Policy and Privacy Considerations for Identity and Access Management in a Federated World

Wednesday, Feb. 8, 2012 – 3 p.m. ET

Ken Klingenstein, Director, Internet2 Middleware and Security

Steven Carmody, Information Architect, Brown University

Rodney Petersen, Managing Director, EDUCAUSE Washington Office
Policy and Privacy Considerations for Identity and Access Management in a Federated World

Ken Klingenstein
Director, Internet2 Middleware and Security
Topics

• A few “original topic” items
  • NSTIC updates
  • A privacy-preserving attribute oriented ecosystem
  • Distinguishing roles and their privacy authorities

• Federation Background and Context

• Key progress areas
  • Shaping the broader marketplace
  • Inter-federation
  • Working through necessity vs consent
  • Attribute bundles and vouched applications

• Still to be worked areas
NSTIC Update

• NSTIC - http://nist.gov/nstic/
  • Well-crafted architecture and approach
  • Faces challenges with limited resources, mixed motives for IdP’s, other federal players, etc
• OMB Directive issued Fall of 2011 to move to external identities where appropriate
• IDTrust Conference March 13-14, 2012
• Solicitation for pilots out
  • http://www.nist.gov/nstic/2012-nstic-ffo-01.pdf
The federated vision of privacy

- Very attribute oriented; protocol agnostic
- Privacy preserving – the IdP and, if appropriate, the user determines what attributes are released
- Common codes of conduct/business practices apply across the federation for both IdP’s and SP’s
- One key missing element in this is zero-knowledge capabilities
Roles, attributes, privacy for individuals

- The term “social identity” blurs key distinctions
- It is important to differentiate the roles, and associated attributes/schema of individuals (distinct from the roles/attributes in their work)
  - Consumer
  - Citizen
  - Enterprise/vertical
  - Geo-temporal
  - Personal “wallet”
- Same identity; different roles; different privacy policies and governance
Federation Background and Contexts

• InCommon in a slide
• Important distinctions in participant use
• International considerations are critical for the community
InCommon today

• 260+ universities, 370 total participants, growth continues rapid
• > 10 M users
• Traditional uses continue to grow:
  • Outsourced services, government applications, access to software, access to licensed content, etc.
• New uses bloom:
  • Access to wikis, shared services, cloud services, calendaring, command line apps, medical, etc.
• FICAM certified at LOA 1 and 2 (Bronze and Silver).
• Certificate services bind the InCommon trust policies to new applications, including signing, encryption, etc.
Types of IdP/SP use cases

• Contractual
  • Directly – e.g. testing companies, content providers
  • Through an aggregator – e.g. content providers
  • Contracting unit not associated with central services

• Non-contractual
  • CIlogon, Teragrid, etc
  • Research.gov and CTSA wikis
  • Spaces, Terena web sites, Czech medical atlas
  • Student travel, software, etc
Dimensions of applications

• Historically, the only classification was classical NIST LOA level of assurance requirement

• Several new important dimensions/characteristics of apps are emerging:
  • Required attributes
  • Code of conduct adhered to
Privacy, attribute release policies, consent

• Complex, sometimes contradictory requirements from governments around the world
• Whose national policy applies – IdP, SP, user?
• In federated identity, the key focus is around attribute release and consent
  • Some attributes required for transaction; some may be optional
  • Control points at service provider, at identity provider, and with the user
  • Consent at collection of information or release
International R&E federations

• > 100M users across >30 countries
• Coverage in several countries is 100%, and extensive in many others.
• Generally part of the NREN but associated with another org or independent in a few
• Frequently linked to several government activities, in research, education, governance, health, etc.
• Some interfederation activities, including the Kalmar2 union and eduGAIN.
• www.refeds.org
R&E federations

This map is intended to provide a high-level overview of countries with identity federations.

Last update: 15 April 2011
Key areas of privacy activity

• Shaping the broader marketplace
• Interfederation that will solidify some international policy issues
• Working through necessity vs consent
• Scaleable attribute release management
Shaping the Broader Marketplace

• Both the NSTIC and EU (STORK) models closely resemble a drawing done in 2001 on an Ethiopian restaurant placemat…
• Evolving EU privacy mandates reflect sets of concerns raised by R&E community
  • Our roles as both operational federation leaders and a privacy-aware community
• The emergence of commercial attribute authorities and the monetization of attributes
  • Caution: Disruptive technology development…
Interfederation

• The key technology pieces
  • PEER – public end-end registry – can hold and manage signing keys globally, dynamically
  • MDX – the metadata exchange protocol
  • Shibboleth as software being able to use MDX

• The key policy pieces
  • eduGAIN, Kalmar2

• Missing pieces
  • Global privacy, Adjudication, Liability, Business model impact assessment
Working Through Privacy

• Definitions of Privacy
  • Social Norms
  • Cultural Norms
  • Context
  • National, state law
  • Evolving case law

• Governance
  • Who is responsible
  • Who is liable

• Does it still exist?
  • Facebook knows everything

• When is Privacy not the primary concern?
Goals for Attribute Sharing

• Facilitate easy sharing of appropriate end users’ attributes by his/her home organization with remote Service Providers
• Make it as simple as possible for campus users to successfully login and enter destination SP sites
• Find an appropriate balance between risk and value for all parties
  • Legalisms
  • Privacy
EU-based eduGAIN, REFEDS effort

• DRAFT (EU, eduGAIN) Data Protection Code of Conduct.
  • https://refeds.terena.org/index.php/Data_protection_co

• Minimize Risk -- But it will not go to zero
• IDPs and SPs should rely on the NECESSARY legal basis for requesting and providing attribute release.
  • the *service* requires that people be able to transfer their existing real-world trust of other members of the collaboration

• User must be INFORMed – no CONSENT required
  • DEFER until Phase 2 the use of user CONSENT
Managing Attribute Release, and Scalability

• SPs need attributes from IdPs
• IdPs default to not sending any
• If every SP (700+ of them) had to negotiate with every IdP (200+) there would be 150,000 negotiations
• For large, contract-oriented SPs, this may be OK
• For smaller, "all-comers" SPs (eg support collaboration), the need to negotiate attribute release greatly reduces the value of federation
• Categories are a first step to reducing this friction, opening the value of federation to many more services
Categories – a New Approach

• The category approach is being successfully used in other Higher Ed federations (eg Renater, the French Federation).
• The goal is to increase the likelihood that IDPs release desired attributes:
  • Without manual IDP admin involvement
  • In situations where privacy compromise is not a concern
• InCommon assigns SPs to categories, based on service characteristics
• IDPs can create and deploy attribute release policies for entire categories
• The first category is “Research and Scholarship” (R&S) – our core business
Categories – Actors and Responsibilities

• SPs
  • By signing the InCommon Participation Agreement, they agree to not misuse the attributes they receive
  • Only request attributes that are necessary for their service

• InCommon Federation
  • vets SPs applying for R&S to ensure they meet R&S criteria
  • Identifies (TAGs) R&S SPs in the federation metadata

• IDPs
  • One-time change to extend their default attribute release policy to release a standard set of attributes to R&S SPs
  • Attributes released automatically
  • should provide an errorURL value that SPs could display in some error situations.
Categories – Actors and Responsibilities

• SPs
  • Continue to do Authorization based on received attributes
• Becoming an R&S SP does NOT make an SP an OPEN site!
Scholarly Identity – What is the Problem?

• Attributing identity correctly for scholarly journals is a long-standing challenge.
• A scholarly life may span multiple organizations
• Retrospective cleanup of the existing mess.
• Will extend past a person’s physical life.
• Applies to both journal articles and datasets
Scholarly Identity – Issues

• Who owns it?
• Who can assert it in a trusted fashion?
• Multiple competing technical approaches
  • ORCID
  • VIVO
• Campus IDM systems will have to track values
Areas still needing work

• The end-user active privacy management tool
• Bringing all of this back into a campus context
• Additional categories
• International consensus on approaches
  • Definition of categories
  • Align InCommon Participation Agreement and eduGAIN approach
### Digital ID Card

**Mandatory information for using the service.**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>eduPersonTargetedID</td>
<td>DmJE+eAaAlk/KUO9CHt7xCEIPoU=</td>
</tr>
<tr>
<td>eduPersonScopedAffiliation</td>
<td><a href="mailto:student@example.ac.jp">student@example.ac.jp</a></td>
</tr>
</tbody>
</table>

**Optional information for using the service**  
*(Please check the information may be sent).*

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>surname</td>
<td>Ichikawa</td>
</tr>
<tr>
<td>jasurname</td>
<td>市川</td>
</tr>
<tr>
<td>givenName</td>
<td>Ichiro</td>
</tr>
<tr>
<td>jagivenName</td>
<td>一郎</td>
</tr>
<tr>
<td>displayName</td>
<td>Ichikawa Ichiro</td>
</tr>
<tr>
<td>jadisplayName</td>
<td>市川 一郎</td>
</tr>
<tr>
<td>organizationName</td>
<td>Example ac</td>
</tr>
<tr>
<td>jaorganizationName</td>
<td>Example大学</td>
</tr>
<tr>
<td>organizationalUnit</td>
<td>Test Unit1</td>
</tr>
<tr>
<td>jaorganizationalUnit</td>
<td>第一学部</td>
</tr>
<tr>
<td>eduPersonAffiliation</td>
<td>student</td>
</tr>
<tr>
<td>eduPersonEntitlement</td>
<td>urn:mace:dir:entitlement:common-lib-terms</td>
</tr>
<tr>
<td>eduPersonPrincipalName</td>
<td><a href="mailto:test100@example.ac.jp">test100@example.ac.jp</a></td>
</tr>
<tr>
<td>email</td>
<td><a href="mailto:test100@example.ac.jp">test100@example.ac.jp</a></td>
</tr>
</tbody>
</table>
Campus policy issues

• Where is the right place on campus to have the
discussions and make these decisions?
• Moving to normative business processes
• Managing delegation of authorization/attribute release
• Down the road, outsourced identities decorated with
  institutional attributes?
• The monetization of attributes
• Campus Role in supporting Scholarly Identity
• Impact of Interfederation
Next IAM Online
March 14, 2012 – 3 pm ET
Securing Campus Active Directories for InCommon Silver: A Collaborative Effort
Nick Roy, University of Iowa
Mark Rank, University of Wisconsin-Milwaukee
Ann West, Internet2/InCommon

Shibboleth Workshop Series
http://www.incommon.org/educate/shibboleth/

• April 12-13 – Columbia, Missouri
• mid-July – Baltimore, Maryland
• Two other workshops in the fall
Evaluation
Please complete the evaluation of today’s IAM Online: www.surveymonkey.com/s/iamonline_feb_2012

IAM Online Announcement List
Email sympa@incommon.org with the subject: subscribe iamonline

Thank you to InCommon Affiliates for helping to make IAM Online possible.