US eGov Update:
Unofficial, but with a good view
Topics

• Refeds influence if not consequence
• White House MFA announcement
• Egov and InCommon
• Other pilots
  – High assurance in low value
• Trust marks
  – Human vs machine readable
  – Granularity vs. Composition
• ISOC Utrecht meeting
  – Snowden and insider threats
  – VOTC and Attribute metadata
• Attribute bundles
• PL as a paradigm
US Government Identity Activities

• **FICAM**
  - Classic identity services for government; moving “forward”
  - Includes high assurance PIV cards and PKI, federated identity, the F6 Gateway, etc.
  - Provides the LOA certifications that motivate the InCommon assurance program, including Silver and Bronze

• **NSTIC**
  - Aimed at Next Gen – services, privacy, etc.
  - Has distinct governance and pilots efforts
  - Scoping is a finesse: affecting government identity interactions (along with FICAM), influencing a commercial marketplace, influencing a global identity ecosystem
  - Scalable Privacy, a grant to Internet2, is one of the pilots
  - [www.nist.gov/nstic](http://www.nist.gov/nstic)
White House announcement

  - Part 1 outlines chip and PIN (or other "enhanced security") for federal agencies accepting payment cards
  - Part 2 outlines additional outreach and remediation for citizens related to identity theft
  - Part 3 outlines second factor requirements and stronger identity proofing related to accessing federal systems that contain personal data
- Will it have consequence?
Attribute bundles

- Attributes that tend to travel together – are typically used in concert by classes of applications.
- A bundle to service R&S:
  - personal identifiers: email address, person name, eduPersonPrincipalName
    - where email address refers to the mail attribute and person name
    - refers to displayName and optionally givenName and sn (i.e., surName).
  - pseudonymous identifier: eduPersonTargetedID
  - affiliation: eduPersonScopedAffiliation
- A bundle to resolve identity:
  - Legal First Name Legal Last Name Middle Name or Initial
  - Current Address: (Parsed and Full)
  - Date of Birth: (Parsed and Full)
  - Social Security Number: (Parsed and Full)
  - Email Address
Attribute Bundles

- Akin to scopes in OpenId Connect
- To manage developers desire to have it all and liability issues, etc.
- To manage users abilities perform meaningful consent
  - Front and center issue for UI
- How about two flavors of ice cream and a few add-ins?
  - Vanilla – privacy preserving
  - Chocolate – core set of identity attributes
PrivacyLens as a paradigm

• Enabling effective and informed end-user consent
• Embraces a set of capabilities
  – Hierarchical information, fine grain control, bundling, revocation of consent, flexible notifications, etc.
• Embraces a style of presentation
  – Clear screens and slides
  – Optional display of values being sent
  – Affirmative user actions
• Embraces a variety of platforms and management approaches
  – Protocol-agnostic
  – Enterprise management consoles and management
  – Audit and security logs