SAML, The Liberty Alliance, and Federation*

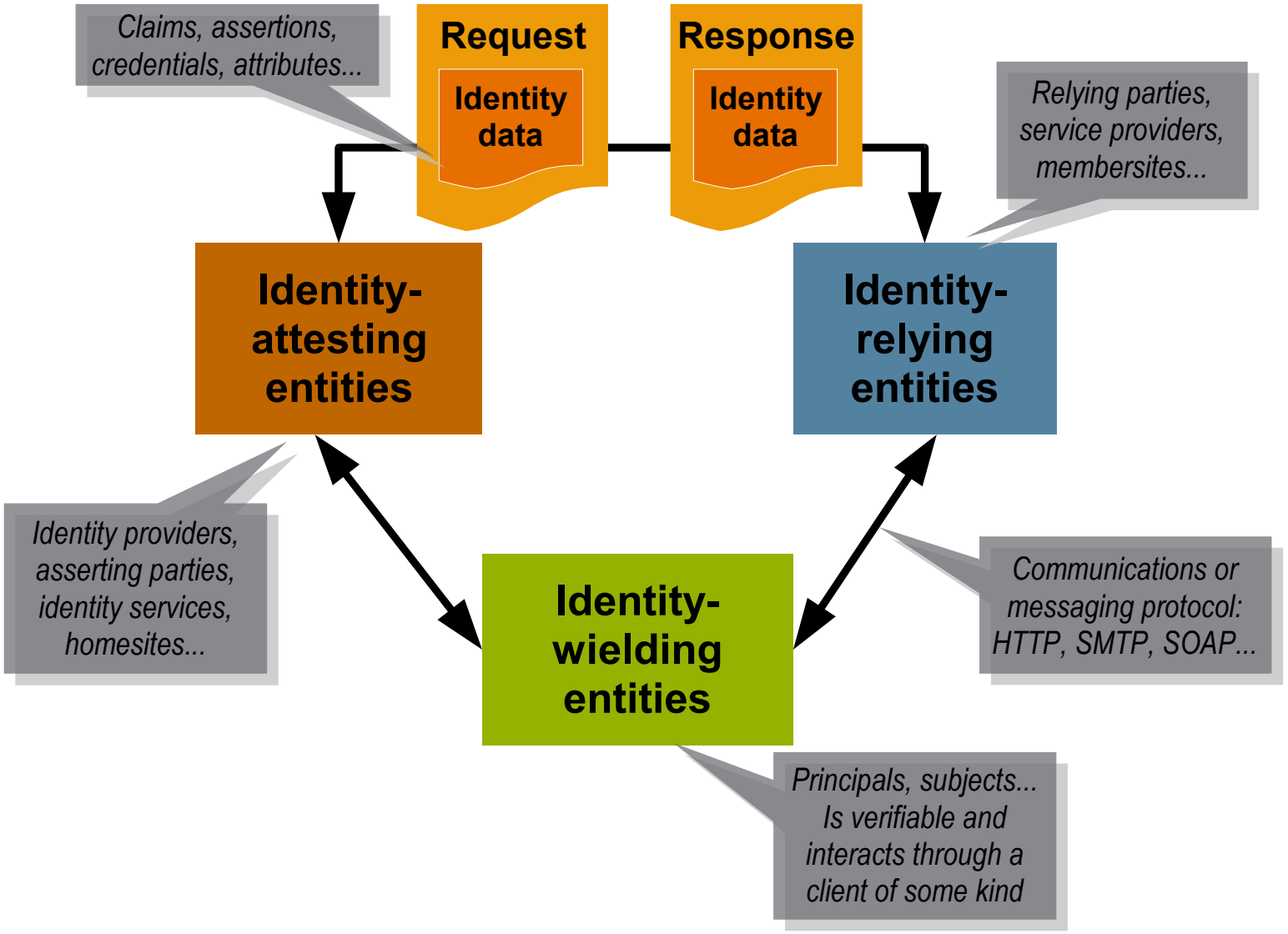
Eve Maler
eve.maler@sun.com
http://www.xmlgrrl.com/blog

IIWb, Mountain View, CA, 4 December 2006

When you “distribute” identity tasks and information in the right way...

- People can:
  - Unify management of their identity information
  - Avoid authenticating repeatedly
  - Have better-personalized online experiences
  - Gain better privacy control
- Services and applications on the web can:
  - Offload authentication and identity lookup tasks
  - Unify treatment of all “things with identities”
  - Provide finer-grained access control and differentiation
- Organizations can:
  - More securely outsource business functions

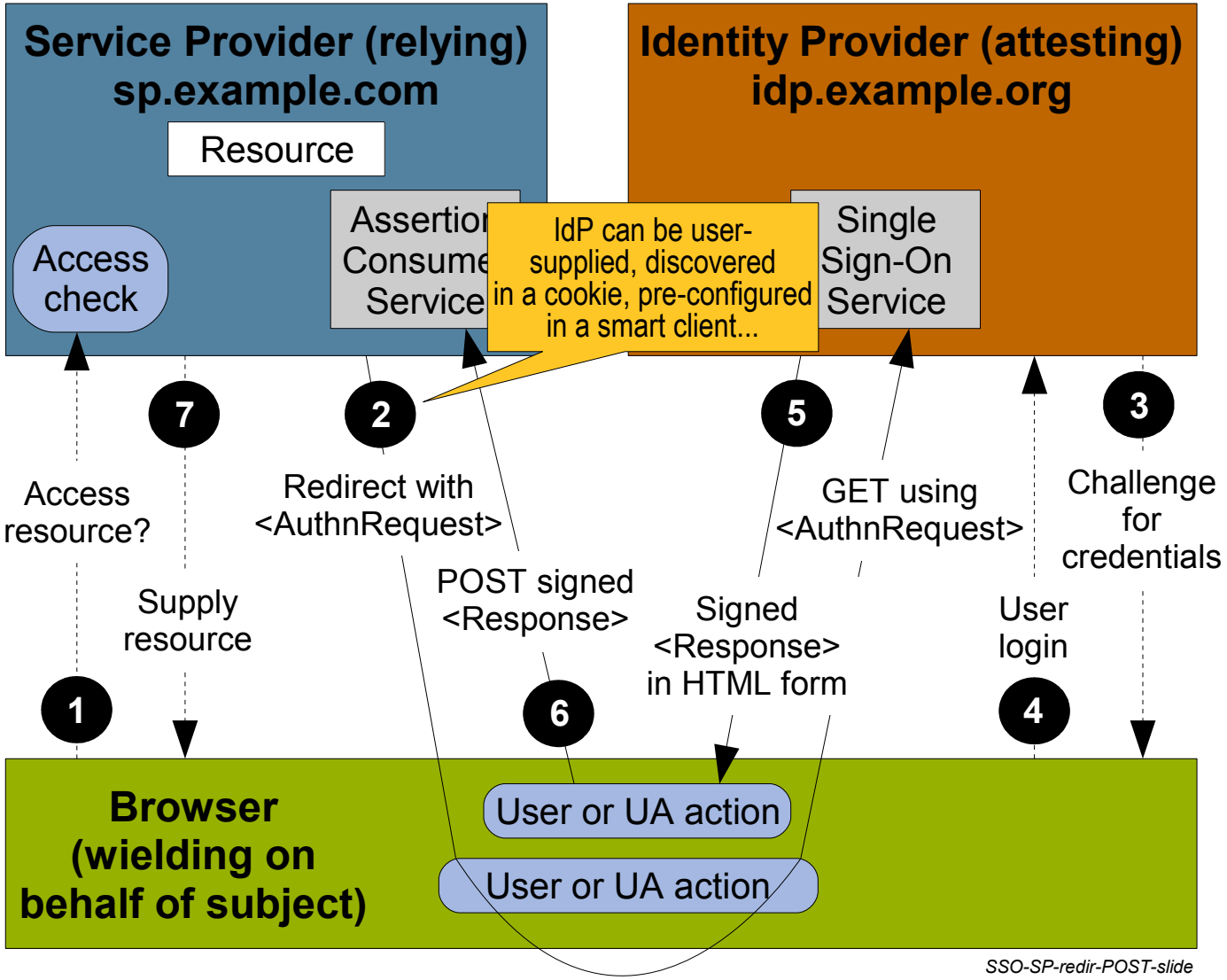
The system entities and communication modes in SAML/Liberty should be familiar



Major SAML use cases

- "Distributed" authentication (**single sign-on**) of several varieties
  - With detailed descriptors for authentication type/strength
- Linking two of a user's existing web accounts (**identity federation**) without having to compromise privacy
- Attribute exchange
- Single logout from several apps across a single distributed authentication session
- Anyone can satisfy other use cases with profiling/extension
  - JeffH and ScottC's "SimpleSign" and "Lightweight SSO" for 100% XMLSig-free SSO
  - WS-Security usage of SAML assertions to secure SOAP messages

A common way to use SAML for SSO (RP-initiated, request redirected, response POSTed)



SSO-SP-redir-POST-slide

Sometimes “who the user is” needs to be obscured

- In a world where identity tasks and information are becoming much more “distributed”, there's still:
  - A principle of minimal disclosure
  - Issues of compliance with privacy laws
  - Whistleblower scenarios
- Shibboleth allows for “anonymous authorization” to use research materials at an affiliated university
- Sun outsources some employee services, which customize their offerings without knowing precisely who is using them
- SAML and Liberty offer **pseudonyms** for privacy – transient or persistent opaque handles that make sense in only one usage context
  - Along with other privacy, security, and informed-consent features

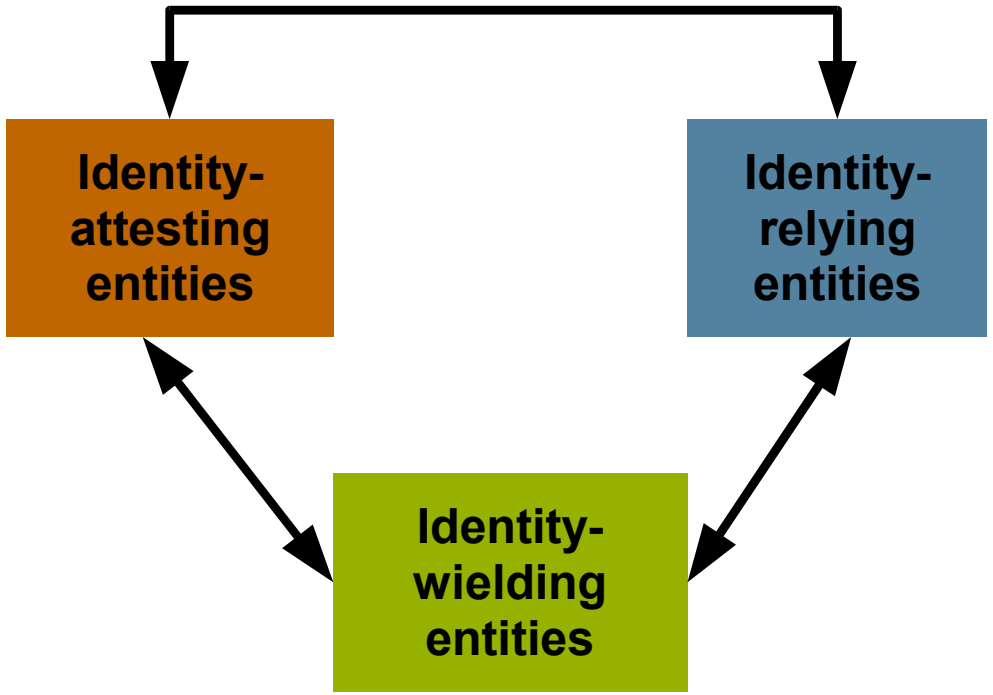
Liberty Alliance (the organization)

- Mission:
  - Foster a ubiquitous, interoperable, privacy-respecting identity layer
- Deliverables:
  - Technology specs and guidelines (currently around **identity services**), business and privacy guidelines, coordination of interop testing, adoption activities...
- Key goals:
  - Work with *all* network devices
  - Deal with transactions where humans are/*aren't* present
  - Enable anonymity, security, and informed user consent

Liberty (the specs (to date))

ID-WSF: Identity Web Services Framework
- Focused on application-to-application interaction

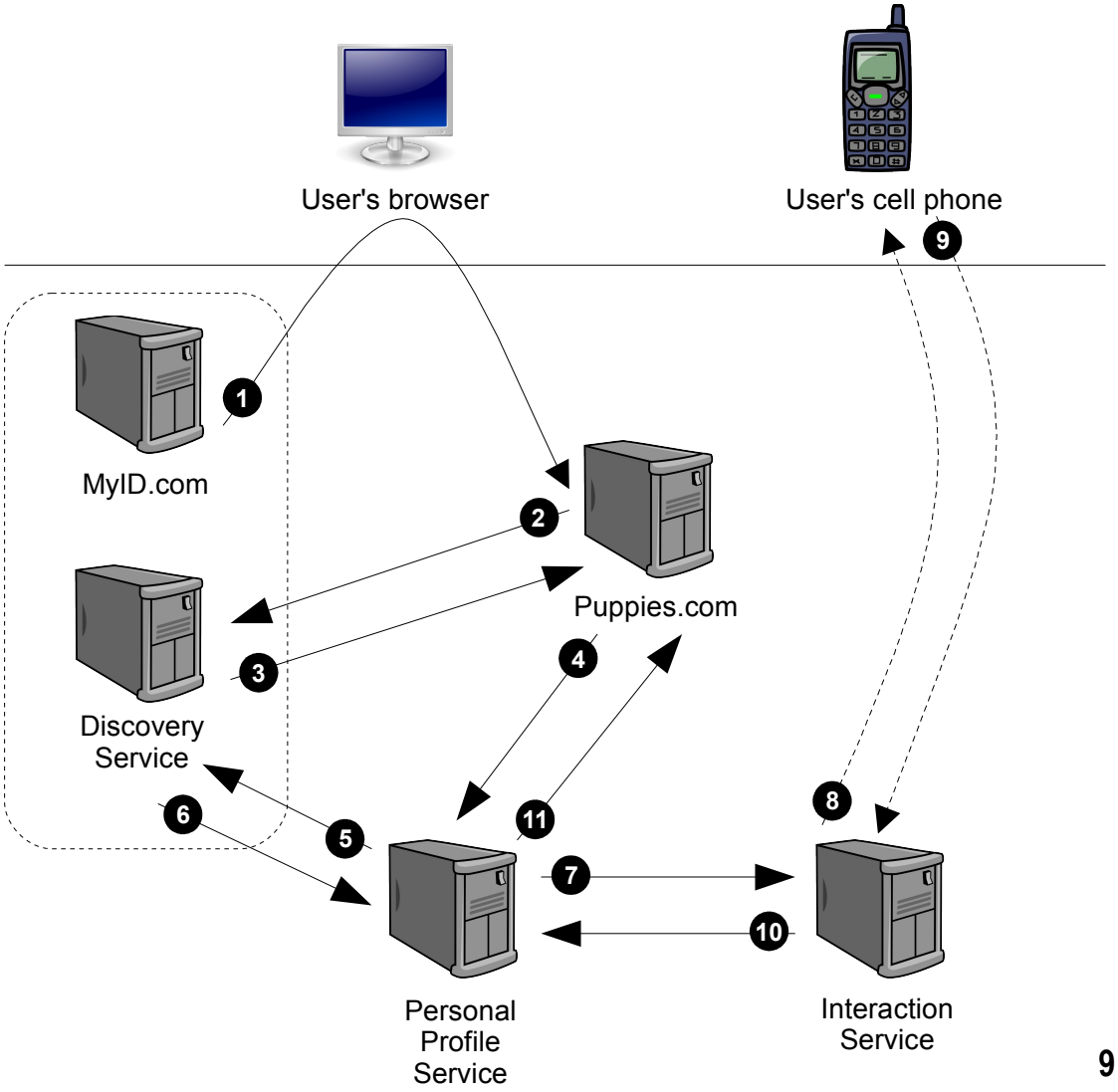
ID-SIS: Service Interface Specifications
- Focused on particular identity-based services
- Personal profile, presence, geolocation...



ID-FF: Identity Federation Framework
- Focused on human-to-application interaction
- Now converged with SAML V2.0

Comprehensive Liberty use case for "distributing" identity services

- Puppies.com website allows Tiffani to SSO from MyID.com; in the process it learns where her identity Discovery Service is (1)
- Puppies.com uses DS (2,3) to learn where Tiffani's Personal Profile service is and gets OK'd to use it (4)
- PP service uses DS (5,6) to learn where Tiffani's Interaction Service is and gets OK'd to use it, to ask (7,10) for SMS'd approval (8,9) to give (11) her name and address to Puppies.com
- These logical components were designed in for maximum privacy and flexibility – but not every deployment needs them all



The Liberty People Service

- Lets you share (grant access rights to) your online resources and services with other people
  - Even if your identities are not managed at the same place
  - Whereas today in (e.g.) Flickr, you can create ACLs only for those with Flickr IDs
- With the People Service you can create **person-to-person federations** between you and others
- Useful for social *and* business scenarios:
  - Business networking, access-controlled collaborative spec editing, project-specific confidential material access...

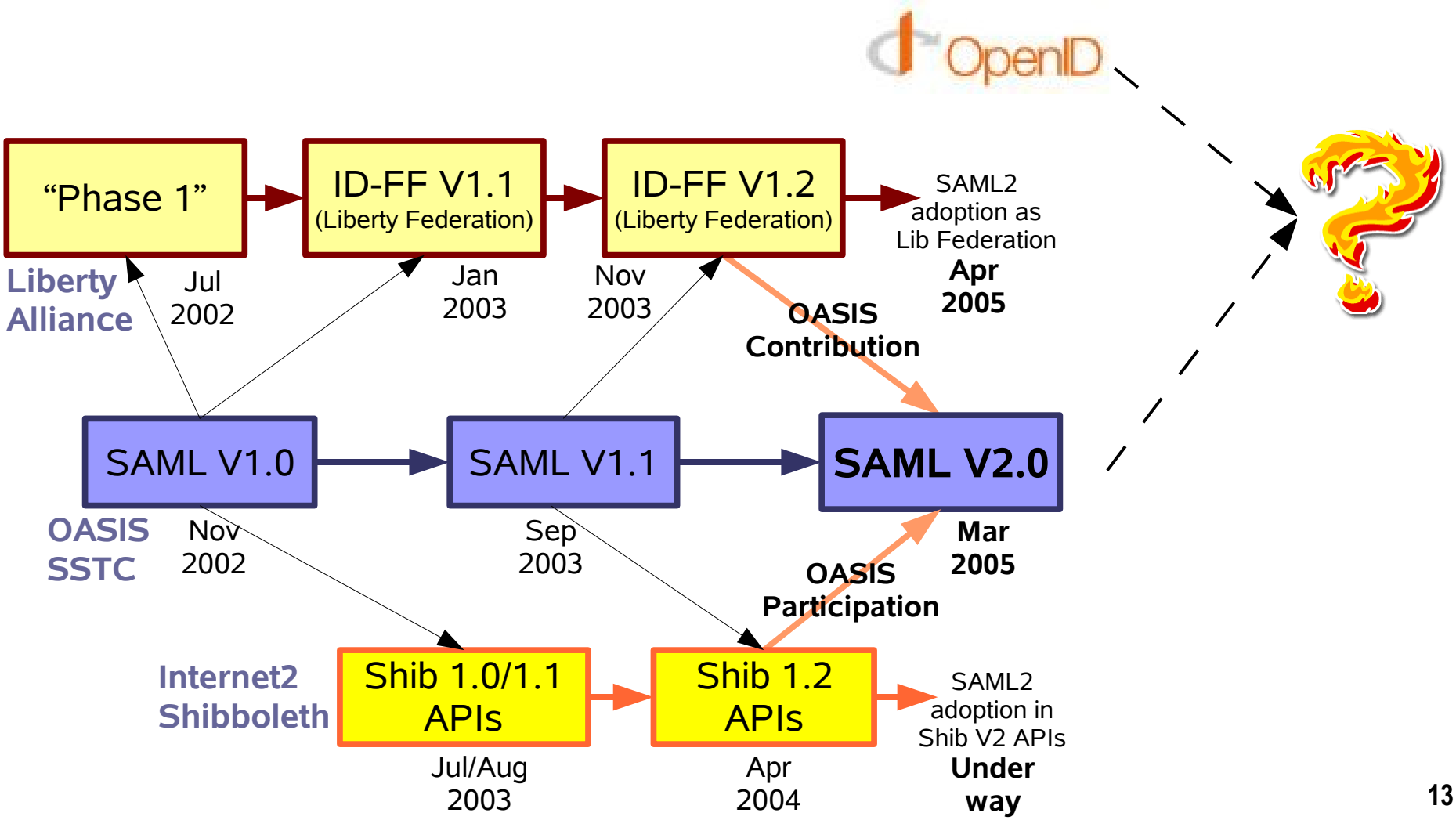
Major open-source implementations

- Sun's http://OpenSSO.dev.java.net
  - SAML, ID-FF, ID-WSF... in Java; SAML... in PHP (“Lightbulb”)
- Internet2's http://www.OpenSAML.org
  - SAML in Java and C++
- Internet2's http://sourceforge.net/projects/guanxi/
  - Shibboleth profile of SAML in Java
- Ping Identity's http://www.SourceID.org
  - SAML and ID-FF (and WS-Fed) variously in Java, .NET, Apache
- Entrouvert's http://LaSSO.Entrouvert.org
  - SAML, ID-FF, ID-WSF in C
- Symlabs' http://ZXID.org
  - SAML, ID-FF, ID-WSF (and WS-Fed) in C and scripty wrappers
- Conor's http://www.cahillfamily.com/OpenSource/
  - ID-WSF in C

Thoughts on open-Internet usage of SAML and Liberty

- Many *deployments* assume pre-existing business trust, but the *protocols* don't require them
  - Examples in the wild are OpenIdP.org and ProtectNetwork.com, IdPs that offer logins for use with Shibboleth web apps
- The technologies are agnostic as to ownership of the identifier
  - You, your employer, a government agency...
  - The do assume, however, that you have many! (I have ~380)
- The means of locating and learning about the "authentication authority" are flexible
- Many of the basic use cases for SAML and OpenID are extremely similar
  - Though the design centers are not identical

Some convergence history ...and future history?



Can the SAML/Liberty and OpenID communities learn from each other?

What can they learn from each other?

- Internet scale...and robustness
- User experience...and security
- Personalization...and anonymity
- Freedom...and trust
- “Being present to win”...and the “break glass” scenario

- Is it possible to have it all? Join in on IIWb sessions to discuss...
  - > Specifics of potential convergence touchpoints (David/Eve)
  - > Lightbulb code with new support for OpenID identifiers (Pat)
  - > More? (you?)