Topics

- Assurance levels, “frameworks“, interparty liability
- Tokens: mobile; smartcards; browser, etc.
  - PKI, non-PKI
Assurance levels, “frameworks“, interparty liability

PKI

– FBCA
  • Six increasing, qualitative levels of assurance: Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High.
  – Also Medium Hardware Commercial Best Practices (CBP) Assurance Requirements

Non-PKI

– FICAM
Non-PKI TFPs

**FICAM certified**
- LOA 1 – OIX
- LOA 1-2 – InCommon
- LOA 1-3 – Kantara
  - Certification program for IdP/CSP in place and operating
  - At least one IdP in process
  - TFP Only

**In process**
- LOA 2-3 – SAFE-BioPharma Assn
- In TFET review
- Certification program defined and will be operational upon FICAM certification
- Also issues both PKI and non-PKI level 2 and 3 credentials
Interparty Liability

SAFE-BioPharma
- Closed membership association
- Dispute resolution process governs adjudication
  - Agree not to sue but rather arbitrate
- Liability covered under Operating Policies and Member/Issuer Agreements
  - Specific caps related to credential management only
  - Does not cover use of credentials

Other TFPs
- Part of why we are here
Authentication and credentials

PKI is covered by the FBCA CP and CPS
- Multiple certificate types
- Hardware, software and roaming
  - Roaming currently classed as software by the FBCA
  - Moving to cloud-based solutions – SAFE-BioPharma/Verizon offering cloud-based HSM protected certificates

Non-PKI
- NIST SP 800-63
- Issue – currently approved version dates to 2006 and is technically out of date and does not recognize non-PKI multi-factor tokens
- Much of industry working with the Dec 2008 (now Jun 2011 draft)
  - Includes much broader definitions of acceptable tokens at various LOAs
Token types

- **Who is doing what and how?**

- **PKI**
  - Smartcards, USB hardware tokens, software tokens on machines/mobile devices, cloud HSMs

- **Non-PKI**
  - LOA 1&2 – memorized secrets, pre-registered knowledge tokens
  - LOA 2 - look up secret, out of band, SF one-time password device, SF crypto device
  - LOA 3 – multiple tokens (NIST SP 800-63 (June 2011 draft), Table 7)