Who am I?
The Age of the Digital Identity

Rob Richards
OSCON 2007
7/25/2007

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

LOCAL THUNDER®

“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

LOCAL THUNDER®

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>

rrichards@localthunder.com
Rob Richards
Development Manager

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

7 Laws of Identity

I. User Control and Consent

II. Minimal Disclosure for a Constrained Use

III. Justifiable Parties

IV. Directed Identity

V. Pluralism of Operators and Technologies

VI. Human Integration

VII. Consistent Experience Across Contexts

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

Identity Context Examples

- **Browsing:** a self-asserted identity for exploring the Web (giving away no real data)
- **Personal:** a self-asserted identity for sites with which I want an ongoing but 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

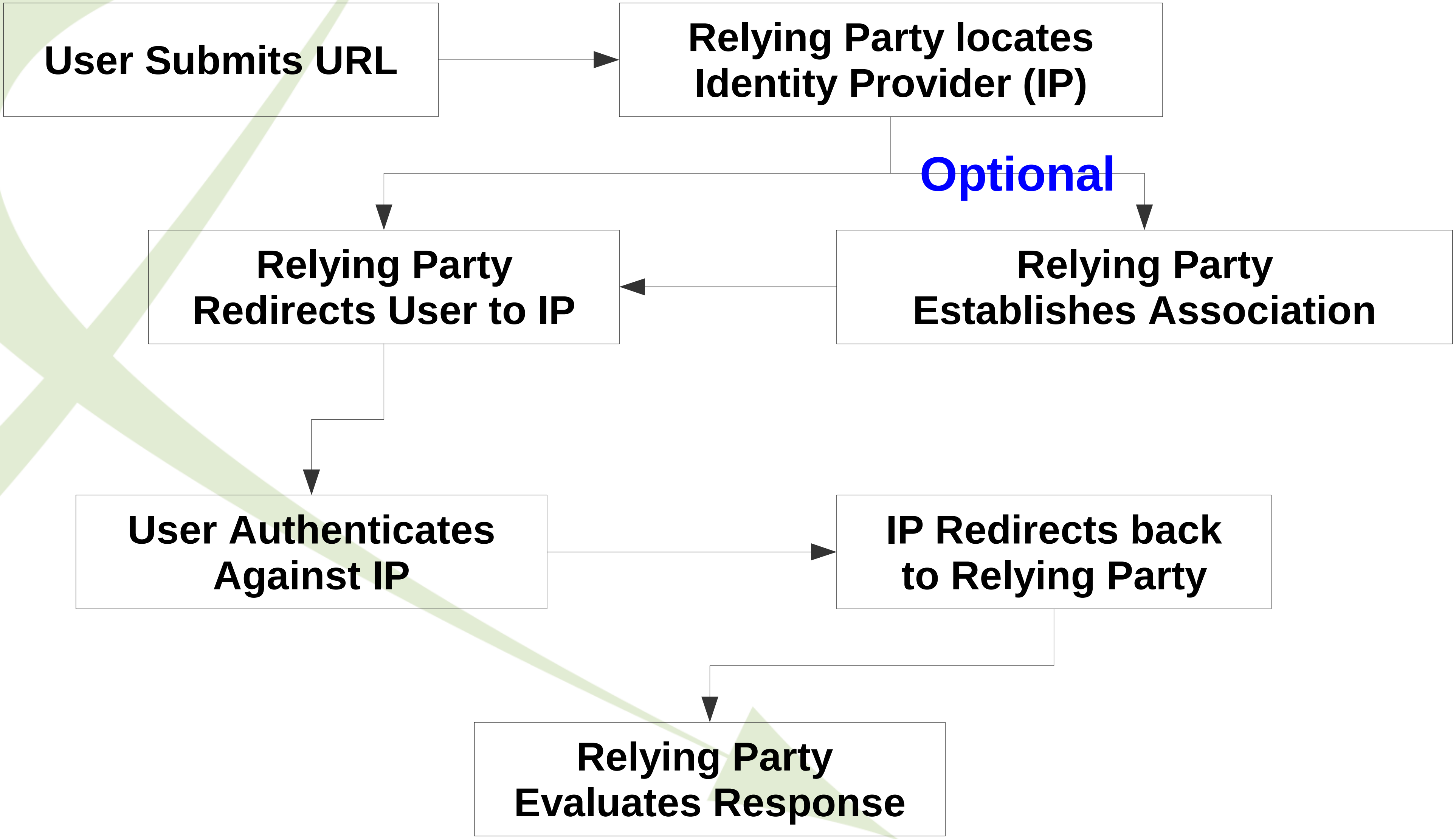
OpenID and Information Cards

- Allow for Single Sign On
- Decentralized
- User-Centric
  - ✧ User is in control of data
  - ✧ User aware of information exchange
- Can reduce amount of personal information a remote site would need to store
- Potential to increase the Web experience while maintaining User privacy

OpenID

- URL based
  - ✧ http://rrichards.pip.verisignlabs.com/
  - ✧ =rob.richards (http://xri.net/=rob.richards)
- Not Machine Dependant
- Based on Simplicity
  - ✧ HTTP/S
  - ✧ URLs
- PHP Libraries (There are More . . .)
  - ✧ PHP OpenID library (http://www.openidenabled.com/openid/libraries/php)
  - ✧ OmniTI OpenID (https://labs.omniti.com/trac/alexandria/wiki)

OpenID Interaction



User Submits URL

Relying Party locates Identity Provider (IP)

Optional

Relying Party Redirects User to IP

Relying Party Establishes Association

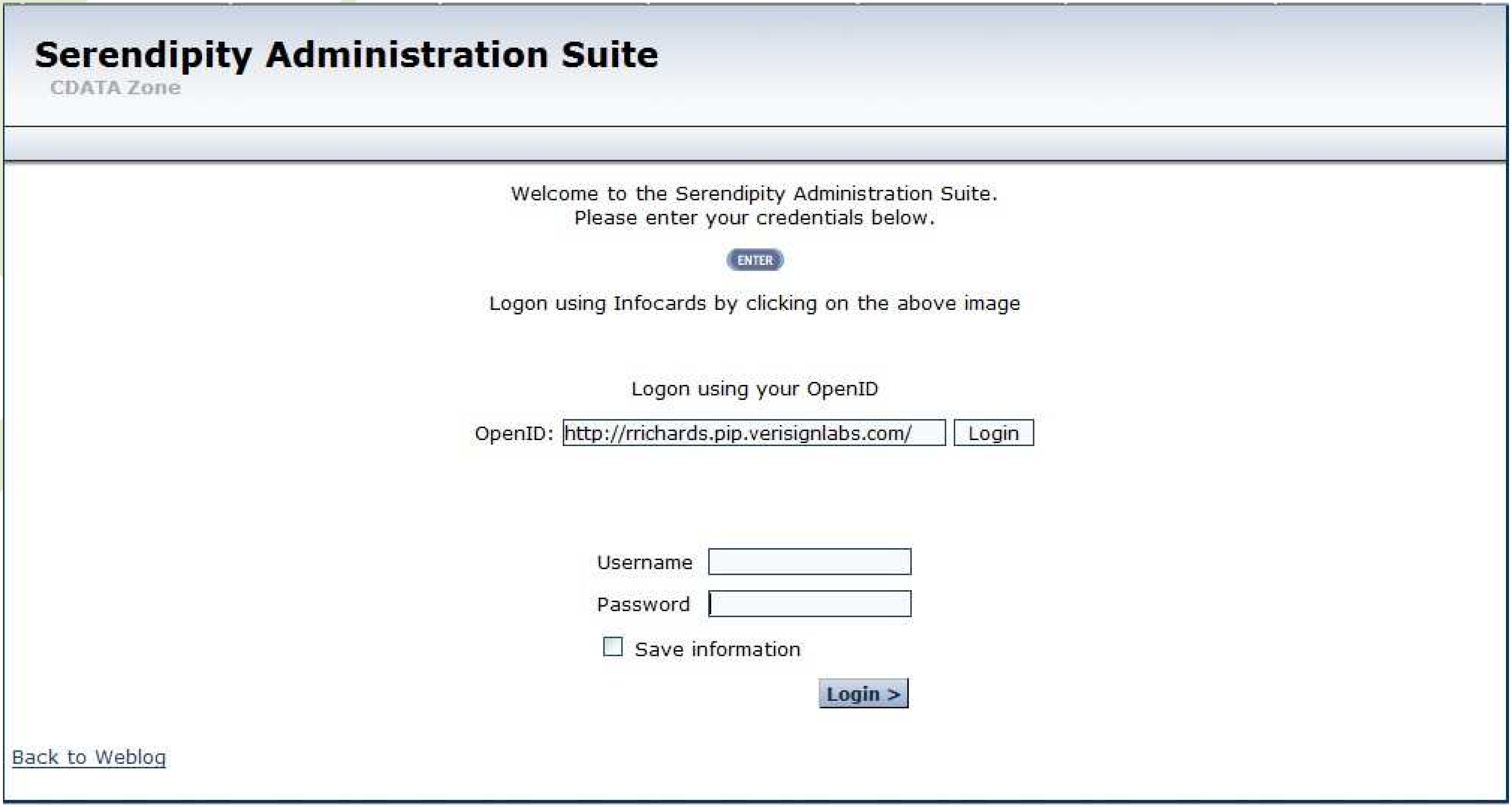
User Authenticates Against IP

IP Redirects back to Relying Party

Relying Party Evaluates Response

OpenID Validation Example

Site Login Page



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

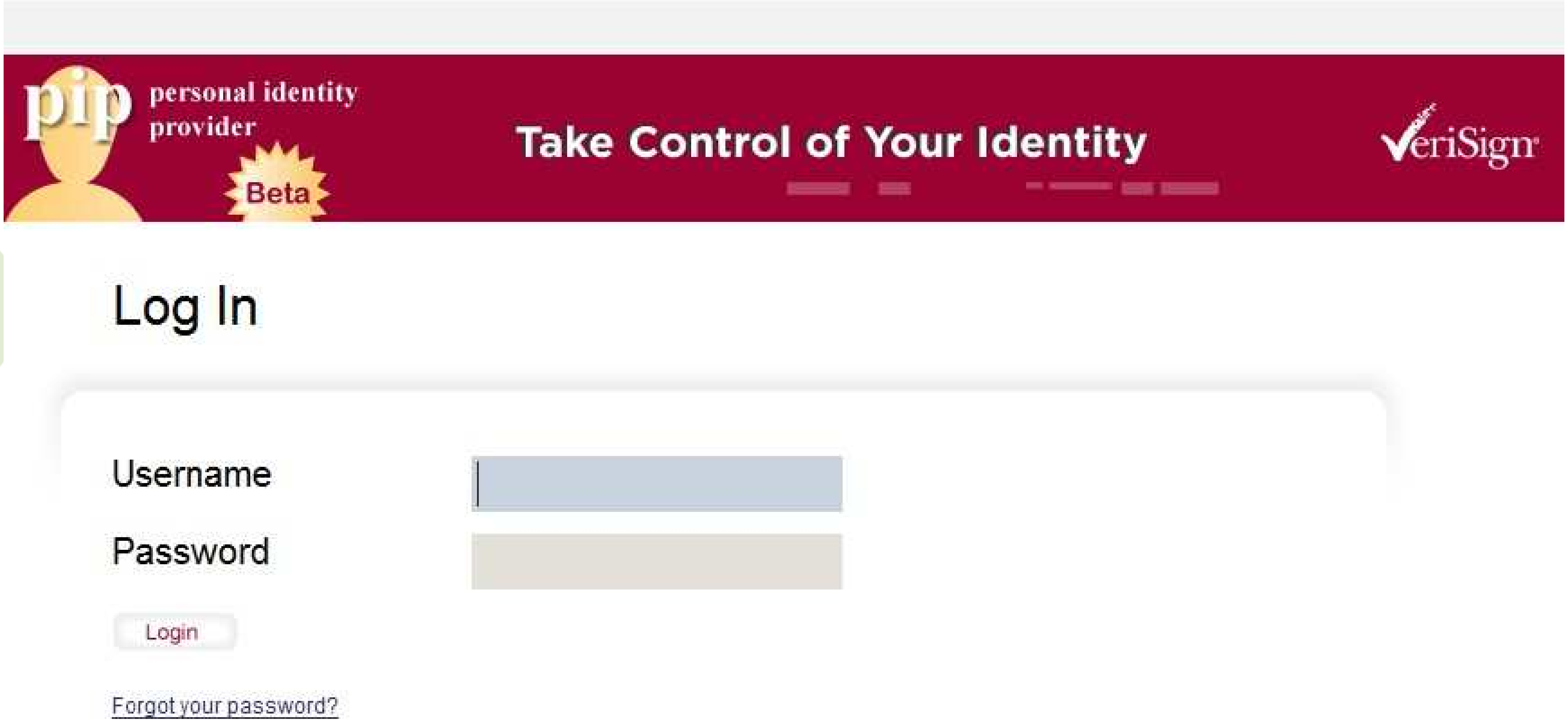
OpenID: http://rrichards.pip.verisignlabs.com/

Username

Password

□ Save information

OpenID Verification



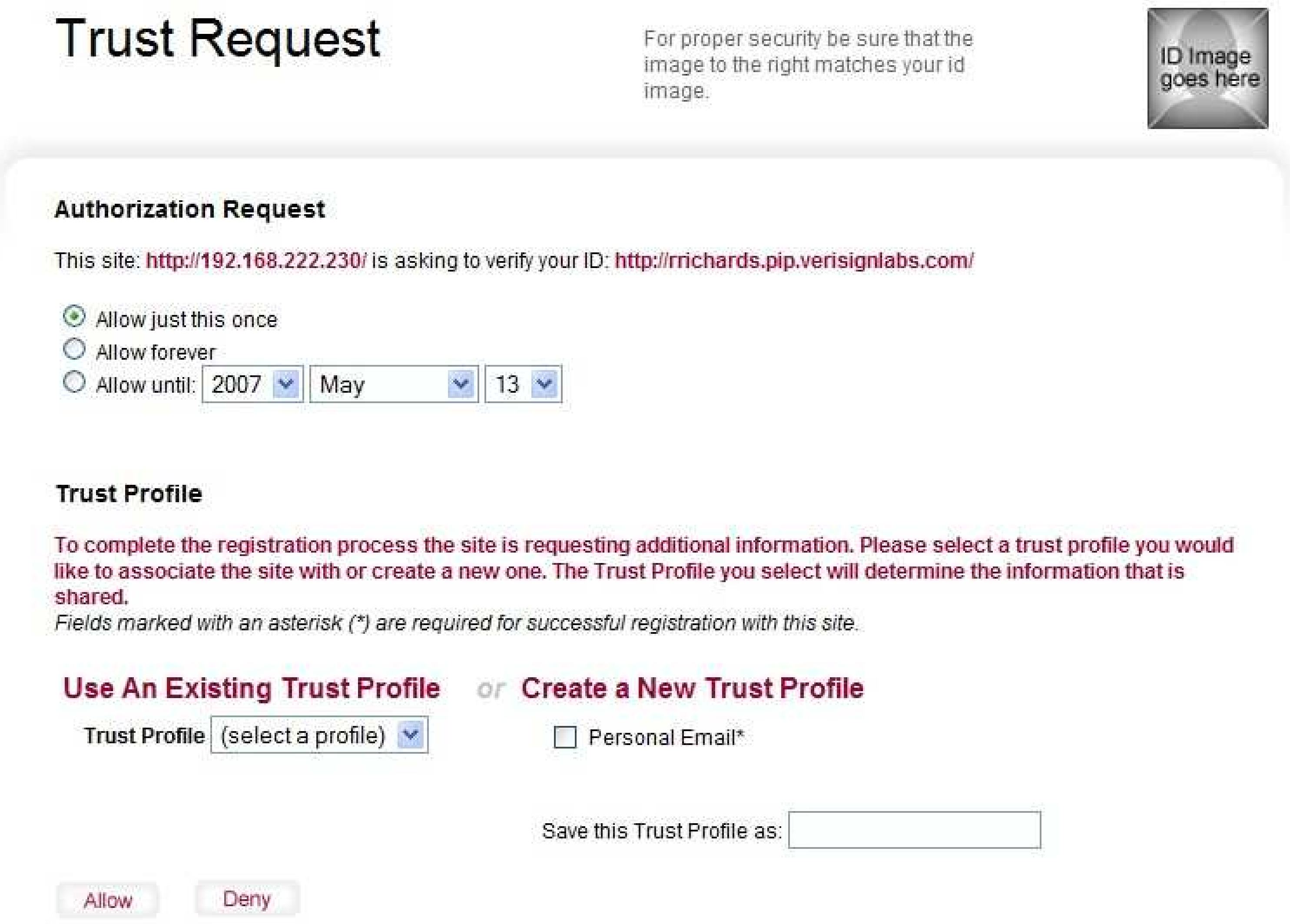
Log In

Username

Password

Forgot your password?

User Trust Consent



Trust Request

For proper security be sure that the image to the right matches your id image.

Authorization Request

This site: http://192.168.222.230/ is asking to verify your ID: http://rrichards.pip.verisignlabs.com/

● Allow just this once
○ Allow forever
○ Allow until: 2007 May 13

Trust Profile

To complete the registration process the site is requesting additional information. Please select a trust profile you would like to associate the site with or create a new one. The Trust Profile you select will determine the information that is shared.
Fields marked with an asterisk (*) are required for successful registration with this site.

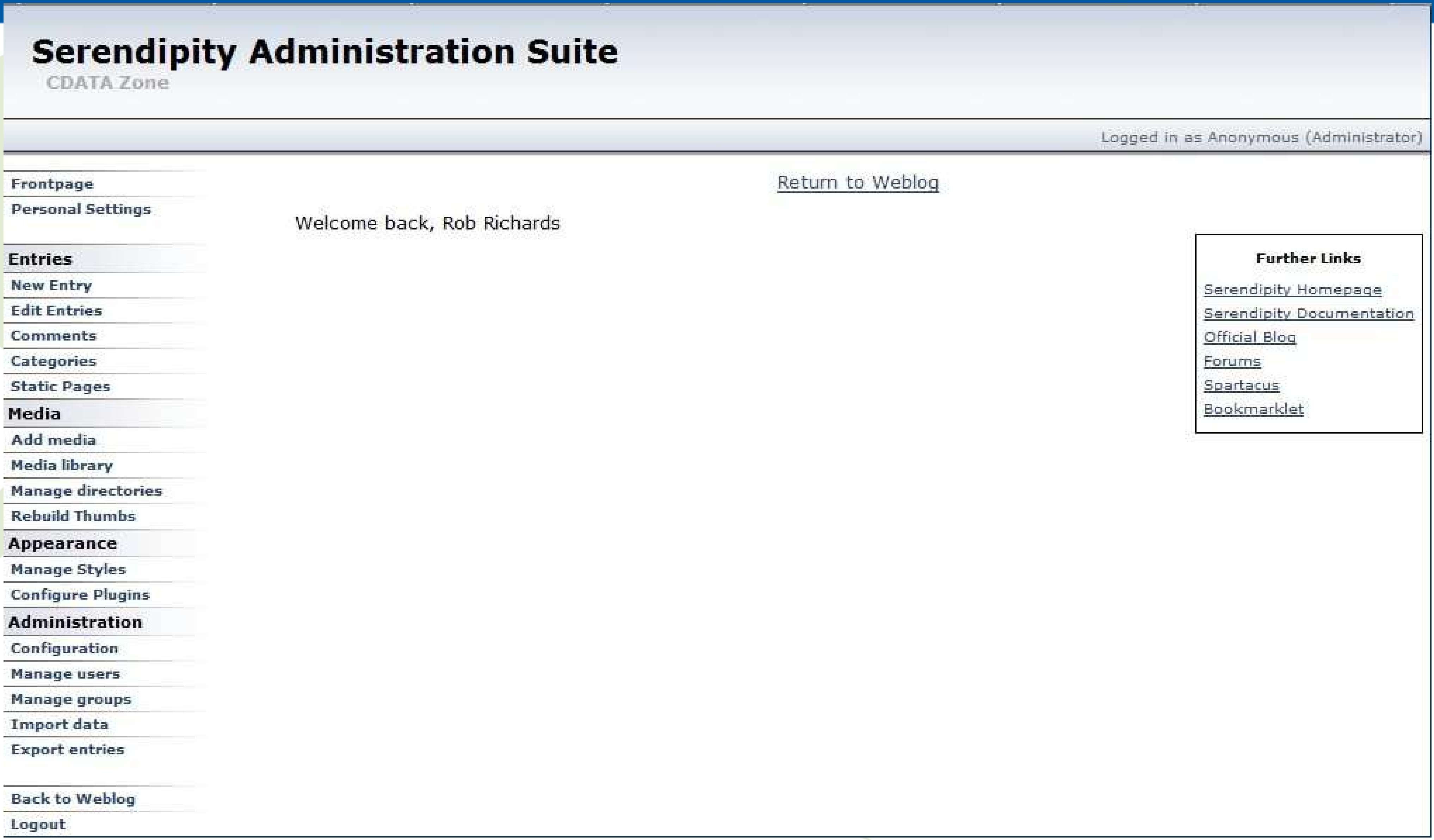
Use An Existing Trust Profile or **Create a New Trust Profile**

Trust Profile (select a profile)

□ Personal Email*

Save this Trust Profile as:

OpenID validated



Serendipity Administration Suite

CDATA Zone

Logged in as Anonymous (Administrator)

Welcome back, Rob Richards

Further Links

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/

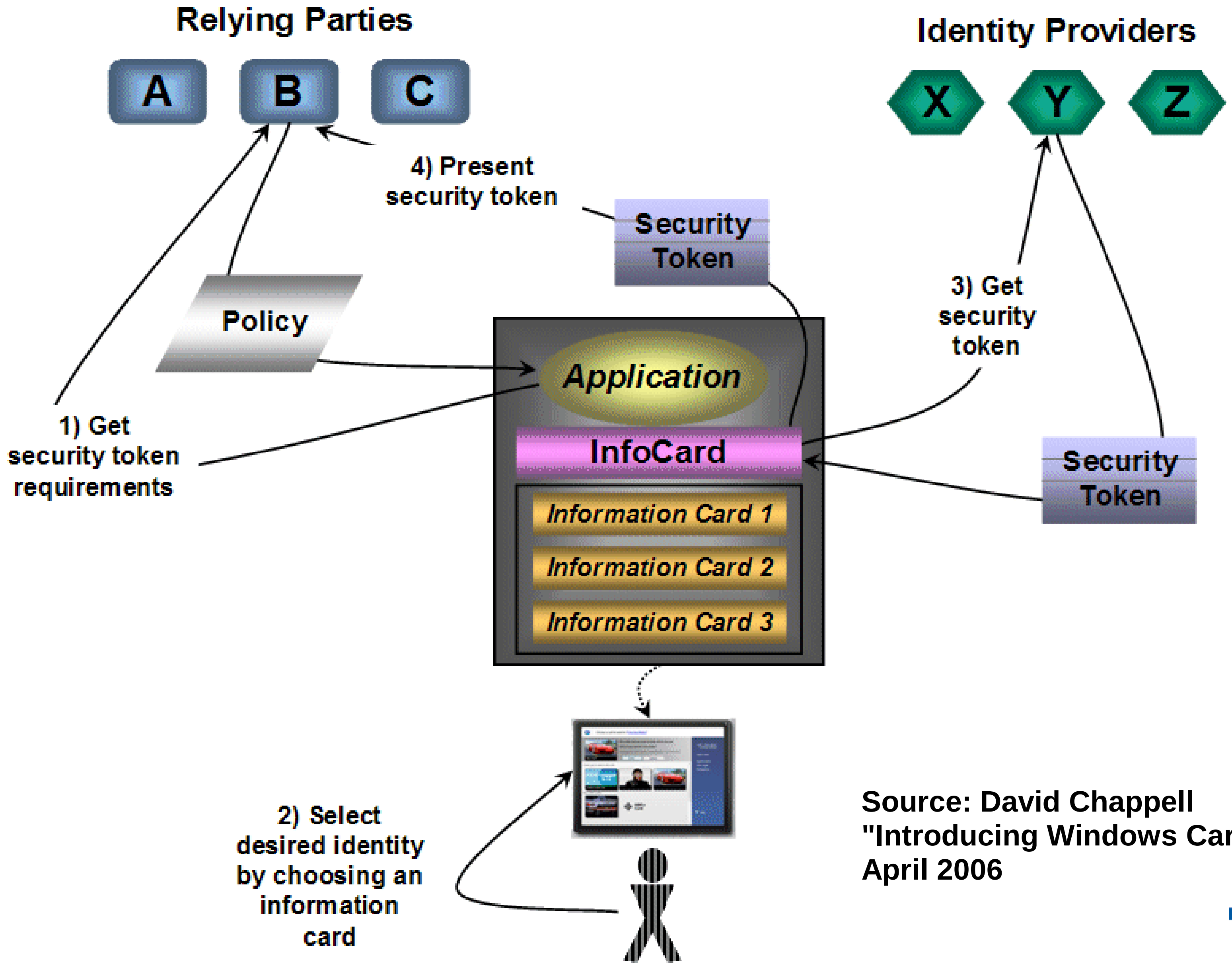
openid.signed=identity,return_to,mode

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

Information Cards (Infocards)

- CardSpace != Information Cards
  - ✧ Information Cards are not Microsoft specific
  - ✧ Variety of selectors for various OSs (xmldap / Higgins)
- Identities represented as cards
  - ✧ Self Asserted
  - ✧ Managed (Third Party provided)
- Identifier is unique amongst parties
- Complex Technologies
  - ✧ SAML
  - ✧ WS-Security / WS-Policy / WS-Trust

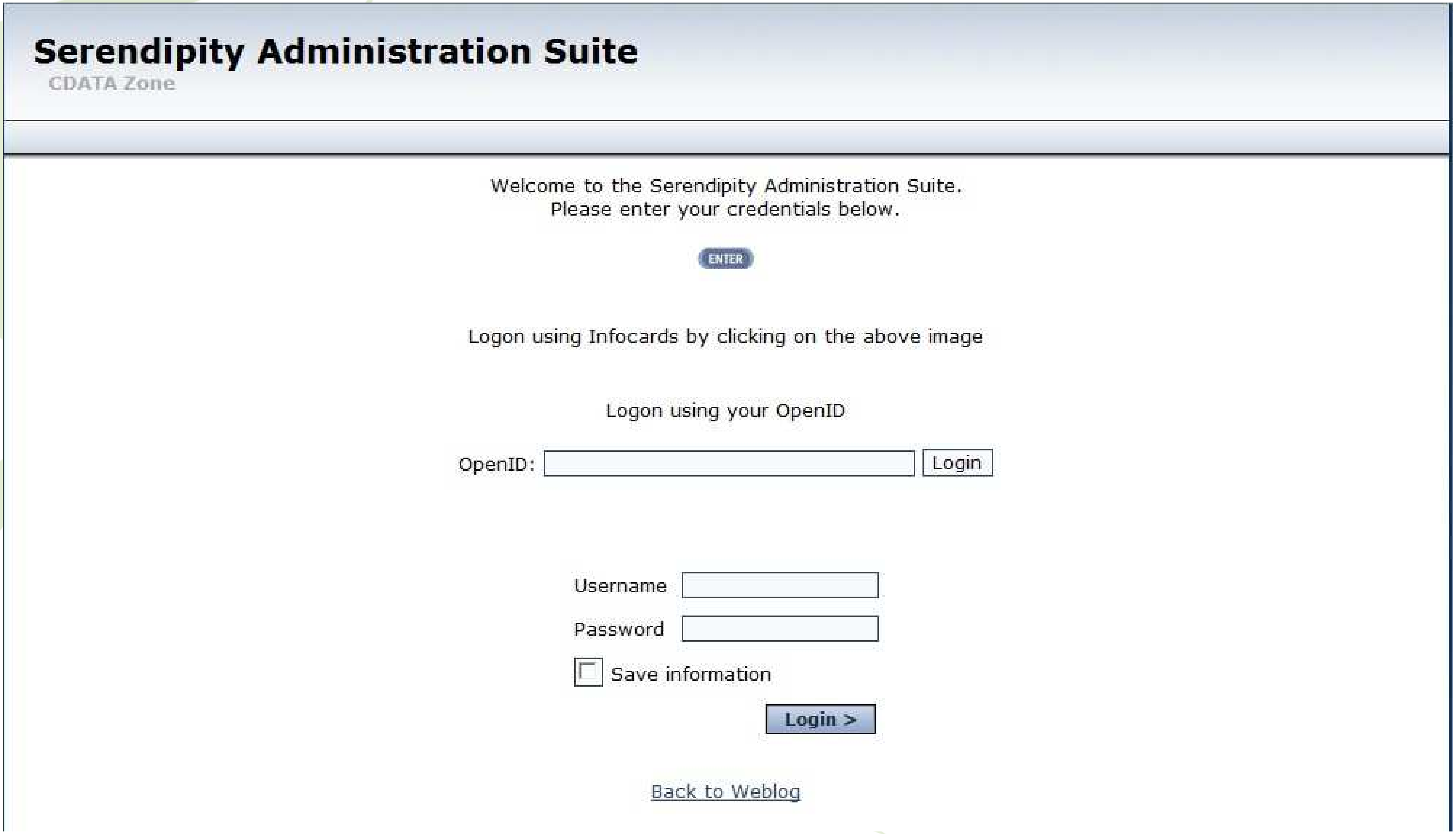
Information Cards Interaction



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.

Logon using Infocards by clicking on the above image

Logon using your OpenID

OpenID:

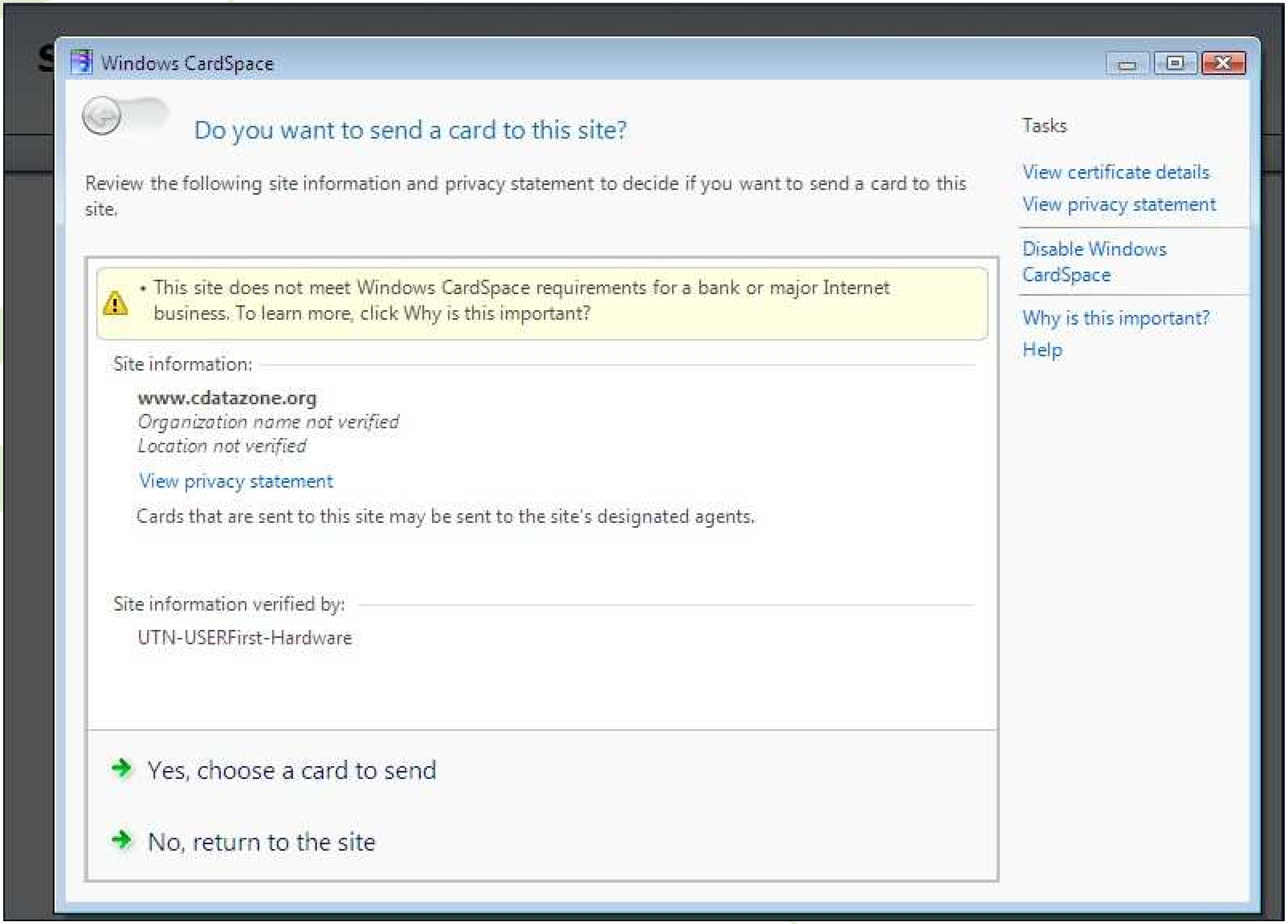
Username

Password

□ Save information

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

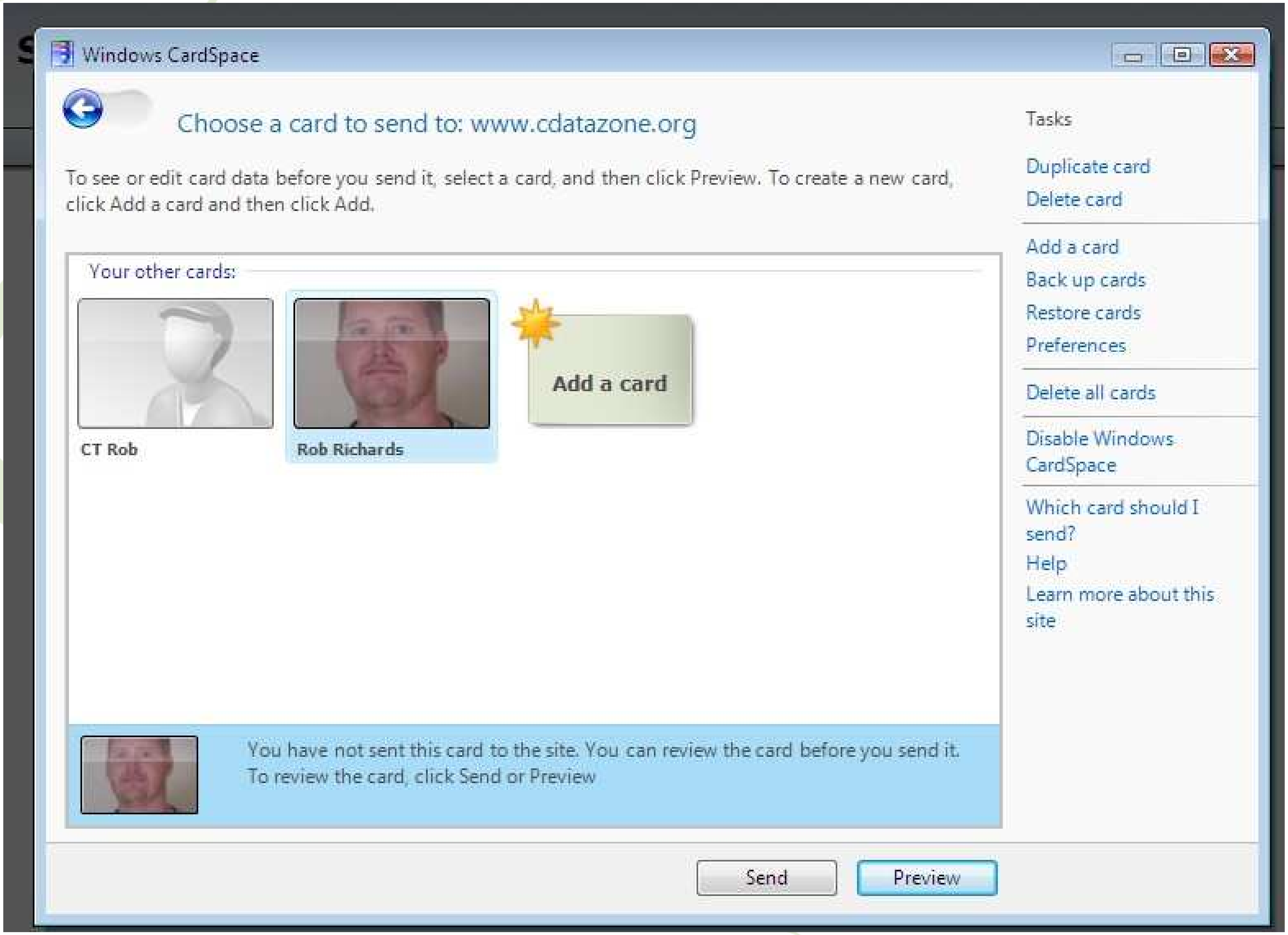
View privacy statement

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



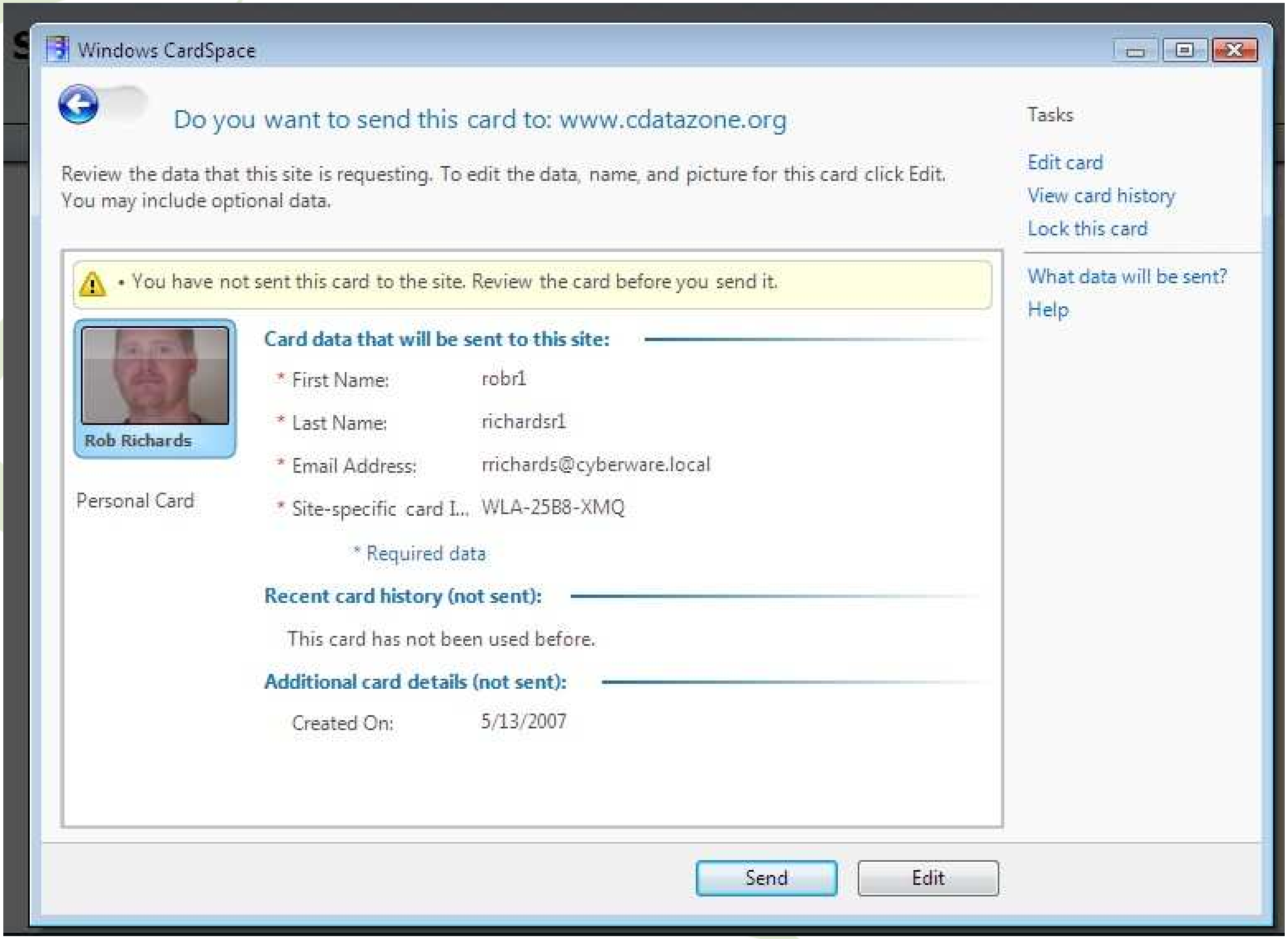
Choose a card to send to: www.cdatazone.org

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.

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

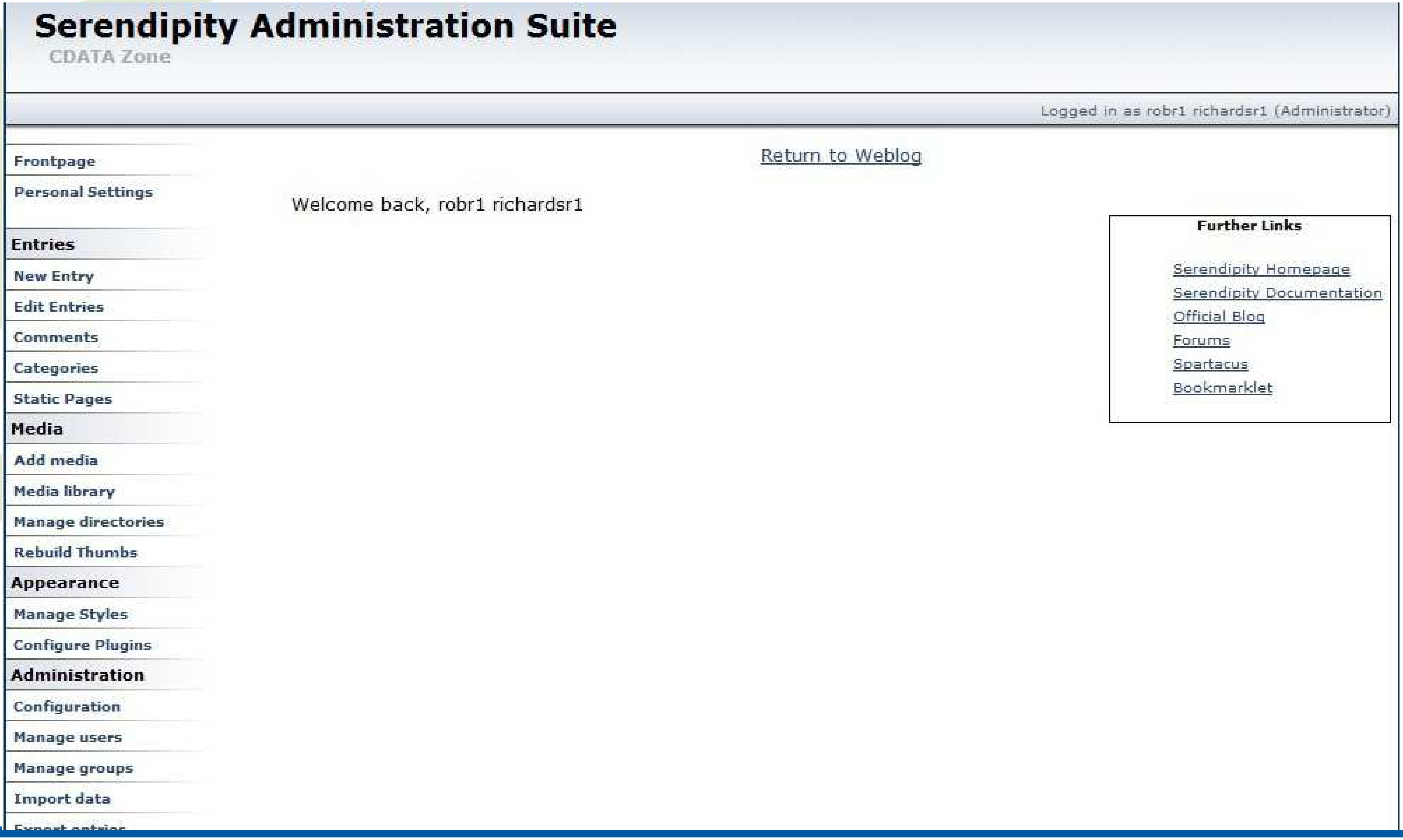
Recent card history (not sent):

This card has not been used before.

Additional card details (not sent):

Created On:	5/13/2007

Information Card Validated



Serendipity Administration Suite

CDATA Zone

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/enter.gif" 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

- xmlseclibs.php
  - ✧ XMLDSig
  - ✧ XMLENC
- infocard-lib.php
  - ✧ Decrypts submitted XML Token
  - ✧ Verifies Signed SAML Token
  - ✧ Parses Assertions

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>
```

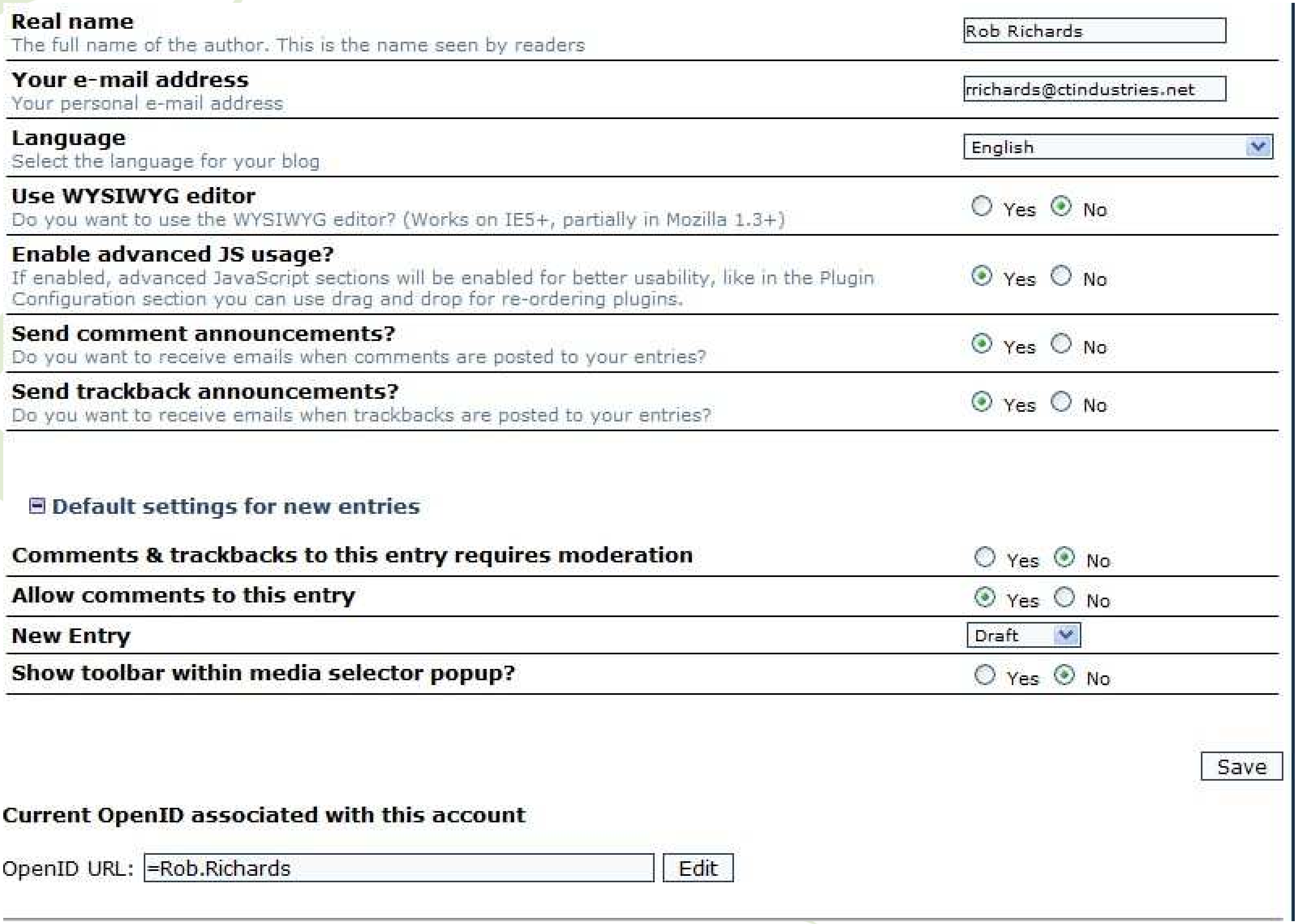
Serendipity Weblog

- http://www.s9y.org/
- Account based
  - ✧ Traditional Username/Password Authentication
  - ✧ Usergroup permission scheme
- Commenting Capabilities
  - ✧ Anonymous
  - ✧ Authenticated Users Only Option
  - ✧ Captchas and other spam blocking techniques

Integrating with User Accounts

- How is the initial association performed?
- Who has the ability to change a users ID?
  - ✧ Users should always have control over their ID
  - ✧ Can an Administrator change a user's ID?
- Is owner verification of ID required prior to change?

OpenID Association



Real name The full name of the author. This is the name seen by readers	Rob Richards
Your e-mail address Your personal e-mail address	rrichards@ctindustries.net
Language Select the language for your blog	English
Use WYSIWYG editor Do you want to use the WYSIWYG editor? (Works on IE5+, partially in Mozilla 1.3+)	○ Yes ● No
Enable advanced JS usage? If enabled, advanced JavaScript sections will be enabled for better usability, like in the Plugin Configuration section you can use drag and drop for re-ordering plugins.	● Yes ○ No
Send comment announcements? Do you want to receive emails when comments are posted to your entries?	● Yes ○ No
Send trackback announcements? Do you want to receive emails when trackbacks are posted to your entries?	● Yes ○ No

⊟ **Default settings for new entries**

Comments & trackbacks to this entry requires moderation	○ Yes ● No
Allow comments to this entry	● Yes ○ No
New Entry	Draft
Show toolbar within media selector popup?	○ Yes ● No

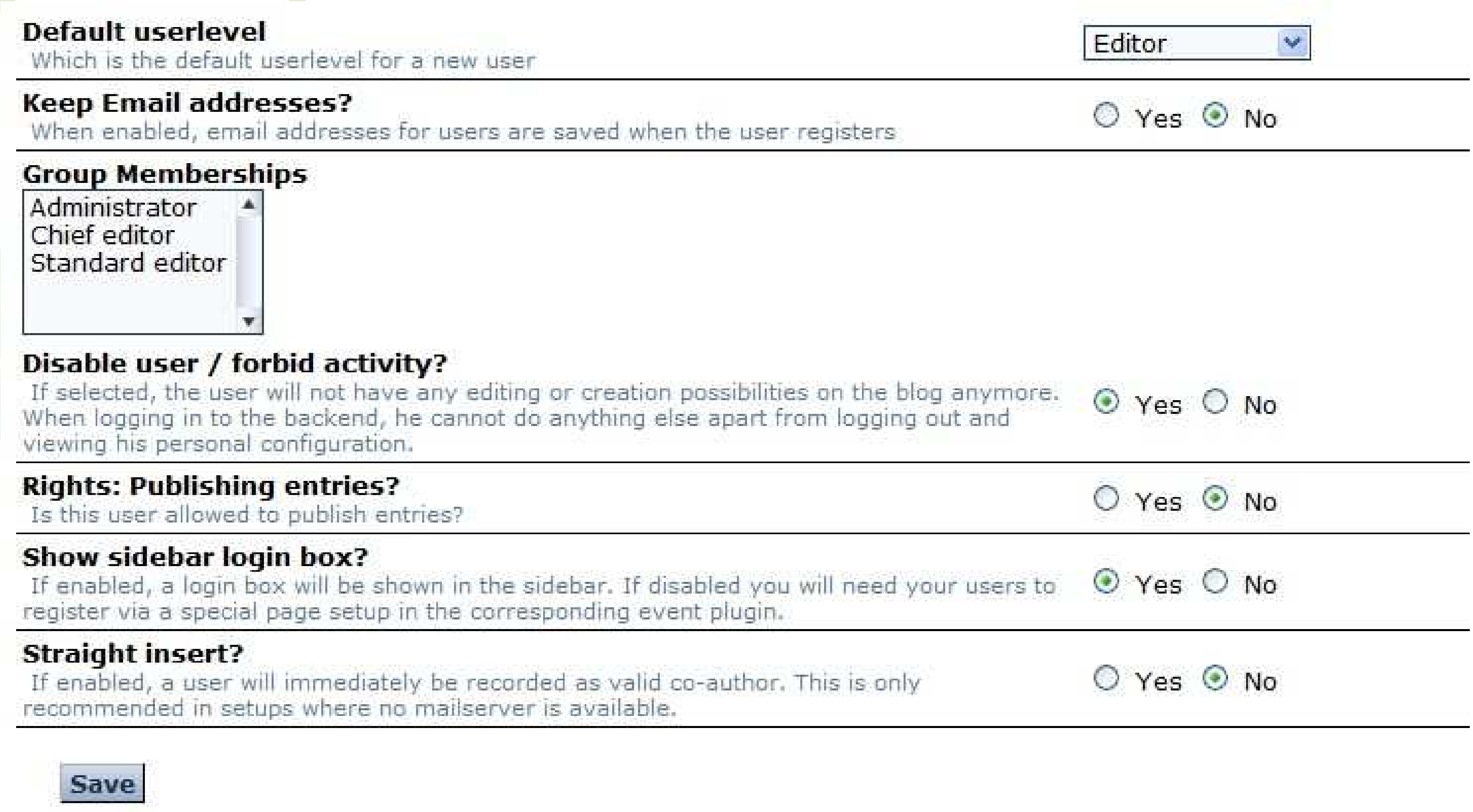
Current OpenID associated with this account

OpenID URL: =Rob.Richards

Untrusted Users

- Is an account required?
  - ✧ Is the software flexible enough to handle identity without an account?
  - ✧ Should anonymous accounts be allowed?
  - ✧ Should anonymous users be allowed to set personal preferences?
- Do you require any additional information from these users?
  - ✧ OpenID: Simple Registration Extension
  - ✧ InfoCards: can specify required information

InfoCard Self-Registration



Default userlevel
Which is the default userlevel for a new user
Editor

Keep Email addresses?
When enabled, email addresses for users are saved when the user registers
○ Yes ● No

Group Memberships
Administrator
Chief editor
Standard editor

Disable user / forbid activity?
If selected, the user will not have any editing or creation possibilities on the blog anymore. When logging in to the backend, he cannot do anything else apart from logging out and viewing his personal configuration.
● Yes ○ No

Rights: Publishing entries?
Is this user allowed to publish entries?
○ Yes ● No

Show sidebar login box?
If enabled, a login box will be shown in the sidebar. If disabled you will need your users to register via a special page setup in the corresponding event plugin.
● Yes ○ No

Straight insert?
If enabled, a user will immediately be recorded as valid co-author. This is only recommended in setups where no mailserver is available.
○ Yes ● No

Questions?

Who am I?
The Age of the Digital Identity

Rob Richards
OSCON 2007
7/25/2007

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

www.cdatazone.org

LOCAL THUNDER