

Who am I? The Age of the Digital Identity

Rob Richards
5/23/2007

www.cdatazone.org
<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

Who Am I?

- PHP Developer
- libxml2 contributor
- Author of Pro PHP XML & Web Services
- Robert Richards
- <address>
- <DOB>
- <Driver license #>
- Tiger
- Dragon
- Snake
- Crane
- Co-Worker
- Coffee junkie

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 Digitally?

=rob.richards

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

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

richards@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

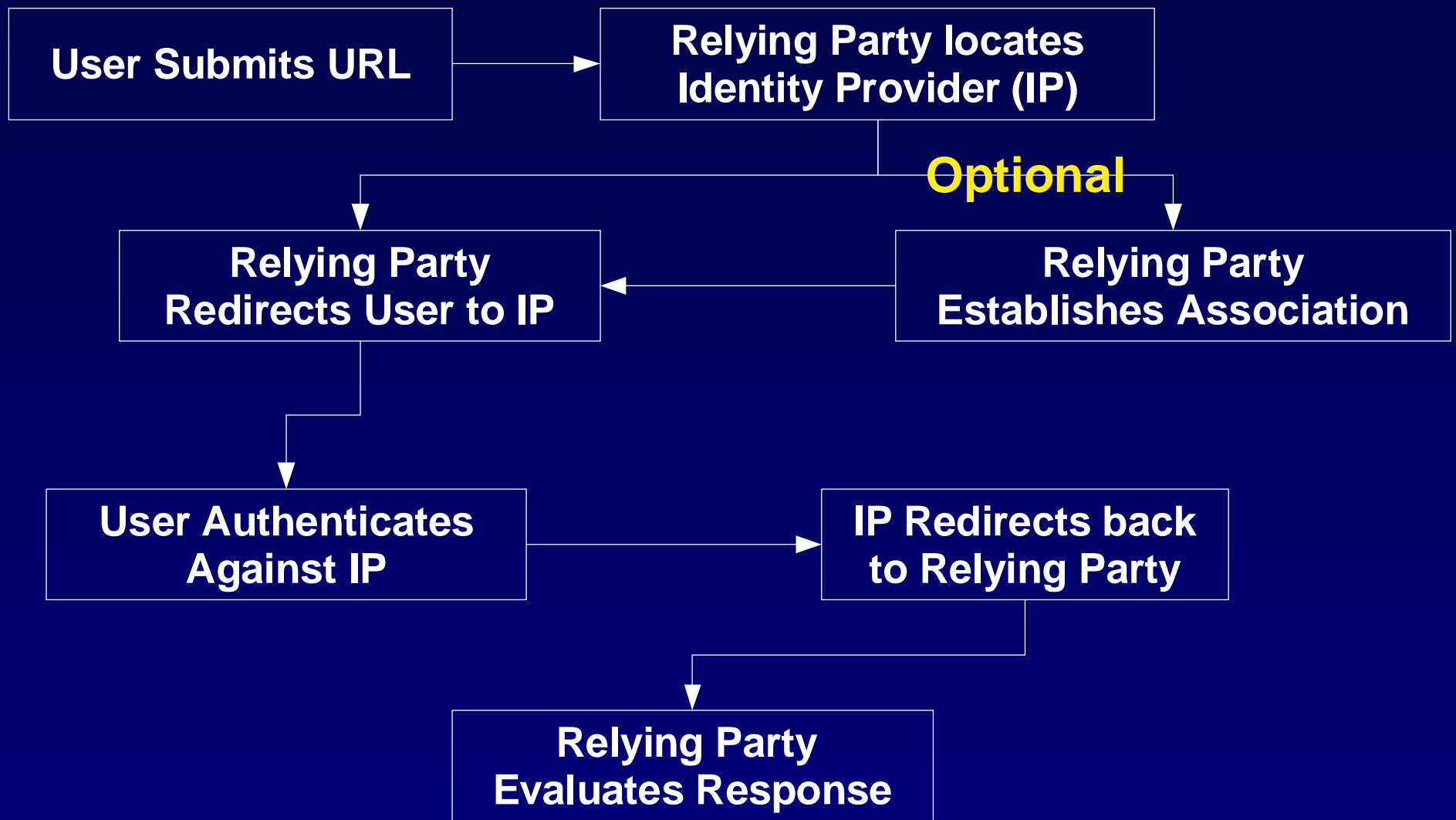
OpenID and Information Cards

- Decentralized
- User-Centric
 - User is in control of data
 - User aware of information exchange
- Allow for Single Sign On
- 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



OpenID Validation Example

Site Login Page

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:

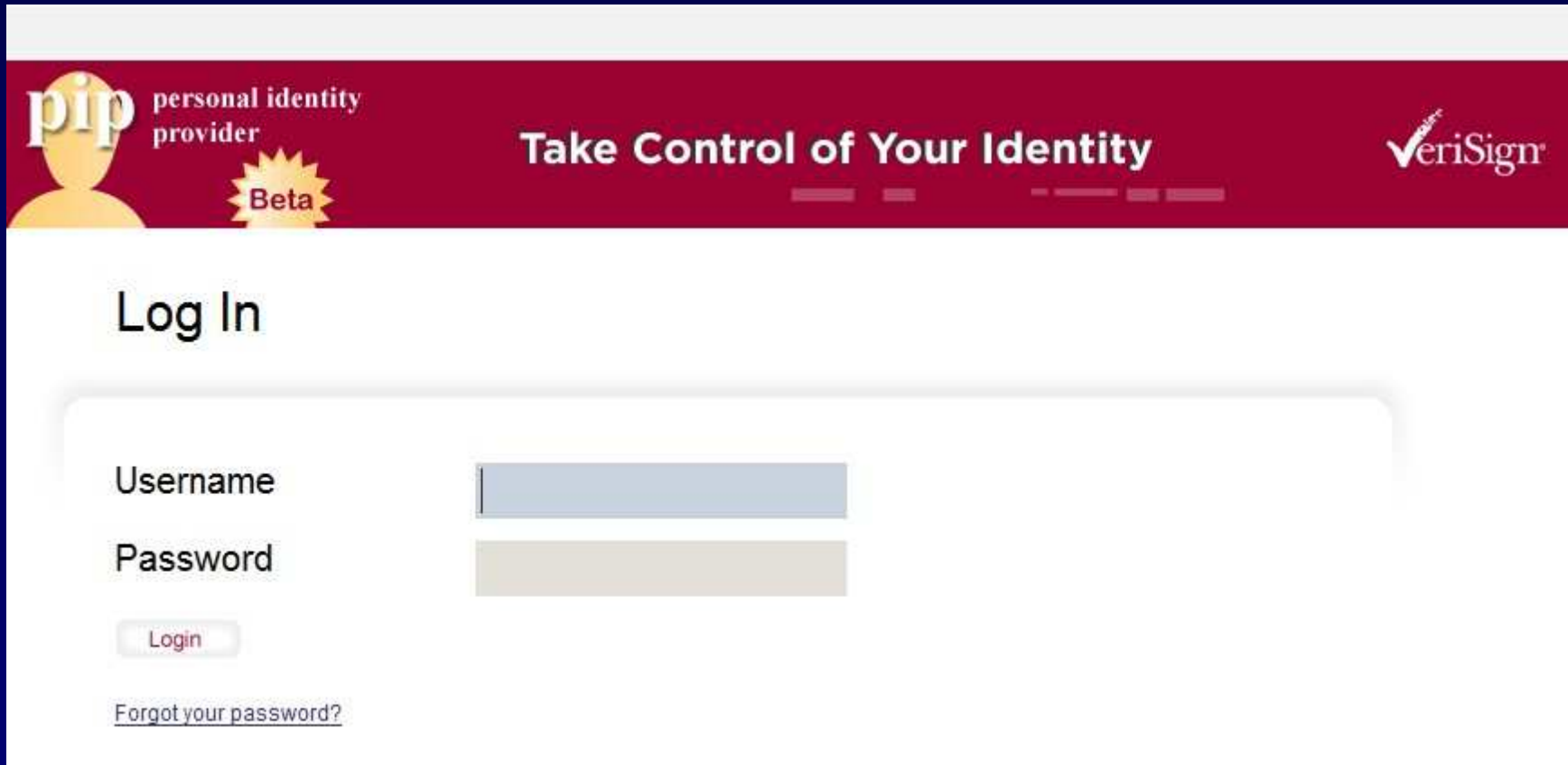
Username

Password

Save information

[Back to Weblog](#)

OpenID Verification



pip personal identity provider
Beta

Take Control of Your Identity

VeriSign

Log In

Username

Password


Login

[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:

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 Personal Email*

Save this Trust Profile as:

OpenID validated

Serendipity Administration Suite

CDATA Zone

Logged in as Anonymous (Administrator)

[Frontpage](#)

[Personal Settings](#)

Welcome back, Rob Richards

[Return to Weblog](#)

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](#)

Further Links

[Serendipity Homepage](#)

[Serendipity Documentation](#)

[Official Blog](#)

[Forums](#)

[Spartacus](#)

[Bookmarklet](#)

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

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

$redirect_url = $auth_request->redirectURL($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);

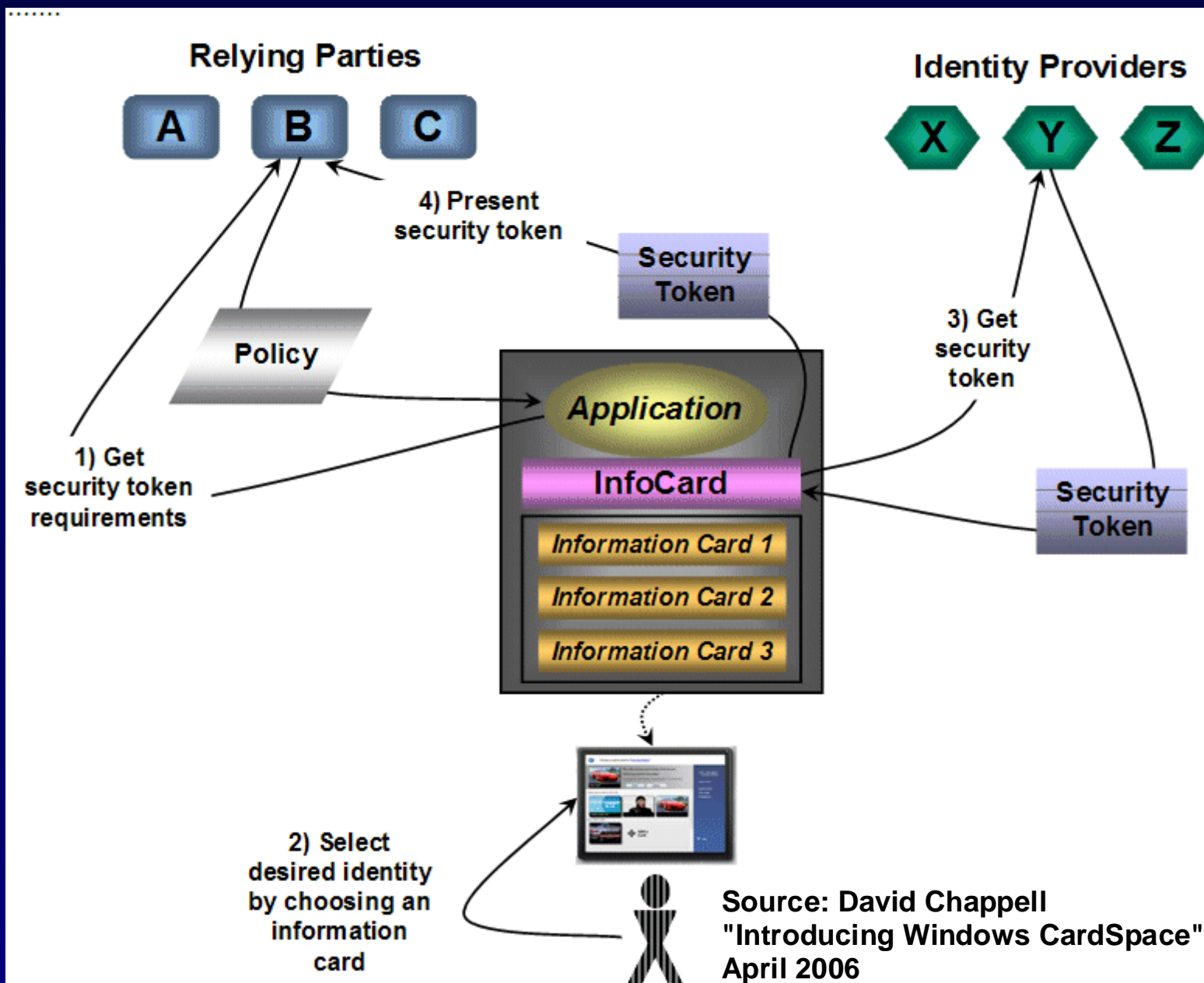
$response = $consumer->complete($_GET);

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');
}
```

Information Cards (Infocards)

- CardSpace != Information Cards
 - Information Cards are not Microsoft specific
 - Variety of selectors for various OSs (xmlldap / Higgins)
- Identities represented as cards
 - Self Asserted
 - Managed
- 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.

ENTER

Logon using Infocards by clicking on the above image

Logon using your OpenID

OpenID:

Username

Password

Save information

[Back to Weblog](#)

Site Information

The screenshot shows a Windows CardSpace dialog box titled "Do you want to send a card to this site?". The dialog is divided into several sections. At the top, there is a toggle switch and the question "Do you want to send a card to this site?". Below this, a paragraph instructs the user to review site information and privacy statements. A yellow warning box contains a message: "This site does not meet Windows CardSpace requirements for a bank or major Internet business. To learn more, click Why is this important?". The "Site information" section lists the URL "www.cdatazone.org" and notes that the organization name and location are not verified. It also includes a link to "View privacy statement" and a warning that cards sent to the site may be sent to designated agents. The "Site information verified by:" section shows "UTN-USERFirst-Hardware". On the right side, a "Tasks" panel lists links for "View certificate details", "View privacy statement", "Disable Windows CardSpace", "Why is this important?", and "Help". At the bottom, there are two buttons: "Yes, choose a card to send" and "No, return to the site".

Windows CardSpace

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.

Warning: 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](#)

[Yes, choose a card to send](#)

[No, return to the site](#)

Tasks

[View certificate details](#)

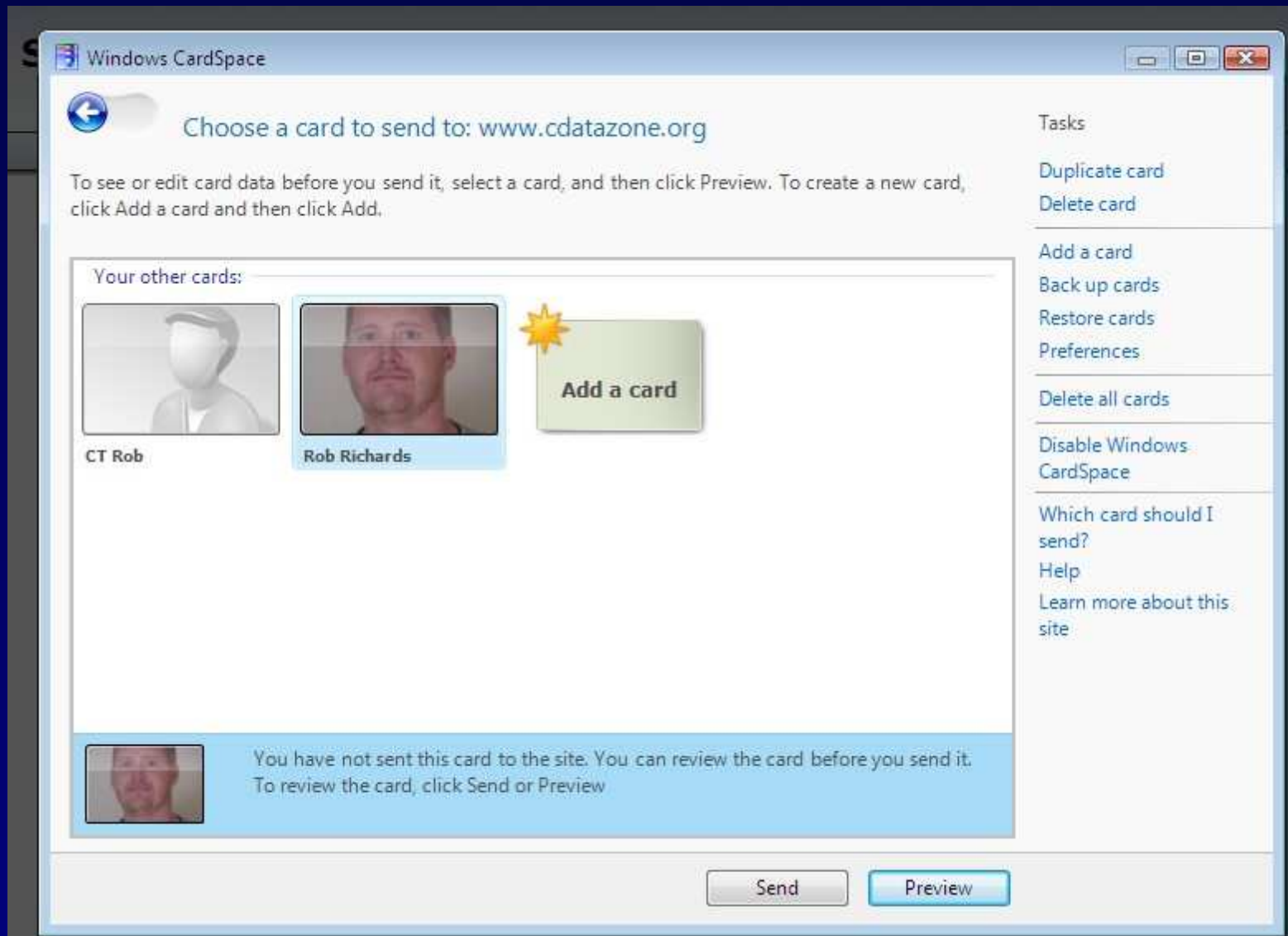
[View privacy statement](#)

[Disable Windows CardSpace](#)

[Why is this important?](#)

[Help](#)

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

Warning: 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

Personal Card

Rob Richards

Send Edit

Information Card Validated

Serendipity Administration Suite

CDATA Zone

Logged in as robr1 richardsr1 (Administrator)

[Frontpage](#)

[Return to Weblog](#)

[Personal Settings](#)

Welcome back, robr1 richardsr1

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](#)

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 />
    </PARAM>
  </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'];
}
```

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 | <input type="text" value="Rob Richards"/> |
| Your e-mail address Your personal e-mail address | <input type="text" value="r-richards@ctindustries.net"/> |
| Language Select the language for your blog | <input type="text" value="English"/> |
| Use WYSIWYG editor Do you want to use the WYSIWYG editor? (Works on IE5+, partially in Mozilla 1.3+) | <input type="radio"/> Yes <input checked="" type="radio"/> 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. | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Send comment announcements? Do you want to receive emails when comments are posted to your entries? | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Send trackback announcements? Do you want to receive emails when trackbacks are posted to your entries? | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| <input type="checkbox"/> Default settings for new entries | |
| Comments & trackbacks to this entry requires moderation | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Allow comments to this entry | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| New Entry | <input type="text" value="Draft"/> |
| Show toolbar within media selector popup? | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| <div style="text-align: right;"><input type="button" value="Save"/></div> | |
| Current OpenID associated with this account | |
| OpenID URL: <input type="text" value="=Rob.Richards"/> | <input type="button" value="Edit"/> |

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 | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Group Memberships <div style="border: 1px solid #ccc; padding: 5px;"><p>Administrator ▲</p><p>Chief editor</p><p>Standard editor ▼</p></div> | |
| 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. | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Rights: Publishing entries? Is this user allowed to publish entries? | <input type="radio"/> Yes <input checked="" type="radio"/> 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. | <input checked="" type="radio"/> Yes <input type="radio"/> 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. | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| <input type="button" value="Save"/> | |

Questions?

Who am I?

The Age of the Digital Identity

Rob Richards

5/23/2007

www.cdatazone.org

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