Federal CIO Council
Information Security and Identity Management Committee

Identity, Credential, and Access Management

Open Identity Solutions
Trust Frameworks

March 9, 2011

Chris Louden

Agenda

- Policy Foundation
- Portable Identity Approach
  - Technology
  - Trust
- Implementation

Policy Foundation: OMB M04-04

E-Authentication Guidance for Federal Agencies

- Defines 4 Assurance Levels
- *"Agencies should determine assurance levels using the following steps, (described in Section 2.3):*
  1. *Conduct a risk assessment of the e-government system.*
  2. *Map identified risks to the applicable assurance level.*
  3. *Select technology based on e-authentication technical guidance.*
  4. *Validate that the implemented system has achieved the required assurance level.*
  5. *Periodically reassess the system to determine technology refresh requirements. "*

Policy Foundation: OMB M04-04

FIPS 199 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

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

Agenda

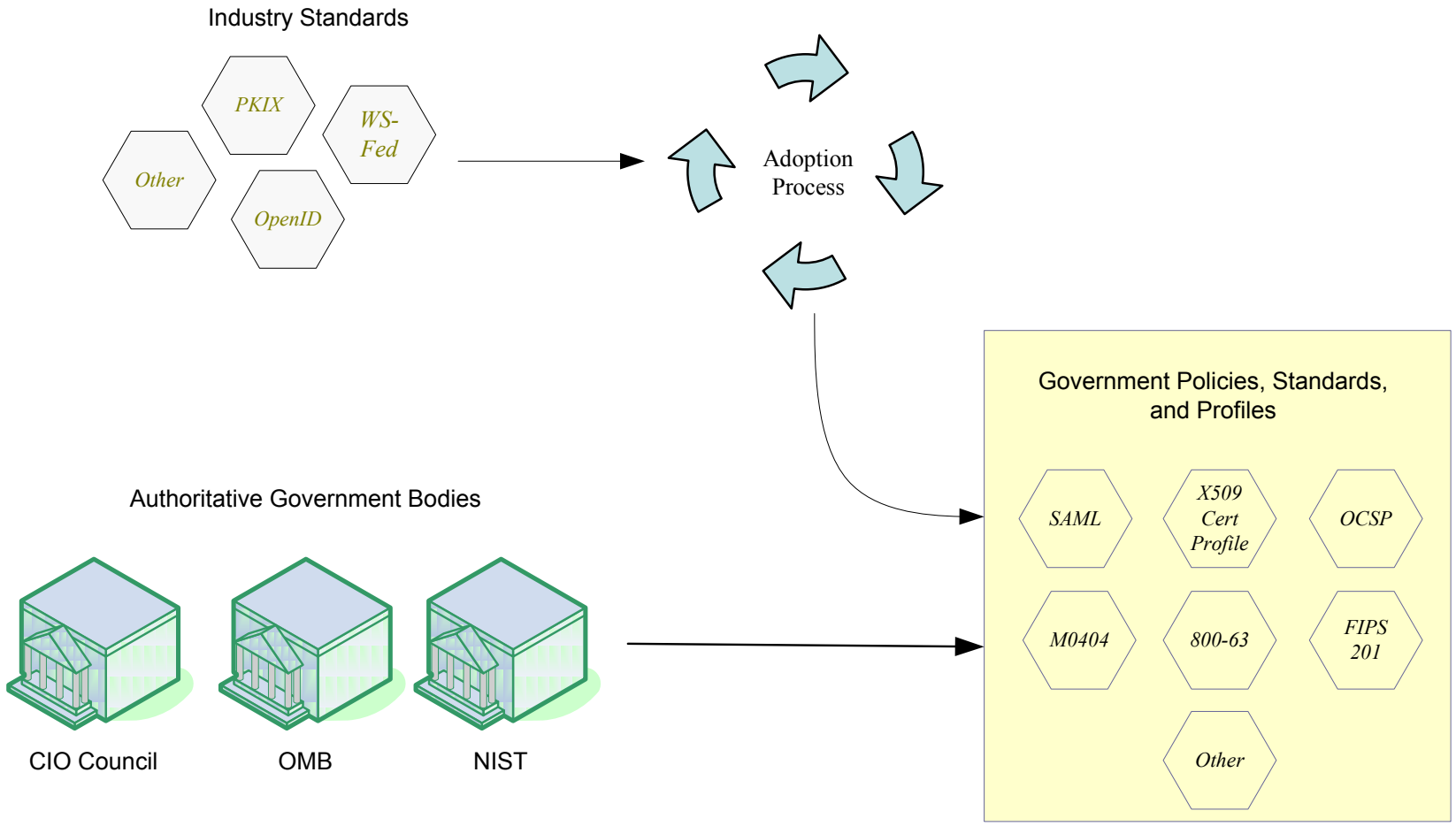
- ✓ Policy Foundation
- ➢ Portable Identity Approach
  - ➢ Technology
  - ▪ Trust
- ▪ Implementation

Approach

- Adopt technologies in use by industry
  - "Scheme Adoption"
- Adopt industry Trust Models
  - "Trust Framework Adoption"

- Approach documents posted on http://www.IDmanagement.gov

Approach: Scheme Adoption



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, Information Card (IMI), and SAML.

- *Federal ICAM Identity Scheme Adoption Process* and scheme profiles posted on http://www.IDmanagement.gov

Agenda

- ✓ Policy Foundation
- ➢ Portable Identity Approach
  - ✓ Technology
  - ➢ Trust
- ▪ Implementation

Approach: Trust Framework Adoption

- 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 included
  - Opt in
  - Minimalism
  - Activity Tracking
  - Adequate Notice
  - Non Compulsory
  - Termination

❖ *Federal ICAM Trust Framework Provider Adoption Process posted on http://www.IDmanagement.gov*

Approach: Trust Framework Adoption

- Adopted Trust Framework Providers
  - Open Identity Exchange (OIX) (http://openidentityexchange.org/)
  - Kantarra Initiative (http://kantarainitiative.org/)
  - InCommon in progress (http://www.incommonfederation.org/)

- Approved Trust Framework Providers and Identity Providers posted on http://www.IDmanagement.gov

Kantara

Trustees

Leadership Council Representatives: Colin Wallis, John Bradley

Member Organizations

[!aarp_logo.gif!]

Center for Public Management and eGovernment

Helsinki Institute of Physics

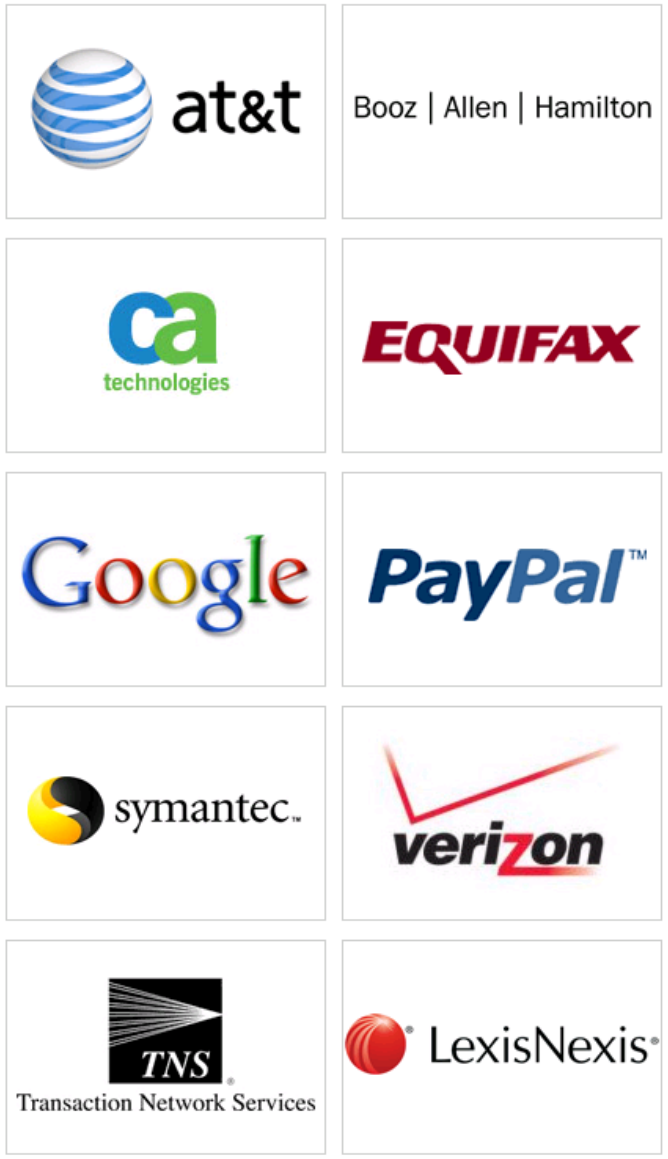
Information Card Foundation (ICF)

The Boeing Company

University of Namur, Belgium

Open Identity Exchange

Executive Members



InCommon

- 202 Education Participants, 8 Govt/Non-Profit, 72 Sponsored Partners
- 5 million users

Current InCommon Participants

A community of more than **5 million end users**.

(Source: Higher Education Students, Faculty, and Staff, Integrated Postsecondary Education Data System. Calculated October 2010.)

Higher Education Participants (202)	Government and Nonprofit Laboratories, Research Centers, and Agencies (8)	Sponsored Partners (72)
American University	Argonne National Laboratory	Absolute Software, Inc.
Arizona State University	Energy Sciences Network (ESNet)	ALEKS Corporation
Augsburg College	Fermi National Accelerator Laboratory	Alexander Street Press
Baylor College of Medicine	Lawrence Berkeley National Laboratory	Apple - iTunes U
Baylor University	Moss Landing Marine Laboratories	Atlas Systems, Inc.
Boise State University	National Institutes of Health	BioOne, Inc.
Brown University	National Science Foundation	Blackboard, Inc.
California Institute of Technology	TeraGrid	Blatant Media Corporation
California Maritime Academy		Burton Group
California Polytechnic State University, San Luis Obispo		Cambridge University Press
California State Polytechnic University, Pomona		Cayuse, Inc.
California State University, Bakersfield		Cengage Learning, Inc.
California State University, Channel Islands		Colorado Alliance of Research Libraries
California State University, Chico		CSO Research, Inc.
California State University, Dominguez Hills		Davie County Schools
California State University, East Bay		Desire2Learn
California State University, Fresno		Digital Measures
California State University, Fullerton		Docufide, Inc.
California State University, Long Beach		e-academy, Inc.
California State University, Los Angeles		e2Campus by Omnilert, LLC
California State University, Monterey Bay		Ebook Library - EBL
California State University, Northridge		EBSCO Publishing
California State University, Office of the Chancellor		EDUCAUSE
California State University, Sacramento		Elsevier

Approach: Trust Framework Adoption

- Approved Identity Providers

IDP	LOA	Scheme	TFP
Google	1	OpenID	OIX
Equifax	1	IMI, OpenID	OIX
Paypal	1	IMI, OpenID	OIX
Verisign	1	OpenID	OIX
Wave	1	OpenID	OIX

- Approved Trust Framework Providers and Identity Providers posted on http://www.IDmanagement.gov

Agenda

- ✓ Policy Foundation
- ✓ Portable Identity Approach
  - ✓ Technology
  - ✓ Trust
- ➢ Implementation

Implementation

- Determine LOA for your application
  - M -04-04 levels of assurance
- Review Privacy Impact Assessment
  - use of third party credentials may effect PIA

Implementation

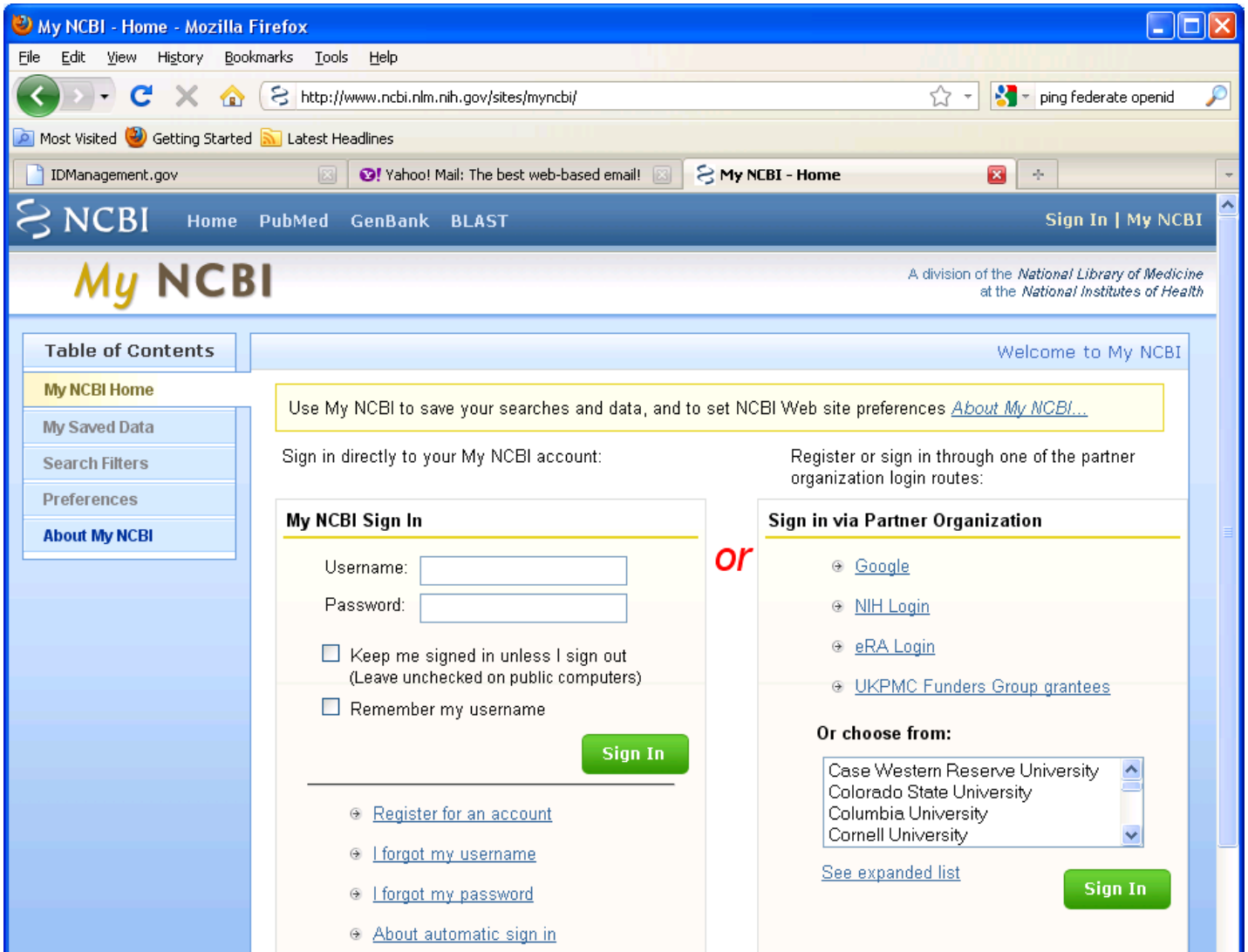
- Implement the appropriate scheme
  - e.g. “OpenID Enable” your site
  - OpenID, SAML, IMI Profiles on idmanagment.gov
  - Open Source, Free Libraries, Platform Modules, Commercial Products available
  - Schemes should be integrated into your existing application, probably by your existing web team
  - Details depend on how you built your website
  - Consider which IDPs support which schemes
  - Help available from the ICAM SC Lab

Implementation Considerations

- Configure metadata for approved IDPs
  - URLs, Configuration information for each IDP
  - Coordinate through ICAM SC Lab
- Consider User Interface (UI)

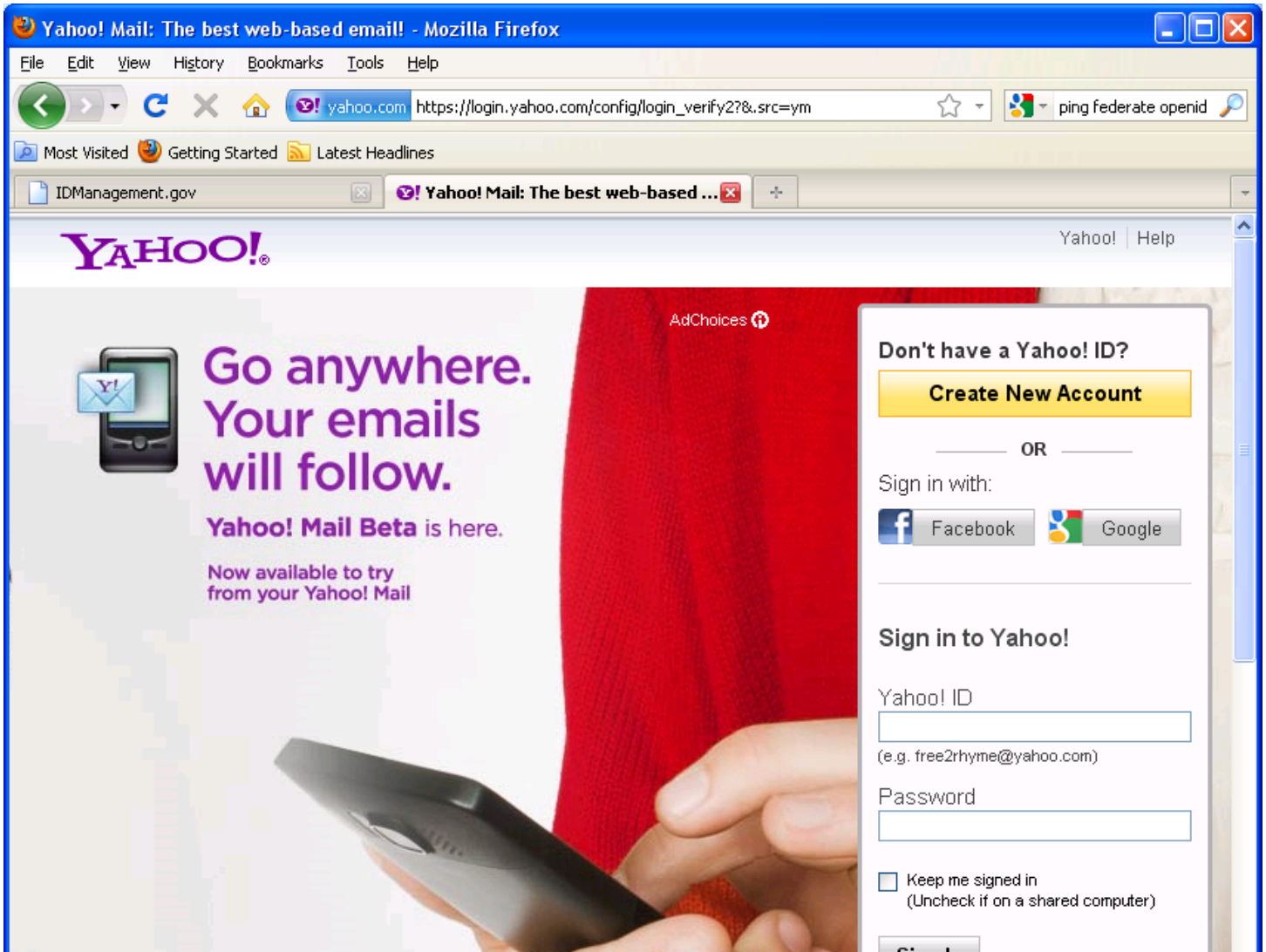
Implementation Considerations

- UI



Implementation Considerations

- UI



Implementation Considerations

- Not rocket science
  - thousands of sites have implemented these technologies
  - does require attention from your web team
  - will impact release planning
  - does not require new commercial software, servers, bandwidth, capital expenditures, etc
  - impact similar to any new feature integrated into your site

Agenda

- ✓ Policy Foundation
- ✓ Portable Identity Approach
  - ✓ Technology
  - ✓ Trust
- ✓ Implementation
- ➢ Questions?

Backup Slides

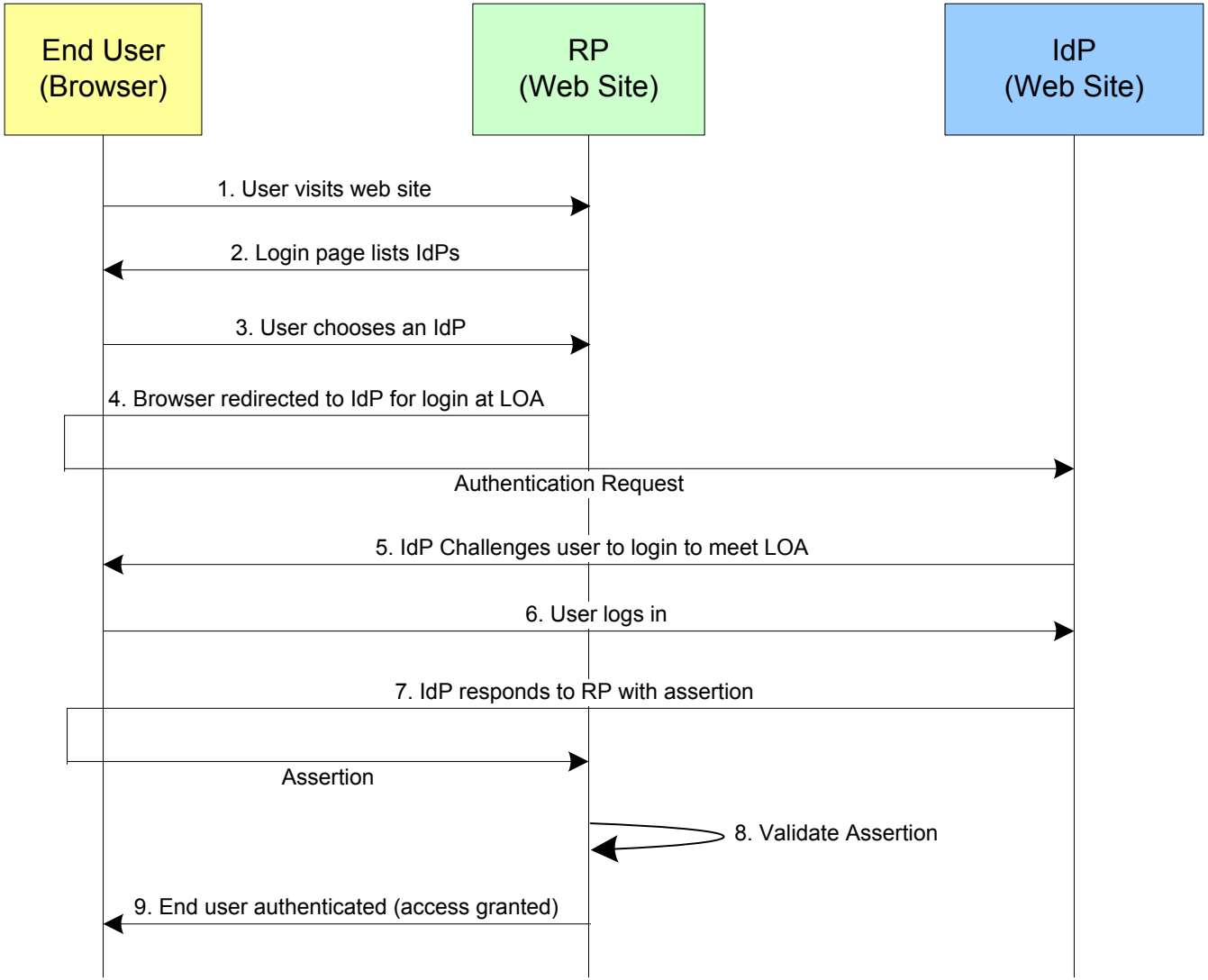
Backup Slides

- Scheme Details

Portable Identity Schemes: SAML

- SAML
  - OASIS SAML 2.0
  - Based on E-Gov Profile developed through Liberty
  - Broad COTS support
  - Has been used by government before
- Federal Profile
  - Requires E-Gov Profile
  - Requires encryption of PII

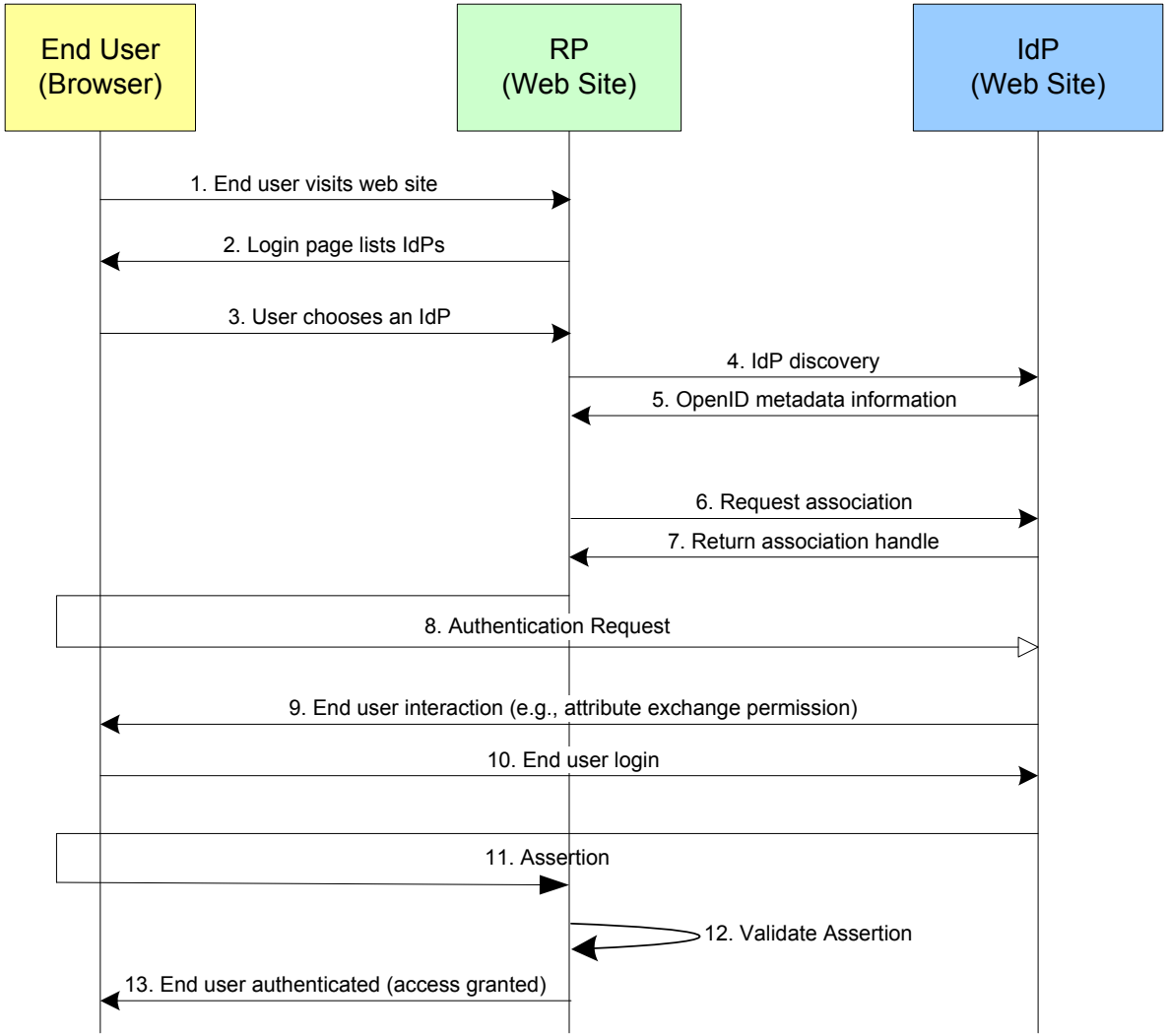
Portable Identity Schemes: SAML



Portable Identity Schemes: OpenID

- OpenID
  - Open Source roots
  - OpenID Foundation serves as steward and provides necessary infrastructure
  - Used/supported by JanRain, SixApart, Google, Yahoo, Facebook, AOL, MySpace, Novell, Sun, etc.
  - 1 billion+ OpenID-enabled accounts
  - 40,000+ web sites support OpenID
- Federal Profile
  - Profile based on OpenID 2.0
  - Requires SSL/TLS on all endpoints
  - Requires *Directed Identity* Approach
  - Requires pair-wise unique pseudonymous identifiers
  - Requires short-lived association handles

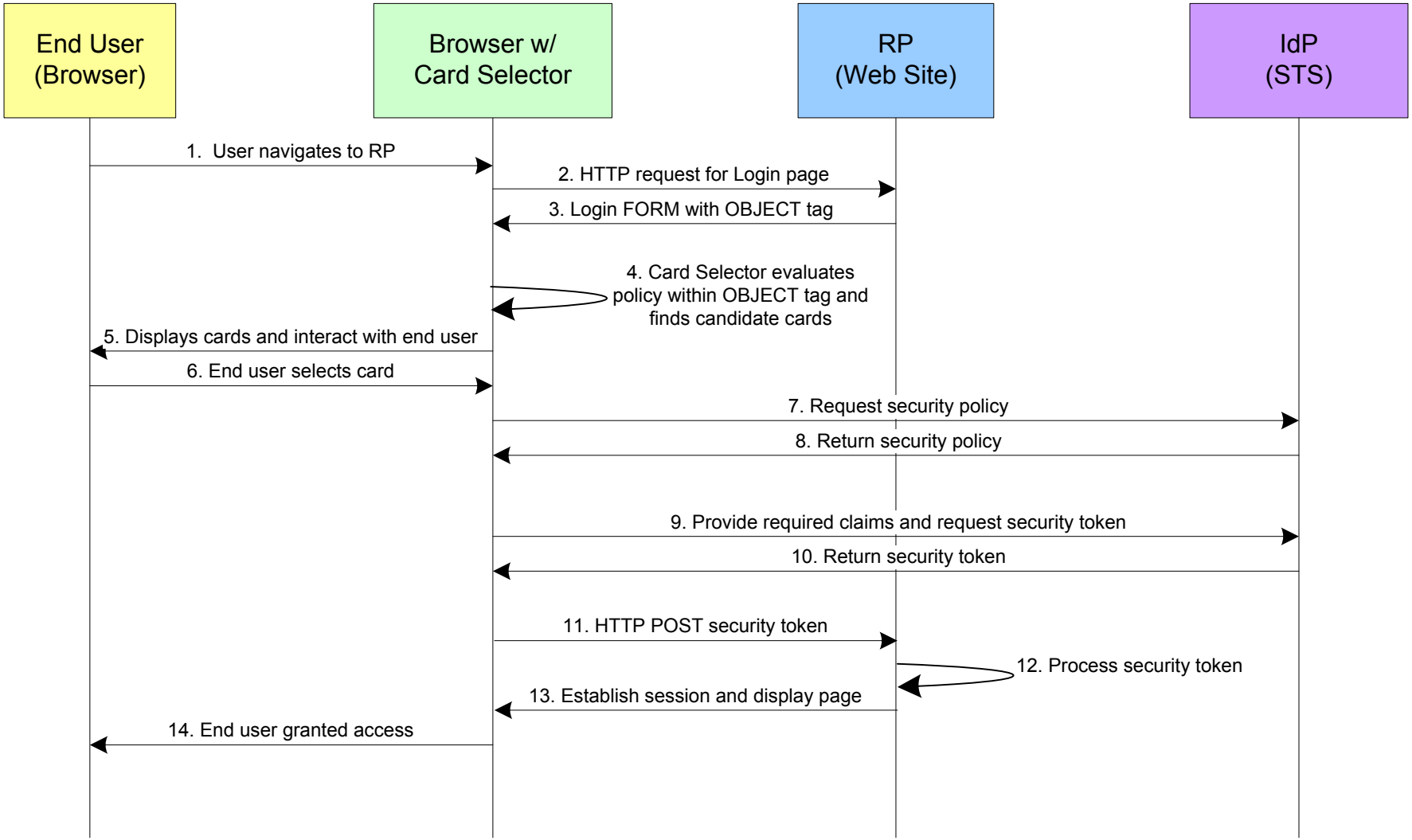
Portable Identity Schemes: OpenID



Portable Identity Schemes: Information Card (IMI)

- Information Card
  - Analogous to the cards you carry in wallet
  - Open Source & industry standards
  - Supported by Azigo, CA, Equifax, Google, Intel, Microsoft, Novell, Oracle, Paypal, etc.
  - Built into MS Vista; option for XP
  - Earlier stage of adoption than OpenID
  - ALs 1 thru 3; possibly AL 4
- Federal Profile
  - Profile of *Identity Metasystem Interoperability Document 1.0* (IMI)
  - Requires encryption of PII
  - Requires use of optional *Private Personal Identifier* (PPID)
  - Managed cards only

Portable Identity Schemes: Information Cards (IMI)



Backup Slides

- Full Privacy Principles

Trust Framework Privacy Principles

1. **Opt In** Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of individual attributes for each transaction.
2. **Minimalism** – Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile. RP Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002.

Trust Framework Privacy Principles

3. **Activity Tracking** – Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication. RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002.
4. **Adequate Notice** – Identity Provider must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process.

Trust Framework Privacy Principles

5. **Non Compulsory** – As an alternative to 3rd-party identity providers, agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service.
6. **Termination** – In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.

Backup Slides

- IDManagement.gov

Identity, Credential, and Access Management

Identity, Credential, and Access Management