Identity in the browser at 5. Lessons learned.

Paul Trevithick
paul@azigo.com
informationcard.net
higgins-project.org
Infocard in 60 seconds flat
Click: Card picker window appears
User clicks on a card

- IdP
- IdP
- IdP
- Browser
  - Plug-in
- Website
  - Policy
User authenticates to card/IdP
Token is retrieved and HTTPS POST-ed to site
Good & bad

• We got it right from the start
• We got it wrong at first but eventually got it right
• We still haven’t got it right
Capabilities

- User-centric and decentralized architecture
- Claims (attributes) not identifiers
- Self-asserted and third-party asserted claims
- Extensible schema
- Claims as URIs
- End-to-end crypto, audience restriction, verified claims
- Separation of token format from network protocol
- Browser-initiated (not SP-initiated) flow; anti-phishing protection
- Passive advertisement of website policy
- Privacy: minimal disclosure, pseudonym generation
User Experience

- Support for multiple identities (cards)
- Automatic card matching & filtering (no more NASCAR)
- Roaming support
- Cross-browser, cross-platform (including mobile)
- Unmodified browser support
- Cross-protocol: should have invested more in building bridges
- Finding the right balance
  - Transparency, notice & consent vs. usability
  - Performance vs. security
User Experience

• Dynamic claims (e.g. for payment use-cases)
• Claims aggregation
• Attribute/claim providers vs. identity providers
Driving adoption

- Put majority of resources on winning SPs/RPs (not IdPs)
- Avoid having a single, dominant vendor in the ecosystem