

Killer Attributes (and the apps that love them)



Ken Klingenstein
Internet2 Middleware



Topics

- The importance of attributes
- Characteristics and issues in the attribute ecosystem
- Some killer attributes and their apps
- Ways to move it forward

The importance of attributes

- The need to scale access control
 - Federated identity creates the requirement
 - Number of sites, number of users, etc...
 - The value of roles in regulated verticals
- The need to provide security and protect privacy
 - Put the organization and the user in control
 - The need to provide secrecy
- New and deeply tangled policy area, both nationally and internationally
- Tools, and so issues, are coming...

Characteristics and Issues of the Ecosystem

- Schema
 - Attribute bundles
- Complexity and Extensibility
 - Tagging
 - Complexity vs Metadata
- Attribute flows
 - Creation, transport
 - Attribute authorities and LOA of attributes
- Privacy, user attribute release and consent
 - IdP releasing vs SP asking
 - Query languages
 - The Challenges of Consent



A Fawcett Gold Medal Book

THE BAD ONES

Gangsters
of the '30s
and their molls

By LEW LOUDERBACK

DOZENS OF SENSATIONAL PHOTOS



INTERNET®

kjk@internet2.edu

The Layering of General and Domain Schema

- The standards
 - Person, orgperson, inetorgperson
- An international community
 - eduPerson, schacperson, social profiles
- The federation and/or the vertical
 - National or local operational – hakaperson, switchai, gfipm.net, etc
- A collaboration

R&E basic attributes (eduPerson et al)

- High-level affiliation (eg, member, faculty, staff, student)
- Opaque, persistent and non-correlating identifiers (ePTID)
- A persistent and human-usable identifier (eg, kjk@internet2.edu)
- Name (e.g. Display Name)
- Email address
- An open-ended set of entitlements assigned by the institution, including group membership

Attributes by attribute authorities

- Institutional/enterprise
 - User who has an established, authenticated identity
 - Organizational roles and groups
 - Reassertion of other official credentials (e.g. citizenship, age, etc.)
- Governmental
- Temporal – geolocation, etc.
- Community or collaboration asserted
 - Formal – Virtual organizations, groups
 - Informal – Reputation systems, FoF
- Self-asserted – Preferred language, accessibility

Verticals, roles, schema and federation

- Regulated verticals have structured roles
 - Pharmaceutical, Real estate, Securities
 - DoD, DHS, DoJ
- Unregulated verticals need structured roles
 - Higher Ed and Institutional Review Boards
 - Wikipedia, etc and authorship/review/edit
- Structured roles enable vertical schema for inter-organizational use
- Federations are more than shared identities; they can be shared roles

One PII taxonomy

- 0) Attributes that do not identify a unique user (e.g. ePSA)
- 1) Indirect identifiers designed for privacy (e.g. ePTID)
- 2) Indirect identifiers not designed for privacy (e.g. IP address)
- 3) Direct identifiers (e.g. name, address)
- 4) E-mail address & fax number
- 5) Location information (e.g. mobile phone cell)
- 6) Sensitive personal data (health, race, religion, etc.)

Attribute Complexity and Extensibility

- Complexity
 - Tagging within attribute vs use of metadata vs context
 - Knowing which IdP to ask for which attributes, especially as we get into aggregation
- Extensibility
 - The ability to add new controlled values, and parameters like validation, date, terms of use
 - How much flat attribute proliferation can be managed through a structured data space?

Some attribute flow issues

- Protocols and packaging
 - Um, enough said...
- Entitlements and attributes
- Aggregation
- Reassertion vs delegation

Of Entitlements and Attributes: Who da' PDP?

- In entitlements, SP community passes business logic to IdP's, who compute authorization and pass entitlement
 - To scale, must have common license terms
 - SP's need to be willing to expose business logic
 - Can greatly reduce the complexity of SP life
- In attributes, IdP's pass attributes to SP for authorization
 - Raises significant privacy issues
 - To scale, must have shared community attributes

Attribute aggregation

- Can be done at IdP, SP, or intermediary
 - Code supports it
 - Installations are using it
- Can complicate or simplify trust
- Leads to lots of issues, including reconciling conflicting values, handling incomplete data

Reassertion and delegation

- Reassertion
 - By VO, by portal
 - By revetter – e.g. university and SEVIS
- Delegation
 - Attribute delegation is tricky
 - Embedded base of identity delegation needs to be accommodated

Privacy, attribute release policies, consent

- Complex, sometimes contradictory requirements from governments around the world
 - EU Privacy Directives important, confusing, and under revision
 - FICAM Directives important, confusing, and under revision
 - State and local laws and lots of institutional folklore
- 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

Jurisdictional Issues at the Start

- At least three policy spaces at play
 - IdP location
 - SP location
 - User's national and local laws
- Known exploits exist today...

When to do Consent

- At the point of collection of information
 - “We intend to use what you give us in the following ways”
- At the point of release of information
 - “I authorize the release of this data in order to get my rubber squeeze toy...”
 - Per transaction or persistent for some time

User attribute release management

uApprove

- For scaling of number of sites, number of IdP's, number of countries, number of laws, numbers of users
- Lots still to figure out
 - Minimum vs desired; inform vs consent
 - Bundles
 - UI, both presentation and clue
- Getting the UI, and the defaults, right... the multiplier is in the billions...
- Deployments have begun...

This is the Digital ID Card to be sent to 'https://aai-demo.switch.ch':

Digital ID Card

Surname	SWITCHaai
Given name	Demouser
Unique ID	234567@example.org
User ID	demouser
Home organization	example.org
Home organization type	other
Affiliation	staff
Entitlement	http://example.org/res/99999 http://publisher-xy.com/e-journals

Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.

Cancel

Confirm

Firefox

Inbox (5) - marc_doughty@brown.ed... VMware Communities: VMware Work... null

https://sso.brown.edu/uApprove/Controller?terms-agree=on&terms-confirm=Confirm

vmware workstation 2.6.38

Brown University

Authentication Required

To use 'spaces.internet2.edu', their system needs to receive some information about you in the form of a Digital ID Card. You will need to agree to send the following information to access their services. All this information is needed or access to the service will not be granted.


Digital ID Card	
email	Marc_Doughty@brown.edu
eduPersonPrincipalName	mdoughty
storeIdOracle	ujbMRsDo5eeKRrsOItCcvMsrF50=
displayName	Marc P. Doughty

Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future to this site as well as to other services I will access.

Cancel Confirm

[Brown Home](#) | [Help](#) | [myAccount](#) | **New Users: [Activate your account now](#)**

The face of web authentication at Brown is changing! You are using Brown's new web authentication service, Shibboleth. During 2009, Shibboleth will gradually replace WebAuth as Brown's Single Sign-on web authentication service. Shibboleth is more useful, more secure, and more widely used throughout higher education.



Shibboleth. Shibboleth is different - learn how to [safely and securely use Shibboleth](#).

Additional information regarding Brown's Shibboleth implementation [is located on the CIS documentation wiki](#).



INTERNET[®]

kjk@internet2.edu

Killer Attributes

- Attributes needing institutional/official values but for mass applications
- Killer in their broad and distinctive impacts and use
- Examples
 - Human readable identifiers (email address, eppn, display name, etc)
 - Opaque identifiers - ePTID
 - Affiliation
 - Citizenship
 - Over legal age
 - Preferred language, capabilities

The Apps that Love them

- Access control by legal age
 - Privacy preservation a plus
- Citizen and/or export controlled apps
- Accessibility needful apps
- Collaboration apps

Moving it forward

- The Tao of attributes
 - Schema work
 - Metadata evolution
- Interfederation
- Best practices

The Tao of Attributes

- A workshop run by NIH and Internet2 in Sept 2009 that established the existence of a Tao, and not much more
 - <http://middleware.internet2.edu/tao-of-attributes/>
- An ongoing individual sense of the looming importance of the issues, and an occasional sighting of the need
- Must be at one with the environment and the vertical it exists in
- Needs a home...

Principles of the Tao 属性之道

- Least privilege/minimal release
- Using data “closest” to source of authority
- Late and dynamic bindings where possible
- Dynamic identity data increases in value the shorter the exposure. If identity data is cached away from the source there is increased likelihood of staleness and over-exposure which can lead to privacy and data accuracy concerns.

Schema Work

- Distill good practices in verticals from existing environments
- Evolve a set of core attributes for use in the public sector
 - USperson as an anchor tenant – incorporate a limited set of relevance and proven value attributes and schema
 - Create extensibility mechanisms
 - Work the internationalization issues
- Develop approaches to minimize attribute mapping and to do it effectively when needed

Metadata evolution

- Handling static and dynamic metadata
- LOA of attributes
 - Specifying semantic rules
- Terms of use
- Time limits
- Query languages, etc

Interfederation

- Connecting autonomous federations
- Critical for global scaling, accommodating state and local federations, integration across vertical sectors
- Several operational “instances” – Kalmar2 Union, eduGAIN
- Has technical, financial and policy dimensions
- Key technologies moving forward – PEER, metadata enhancements and tools, discovery
- Has massive impact on the attribute ecosystem

Best Practices

- Beginning in several areas
 - federation participation
 - Organization presence and contacts, technical capabilities, software maintenance, incident handling, discovery, etc
 - <https://spaces.internet2.edu/display/InCCollaborate/Recommended+Practices+for+InCommon+Participants>
 - assignment of values to attributes
 - <https://spaces.internet2.edu/display/InCCollaborate/How+Better+Attribute+Management+Helps+Federation>
- Unknown in several realms – Fed ops, ecosystem-friendly behaviors, intermediaries, etc.