Impact of Requirements on Identity Management Solutions

Frederick Hirsch, 24 May 2011

Nokia, Co-Chair W3C Device APIs WG*

@fjhirsch

*Disclaimer: These slides do not reflect the official positions of Nokia and/or the DAP WG but only my personal opinion.

Conceptually simple requirements can have large implications on adoption

- Policy authoring (DAP experience)
- Credential provisioning (PKI etc)
- Discovery and centralized components
- Privacy and Security attacks considered (and not)
    - E.g., correlation among service providers

Lessons from Previous Work

- Liberty Alliance ID-FF, ID-WSF
  – Based on combined legal, business and technical requirements; circles of trust
  – ID-FF: Opaque pairwise name identifiers. Web redirection.
  – ID-WSF: Discovery Service, Interaction Service.
  – Controlled attribute exchange
- Cardspace/Infocard
  – User interface approach toward sharing information

General Requirements*

- Implemented universally, e.g. applicable to all browsers and web clients,
- Usability, including ease of discovery and use,
- User's choice should be persistent,
- Solution should be effective and enforceable;
- Applicable to variety of services.

*FTC DNT requirements Referenced in Adobe position paper, MeMe Jacobs Rasmussen, http://www.w3.org/2011/track-privacy/papers/adobe.pdf"

Additional Requirements

- Business Requirements
  - Incremental adoption, incentives for all stakeholders, time to market
  - Combination of technical and non-technical solution
- General Technical Requirements
  - Security, privacy, interop, scale
- Privacy by Design (and by default)
- Distributed system, no centralized control?

See also

- http://www.w3.org/2011/identity-ws/papers/idbrowser2011_submission_31.html
- http://www.projectliberty.org/
- http://www.identityblog.com/stories/2004/12/09/thelaws.html
- http://www.w3.org/2011/track-privacy/
- http://www.w3.org/2009/dap/

Thanks

Frederick.hirsch@nokia.com

@fjhirsch