NSTIC Day

How does industry drive forward
Topics

- **Topic C:** Assurance levels, “frameworks“, interparty liability
- **Topic D:** Device-specific methods: mobile; smartcards; browser DNT, etc.
  - PKI, non-PKI
Assurance levels, “frameworks“, interparty liability

**OMB 04-04**
- Level 1: Little or no confidence in the asserted identity’s validity
- Level 2: Some confidence in the asserted identity’s validity
- Level 3: High confidence in the asserted identity’s validity
- Level 4: Very high confidence in the asserted identity’s validity

**NIST SP 800-63 provides additional guidance per level**
- Registration and identity proofing
- Tokens
- Token and credential management mechanisms
- Protocols used to support the authentication mechanism between the Claimant and the Verifier
- Assertion mechanisms
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
  - Levels 1-3
Non-PKI TFPs

- **FICAM certified**
  - LOA 1 – OIX
  - LOA 1-2 – InCommon
  - LOA 1-3 – Kantara

- **In process**
  - LOA 2-3 – SAFE-BioPharma Assn
  - Under TFET review
**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- Issue – currently approved version dates to 2006 and is technically out of date and does not recognize non-PKI multi-factor tokens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)