Scalable Consent: Instrumenting for Researchers

Ken Klingenstein, Internet2

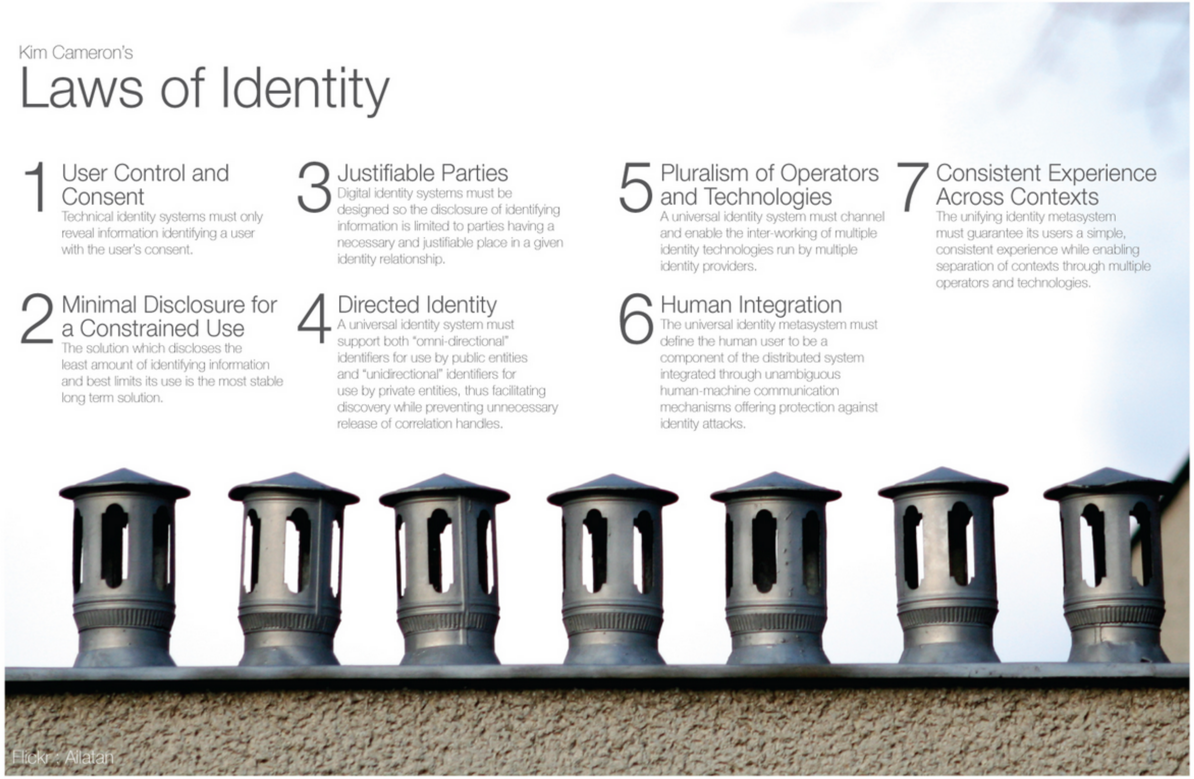
Topics

- The Emerging Identity and Attribute Landscape
- Consent Requirements
- Basics of Scalable Consent
- Core subsystems – UI, Informed Consent Management, Informed Content
- Expected deployment uses, timing, and growth
- Instrumenting for researchers
  - Why
  - What
  - How
  - Staying in touch

The Emerging Identity and Attribute Landscape

- Federated (and interfederated) identity is becoming a ubiquitous approach by many sectors
  - In R&E, InCommon and similar national federations now comprise 40+ countries and >10M users
  - Rich sets of attributes being exchanged
  - Similar federations exist in Law Enforcement, BioPharma and other verticals
  - Uses span C2B, C2C, C2G,B2G, G2G
- Social identities are ubiquitous
  - LOA issues
  - Limited set of interoperable attributes, limited multilateral relationships
- Gateways exist to integrate the two worlds
- Its now more about the Tao of attributes than the mechanics of identity

Kim Cameron's Laws of Identity



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 correlation handles.

5 Pluralism of Operators and Technologies
A universal identity system must channel and enable the inter-working 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 unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Flickr : Ailatan

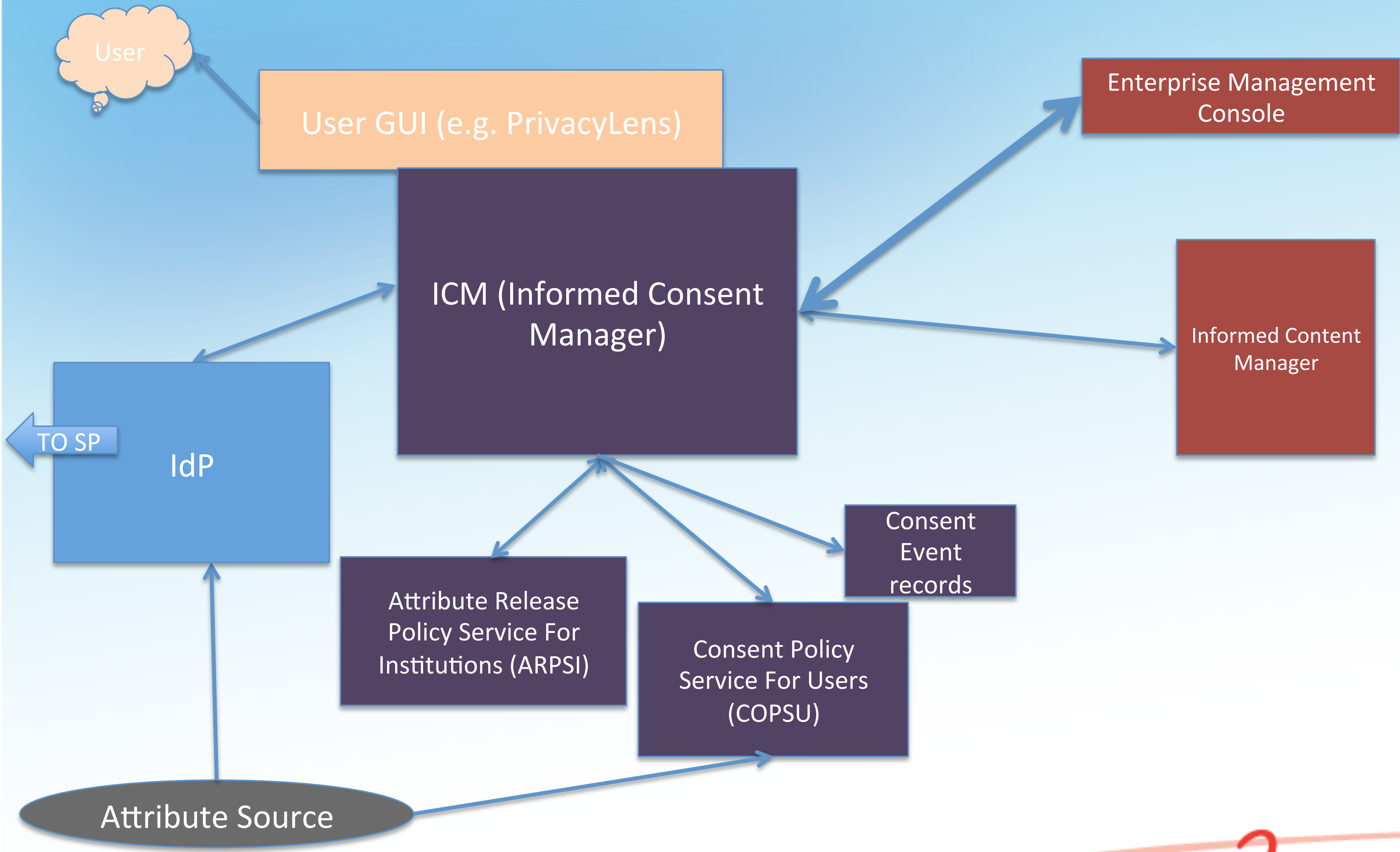
Download the poster. Read the explanation of the Laws of Identity.

Consent Requirements

- Derived from use cases, usable privacy research, legal regulations, etc.
- Fine-grain attribute release capabilities, with use of “bundles” and “meta-attributes” as needed
- Informed consent that is 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

Scalable Consent Basics

- Components to create a scalable consent experience and infrastructure
- Catalyzed by multi-year NIST grant to Internet2 and colleagues for scalable privacy in federated identity
- Intended to be deployed institutionally at scale within R&E and beyond
- Spans multiple protocols (SAML, OIDC, Oauth), deployment models (IdP server-side, consent as a service)
  - Consent for attribute release
- Cognizant of existing practices and regulations
- Rolling out over the next year as open source
- Has three key component subsystems
  - UI, e.g. PrivacyLens
  - Informed Consent Manager and internals
  - Informed Content for effective decisions



User

User GUI (e.g. PrivacyLens)

Enterprise Management Console

ICM (Informed Consent Manager)

Informed Content Manager

TO SP

IdP

Consent Event records

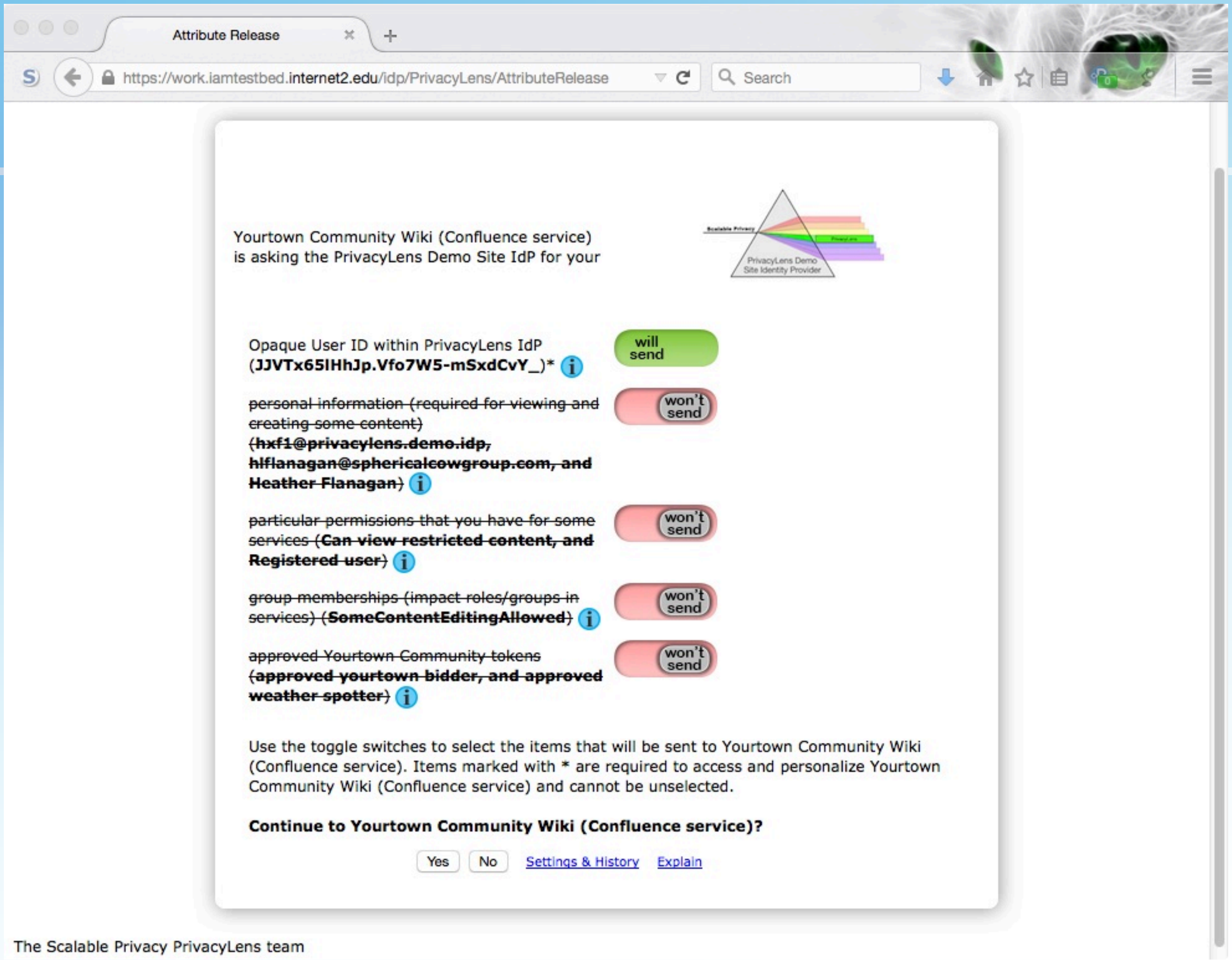
Attribute Release Policy Service For Institutions (ARPSI)

Consent Policy Service For Users (COPSU)

Attribute Source

Model of a good UI

- 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.


Attribute Release
https://work.iamtestbed.internet2.edu/idp/PrivacyLens/AttributeRelease
Search
Scalable Privacy
PrivacyLens
PrivacyLens Demo Site Identity Provider

Yourtown Community Wiki (Confluence service) is asking the PrivacyLens Demo Site IdP for your

Opaque User ID within PrivacyLens IdP (**JJVTx65lHhJp.Vfo7W5-mSxdCvY_**)* ⓘ — will send

~~personal information (required for viewing and creating some content) (**hxf1@privacylens.demo.idp, hlflanagan@sphericalcowgroup.com, and Heather Flanagan**)~~ ⓘ — won't send

~~particular permissions that you have for some services (**Can view restricted content, and Registered user**)~~ ⓘ — won't send

~~group memberships (impact roles/groups in services) (**SomeContentEditingAllowed**)~~ ⓘ — won't send

~~approved Yourtown Community tokens (**approved yourtown bidder, and approved weather spotter**)~~ ⓘ — won't send

Use the toggle switches to select the items that will be sent to Yourtown Community Wiki (Confluence service). Items marked with * are required to access and personalize Yourtown Community Wiki (Confluence service) and cannot be unselected.

Continue to Yourtown Community Wiki (Confluence service)?

Yes No Settings & History Explain

The Scalable Privacy PrivacyLens team

PrivacyLens - Lujo Bauer et al, CMU
]

Informed Consent Management

- Integrates institutional and individual desires for attribute release
  - The ICM integrates the institutional ARPSI with the user COPSU
- Serves multiple use cases
  - Real-time
  - When the user is not present
  - Persistent
- Works closely with UI and presentation
  - Implemented via API's to manage security and privacy concerns
  - Marshalls informed content to UI
- Key issues include revocation of consent, suppression of consent, reconsent, informed content integration
- Policy languages and issues all the way down
- Consent event records interacts with numerous use cases

Informed Content

- What is it?
  - Icons for IdP and SP
    - mdui field in SAML metadata
  - SP IsRequired and Optional Attribute Needs
    - SAML metadata
  - Displaynames and values for everything
  - Trustmarks
  - Privacy and third-party use policy pointer
  - Additional information feeds
    - Vetted, self-asserted, reputation systems, etc
- Issues
  - Creating and gathering
    - Services, marketplaces, etc
  - Structuring for users
  - Trust (self-asserted versus vetted vs reputation vs …)

Likely deployment pattern

- Considerable number of institutions running some sort of consent now
- Scalable Consent code available fall; alpha deploys expected
- Initiative for wide deployments over the next 6-12 months
- Challenges include:
  - Informed content and trust issues
  - Institutional policies
- Discussions with OIDC communities on use
  - Multi-lateral federations emerging now
  - Value of ARPSI serving hard social use cases (e.g.regulation)
- Intent is an Internet-scale consent substrate, serving security and privacy needs

Distinctive Research Opportunities

- A very broad set of users doing real world transactions
  - Daily use across a variety of situations with both low-value and high-value interactions
  - Responsive to a broad set of regulation regimes, from FERPA to HIPPA to GDPR
- A deployment community that wants more usable privacy and security
  - Urgency to deploying consent infrastructure
  - Interest in providing data and consuming research results
- An architecture that permits experimentation
  - Modular components
  - Local deployment variations easily done
  - All open source code

Instrumenting for researchers

- Working within the built-in scalable consent privacy options
- What to capture
  - User usage patterns, dwell times, suppression choices, preferred or alternative informed content sources, etc.
  - Other data as needed, e.g. predictive release tool success rates, etc.
- What to work with
  - Policy languages in ICM, ARPSI, COPSU
- How to provide
  - Research anonymization needs and existing anonymization approaches
- Staying in touch
  - kjk@internet2.edu

More information

- https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home
  - Scalable Consent Overview
- https://work.iamtestbed.internet2.edu/drupal/
  - PrivacyLens and Consent Management demo
- https://work.iamtestbed.internet2.edu/confluence/display/YCW/Yourtown+Community+Wiki+and+Service+Portal
  - Privacy-responsive and attribute aware applications