Some thoughts on Identity Management for Distributed Science

Von Welch

MAGIC Teleconference
October 5, 2011
This talk…

• Some thoughts on what we have created with PKIs/X.509
• Challenges of (federated) identity to support distributed science.
• Recommendations

Kudos to Jim Basney of NCSA for many contributions to the ideas in this talk.
Looking back at PKIs

• An impressive infrastructure of global interoperability.
• Usability has been the biggest failure. Revocation close behind.

The argument that certificates don’t belong in the hands of users is compelling.
Short-lived certificates based on existing IdM systems has done much to address this.
Lots of swimming upstream against dogma.
Looking back at PKIs (cont.)

• Events (Commodo, DigiNotar) showing incentives problems in commercial PKIs.
  This is a hairy problem. We need a better trust model that matches incentives.

• PKIs are still a good (if not only) answer for service and service-to-service authentication in distributed science.
  Maybe evolving in to a different form – DANE/DNSSec, SSH pubkey, Perspectives, etc.
IdM Challenges of the Distributed Science Community

• Privacy/Attribute release is a barrier to collaboration
  See TeraGrid experiences [1]
  EU laws and InCommon/Shibboleth de facto policy
  “Attribute bundles” will help in U.S.

• International collaborations
  IGTTF is only US-EU bridge
  REFEDS working on it

• Non-web applications
  CILogon/Moonshot/eduroam/ SAML ECP will solve
Challenges (cont.)

• Relationship with NSTIC, Social Ids
  Churns the waters. Friend or foe? http://xkcd.com/927/

• Adoption slow, Change slower?

• Acceptance by OpSec is a hurdle
  Need to demonstrate trust and risks are understood.
  People are not used to outsourcing these things.

• Compelling Vision
  I’ve tried [2]. Hard to make compelling for the scientist.
  Is this IT house keeping?
Recommendations for MAGIC

• Foster international interoperability

• Define community requirements
  E.g. LOA comes from Risk, risk comes from assets, which are increasingly data, but I know of no data security needs assessment.
  E.g. Should we be leveraging outside IdM rather than rolling our own? If so, what would we need from InCommon, OpenId, NSTIC, etc.?

• Monitor Moonshot/SAML ECP and jump in and support winner at appropriate time
References
