CIC + Friends InC Silver doc group -- May 17, 2013

- Roll call

Ann West -- Internet2
Ron Thelen -- Chicago
Jeff Capehart -- Florida
David Badger -- Rutgers
David Barks Maryland
Mary Dunker -- Virginia Tech
Phil Tracy -- Northwestern

- Security considerations for SAML 2.0 -- Jeff Capehart, U. of Florida
  - relationship of this document to IAP and IAAF
  - relationship of IAP and IAAF to SAML and Shibboleth
  - are all institutions using Shibboleth/SAML 2.0 to implement Silver/Bronze technically?

Shibboleth --
SAML 2 -- use all these features --
audit side -- assertion data -- digitally signed/encrypted, or transmitted directly between SP and IdP
client and web browser takes it and hands it to the IdP -- SHA-1 digital signatures
SHA-1 disallowed after this year -- no longer approved algorithm -- or accepted alternative means statement -- because SHA-1 is so ubiquitous -- Ron plans to submit alternative means statement on this
version 3 of Shib is working on SHA-256
SHA-1 deprecated in 2010 -- by NIST -- stronger algorithms need to be used for digital signature
ADFS -- have to downgrade from SHA-256 to SHA-1 to work with Shibboleth
valid from implementor standpoint as well as developers of the tools
checklist of Shib countermeasures

Mary Dunker --- Educause security guide

- Round robin
  - MSU
    InCommon Silver officially tabled
    Position with regard to federation in general is under heavy review, though I believe MSU will continue our involvement
    series of IdM strategy meetings will continue
    Jim -- new job -- Manager, Infrastructure Planning
    Will be disengaging from IdM largely, may still participate on advisory committees, etc.
    We are looking for a volunteer to take over leadership of this group
  - Chicago
    working with auditors
    refining our management assertions
    interesting process
    alternative means statements
    doing several things in parallel
    may put the audit on hold til later in the summer
    will be able to share managment assertions later
    encryption algorithms
    Silver AD working group also doing encryption algorithms
    audit certain events on the network and remove Silver status if they pop up in the audit
    if you find credentials transmitted in the clear
    your client might do LDAP binds to AD entirely in the clear
    settings on both the client and server side -- catch misconfigured client through audit process
    VLAN solution -- part of IdMS infrastructure uses a backnet that is not protected but is completely private
  - Rutgers -- have not spent a lot of time -- U. of Medical and Dental of NJ -- integration done July 1
    planning stage -- hopes of starting to work on it as far back as September -- but got back burnered
  - John Pfeiffer Maryland -- have been reading up and doing some research -- there is definitely interest
  - Mary VT -- need to be sure that they comply with 1.2 spec
    begun to write up alternative means -- Safenet e-token digital certificate 2-factor tokens.
  - Florida -- Jeff -- reviewing draft gap analysis report -- not going to meet it with existing 2 issues Bronze 6 issues Silver
    probably be out next week for managment to look at
    approved algorithms
    protected channels
    AD meeting alternative means
    back end channels with IdMS systems -- not well documented
  - Phil -- Northwestern -- in the gap analysis phase

Ron -- documentation showed links of systems but didn't show channel protection methods in detail

- Ann -- AD group -- updated cookbook
  alternative means -- creative ways of how to address requirement
  VT -- doc group discussions -- were helpful to them

GSA -- Bronze and SIlver great but we think we'll need even higher levels of Assurance ~~-- CIO Forum and Internet2 --~~ FICAM presentation
Obamacare -- how to exhcange health records -- security and assurance around that -- patient record access -- will be LOA 3 -- looking at really multi-factor -- disconnect between the FICAM profiles and what the agencies are coming out and saying -- "OK with LOA2 + multifactor" LOA3 is going to be where a lot of the interesting services are going to be