DRAFT - New Attribute Release Recommendations

(DRAFT) Resolution: InCommon Identity Provider Operators should release publicly-available identity information using a federated transaction to Service Providers in the InCommon metadata aggregate. Identity Providers should also implement consent to enable individuals to control the release of their own information.

Intent

Current State
Far too often individuals attempting to use InCommon to access Service Providers supporting shared academic work encounter an unacceptable user experience.

Since its inception, InCommon has emphasized and promoted the privacy-preserving nature of our SAML federation. An IDP Operator should only share user information with identified services based on an agreement or contract.[1]

This approach required that IT operations develop an attribute release policy for each service provider. If one federated with 50 services, an IdP would need access to 50 release policies. Further, it assumed that researchers, faculty, staff and students collaborating with colleagues outside the institution could easily request that specific attribute information be released to their partners' service operators. The idea was that either 1) campuses would expose services to make this request process easy and smooth, or 2) campuses would add the available user consent software to their IDPs and delegate to users the authority to release their attributes.

What's Changed?
Social Media and Getting Used to Releasing Information: Since InCommon was established over 10 years ago, a more nuanced understanding of the Internet and privacy has emerged. A significant fraction of campus communities use social networking sites (Facebook), have personal identities at the big providers (Google, Yahoo, etc), and have learned how these sites share information about them with third parties. This experience has helped to educate our communities, and helped people to see both the value and the risk of sharing their information with others.

However, this social account is not linked to their campus home. People outside the project will not see these people as individuals, and not as associated with their home campus.

---

[1] InCommon's Attribute Recommendations: https://www.incommon.org/federation/attributes.html

There is a growing awareness that in many academic situations that the value of sharing these identity attributes outweighs the privacy risk. Researchers want their identity assocaited with their contributions to these projects. The EU academic community has recognized this, and recently made a similar recommendation[2]. In key research areas, minimal default release policies are now perceived as blocking progress on academic work.

Easily Deployable Use Consent: FInally, enabling user consent for the release of their personal information is now easily deployable with the recently released Shibboleth Version 3, the most popular SAML2 identity provider software used by InCommon Participants. This puts the individual in the drivers seat, enables them to make the decision on what a service provider should know about them, and reduces the IT Operational burden.

Trusted Statements about FERPA and Federation: Many campuses have cited FERPA as a reason for tight policies. However, these campuses have already stated via their FERPA "directory information" disclosure that they will release many values unless a student has opted out. LeRoy Rooker, who worked for many years in the federal Dept of Education and was widely viewed as an informed voice on interpreting FERPA, has stated that releasing this information via Shibboleth “is not materially different than publishing it via other means”.

Benefits

To achieve the ROI for organizations that have invested in federation as well as increase customer service, we see the following benefits for this approach:

- **Enable Collaboration.** Faculty, Researchers, Staff and Students that collaborate with others outside the organization and need access to a federated resource must contact IT to develop a specific-release policy for the service provider. This puts undue burden on the individual needing access, both to know who to contact in IT and then to know enough to explain what they need. This limits the IdP’s ROI for Federation.
- **Put Information Release in the Hands of the Individual** Putting the individual in charge of the release of their own attributes removes the policy
- **Reduce IT Operational Burden.** Growing number of services only want minimal attributes that are publically available
- **Leverage publically-available information policy as an online directory.** All campuses are required by FERPA to publish a list of the attributes they will make available for every student (unless a student opts-out). Brown’s statement includes name, local and home addresses, and major field of study. Most campuses provide a publicly searchable directory that includes almost their entire communities. These don’t publish all the information allowed under FERPA, but are very useful. In many states, state law requires publicly funded institutions to make available specific PII information for all state employees (eg name, title, and often salary).

[2] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

Default Attributes

Therefore, InCommon recommends that IDP Operators release:

1. for their faculty and staff
2. for students who have NOT opted out under FERPA
3. to ALL Service Providers in the InCommon metadata file
    a. ? except commercial library-related services
    b. ? except SPs that are NOT InCommon members
4. the following attributes:
    a. Name
    b. Email
    c. EPPN
    d. Affiliation

---

http://www.brown.edu/Student_Services/Office_of_Student_Life/judicial_affairs/randr/federal/ferpa.html

From LeRoy Rooker: As we discussed today, provided that the student record information being disclosed as "directory information" has been so designated by the institution and information on any student who has opted out of the institution's directory information is not included in the disclosure, then there would be not be a FERPA problem with the kind of release you describe in your email below.

(from stc) Releasing directory information traditionally meant releasing information to a newspaper, or publishing this information (or a subset) in an online directory. In addition, it is entirely legal for a campus to release to an outsourced Service Provider, via Shibboleth, any of the information it has classified as directory information, for any student who has not "opt'ed out". This information is already available via multiple means; Shibboleth is just a new mechanism for publishing this information. Using Shibboleth to publish this information is not materially different than publishing it via other means.