Consumer Third Party Authentication

Craig H. Wittenberg
W3C Identity in the Browser Workshop
May 24, 25 2011
Agenda

• Scenarios Classes
• Challenges
• Solutions
• Practical Next Steps
Scenario Classes

Transaction (verified information)

Claims Provider
- e.g. Government or Commercial entity

User
- Browser

Relying Party
- Service

Login

2-Party

AuthN Provider
- e.g., Commercial entity

User
- Browser

Relying Party
- Service

3-Party

User
- Browser

Relying Party
- Service
Challenges

Privacy
- Authentication events
- Tracking across sites

Reliability
- Availability
- Support

Brand Experience
Solutions

Privacy Friendly Login Certificates

Shared, Symmetric, Strong Secrets

Trust Frameworks
Practical Next Steps

• Identifier and shared secret (a.k.a. username and password)
  – Form field annotation
  – Change process, linking additional identifiers
  – Minimum standards for generation, encryption / sync

• Authentication trigger
  – For interactive user, 200 ok
  – For programmatic client, 401 or similar

• Trusted popup for user interactions
  – Align on visuals and mechanisms to trigger
  – Wide variety of scenarios enabled

• Crypto primitives in the browser
  – Start with functional features (SHA, AES, HMAC, random numbers, ...)
  – Enable encrypted storage based on variety of key types