



# **ESE 2008: Higgins**

**Markus Sabadello [msabadello@parityinc.net](mailto:msabadello@parityinc.net)**

- 1:** A species of Tasmanian long-tailed mouse
- 2:** An open source identity framework being developed at the Eclipse Foundation

Higgins Identity Framework

# INTRODUCTION



# Higgins Identity Framework

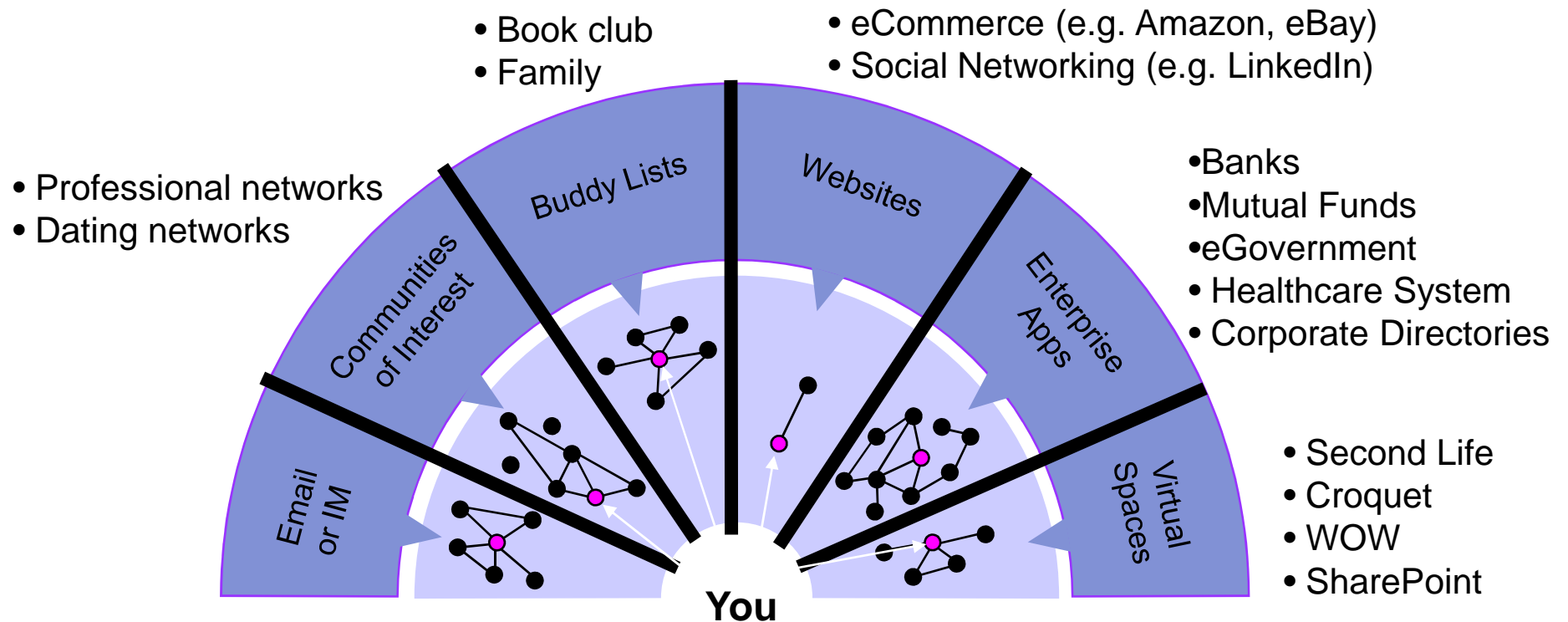
Tries to 1) model and 2) create technologies for personal Identity on the Internet.

Invents little, but implements existing standards.



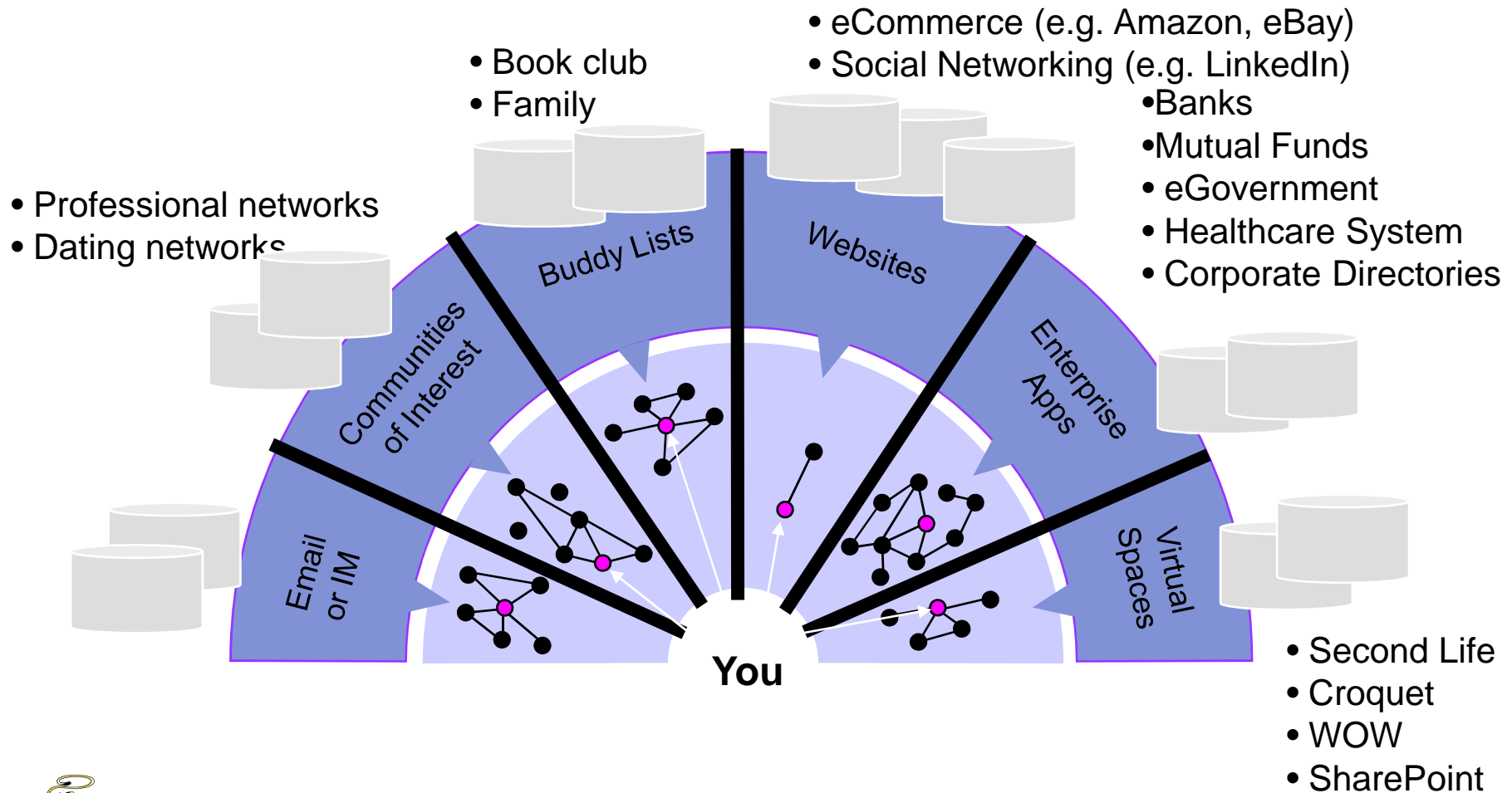
# Identity on the Internet

## Username, Password, Attributes...



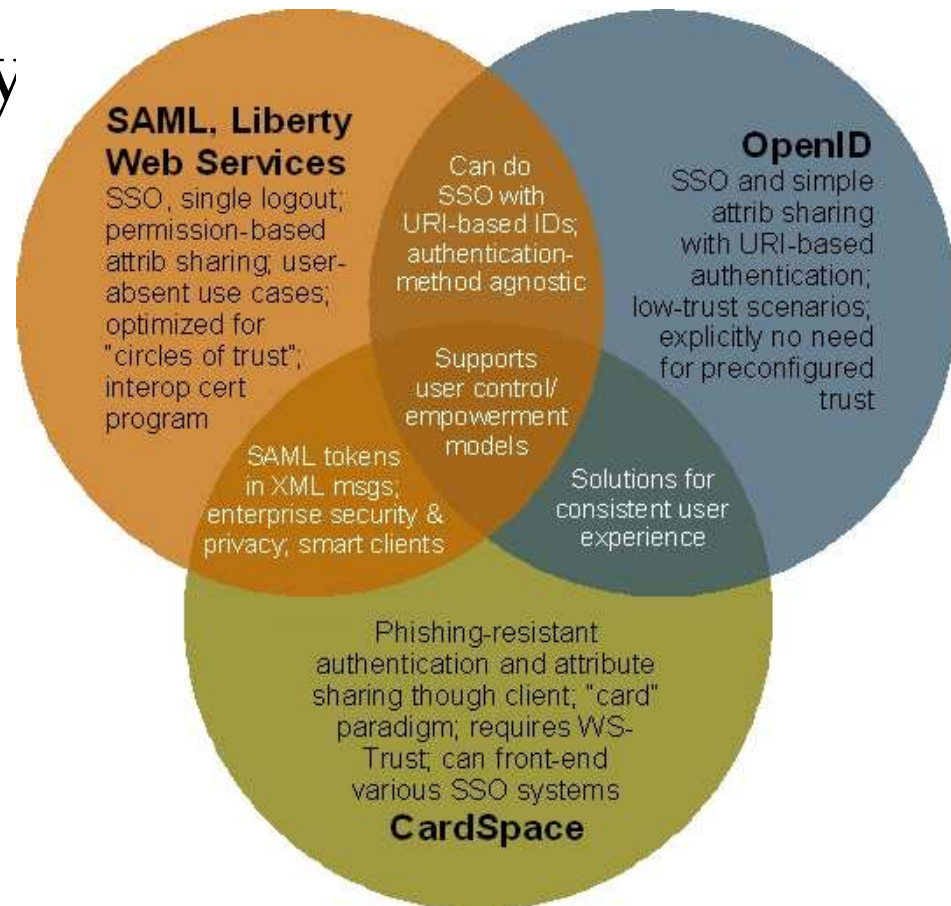
# Each Identity in its own “silo”

## Username, Password, Attributes...



# Solutions

- « Venn » of Identity
  - OpenID
  - SAML
  - Information Cards
- Goals:
  - Make life easier
  - ...and more secure



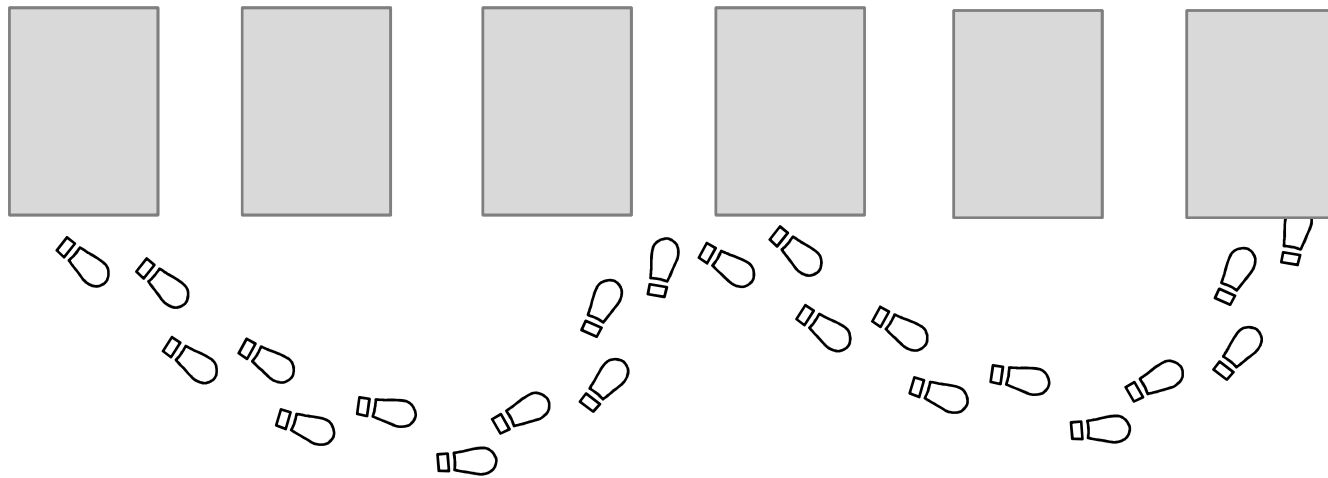
End-users experience Higgins through the UI metaphor of Information Cards using an app called an *Identity Selector*

Information Cards and selectors are just tip of the iceberg of what can be done with Higgins, but it's a place to start...



# Today you go from site to site filling in forms and passwords

Websites...

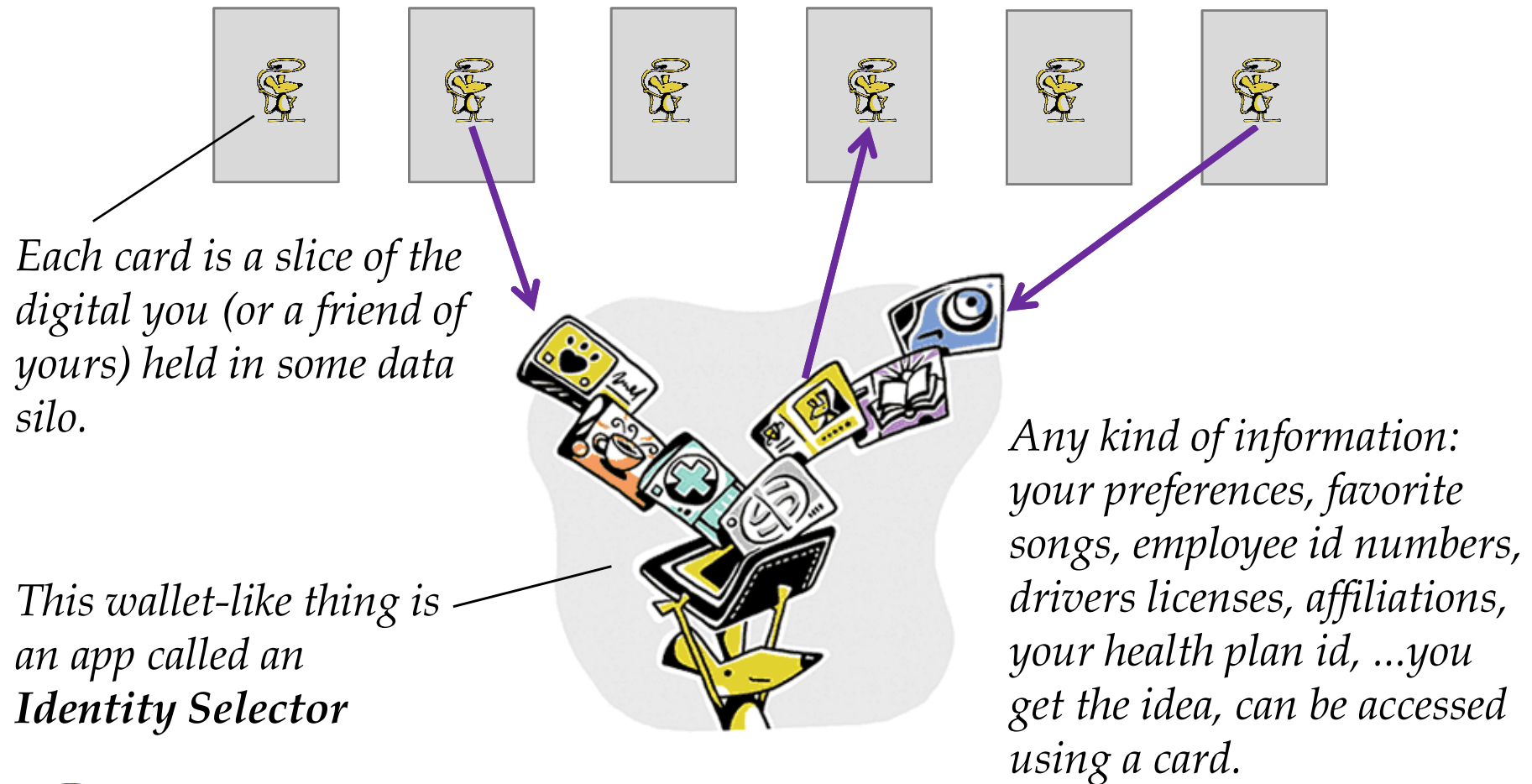


Type, type, type. Click, click.  
Here a password, there a password.  
Everywhere a password.  
Here a form, there a form, ...



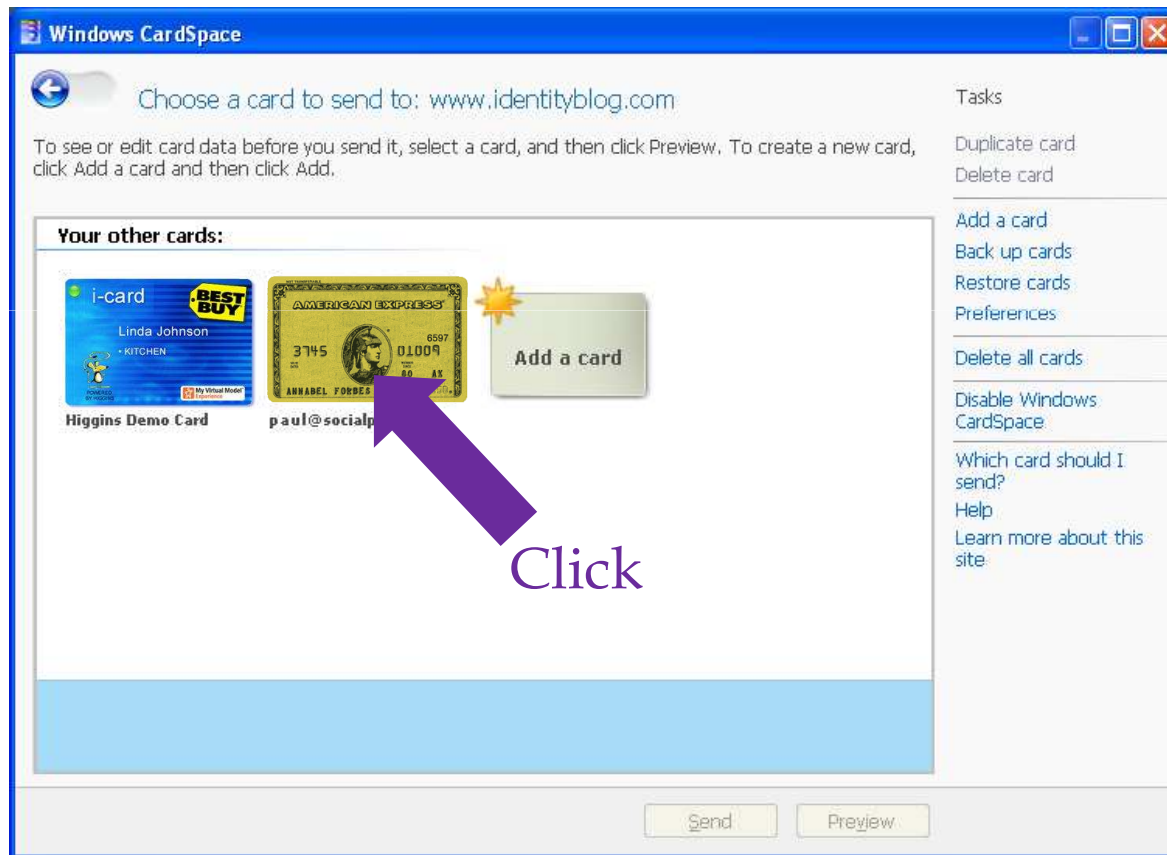


# Information Cards Put You in Control



# Identity Selector “Wallet”

Click on a card to send it to a site



Higgins is interoperable with Microsoft CardSpace™ shown here



# i-cards



## Managed

What someone (bank, government, etc.) says about you.



## Personal (aka self-issued)

What you say about yourself.



## Relationship (under development)

What you and Best Buy say about you right now.

Higgins Identity Framework

# DATA MODEL



# Context Data Model (CDM)

- Data sources are called *Contexts*
  - E.g. enterprise directories, social networks, RDF repositories
- Contexts contain objects called *Entities*
  - Entities represent people, organizations, etc.
- Entities have *Attributes*; Attributes have values
- The core semantics of the model are based on RDF & OWL

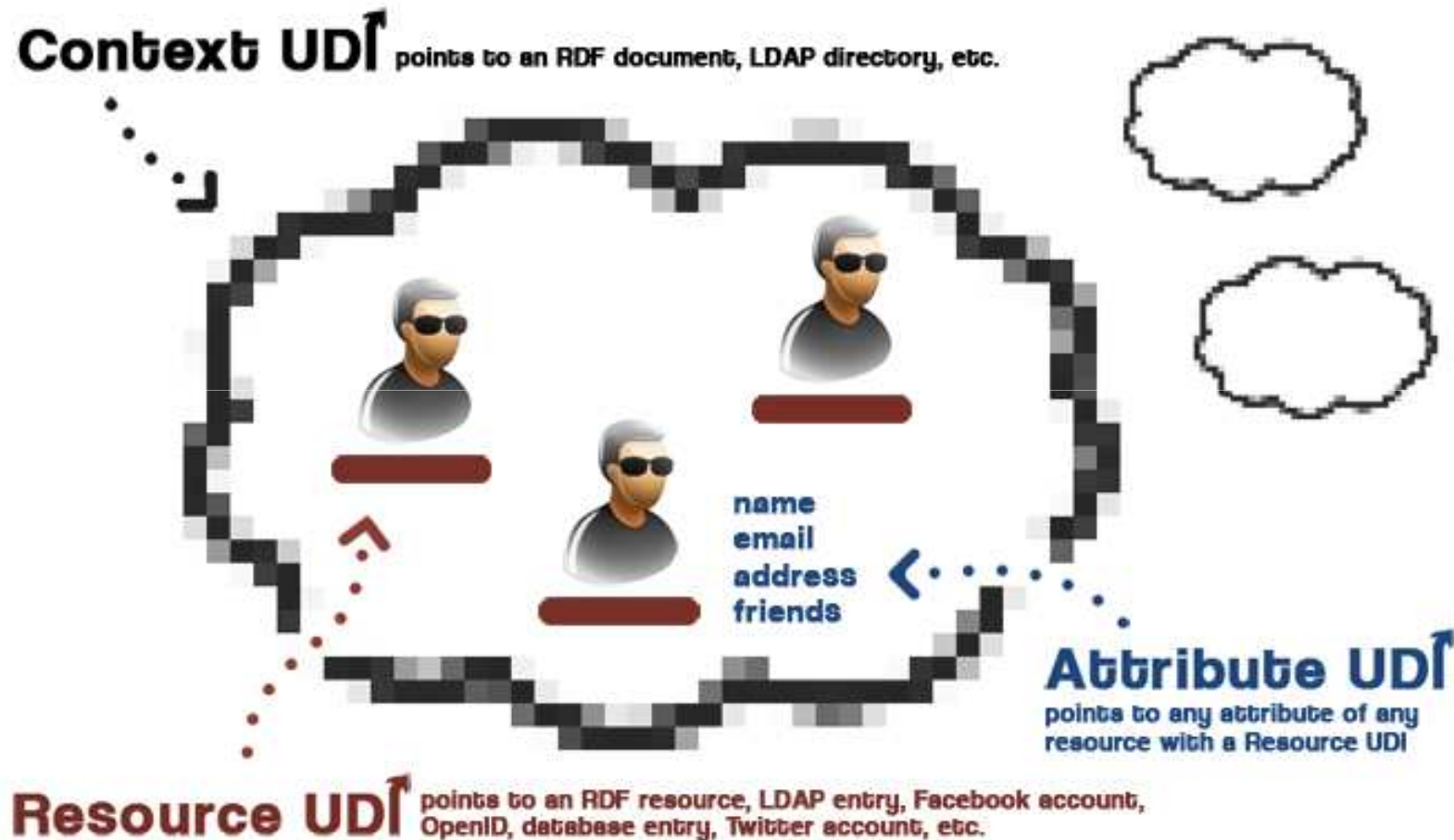


# Universal Data Identifiers (UDI)

- Globally linked data
  - Higgins uses UDIs to point to *Contexts*, *Entities* and *Attributes*
  - UDIs may be globally resolved into a global object graph, others may be local
- Different forms
  - URIs: **<http://dbpedia.org/resource/Berlin>**
  - XRI: **@parity\*contexts/(+ldap)**
  - Others



# Universal Data Identifiers (UDI)



Higgins

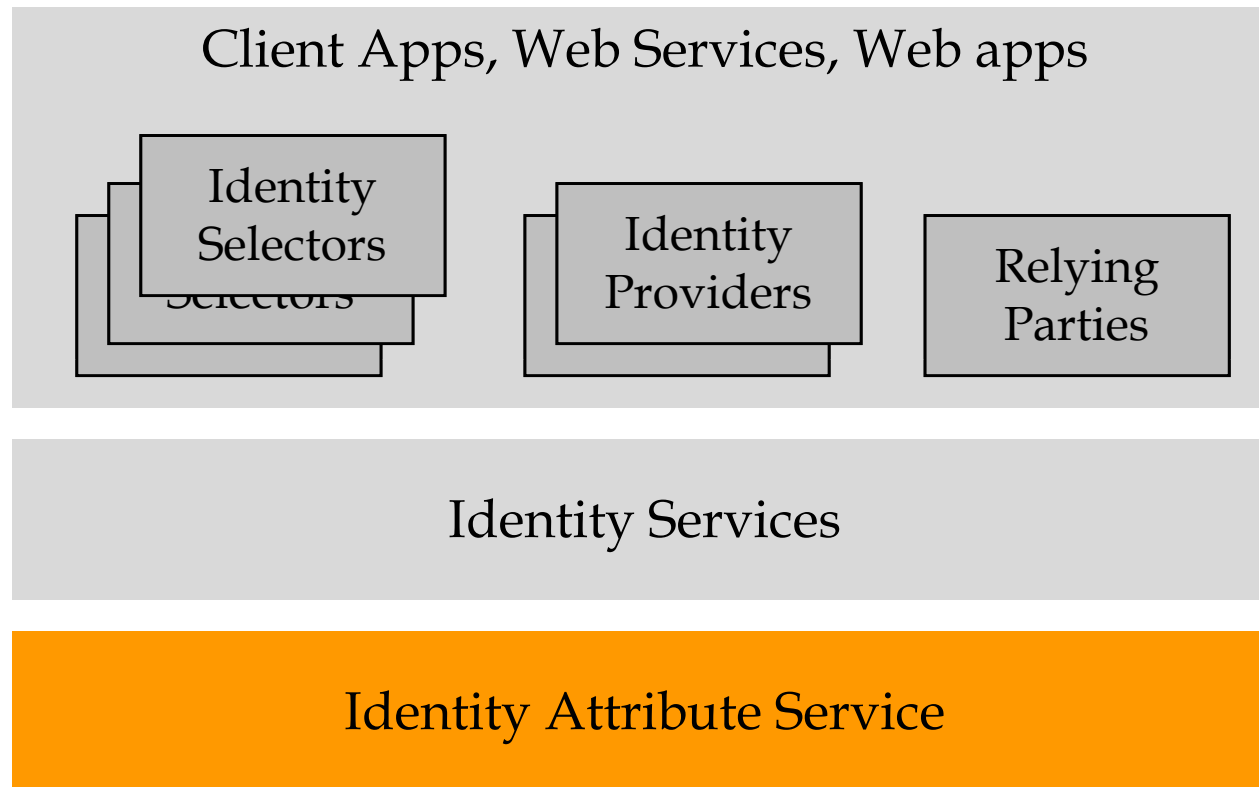
# ARCHITECTURE



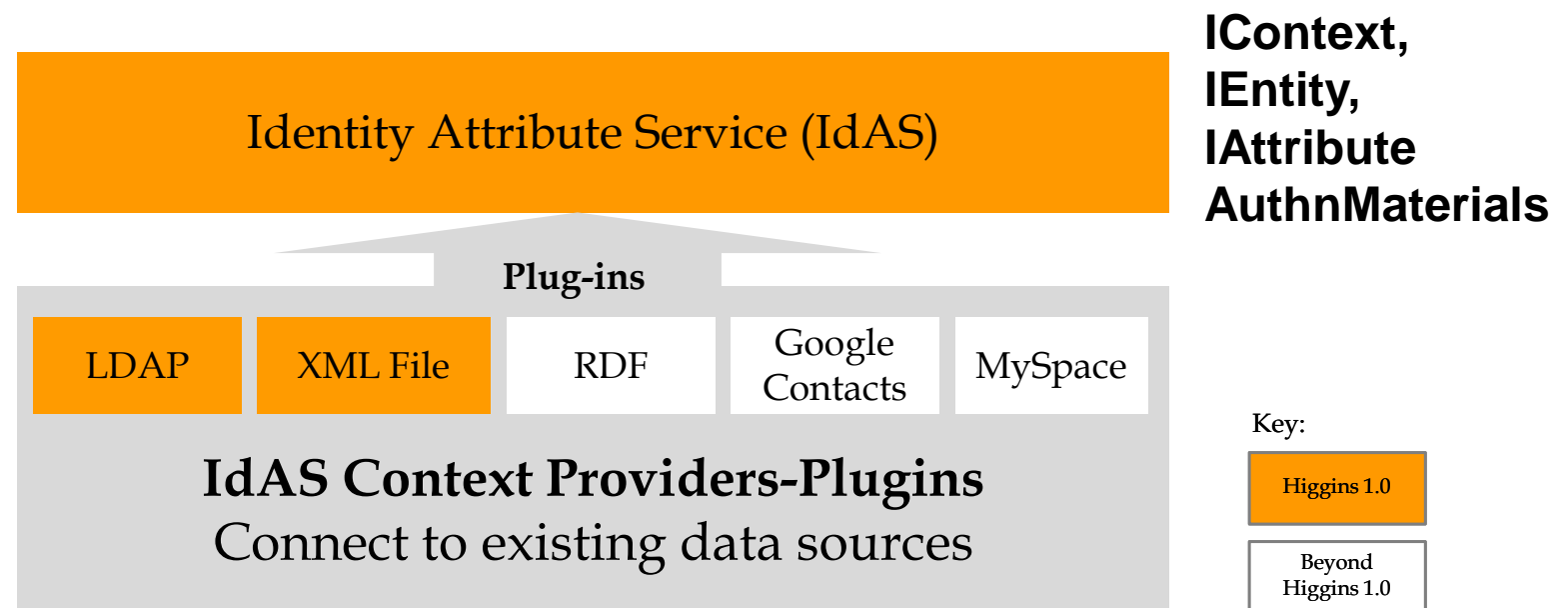


# Architecture

## Identity Attribute Service



# *Extensible* Identity Attribute Service



# Identity Attribute Service

- The Context Data Model is implemented by the Identity Attribute Service
- Abstraction Layer
- IdAS API is implemented by Context Providers
- Typical Usage:
  1. Resolve a UDI to a Context
  2. Open the Context with AuthnMaterials
  3. Look up an Entity
  4. Read/Write Attribute Values



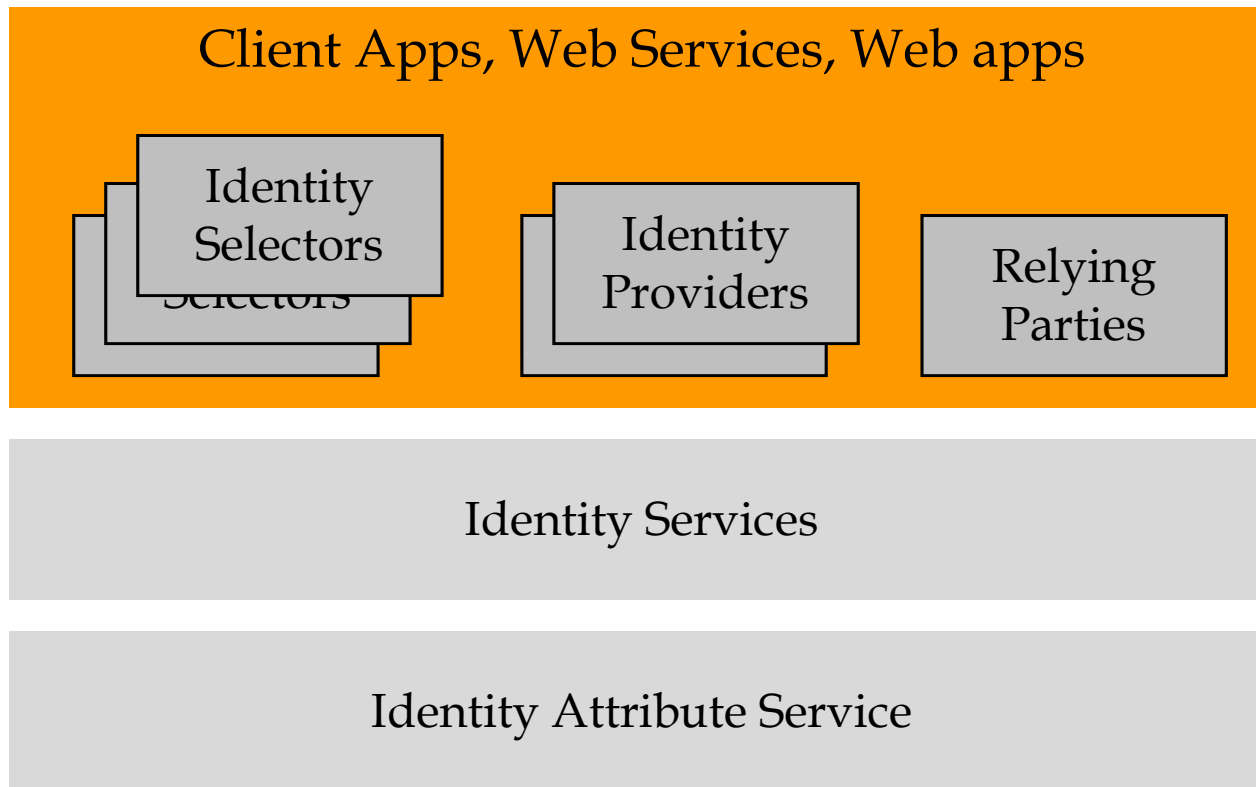
# Identity Attribute Service

- Contexts, Entities, Attributes
- Authentication Materials
- Transactions
- Filters
- Access Control



# Architecture

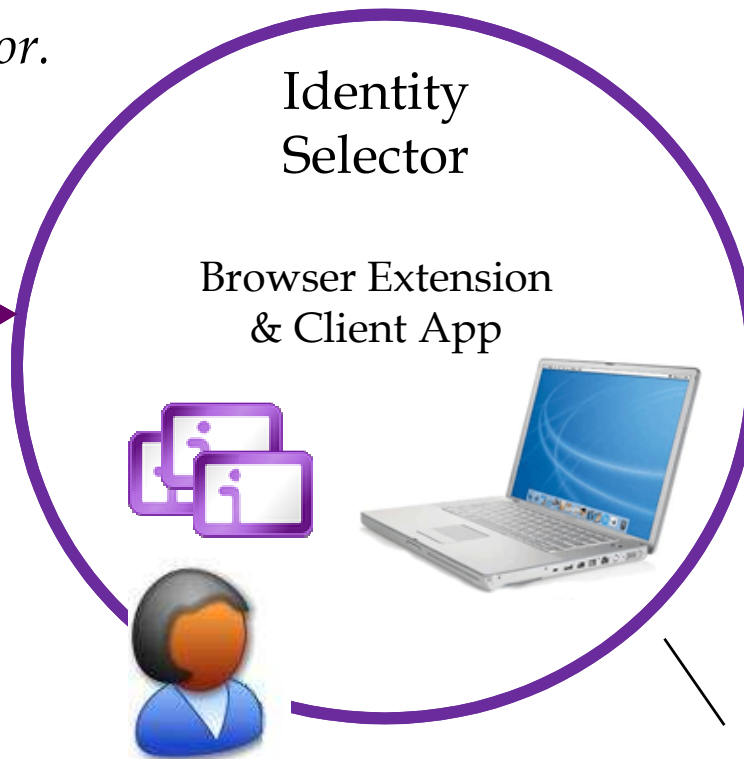
## Interoperability Points



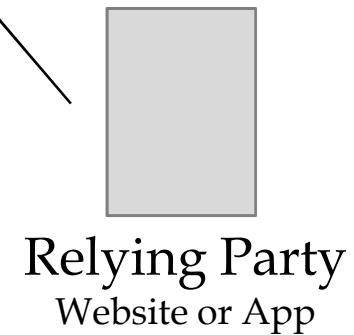
# Identity Selectors

## Cards and Tokens Flow

*Cards are generated and downloaded from here. A local Token Service issues tokens as requested by Selector.*



*Tokens containing claim data is requested and received here*

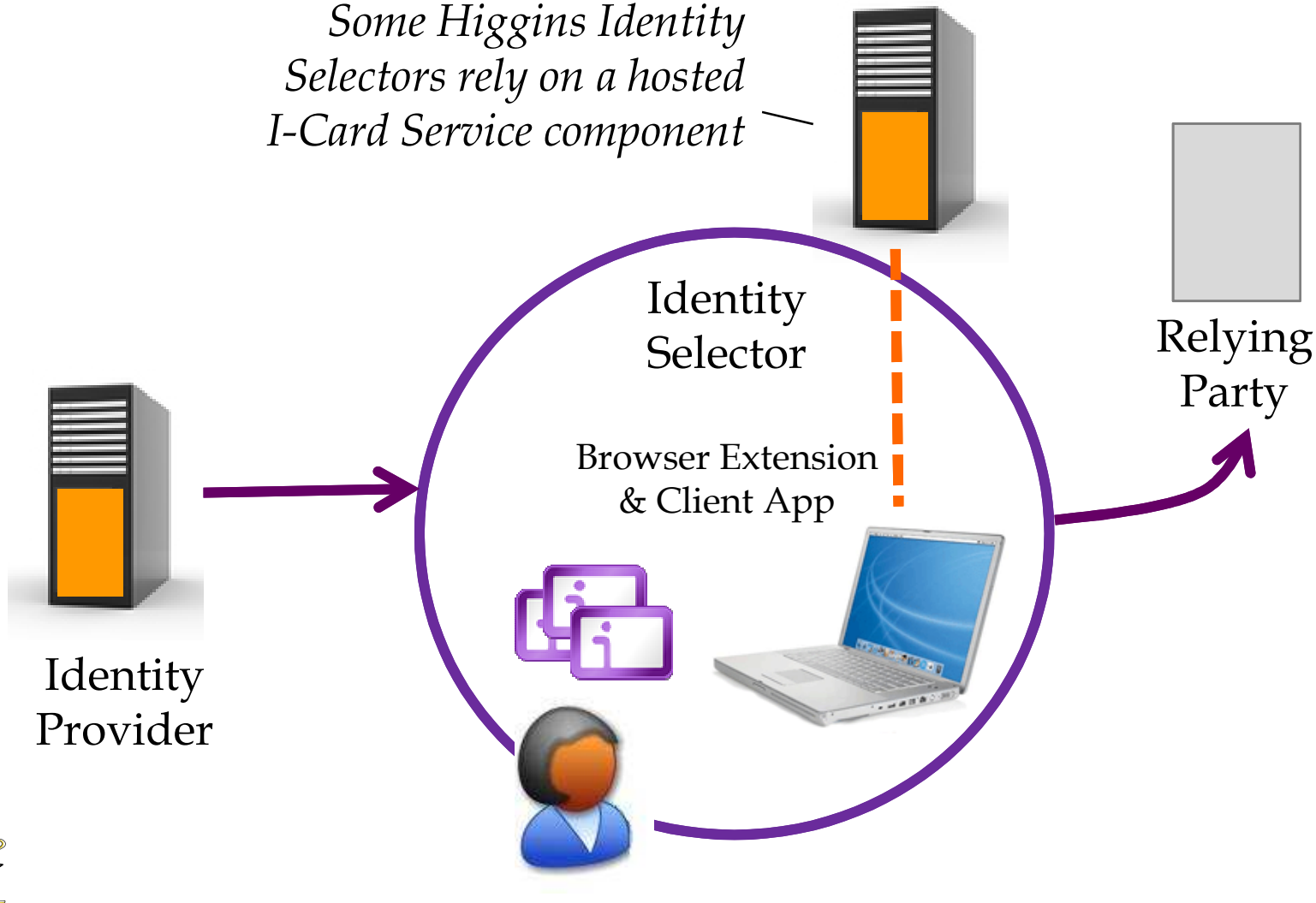


*Cards are stored and selected here*

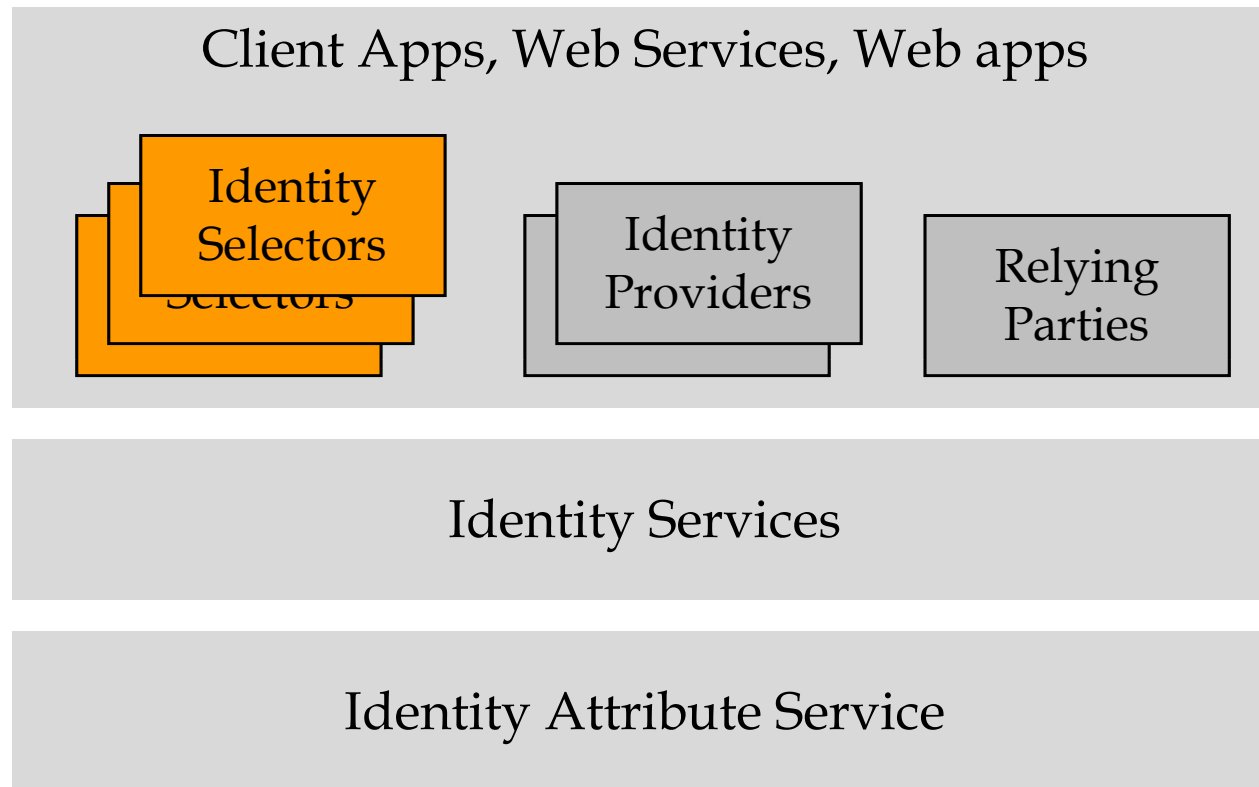
# Identity Selectors

## Cards and Tokens Flow

*Some Higgins Identity Selectors rely on a hosted I-Card Service component*



# Higgins Identity Selectors






# Identity Selectors

- Firefox-embedded Selector (Javascript)
- GTK / Cocoa Selector (C++)
- Eclipse RCP Selector (Java)
- Adobe AIR Selector
- iPhone Selector





# Adobe AIR Selector



This site is requesting a card:  
**xmlidap.org**

Site location: xmlidap.org  
Certificate issued for: xmlidap.org  
Certificate verified by: Go Daddy Secure Certification Authority in US  
[View privacy policy](#)

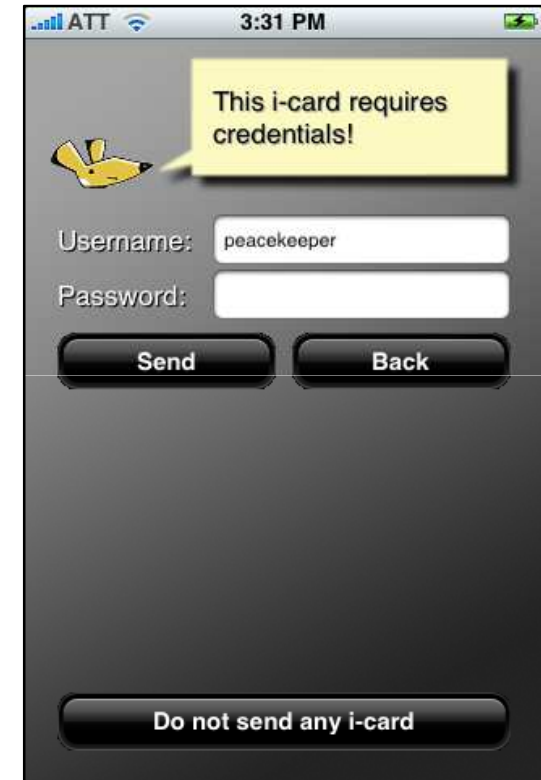
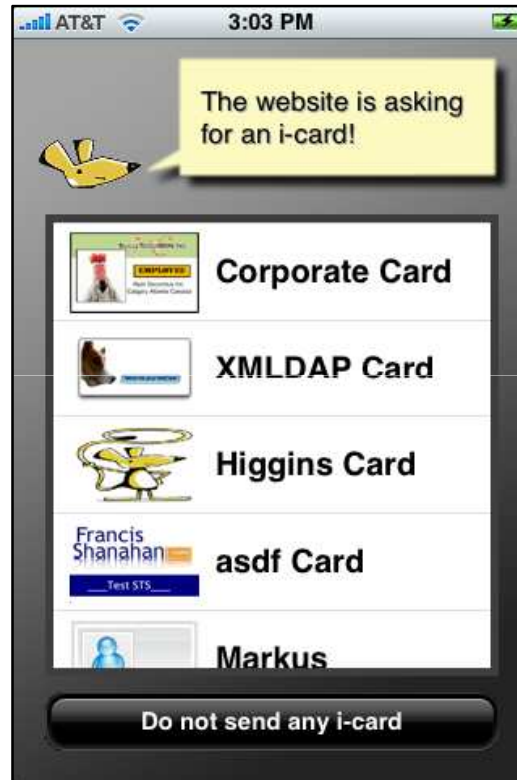
Select a card	Requested data		Value
<b>Required</b>			
	Email	<input checked="" type="checkbox"/>	slight@email.com
	Firstname	<input checked="" type="checkbox"/>	Andrew
	Lastname	<input checked="" type="checkbox"/>	slight
	SPID	<input checked="" type="checkbox"/>	
<b>Optional</b>			
	Address	<input type="checkbox"/>	123 Main St.
	City	<input type="checkbox"/>	Boston
	State	<input type="checkbox"/>	MA
	Zip	<input type="checkbox"/>	12345
	Country	<input type="checkbox"/>	USA
	Home Phone	<input type="checkbox"/>	617-456-7890
	2nd Phone	<input type="checkbox"/>	
	Mobile	<input type="checkbox"/>	617-654-3210
	Birthday	<input type="checkbox"/>	1/1/1919
	Gender	<input type="checkbox"/>	M

☐ Use this card everytime I visit this site

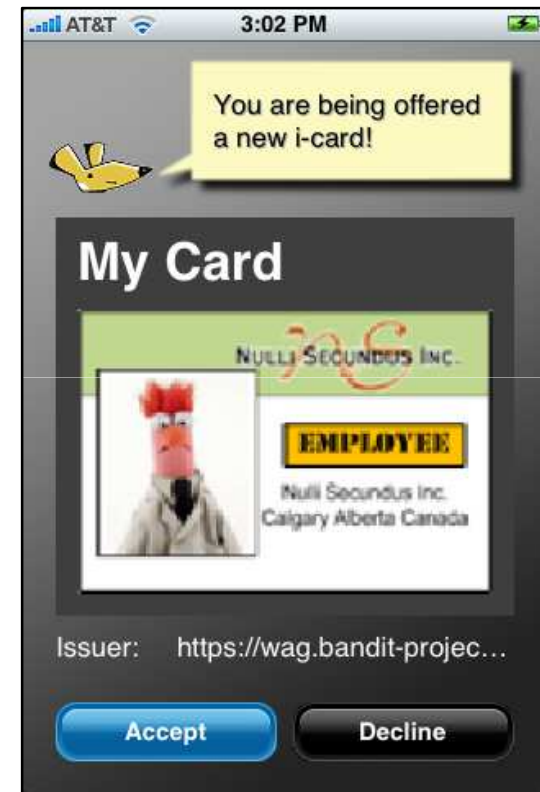
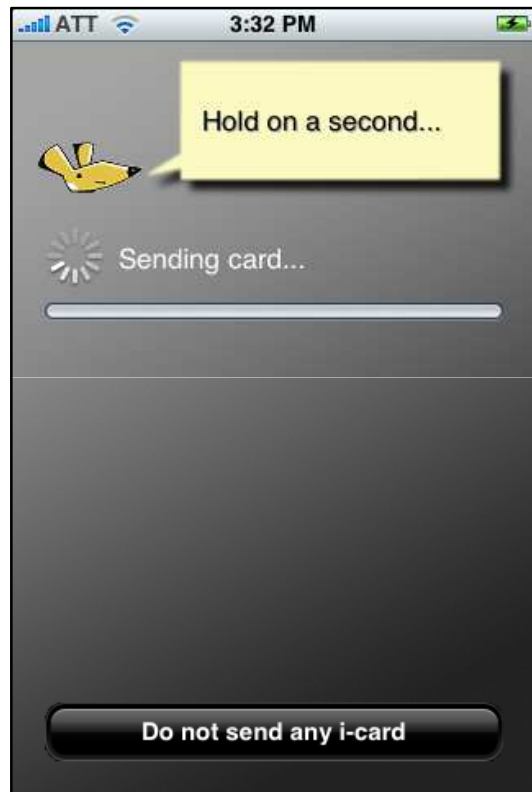
[Help](#) [Cancel](#) [Send this card](#)



# iPhone Selector

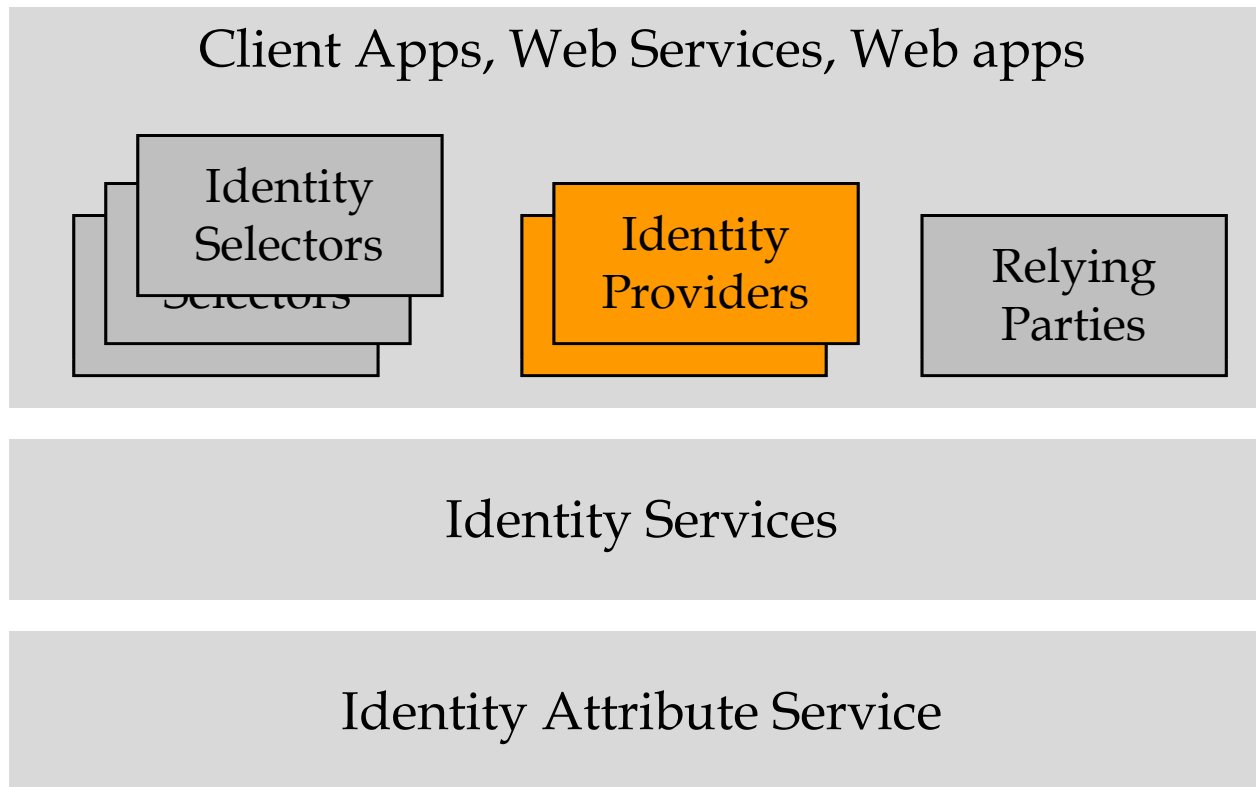


# iPhone Selector



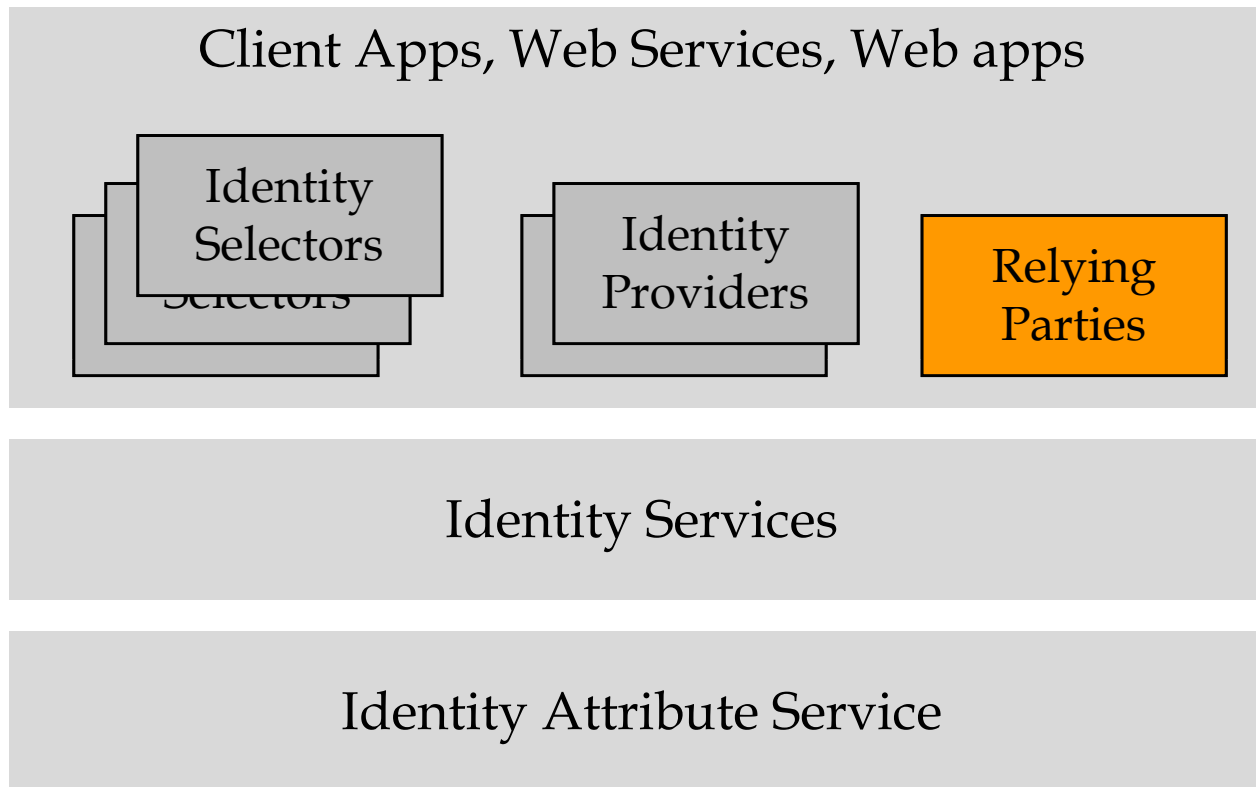
# Architecture

## Identity Providers



# Architecture

## Relying Party Website



Higgins Identity Framework

# ADVANCED COMPONENTS



# Relationship Cards



## Relationship Card

What you and Best Buy say about you





# Relationship Cards

## Human Friendly Data References



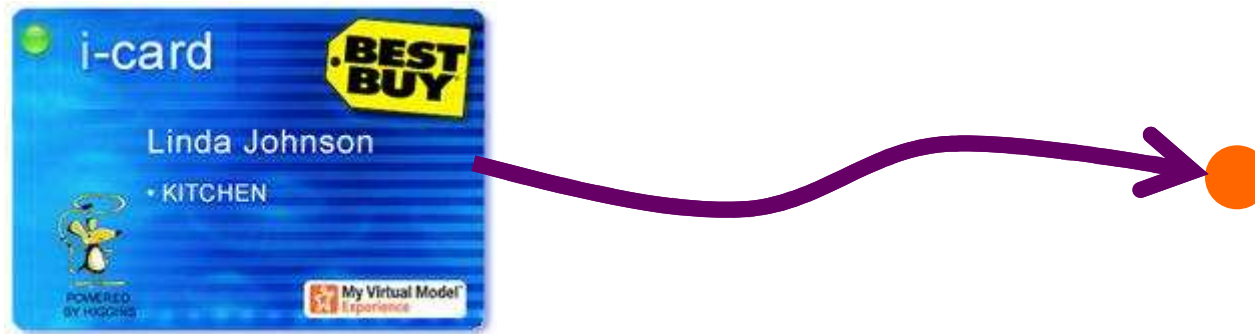
Data object  
(called an  
*Entity*)

- Card holds a UDI reference:
  - A *Context* that identifies a data source, and
  - An *Entity* within the context



# Relationship Cards

## Data Location and Authority

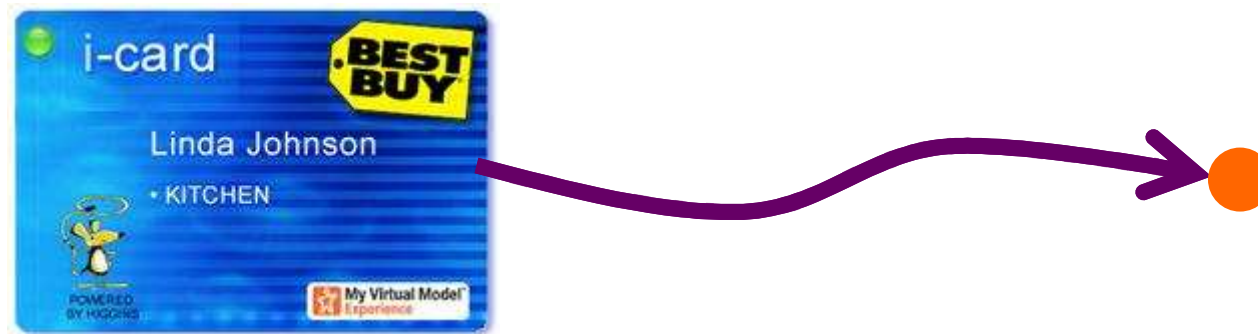


- Best Buy issued card
- Entity is stored in Best Buy's data center
- Best Buy is authoritative over some attributes
- You are authoritative over some attributes (e.g. street address)



# Relationship Cards

## Data Model



- The Entity is described by the Higgins *Context Data Model*
- Can be accessed using the Identity Attribute Service



# Other New Card Types

- Username/Password Card
  - To log in to traditional un/pw sites
- SAML Card (aka S-card) [maybe]
  - Uses SAML protocol to retrieve token
- Idemix card (aka Z-card) [maybe]
  - Support for a new privacy-enhancing token type based on zero-knowledge proofs
  - Improved support for selective disclosure



# Identity Attribute Service

## XDI Protocol Support

- XDI Engine provides a new binding for the IdAS Service
  - Allows any/all attribute data managed by IdAS to be exposed as an XDI data service
- XDI Context Provider
  - Allows IdAS to read/write XDI-native data sources



Higgins Identity Framework

# ORIGINAL PROJECT GOALS



# Goals: 1 of 5

- **Provide a consistent user experience based on card icons for the management and release of identity data**
- This is needed in order to have a trusted mechanism for authentication and other interactions that is less vulnerable to phishing and other attacks and that works for a wide variety of users and systems
- See Higgins 1.0 Identity Selector



## Goals: 2 of 5

- **Empower users with more convenience and control over personal information distributed across external information silos**
- Provide a single point of control over multiple identities, preferences and relationships
- See Higgins 1.0 Identity Selector





## Goals: 3 of 5

- **Provide an API and data model for the virtual integration and federation of identity and security information from a wide variety of sources**
- See Higgins 1.0 Framework



## Goals: 4 of 5

- **Provide plug-in adapters to enable existing data sources including directories, communications systems, collaboration systems and databases each using differing protocols and schemas to be integrated into the framework**
- See Higgins 1.0 Identity Attribute Service and Context Providers (plugins)



## Goals: 5 of 5

- **Provide a social relationship data integration framework that enables these relationships to be persistent and reusable across application boundaries**
- It organizes relationships into a set of distinct social contexts within which a person expresses different personas and roles
- See Higgins 1.0 Context Data Model (CDM)



Higgins Identity Framework

**GET INVOLVED**



# How to get involved

- Website: **<http://eclipse.org/higgins>**
- Mailing List:  
**<http://dev.eclipse.org/mailman/listinfo/higgins-dev>**
- IRC Channel: **#higgins** at Freenode
- Interop Events: RSA, OSIS
- Me: **[msabadello@parityinc.net](mailto:msabadello@parityinc.net)**



Higgins Identity Framework

**THANK YOU...**

