INTERNET2

2022 TECHNOLOGY exchange

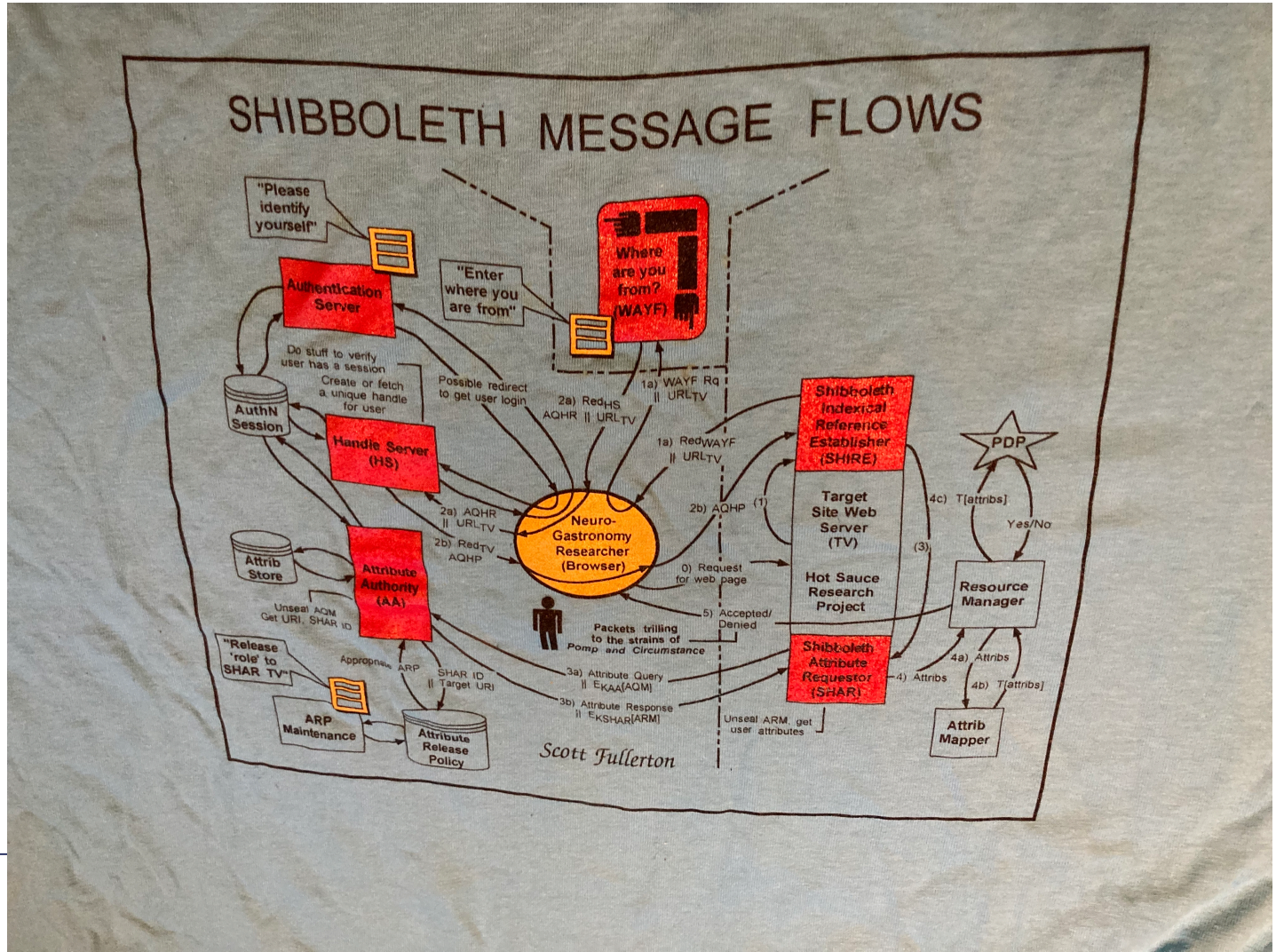
The ongoing challenges of attribute release: How we got here and where can we go now?

Rob Carter, Leif Johannson, Albert Wu, Ken Klingenstein

INTERNET2

Topics

- How we got here
  - The placemat and the T-shirt
  - The intervening years
  - The current reality
- How can we go forward
  - End-entity or other meta-data driven IdP - Albert
  - Consent-Informed IdP Attribute Release – Rob
  - Verifiable credentials - Leif


SHIBBOLETH MESSAGE FLOWS
"Please identify yourself"
Authentication Server
"Enter where you are from"
Where are you from? (WAYF)
Do stuff to verify user has a session
Create or fetch a unique handle for user
AuthN Session
Handle Server (HS)
Possible redirect to get user login
2a) Red HS AQHR || URL TV
1a) WAYF Rq || URL TV
1a) Red WAYF || URL TV
Shibboleth Indexical Reference Establisher (SHIRE)
PDP
Target Site Web Server (TV)
Hot Sauce Research Project
Resource Manager
2b) AQHP (1)
4c) T[attribs]
Yes/No
(3)
2a) AQHR || URL TV
2b) Red TV AQHP
Neuro-Gastronomy Researcher (Browser)
0) Request for web page
Attrib Store
Attribute Authority (AA)
Unseal AQM Get URI, SHAR ID
5) Accepted/ Denied
Packets trilling to the strains of Pomp and Circumstance
"Release 'role' to SHAR TV"
Appropriate ARP
SHAR ID || Target URI
3a) Attribute Query || E KAA[AQM]
3b) Attribute Response || E KSHAR[ARM]
Shibboleth Attribute Requestor (SHAR)
4) Attribs
4a) Attribs
4b) T[attribs]
Unseal ARM, get user attributes
ARP Maintenance
Attribute Release Policy
Attrib Mapper
Scott Fullerton

The intervening years

- Institutional friction
- Limited end-user consent capabilities
- Work-arounds
- A continuing incomplete on compliance

Where we got to

- Whilst in past years the lack of **attributes released** by the IdPs was a major frustration, this aspect was hardly mentioned at the last FIM4R meeting. This does not mean the problem is solved. The main difference is that many research collaborations have found a workaround to handle the lack of attributes, by operating proxies, in line with the AARC blueprint architecture.
- Identity federations keep fighting the ‘attribute’ battle. REFEDS is championing the Entity Category as the scalable approach to ensure that service providers can automatically receive the attributes specified in that category. The uptake of entity categories among the Identity Providers is growing but not as fast as it was hoped.
  - FIM4R Reloaded Report, Oct 2017

Where Else We Got To

- Use of social IdP's and self-asserted attributes.
- Limited use of attributes for access control
- No development of a purpose of use taxonomy

Where Do We Go From Here

- Rob Carter – Institutional and end-user attribute release controls
- Albert Wu – End-entity tags and other metadata approaches, e.g. required/optional
- Leif Johannson – Verifiable credentials
- Discussion

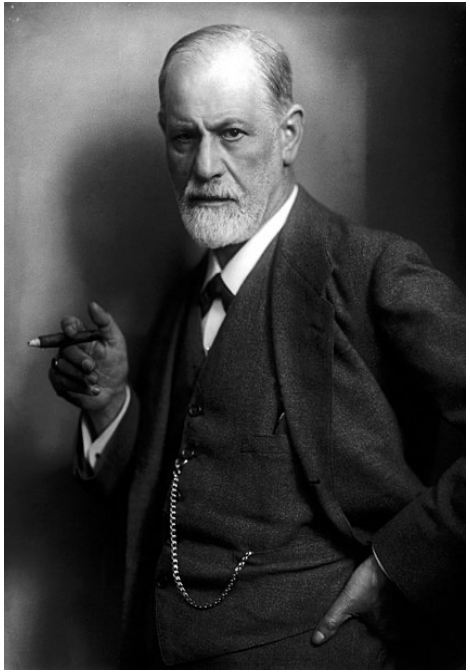
The Psychology of Attribute Release

The Abnormal Psychology of Traditional Attribute Release

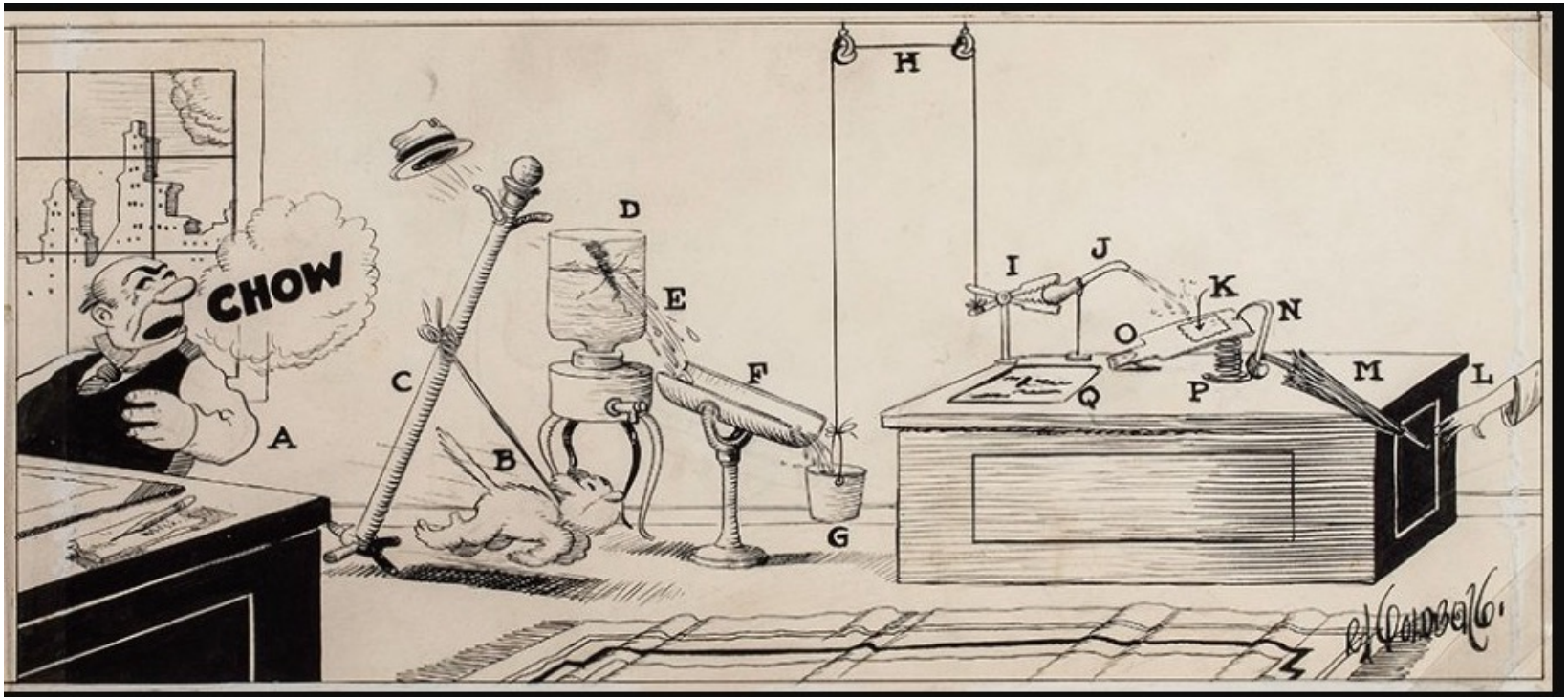
The Abnormal Psychology of Traditional Attribute Release

The Abnormal Psychology of Traditional Attribute Release

- Traditional AR
  - Contract between AP and RP **only**
  - IDPs are “in loco parentis” for users
  - RPs are petitioners, “negotiating favorable terms”
- IDPs tend toward “Attribute Retentiveness”
  - Data minimization – ok, sure!
  - Privacy liability (HIPAA, FERPA, GDPR) – um… wait…
  - “Bother!” said the Op, “This attribute release configuration is hard!”
  - Mantra becomes “**First,** do no harm” (expose only what you ”can’t not”)
- RPs develop scarcity psychology
  - ”Require everything” **just in case**
  - Negotiating is hard, shopping is easy (Facebook? Google?)
    - User experience **and** trust suffer using commercial, libertine IDPs



Psych 201: Complexity Bias



Psych 201: Complexity Bias

- Human nature
  - Confucius: “Life is really simple, but we insist on making it complicated
  - If it’s hard to understand, it **must** be <insert desirable property>!
- In order to make hard things possible, we make simple things hard
  - XML, anyone?
- Configuring attribute release is hard for a reason…
  - …but maybe it doesn’t have to be
- Automatic release policies (entity tagging, attribute bundling)
  - All R&S RPs get {X, Y, Z}
- Default releases by fiat
  - All trusted RPs get {A, W}
- …But what of the privacy liability?

Engaging with your inner child

Engaging with your user

User-engaged attribute release (ok, “consent”, if you must)

- Three-party, transitive trust relationship (IDP <-> user <-> RP)
  - IDP and user have trust, IDP and RP have trust, RP and user have trust
  - Traditional AR focuses on the IDP<->RP trust and not the two user trusts
- User Engagement as mitigation for “in loco parentis” problem
  - IDP remains responsible for data accuracy, currency, security, its trust relationships
  - RP remains responsible for minimizing data requirements, privacy policy, its trust relationships
  - **User** acquires
    - Process insight and transparency – what’s going to whom when?
    - Responsibility for decision-making: Do I want the marshmallow if it costs me **this much** privacy?
  - IDPs may relax ARPs; RPs may be driven to consider their ARs

It’s a Big, Wide, Wonderful World (for consent)

To continue, Google will share your name, email address, language preference, and profile picture with Depositphotos. Before using this app, you can review Depositphotos’s privacy policy and terms of service.

When you sign up with Facebook, we set up your Accounts Center and add your Facebook account and newly created Instagram account. This will enable connected experiences that make it easier to do things across accounts like using Facebook Pay, logging in with Facebook or Instagram and posting across accounts. You can manage these accounts and experiences at any time in Settings.

If you sign up with Facebook

We combine and use info across accounts in Accounts Center

- We’ll suggest friends and accounts to follow
- We’ll personalize ads for you and others and measure heir performance
- We’ll provide more personalized features, content and uggestions
- ɔu remove your account, it can take us up to 3 ıths to stop combining your info.

n if you sign up with phone or email

use info across our products as outlined in our ...vacy Policy.

We use info across all of our products to:

- More accurately count people and understand how they use our products
- Keep you and others safe

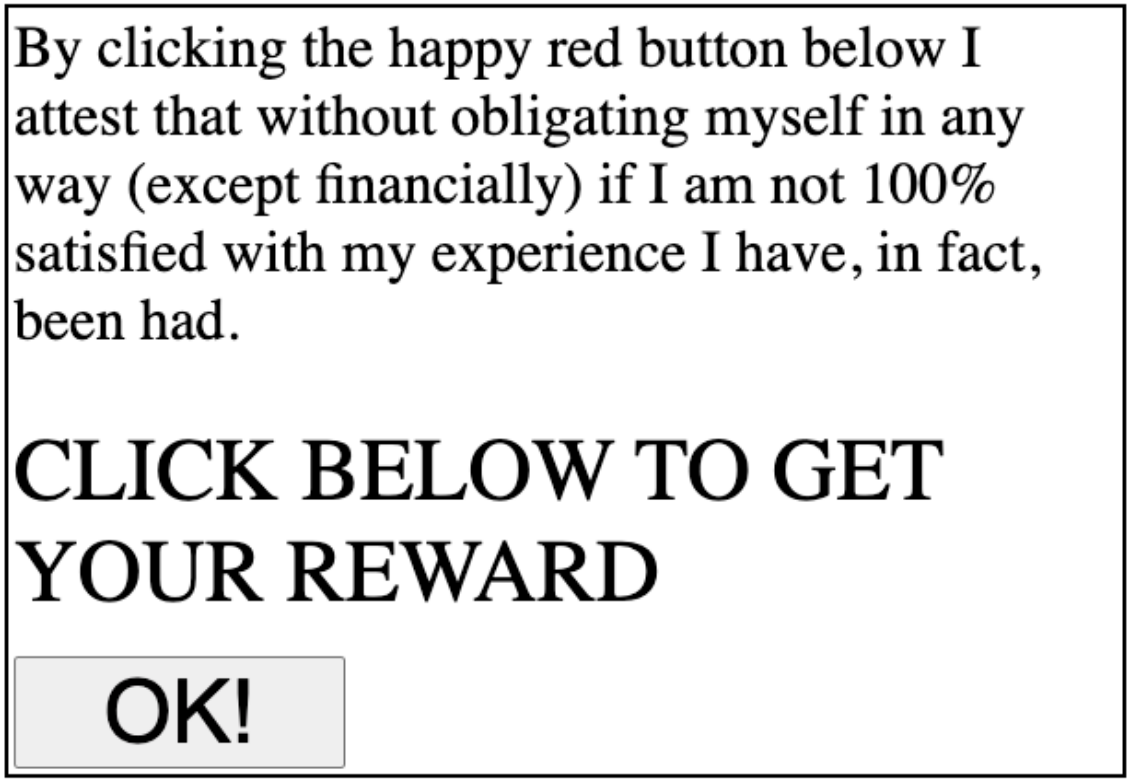
Across Instagram and Facebook, we use info to:

- Show personalized ads and measure their performance on Instagram and Facebook
- Provide more personalized features, content and suggestions on Instagram and Facebook

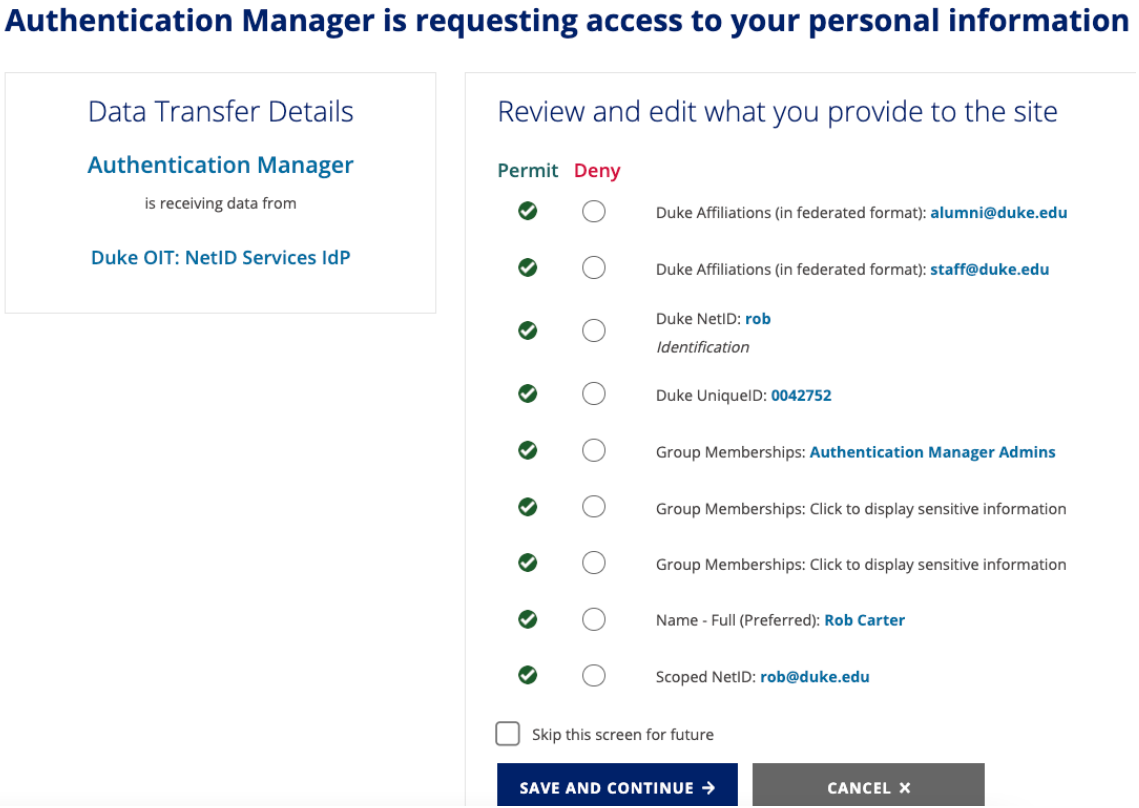
On Instagram, we also use info to suggest accounts to follow.

Learn more about how we use your info.

It’s a Big, Wide, Wonderful World (for consent)



It’s a Big, Wide, Wonderful World (for consent)



It’s a Big, Wide, Wonderful World (for consent)

- Duke work on CAR (Consent-Informed Attribute Release)
  - User-transparency and consent for information release
  - Standalone service (acts as PDP in XACML terms)
- Critical features of successful AR consent strategies
  - Recognize that services (IDP and RP) **as well as** users are stakeholders
    - CAR concept: **(Institutional Policy + User Policy) | (Meta Policy) => Decision**
  - Strive for **informed decision-making**
    - Display names and values for attributes; recognized icons; privacy policies
  - Aggregate institutional policies are easier to write, review, approve, and manage
    - ”Everyone gets transparency”
    - “Students with FERPA restrictions accessing non-InCommon R&S sites get consent, with recommendation to deny <…> and allow <…>”

It’s a Big, Wide, Wonderful World (for consent)

- User policies need defaults **and** granular control
  - I may want to express my general preferences as defaults
  - I may want the opportunity to ”let the institution do what it thinks is best”
  - I always want to know what’s happening, and have the option of changing it.
- Cognitive load is a crucial UI concern
- Consent judiciously, inform liberally

Let’s Talk Entity Categories

But is “Entity Category” really the topic?

Entity Category

Entity Category is a mechanism to signal (in SAML metadata) a federated entity's qualification, adherence, or participation according to a common criteria.

When used in attribute release context:

The **service provider (SP)** is tagged with a category when it meets the category's requirements.

The "registrar" / the party responsible for tagging the SP with said category verifies the SP's conformance with category requirements.

The **identity provider (IdP)** indicates "support" by tagging itself with a support attribute - it agrees to release attributes defined in the category to any SP tagged with the category.

Today's Entity Category - Research & Scholarship

Identity Provider

"Support" by release R&S defined attributes to all "R&S" SPs without manual data release approval flow that'd slow down user access

"Registrar"

At InCommon, it's the InCommon Federation Operator.

Vetts SP for R&S criteria conformance and tags SP accordingly.

Service Provider

Primarily provides research and scholarly collaboration;

Agrees to R&S requirements.

Challenges with Today's Entity Category - Awareness

- Entity Category is a R&E invention. It is not defined core SAML.
- Vendors don't know this exists, or why it exists
- Generational shift - Today's IAM teams in HE largely inherited a platform/architecture/solution from their predecessors. They might be missing key contexts to why this is useful/important
- Will more precise "when and how to use" guidance help?

Challenges with Today's Entity Category - Scope

What we have defined doesn't cover enough data release concerns.

- There are SPs beyond research and scholarly collaborations. (some) SPs have to ask for additional/different/less attributes.
- Gap between category definitions and institution data stewards' model for managing data release

Challenges with Today's Entity Category - Competition?

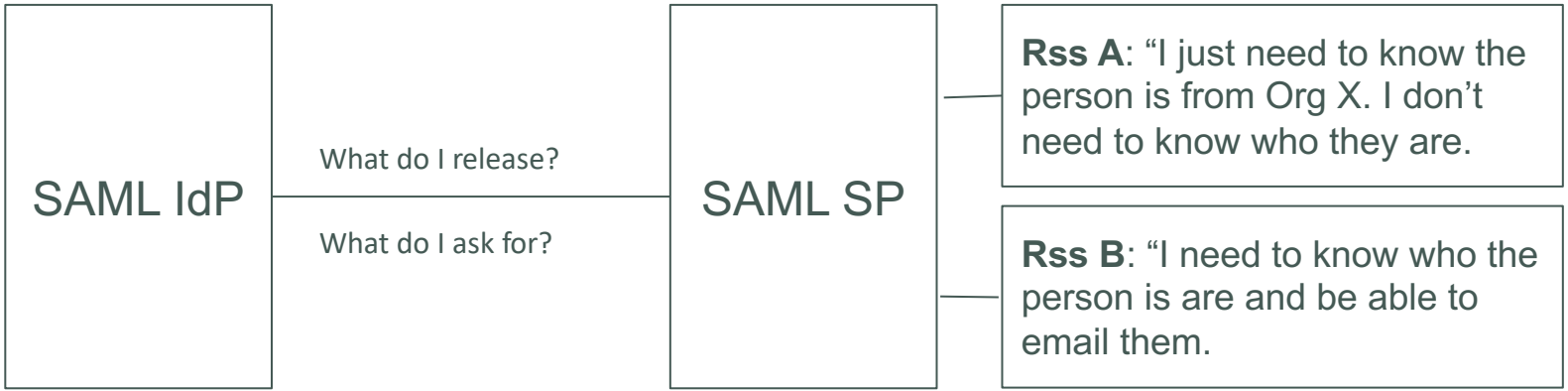
We are not the only game in town anymore – vendors / other verticals are creating "data specs", therefore their respective centers of gravity for "data standards"

- Teams are having to navigate multiple paradigms
- Miscommunication: Parties involved an integration don't have clear direction; they default to vendor's generic default even when the vendor is willing to support additional schemes.
- What can we do to help ease the pain? Does making attribute release schemes "required" in federation help?

Challenges with ~~Today's Entity Category~~ - Others

Attribute Release Management

(Mis)alignment between "resource" and "SAML entity":



New categories around the corner

Anonymous Access

"I only need to know the person authenticated and is from your organization and that they are entitled to access the service I provide. I don't want to know who this is."

Pseudonymous Access

"... I still don't need to know who this is, but I would like a privacy-preserving identifier to help me remember this person's preferences in my service in order to provide better service."

https://wiki.refeds.org/display/CON/Entity+Category+Consultation%3A+Anonymous+Access
https://wiki.refeds.org/display/CON/Entity+Category+Consultation%3A+Pseudonymous+Access

New categories around the corner

Personalized Access

- Person identity
- Email
- Affiliation
- Identity Assurance

Very similar to Research & Scholarship category, except for the “SP primarily performs “research and scholarly collaboration” requirement.

https://wiki.refeds.org/display/CON/Entity+Category+Consultation%3A+Personalized+Access

Disruptive Technologies on the horizon

Entity Category is largely a SAML construct. It assumes that the IdP, therefore the IdP operator, controls user data release. Emerging technologies challenge that paradigm. How do we proceed?