Update on Consent

Rob Carter, Rich Graves, Ken Klingenstein, Keith Wessel
Topics

• Basics – kjk
  – Consent, Regulation, Appropriate Use
  – Current Options and Integration across attribute release situations
  – Consent-Informed Attribute Release (aka CAR, aka Scalable Consent)
• Carleton – Rich Graves
  – The “standard” FERPA use case
  – Deployment experiences
• Illinois - Keith Wessel
  – Use cases
  – Deployment decisions and experiences
• Duke – Rob Carter
  – Duke use cases
  – CAR rollout at Duke - “All in in Alphaville”
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

1. User Control and Consent
   Technical identity systems must only record information identifying a user with the user’s consent.

2. Minimal Disclosure for a Constrained Use
   The volume which discloses the least amount of identifying information and least 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 needing it, necessary, and justifiable for a given identity relationship.

4. Directed Identity
   A universal identity system must support both "unidirectional" identifiers for use by public entities and "bidirectional" 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 to ensure a user’s identity proactively.

6. Human Integration
   The universal identity system need deftly 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 single user ID mechanism must guarantee its users a simple, consistent experience while allowing separation of contexts through multiple operators and technologies.
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
    • Integration with Shibboleth
• Consent as a cloud service
• Integration across situations
  – External services
  – External IdP’s – Google, Azure/Office
• Goal: a consistent and effective attribute and information release experience for the user
Consent-Informed Attribute Release (CAR) Basics

- Components to create a scalable consent experience and infrastructure
  - Integrates institutional and individual choices for attribute release
  - Support for user consent decisions that are informed, effective, revocable, accessible, etc.
- Catalyzed by multi-year NIST grant to Internet2 and now a TIER component
- 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
- Includes a published API (ICM API) and HA code that implements the API
- Includes UI for end-users in a variety of use cases (in-line, off-line, persistent) and management UI for end-user self-service, policy administrators, configuration, etc.
Next-gen UI

CARMA (Consent-informed Attribute Release MAnager)

IdP

Attribute Source

User

Enterprise Management Console

Informed Content Manager

Consent Event records

Consent Policy Service For Users (COPSU)

Attribute Release Policy Service For Institutions (ARPSI)