



Open Identity Trust Frameworks

Dec 1, 2011

John Bradley
Protiviti Government Services





Identity, Credential, and Access Management

Open Identity Trust Frameworks



Agenda

★ Standard Disclaimer

★ Background / Scope

▶ Goals / Drivers

▶ Policy Foundation

★ Trust Frameworks

★ Structure



Goals / Drivers

- ★ Principle focus on Government to Citizen
- ★ Support E-Government traction
 - ▶ Electronic methods are cheaper, easier
 - ▶ Authentication often necessary
- ★ Avoid credentialing of citizens
 - ▶ Costly, cumbersome to manage
- ★ “One more password” for citizens
- ★ Accept identity asserted from trusted commercial providers
- ★ Government instance of NSTIC Vision



Policy Foundation: OMB M04-04

Risk/Impact Profiles

Potential Impact Categories for Authentication Errors	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 Pub 800-63

★ SP 800-63 Technical Guidance

Allowed Token Types	Assurance Level			
	1	2	3	4
Hard crypto token	X	X	X	X
One-time Password Device	X	X	X	
Soft crypto token	X	X	X	
Password & PINs	X	X		



Non-PKI Approach: Scheme Adoption

★ Scheme Adoption

- ▶ Scheme – specific type of authentication token and associated protocols (e.g. user ID & password; PKI; SAML assertion)
- ▶ Scheme Adoption produces a Federal Profile
- ▶ Profile defines MUSTs, SHOULDs, SHOULD NOTs, etc. for Identity Providers (IdPs) & Relying Parties (RPs)
 - Goal is not to change the existing technical standard
- ▶ Profiles complete for OpenID 2.0, Information Card (IMI), and SAML. OAuth2 & OpenID Connect in Progress

★ Federal ICAM Identity Scheme Adoption Process and scheme profiles posted on <http://www.IDmanagement.gov/pages.cfm/page/Trust-Frameworks>



Non-PKI Approach: Trust Framework

★ Trust Framework Adoption

- ▶ Adoption of Industry Trust Frameworks
- ▶ Adopts at Assurance Levels
- ▶ Considers requirements of NIST SP 800-63
- ▶ Trust Framework Evaluation Team (TFET) reviews applications

★ Privacy Principles include

● Opt in	● Adequate Notice
● Minimalism	● Non Compulsory
● Activity Tracking	● Termination

★ Federal ICAM Trust Framework Provider Adoption Process posted on <http://www.IDmanagement.gov>



Non-PKI Approach: Trust Framework Adoption

★ Adopted Trust Framework Providers (TFP)

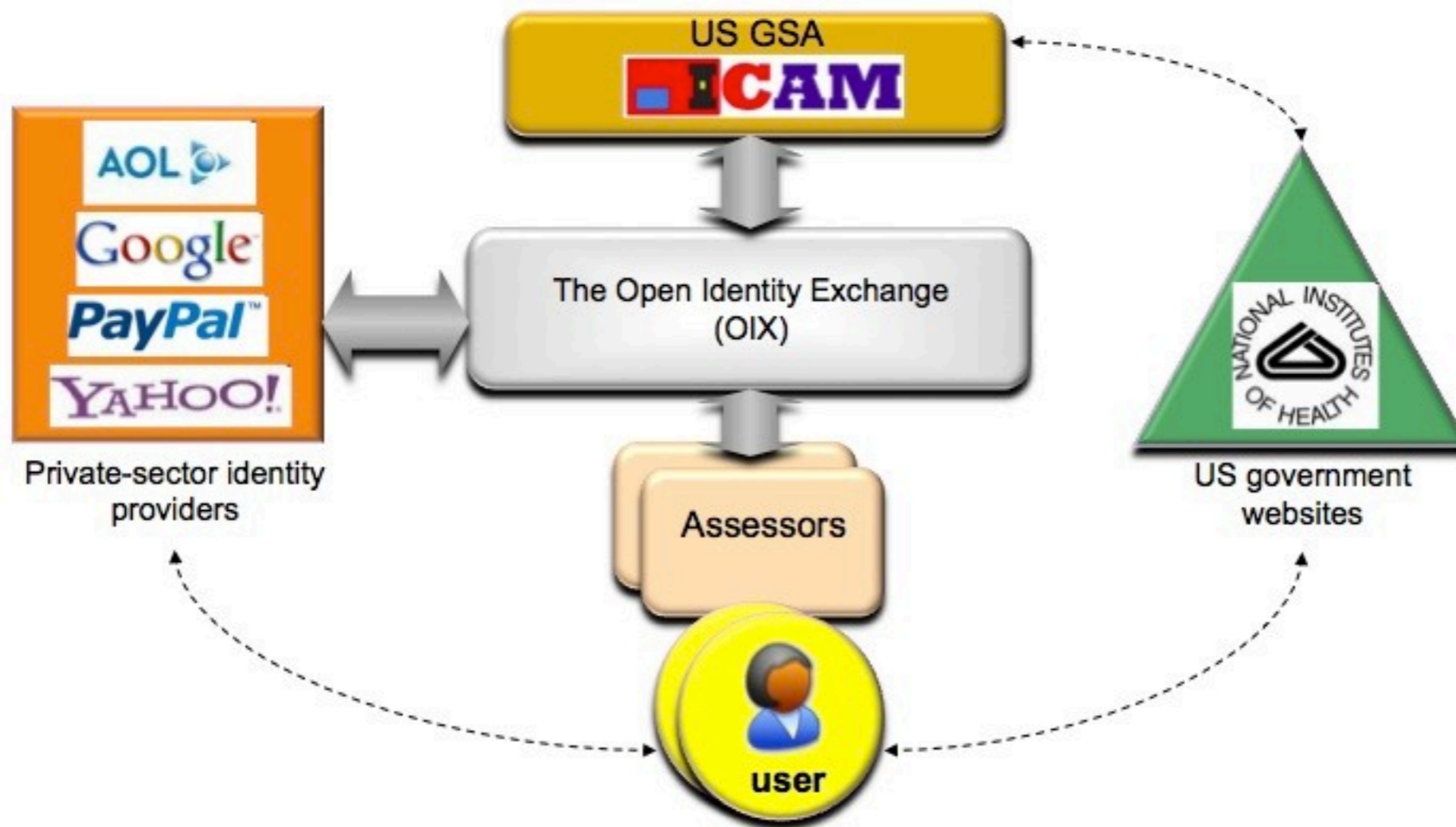
- ▶ Open Identity Exchange (OIX) (<http://openidentityexchange.org/>)
- ▶ Kantarra Initiative (<http://kantarrainitiative.org/>)
- ▶ InCommon (<http://www.incommonfederation.org/>)

★ TFP's are key

- ▶ Public / Private partnership
- ▶ Scalability



US ICAM Trust Framework





Non-PKI Approach: Trust Framework Adoption

Approved Identity Providers			
IDP	LOA	Scheme	TFP
Google	1	OpenID	OIX
Equifax	1	OpenID	OIX
Symantec	1	OpenID	OIX
Paypal	1	OpenID	OIX
Wave	1	OpenID	OIX
Verizon	3	SAML	Kantara



Structure

★ Identity Credentialing and Access Sub Committee (ICAMSC)

- ▶ Federal CIO Council
- ▶ Information Security and Identity Management Committee (ISIMC)

★ Trust Framework Evaluation Team (TFET)

- ▶ Assesses Trust Framework Providers
- ▶ Stakeholder Representation – DHS, FTC, GSA, IRS, NASA, NIH, NSS

★ Architecture Working Group (AWG)

- ▶ Scheme profiles

★ Infrastructure

- ▶ E-Governance Trust Services (EGTS)
 - Metadata, IDP Certificates