Free the Attributes!
Attribute Release, Scalable Consent, and User Convenience

IAM Online
April 13, 2016

Keith Wessel, University of Illinois Urbana-Champaign
Rob Carter, Duke University
Ken Klingenstein, Internet2

Host: Tom Barton, University Chicago and Internet2
Why Release Attributes?

- “Authenticate locally, authorize globally”
  - Original Federation mantra
  - Entitlements: common-lib-terms. Else?
  - eduPerson[Scoped]Affiliation? Student, member@foo.edu. Else?

- We used to think so, but it turns out that authorization is usually not based on locally sourced attributes!

_Federated access management is a whole other story_
Then Why, Really?

- **User experience** – valuable SP services don’t work
  - Especially important when they serve academic purposes
- What do SPs usually need?

| Persistent identifier | • SP specific profile & personalization
| | • SP specific groups & roles
| | • Reporting (eg, funding agencies)
| Email | • SP related notification
| Name | • Citation & provenance
| | • Hello cc560ca25b6d48db87352bd892d2e199! |
When? Many variations…

- Different for faculty, staff, students?
- FERPA/Buckley election?
- Explicit or implicit terms under which SPs operate?
  - InCommon Participation Agreement Section 9
  - Regulatory regimes about privacy, or maybe lack of
- Automatically, or after SP request to IdP operator?
- With prior user consent?
- Research & Scholarship (R&S) entity category & attribute bundle
  - R&E Federations tag SPs that support R&S activities
  - ePPN, ePTID, name, ePSA, email
CIC Attribute Release Survey

Chicago, Illinois, Indiana, Iowa, Maryland, Minnesota, Nebraska, Northwestern, Ohio State, Penn State, Purdue, Rutgers, Wisconsin

IdP supports user experience by providing attributes

<table>
<thead>
<tr>
<th>Campus</th>
<th>All InCommon</th>
<th>R&amp;S more or less</th>
<th>All eduGain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IdP supports user consent

<table>
<thead>
<tr>
<th>Now</th>
<th>Planned</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
An Unexpected Journey

Attributes@Duke
...First, the Earth cooled...

- Early 2000’s Duke joins InCommon
- Single IDP, no federated SPs
- Pre-existing CAS-like web initial sign-on with ca. 75 relying parties
- No default attribute release policy
- No local federation
- Purely for research access
...Then, the dinosaurs came...

- Five years on, we had a dinosaur federation
  - Manual registration of SPs
  - IT + Stewards approve individual releases
  - Average time to register SP: 5-7 days
- With predictable results
  - Only ~ 300 local SPs registered (mostly owned by OIT)
  - Lots of pushback on ITSO re: SAML
Eureka! Moment

- ITSO pressure to move to SAML on-campus
  - Single point of control
  - Centralized security envelope
- Feedback from webapp owners
  - SP registration process unclear
  - SP registration process too slow
  - Even “public” attributes hard to get
- TL;DR: Fix your ^&*)*& registration process!
Attribute Categorization

- Data Steward / ITSO / IDM negotiation
  - Some attributes already considered “public” in local LDAP
  - Somewhat odd position of previous University Registrar
  - Separate from “data classification” effort by ITSO

- Arrived at four initial release categories
  - Release-by-default for local federation
  - Release-on-request for local federation
  - Restricted release for local federation
  - Release by default to external federation

- This, in turn, led to...
Automation and Self-Service

- Web-based self-service SP registration application
  - Local SPs submit metadata via form
  - Includes attribute release requests
    - “public” release attributes automatically approved
    - “restricted” release attributes queued for approval
  - Applicable to local and external SPs, but not to InCommon SPs
  - Really only feasible because of attribute category agreements
Service Provider Details

Generate a self-signed key/cert. Copy the cert (between the header and trailer) and paste here. Use a long life span for the certificate of 5, 10 or more years.

Certificate

copy and paste cert

Assertion Consumer Service

These are where the information from the IdP gets consumed and decrypted for the Service Provider. Generally, use SAML 2 HTTP-POST for most cases. The Location for this will be in the form of 'https://your.host.duke.edu/Shibboleth.sso/SAML2/POST'. If you have more than one ACS, choose a default if you have a dependency on one

Binding

urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

Location

https://your.host/Shibboleth.sso/SAML2/POST

Is default

Remove this assertion

Add an assertion
26 “public release” attributes:
- cn,
- middlename,
- PeopleSoft EmplID, UserAlias
- SAP Active Staffer ID, Company,
- First/ Last Name, OrgUnit,
- PayrollArea
- TimeTrackerID
- Emergency SMS number,
- eduPersonAffiliation,
- eduPersonEntitlement,
- eduPersonNickname,
- eduPersonPrimaryAffiliation,
- eduPersonPrincipalName,
- Scoped Affiliation,
- givenName,
- mail,
- sn,
- ou,
- title,
- telephoneNumber,
- transient ID,
- NetID (UID)

13 “restricted release” attrs:
- CostCenter Code (fund code),
- Alumni EntityID,
- Ellucian ID,
- Duke Unique ID (cf. Registrar),
- ProxyTokens,
Local Federation Registrations

Chart Title

- Series 1
- Column1
- Column2

Self-Reg Site

- 2004
- 2010
- 2012
- 2016

0
500
1000
1500
2000
2500

2000
1100
2200

Series 1
Column1
Column2
Recent Developments ( Relevant )

- **2012-2013:** MFA integration in IDP
  - Driving more interest among web app owners

- **Early 2015:** Agreement to release R&S attributes to R&S Category RPs
  - Name, email, eduPersonPrincipalName
  - Also eduPersonScopedAffiliation

- **Late 2015:** IDP v3 deployment; Automatic R&S attribute release
  - Previous IDPv2 release too old to easily consume SP category metadata

- Significantly, this does for R&S RPs what we did previously for our local federation
Slide 11: A New Hope

- Scalable Consent
  - Previous Registrar: FERPA doesn’t matter with informed, revocable consent
  - Local Federation: Convert “restricted” to “with consent only”
  - External Federation: Same (caveat R&S, etc.)?

- Consent Infrastructure
  - More than just SAML
    - OAuth2 / OIDC
    - Other APIs (Calendar data, Financial data, Location data, etc...)
Attribute Release at the University of Illinois at Urbana-Champaign

Keith Wessel
IDP operator, Identity service manager
What we release

- The full Research and Scholarship bundle to all InCommon SPs
  - eppn, name, e-mail, targeted ID, and scoped affiliation
- Released for all users except for those who have elected FERPA suppression
- FERPA-suppressed users only have a generic scoped affiliation value released
- University federation and locally added SPs get requested attributes
Why we do it that way

• Mike Grady, Mike Corn, Carol Malmgren
• The InCommon participation agreement (section 9)
• InCommon SP operators fit into the category of “university officials”
• The goal: faster on-boarding and a better user experience
• The pay-off: limited involvement from the IDP operator, happy users
eduGAIN: The attribute heard ‘round the world

• eduGAIN was a slight game changer
• No common safeguard for data stewardship
• Releasing directory data is still okay
• We’ve stopped releasing data for FERPA-suppressed users
What next?

• Enable user attribute consent later this year
• Give users control of their own attribute release
• With consent, start releasing FERPA-suppressed user data again
• Distinct attribute release policies based on categories
# Categories for attribute consent

<table>
<thead>
<tr>
<th>Federation</th>
<th>Category</th>
<th>Requested attributes?</th>
<th>What?</th>
<th>Consent?</th>
</tr>
</thead>
<tbody>
<tr>
<td>InCommon &amp; eduGAIN</td>
<td>Global R&amp;S SPs</td>
<td>N/A</td>
<td>R&amp;S bundle</td>
<td>No</td>
</tr>
<tr>
<td>InCommon &amp; eduGAIN</td>
<td>Other SPs</td>
<td>Yes</td>
<td>Requested attributes only</td>
<td>Yes</td>
</tr>
<tr>
<td>InCommon &amp; eduGAIN</td>
<td>Other SPs</td>
<td>No</td>
<td>R&amp;S bundle</td>
<td>Yes</td>
</tr>
<tr>
<td>University &amp; non-federated</td>
<td>All SPs</td>
<td>Yes</td>
<td>Requested attributes only</td>
<td>No</td>
</tr>
</tbody>
</table>
Attribute Release and Consent

Ken Klingenstein, Internet2
Kim Cameron’s Laws of Identity

1. User Control and Consent
   Technical identity systems must only reveal information identifying a user with the user’s consent.

2. Minimal Disclosure for a Constrained Use
   The solution which discloses the least amount of identifying information and best limits its use is the most stable long-term solution.

3. Justifiable Parties
   Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4. Directed Identity
   A universal identity system must support both “omni-directional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of credential handles.

5. Pluralism of Operators and Technologies
   A universal identity system must enable the interworking of multiple identity technologies run by multiple identity providers.

6. Human Integration
   The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7. Consistent Experience Across Contexts
   The universal identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Download the poster. Read the explanation of the Laws of Identity.
Approaches to attribute release

- Institutional policies
- End-entity categories (e.g. Research and Scholarship)
- End-user consent
  - Client side consent
  - Server-side Shib
  - General purpose consent infrastructure
The internal and federated use cases

• External consent
  – Classic federated use cases:
    • Difficult because of their often international aspects
    • In the US, a significant number of “policy deciders” are not in central IT
    • EU GDPR (General Data Protection Regulation) has raised the bar

• Internal consent
  – Examples are the student app marketplace at Duke and the departmental app marketplace at UW
  – Consent needed per requirements of data stewards, both central and distributed
  – May involve protocols beyond SAML, including OAuth and OpenId Connect
Scalable Consent

- Components to create a scalable consent experience and infrastructure
  - An infrastructure to deliver the capabilities and the information to allow users and administrators manage their attribute release from their identity provider at scale
  - A user interface that enables a user to make effective and informed decisions about attribute release
  - Tools for an enterprise to manage that user experience
- Catalyzed by an NSTIC grant from NIST, becoming part of the TIER suite
- Web site
  - https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home
Consent Requirements

- Derived from use cases, TIER needs, usable privacy research, legal regulations, etc.
- Fine-grain attribute release capabilities, with use of “bundles” and “meta-attributes” as needed
- Informed consent that is hierarchical, flexible, accessible, etc, with clear, concise human-readable explanations of attributes to be sent
  - Additional detail provided when needed, including which attributes are required, values of attributes, how SP will use each attribute, how long SP will keep each attribute (attribute privacy policy)
- Revocation of an attribute release policy (out of band is fine)
- Ability to convey trust marks and other guides to user
- Providing a variety of options for attribute release during future visits to the same site, including using the current settings, periodic resets or reconfirmations, out-of-band notifications, etc.
- Provide an audit interface and history to support both privacy and security
- Ability to work across protocols
- Ability to work on-line and off-line
- Support for identity portability
UI (PrivacyLens) as a paradigm

- Enabling effective and informed end-user consent
- Embraces a set of capabilities
  - Hierarchical information, fine grain control, bundling, revocation of consent, flexible notifications, etc.
- Embraces a style of presentation
  - Clear screens and slides
  - Optional display of values being sent
  - Affirmative user actions
- Integrates across use cases
  - Protocol-agnostic
  - On-line and off-line
  - Allows a variety of information sources
- UI built on an open consent management infrastructure
  - Can be replaced, skinned, etc.
Releasing an opaque identifier only
Anonymous comments

With only the opaque identifier released, individuals may post comments while preserving their anonymity within the community.
Components of a Shib consent infrastructure

- **IdP**
- **Attribute Source**
- **User GUI (e.g., PrivacyLens)**
- **ICM (Informed Consent Manager)**
- **Enterprise Management Console**
  - Internal informed consent and metadata management
  - External informed consent and metadata management
- **Consent Event records**
- **Consent Policy Service for Users (COPSU)**
- **Attribute Release Policy Service for Institutions (ARPSI)**
- **Geek to English - Attribute name/value mapping support**
- **Notification/Query Service**
Lessons Learned – Consent Management

- Consent management at scale seems viable, but needs plumbing infrastructure and content
- Participants need to post metadata
  - E.g. mdui, isRequired, privacy policies on use, etc.
- Need to guard against user habituation, oppressiveness; need to permit rubber squeeze toys
- Applications don’t know how to do data minimization
  - Very few are privacy-preserving; most lead with a request for identity when, at that point, only statefulness is needed
  - “You are what you release” functionality not leveraged
- Deep devils in the details
  - Selective release of values from a multivalued attribute
- The hard part will not be the infrastructure design and build but developing and maintaining the information that runs through it
For more information:

• [https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home](https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home)
  – Scalable Consent Overview
• [https://work.iamtestbed.internet2.edu/drupal/](https://work.iamtestbed.internet2.edu/drupal/)
  – PrivacyLens and Consent Management infrastructure
• [https://work.iamtestbed.internet2.edu/confluence/display/YCW/Yourtown+Community+Wiki+and+Service+Portal](https://work.iamtestbed.internet2.edu/confluence/display/YCW/Yourtown+Community+Wiki+and+Service+Portal)
  – Privacy-responsive and attribute aware applications
Questions?
IAM Online Evaluation

Please complete a short evaluation of today’s presentation

https://www.surveymonkey.com/r/IAM_Online_Apr_2016
InCommon Shibboleth Installation Workshops

May 19 - 20, 2016 – University of Chicago
June 23-24, 2016 – Rochester Institute of Technology, Rochester, NY

Details and registration at incommon.org/shibtraining