

Navigating User-Centric Identity

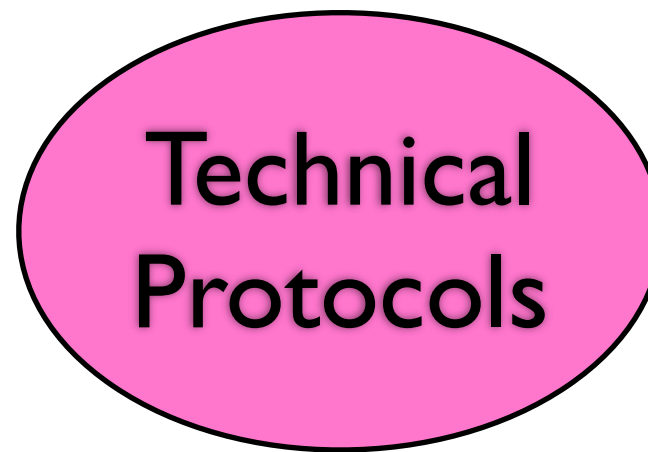
Phillip J. Windley, Ph.D.

phil@windley.org

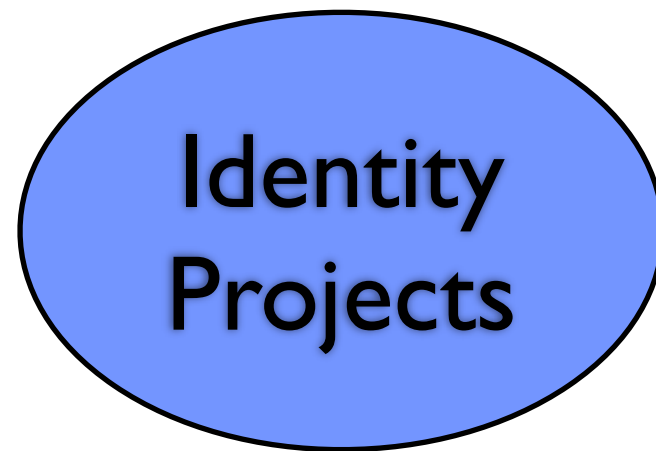
www.windley.com



**Technical
Protocols**



Technical
Protocols



Identity
Projects

**Technical
Protocols**

**Identity
Projects**

**Interop
Projects**



**Technical
Protocols**

**Identity
Projects**

**Interop
Projects**

**Industry
Consortia**



**Technical
Protocols**

**Identity
Projects**

**New
Horizons**

**Interop
Projects**

**Industry
Consortia**

Some Terminology

- Identity Provide (IdP)
- Relying Party (RP) or Service Provider (SP)
- User
- See the identity lexicon for complete list
 - <http://identitygang.org/moin.cgi/Lexicon>

Cameron's Laws of Identity

1. User consent and control
2. Minimal disclosure
3. Justifiable parties
4. Directed identity
5. Pluralism
6. Human integration
7. Consistent experience across contexts

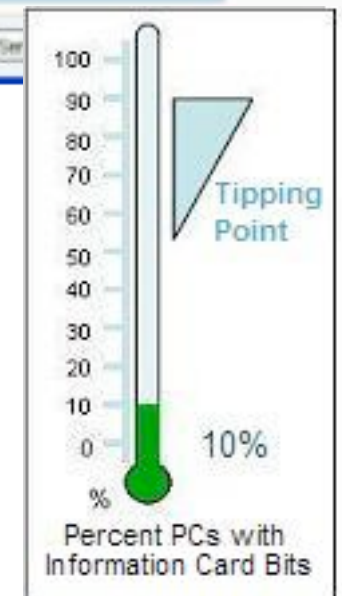
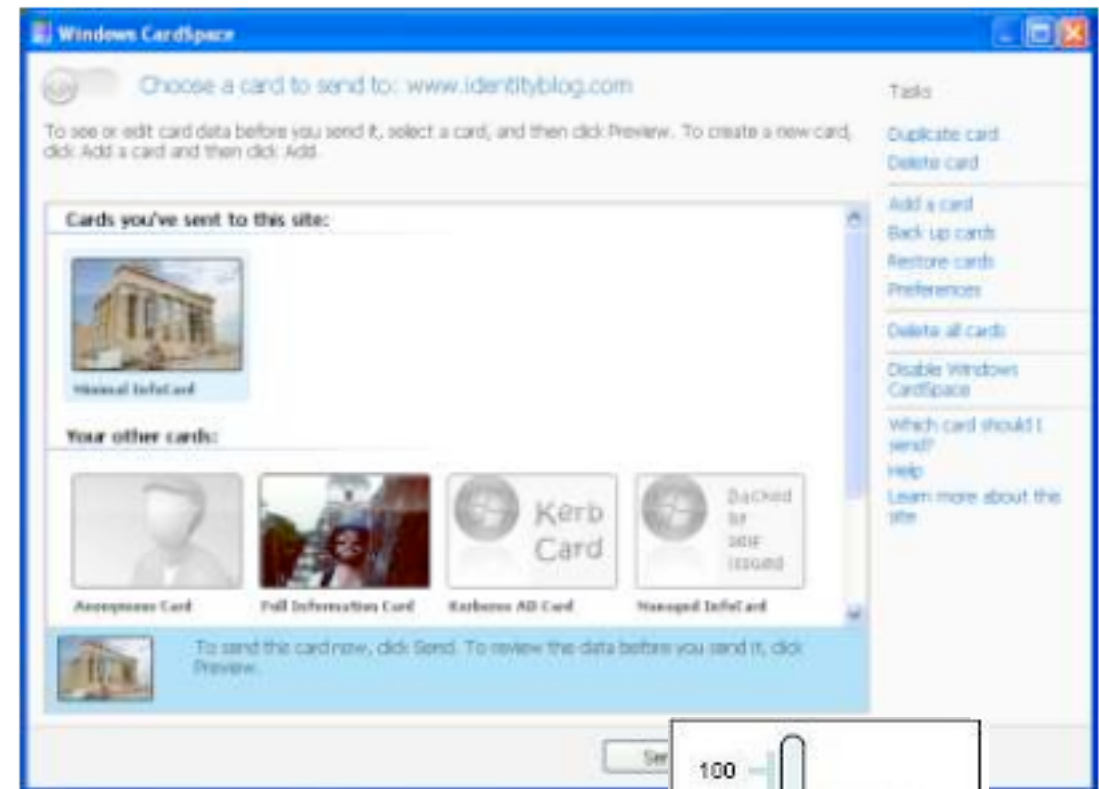




Technical Protocols

CardSpace & Information Cards

- Protocol for exchanging token-based claims
Identity selector
- WS-Trust, STS, WS-Security
- Microsoft lead, with lots of community involvement



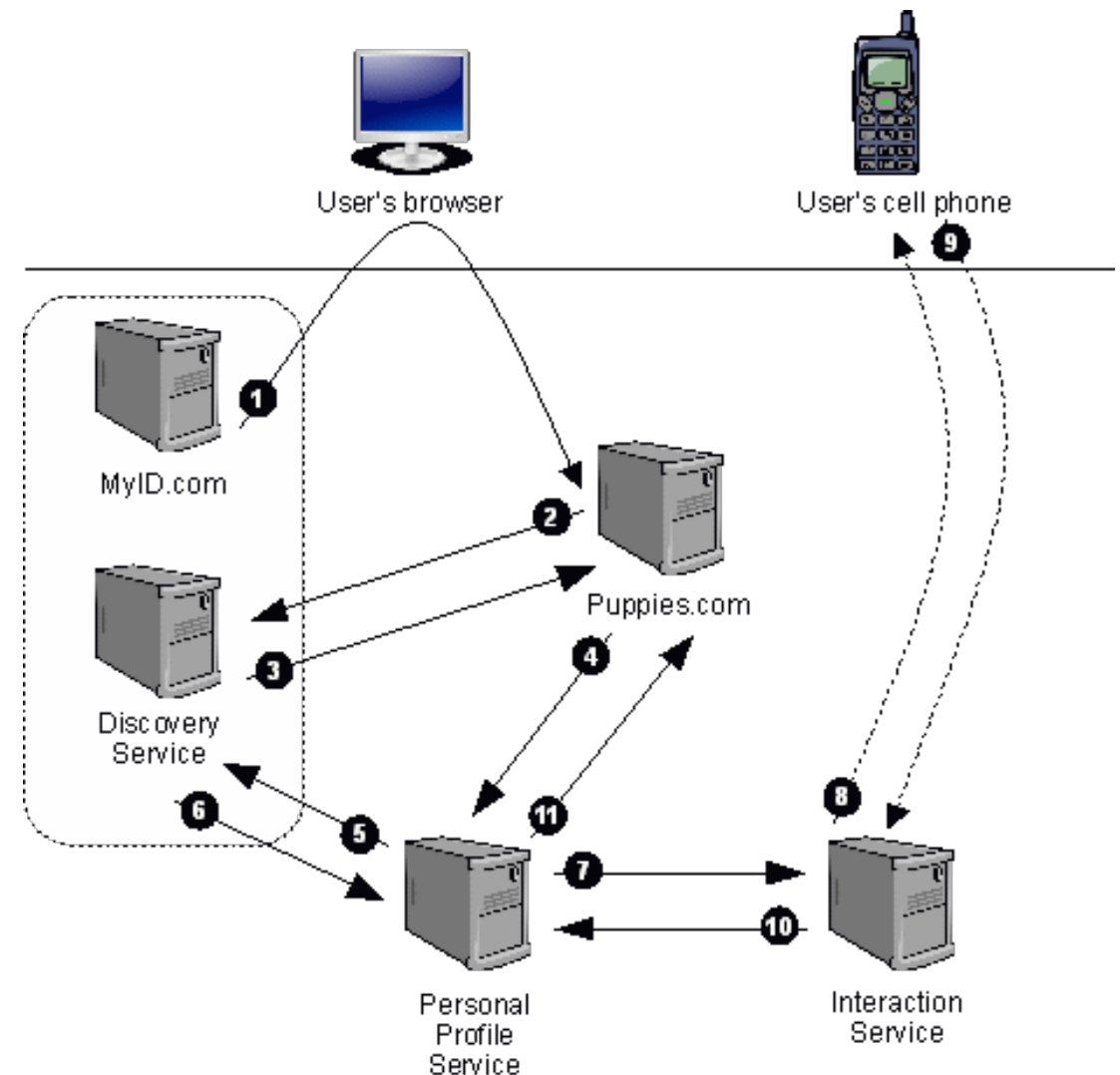


- URL-based identity
- Provides RP with evidence user has a shared secret with IdP
- AOL, Orange, Technorati, Wordpress.com, LiveJournal members all have them
- Thousands of RPs (depending on who's counting)
- 2.0 standard still not approved

SAML

- Security Assertion Markup Language
- XML framework for describing and exchanging
 - Authentication information
 - Attributes
- Used by other identity protocols (CardSpace, OpenID extensions)
- Solves used cases in it's own right

- Web services framework for identity
- Optimized for SAML
- Privacy protection
- Discovery
- Attribute sharing



OAuth

- An open protocol to allow secure API authentication in a simple and standard method from desk top and web applications
- Designed for safe delegation of authority within limits set by the user
- Mashups!

XRI

- eXtensible Resource Identifier
- Industry support for standard (OASIS)
- Persistent identifier
 - iname (=windley)
 - inumber
- Semantic tagging

XDI

- Data sharing protocol based on XRI
- XRI's provide semantic information for data via linking
- Personal profile information is a primary use case

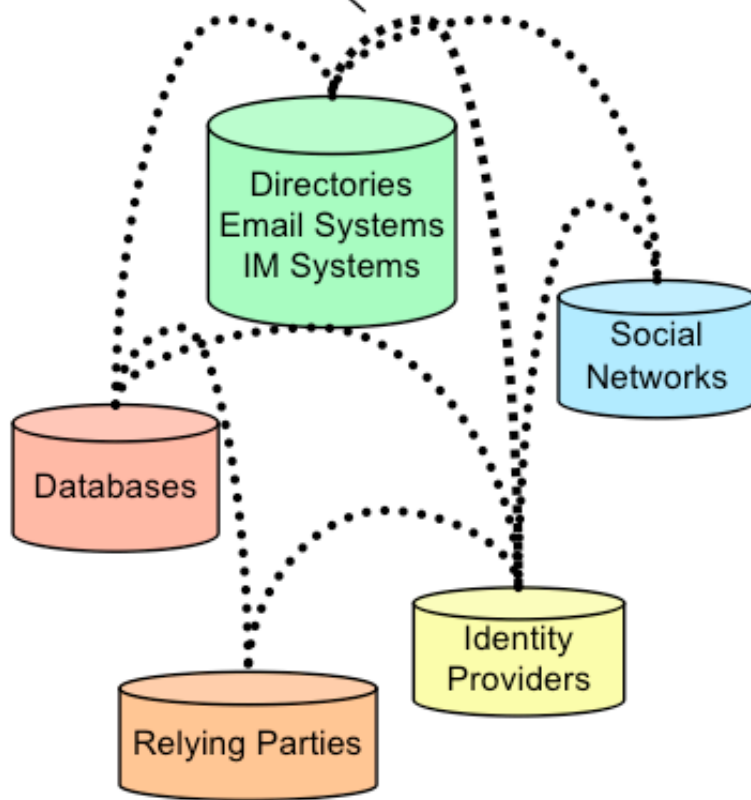


**Identity
Projects**

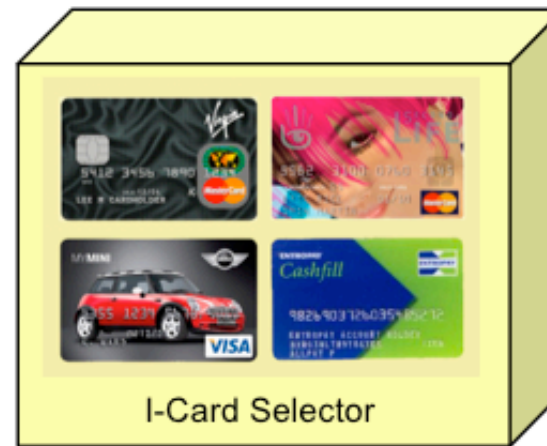


The Higgins Project

Trusted, authorized access to identity data within each context



Higgins IdAS (Identity Attribute Service) creates bridges between data islands called *contexts*.

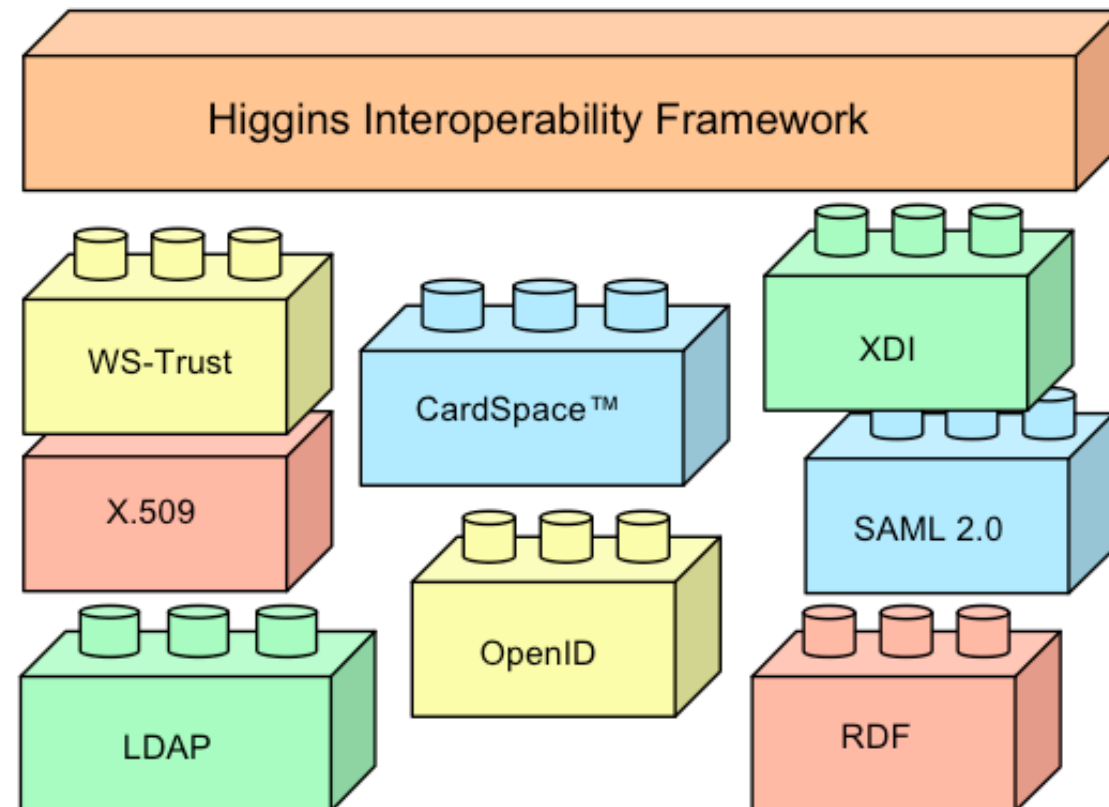


Consistent i-card user experience across multiple:

- Protocols
- Token types
- Schemas
- Data sources
- Platforms

End-user Apps

Developer Components



Bandit

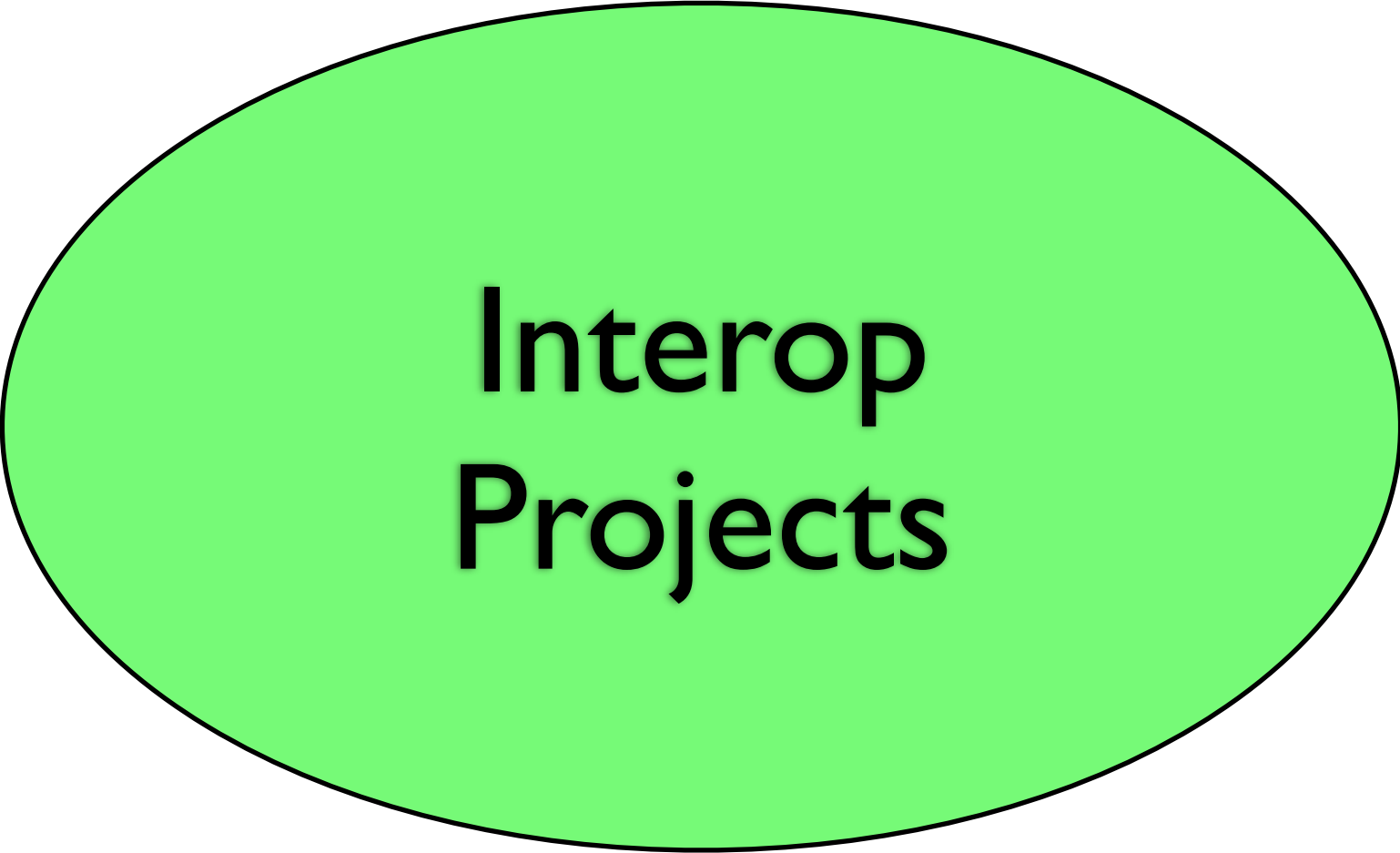
- Open source project sponsored by Novell
- Building identity components
- Multiple protocols supported
- Identity selectors for Mac and Linux



Sxipper

- Free Firefox plug-in
- Password management
- OpenID Support
- Browser-based identity selector





**Interop
Projects**

OSIS

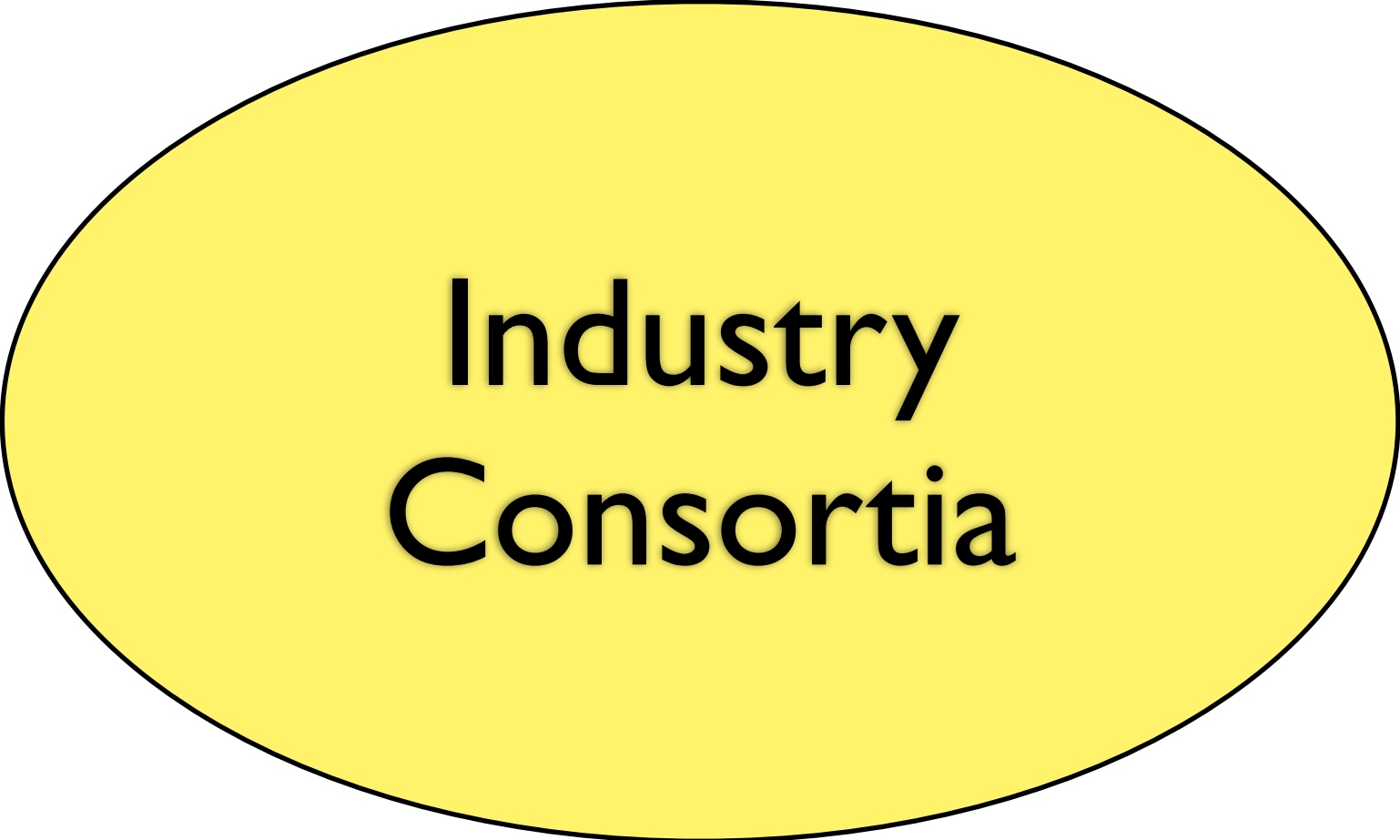
- Project interoperability
- Runs multiple interop events each year
- Identity Commons working group

Concordia

- Defines use cases for interop
- Focus on use cases not supported by current protocols
- Drives identity protocols forward
- Broad industry support

The Pamela Project

- Grassroots effort
- Support for technical and non-technical users
- Focus on relying party code development



**Industry
Consortia**

Liberty Alliance

- Industry consortium with long history in federation
- Sponsors multiple projects and working groups
- Liberty Federation
- Liberty Web services
- Open Liberty (open source)



Liberty PPEG Privacy Summits

- Public Policy Expert Group
- Discussions/meetings about privacy among
 - Industry
 - Legal
 - Academia
 - Policy
- Shared models and terminology



Shibboleth

- Roots in higher-education
- Internet2 project
- Based on SAML
- Provided RP and IdP code



Shibboleth.

ITU-T Focus Group on IdM

- Telephone standards
- Deliverables:
 - Requiements for Global Identity Management, Interoperability, and Trust (Rec X.125)
 - Standards for nextgen networks
 - Global registries for XRI, SPIDs, and network elements

OASIS ID Trust

- Founded in 1991 as PKI Forum
- Focus on trust infrastructures
 - Identity and trust infrastructures
 - Trust policies
 - Barriers and emerging issues
 - Outreach and education
- IDTrust 2008

Identity Commons

- Supports creation of open identity layer for the Web
- Serves as an umbrella legal entity for working groups
- Internet Identity Workshop, OSIS, OpenID, others
- Governed by Stewards Council



**New
Horizons**

Project VRM

- Vendor Relationship Management
- Dual of Customer Relationship Management
- Allows demand to inform supply (rather supply trying to “create” demand)



The End

Questions?

Contact me:

Phil Windley

phil@windley.org

www.windley.com

