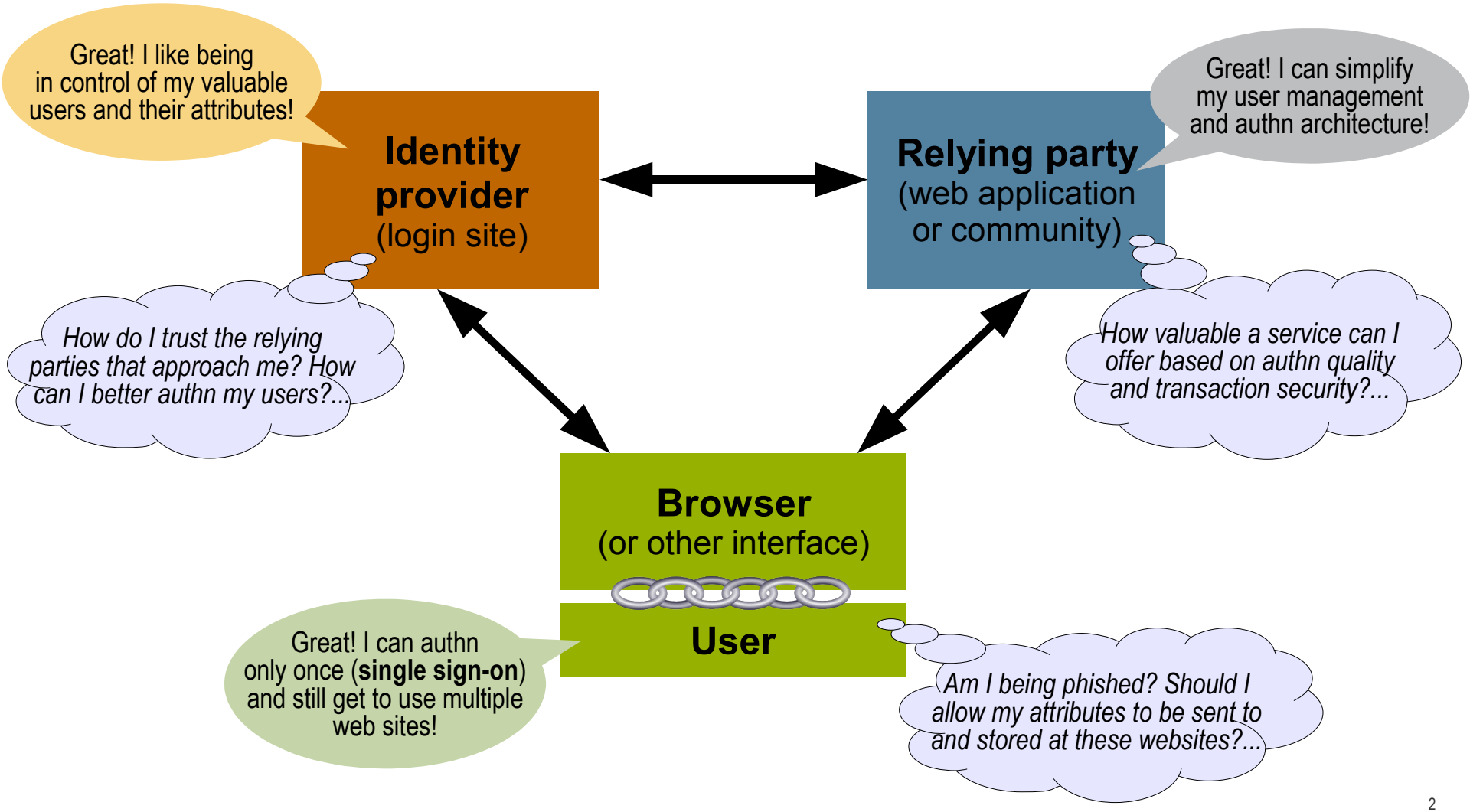
# SAML, Liberty Alliance, openLiberty, and Concordia

**Eve Maler**
Sun Microsystems, Inc.
www.xmlgrrl.com/blog

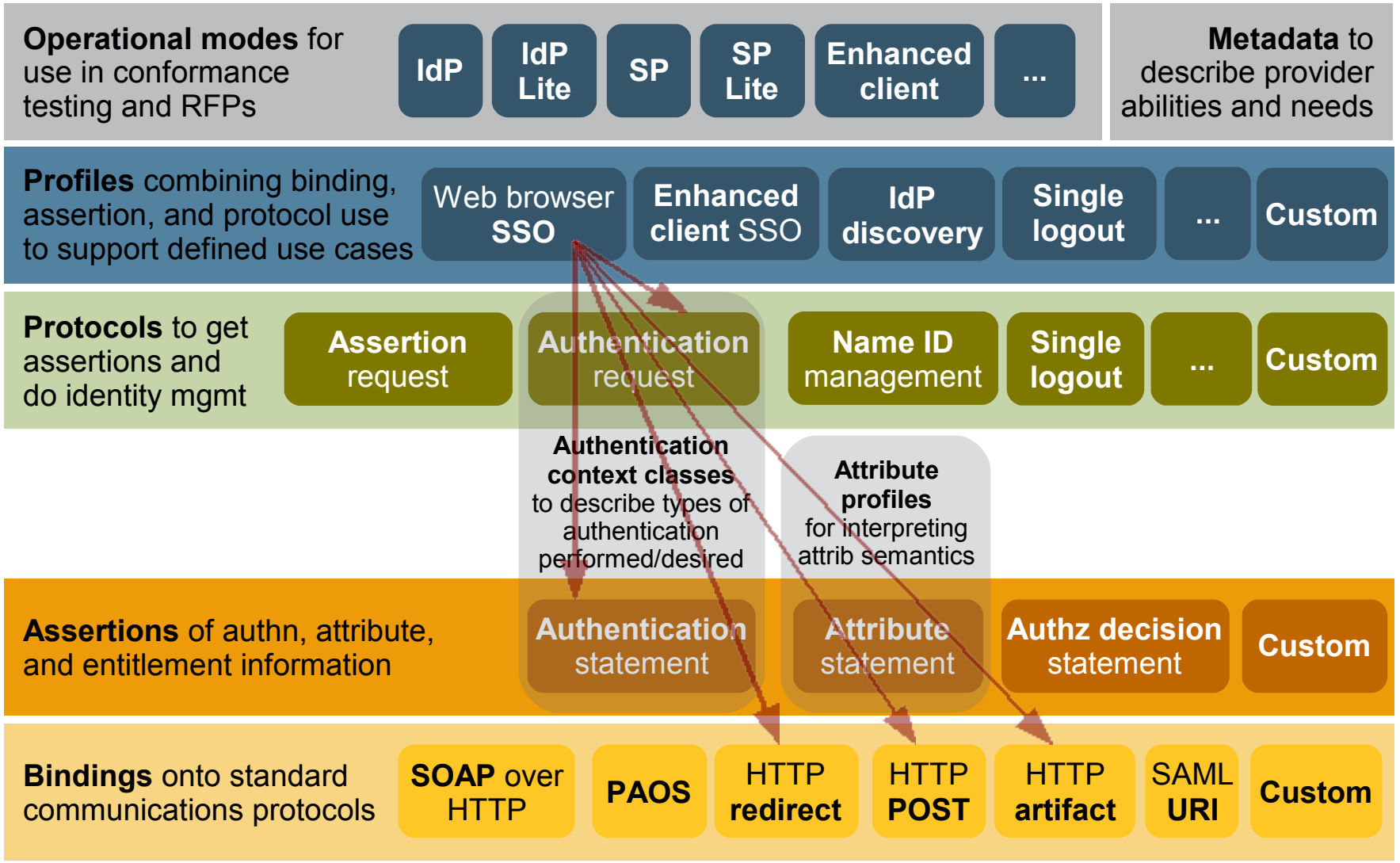
# Federated identity means distributing *identity tasks and information* across domains



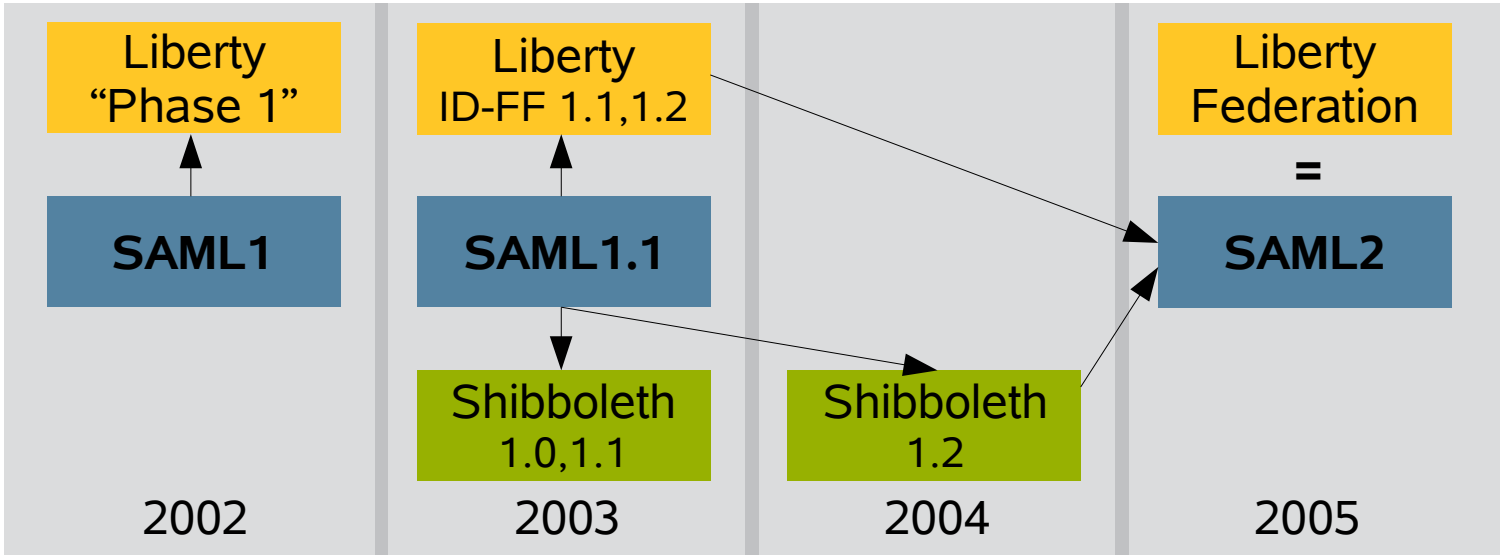
# SAML in a verbal nutshell


- XML-based framework standardized at OASIS for:
  - Marshaling security and identity information
  - Exchanging it across domain boundaries
- Out-of-the-box profiles for:
  - Single sign-on, single logout, privacy-preserving account linking, simple arbitrary attribute exchange...
- At SAML's core: assertions about subjects
  - Authentication, attributes, entitlements
  - SAML assertions are reused in many other specs
- SAML V2.0 + business guidelines + interop certification testing = “Liberty Federation”

# SAML in a pictorial nutshell



# SAML, Shibboleth, and Liberty Federation Framework convergence timeline




Liberty bases new federation standard on emerging SAML standard

Liberty tracks SAML evolution; Internet2 Shibboleth bases its solutions on SAML also

Liberty contributes ID-FF to OASIS for SAML2 convergence; Shibboleth also takes part

Liberty endorses SAML2 as its identity federation solution and provides interop and conformance testing; Shibboleth is working on new SAML2-based APIs

**x⟶y** = design of X feeds into Y (with direct dependencies except in the SAML2 case)

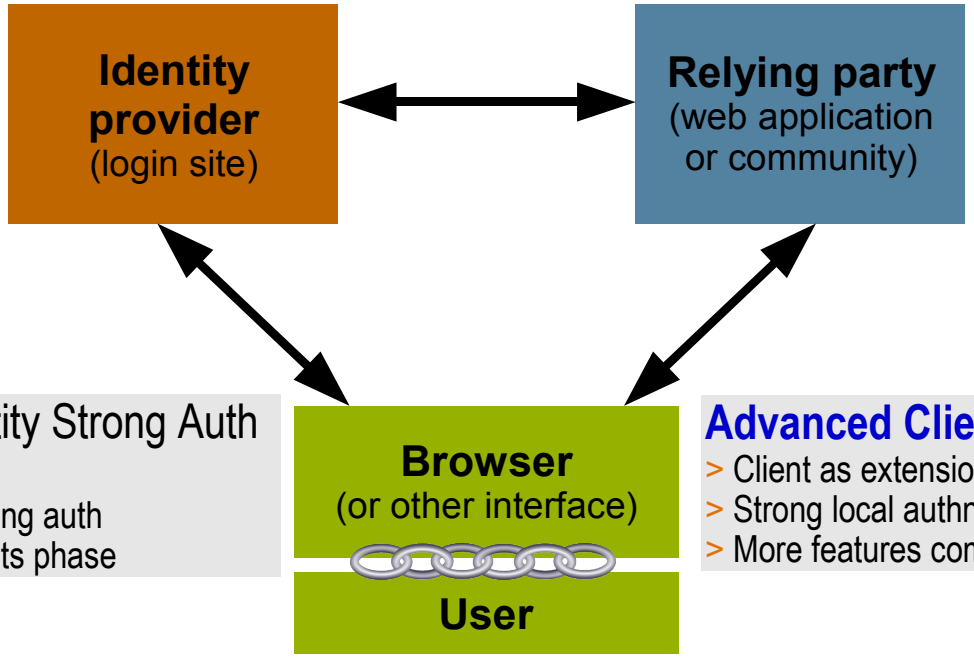
# Liberty Alliance in a verbal nutshell

- A community of ~150 businesses, organizations, government agencies – and now individuals
  - With a long list of .org relationships...
- Its mission since 2001:
  - Foster a ubiquitous, interoperable, privacy-respecting federated identity layer for web applications and services
- Deliverables are the result of three work streams:
  - Gathering requirements from deployers and users
  - Gathing privacy policy and global regulatory requirements
  - Developing open technology standards (and testing software for interop)
- Tackles business and technical requirements for “trust”

# Liberty in a pictorial nutshell

**ID-WSF**: Identity Web Services Framework
> Focused on application-to-application interaction
> Permission-based attribute sharing and user-absent scenarios

**ID-SIS**: Identity Service Interface Specifications
> Focused on ID-based services
> Personal profile, geolocation...
> Uses WSP/WSC terminology
> **Liberty Web Services** = ID-WSF + ID-SIS




**openLiberty.org**: open source for web service consumers
> Eventually other projects too

**ID-SAFE**: Identity Strong Auth Framework
> Interoperable strong auth
> In the requirements phase

**Advanced Client**
> Client as extension of the IdP
> Strong local authn, and local-hosted services
> More features coming soon

**ID-FF**: Identity Federation Framework
> Focused on human-to-application interaction
> Now converged with SAML2

# The Liberty People Service

- A “groups and roles” service that is agnostic as to where all the identities are managed
  - You can base ACLs and other behavior on them
  - Versus today's popular web apps, which restrict the means of building ACLs
- You are effectively creating person-to-person federations between you and others
- Useful for social and business scenarios:
  - Soccer team calendar control, business networking, access-controlled collaborative spec editing, project-specific confidential material access...

# Some FOSS for SAML and Liberty

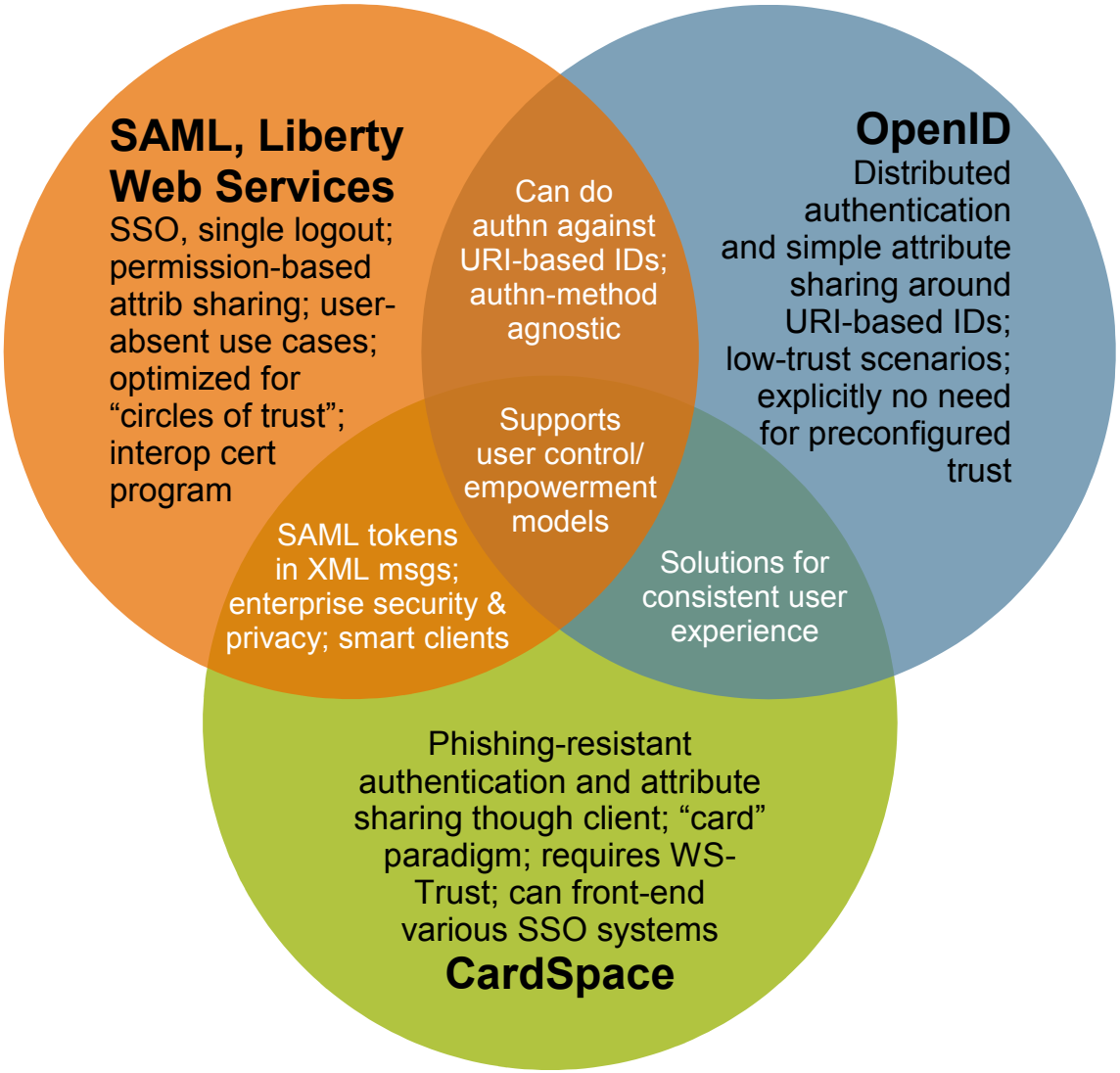
Thanks to John Kemp for doing most of the data compilation!

- openLiberty.org (http://www.openliberty.org)
  - The new home for Liberty-related OSS
- OpenSAML (http://www.opensaml.org) - Apache license
  - Java/C++ libraries giving low-level access to SAML 1.x functionality
- Shibboleth (https://spaces.internet2.edu/display/SHIB/WebHome) - Apache license
  - SAML 1.x IdP, SP functionality
  - Plugs in to Apache httpd, IIS, Sun/iPlanet
- OpenSSO (http://opensso.dev.java.net) - CDDL license based on Mozilla Public License 1.1
  - Java-based ID-FF, SAML and ID-WSF support, “Project Lightbulb” adds PHP and Ruby
  - (OpenID support now available too)
- Lasso (http://lasso.entrouvert.org/) - GPL or commercial license
  - C libraries offering Liberty ID-FF 1.2, ID-WSF 1.x low-level support
  - SWIGified bindings for Python, Perl, Java and PHP
- ZXID (http://www.zxid.org)
  - C, Perl (SWIGified) libraries with ID-FF 1.2, SAML 2, ID-WSF 1.x, 2 low-level support
  - C executable CGI, Perl and PHP scripts for acting as an SP
- “Conor’s Stuff” (http://www.cahillfamily.com/OpenSource/) - BSD license
  - C libraries for ID-WSF 1.x, 2.0 WSC, Java WSP libraries

# The Concordia Program


- Umbrella initiative to drive harmonization and interop of multiple identity protocols
- Based on open discussions/events to develop use cases exploring the “seams” where heterogeneous protocols meet (or don't) in deployment
- Could result in additional specs, profiles, or services being developed at Liberty or elsewhere
- Anticipates expansion of the Liberty Interoperable program
- See the wiki for use cases and to get involved
- Let's hold an IIW session on use cases...

# The Venn of identity: SAML and Liberty with a bit of context (remember **Saki**)




Thanks to Paul Madsen for the initial content and Johannes Ernst for the "three standards" paradigm!

# References

- SAML at OASIS: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
- SAML2 Basics slides: http://www.oasis-open.org/committees/download.php/20520/SAMLV2.0-basics-Oct2006.pdf
- Liberty Alliance: http://www.projectliberty.org/
- ID-FF interoperability matrices: http://www.projectliberty.org/liberty/liberty_interoperable/interoperable_products
- ID-WSF Basics slides: http://www.projectliberty.org/liberty/content/download/2661/17923/file/idwsf-basics-22jan2007-Eve Maler.pdf
- ID-SIS specifications: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_sis_1_0_specifications
- Advanced Client specs overview: http://www.projectliberty.org/liberty/content/download/2658/17911/file/AdvancedClient-20070122-Conor Cahill.pdf
- ID-SAFE FAQ: http://www.projectliberty.org/liberty/resource_center/faq/strong_authentication__1
- Concordia wiki: http://wiki.projectliberty.org/index.php/Concordia


# Thanks!
# Questions?

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