Government-University Identity Management Opportunities

Peter Alterman, Ph.D.

Chair, U.S. Federal PKI Policy Authority and

Assistant CIO/E-Authentication, NIH

Current State of Affairs (60 years old now)

- You apply to the application owner for a password
- You use the password to access the system
- You forget the password
- The application owner gives you a new password
- You use the new password to access the system
- You forget the password
- <infinite do loop>
- No identity proofing
- No way to know who is actually on the system (Your

Foundational Assumption

- *Government online services shall trust externally-issued electronic identity credentials at known levels of assurance (LOA)*

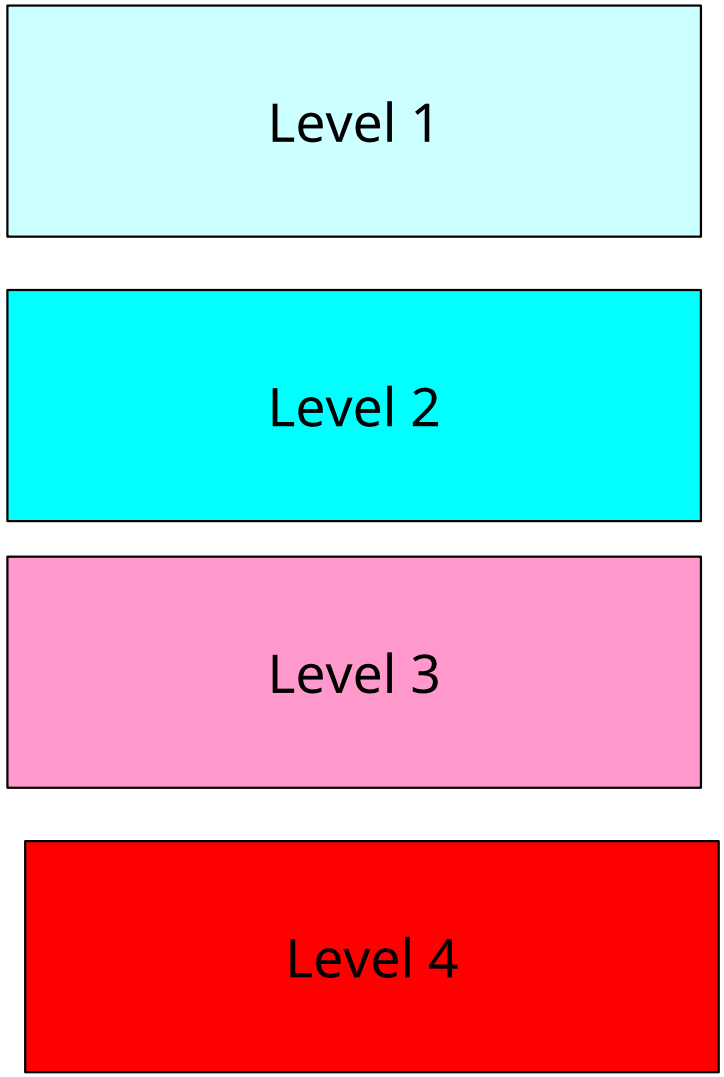
- *Online applications shall determine required credential LOA using a standard methodology based on:*

  Risk assessment using standard tool,

  OMB M-04-04 determines required authN LOA

  NIST SP 800-63 translates required LOA to credential technology

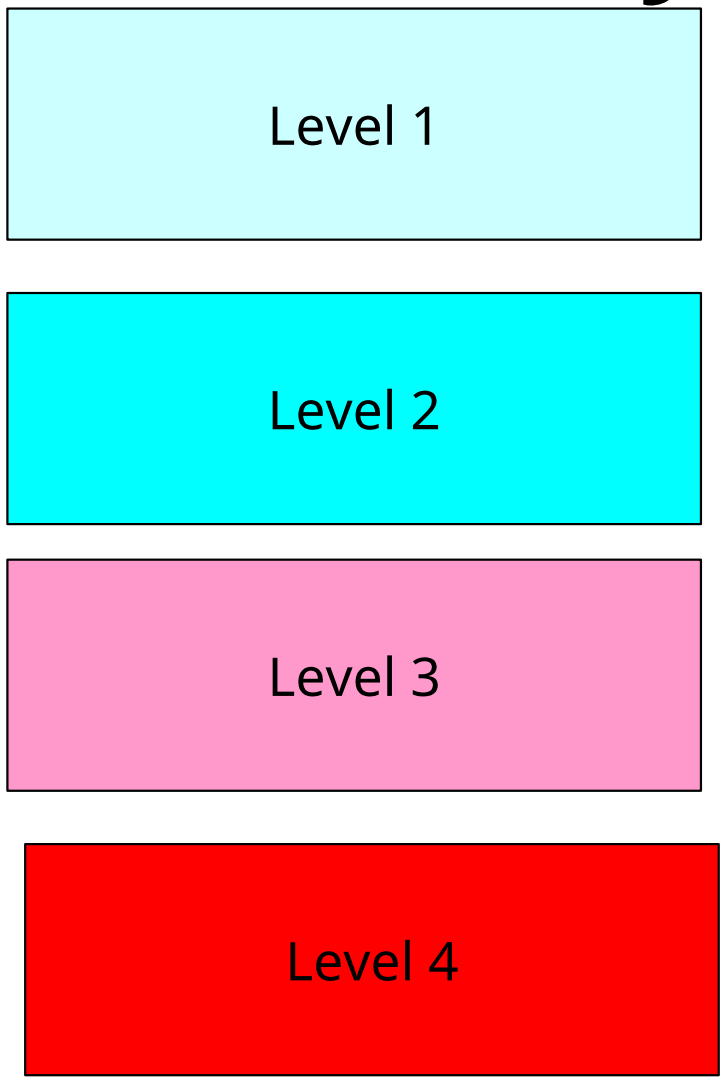
E-Authentication LOA and What They Mean



- Little or no assurance of identity; assertion-based identity authentication
- Some assurance of identity; assertion-based identity authentication or policy-thin PKI
- Substantial assurance of identity; cryptographically-based identity authentication
- High assurance of identity; cryptographically-based identity authentication

**** Codified in OMB Memorandum 04-04***

*E-Authentication LOA and What They Service***



- Online applications with little or no risk of harm from fraud, hacking; low risk
- Online applications with risk of some harm from fraud, hacking; some risks
- Online applications where there is risk of significant harm from fraud, hacking; significant risks
- Online applications where there is risk of substantial harm from fraud, hacking; substantial risks

*** Codified in NIST SP 800-63***

General Considerations for Determining LOA of an Electronic Identity Credential (EIC)

- **Identity Proofing** – *how sure are you that the person is who he or she claims to be?*

- **Identity Binding** – *how sure are you that the person proffering the EIC is the person to whom the credential was issued?*

- **Credential integrity** – *how well does the technology and its implementation resist*

Summary of Lower-Level Identity Credentials

- **Level 1**: *UserID/Password, SAML assertion (XML text)*

- **Level 2:** *"High entropy" UserID/Password; "policy-lite" PKI, e.g., Fed PKI Citizen and Commerce Class & Federal PKI Rudimentary, TAGPMA Classic Plus (in development)*

Summary of Cryptographic-Based Identity Credentials

- **Level 3:** *One-time Password; Substantial assurance PKI at FPKI Basic, Medium*

- **Level 4:** *High assurance PKI at FPKI Medium Hardware, High*

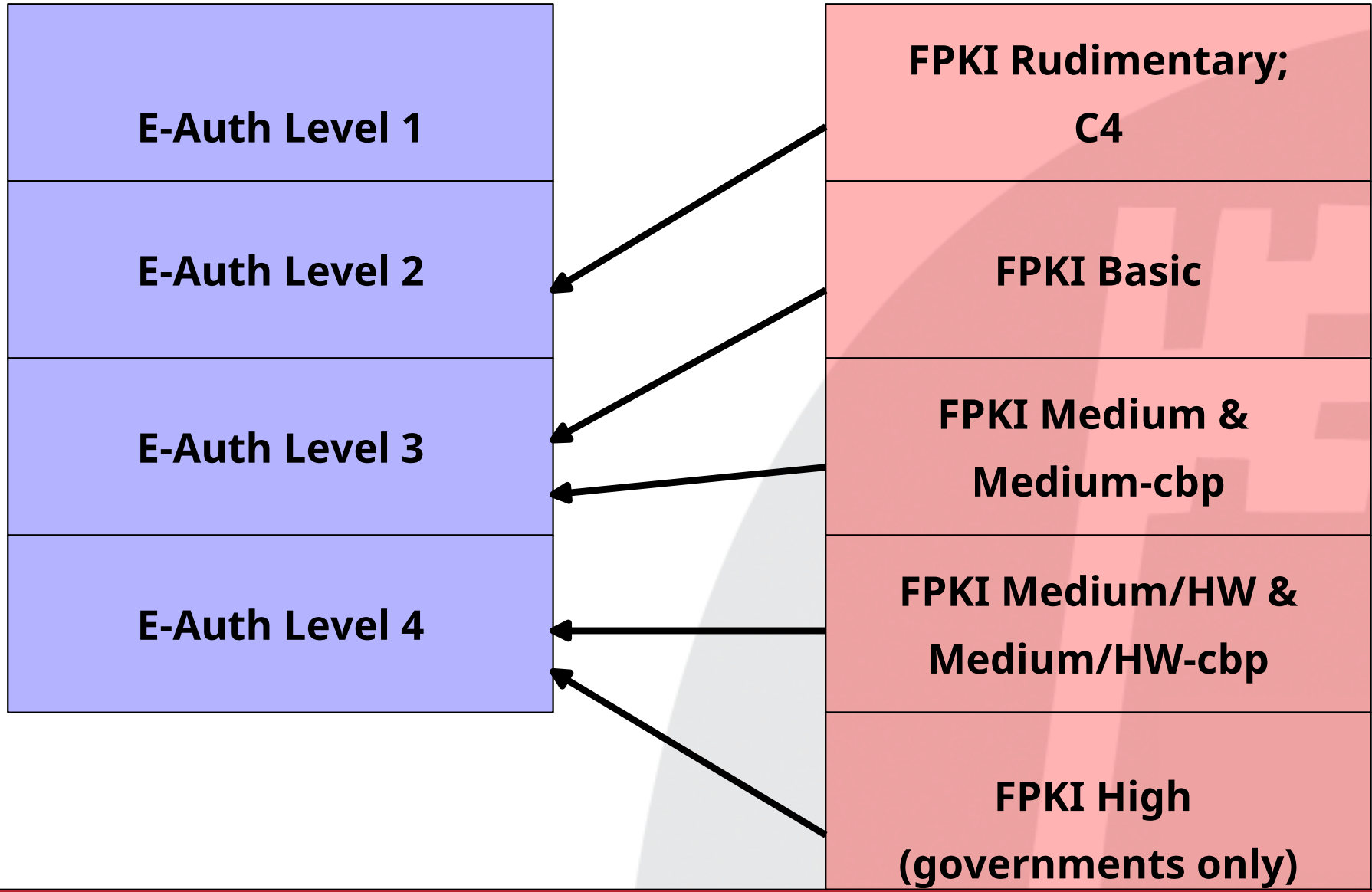
A Little Complication

- The government has TWO LOA classifications:

  Federal PKI LOA codified in the Certificate Policies of the Federal PKI Policy Authority

  E-Authentication LOA codified in OMB M-04-04

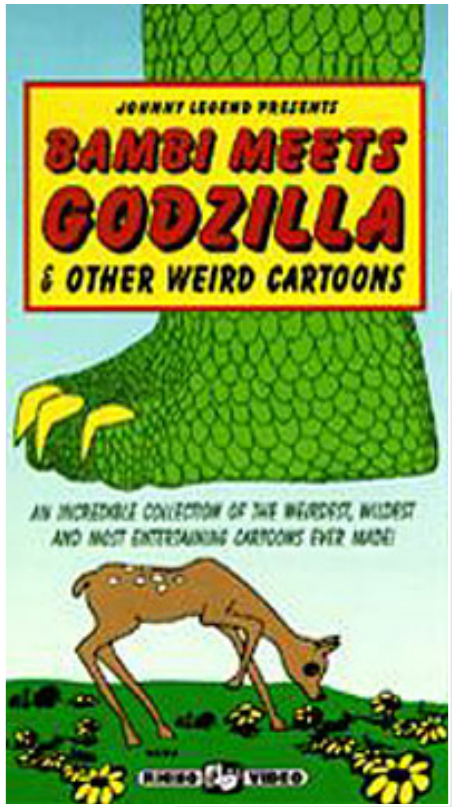
LOA Mapping E-Auth to Fed PKI



How Can A School Credential be Trusted and Used by a Government Application?

- **Preferred path** - School joins an Identity Federation that has policy and technology interoperability agreements with E-Authentication Federation
- **Requirements –** Each Federation agrees to ensure its members operate according to minimum requirements for members of the other's Federation.
  - *Presumes substantive policy, technology and management commonality*
- **Alternate path 1 –** School becomes a member Credential Service Provider (CSP) of the E-Authentication Federation directly, signing on to the Federation's technology, business, operating and legal requirements
- **Alternate path 2 –** One-to-one relationships (*sssh!*)

US Government E-Authentication Interfederation Model



E-Authentication Federation Membership Requirements

- Credential service providers [CSP] submit to credential assessment and evaluation of LOA

- Both Application providers and CSPs sign on to Federation business and operating “standards,” legal agreements.

E-Authentication – InCommon Interfederation Status

- Candor requires this disclaimer: they're still trying to figure it out after two years and two tries

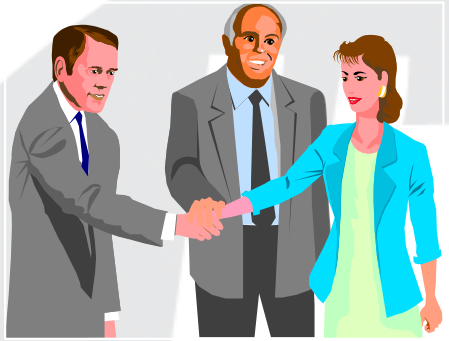
- Current status: Said to be getting close with inCommon. Policy-grounded MOA on the table and molding; technical interoperability targeted for SAML 2.0; USPerson profile analog of eduPerson profile in 2.0 version but still pretty much generic.

- inCommon needs to up its policy, procedures, documentation and audit requirements to play long-term

Fed PKI "Interfederation" Model

Fed PKI Cross Certification Process

- ***Application - LOA?***
- ***Policy Mapping***
  - Mapping Matrices online
  - Cert Policy WG mapping review
  - Collegial back and forth discussions
- ***Technical Interoperability Testing***
  - Testing Protocol online
  - Directory and profiles tested (LDAP and/or X.500)
- ***Review of summary of independent audit results***
  - Map CP –> CPS and CPS -> PKI Operations
  - Independent auditors, not FPKI auditors
- ***Whole process laid out in "Criteria & Methodology" document online***



FPKI Does Interfederate

- Cross-certified (test) with Higher Education PKI Bridge, 01/2002
- Cross-certified (production) with CertiPath – Aerospace Industry PKI Bridge at Medium Hardware (EAuth Level 4), 07/2006
- Cross-certification under way with SAFE-Biopharma PKI Bridge, Medium and Medium Hardware
- Processes and procedures spelled out in “Criteria and Methodology” Document online

Current Model for Assertion-Based Interfederation (still a work in progress)

- For E-Authentication Federation and InCommon to interfederate at LOA 1 (!), E-Auth is requiring InC to:
  - *upgrade its policy, audit and management infrastructure to comply with EAuth model, e.g., compliance with Credential Assessment Framework for LOA 1, signing Business and Operating Standards and sign Legal Agreement*
  - *Satisfy technical interoperability testing using SAML 1.0 technology, though work is proceeding to migrate to SAML 2.0 technology*
- InCommon has designated this state of operation "InCommon Bronze"
- Compatibility with E-Authentication requirements for LOA 2 is called "InCommon Silver"

What about Level 3 Government Apps Today?

- Universities issuing PKI-based electronic credentials may cross-certify with the Federal PKI at Basic Assurance or above
  - *Ex. MIT Lincoln Lab, University of Texas System (in process)*
  - *Usually 3 – 6 months*
- Or acquire digital certificates from a vendor currently cross-certified with the Federal Bridge at Basic assurance or above

Seeded Questions

- Q: What about the recent DOD notice that PKI individual certs are required for access to their web resources. Will DOD sites ever trust university-issued certificates for access or will we have to shell out $$ to get to them?
- A: If you think YOU are fussing about this, imagine how furious State Dep't. and NASA are. Imagine how furious their contractors are.
- A: We (Fed PKI) have been talking to DOD about this issue and we hope to see progress in 2007.
- Q: What the heck is "password entropy?"

*Password Entropy (Copied From Bill Burr)**

- Entropy is measure of randomness in a password
  - *Stated in bits, a password with 24 bits of entropy is as hard to guess as a 24 bit random number*
  - *The more entropy required in the password, the more trials the system can allow*
- It's easy to calculate the entropy of a system-generated, random password
  —But users can't remember these
- Much harder to estimate the entropy of user-chosen passwords

***NIST KBA Symposium, Feb. 9, 2004**

Resources

- www.cio.gov/eauthentication
- www.cio.gov/fpkipa
- http://csrc.nist.gov
- www.cio.gov/ficc

Notes

- 1.) How does your institution issue IDs? Is there a signature station requiring photo ID? What about non-resident scientists from Japan?
  2.) What is password entropy? Complex vs. long passwords. How often must they be changed? Can they be re-used? Pass dictionary test?
  3.) How secure is the authentication infrastructure? Can one person jeopardize the process? How are ID records stored?
  4.) How is the process documented? Are there templates to use as a framework that will pass Federal standards?