Some Thoughts About Requirements

Dan Schutzer, CTO
dan@fsround.org
Financial Services Roundtable/BITS

W3C Workshop – Identity in the Browser
May 25, 2010

BITS
FINANCIAL SERVICES ROUNDTABLE

FSTC
FINANCIAL SERVICES TECHNOLOGY CONSORTIUM
FINANCIAL SERVICES ROUNDTABLE

Why now may be the right time for a change in authentication?

- Increasing sophistication and success of malware and cyber fraud
- Government drive
  - NSTIC
  - FFIEC Authentication Guidance
  - PIV-I roll-outs
- Social networks and increasing desire for secure and private sharing
- Emergence of the cloud and identity services
- Growth of apps and mobile

Barriers

- Historical precedence – hard to displace something people have grown used to
- Must be significantly easier to use
- Must be easy to interface to
- Must not add complexity, time or other difficulties
- Easy to integrate into existing applications
- Must offer some immediate benefits
- Help is perceived to be “cool”

Security needs for High Risk Applications

- Mutual authentication
- Trusted secure path– user, credential, device and web service
- Verify identity, authorizations, entitlements and privileges, with sufficient granularity
  - Can grant different privileges to end user and to their representative
  - privacy enhancing; e.g. decouple proofing from authentication
- Need to relate current transaction to past transactions, enabling current to be conducted in context with the past
- Able to detect, deter and prosecute fraud, while remaining privacy-enhancing

Requirements – Wish list

- Provide secure and reliable identification and mutual authentication of all parties
- Create secure trusted path between user, credential/device and web service
- Enable non-repudiation of transactions and information exchanges and support dispute resolution
- Able to maintain context across transactions
- Easy to evolve and adapt to future fraudster attack innovations
- Be perceived as compelling to users, providing greater convenience, security, privacy and other benefits
- Be open standards based, easily interfaced to applications and certifiable
- Be interoperable with respect to issuance/enrollment and authentication protocols, where strength is linked to standard known assurance levels
- Include necessary policies, rules and operation bodies to provide stronger trust

Requirements – Wish list

- Easy to interface to existing applications, optimally requiring no change
- Work with diversity of devices
- Offers some combination of lower costs to operate, lower liabilities, and demonstrated user demand
- Capable of supporting continuous improvement and innovation
- Be risk-based, such that one can escalate challenge when there is anomalous behavior
- Support decoupling of identity proofing process from authentication process
- Spoof resistant
- Support credentials that work off-line as well as on-line
- Built on top of existing infrastructure that ahs already achieved widespread market acceptance and critical mass