Privacy Manager Activities

Topics

- Goals:
  - Design considerations
  - Prototypes
  - Feedback loops from test deploys and open source release
- Challenges
- Timeframes and deliverables
- Emergent issues

INTERNET2

Team

- CMU - Lujo Bauer, P.I., with engagement from EE, Center for Usable Privacy and Security, and central IT
  - Design guidelines, prototypes

- Internet2/InCommon and International
  - Drive

- Set of leader universities
  - To review design, drive policy, test and deploy

INTERNET 2

Key design considerations

- Usability

- Informed consent

- GPII

- MFA

- Awareness of out-of-band considerations

- Minimal disclosure for constrained purpose

INTERNET 2

Major milestones and deliverables (Y1)

- Initial set of reports
  - Lessons Gleaned from Warnings, Malware, etc
    - Some design considerations
  - Evaluations of common UI on design considerations
  - Informed consent, out of band consent, others
  - Bundles, contexts roles implications
  - Integration of anon credentials at a UI level
- General design guidelines for a PM
  - Based on reports, research, testing, etc.
  - Also integration of CPO, etc at enterprise level
- Fostering additional research
- Prototype development
  - Joint effort at CMU with EE and IT
  - Engagement with a pilot set for testing and feedback

INTERNET 2

Major milestones and deliverables (Y2)

- Architecture of a PM and integration with Shib IdP futures
- Integration of anon cred classic UI and federated UI
- Reengineering and redesign
- Inclusion of informed consent mechanisms

INTERNET 2

Campus participants

- A rolling set of players, but drawn from a set of pilot institutions
  - Privacy offices to review approaches, issues, etc
  - UI
  - Disability offices to review approaches

INTERNET 2

Privacy manager

- Informed consent
  - How much do we want to get into the deep waters
  - How to provide?
  - How to evaluate?
- Out of band (prior) consent
  - When to use?
  - How to implement?
- Other consent alternatives, including avoidance

INTERNET2

Consent

- When is consent not needed?

- Negotiated consent (non-binary)

- What does informed consent actually mean?
  - "Tell me more" provides clear information with a reason to trust
- What are the options for consent?
  - At the time of enrollment
  - Out of band but fresh
  - Per release

INTERNET2

Contexts, Bundles, Attributes, etc

- Contexts and their implications
- Bundle Models
- Attributes

INTERNET2

AccessforAll (AfA) Conceptual Model
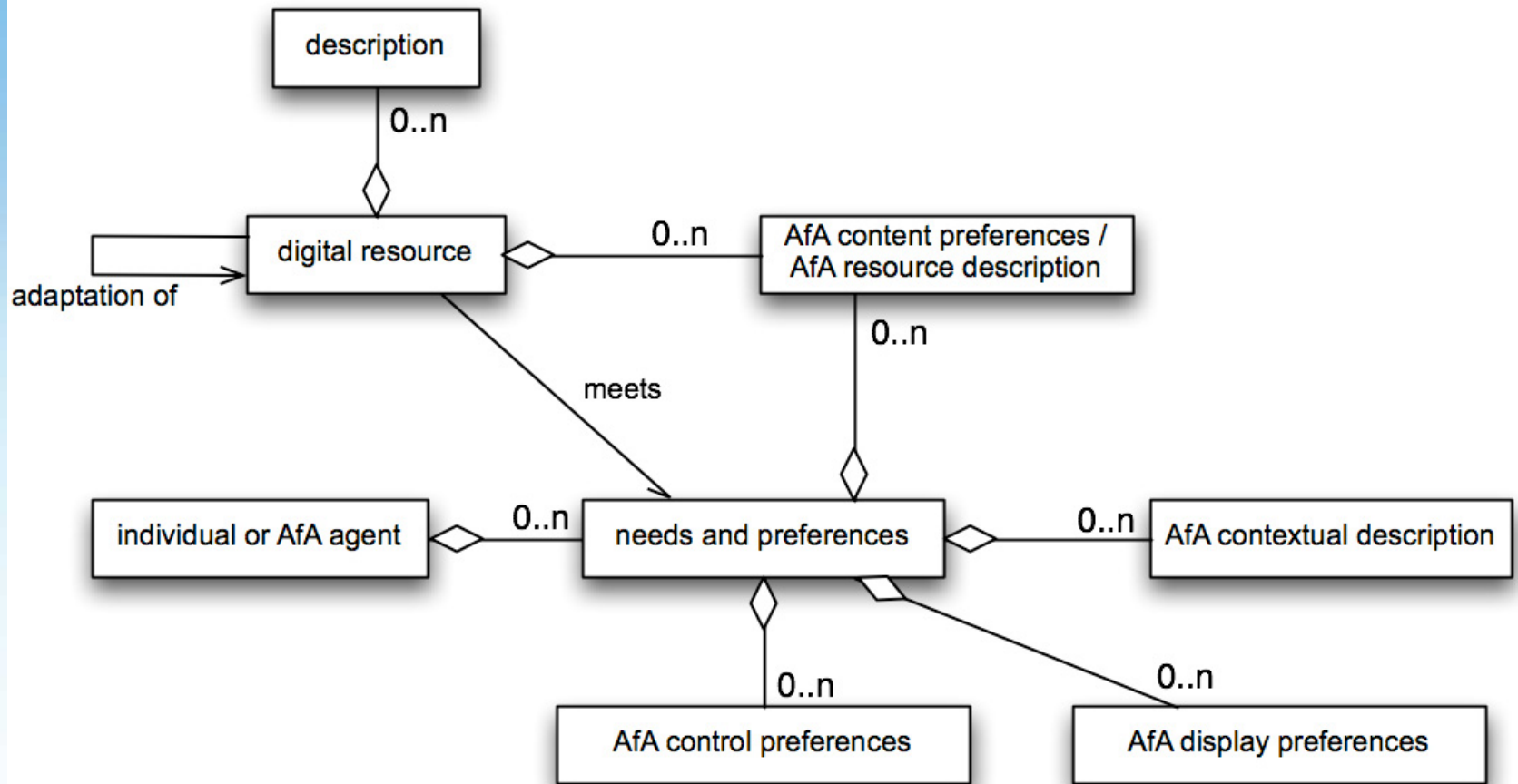
Emergent issues

Privacy Manager – Stage 1

- Who's involved:
  - CMU team {Cranor, Bauer, Gettes, RA's}
  - Architect advisory group

- Work items:
  - Assessing the current state of the art in privacy management
    - Collect approaches from Refeds and corporate side
  - Fact finding on architectural options
    - Where can privacy management be deployed in the ecosystem (e.g. browsers, portals, third parties, apps, relying parties, etc...)
  - Distilling the malware/browser/OS/other dialogues lessons on consenting
  - Identifying factors that influence short/long adoption cycles in UI
  - Investigating issues and approaches on translating technical attribute names and values to more understandable options
    - Is consent needed for releasing entitlements

INTERNET2