

IAB Identity Management Panel

May 6, 2009

Guiding Documents and Standards

- OMB M-04-04
- NIST SP 800-63
- Federal Public Key Infrastructure (FPKI)
- Security Assertion Markup Language (SAML)

Policy Foundation: OMB Memorandum M-04-04

Potential Impact Categories for Authentication Errors (Risk)	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

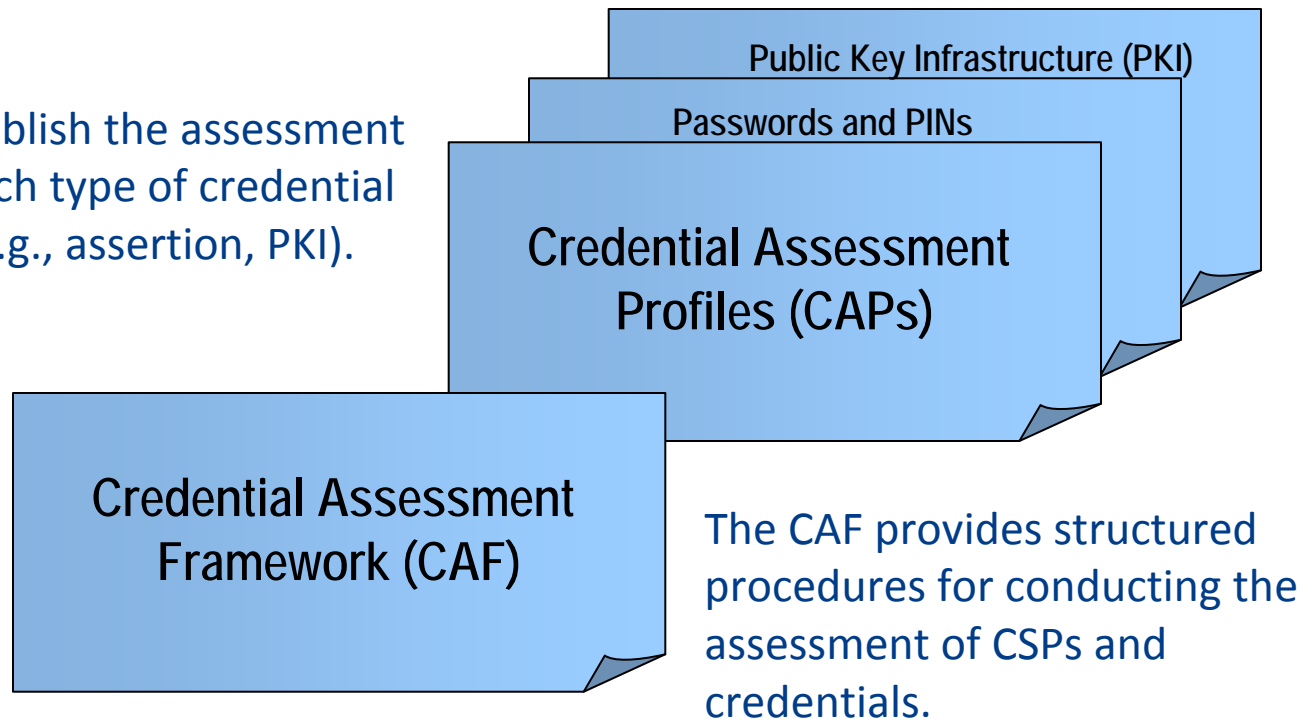
Policy Foundation: NIST Special Publication 800-63

Allowed Token Types	Assurance Level Impact Profiles			
	1	2	3	4
Hard crypto token	√	√	√	√
Soft crypto token	√	√	√	
Zero knowledge password	√	√	√	
One-time password device	√	√	√	
Passwords and PIN	√	√		

Note: Shaded tokens are not currently in use by the Federation.

The Credential Assessment Framework (CAF) Suite for Assessing Credentials

The CAPs establish the assessment criteria for each type of credential technology (e.g., assertion, PKI).



Based on OMB policy and NIST technical guidance, the CAF establishes the structured means for providing assurances to Federal agencies regarding the veracity and dependability of identity credentials.

E-Government is a Necessity

- Americans want their government to be accessible online:
 - 78% of Internet users (more than 166 million Americans) have visited government websites to seek information and/or assistance (PEW)
- Americans want a cost effective government:
 - A 2004 study found that typical government service conducted in person is **230% More Expensive** than one conducted over the Internet (\$28 in person vs. \$0.65 over the Internet)
- Americans increasingly want to interact with our government online
- E-Government interactions must be **SECURE** and **EASY**



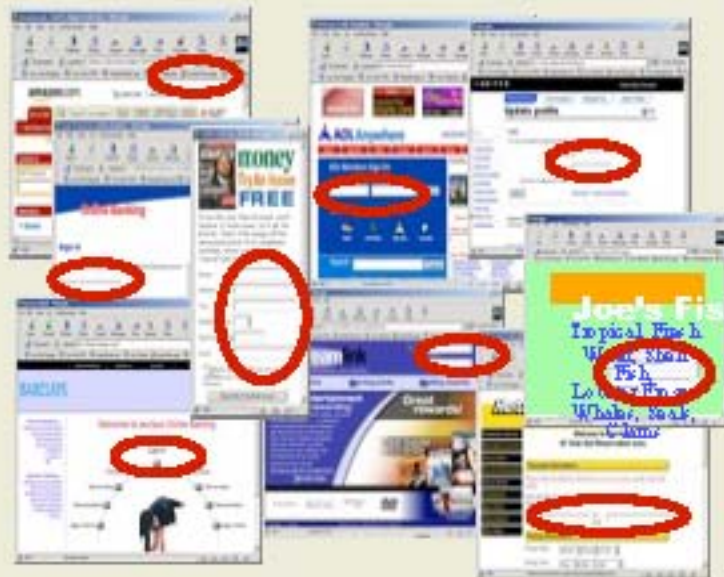
Today's Collection of Identity Silos

The collage illustrates various online identity silos, each with a highlighted login or registration form:

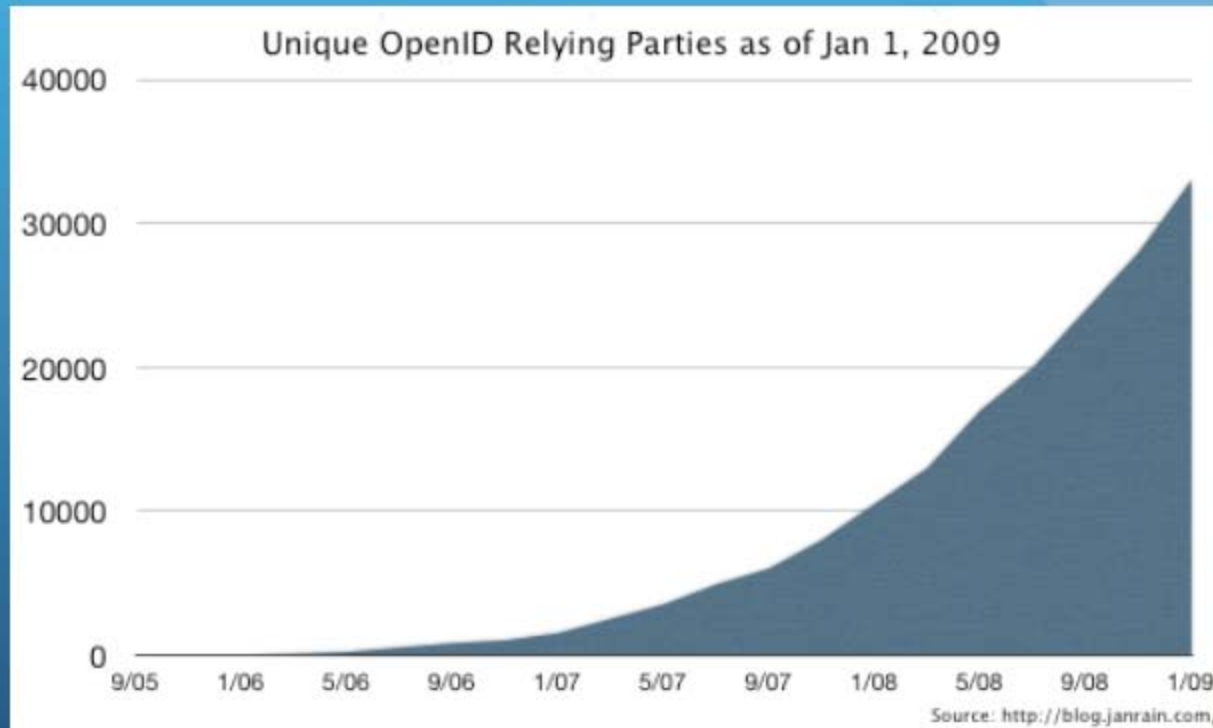
- Amazon.com:** "Forgot Message" link highlighted.
- Bank of America Online Banking:** "Sign In" form highlighted.
- AOL Anywhere:** "AOL Members Sign On" form highlighted.
- United:** "Update profile" login form highlighted.
- Joe's Fish Market.Com:** Registration form highlighted.
- Barclays:** "Log-in" form highlighted.
- Herzi:** "Welcome to the Herzi #1 Club Gold Reservation area" registration form highlighted.

What the User wants...

- **Simplified online experience**
 - Get rid of the need for multiple user-ids and passwords
 - Fewer clicks
- **Protected personal information**
 - Reduce my risk from fraud
- **Better product & service offerings**
 - Web 2.0 and/or “smart phone” data service integration



Over 35,000 OpenID Relying Parties



**from OpenID Foundation*

Identity Assurance Framework

- **What is it?**
 - Framework supporting mutual acceptance, validation and lifecycle maintenance across identity federations (i.e. systems that trust each other)
 - Started with EAP Trust Framework, UK *tScheme* and US e-Auth Federation Credential Assessment Framework as baseline
 - Harmonized, best-of-breed industry identity assurance standard
 - Identity credential policy
 - Business procedure and rule set
 - Baseline commercial terms
 - Guideline to foster inter-federation (i.e. inter-trust) on a global scale
- **It consists of 4 parts:**
 - Assurance Levels
 - Service Assessment Criteria
 - Accreditation and Certification Scheme
 - Business Rules/Deployment Guidelines