Enabling Digital Identity

David Recordon
Innovator for Advanced Products & Research

DC PHP Conference 2006
Overview

+ Web 2.0
+ Identity...so what?
+ Identity 2.0
+ “Competitive” Overview
+ Digging into OpenID
+ Example Relying Party
What is Web 2.0?
Web 2.0

+ Users in Control
+ Data Sharing
+ Social Networking
+ Collaboration Tools
+ Lightweight Business Models
+ Perpetual Beta
+ The Long Tail
+ Application Platform
What is Identity?

“The collective aspect of the set of characteristics by which a thing is definitively recognizable or known.”

-Dictionary.com
Offline Identity

- David Recordon
- 09/04/1986
- Oregon
- Black Hair and Brown Eyes
- Central Pocket Loop
- Size 12 Shoes
- Drive a Subaru
- Work for VeriSign
- Star Alliance Gold
- AOW Scuba Diver
- CPR / AED / First Aid Trained
- etc
Online Identity

+ David Recordon
+ Daveman692
+ recordond
+ http://daveman692.livejournal.com
+ recordond@gmail.com
+ drecordon@verisign.com
+ david@simplemachines.org
+ david@boardnation.com
Identity…why do we need technology?

+ Accuracy
  ▪ Biometrics
+ Convenience
  ▪ Verification
+ Security
  ▪ Authorization
+ Privacy
  ▪ Limited Disclosure
+ Portability
  ▪ HSPD-12
Identity 1.0 on the Web

+ Proprietary
  - AOL
  - Yahoo!
  - Microsoft
  - Google
+ Segregated
+ Federation
+ Little User Choice
+ Many Usernames
+ Few Passwords
Identity 2.0

+ Internet Scale
  ▪ Decentralized

+ Privacy Protecting
  ▪ Disclose only as much as is needed

+ Easy to Adopt
  ▪ Add to your application in a weekend

+ Community Driven
  ▪ Open Source development
and that means…

+ User Choice
  ▪ Who hosts their identity

+ Collaboration
  ▪ Moving between contexts

+ The Long Tail
  ▪ Identity is more than just “Military Grade”

+ Emerging Business Models

+ Supporting the Web as an Application Framework
Forums and Conferences

+ ACM
+ Apache Software Foundation
+ BarCamp
+ Digital ID World conference
+ Eclipse Foundation
+ ID World conference
+ Identity Commons
+ Internet Identity Workshop series
+ IETF
+ Liberty Alliance
+ O’Reilly’s OSCON, eTech, FooCamp, and Web 2.0 conferences
+ OASIS
+ OSIS
+ W3C
“Competitive” Situation

Identity in 2006

URL-based (grassroots, open source, blogging)

WS-* based (Microsoft Vista)

Liberty-based (Liberty Alliance companies)

Identifier-based paradigm

OSI S Agreement “historic development” (ZDNet)

Card-based paradigm

Invisible to the user

Red Hat
Novell
VeriSign
Sun
IBM
Microsoft
Cordance
Higgins
Shibboleth
Sxip
NetMesh
Oracle

NetMesh
VeriSign
Identity 2.0 Technologies

+ Higgins Identity Framework
  - Not a protocol
  - FOSS via Eclipse Foundation

+ SAML
  - Liberty Alliance
  - Fewer Open Source implementations

+ Microsoft CardSpace
  - Developed by Microsoft and will ship in Windows Vista
  - Part of .Net

+ OpenID
  - Protocol framework (Discovery, Authentication, Data Exchange, …)
  - Decentralized
  - FOSS via Apache Software Foundation
CardSpace Overview

+ Simple user abstraction for digital identity
  ▪ For managing collections of claims
  ▪ For managing keys for sign-in and other uses

+ Grounded in real-world metaphor of physical cards
  ▪ Government ID card, driver’s license, credit card, membership card, etc...
  ▪ Self-issued cards signed by user
  ▪ Managed cards signed by external authority

+ Shipping in Windows Vista
  ▪ Runs on Windows Vista, XP, and Server 2003

+ Implemented as protected subsystem
Implementation Properties

+ Cards represent references to identity providers
  - Cards have:
    - Address of identity provider
    - Names of claims
    - Required credential
  - Not claim values

+ CardSpace data not visible to applications
  - Stored in files encrypted under system key
  - User interface runs on separate desktop

+ Simple self-issue identity provider
  - Stores name, address, email, telephone, age, gender
  - No high value information
  - User must opt-in
WS-* Metasystem Architecture

ID Provider
- Kerberos
  - Security Token Service

Relying Party
- SAML
  - WS-SecurityPolicy
- Subject
  - Identity Selector

ID Provider
- x509
  - Security Token Service

Relying Party
- ...
  - WS-SecurityPolicy

WS-Trust, WS-MetadataExchange
Microsoft CardSpace
What was OpenID 1.1?

+ An identity authentication system
+ A protocol
  - gratis, libre
+ Not a service or company
  - Not Passport
  - Not TypeKey
+ Survives if companies turn evil or go out of business
Design Goals For Auth

+ Low barrier to entry
  - Works with static HTML pages
  - Decentralized
  - Understandable identity (a URI)
    - No new namespace
    - No public keys (key revocation, etc...)
  - No SSL required
  - No browser plugins

+ Most simple protocol possible
  - Other needs layered atop
What is OpenID 2.0?

+ An identity system framework
+ Multiple protocols
  - Discovery (Yadis)
  - Authentication
    - URIs
  - Messaging (DTP)
  - Attribute Exchange
+ Still not a service or company
+ Open community development within the Apache Heraldry Podling
+ General consensus based spec process on specs@openid.net
Design Goals For OpenID 2.0

+ Identity 2.0
  - User Centric
  - Internet Scale
  - Privacy Protecting
  - Community Driven

+ Framework of interoperable specifications
  - Handful of twenty page specs versus one one-hundred-fifty page spec

+ Extensible

+ Interoperable
OpenID Framework
How's Auth Work?

+ Proves “who” you are
  - You own a URL or an i-name
  - One-time assertions w/ digital signature
  - See openid.net for specs, libraries, etc

+ Not a trust system…yet
  - Spammers can/will/have setup OpenID Authentication servers
  - Better than the state of email today
  - Trust/reputation providers can easily build atop the OpenID framework
Why Should You Care?

+ Developers
  - Less code since don’t need
    - Complex registration pages
    - Security questions
    - Password reset emails
  - FOSS libraries already exist

+ Product Managers
  - Low barrier to entry
  - Promote your brand (http://username.YourSite.com)

+ Users
  - One password
    - Or other credentials
  - Simple
  - Globally recognizable identity
Highlighted Deployment

+ Relying Parties
  - LiveJournal and MoveableType
  - Technorati
  - Zooomr
  - ClaimID
  - Opinity
  - WikiTravel

+ Patches / Active Development
  - WordPress
  - MoinMoin
  - Drupal
  - phpBB
  - MediaWiki
  - Joomla
  - Zope / Plone

+ Identity Providers
  - pip.VerisignLabs.com
  - MyOpenID.com
  - GetOpenID.net
Developer Bounty Program

+ Implement OpenID 2.0 support
+ Are distributed as part of a project’s core
+ Project distributed under an OSI-approved license
+ Serve at least 200,000 internet users or 5,000 downloads per month
+ Require no more than one configuration setting for an administrator to enable support
+ Include the OpenID logo in the signon form
+ http://IWantMyOpenID.org
Code!

+ Free libraries on OpenID.net
  - PHP
  - Perl
  - Python
  - C#
  - Ruby
  - Java
  - C++

+ Similar API across languages
+ Hides low level details of the protocol
OpenID Login Flow *(demo without internet)*

**So, what is all of this OpenID Stuff?**

OpenID is a simple single sign-on mechanism that allows you to login at multiple websites with the same identity.

**What does that all mean for me?**

Simply that once you create an OpenID, you can use it on other websites -- not just Zoomr.

**Already on Zoomr and using Google or Meetro?**

Never fear! You can merge your Zoomr account to OpenID.
So, what is all of this OpenID Stuff?

OpenID is a simple single sign-on mechanism that allows you to login at multiple websites with the same identity.

What does that all mean for me?

Simply that once you create an OpenID, you can use it on other websites -- not just Zoomrr.

Already on Zoomrr and using Google or Metro?

Never fear! You can merge your Zoomrr account to OpenID.
Discovery on http://recordond.pip.verisignlabs.com

<Service>
  <Type>http://openid.net/signon/1.1</Type>
  <Type>http://openid.net/sreg/1.0</Type>
  <URI>https://pip.verisignlabs.com/server</URI>
</Service>

*Simple XML which describes the authoritative provider for my URL*
Trust Request

Authorization Request

This site: http://zoomer.com is asking to verify your ID: http://recordond.pip.verisignlabs.com/

- Allow just this once
- Allow forever
- Allow until: 2006 October 19

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

- Select a profile

Save this Trust Profile as: [ ]

Allow | Deny
Trust Request

Authorization Request

This site: http://zoomr.com/ is asking to verify your ID: http://recordonpiperverisignlabs.com/

- Allow just this once
- Allow forever
- Allow until 2006 [ ] October [ ] 26 [ ]

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) [ ]

- Nickname* [ ] David
- Personal Email* [ ] recordon@gmail.com
- Full Name* [ ] David Benjamin Recordon

Save this Trust Profile as: [ ] Zoomr

Allow  Deny
The Zooomr Beta Test Program

Finalize your Zooomr Account

This is the last step of the Zooomr Sign-up process and the start of your Zooomr experience.

What do we need from you? Just for you to verify your first & last name, email address, and also for you to choose a display name -- Yup, it's as simple as that. So let's get to it!

1. Your Name

   First Name: David
   Last Name: Recordon

2. Your Email

   recordon_d@gmail.com

3. Your Display Name

   David

   OKAY LET'S DO THIS THING
WelcomeMat

Hey, David!

You last logged in on Thu 08 Jun 2006 07:36:14 AM PDT

What would you like to do?

» Upload photos
» View your photos page
» View your profile page

Everyone's Photos

From ~J
From ericshan777
From ericshan777
From ericshan777
From Bingi
Dress Shirt as a Website

The button that comes with the shirt is like the login mechanism for that site.

The hole in the cuff provides user choice in where their Identity is managed.
Extending the Metaphor

Identity 1.0

- Google Accounts
- Microsoft LiveID
- Yahoo BBauth

Identity 2.0

OpenID
<body>
  <h1>PHP OpenID Authentication Example</h1>
  <p>This example consumer uses the <a href="http://www.openidenabled.com/openid/libraries/php/">PHP
    OpenID</a> library. It just verifies that the URL that you enter is your identity URL.</p>
  <?php if (isset($msg)) { print "<div class="alert">$msg</div>"; } ?>
  <?php if (isset($error)) { print "<div class="error">$error</div>"; } ?>
  <?php if (isset($success)) { print "<div class="success">$success</div>"; } ?>

  <div id="verify-form">
    <form method="get" action="try_auth.php">
      Identity URL:
      <input type="hidden" name="action" value="verify" />
      <input type="text" name="openid_url" value="" />
      <input type="submit" value="Verify" />
    </form>
  </div>
</body>
$openid = $_GET['openid_url'];
$process_url = sprintf("http://%s:%s%s/finish_auth.php", 
$_SERVER['SERVER_NAME'], $_SERVER['SERVER_PORT'], 
dirname($_SERVER['PHP_SELF']));

$trust_root = sprintf("http://%s:%s", 
$_SERVER['SERVER_NAME'], $_SERVER['SERVER_PORT'], 
dirname($_SERVER['PHP_SELF']));

// Begin the OpenID authentication process.
$auth_request = $consumer->begin($openid);

if (!$auth_request) {
    $error = "Authentication error."
    include 'index.php';
    exit(0);
}

$auth_request->addExtensionArg('sreg', 'optional', 'email');
$redirect_url = $auth_request->redirectURL($trust_root, $process_url);

header("Location: ". $redirect_url);
PHP Relying Party Example (finish_auth.php)

```php
$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;
    $esc_identity = htmlspecialchars($openid, ENT_QUOTES);
    $success = sprintf('You have successfully verified 
        '<a href="%s">%s</a> as your identity.',
        $esc_identity, $esc_identity);

    $sreg = $response->extensionResponse('sreg');

    if (!$sreg['email']) {
        $success .= " You also returned '".$sreg['email']."' as your email.";
    }
}

include 'index.php';
```
Questions?

David Recordon
drecordon@verisign.com

http://openid.net/
general@openid.net

December 4-6 in Mountain View CA
InternetIdentityWorkshop.net

Thanks to Kaliya Hamlin, Johannes Ernst, and Mike Jones for letting me use some of their slides