



Digital Identity

Rob Richards

October 20, 2009

<http://xri.net/=rob.richards>

Who Am I?

=rob.richards

Rob Richards
<personal email>
<address>
<telephone>

jbobhick
Jimbob Hick
ab3544...@nyms.net
Caribou, Maine

rob@mashery.com
Rob Richards
Sr. Software Architect

<http://rrichards.pip.verisignlabs.com/>

Username/Password Juggling

Online Banking

Enter your User ID and password. For Password changes, sign on to Online Banking. ?

User ID: [Forgot Your User ID?](#)

Password: [Forgot Your Password?](#)

Sign On



Sign in to developer.netflix.com using Mashery ID

Username

Password

Sign In

[Forget your password?](#)

GNOME Bugzilla – Log in to Bugzilla

[Home](#) | [New](#) | [Browse](#) | [Search](#) | **Find** | [Reports](#) | [New Account](#)

I need a legitimate login and password to continue.

Login:

Password:

☒ Remember my Login

☒ Restrict this session to this IP address (using this option improves security)

Log in

Sign in with your
Google Account

Email:

Password:

☒ Stay signed in

Sign in

[Can't access your account?](#)

NETFLIX


Member Sign In

Email

Password

☒ Remember me on this computer.
[What's this?](#)

Continue

 Secure Server

Not a member? [Click here.](#)

Need help signing in? [Click here.](#)



Centralized Authorities

LOCKED INTO THEIR USAGE

Google
AuthSub



Yahoo
BBAuth

A screenshot of the Windows Live ID sign-in page. The title is "Sign in to Windows Live ID website" with a "Help" link. It has two input fields: "E-mail address:" and "Password:". Below the password field is a link "Forgot your password?". A "Sign in" button is on the right. Below the button are three radio button options: "Save my e-mail address and password", "Save my e-mail address" (which is selected), and "Always ask for my e-mail address and password". There is a link "Sign in using enhanced security". At the bottom, the Windows Live ID logo is shown with the text "Works with Windows Live, MSN, and Microsoft Passport sites Account Services".

AOL
OpenAuth

Information Storage

- Concerns over privacy issues
- Security concerns / Identity Theft
- User has no idea who/what is using their information

Sidekick contacts, data gone, T-Mobile says

Phones had outages a week ago; customers told not to reset devices yet

September 29, 2009

EKU inadvertently posts sensitive info online

September 25, 2009

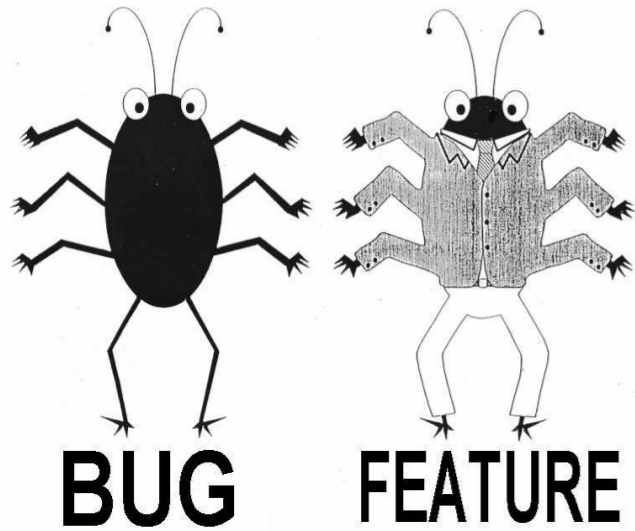
UNC Chapel Hill computer server hacked

August 20, 2009

Radisson Hotels breached

Facebook imposter scam a growing concern

Re-Invent The Wheel?



What Do Can We Do?

OpenID & Information Cards

OpenID and Information Cards

- Allow for Single Sign On
- Decentralized
 - No one entity in control
 - User has choice and freedom
- User-Centric
 - User is in control of data
 - User aware of information exchange
- Possible reduction in amount of personal information a remote site would need to store
- Potential to increase the Web experience while maintaining User privacy

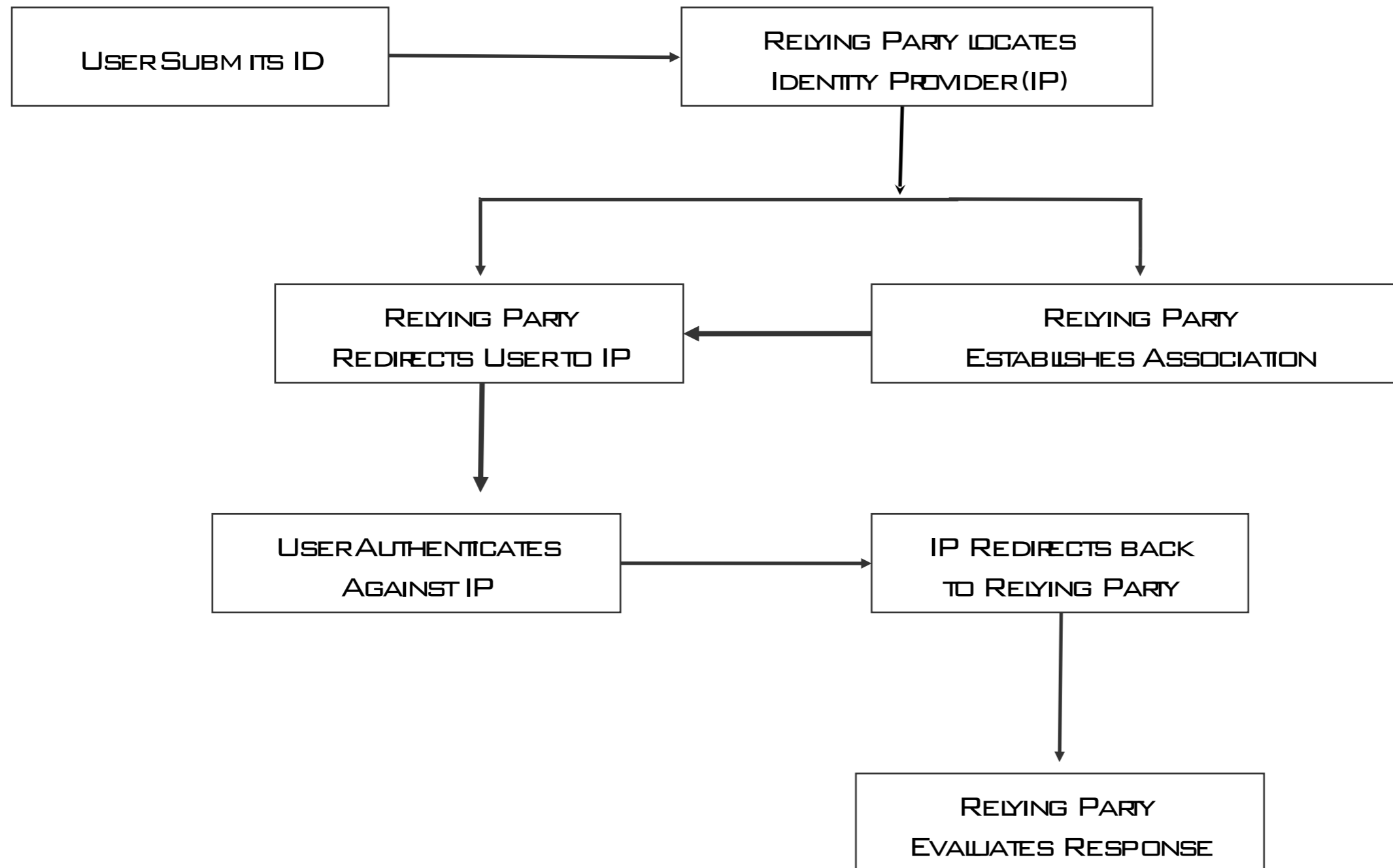
Common Terminology

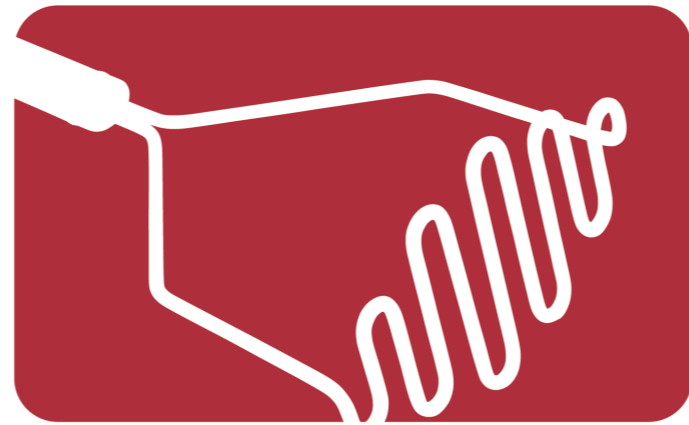
- Subject
 - Entity referenced by identity
- Digital Identity
 - Set of claims made by one digital subject about itself or another
- Relying Party (RP)
 - Site requesting identity
- Identity Provider (IdP) / OpenID Provider (OP)
 - Service that provides or maintains identity information

OpenID

- URL based
 - <http://rrichards.pip.verisignlabs.com/>
 - =rob.richards (<http://xri.net/=rob.richards>)
- Not Machine Dependent
- Based on Simplicity
 - HTTP/S
 - URLs
- PHP Libraries (There are More . . .)
 - PHP OpenID library (<http://www.openidenabled.com/php-openid/>)
 - Zend (<http://framework.zend.com/manual/en/zend.openid.html>)
 - OpenID for PHP (<http://www.openidforphp.org/>)

OpenID Interaction





MASHERY

OPENID VALIDATION EXAMPLE

Serendipity Administration Suite

CDATA Zone

Welcome to the Serendipity Administration Suite.

Please enter your credentials below.



Logon using Infocards by clicking on the above image

Logon using your OpenID

OpenID:


Username

Password


☐ Save information

OpenID Verification


[Home](#) | [Sign In](#) | [Help and Support](#)

 **Personal Identity Provider** Beta

Sign In

Enter your username and password, then click the **Sign In** button below. You may also sign in using an  [information card](#)

Sign In	
Username	<input type="text"/>
Password	<input type="password"/> Forgot my login information




Sign In

Links

- > [Sign In](#)
- > [Learn More About PIP](#)
- > [Sign Up for an Account](#)
- > [Get SeatBelt for Firefox](#)

[About PIP](#) | [About VeriSign](#) | [Contact Us](#) | [Terms of Service](#) | [Privacy](#) | © 2007 VeriSign, Inc. All rights reserved.

VeriSign (Nasdaq: VRSN) operates intelligent infrastructure services that enable and protect billions of interactions across the world's voice and data networks. VeriSign offerings include SSL Certificates, two-factor authentication, identity protection, managed network security, public key infrastructure (PKI), security consulting, information management, as well as solutions for intelligent communications, commerce, and content.









Sign In with Your OpenID

The Web site, <http://192.168.222.230/> is requesting verification that **rrichards** is your OpenID.

Complete the following form, select when you want the trust relationship for this site to expire and click **Allow**.

Click **Deny** to deny this request and return to <http://192.168.222.230/>.

* Required Information

OpenID Information	
Use the My Information section on the right to help complete the form	
* Email Address	<input type="text" value="rrichards@ctindustries.net"/>
<div><div>My Information</div><div>Click  to copy the information to the associated field on the left.</div><div><div> Full Name: Rob Richards</div><div><div> Email Address: rrichards@ctindustries.net</div><div><div> Blog: http://www.cdatazone.org</div></div></div></div></div>	
Trusted Site Expiration	
Expiration	<div><input type="radio"/> Never Expire</div> <div><input type="radio"/> Expire on: <input type="text" value="Mar"/> <input type="text" value="08"/> <input type="text" value="2008"/></div> <div><input checked="" type="radio"/> Expire After Signing In</div>

Deny

Allow

OpenID validated

Serendipity Administration Suite

CDATA Zone

Logged in as Anonymous (Administrator)

- Frontpage
- Personal Settings
- Entries
 - New Entry
 - Edit Entries
 - Comments
 - Categories
 - Static Pages
- Media
 - Add media
 - Media library
 - Manage directories
 - Rebuild Thumbs
- Appearance
 - Manage Styles
 - Configure Plugins
- Administration
 - Configuration
 - Manage users
 - Manage groups
 - Import data
 - Export entries
- Back to Weblog
- Logout

Welcome back, Rob Richards

[Return to Weblog](#)

Further Links

[Serendipity Homepage](#)

[Serendipity Documentation](#)

[Official Blog](#)

[Forums](#)

[Spartacus](#)

[Bookmarklet](#)



Delegation

- Use your own site without having to be an OpenID Provider
- Delegate authentication

```
<link rel="openid2.provider openid.server"
      href="http://https://pip.verisignlabs.com/server"/>
<link rel="openid2.local_id openid.delegate"
      href="http://cdatazone.org"/>
```

Simple Registration Extension

Basic attributes can be send to Relaying Party
from OpenID Provider

openid.sreg.nickname

openid.sreg.email

openid.sreg.fullname

openid.sreg.dob

openid.sreg.gender

openid.sreg.postcode

openid.sreg.country

openid.sreg.language

openid.sreg.timezone

OpenID 2.0

- Attribute Exchange Extension
 - Extensible attribute support
 - Identity Provider can be asked to store certain attributes
- Extension Support
 - Namespaced extensions
- Directed Identity
 - URL can identify Identity Provider
 - Identity Provider determines what ID to send to Relying Party
- Official i-name Support

OpenID: Potential Issues

- Phishing / Pharming
- Cross-Site Scripting (XSS) / Cross-Site Request Forgery (CSRF)
 - Feature to trust sites and not require login
 - Attacker could access sites unbeknownst to user
- DNS Poisoning
- Web Page Defacement
- Realm Spoofing
 - Open Redirect Servers
 - XSS exploited
- ID recycling
- Your provider knows every site you use your id on

Information Cards: Identities

Identities represented as cards in a wallet

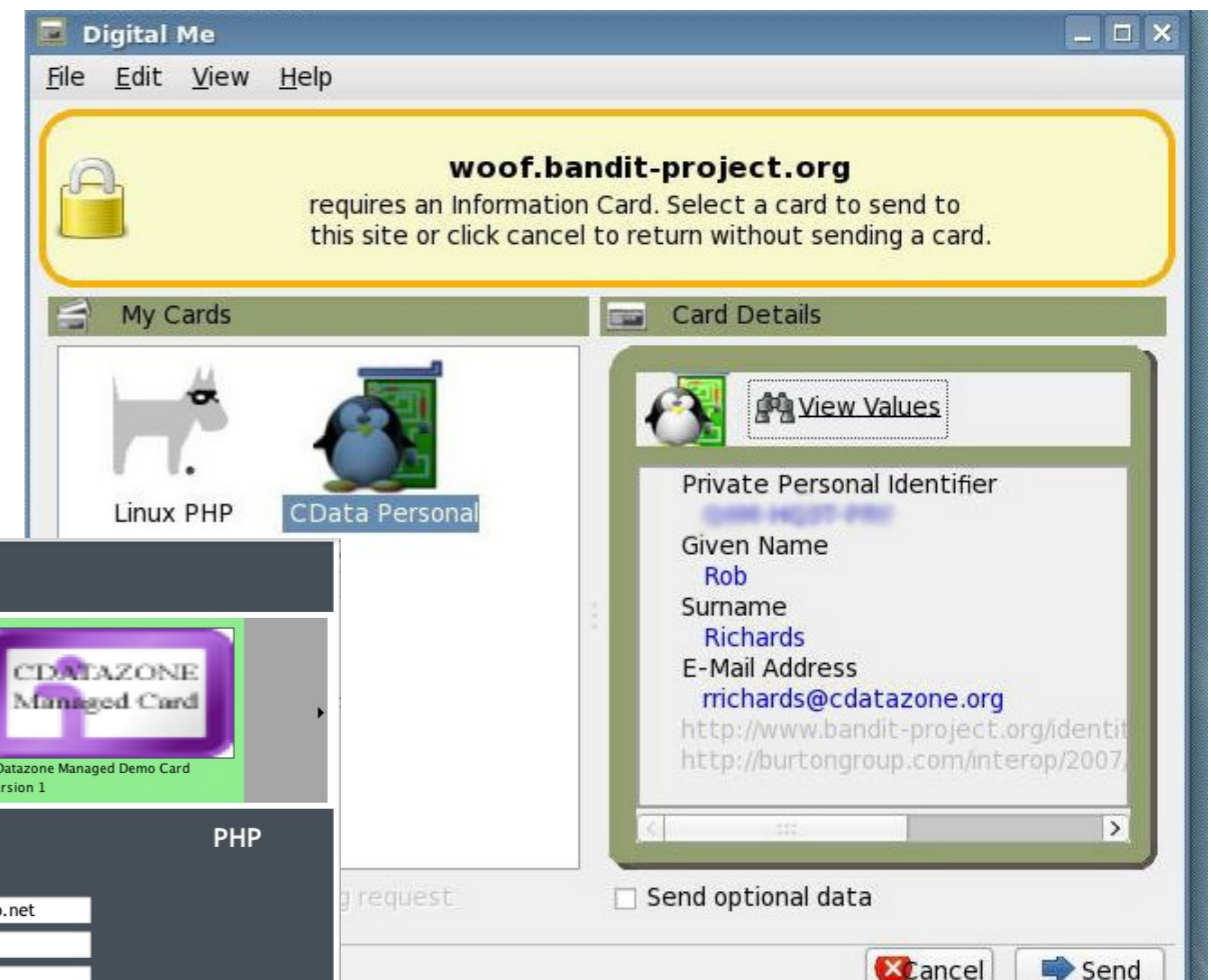
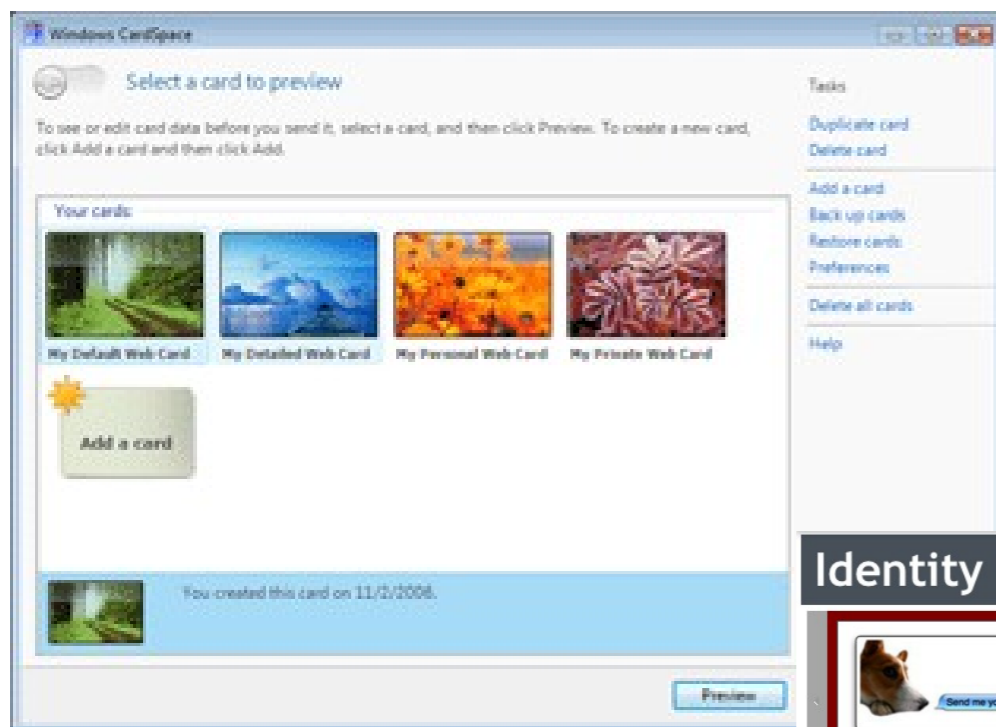
- Self Asserted
- Managed (Third Party provided)



Information Cards: Selectors

CardSpace != Information Cards

Information Cards are not Microsoft specific

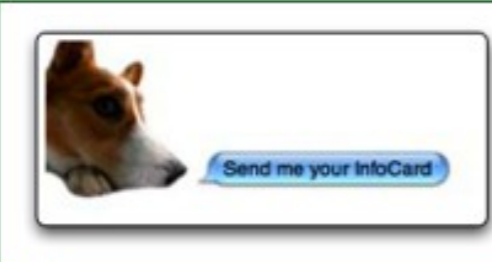
Two overlapping screenshots of forms. The top one is the "Identity Selector" dialog, which shows three card options: "PHP Version 1" (with a dog icon), "VeriSign Labs Personal Identity Provider Account Card" (with a checkmark icon), and "CDatazone Managed Card Version 1" (with a penguin icon). The bottom one is the "Self Asserted Card" form, which is a data entry form for a "PHP" card. It has fields for: First Name (Rob), Last Name (Richards), Street, City, State, Zip, Country, Email (rrichards@php.net), Phone, Mobile Phone, Other Phone, Date of Birth, Gender, and Image URL. At the bottom are buttons: "Use this Card", "New Card", "Delete Card", and "Cancel".

Information Cards


- Identifier is unique amongst parties
 - Distinct digital key for each realm
- Protections against Phishing
 - Visual indicators of previous interactions
 - x509 certificate checking
- Complex Technologies
 - SAML
 - WS-Security / WS-Policy / WS-Trust
 - x509

Information Cards: Making Claims

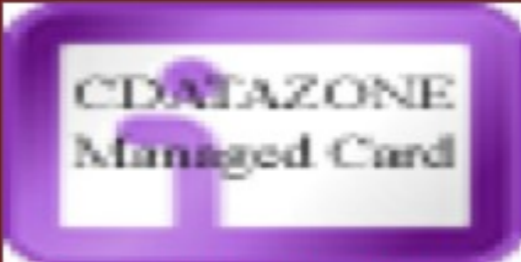
Identity Selector



PHP
Version 1



rrichards (Account)
Version 1



CDatazone Managed Demo Card
Version 1

Self Asserted Card

PHP

<input checked="" type="checkbox"/> First Name:	<input type="text" value="Rob"/>	<input checked="" type="checkbox"/> Email:	<input type="text" value="rrichards@php.net"/>
<input checked="" type="checkbox"/> Last Name:	<input type="text" value="Richards"/>	<input type="checkbox"/> Phone:	<input type="text"/>
<input type="checkbox"/> Street:	<input type="text"/>	<input type="checkbox"/> Mobile Phone:	<input type="text"/>
<input type="checkbox"/> City:	<input type="text"/>	<input type="checkbox"/> Other Phone:	<input type="text"/>
<input type="checkbox"/> State:	<input type="text"/>	<input type="checkbox"/> Date of Birth:	<input type="text"/>
<input type="checkbox"/> Zip:	<input type="text"/>	<input type="checkbox"/> Gender:	<input type="text"/>
<input type="checkbox"/> Country:	<input type="text"/>	Image URL:	<input type="text"/>



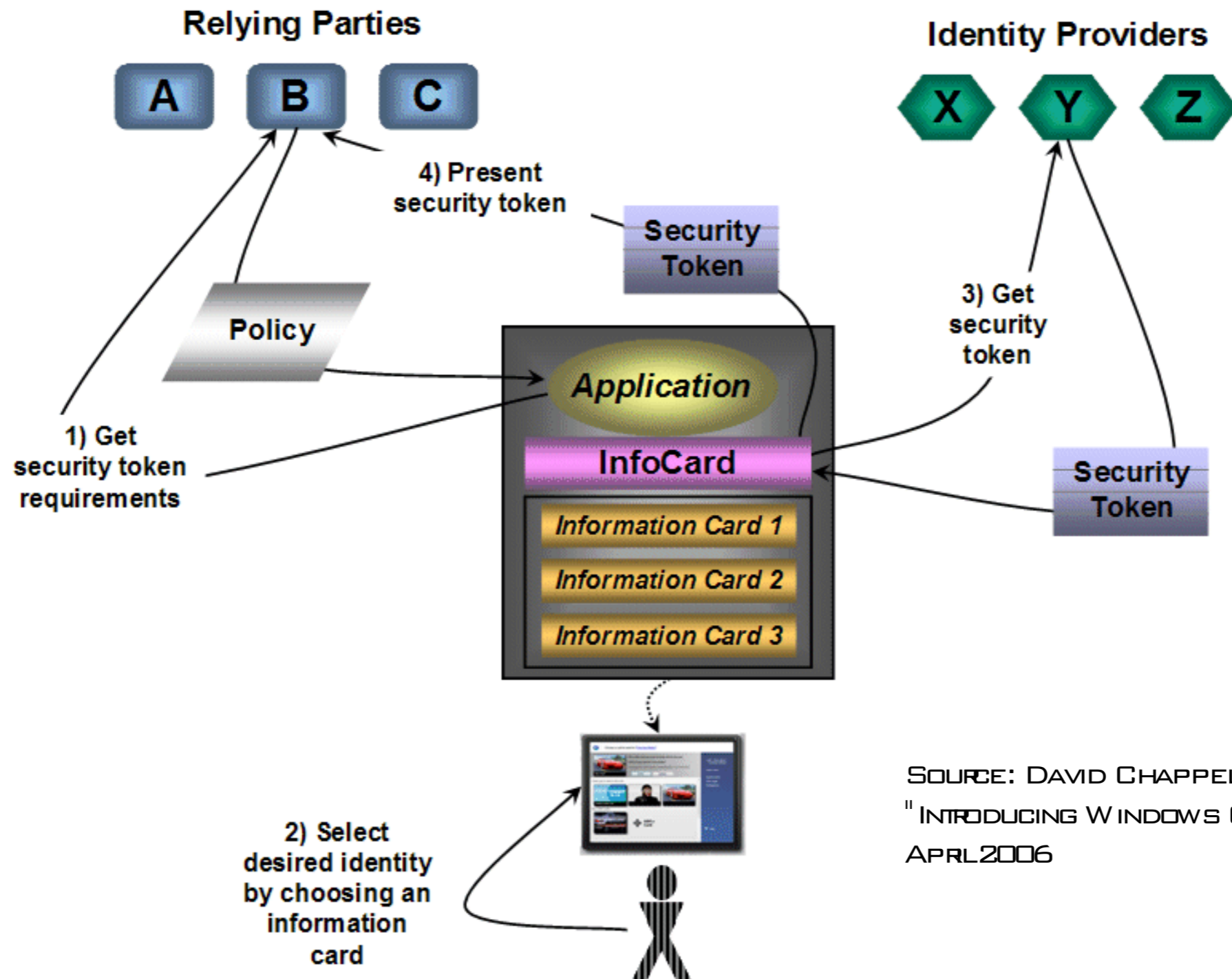
Use this Card

New Card

Delete Card

Cancel

Information Cards Interaction



SOURCE: DAVID CHAPPEL
"INTRODUCING WINDOWS CARDSPACE"
APRIL 2006



Information Card Validation Example

Information Card Login

Serendipity Administration Suite
CDATA Zone

Welcome to the Serendipity Administration Suite.
Please enter your credentials below.

ENTER

Logon using Infocards by clicking on the above image

Logon using your OpenID

OpenID: Login

Username

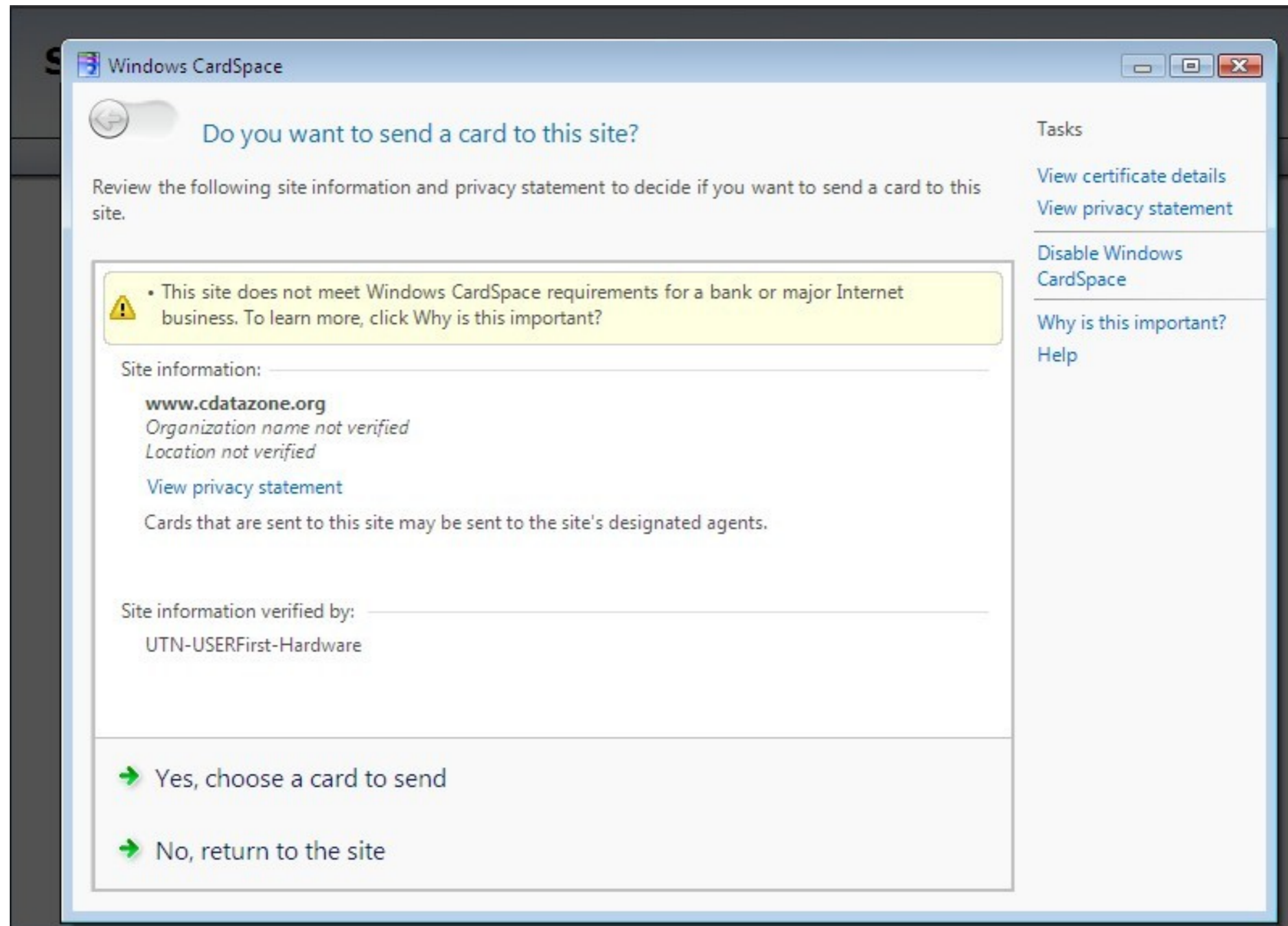
Password

☐ Save information

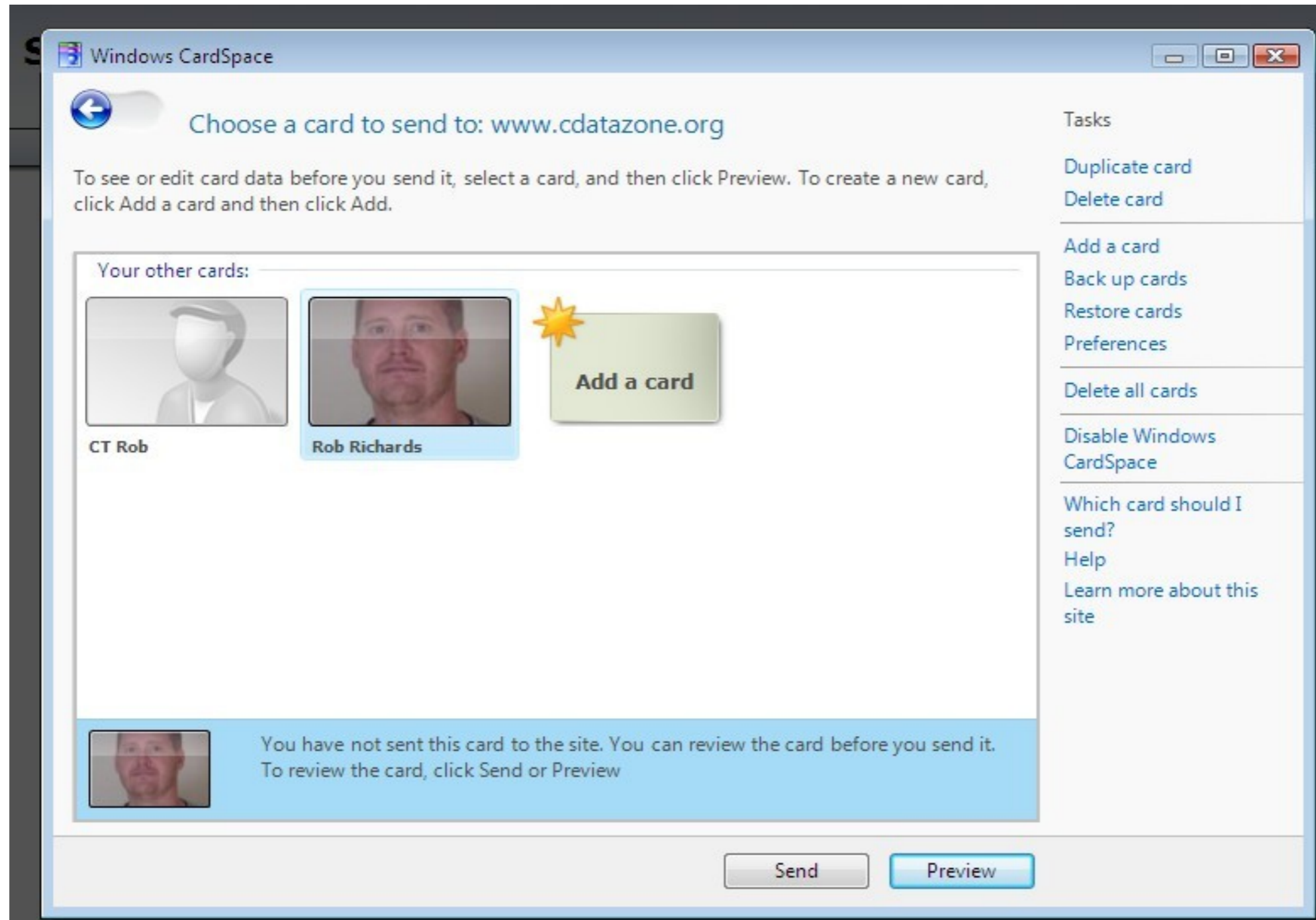
Login >

[Back to Weblog](#)

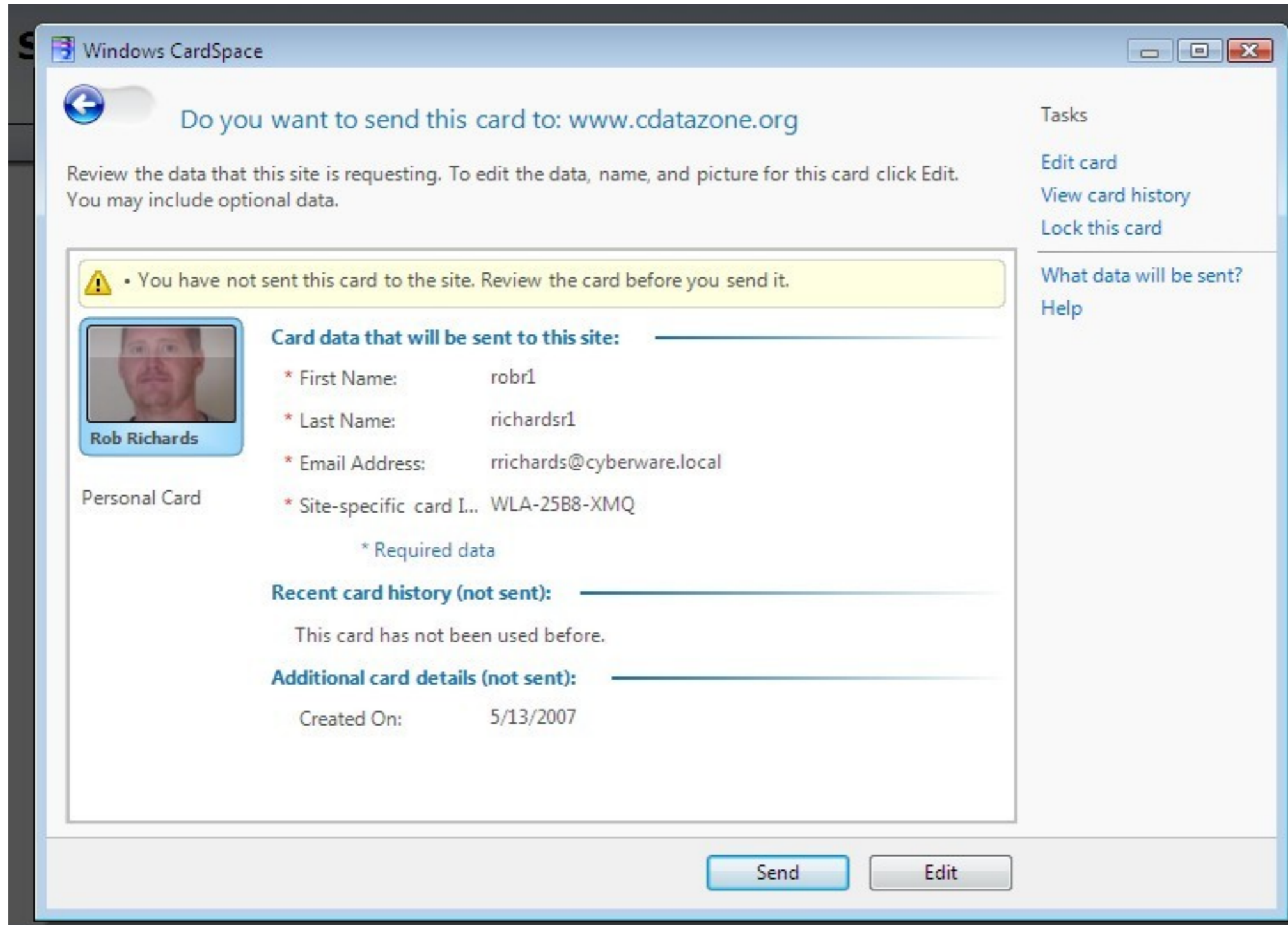
Site Information



Select or Create Card



Preview Information To Be Sent



Information Card Validated

Serendipity Administration Suite

CDATA Zone

Logged in as robr1 richardsr1 (Administrator)

Frontpage

Personal Settings

Entries

New Entry

Edit Entries

Comments

Categories

Static Pages

Media

Add media

Media library

Manage directories

Rebuild Thumbs

Appearance

Manage Styles

Configure Plugins

Administration

Configuration

Manage users

Manage groups

Import data

Export entries

Return to Weblog

Welcome back, robr1 richardsr1

Further Links

[Serendipity Homepage](#)

[Serendipity Documentation](#)

[Official Blog](#)

[Forums](#)

[Spartacus](#)

[Bookmarklet](#)

InfoCard Selector Initiation

```
<form id="infocard" method="post" action="serendipity_admin.php">
  <center>
    
  </center>

  <OBJECT type="application/x-informationCard" name="xmlToken">
    <PARAM Name="tokenType" Value="urn:oasis:names:tc:SAML:1.0:assertion">
    <PARAM Name="requiredClaims"
      Value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" />
    </OBJECT>

</form>
```

Decrypted Self-Asserted Card

```
<saml:Attribute AttributeName="emailaddress"
  AttributeNamespace=". . ./identity/claims">
  <saml:AttributeValue>rrichards@php.net</saml:AttributeValue>
</saml:Attribute>
```

```
<saml:Attribute AttributeName="givenname"
  AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">
  <saml:AttributeValue>Rob</saml:AttributeValue>
</saml:Attribute>
```

```
<saml:Attribute AttributeName="surname"
  AttributeNamespace=". . ./identity/claims">
  <saml:AttributeValue>Richards</saml:AttributeValue>
</saml:Attribute>
```

```
<saml:Attribute AttributeName="privatepersonalidentifier" AttributeNamespace=". .
./identity/claims">
  <saml:AttributeValue>mzhu+UCL. . .</saml:AttributeValue>
</saml:Attribute>
```

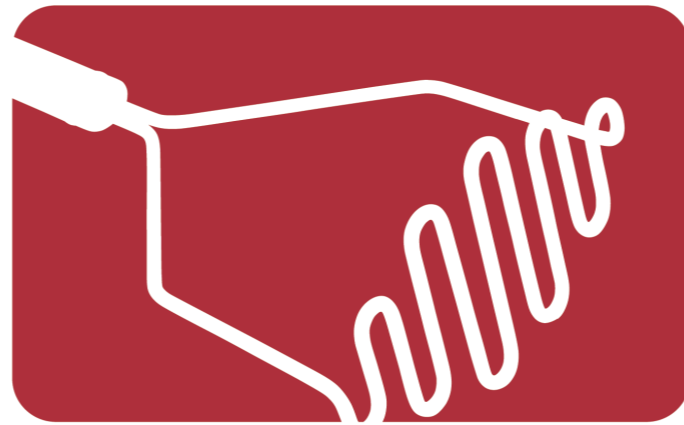
Information Card Issues

- Still in infancy
 - Few number of selectors
 - Differing functionality between selectors
 - Small numbers in production
- CardStore not easily transportable
- Third party applications required for non Windows systems
- Third party applications/plugins required
- More difficult to implement than most Identity technologies

Digital Identity: What Are You Using It For?

- Identity for public or private use?
- Is it a part of a reputation?
- How valuable is the data to be protected?
- What are the individual privacy concerns?
- Consequences if a users identity is compromised?

QUESTIONS?



MASHERY

Digital Identity

Rob Richards

<http://xri.net/=rob.richards>
www.cdatazone.org