

Open Solutions for Open Government

Portable Identity Technical Approach

Privacy Workshop

August 10, 2009

Chris Loudon

Agenda

- ❑ Goals
- ❑ Policy Foundation
- ❑ Approach
 - Technology
 - Trust
 - Privacy Principles
- ❑ Portable Identity Schemes
 - SAML
 - OpenID
 - Information Cards

Goals

- ❑ Make Government more transparent to citizenry
- ❑ Make it easier for citizenry to access government information
- ❑ Avoid issuance of application-specific credentials
- ❑ Leverage Industry credentials for Government use
- ❑ Leverage Web 2.0 technologies

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

❑ Risks

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

<i>Allowed Token Types</i>	1	2	3	4
Hard crypto token	√	√	√	√
One-time Password Device	√	√	√	
Soft crypto token	√	√	√	
Password & PINs	√	√		

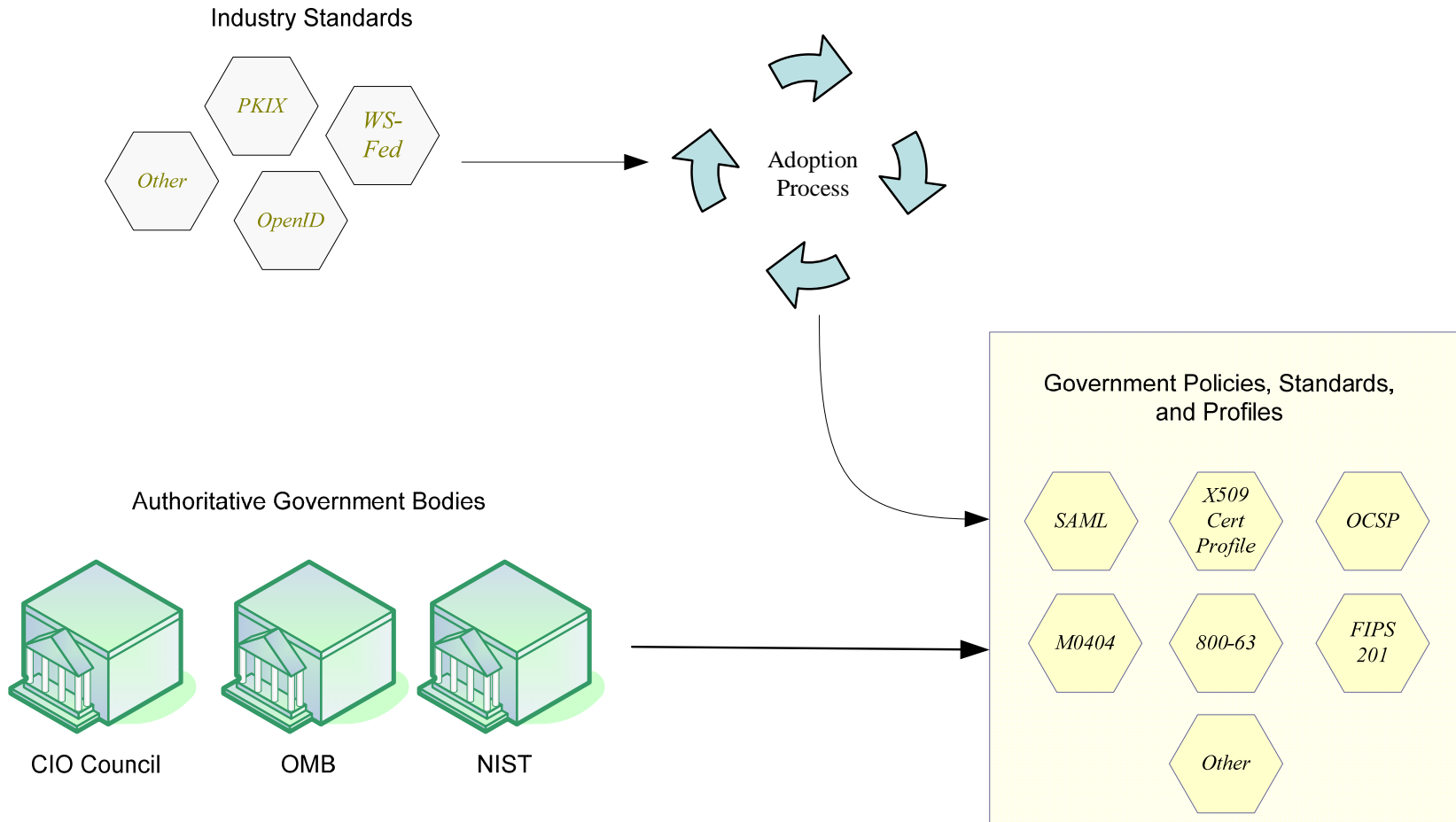
Agenda

- ✓ Goals
- ✓ Policy Foundation
- Approach
 - Technology
 - Trust
 - Privacy Principles
- Portable Identity Schemes
 - SAML
 - OpenID
 - Information Cards

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 IdPs & RPs
 - Goal is not to change the existing technical standard
 - Profiles in progress for OpenID, Information Card (IMI), and SAML.
 - WS-Federation next
- ❖ *Federal ICAM Identity Scheme Adoption Process* posted on <http://www.IDmanagement.gov>

Approach: Trust Framework Adoption

- ❑ Trust Framework Adoption
 - Adoption of Industry Trust Frameworks
 - Adopts at Assurance Levels (ALs)
 - Considers requirements of NIST SP 800-63
- ❑ Privacy Principles enforced through the Trust Framework
- ❑ Participation expected from InCommon, OpenID Foundation,, Information Card Foundation, Liberty/Kantara

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

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.

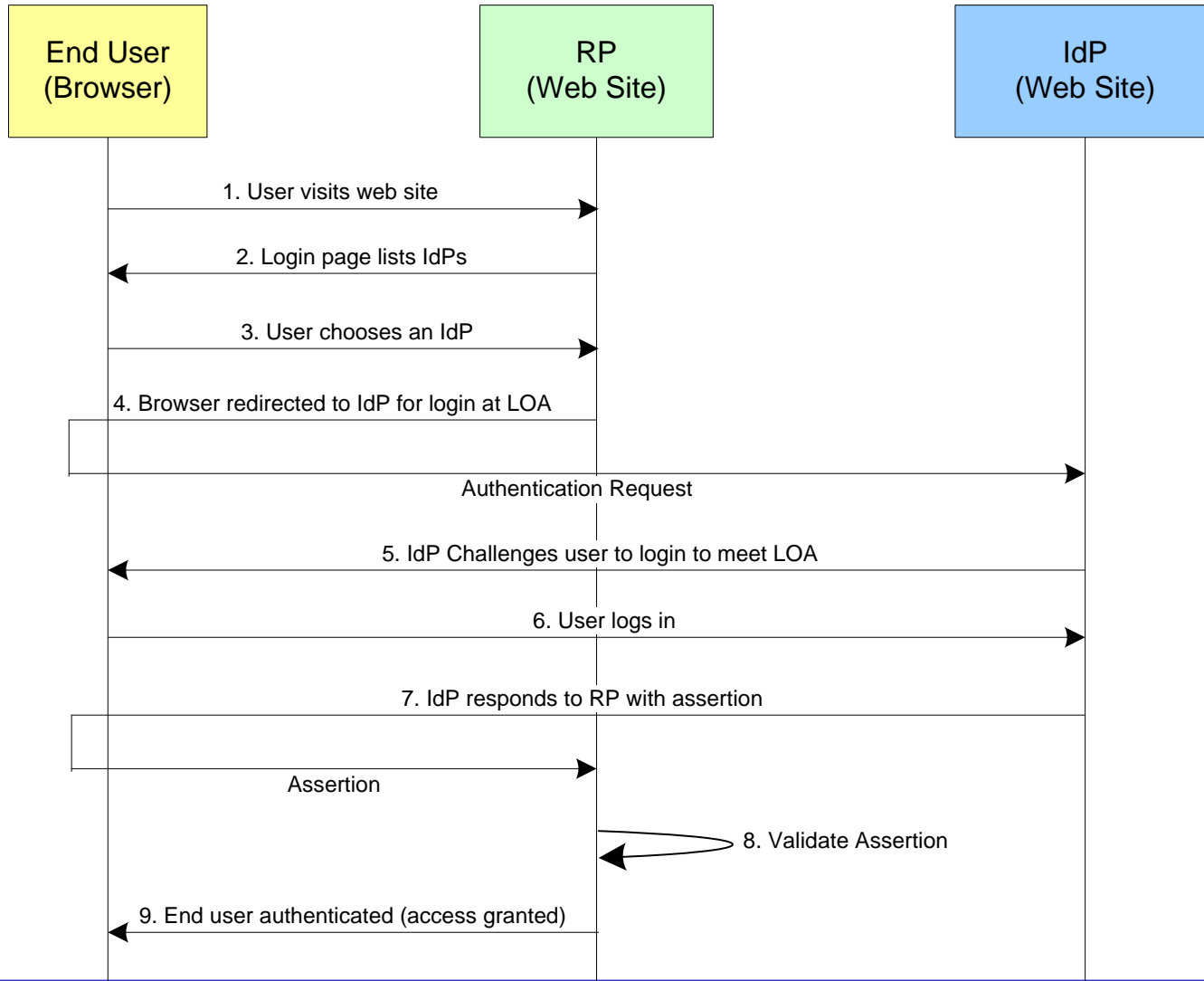
Agenda

- ✓ Goals
- ✓ Policy Foundation
- ✓ Approach
 - ✓ Technology
 - ✓ Trust
 - ✓ Privacy Principles
- Portable Identity Schemes
 - SAML
 - OpenID
 - Information Cards

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

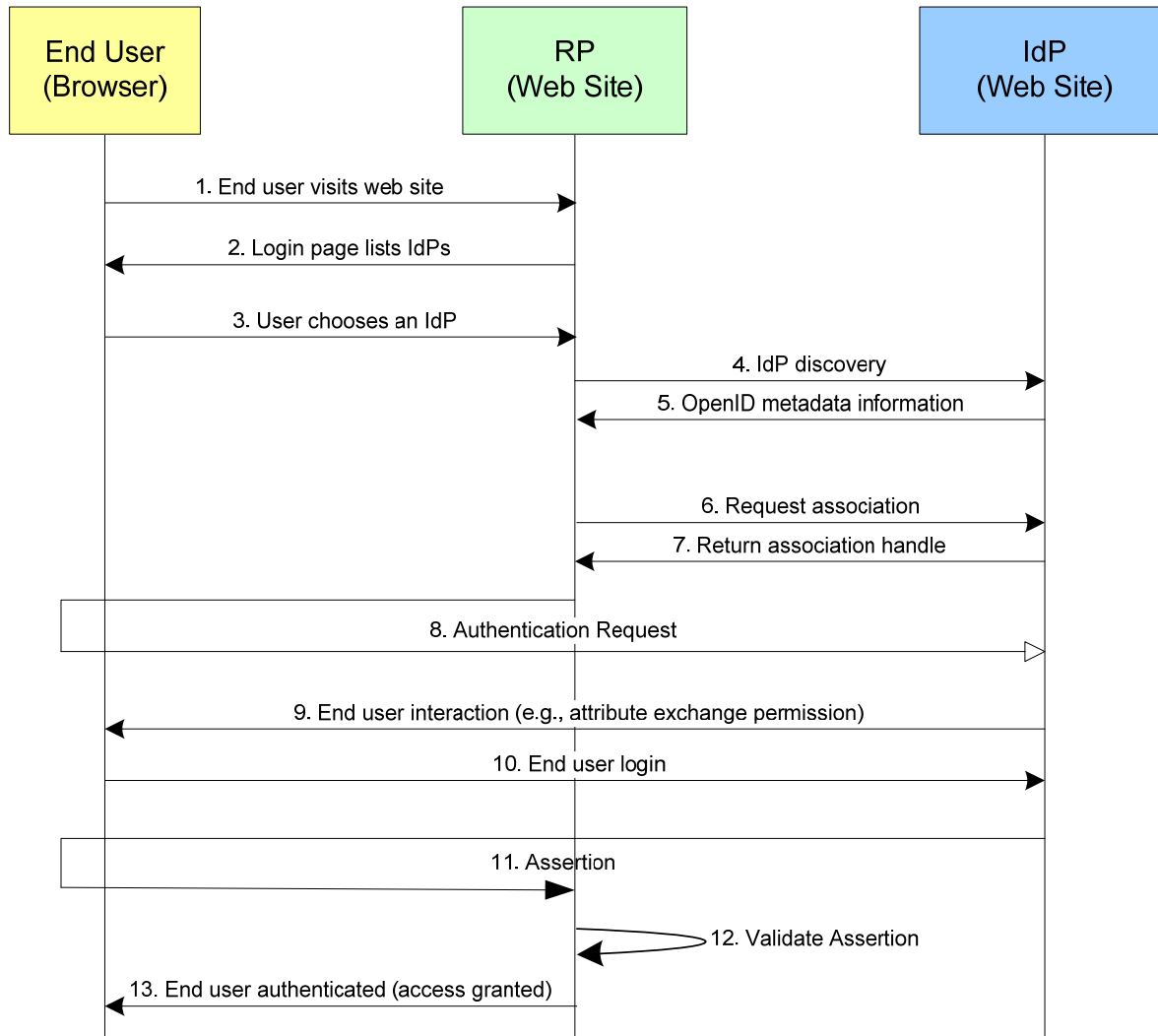
❑ OpenID

- 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)

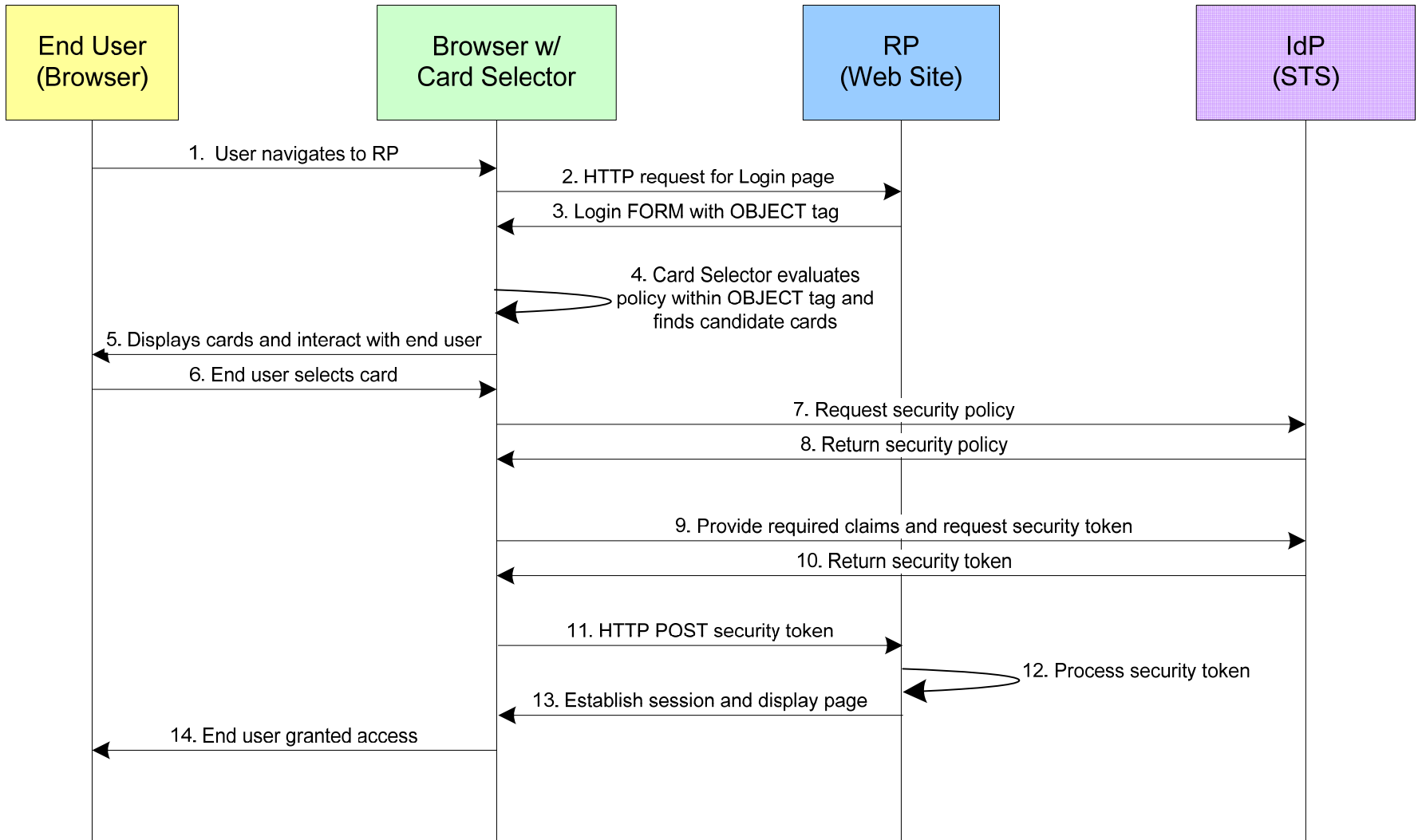
❑ Information Card

- 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)



Agenda

- ✓ Goals
 - ✓ Policy Foundation
 - ✓ Approach
 - ✓ Technology
 - ✓ Trust
 - ✓ Privacy Principles
 - ✓ Portable Identity Schemes
 - ✓ SAML
 - ✓ OpenID
 - ✓ Information Cards
- ❖ Approach documents posted on <http://www.IDmanagement.gov>