



LARPP and PrivacyLens: Enabling the Attribute Rich Lifestyle

Topics

- US Government identity activities – FICAM and NSTIC
- Scalable Privacy grant
 - MFA, Citizen-centric attributes, Anonymous credentials, Attribute ecosystem, privacy and consent management
- Privacy and Consent Management
 - Basics of consent, the pain of attribute retentive institutions
 - Consent managements and PrivacyLens (PL) UI and Internals
- Attribute rich lifestyle
 - Bundles, GPID, IsMemberOf and Entitlements, etc.
 - LARPP
- Outcomes
 - What we've learned
 - What we need to learn
 - What comes next

Scalable Privacy

- 2+ year grant to Internet2/InCommon
- Development partners include CMU, Brown, Wisconsin, Ohio State and others
- Several focal points
 - Promotion of multi-factor authentication
 - Citizen-centric attributes and schema
 - Development and deployment of privacy managers
 - Examination of anonymous credentials
- <https://spaces.internet2.edu/display/scalepriv>

Work described in this presentation is supported by the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office and the National Institute of Standards and Technology (NIST). The views in this presentation do not necessarily reflect the official policies of the NIST or NSTIC, nor does mention by trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Fulfilling the original federated identity vision

- The original vision was for
 - Rich attributes
 - Active end user privacy management options for those attributes on a meaningful level
- Along the way, we created SAML, SSO, Shibboleth, InCommon, etc.
- We are now returning to that vision with a set of powerful capabilities (schema and identifiers) and new end user privacy tools
- Identity management isn't about identity. Its about attributes. Some of which may be identifiers that can connect to a specific identity and blah blah blah
- BTW, original vision missed how complex the trust would be

Consent and the law

- Globally, the driving force is EU policy directives
 - The US and Asian countries tend to lack national level laws
 - EU policy directives tend to be EU centric, e.g. EU to EU policies and EU to the rest of the world policies
 - Article 7 of the EU Privacy Directive requires user consent or alternative justification
 - <https://www.terena.org/mail-archives/refeds/pdfRxzCwYW7Sr.pdf>
- Consent now comes with requirements, including informed, accessible, revocable, etc.
- Conventional wisdom is that consent is hard to do and so use some other justification for an institutional decision.
 - Standard exceptions (medical emergency, law enforcement, etc.)
 - Contractual basis (e.g. outsourced service supplied to employees)
 - “Legitimate interests” of the RP (hmmmm)
- The key distinctions of hide/inform/consent the release to the user

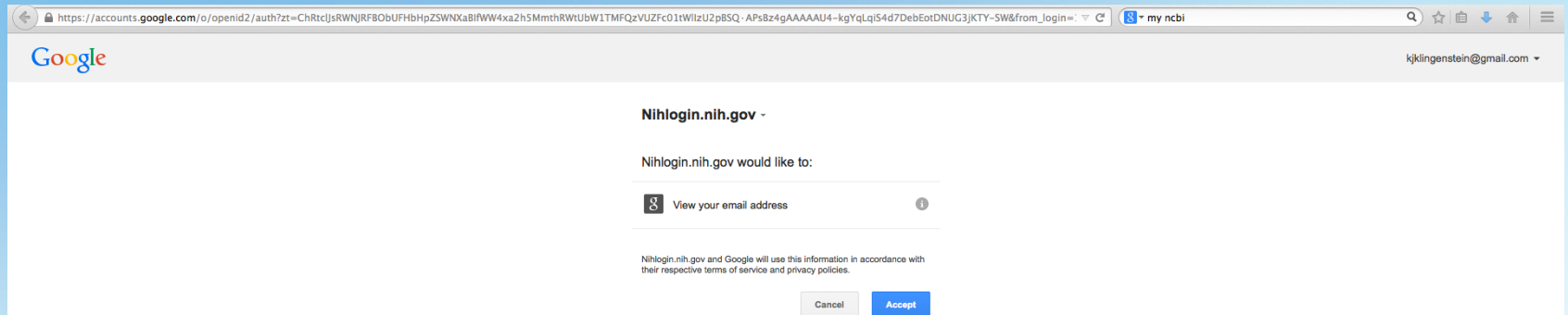
International issues

- How to handle campuses in other countries?
 - Attribute release and local policy
 - Personal data storage
- Several possible parameters
 - Location of RP, location of IdP, nationality of user, location of campus
- A growing number of federations now think that consent will be required for interfederation
- Consistency of attribute meanings between countries
 - Fac, staff and student

The dangers of consent

- The user may say no
 - It is likely that the application will fail in a graceless way
- Consent may not relieve the IdP of responsibilities or liabilities
- The user may become numbed
 - Is this an equivalent to the invalid SSL certificate users click through
- How to implement informed consent and not be intrusive

Google and consent





kjklngstein@gmail.com

Idecosystem.org -

Idecosystem.org would like to:

View your email address

View basic information about your account

Idecosystem.org and Google will use this information in accordance with their respective terms of service and privacy policies.

Cancel

Accept



kjkingenstein@gmail.com

Idecosystem.org -

Idecosystem.org would like to:

View your email address

View basic information about your account

Idecosystem.org and Google will use this information in accordance with their respective terms of service and privacy policies.

Cancel Accept

More info

View your name, public profile URL, and photo

View your gender

View your country, language, and timezone

OK

PrivacyLens background and future


- Based, in plumbing, on the original Swiss uApprove and the Japanese enhancements
- Discussions with CMU privacy research community and a resulting centerpiece in the NSTIC grant proposal
- Research, human subject testing, and development work over the past 18 months
- Has two major dimensions
 - The UI
 - Internals, including enterprise management console, histories and audit logs, portable release preferences, revocation mechanisms, informed consent dialogues, etc.
- Open source hoping to create community

PrivacyLens UI





- Well-researched and clear UI
- Hierarchical informed consent enabled
- Fine grain attribute release control
- Affirmative actions
- Defaults to minimal release
- Histories and logs
- Variety of notification (and suppression) options
- Easily configurable privacy
- Designed for the spectrum of users
- V 1.0 beta available on github 11/1
 - <https://github.com/cmu-cylab-privacylens/Privacy-Lens>

Attribute Release

https://scalepriv-idp.ece.cmu.edu/idp/uApprove/AttributeRelease



CMU's Calendar is asking CMU for your

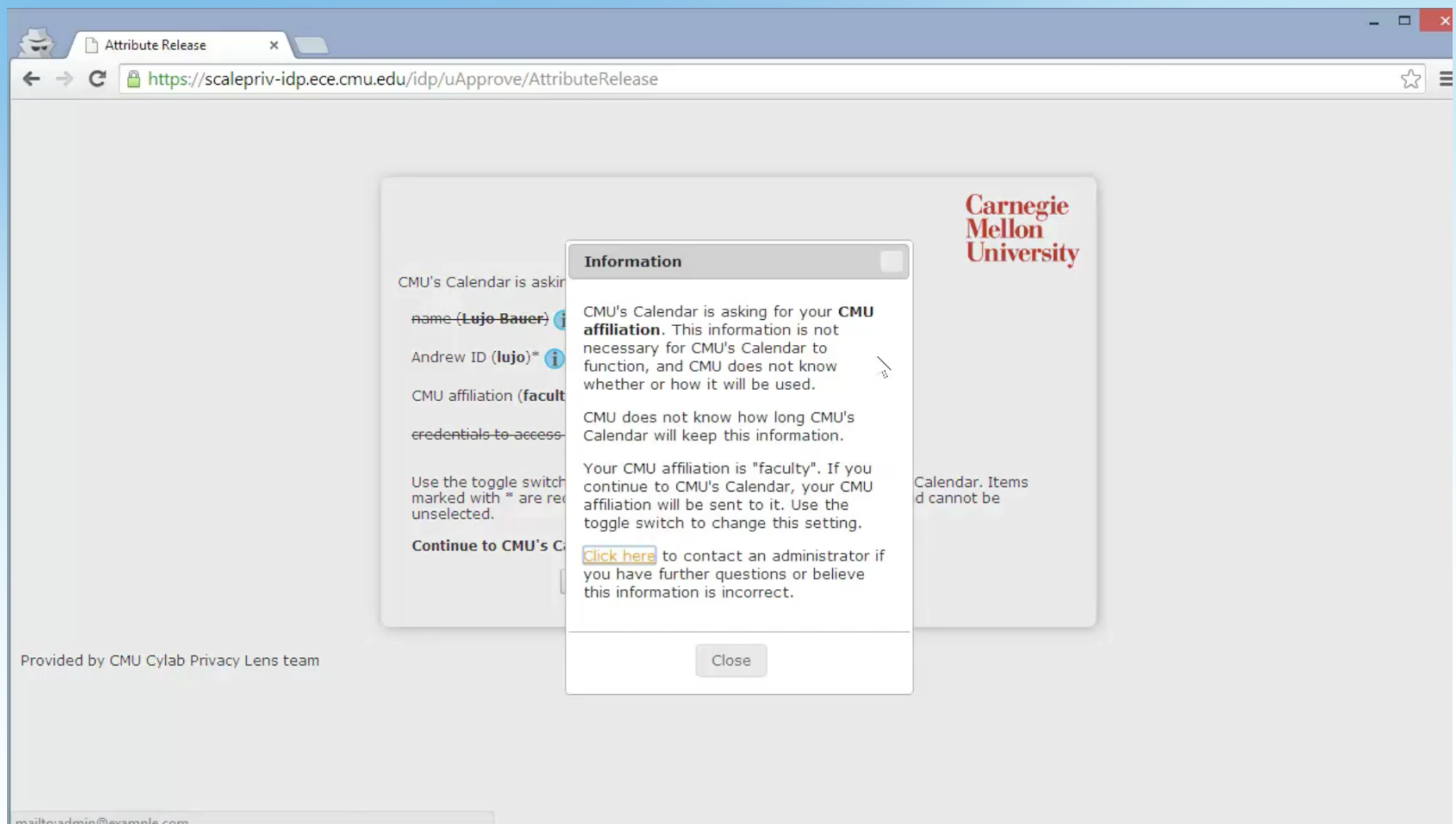
name (Lujo Bauer) 	<input type="checkbox"/> won't send
Andrew ID (lujo) [*] 	<input checked="" type="checkbox"/> will send
CMU affiliation (faculty) 	<input checked="" type="checkbox"/> will send
credentials to access CMU services 	<input type="checkbox"/> won't send

Use the toggle switches to select the items that will be sent to CMU's Calendar. Items marked with * are required to access and personalize the calendar and cannot be unselected.

Continue to CMU's Calendar?

[Settings & History](#) [Explain](#)

Provided by CMU CyLab Privacy Lens team




Login Event

← → ↻

https://scalepriv-idp.ece.cmu.edu/idp/uApprove/AdminServlet

☆ ≡



Logged in to **CMU's Calendar** on 2014-05-05 23:10

Items sent:

Andrew ID: "lujo"
CMU affiliation: "faculty"

Next time you access CMU's Calendar, CMU should:

- ☒ Ask whether and what items to send to CMU's Calendar.
- ☐ Send the following items automatically, but remind you that they are being sent.

Save

Back

Provided by CMU Cylab Privacy Lens team

Login Event

https://scalepriv-idp.ece.cmu.edu/idp/uApprove/AdminServlet

Carnegie Mellon University

Logged in to **CMU's Calendar** on 2014-05-05 23:10

Items sent:
Andrew ID: "lujo"
CMU affiliation: "faculty"

Next time you access CMU's Calendar, CMU should:
☐ Ask whether and what items to send to CMU's Calendar.
☒ Send the following items automatically, but remind you that they are being sent.

Andrew ID (**lujo**) ⓘ

will send

credentials to access CMU services ⓘ

won't send

full name (**Lujo Bauer**) ⓘ

will send

surname (**Bauer**) ⓘ

will send

CMU affiliation (**faculty**) ⓘ

will send

CMU will remind you what items are being sent...
Every you log into CMU's Calendar.

Save

Back

Provided by CMU CyLab Privacy Lens team

The Westin Privacy Indices

- Privacy fundamentalists
 - Fundamentalists are generally distrustful of organizations that ask for their personal information, worried about the accuracy of computerized information and additional uses made of it, and are in favor of new laws and regulatory actions to spell out privacy rights and provide enforceable remedies. They generally choose privacy controls over consumer-service benefits when these compete with each other. About 25% of the public are privacy Fundamentalists.
- The pragmatics
 - They weigh the benefits to them of various consumer opportunities and services, protections of public safety or enforcement of personal morality against the degree of intrusiveness of personal information sought and the increase in government power involved. They look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved. They believe that business organizations or government should “earn” the public’s trust rather than assume automatically that they have it. And, where consumer matters are involved, they want the opportunity to decide whether to opt out of even non-evaluative uses of their personal information as in compilations of mailing lists. About 57%.
- The Unconcerned
 - The Unconcerned are generally trustful of organizations collecting their personal information, comfortable with existing organizational procedures and uses are ready to forego privacy claims to secure consumer-service benefits or public-order values and not in favor of the enactment of new privacy laws or regulations. About 18%

Serving the Spectrum of Users

- Privacy fundamentalists
 - Fine grain attribute release management
 - Variety of informed consent mechanisms
 - Displays trust marks, reputation systems, etc.
 - Ability to review each transaction
 - Intelligent design
- Pragmatics
 - First use is minimal release setting
 - In recurring use, comes up in last used setting
 - Intelligent design
- Unconcerned
 - First use is minimal release setting
 - In recurring use, comes up in last used setting
 - Can be set to only reappear after change/time triggers

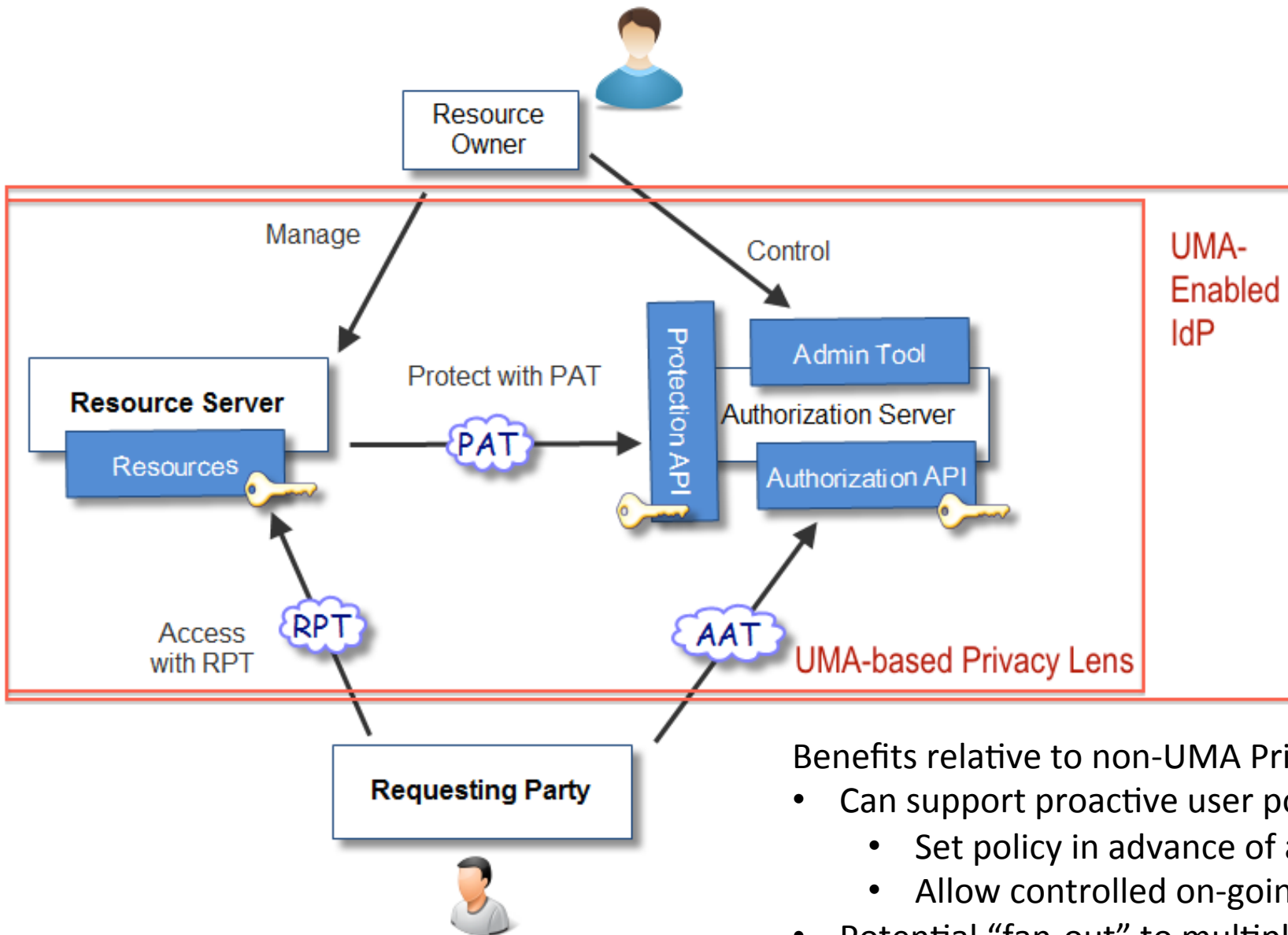
The internals landscape

- Permits the porting of components between platforms (the varieties of SAML providers and the OpenId Connect based IdP's)
- Affects, accessibility, integration with a variety of trust environments, modularity, security, etc.
- Affects enterprise IdP manageability
- Identity portability is a key characteristic of the NSTIC vision
- The key to interoperability, creating a marketplace

Key internal elements

- The internal data stores
 - Saved attribute release preferences
 - Audit logs and user visible logs
- The links to external metadata
 - Trustmarks
 - Informed consent API's
- Interactions with related subsystems, e.g. MFA mechanisms, discovery services, etc.
- UMA capabilities for off-line control
- Attribute descriptions
- Enterprise IdP management console
- Mappings and multilingual support
- Revocation support

Potential UMA-Based Privacy Lens



Benefits relative to non-UMA Privacy Lens

- Can support proactive user policy
 - Set policy in advance of access
 - Allow controlled on-going access
- Potential "fan-out" to multiple AAs
 - In a standards-based manner

Key functions - IdP Management Console

- Establishing user choice options in UI
- Managing audit logs
- Security for console
- Mapping attribute names, etc
- Interfacing with metadata
- Linking to informed consent mechanisms

Attribute rich Lifestyle

- Basic attributes
 - Core identifiers
 - Eduperson
- Extensible attributes
 - IsMemberOf, entitlements
- Bundles
 - Flavors and Add-ins
- Schema
 - GPII for accessibility
 - DD214 for Veteran's Support

Lifestyles of the Attribute Rich and Privacy Preserved (LARPP)

- A set of avatar institutions that are exploring the issues in deploying attribute rich environments with PrivacyLens as a consent manager.
- Sponsored by the Scalable Privacy NSTIC grant
- Initial set of webinars explored the basic issues and just did an assessment and next steps process
- <https://wiki.larpp.internet2.edu/confluence/display/LARPP/LARPP+Home>

Not Live Action Role Playing



Lessons Learned

- The leverage of federated identity and MFA is huge, but the economics are inverted (IdP pays, RP benefits)
- The use of the right kind of identifiers is critical to preserving privacy
- There is an open standard open source set of components and capabilities that can be plumbed together and implement virtually all of the NSTIC vision.
 - Unobservability classic remains hard
- Social2SAML is quite viable but has deep policy issues
- Privacy can be managed; informed consent is viable.

Lessons Learned

- The pain of attribute release
- What is deployed (Michigan, SwitchAAI) is working
- PrivacyLens user interface becoming US Gov paradigm
- Internals to support the PL interface are not developed
- International Issues are important and complex

Lessons not yet learned

- Hands on demo experience
- Campus policy issues
 - Framing the values and limits of consent
 - Deciding who decides what for whom
 - Planning a deployment
 - Are we selling or saviors?
- Lots of missing human glue
 - Dialogues, human-readable renderings of attributes, help desk support, etc
- Accessibility opportunities
- Internals and management

Questions

- Where is the gap between those feeling pain (e.g. researchers) and the InCommon campus representatives who report no reports?
 - Work arounds, often one-one resetting versus one to many
 - Fails in SP discovery construction, delays, abandonment
- What is the campus timing for IdP v3?
 - Next summer, good time to do both
- Who worries about the international issues for your institution and the potential need for consent from that?
 - A genuine issue
- Is the accessibility potential worth a discussion group?
 - Needs a demo
- Are there immediate campus problems for which PL would be an answer?
 - Yes.
 - The informed bar in consent is low
- Others?

Next steps

- InCommon international discussion group
 - Attribute release storage and related issues
- Working demo site
 - campus discussion materials
- Develop some of the missing glue
- Decide on skunk works support approach and then encourage skunkwork deployments
- Create an enterprise management group to discuss required and desired features
- Create Shibboleth based implementation of internals to support UI
- Others?