Scalable Consent: Basics

Ken Klingenstein, Internet2

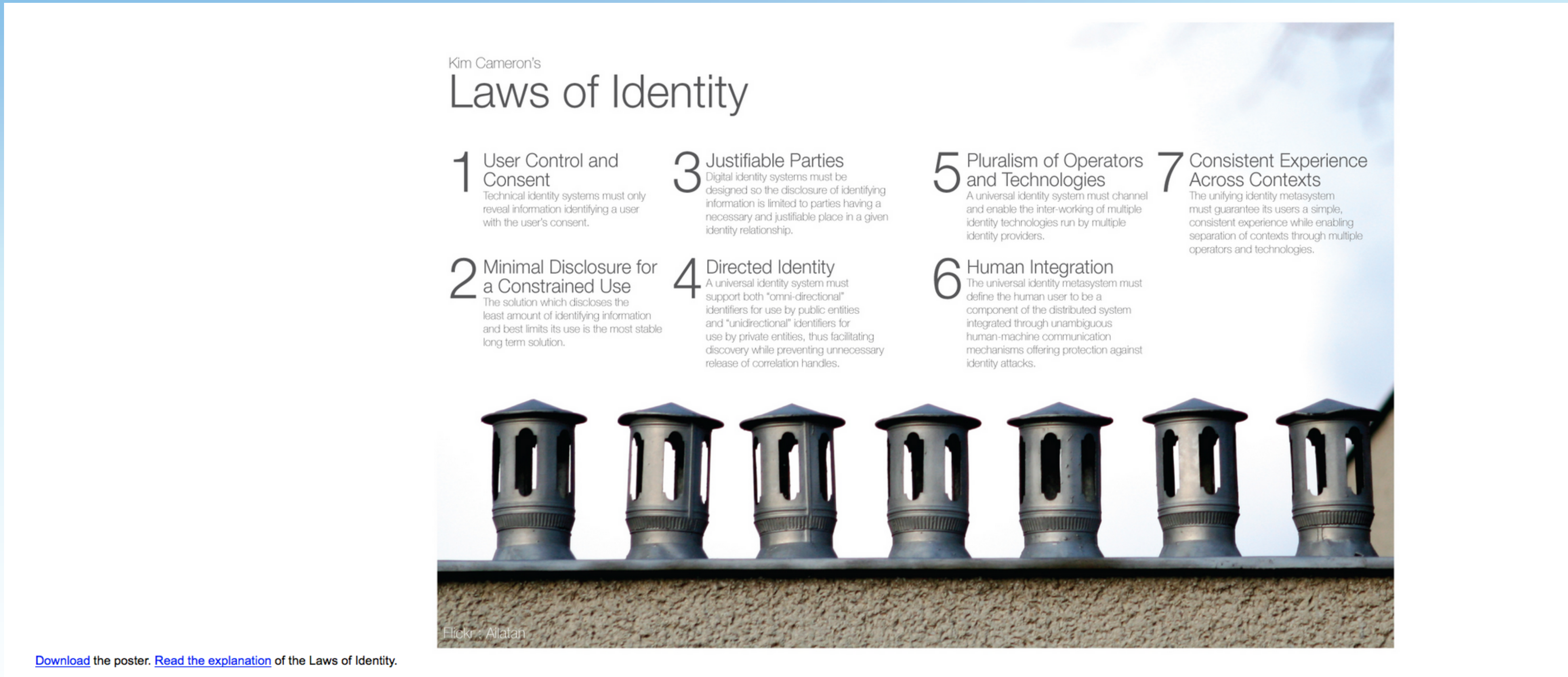
Topics

- Consent Today
  - Consent, Regulation, Appropriate Use
  - Current Options
- Basics of Scalable Consent
  - Use Cases and Requirements
  - Design and Development Process
- Core subsystems
  - UX, e.g. PrivacyLens
  - Informed Consent Manager and internals
  - Informed Content for effective decisions
- Timelines for product development

Consent, Regulation and Appropriate Use

- Use cases where consent is inappropriate
  - By contract – institutional use of software as a service
  - By regulation – e.g. some GDPR (EU Privacy Regulation) stipulations
  - By business rules – e.g. ”negative” rights (blacklists, etc.)
- Use cases where consent is required
  - Installation of most applications on a smartphone
  - By regulation – e.g. some GDPR (EU Privacy Regulation) stipulations
  - To provide a consent event record for audit
- Use cases where consent is helpful
  - To provide selective release of values
  - To permit user control over their privacy
  - To encourage applications to be privacy-preserving

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 : Allatan

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

A compilation of consent requirements

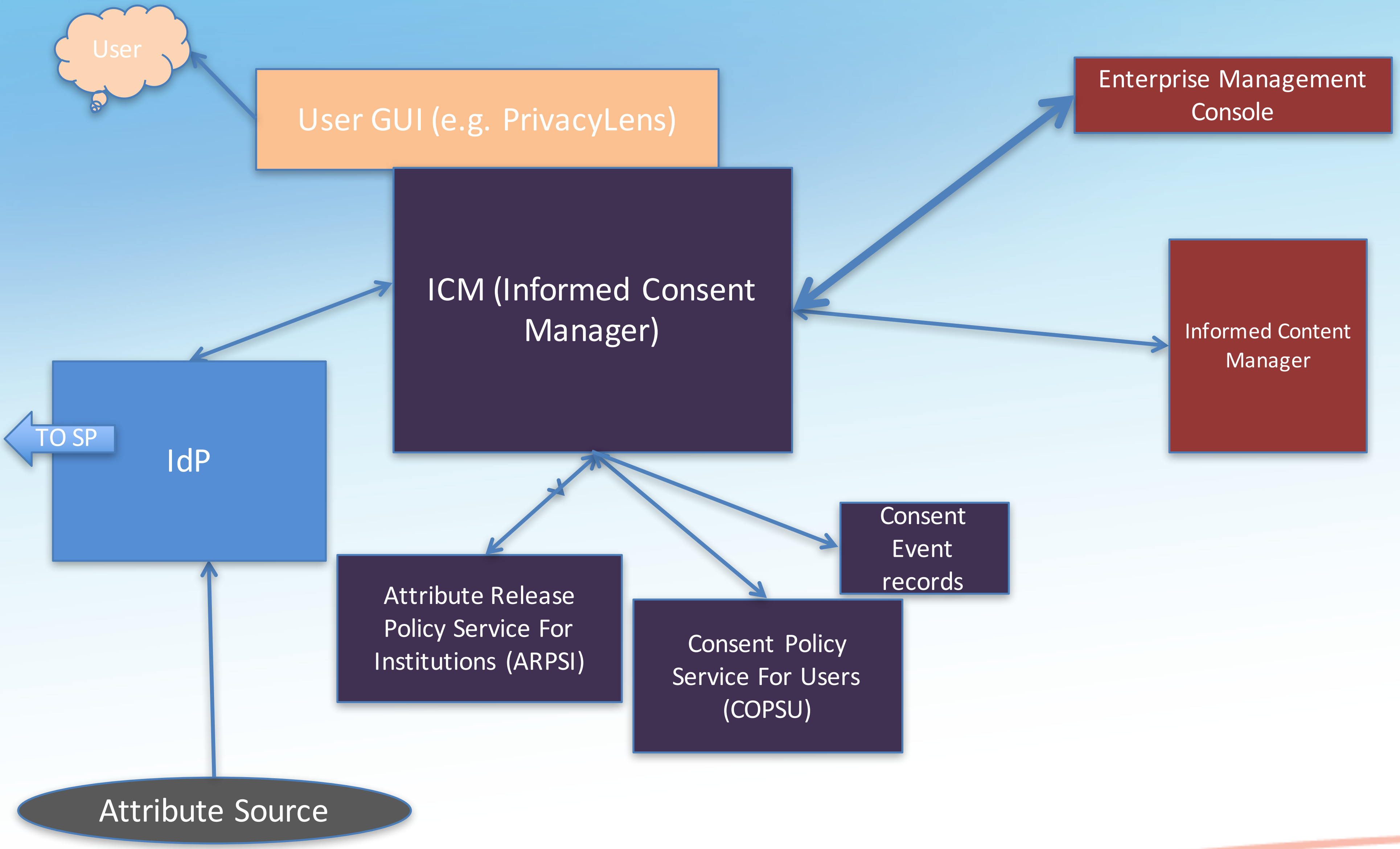
- Capabilities
  - User-centric consistency across use cases, protocols and technology environments
  - Support a variety of on-line/offline, one time and ongoing consent requests
  - Fine-grain attribute release with meta-attributes possible
  - Support for informed content
  - Support consent event records for audit, histories, etc.
- Presentation
  - Clear affirmative actions
  - Multi-lingual and accessibility support
  - Informed content access
    - Icons for IdP, RP, trustmarks, etc
    - Human-readable values for attributes and values, etc.
    - Links to privacy policies, dialogue boxes, etc
- User administration
  - Management of consent – revocation, automatic reconsent triggers and use of notification service
  - Support for identity portability among IdP’s

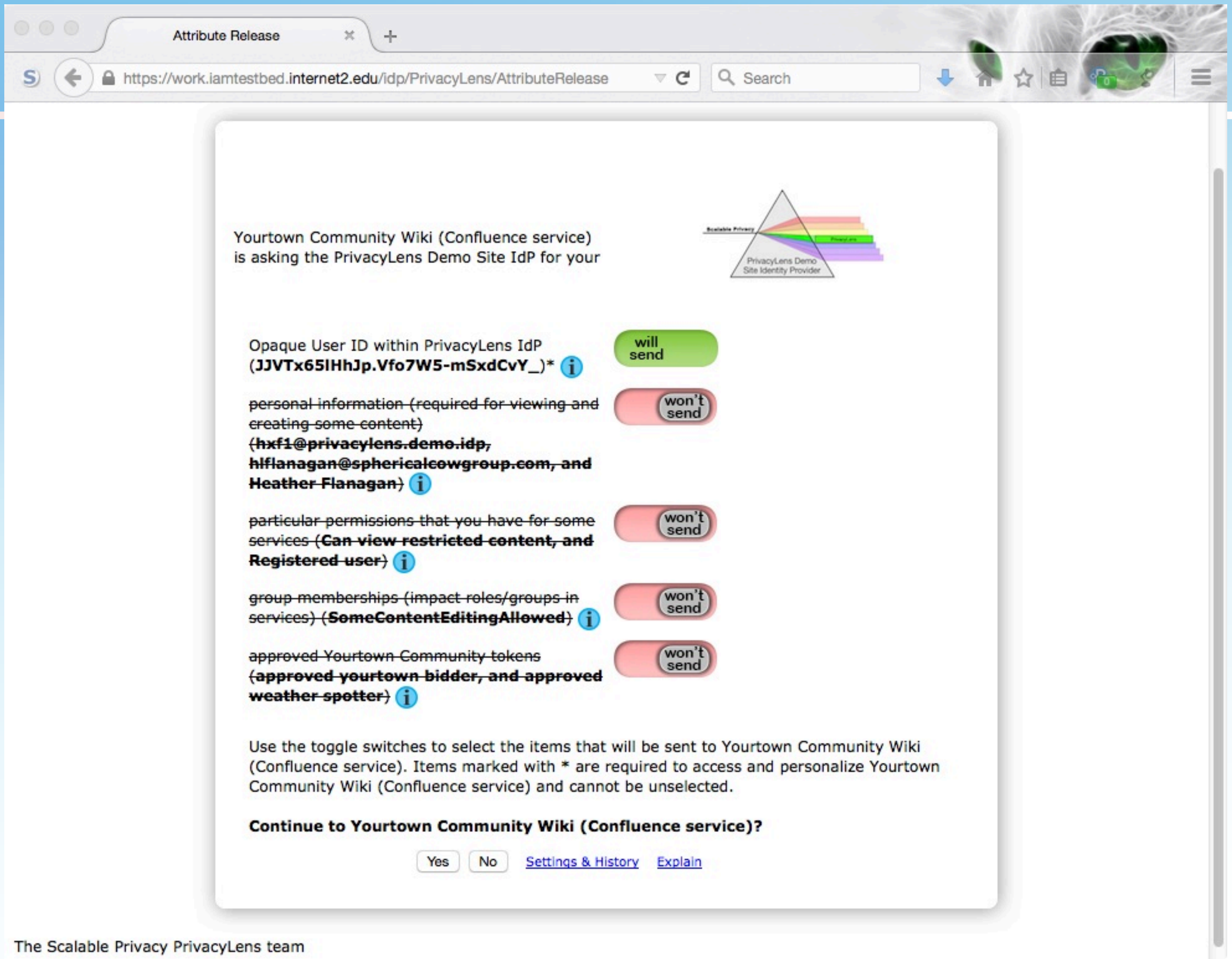
Consent options

- Per application, brokered by device OS (e.g. mobile) or via web
- At an identity provider
  - Client side storage
  - Shib IdP v3 server side
  - Consent as a stand-alone multi-protocol service
    - Need shims for Shib
- Consent as a service

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 or permissions for applications to access personal data
- Rolling out over the next year as open source; part of TIER


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


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
- Rich policy issues
- Consent event records interacts with numerous use cases – notification requirements, user self-administration

Timelines

- API’s largely done and available now
- Workable code units for the API’s being developed by Duke
  - First modules to work with in August
  - Fullish complement of modules by the end of the year
- Available as consent as a service or integrated with an IdP
- Integration with Shib IdP a key issue
  - The Shib IdP attribute filter flows are different
  - Short-term shims being developed; long-term Shib Consortium is open to new flows and contributions
- Informed Content issues to be worked ongoing

Informed Content

- The fuel that drives effective and informed user consent decisions
- Limited, though extensible sets of marks, assessments, policies, etc.
    - Icons for IdP and SP
    - SP IsRequired and Optional Attribute Needs
        - SAML metadata today
    - Displaynames and values for everything
    - Trustmark information
    - Explanatory application-specific dialogue boxes (e.g. why attribute is needed)
    - Privacy and third-party use policy pointer
    - Additional information feeds
        - Vetted, self-asserted, reputation systems, etc

Informed content dimensions

- Data fields
  - Icons, required attributes, trustmarks, privacy policies, etc.
  - Federated agreements on syntax and semantics of attributes
  - Much doesn’t yet exist and driving a value-prop for it is uncertain
  - Easier for internal federations to manage
- Transports
  - SAML metadata, well-known URI’s, publish and subscribe mechanisms, etc.
  - Much to understand on the fit of transport to data to trust
- Trust management
  - Vetted, self-asserted, reputation system based
  - Structuring for human consumption

Next steps

- Identify and convene an ad hoc groups of those doing 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

Why might you be interested?

- Consent is part of the long-term IdM landscape
  - There are many situations where consent is not needed or explicitly not permitted by regulation (e.g. some GDPR use cases)
  - There are many situations where consent is useful or explicitly needed (e.g. p2p apps and some GDPR use cases)
- Internal federation use
  - Department to department or student to student app interactions
- Use with external services (replacing Google consent?)
- Doing the right thing is still important