.

Service Catalog idea from last meeting

- David - reviewing the links, those were not successfully completed & work stopped
- Chris - helpful to have things that help people find services vs baseline expectations. Service Catalog is valuable for the federation.
- Mike - who would use the Service Catalog?
- Rick - librarians wanting to find out if a service already has SSO won't ask the IAM team, they will ask the journal provider.
- Chris - UWaterloo - someone wants to know if they can access something, but the SP wasn't in eduGain. UK Federation and Canary worked together. Can people help themselves?
- Andy - As an IDP operator, I'm not really aware of the services that are provided via the federation. It's hard to sell the federation without this knowledge.
- David - my library maintains a list of journals. It's probably not the primary way people access the journal, but it helps. A service catalog entry needs additional information than just Name and URI. As an IDP operator, I get requests for SSO for services, but we don't know whether the service already supports SSO and what attributes are needed.
- Mike - is this use-case important enough? A Service Catalog would need to be promoted to the part of the organization that is in tight contact with the people at the university.
- Andy - where would we publicize the "badges" we've discussed promoting? The Service Catalog?
- Chris - Other federations have created entity categories to categorize their services (11 different categories).
- David - service discovery, folks wanting to use a service expect a simple "click here" button.
- Chris - not BE3 - two different things - use the platform (Okta, Azure). the metadata is the platform, it's the circle of trust.
- Andy - do we need a simple "button" way to turn on an integration within the federation (assuming there isn't automated attribute release)?
- Rob - we've done a good job collecting entity IDs, but we don't collect much information beyond that about entities. What about collecting the purpose or function of a service? IDP operators don't know which services are important to their constituents. The researcher doesn't want Elsevier, they want the journal. If info was in metadata, it could be dynamically processed for presentation.

- Chris - maybe not in North America. Lightning talk on assessing metadata about 4 years. Nothing much has been done for whatever reason. Libraries do this pretty well. We could ask the folks that have done categorization if they found it worthwhile. eduid.cz and France (name?)

Rob - Back to the other topic - different levels of trust/capabilities in the federation. community colleges may not need to be "NIH-Ready" the same way the R1 institutions do.

- Chris - what do institutions do internally to characterize their services? Okta and other platforms force you to identify and register all of the services, but we don't with the federation.
- Rob - we collect additional information about internal services, and then we stash it in a database and do nothing else with it.
- Andy - OSU has a portal that presents "popular" services to each type of user, and you can search it as well. It would be fun to connect that to the federation, if enough data was available.
- David - Indiana has an app store like interface
-

AI: Chris - reach out to some folks about categories for services (https://www.renater.fr/services/collaborer-simplement/)