



Digital Identity

Rob Richards

September 17, 2008

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

What is a Digital Identity?

- Digital representation of claims about an entity
 - Domain name
 - email address
 - username
 - I-name
- Claims can be made by or about the entity
- No built-in assumption of trust

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/>

What's the Problem?

- Username/Password juggling
- Information is being stored
 - Concerns over privacy issues
 - Security concerns / Identity Theft
- User has no idea who/what is using their information
- Continual re-invention of authentication mechanisms
- Granting access to personal data to another party

*** Sep 17th 2008 ***

http://www.eneews20.com/news_Norwegian_tax_authority_mistakenly_leaks_sensitive_data_11597.html

7 Laws of Identity

- User Control and Consent
- Minimal Disclosure for a Constrained Use
- Justifiable Parties
- Directed Identity
- Pluralism of Operators and Technologies
- Human Integration
- Consistent Experience Across Contexts

Kim Cameron, "Laws of Identity", http://www.identityblog.com/?page_id=354

Identity Context Examples

- Browsing: self-asserted identity for exploring the Web (giving away no real data)
- Personal: self-asserted identity for sites with which I want an ongoing private relationship (including my name and a long-term e-mail address)
- Community: a public identity for collaborating with others
- Professional: a public identity for collaborating issued by my employer
- Credit card: an identity issued by my financial institution
- Citizen: an identity issued by my government

Kim Cameron, "Laws of Identity", http://www.identityblog.com/?page_id=354

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

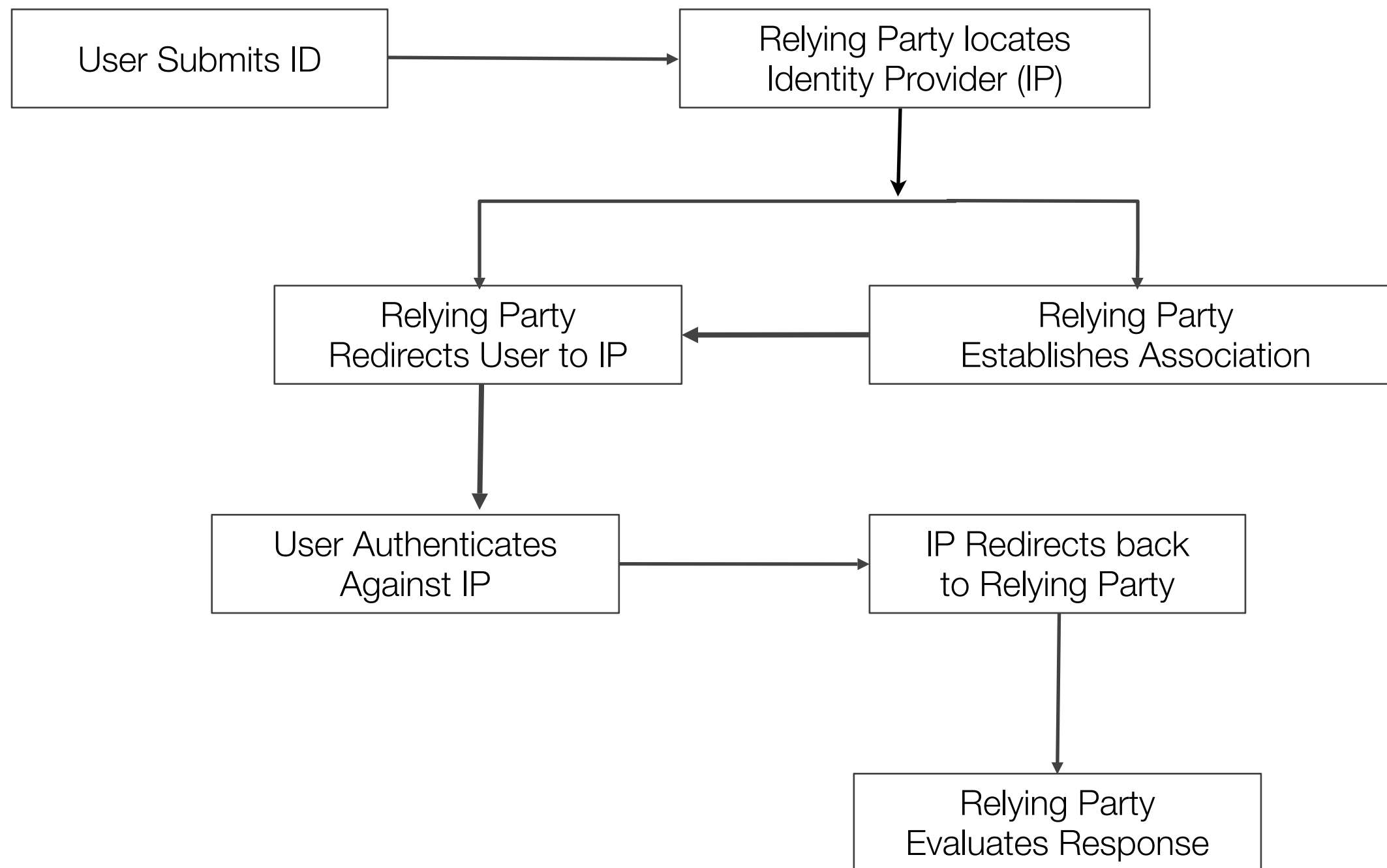
Common Terminology

- 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 Based on OpenID 1.1





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

VeriSign Labs | 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.



Personal
Icon





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><p>Click  to copy the information to the associated field on the left.</p><hr/><p> Full Name: Rob Richards</p><hr/><p> Email Address: rrichards@ctindustries.net</p><hr/><p> Blog: http://www.cdatazone.org</p><hr/></div>	
Trusted Site Expiration	
Expiration	<input type="radio"/> Never Expire
	<input type="radio"/> Expire on: <input type="text" value="Mar"/> <input type="text" value="08"/> <input type="text" value="2008"/>
	<input checked="" type="radio"/> Expire After Signing In
<div>Deny</div> <div>Allow</div>	

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](#)

[Return to Weblog](#)

Welcome back, Rob Richards

Further Links

[Serendipity Homepage](#)

[Serendipity Documentation](#)

[Official Blog](#)

[Forums](#)

[Spartacus](#)

[Bookmarklet](#)

OpenID 2.0

- Extension Support
 - namespaced extensions
- Attribute Exchange Extension
 - Extensible attribute support
 - Identity Provider can be asked to store certain attributes
- HTTP POST Support
 - No longer limited to URL length
 - Larger Requests and Responses
- 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

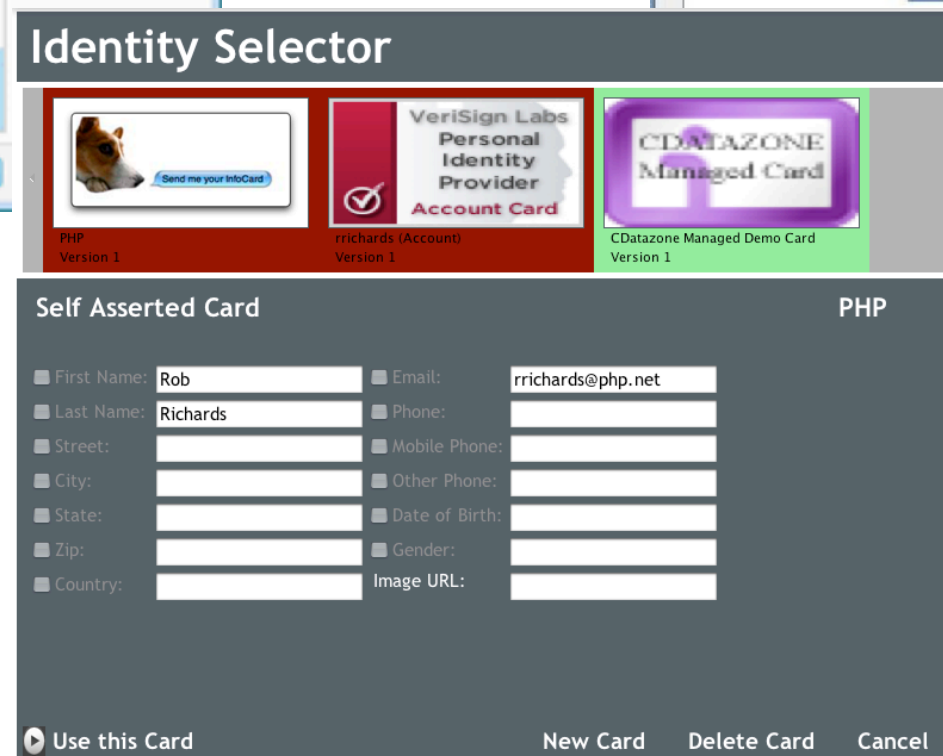
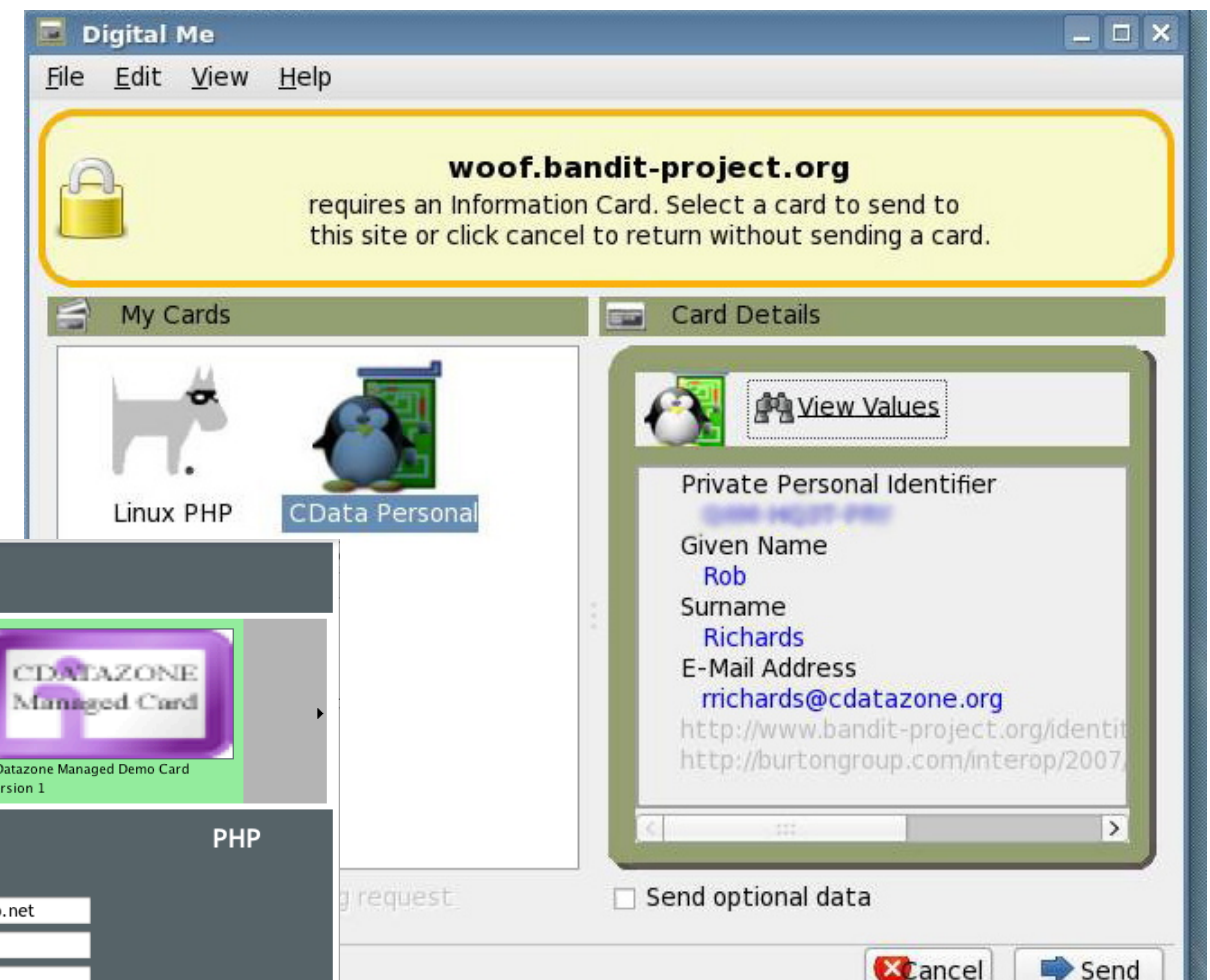
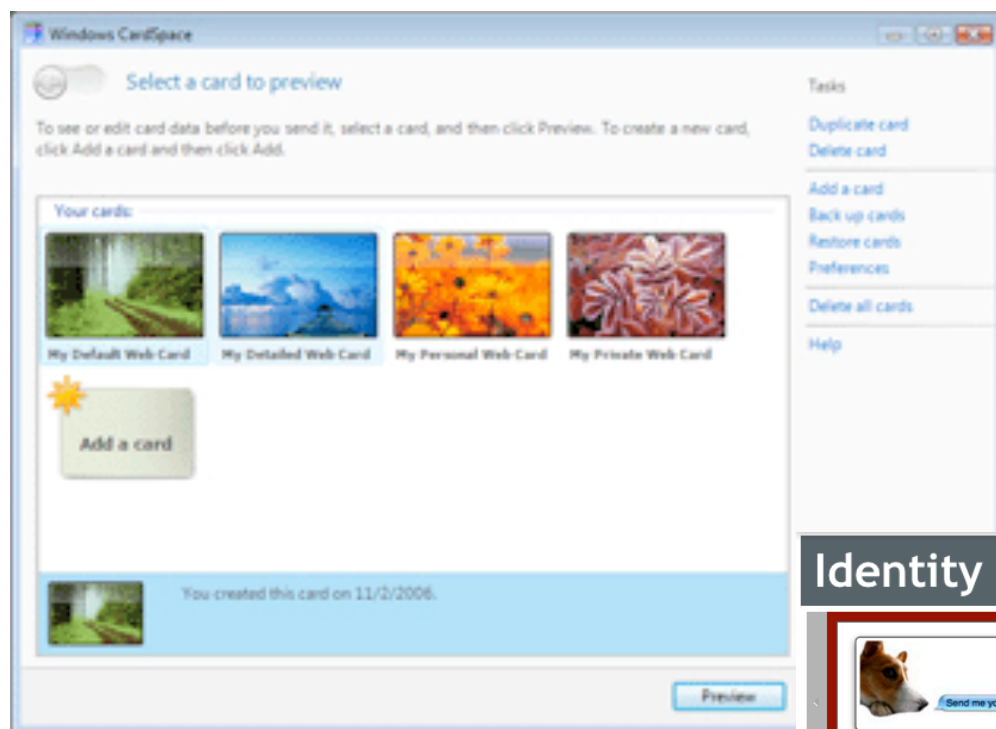
- Self Asserted
- Managed (Third Party provided)



Information Cards: Selectors

CardSpace != Information Cards

Information Cards are not Microsoft specific

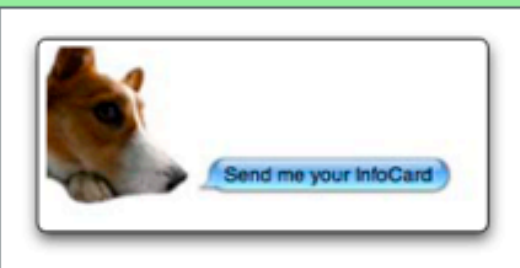


Information Cards

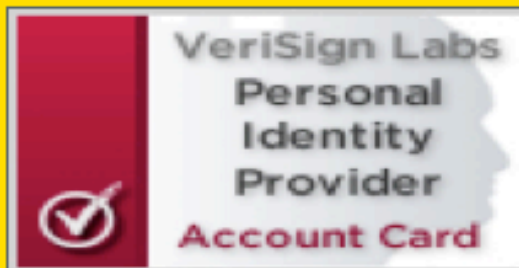
- Identifier is unique amongst parties
 - Distinct digital key for each realm
- Protections against Phishing
 - Visual indicators of previous interactions
 - x509 certificate checking
- Complex Technologies
 - SAML
 - WS-Security / WS-Policy / WS-Trust
 - x509

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"/>

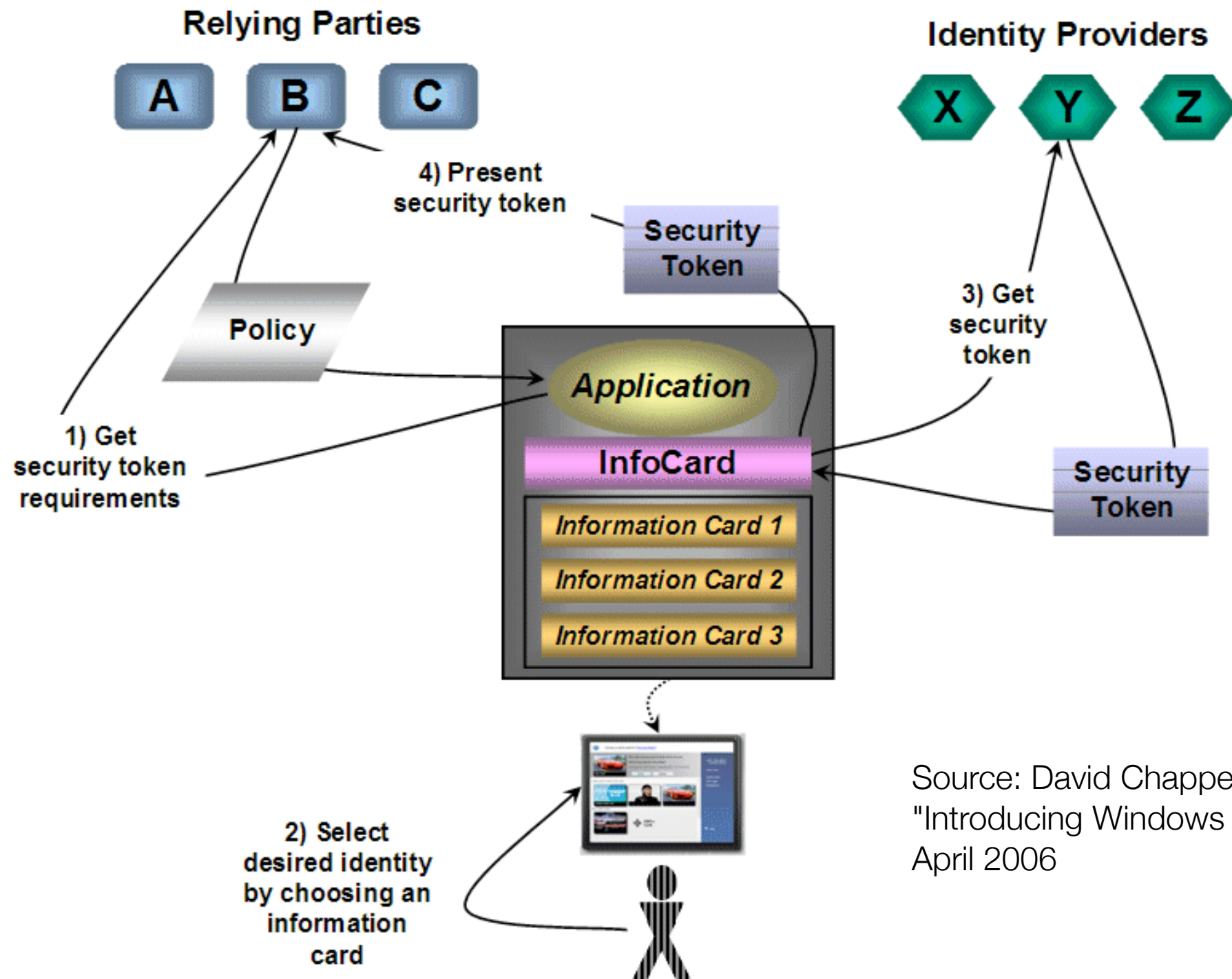
 Use this Card

New Card

Delete Card

Cancel

Information Cards Interaction



Source: David Chappell
"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:

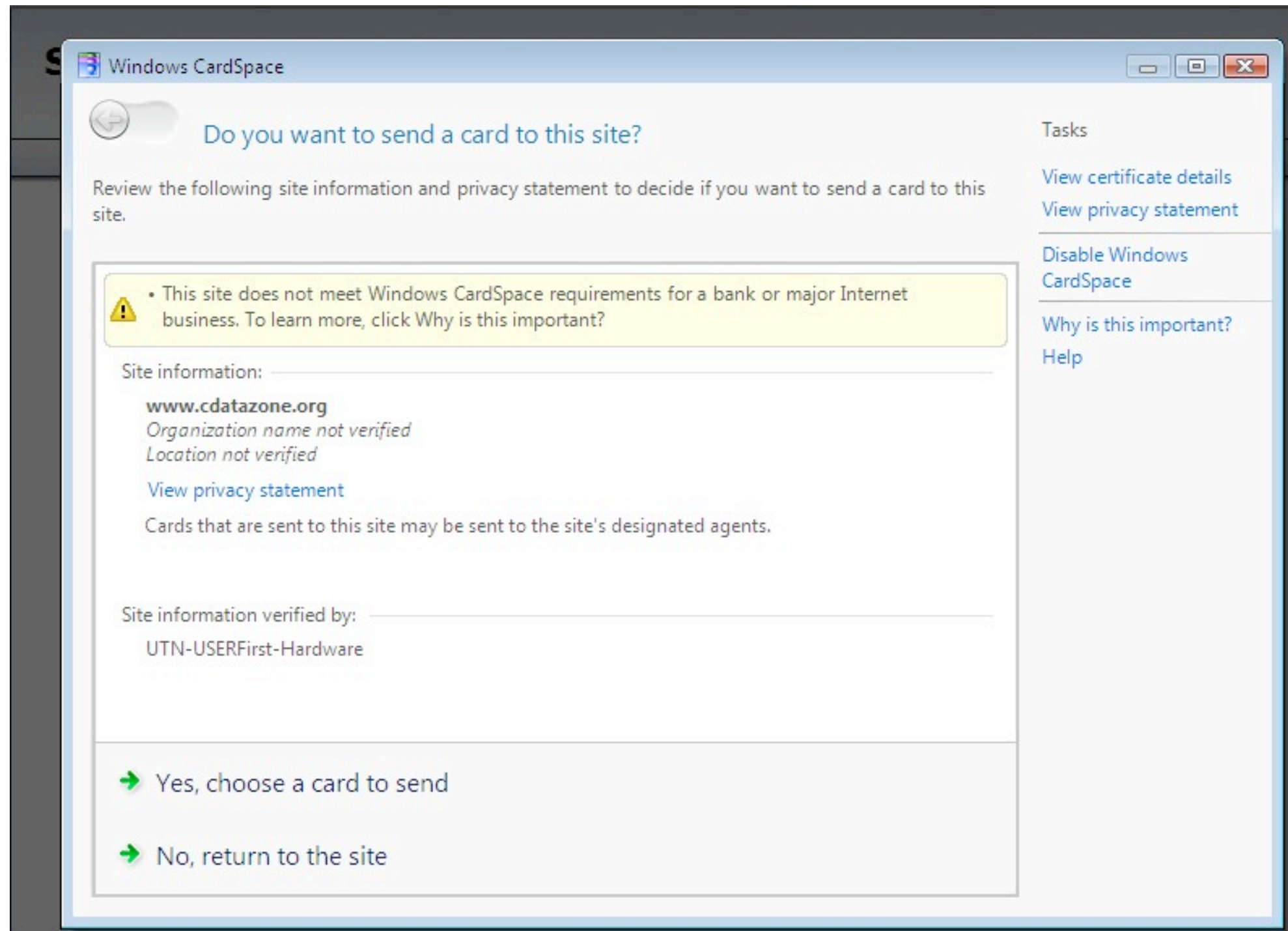
Username

Password

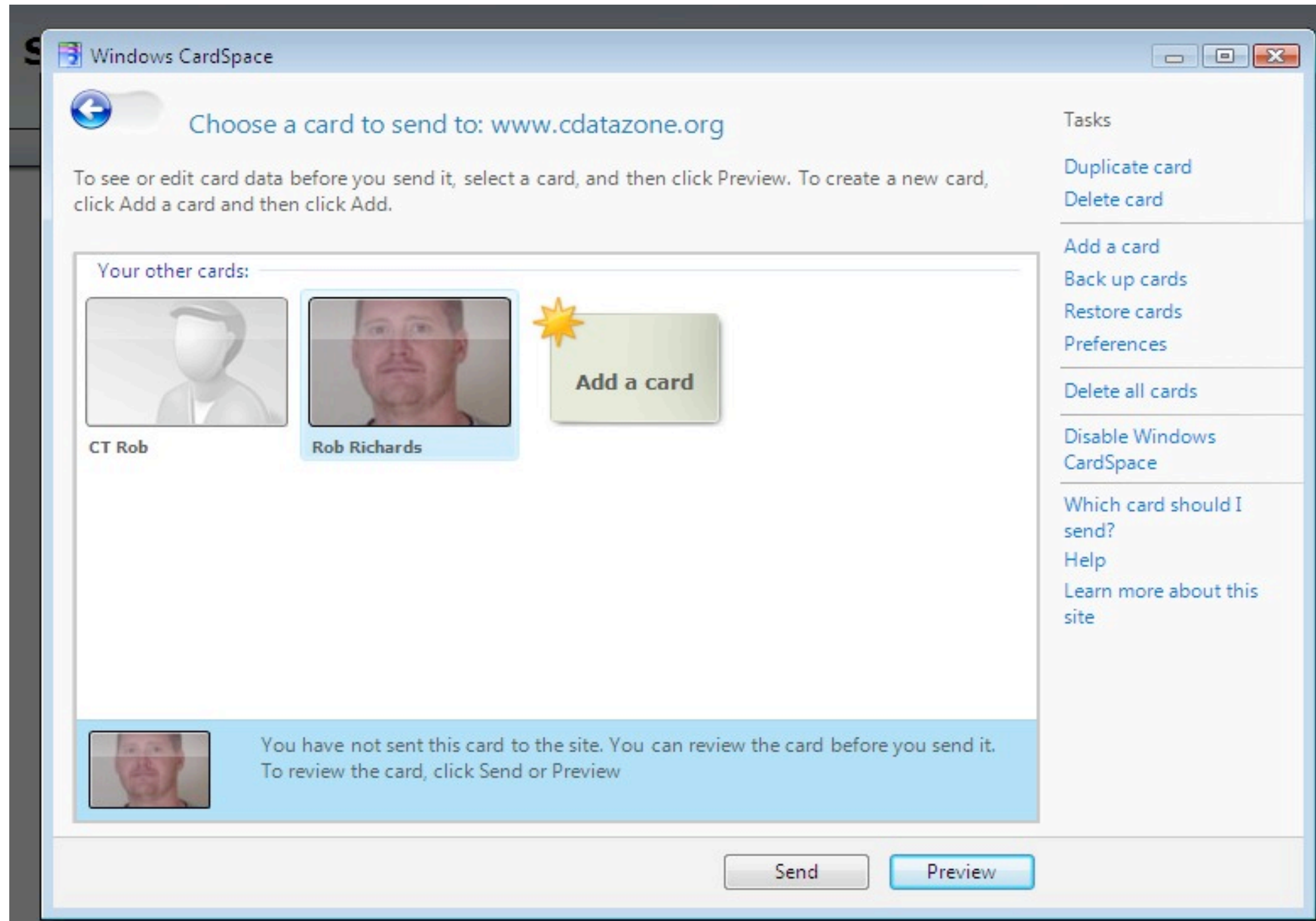
☐ Save information

[Back to Weblog](#)

Site Information



Select or Create Card



Preview Information To Be Sent

Windows CardSpace

Do you want to send this card to: www.cdatazone.org

Review the data that this site is requesting. To edit the data, name, and picture for this card click Edit. You may include optional data.

Tasks

- [Edit card](#)
- [View card history](#)
- [Lock this card](#)
- [What data will be sent?](#)
- [Help](#)

Card data that will be sent to this site:

- * First Name: robr1
- * Last Name: richardsr1
- * Email Address: rrichards@cyberware.local
- * Site-specific card I... WLA-25B8-XMQ

* Required data

Recent card history (not sent):

This card has not been used before.

Additional card details (not sent):

Created On: 5/13/2007

Personal Card

Rob Richards

[Send](#) [Edit](#)

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

Welcome back, robr1 richardsr1

Further Links

[Serendipity Homepage](#)

[Serendipity Documentation](#)

[Official Blog](#)

[Forums](#)

[Spartacus](#)

[Bookmarklet](#)

[Return to Weblog](#)

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" />
    </PARAM>
  </OBJECT>

</form>
```


InfoCard: PHP Code

<http://www.cdatazone.org/index.php?/pages/source.html>

- My own code
 - xmlseclibs.php
 - XMLDSig / XMLENC
 - infocard-lib.php
 - Decrypts submitted XML Token
 - Verifies Signed SAML Token
 - Parses Assertions
- Zend_Infocard
 - <http://framework.zend.com/manual/en/zend.infocard.html>
 - Included with 1.5 release

Submitted Token

```
<enc:EncryptedData xmlns:enc="...xmlenc#" Type="...xmlenc#Element">
  <enc:EncryptionMethod Algorithm="...xmlenc#aes256-cbc" />
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <enc:EncryptedKey>
      <enc:EncryptionMethod Algorithm="...xmlenc#rsa-oaep-mgf1p">
        <ds:DigestMethod Algorithm="...xmldsig#sha1" />
      </enc:EncryptionMethod>
      <ds:KeyInfo>
        <wsse:SecurityTokenReference xmlns:wsse="...ssecurity-secext-1.0.xsd">
          <wsse:KeyIdentifier ValueType="...#ThumbprintSHA1"
            EncodingType="...#Base64Binary">7SSj...</wsse:KeyIdentifier>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
      <enc:CipherData>...</enc:CipherData>
    </enc:EncryptedKey>
  </ds:KeyInfo>
  <enc:CipherData>...</enc:CipherData>
</enc:EncryptedData>
```

Decrypted Self-Asserted Card

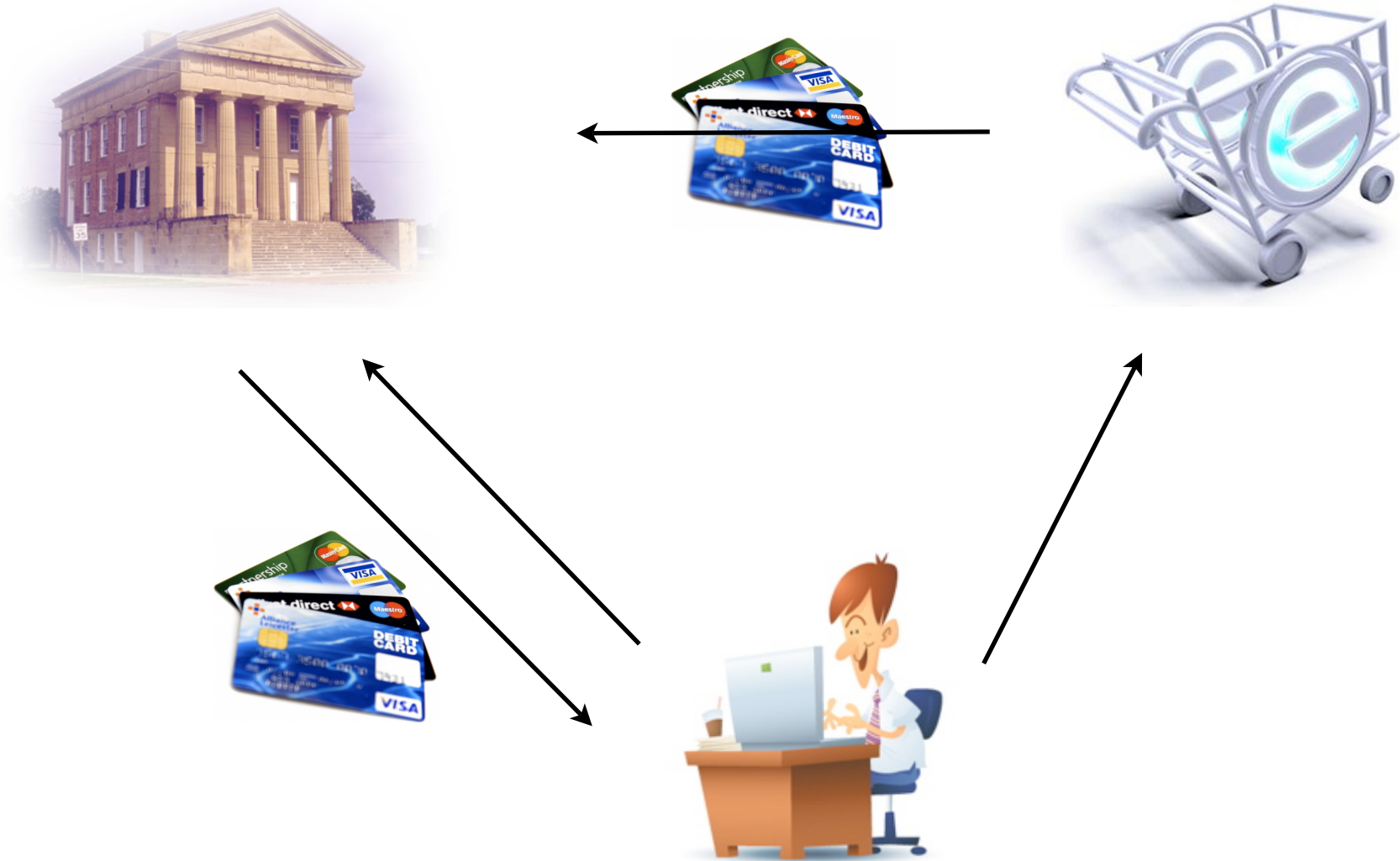
```
<saml:Attribute AttributeName="emailaddress"
  AttributeNamespace=". . ./identity/claims">
  <saml:AttributeValue>rrichards@php.net</saml:AttributeValue>
</saml:Attribute>
```

```
<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 Cards: Into The Future



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?




OAuth

API Authorization Delegation

OAuth: The Problem


Build your network (Why?)


Find contacts who are already on LinkedIn




Web email contacts


Check your address book to find contacts who are on LinkedIn.

☒  Windows Live

☐  Gmail

☐ Other

☐  YAHOO!

☐  AOL

Username: @hotmail.com

Password:

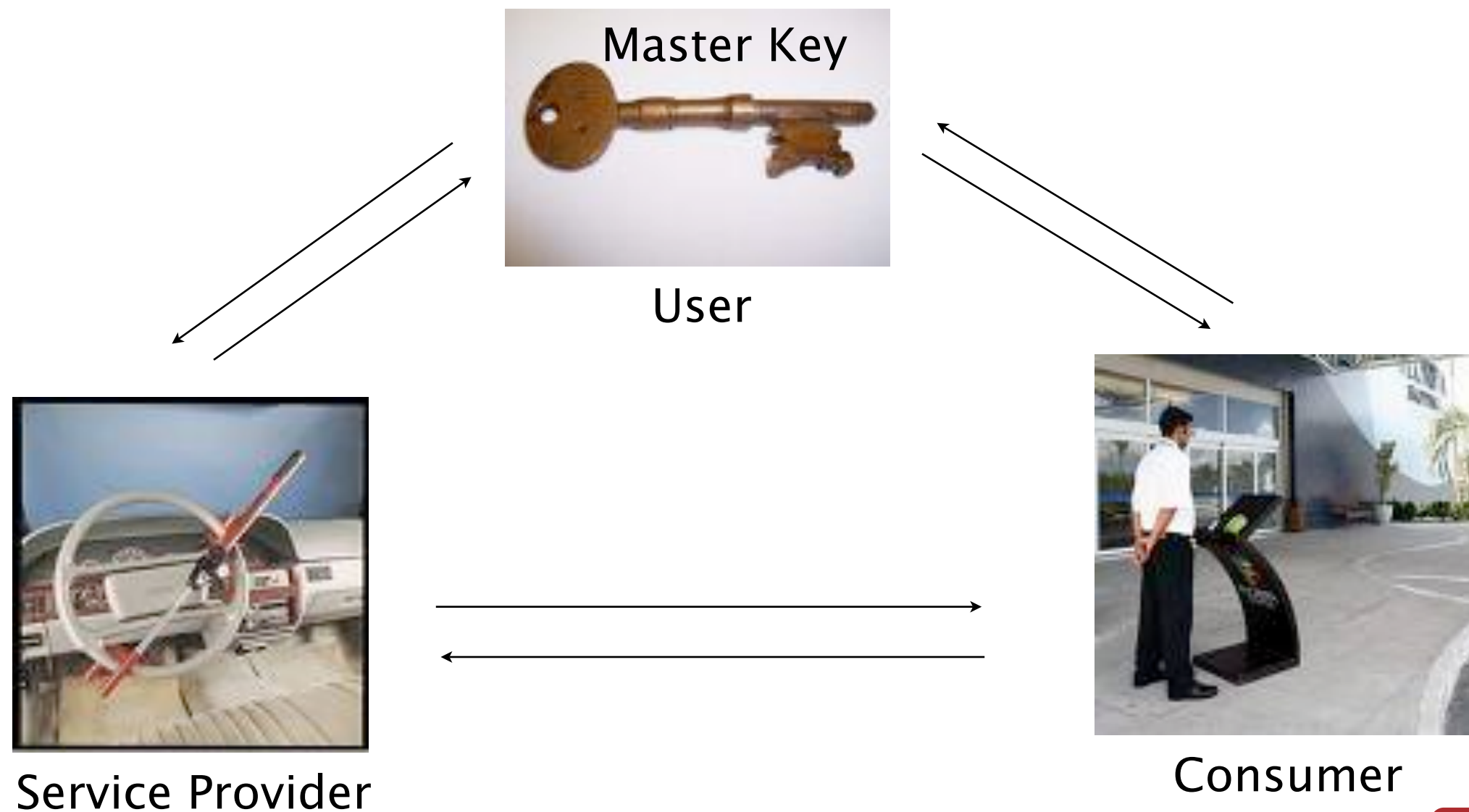
OAuth: The Problem

Stop Asking For My User Credentials!



OAuth: What Is It?

Allows a User to grant access to private resources to another entity without giving away the keys to the Kingdom



OAuth

- OAuth Is Not OpenID
 - Shares common technologies
 - Workflow Appears similar
- Consumer needs to be known to Service Provider
- Token Based
 - Tokens identify the consumer
 - Tokens identify the combination of user and consumer
 - Tokens can be given a lifespan
 - Tokens can be revoked

OAuth Security

- Requests are signed
 - Plaintext
 - HMAC-SHA1
 - RSA-SHA1
- Tokens are passed
 - No sharing of username/password
 - Tokens can be revoked
- Requests pass timestamps
 - Provides validity timeframe
 - Can help prevent replay attacks
- Nonce can be used
 - prevent replay attacks

OAuth: Access Protected Resource




<http://api.getsatisfaction.com/me>

AccessDeniedError


OAuth: Consumer Registration

- Consumer provides information to Service Provider
 - Name
 - URL
 - Description
- Consumer receives unique identifier (Consumer Key)
- Information for Signature is shared
 - Shared secret (Consumer Secret)
 - Consumer Public Key for use in RSA-SHA1 verification
- Request and Access token endpoints made known

OAuth: Consumer Registration

[Home](#) [Companies](#) [Products](#) [You](#) 

Hi Rob (Account) | [Sign out](#)

Find a: Company 

GET SATISFACTION

[Rob's dashboard](#) / [Account Settings](#) / [Extensions](#) / [Application Registrations](#)

[Profile](#) [Products & Companies](#) [Contacts](#) [Account settings](#)

[Account Details](#)
[Login Options](#)
[Employee Of](#)
[Email & Notifications](#)
[API Services](#)

Application Name

Application Description

Callback URL

☐ I Agree to the [terms of service](#)

Help topics for Your Account
[Can I change my profile and account information?](#)
[How do I manage my notifications?](#)
[Can I close my account?](#)
[As an employee, can I change my official title?](#)

OAuth: Consumer Registration

Your registered applications ([new application](#))

Application Name	Status	Consumer Key	Consumer Secret	Issued
Test App	Active	qw01s33n229	lw0v1p9m9v70nqgkud0v32uo7s5at	5 months ago Edit

- *To get a request token:* `http://getsatisfaction.com/api/request_token`
- *Redirect users to:* `http://getsatisfaction.com/api/authorize?oauth_token=XXX` to authorize a request token
- *To exchange an authorized request token to get an access token:*
`http://getsatisfaction.com/api/access_token`

OAuth: Get Request Token

`http://getsatisfaction.com/api/request_token?`

`oauth_consumer_key=qw0xx50kxx29`

`&oauth_nonce=15865e53dbe0c4d4f13d9c2296c49fd8ba7384`

`&oauth_signature=kwwh%2BMO21uExLTAn25jFwLhZfys%3D`

`&oauth_signature_method=HMAC-SHA1`

`&oauth_timestamp=1221478575`

`&oauth_version=1.0`

OAuth: Get Request Token (SP Response)

oauth_token=2147xxxxvz0i

&oauth_token_secret=xuxxtmxxxxxxxxx60bbn8worxxxxxxxxxcr1

OAuth: User Authorization

`http://getsatisfaction.com/api/authorize?`

`oauth_token=pspiu7gw5faq`

`&oauth_callback=http%3A%2F%2Fcdatazone.org
%2Fexample%2Ftest.php`

OAuth: User Authorization

We need your approval!

Hello Rob,

Test App would like you to grant them the ability to use your Get Satisfaction account on their website. Giving this authorization will allow you to post Get Satisfaction topics and replies on **Test App's** site, as well as change your Get Satisfaction profile settings via them.

Agreeing to this means allowing **Test App** to access your private Get Satisfaction data for the purposes of posting to their site, **so only allow access to sites you know and trust!**

Yes, allow it

Or, Cancel and go to my dashboard

OAuth: User Authorization (SP Redirect)

`http://www.cdatazone.org/example/test.php?`

`oauth_token=pspiu7gw5faq`

OAuth: Get Access Token

`http://getsatisfaction.com/api/access_token?
oauth_consumer_key=qw0xx50kxx29
&oauth_nonce=be2ca738ccd024a9524d4eb090c1375b9953
&oauth_signature=2jSjj%2BjqIrxEbvbrxy0HboHrhr0%3D
&oauth_signature_method=HMAC-SHA1
&oauth_timestamp=1221480066
&oauth_token=pspiu7gw5faq
&oauth_version=1.0`

OAuth: Get Access Token (SP Response)

oauth_token=s8xxxjxixxu

&oauth_token_secret=powhxxxxxxxxw9m457xxxxxxxxjom2o

OAuth: Access Protected Resource

<http://api.getsatisfaction.com/me?>

oauth_consumer_key=qw0xx50kxx29

&oauth_nonce=33cc986c57ee57689665ef331058cacacda6ab

&oauth_signature=cWVX7QHx9Fedl29fGiw99msSPfA%3D

&oauth_signature_method=HMAC-SHA1

&oauth_timestamp=1221480525

&oauth_token=s8xxxjxixxu

&oauth_version=1.0

OAuth: Access Protected Resource

Rob



rob_28386

Questions?



Digital Identity

Rob Richards

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