

A short talk on a mouse with a long tail

## Higgins Trust Framework

*Enabling productivity, interoperability, and new end user experiences by integrating identity, profile, and relationship data*

- Mary Ruddy
- Paul Trevithick
- Tony Nadalin
- Dale Olds



# Eclipse Foundation

- Best known for the Eclipse Java IDE
- Has grown to include over 60 other projects
- Extensive support for plug-in architectures
- All code is under Eclipse Public License (EPL)
- EPL allows linking with proprietary code
- Project infrastructure: dev lists, CVS, Wiki, etc.

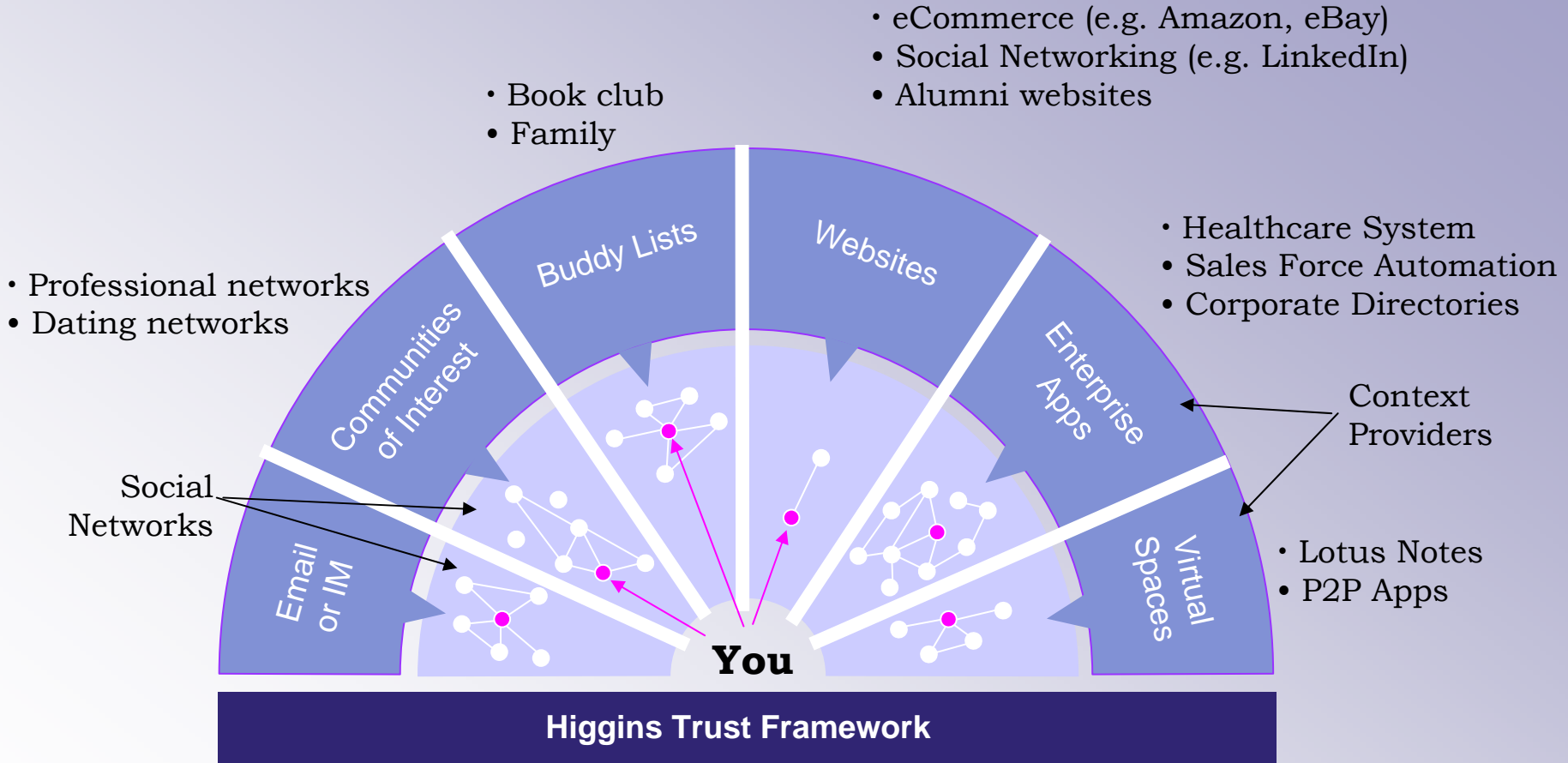


# The Higgins Vision

- Started by a small company that wanted to give users more control over their own personal information
- Necessity is the mother of invention
- We needed an infrastructure on which to build a new breed of user-centric apps
- Our needs
  - Multi-contextual foundation
  - Support for multiple personas
  - Open source
  - Support for existing protocols (not define new ones!)



# The Higgins Vision



# Growing Momentum

- 2003
  - Project started by SocialPhysics-Parity
- 2004
  - Key ecosystem event: DIDW October 2004
- 2005
  - Spring: Accepted into Eclipse
  - Summer: Initial prototype and apps
- 2006
  - February: IBM and Novell announce support
  - June: Early CardSpace™ interop demos
- 2007
  - Summer: Estimated 1.0 release date



# Ecosystem

- 12 Committers
- Committer organization include
  - IBM
  - Novell
  - Parity
- Ecosystem includes
  - Red Hat
  - Oracle
  - Ping
  - Verisign



# Trends: People and Information About Them

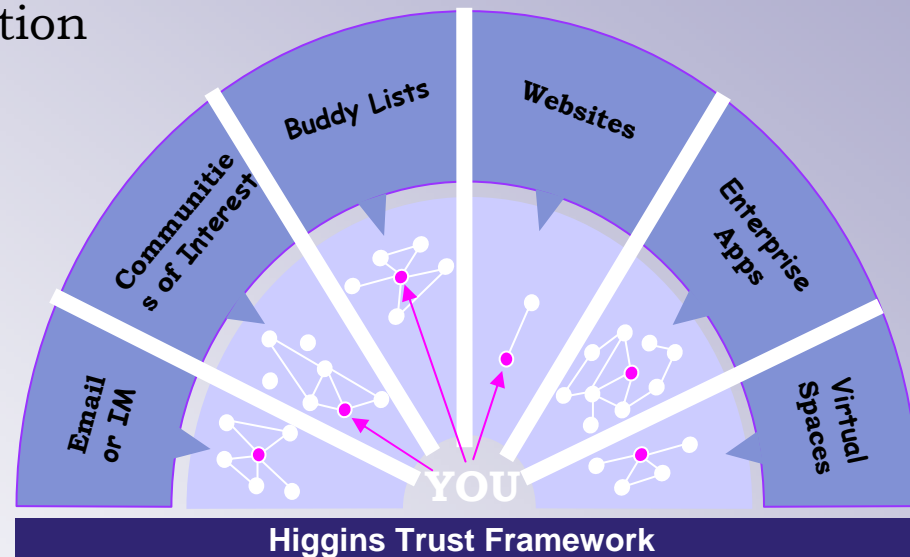
- Productivity is achieved through the integration of people with business processes
- Information about people in the enterprise is abundant and growing in richness and volume
- Information is scattered and not integrated
- A federated, digital representation will emerge
- Maintaining privacy of appropriate user information is key



# New Framework Enhances Identity Management

An Eclipse open source project supported by IBM, Novell, Parity, and others that will:

- Provide a foundation for "user-centric identity" and personal information management applications
- Enable dynamic, automatic capture of people information from disparate information repositories
- Facilitate integration with diverse identity management systems
- Ease management of identity, profile, reputation and relationship data across repositories



# For Developers: Identity Tooling

- Identity management framework
- Saves developer from learning the details of multiple identity systems
- Only one API to learn
- Relies on plug-ins to support major protocols and technologies: CardSpace <sup>™</sup>, OpenID, RSS, XRI, LDAP, etc.



# For End Users: Capabilities

## User-centric authentication

- Provides a consistent user experience
- User picks from a selection of visual “i-cards”
- Privacy-enabled claims to share only what is needed (and protect private information)

## Personal information “link & sync” services

- Remembers passwords, fills in forms
- Links and syncs your info across silos
- Gives you more control over your personal data



# For End Users: An Identity Metasystem

- Higgins provides an Identity Attribute Service to aggregate and federate information across systems and silos
- Its abstract data model can accommodate multiple heterogeneous identity systems
- Context Providers reflect identities and attributives relevant to those contexts



# For End Users: Enabling Privacy

## Manage private information

- Need to access consistent view of their data, metadata

## Share and control access to private information

- Attach (privacy, access) policies at record (e.g. medical records) or attribute (e.g., salary) level

## Present information on an “as needed” basis

- Transform attributes (e.g., bank balance = \$100k), to claims (e.g., bank balance > \$20K) as required
- Relying party only trusts the originating party (e.g. bank) and does not need to trust the transforming intermediary



# For the Enterprise

- Integrate identity, profile, reputation, and relationship information across and among complex enterprises
- Create common interfaces to identity and networking systems
- Support advanced process automation by providing “data context”



# For the Enterprise: Enabling Privacy

- Enterprise privacy policies
  - Necessary but not sufficient to enforce corporate policies through enterprise systems
- Meet scaling requirements
  - Empower users to control more of their private information
  - Empowering does not imply users can override all policies
- Consumer and employee satisfaction
- Ultimately privacy is about the user
- So let's give the user some control !



# Key Concepts

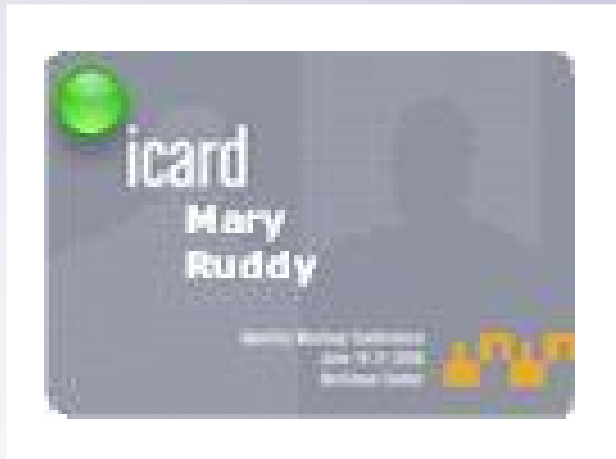


© 2006 by Parity Communications, Inc. made available under the EPL v1.0

© 2006 by International Business Machines; made available under the EPL v1.0

© 2006 by Novell; made available under the EPL v1.0

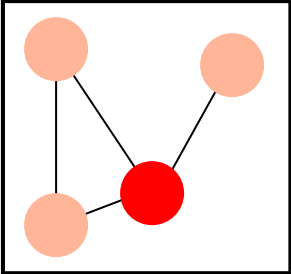
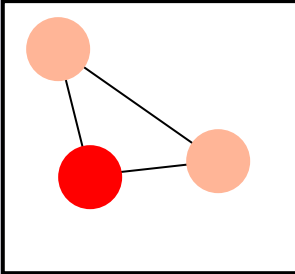
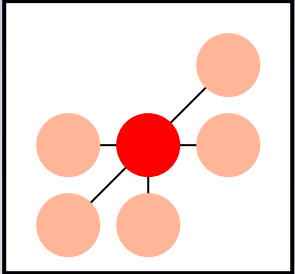
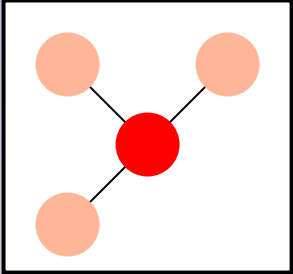
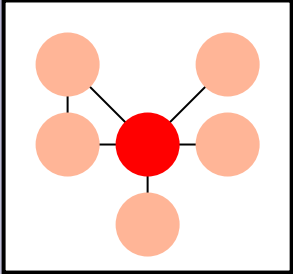
# i-cards



- Store credentials, profiles, personal data, and social networks –*not just for sign-in!*
- Dynamic or Static
- Managed or Personal
- Push or Pull synchronization
- CardSpace™ or OpenID or RSS or ...



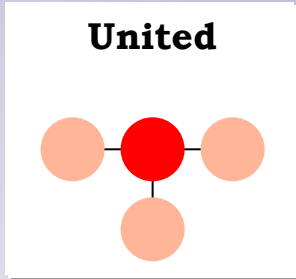
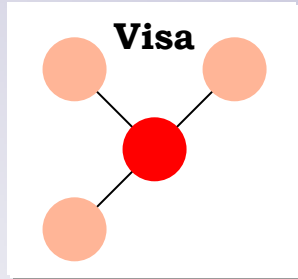
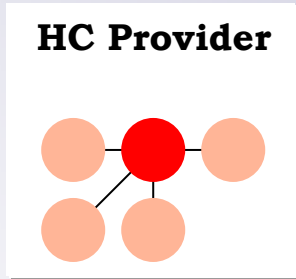
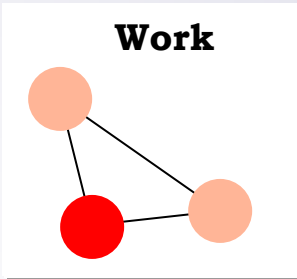
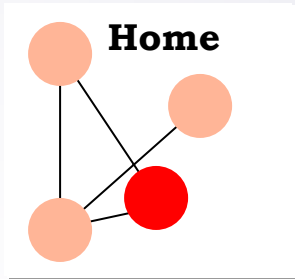
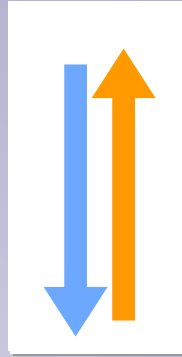
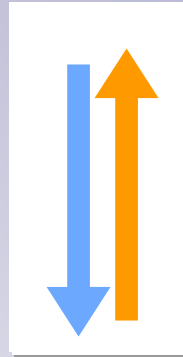
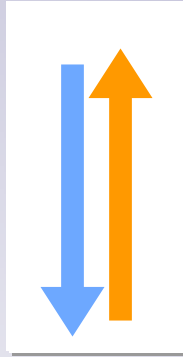
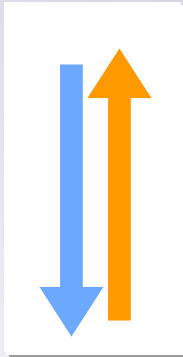
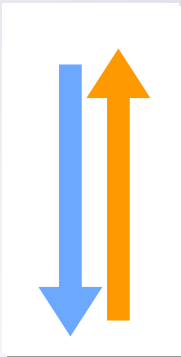
# Multiple contexts, identities, profiles & links

Home	Work	Health Provider	Visa	United
				
329 Main Street, Chestnut Hill, MA  (617) 879 9971  ptrevithick@al um.mit.edu	28 State Street, Boston, MA 02118  (617) 266 2555  paul@parityin c.net  ...	HMO, GroupID, #  Dr. James Levine  175lbs, Type O-  ...	<u>Account</u> <u>number</u>  Credit limit = \$5,000  Balance = \$1,250.22  ''	<u>PTrev</u> <u>pw=batman8</u>  Window seating, vegetarian, non-smoking, economy Marriot rewards, ...



# Existing systems and sites are adapted using Context Providers

## Higgins



# Implementation



© 2006 by Parity Communications, Inc. made available under the EPL v1.0  
© 2006 by International Business Machines; made available under the EPL v1.0  
© 2006 by Novell; made available under the EPL v1.0

# Target Platforms

- OSes and packaging
  - RPM & Debian: Suse, Red Hat, Debian, Ubuntu
  - OSX
  - Windows
  - Eclipse plugins
- Protocols
  - WS-\*, OpenID-H
  - LDAP, RSS-H
- Language bindings
  - Java, C (core components)
  - PHP, Python, Ruby (relying party enablement)



# Industry Collaboration



© 2006 by Parity Communications, Inc. made available under the EPL v1.0

© 2006 by International Business Machines; made available under the EPL v1.0

© 2006 by Novell; made available under the EPL v1.0

# Higgins is a place where vendors and other developers can collaborate on the most pressing challenges of our industry

- Interoperability
  - Across systems and vendors
  - Across protocols
  - Across platforms
- Privacy
  - End user identity rights agreements
  - Control: terms of service agreements
- User-centric foundation
  - Launchpad for entirely new user experiences

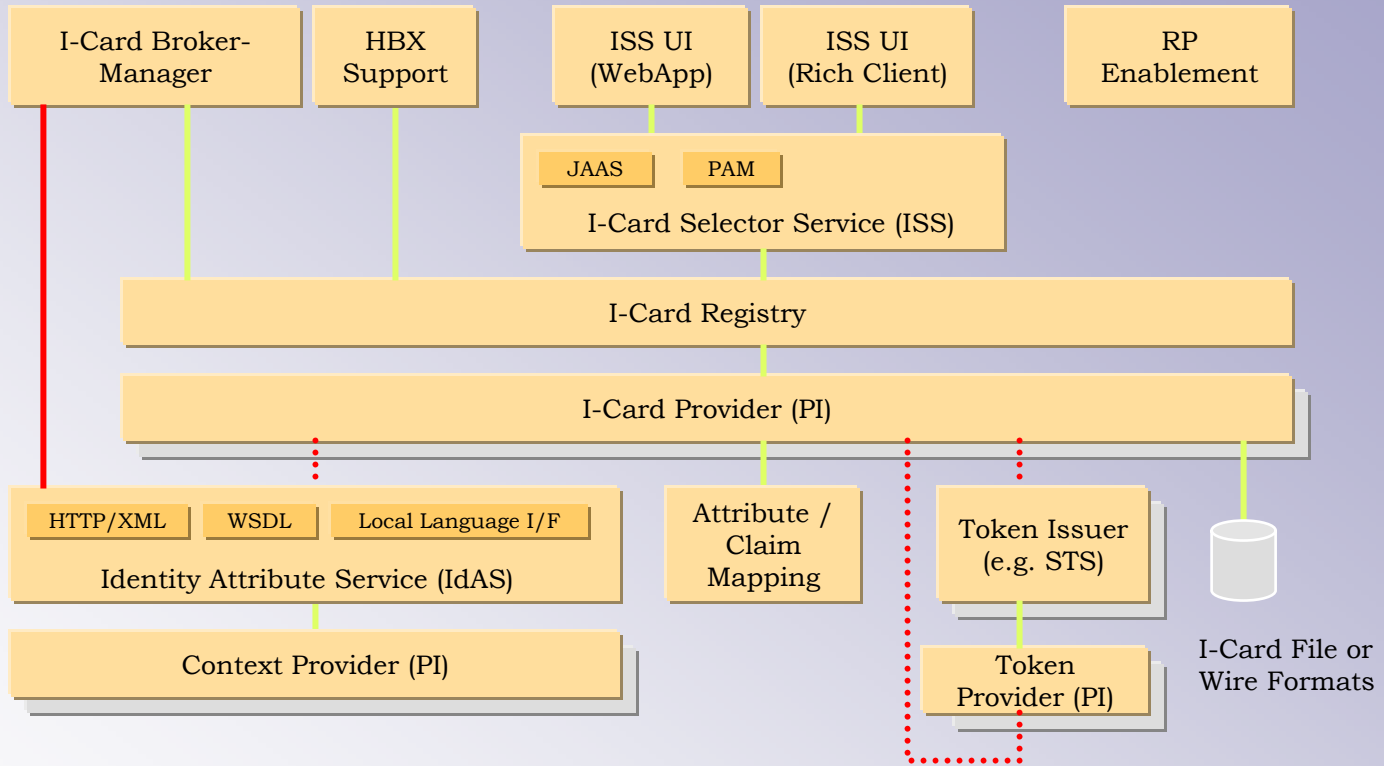


# Extra Slides



© 2006 by Parity Communications, Inc. made available under the EPL v1.0  
© 2006 by International Business Machines; made available under the EPL v1.0  
© 2006 by Novell; made available under the EPL v1.0

# Core Components



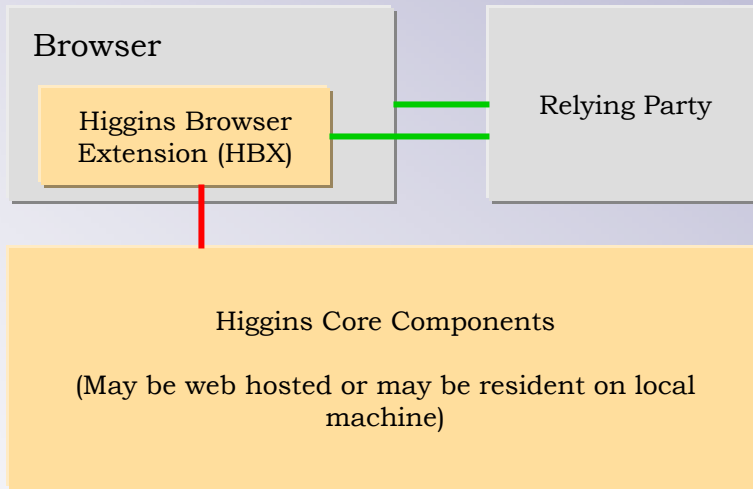
Key:



v23



# Higgins Browser Extension



Key:



# Identity Selector Service (ISS API)

- i-card provider API
- i-card operations
- Digital Identity operations
- Claims operations



# Identity Attribute Service (IdAS API)

- OWL/RDF data abstraction layer
- Context Provider (plug-ins) in the works:
  - LDAP directories
  - RSS+SSE
  - HTML screen scraping and form filling
  - Email



# Higgins Data Model

- Outermost container is a “Context”
- Contexts contain “Digital Subjects”
  - e.g. a person
- Digital Subjects have Attributes
- Attributes include
  - Credentials
  - Profiles
  - Preferences
  - Social networks



# End User Deployment: Two Components

- Higgins Browser Extension (HBX)
  - Firefox and IE
  - HBX relies on Higgins service “back end”
- Higgins service
  - Can be deployed locally or web hosted
  - Connects to Identity Providers (e.g. BofA)
  - Connects to Relying Parties (e.g. Amazon)



# Authentication Compatibility

- Compatible with protocols used by existing and emerging Identity Providers and Relying Parties
- Multi-protocol
  - CardSpace / WS-Trust
  - OpenID
  - ...more to come

