MASHERY

Who am I?
The Age of the Digital Identity

Rob Richards

March 14, 2008

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

“I am whatever you say I am
If I wasn't then why would I say I am”

Eminem, "The Way I Am", The Marshall Mathers LP, 2000

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

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

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

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

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

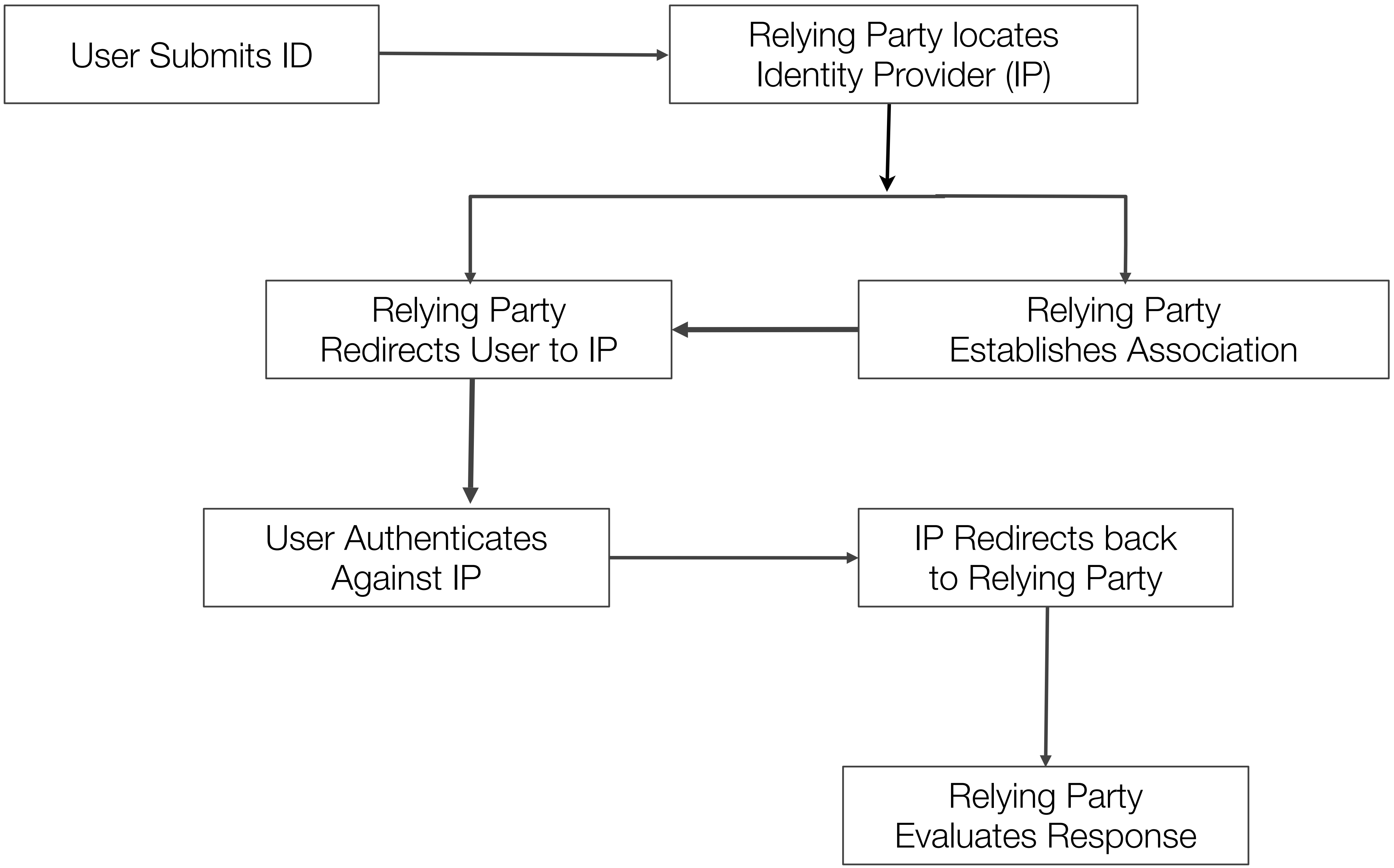
Common Terminology

- 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/)
  - OmniTI OpenID (https://labs.omniti.com/trac/alexandria/wiki)
  - Zend (http://framework.zend.com/manual/en/zend.openid.html)
  - OpenID for PHP (http://www.openidforphp.org/)

OpenID Interaction
Based on OpenID 1.1



User Submits ID

Relying Party locates Identity Provider (IP)

Relying Party Redirects User to IP

Relying Party Establishes Association

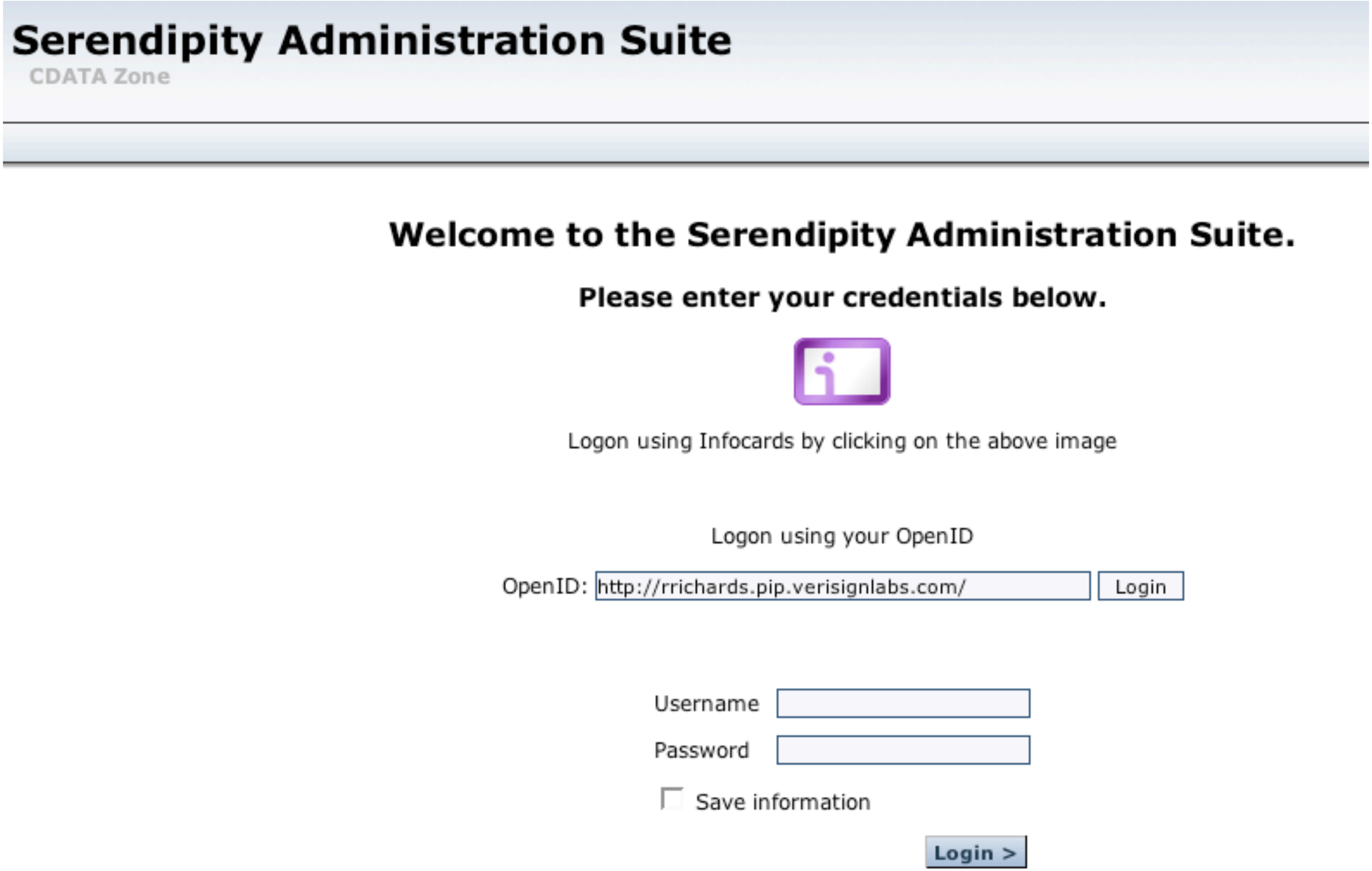
User Authenticates Against IP

IP Redirects back to Relying Party

Relying Party Evaluates Response

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

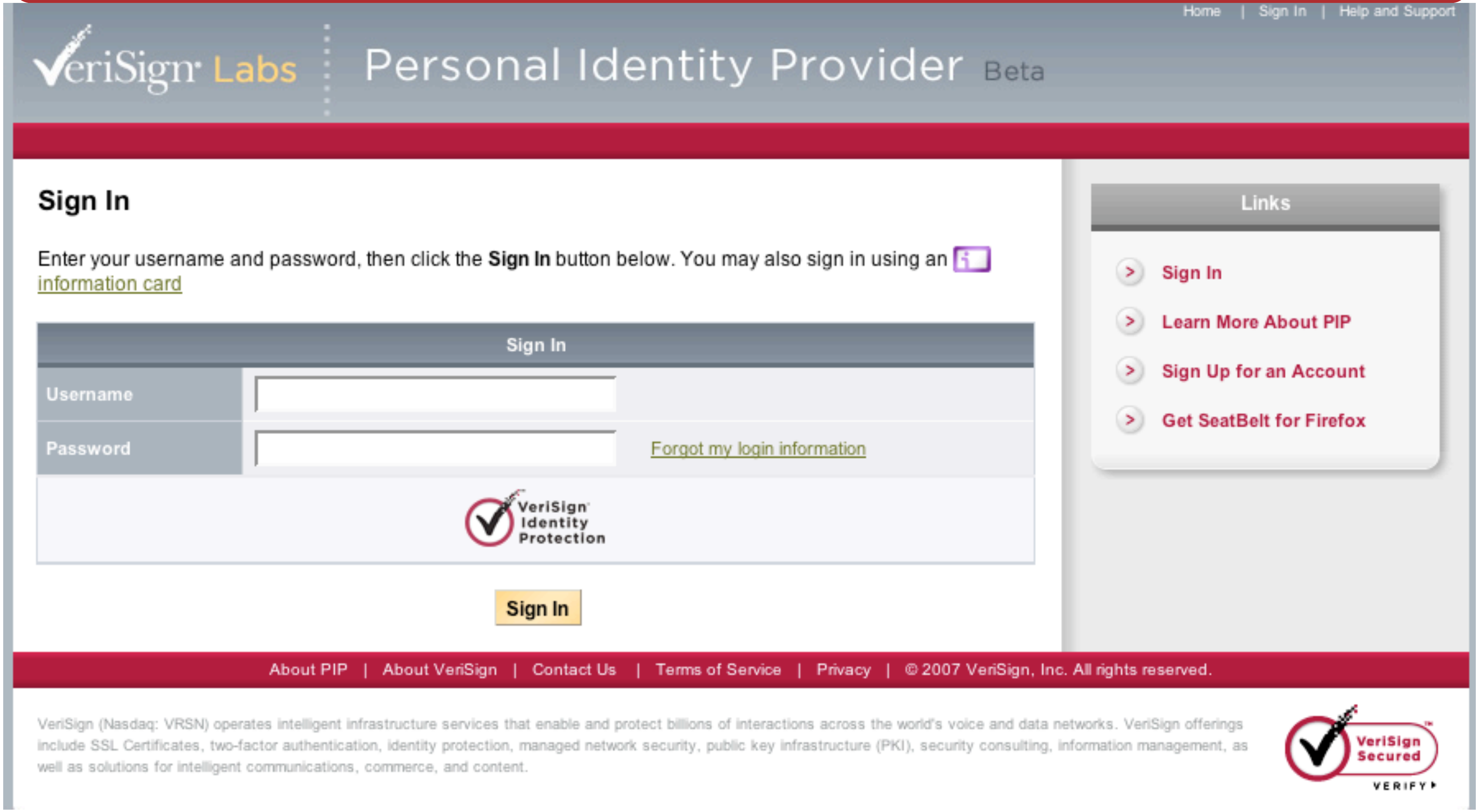
OpenID: http://rrichards.pip.verisignlabs.com/

Username

Password

□ Save information

OpenID Verification



Home | Sign In | Help and Support
VeriSign Labs
Personal Identity Provider Beta

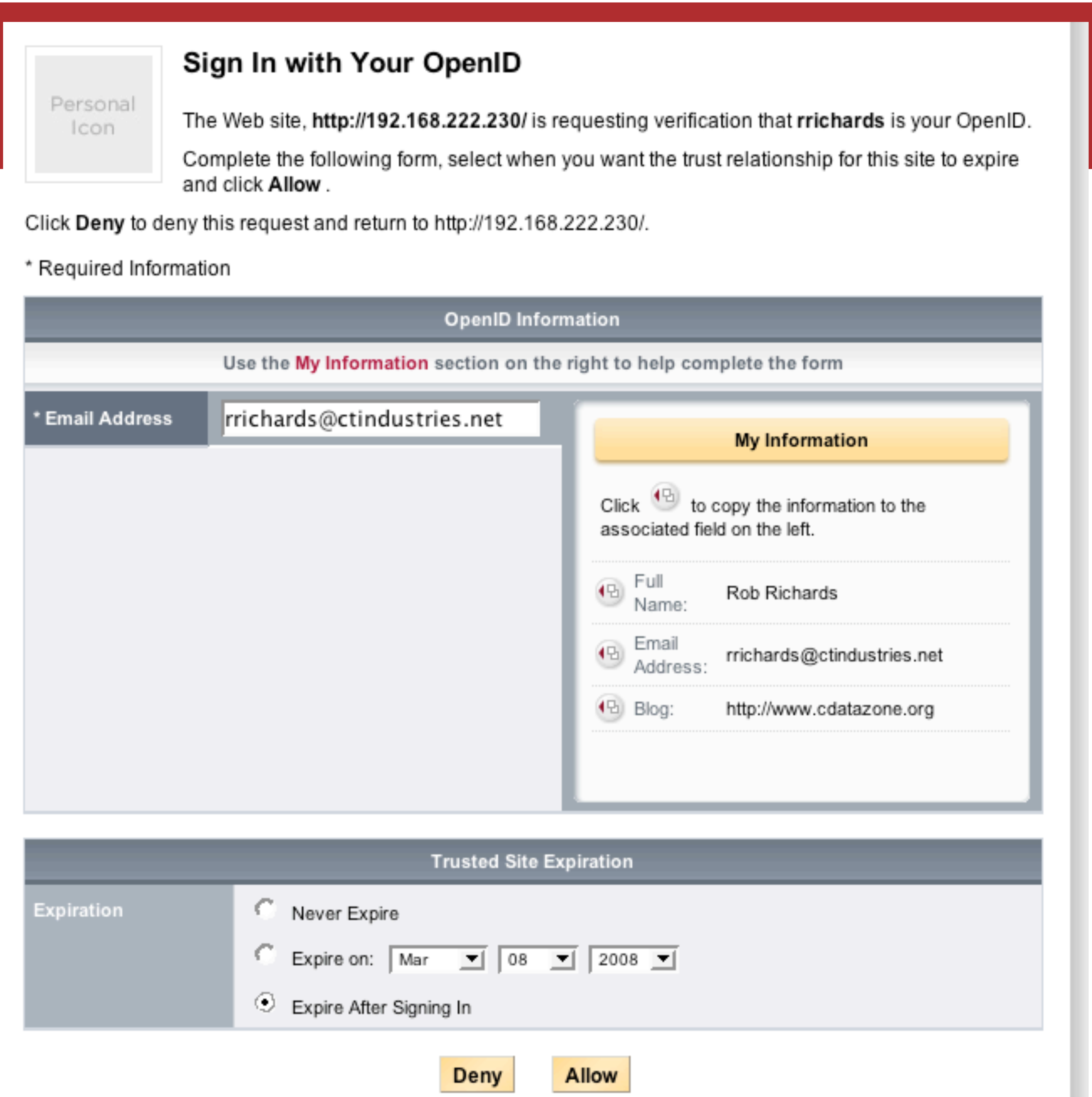
Sign In

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

Sign In	
Username	
Password	Forgot my login information

VeriSign Identity Protection
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	rrichards@ctindustries.net

My Information

Click to copy the information to the associated field on the left.

Full Name:	Rob Richards
Email Address:	rrichards@ctindustries.net
Blog:	http://www.cdatazone.org

Trusted Site Expiration

Expiration

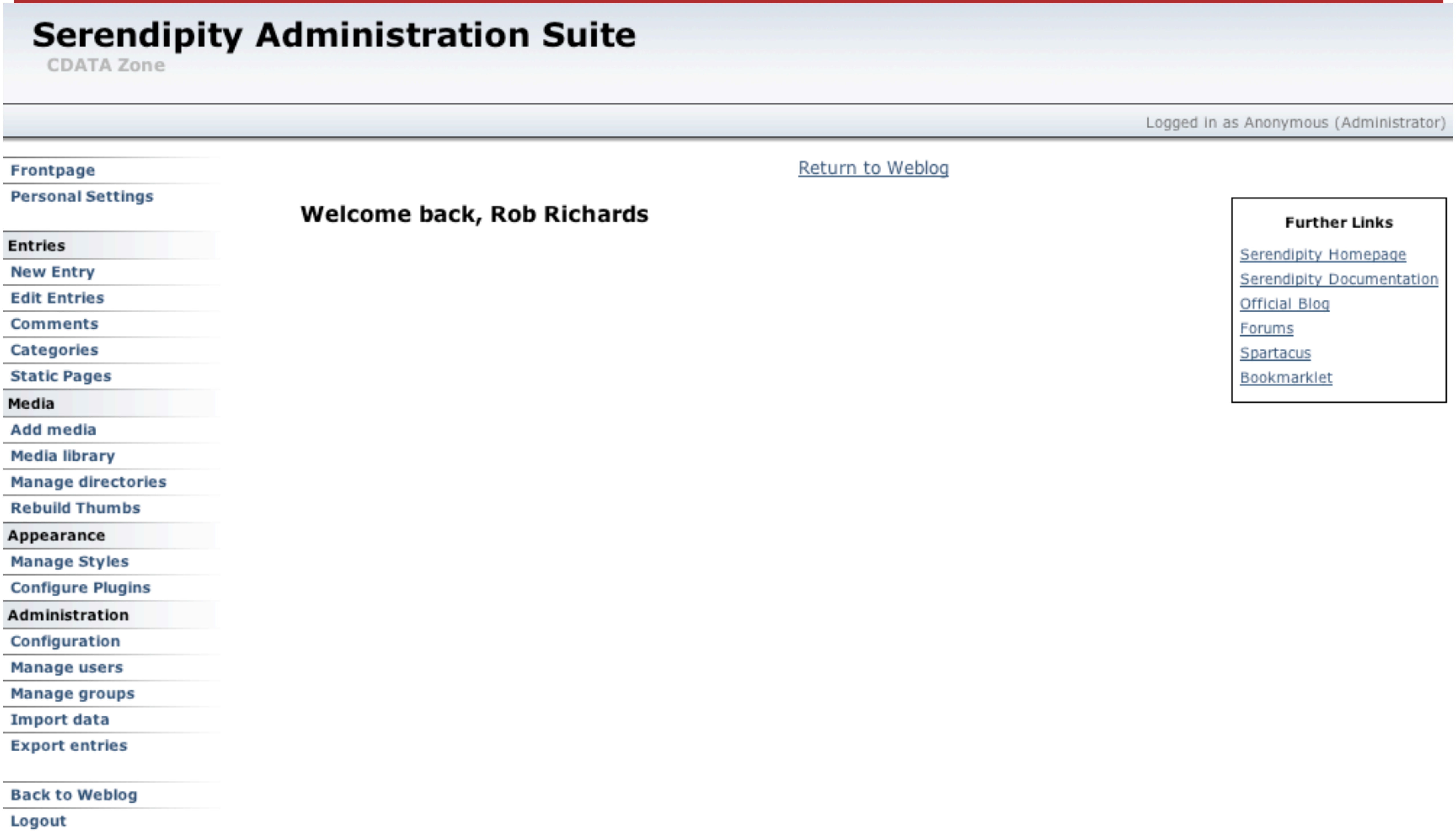
○ Never Expire

○ Expire on: Mar 08 2008

● Expire After Signing In

MASHERY

OpenID validated



Serendipity Administration Suite

CDATA Zone

Logged in as Anonymous (Administrator)

Welcome back, Rob Richards

OpenID Authentication Request

```
require_once("Auth/OpenID/Consumer.php");
require_once("Auth/OpenID/FileStore.php");
$store = new Auth_OpenID_FileStore($store_path);
$consumer = new Auth_OpenID_Consumer($store);

$trust_root = $serendipity['baseURL'];
$process_url = $trust_root . 'serendipity_admin.php';

$auth_req = $consumer->begin($openid_url);
if (!$auth_req)
    return FALSE;

$auth_req->addExtensionArg('sreg', 'required', 'email');

$redirect_url = $auth_req->redirectURL($trust_root, $process_url);

header("Location: ".$redirect_url);
```

OpenID Authentication Response

```
require_once("Auth/OpenID/Consumer.php");
require_once("Auth/OpenID/FileStore.php");
$store = new Auth_OpenID_FileStore($store_path);
$consumer = new Auth_OpenID_Consumer($store);

$response = $consumer->complete($_GET);

if ($response->status == Auth_OpenID_CANCEL) {
   $msg = 'Verification cancelled.';

} else if ($response->status == Auth_OpenID_FAILURE) {
   $msg = "OpenID authentication failed: ".$response->message;

} else if ($response->status == Auth_OpenID_SUCCESS) {
   $openid = $response->identity_url;
   $sreg = $response->extensionResponse('sreg');
}
```

OpenID URL Request

https://pip.verisignlabs.com/server?

openid.assoc_handle={HMAC-SHA1}{469e6747}{Tg0zvA==}

openid.identity=http://rrichards.pip.verisignlabs.com/

openid.mode=checkid_setup

openid.return_to=https://192.168.222.230/serendipity_admin.php?<s9y args>

nonce=mv9ycuTg

openid.sreg.required=email

openid.trust_root=https://192.168.222.230/

OpenID URL Response

https://192.168.222.230/serendipity_admin.php?<s9y args>

nonce=mv9ycuTg&openid.sig=7njhs5bWRbNtIoj1wO8hM3MiIXM=

openid.mode=id_res

openid.return_to=https://192.168.222.230/serendipity_admin.php?<s9y args>

nonce=mv9ycuTg

openid.sreg.email=rrichards@php.net

openid.identity=http://rrichards.pip.verisignlabs.com/

openid.signed=identity,return_to,mode

openid.assoc_handle={HMAC-SHA1}{469e6747}{Tg0zvA==}

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 identity 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

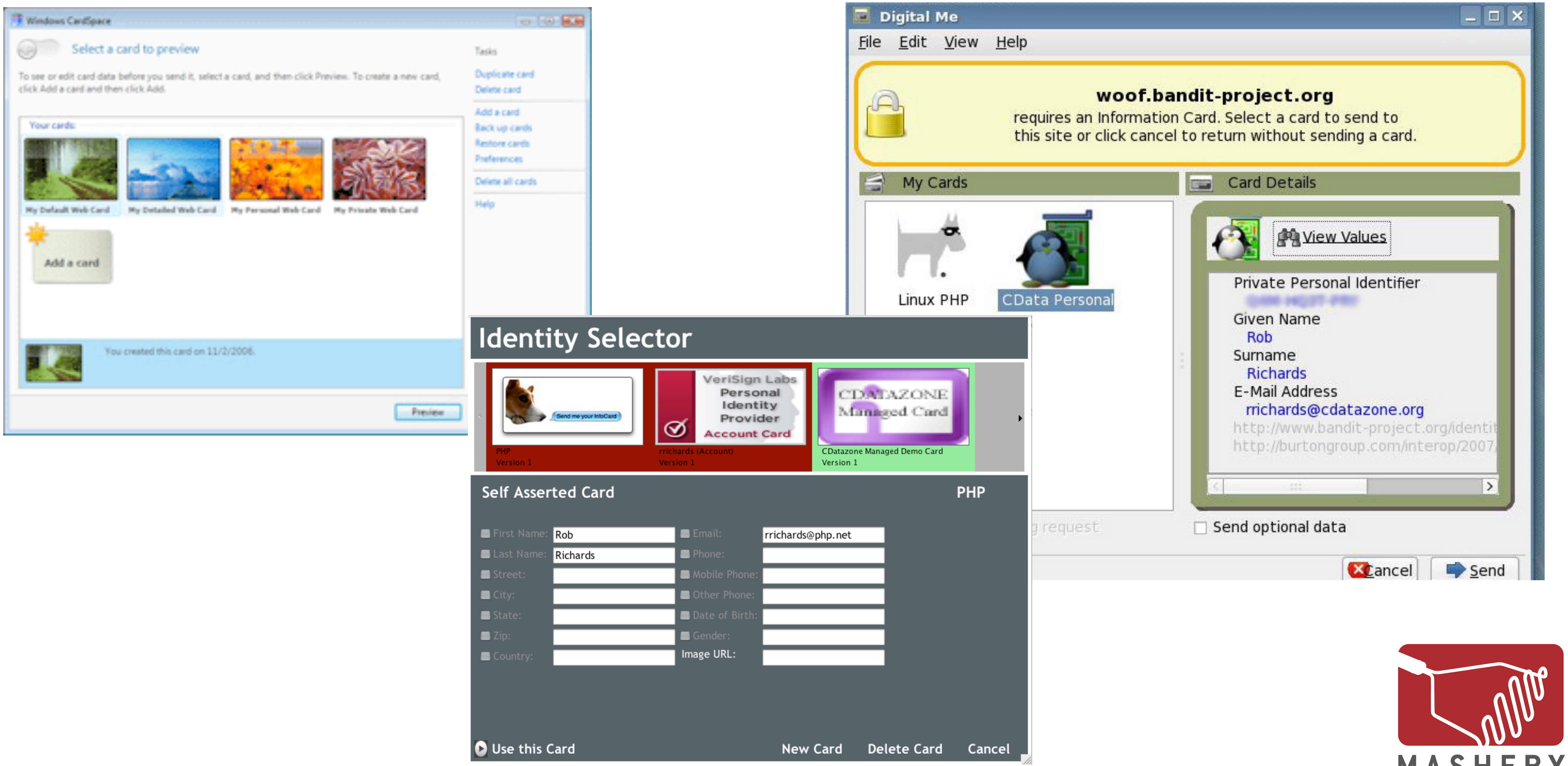
Identities represented as cards in a wallet

- Self Asserted
- Managed (Third Party provided)

Information Cards: Selectors

CardSpace != Information Cards

Information Cards are not Microsoft specific



Windows CardSpace

Select a card to preview

To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

Your cards:

My Default Web Card
My Detailed Web Card
My Personal Web Card
My Private Web Card

Add a card

You created this card on 11/2/2006.

Preview

Tasks
- Duplicate card
- Delete card
- Add a card
- Back up cards
- Restore cards
- Preferences
- Delete all cards
- Help

Digital Me

File Edit View Help

woof.bandit-project.org
requires an Information Card. Select a card to send to this site or click cancel to return without sending a card.

My Cards

Linux PHP
CData Personal

Card Details

View Values

Private Personal Identifier
[redacted]
Given Name
Rob
Surname
Richards
E-Mail Address
rrichards@cdatazone.org
http://www.bandit-project.org/identit
http://burtongroup.com/interop/2007/

...g request

□ Send optional data

Cancel Send

Identity Selector

Send me your InfoCard
PHP
Version 1

VeriSign Labs Personal Identity Provider Account Card
rrichards (Account)
Version 1

CDATAZONE Managed Card
CDatazone Managed Demo Card
Version 1

Self Asserted Card PHP

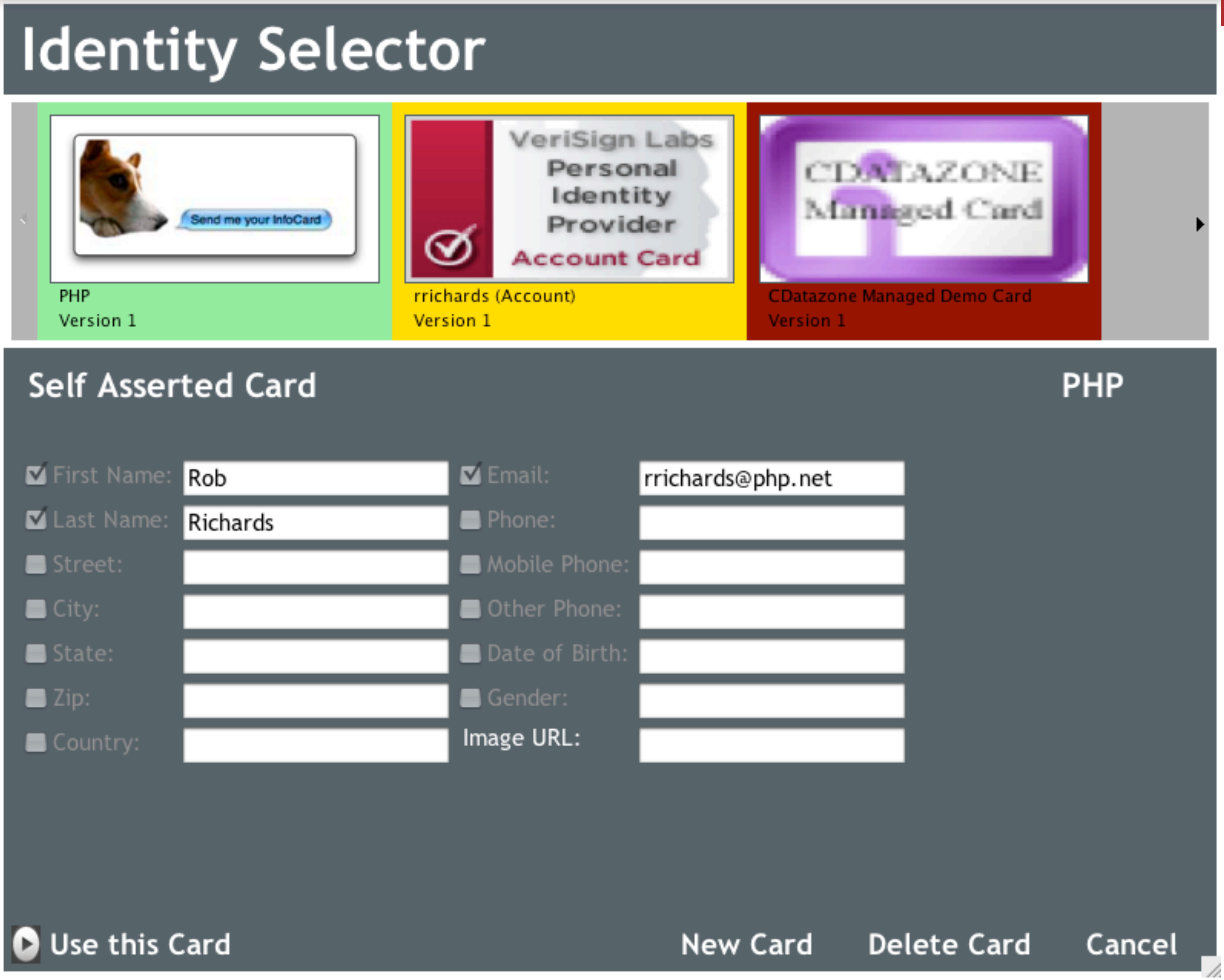
■ First Name:	Rob	■ Email:	rrichards@php.net
■ Last Name:	Richards	■ Phone:	
■ Street:		■ Mobile Phone:	
■ City:		■ Other Phone:	
■ State:		■ Date of Birth:	
■ Zip:		■ Gender:	
■ Country:		Image URL:	

Use this Card New Card Delete Card Cancel

Information Cards

- Identifier is unique amongst parties
  - Distinct digital key for each realm
- Protections again 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

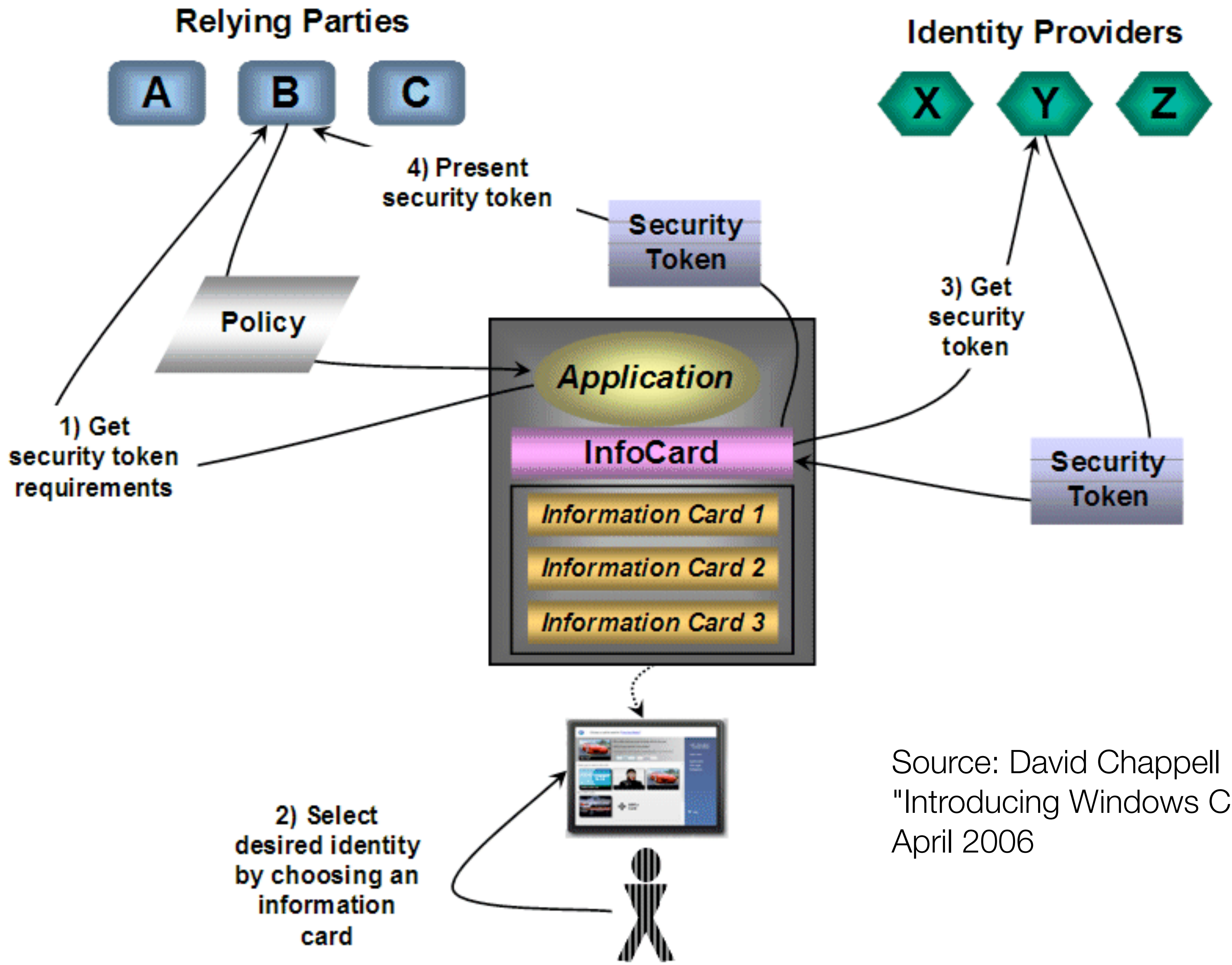
CDatazone Managed Demo Card
Version 1

Self Asserted Card — PHP

☑ First Name:	Rob	☑ Email:	rrichards@php.net
☑ Last Name:	Richards	☐ Phone:	
☐ Street:		☐ Mobile Phone:	
☐ City:		☐ Other Phone:	
☐ State:		☐ Date of Birth:	
☐ Zip:		☐ Gender:	
☐ Country:		Image URL:	

Information Cards Interaction

....



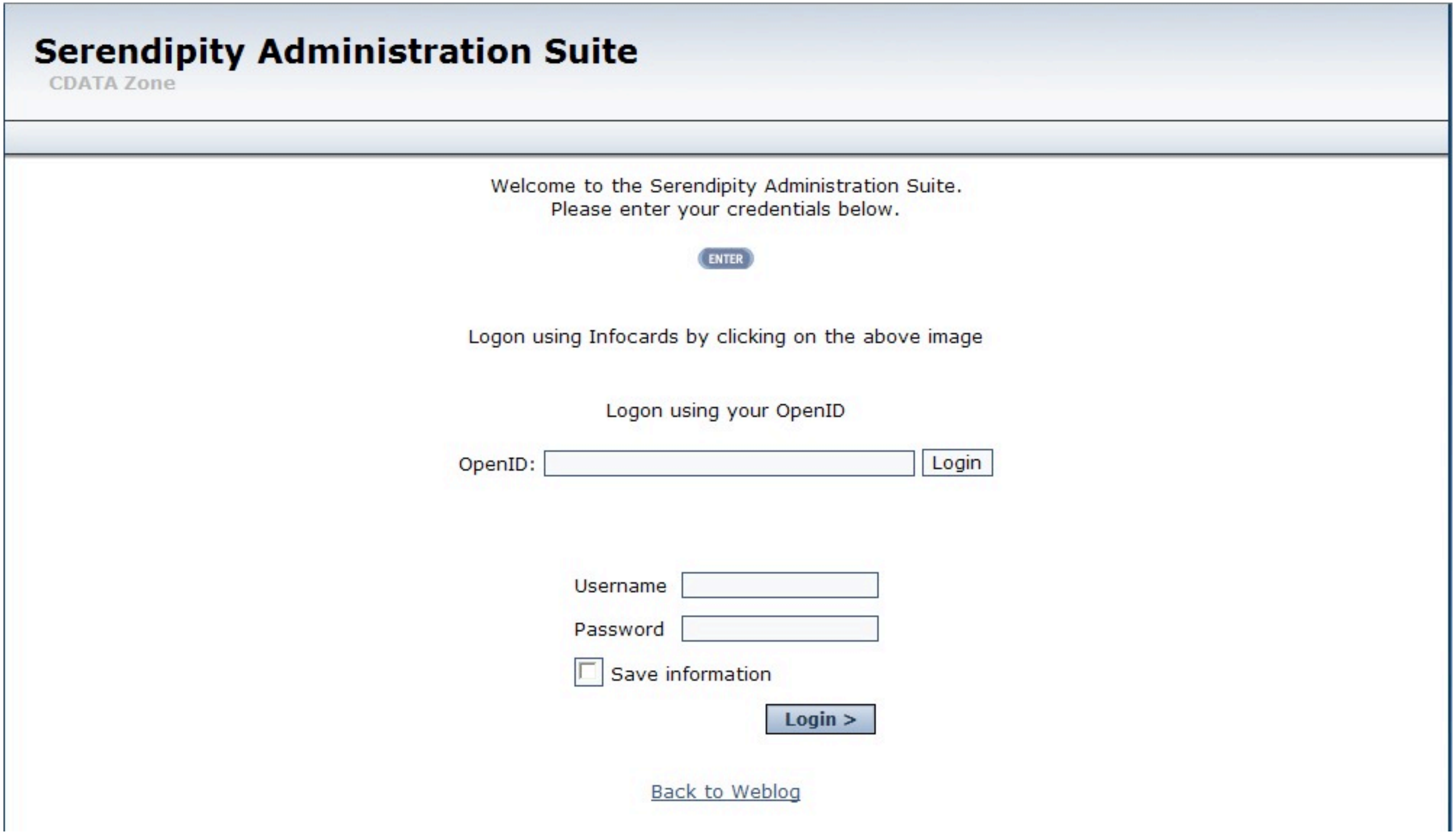
Source: David Chappell
"Introducing Windows CardSpace"
April 2006

MASHERY

MASHERY

Information Card Validation Example

Information Card Login



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: [ ] Login

Username [ ]

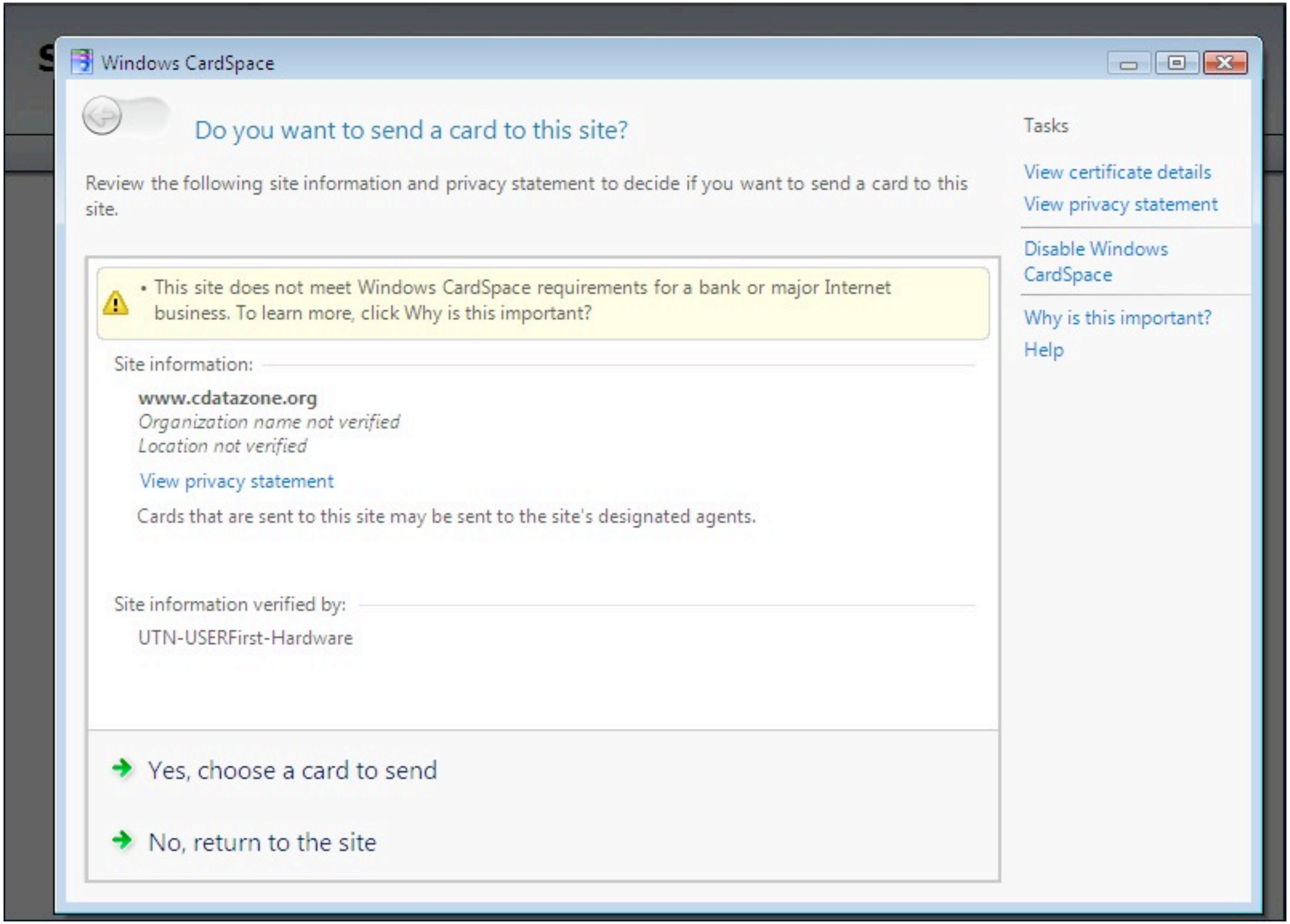
Password [ ]

□ Save information

Login >

Back to Weblog

Site Information



Do you want to send a card to this site?

Review the following site information and privacy statement to decide if you want to send a card to this site.

- This site does not meet Windows CardSpace requirements for a bank or major Internet business. To learn more, click Why is this important?

Site information:

www.cdatazone.org
Organization name not verified
Location not verified

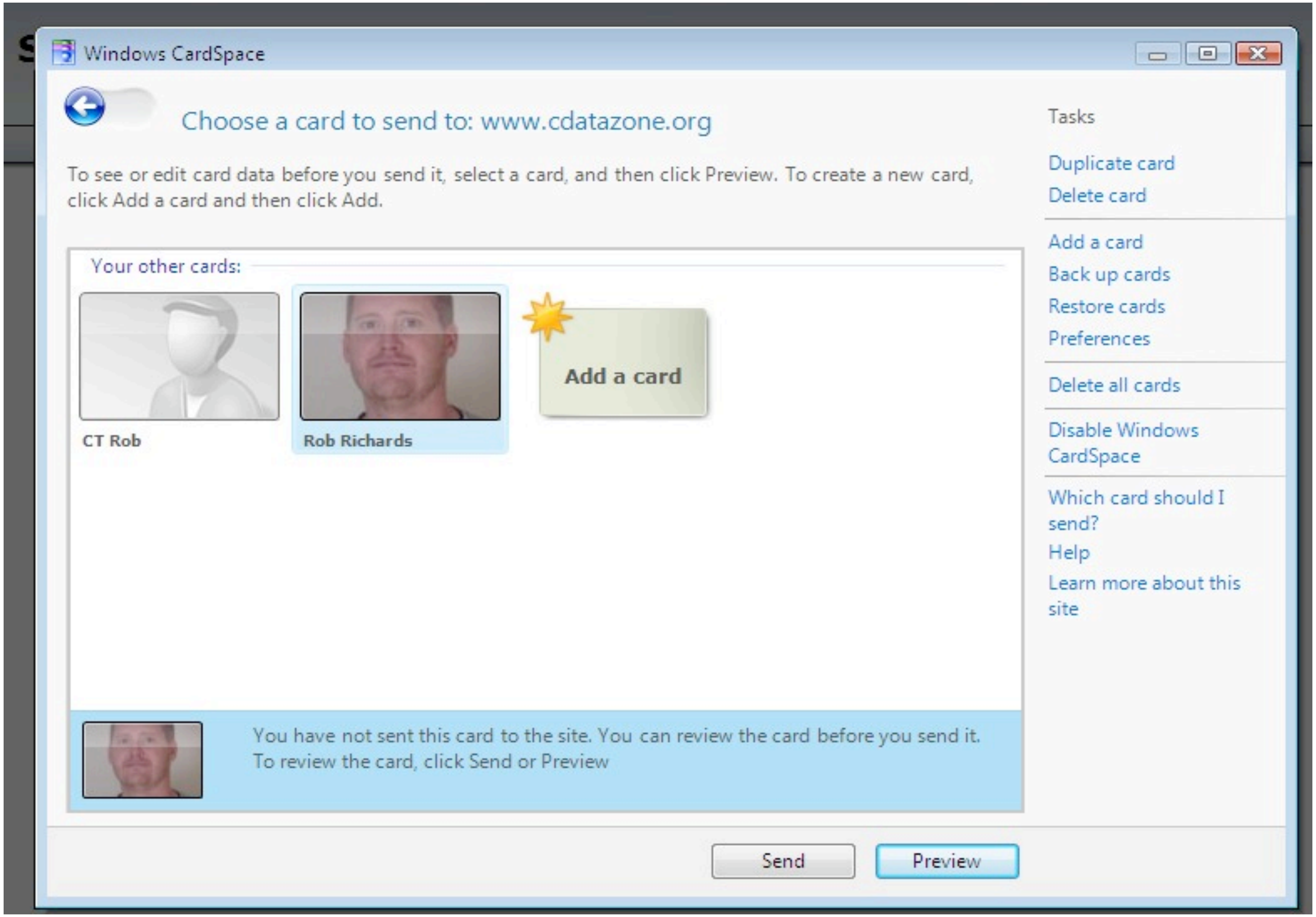
View privacy statement

Cards that are sent to this site may be sent to the site's designated agents.

Site information verified by:

UTN-USERFirst-Hardware

Select or Create Card



Windows CardSpace

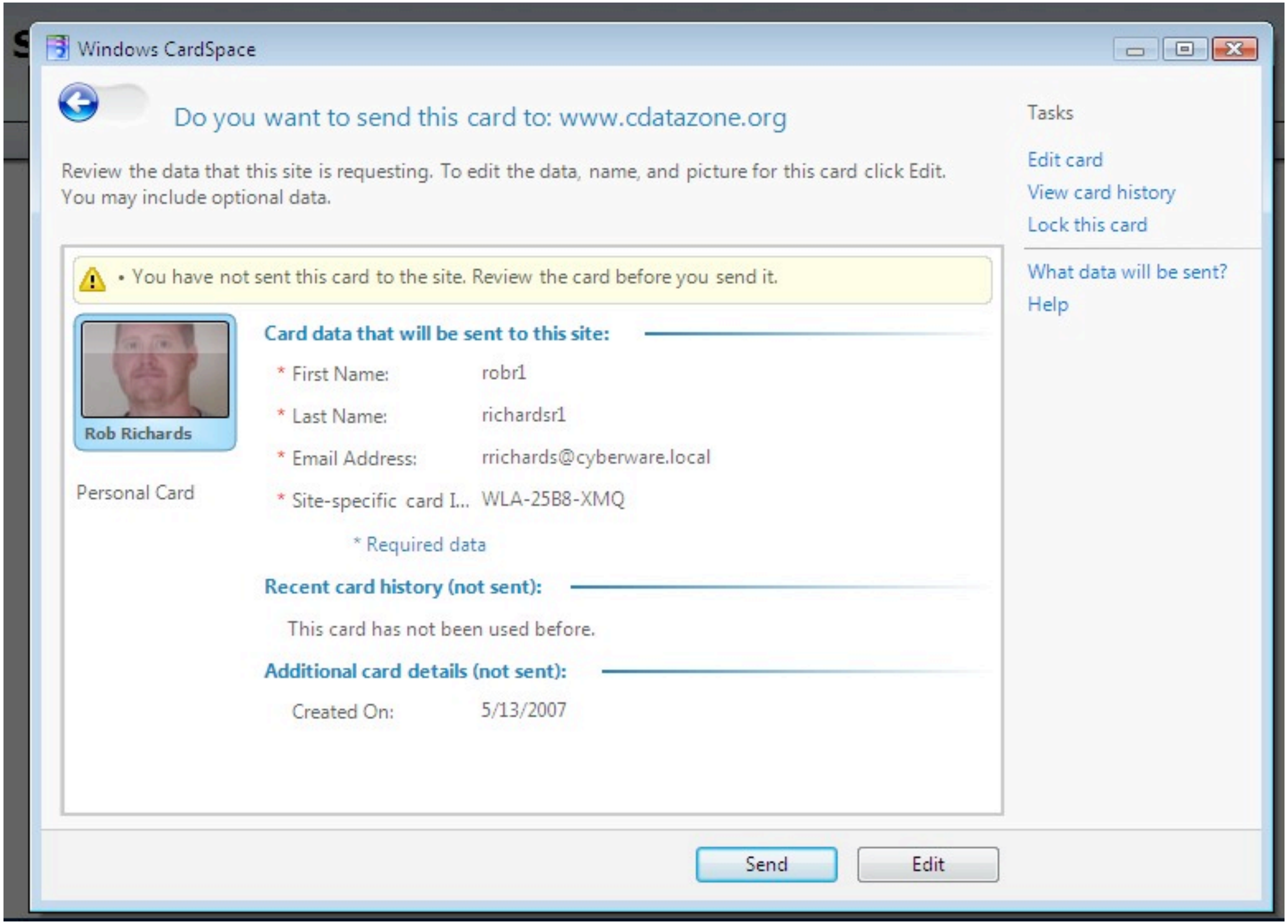
Choose a card to send to: www.cdatazone.org

To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

Your other cards:

You have not sent this card to the site. You can review the card before you send it. To review the card, click Send or Preview

Preview Information To Be Sent



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.

⚠ • You have not sent this card to the site. Review the card before you send it.

Personal Card

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

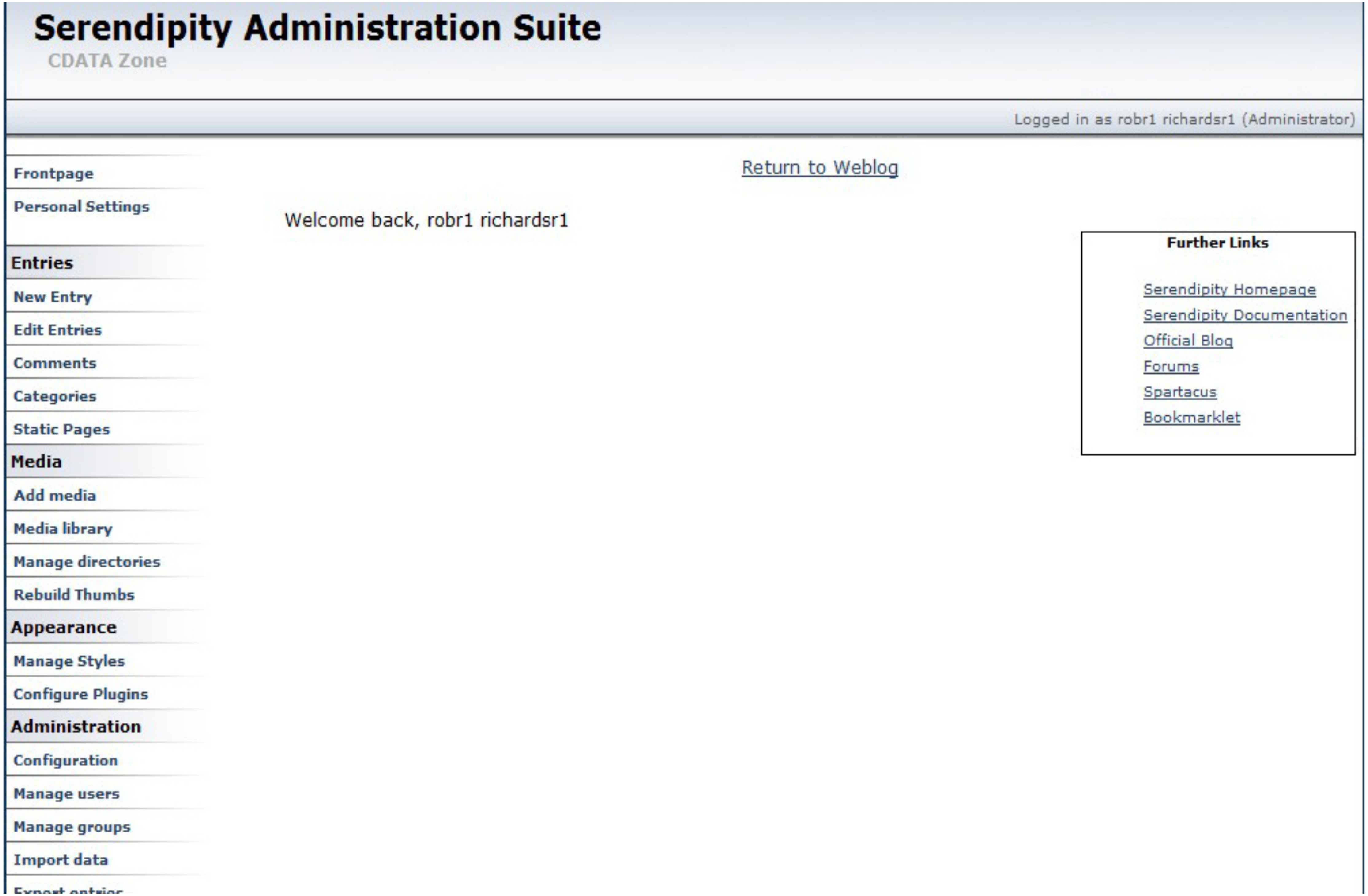
Recent card history (not sent):

This card has not been used before.

Additional card details (not sent):

Created On: 5/13/2007

Information Card Validated



Logged in as robr1 richardsr1 (Administrator)

Welcome back, robr1 richardsr1

InfoCard Selector Initiation

```
<form id="infocard" method="post" action="serendipity_admin.php">
  <center>
    <img src="/infocard/infocard.png" onClick="infocard.submit()"/>
  </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>
```

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

InfoCard: Card Processing

```
$xmlToken = stripslashes($_POST['xmlToken']);
$token = processCard($xmlToken);

if ($token) {
  $asserts = getAssertions($token);

  if (! empty($asserts['privatepersonalidentifier']))
     $identitifier = $asserts['privatepersonalidentifier'];

  if (! empty($asserts['givenname']))
     $name = $asserts['givenname'].' '.$asserts['surname'];

  if (! empty($asserts['emailaddress']))
     $email = $asserts['emailaddress'];
}
```

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

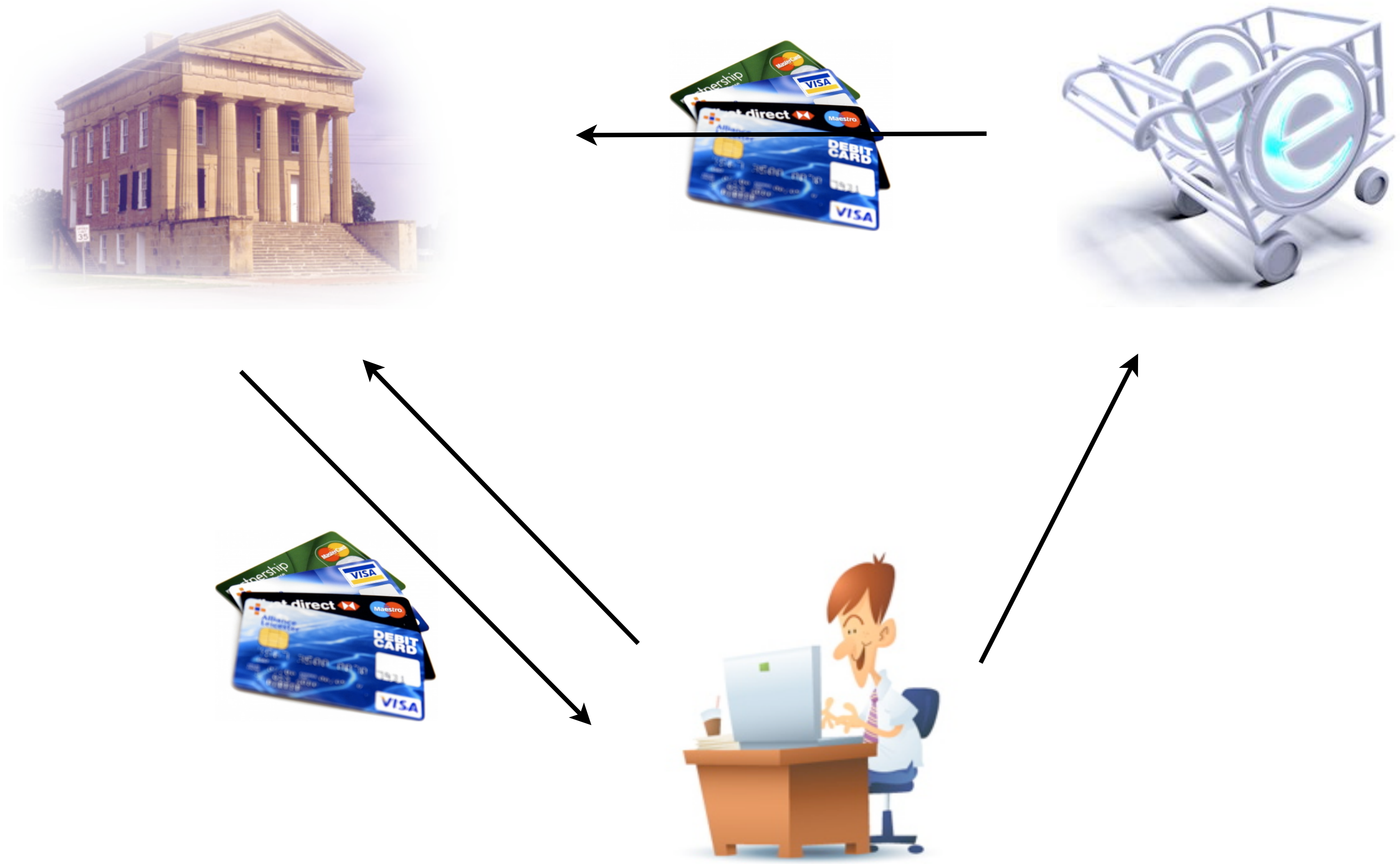
```
<saml:Attribute AttributeName="emailaddress"
  AttributeNamespace=". . ./identity/claims">
    <saml:AttributeValue>rrichards@php.net</saml:AttributeValue>
</saml:Attribute>

<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?

Questions?

MASHERY

Who am I?
The Age of the Digital Identity

Rob Richards

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