Consent Manager Internals

6/27/15

Topics

- Approaches and issues with consent
- Noble principles to be captured in technology
- Buckets of needs
- Some use cases and requirements
- Pipelines and Possible components
- Enterprise manager considerations
- Adjacent issues
  - Minimal viable consent record at https://github.com/KI-CISWG/MVCR/blob/master/mvcr-0.6.md
  - UMA
- How do we proceed

Approaches and issues with consent

- It's proving hard to get the right attributes released
  - Institutions are attribute-retentive
  - International issues are hard
  - Liability impacts are uncertain
- Two approaches to consent
  - Institutional/organizational/IdP decision
  - End-user/individual decision
- Consent has adjectives: informed, accessible, revocable, fine-grain, etc.
- Related problems (e.g. selective release) compound the situations

Examples of problems we'd like to solve

a) Reduce occasions in which user is denied service due to lack of needed attributes.

b) Mitigate IdP institution's risk of providing PII outside of a context in which adequate protection can be expected.

c) Mitigate SP institution's risk of being sued by user for misuse of their PII.

d) Put privacy control in users' hands as a matter of principle, or to comply with conservative IdP institutional privacy policies

e) Design an app that can address problems like those above, regardless of whether it is actually used to address any actual problems.

Noble principles

- Revocation of consent
- Effective informed consent mechanisms
- Identity portability
  - Being able to move one's consent preferences from one IdP to another
  - Not necessarily portability of identifiers, attributes or authorizations
- Unobservability not part of this model, but non-correlating opaque identifiers are
- Auditability for legal or regulatory requirements
- Adding Privacy to Accessibility
- Widespread appreciation for the concepts of required vs optional attributes though it is neither technically implemented yet or marketplace tested.

Three types of “under the UI hood” needs

- Internal data stores
  - Attribute release policies per user
    - Cookies, db, other choices
  - Presentation to user support
  - Attribute mapping between sources and display renderings
- External data sources
  - Calls to federation metadata
  - Optional vs required attributes information
  - Selective release of multi-valued attributes support
  - XML distribution of attribute filters
- Interactions with everything
  - Orchestration with MFA
  - Callable from third party apps
  - API’s

End user consent requirements on internals

- Support for a variety of end-user notification/consent approaches
- Support for presentation to users for a variety of consent needs, from individual attributes to bundles
  - Custom attributes?
- Capability to see the values being released
- Multi-lingual support
- Mobile support
- Ability to release certain sets of attributes while not choosing to release others, on a per instance basis
- Ability to release certain values from a multi-valued attribute, on a per instance basis
- Capabilities to access a variety of informed consent sources, from hierarchical and structured consent to ad hoc reputation systems
- …

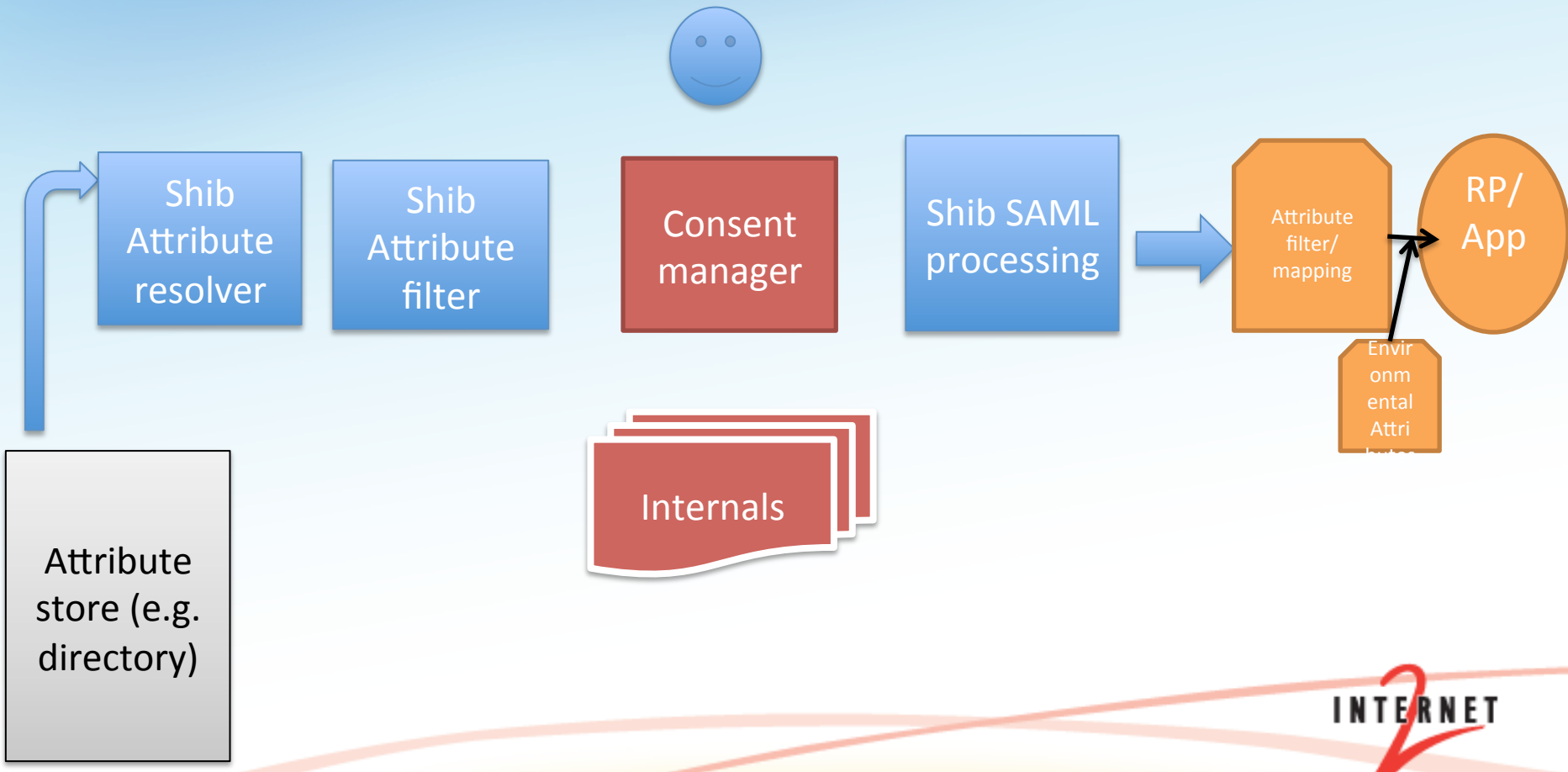
Enterprise IdP requirements

- Control the overall UI
  - Skins, logos, values being presented, etc
- Control what specific choices are presented to user on a per site basis
- Display human-oriented descriptions and values for geek-speak attributes
- Support for off-line release
- Create and manage attribute bundles
- Manage integration with MFA and other elements of the UX flow
- Create and maintain secure audit logs of releases for legal and regulatory requirements
- Providing access to attribute release policies for other applications
- Mapping between attributes in inter-federation contexts
- …

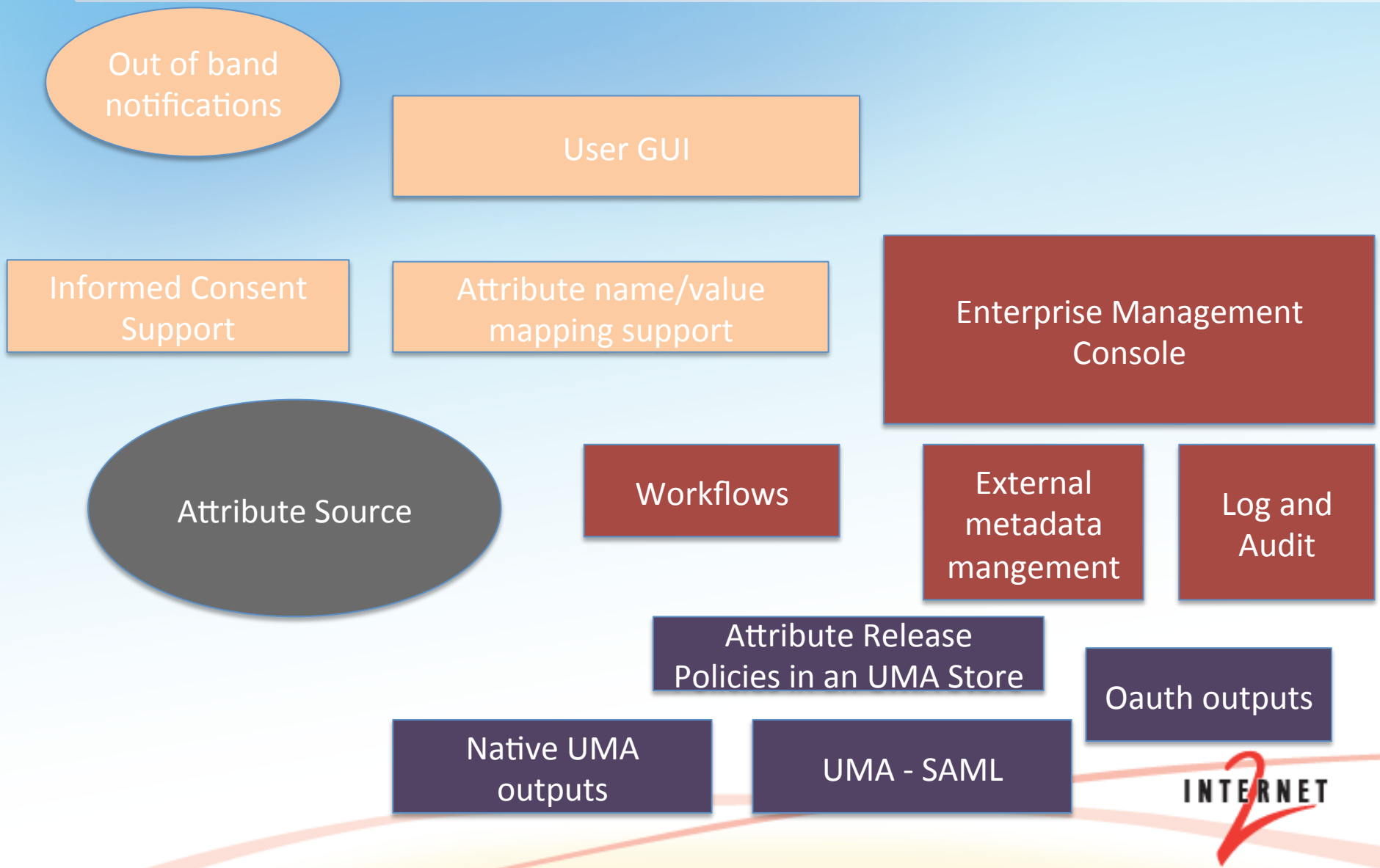
Trust and informed consent related requirements

- The user wants to view trust marks and other guidance for help on decisions
- The user would like a hierarchical format for informed consent for more detail if needed
- The user would like to use alternative forms of information for informed consent – reputation systems, etc.
- The enterprise wants to manage the sources of trust
- The enterprise wants to manage the standard informed consent dialogues
- …

The attribute pipeline in Shib



Components of a consent infrastructure



Components of a consent infrastructure

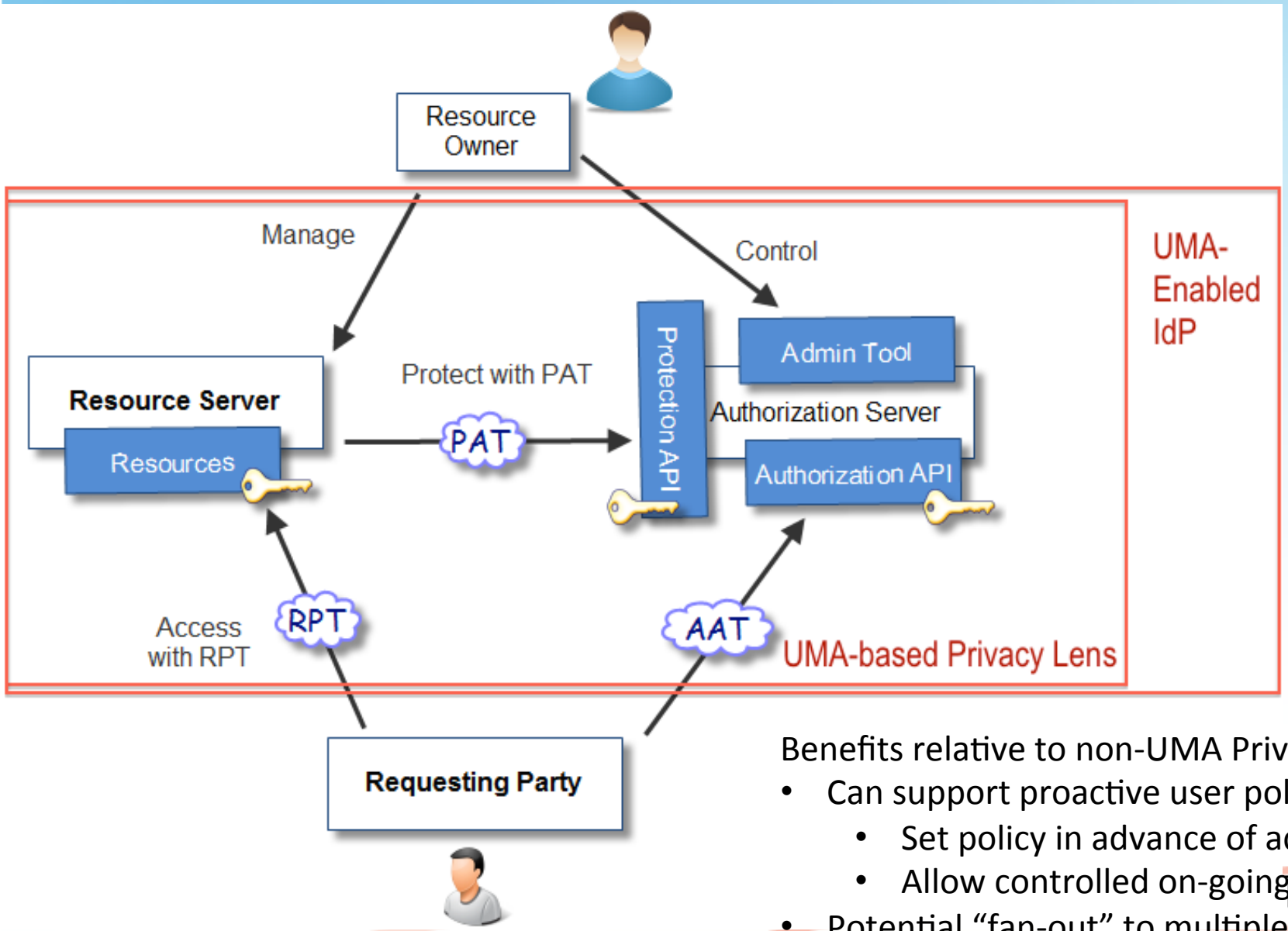
- Enterprise IdP Management Console
  - How much to combine with other IdP management needs (local IdP issues, federation issues, etc.)
  - How much to expose the consent options to other needs (Oauth, UMA, etc.)
  - UX for the admin
- Attribute release store
  - The engine block
  - API to access from other places
  - A good place to factor in UMA
- External access to metadata
  - Federated feeds for required/optional, informed consent dialogues, logos, end-entity tags
  - Local feeds for dialogues, attribute name/value translations, etc.
  - Likely to go beyond SAML metadata capabilities

More components

- Audit logs
- Attribute/name value translations from geek to understandable

INTERNET 2

Potential UMA-Based Privacy Lens



Benefits relative to non-UMA Privacy Lens

- Can support proactive user policy
  - Set policy in advance of access
  - Allow controlled on-going access
- Potential "fan-out" to multiple AAs
  - In a standards-based manner

Key functions - IdP Management Console

- Enterprise IdP Management Console Desirable features:
- Ability to control the UI design and user choices on a per SP basis
- Display of values being sent
- Display of SP Logo, etc
- Options for notification, consent suppression, frequency (e.g. one-time releases vs recurring releases), etc.
- Ability to plug in a variety of notification options
- Integration with revocation mechanism
- Ability to manage the informed consent info via API's, local stores, etc
- Ability to skin the UI
- Ability to change the UI
- Shib integration issues
- Managing audit logs
- Security for console
- Mapping attribute names, etc
- Interfacing with metadata
- Linking to informed consent mechanisms

Federation Services in Support of Consent

- Many federations create “recommended” attribute release policies per SP and distribute them to federation IdP’s.
  - https://www.switch.ch/aai/support/tools/resource-registry/
  - http://jagger.heanet.ie/
  - https://manager.aaf.edu.au/federationregistry/
- Hub-and-spoke federations do consent management at the hub, though that can be pushed out to the end-user.

INTERNET 2