Drupal.org OpenID Proposal

Why OpenID?

OpenID is a user-centric identity system. It is a completely open, free protocol designed for online identity management. With current support and backing from Microsoft, Sun Microsystems, AOL, Verisign, Sixapart, SXIP and several others, OpenID is rapidly gaining momentum as the identity system for the web.

Because it is a free protocol - vendor and language independent - it is a logical choice for adoption. There are no fees to incur for usage, and it can be easily incorporated into Drupal's Drupal implementations, but is not limited to them. Other systems and properties can use single, integrated identity as well by implementing the open protocol.

OpenID has also been vetted for security concerns and has a broader community actively addressing potential issues with the protocol from a design and security perspective. This makes it a far more appealing option for wide scale adoption than anything "home grown".

For more information:
http://openid.net/what/
http://planet.openid.net/

Implementation

For the Drupal.org implementation there are several primary design objectives:

- Provide single sign-on for users across all sites.
- Make registering for new sub-sites a "single click" experience.
- Simplify the authentication process - simplicity is key for usability.
- Give users an easy way to switch between their sites.
- Allow for profile information sharing and updating across the sites.

The high-level plan would be to introduce a Drupal OpenID server to centrally store and manage user identities and offer these features across the entire network.

Key Feature: "Drupal OP"

In OpenID terms, the server that stores the user's identity data (in the simplest case, their username and password) is referred to as the "OpenID Provider" (OP). The initial piece in the implementation would be to establish an OP for Drupal where all user data will be stored and maintained (i.e http://id.drupal.org/).

Notes:
- The OP should run SSL for authentication

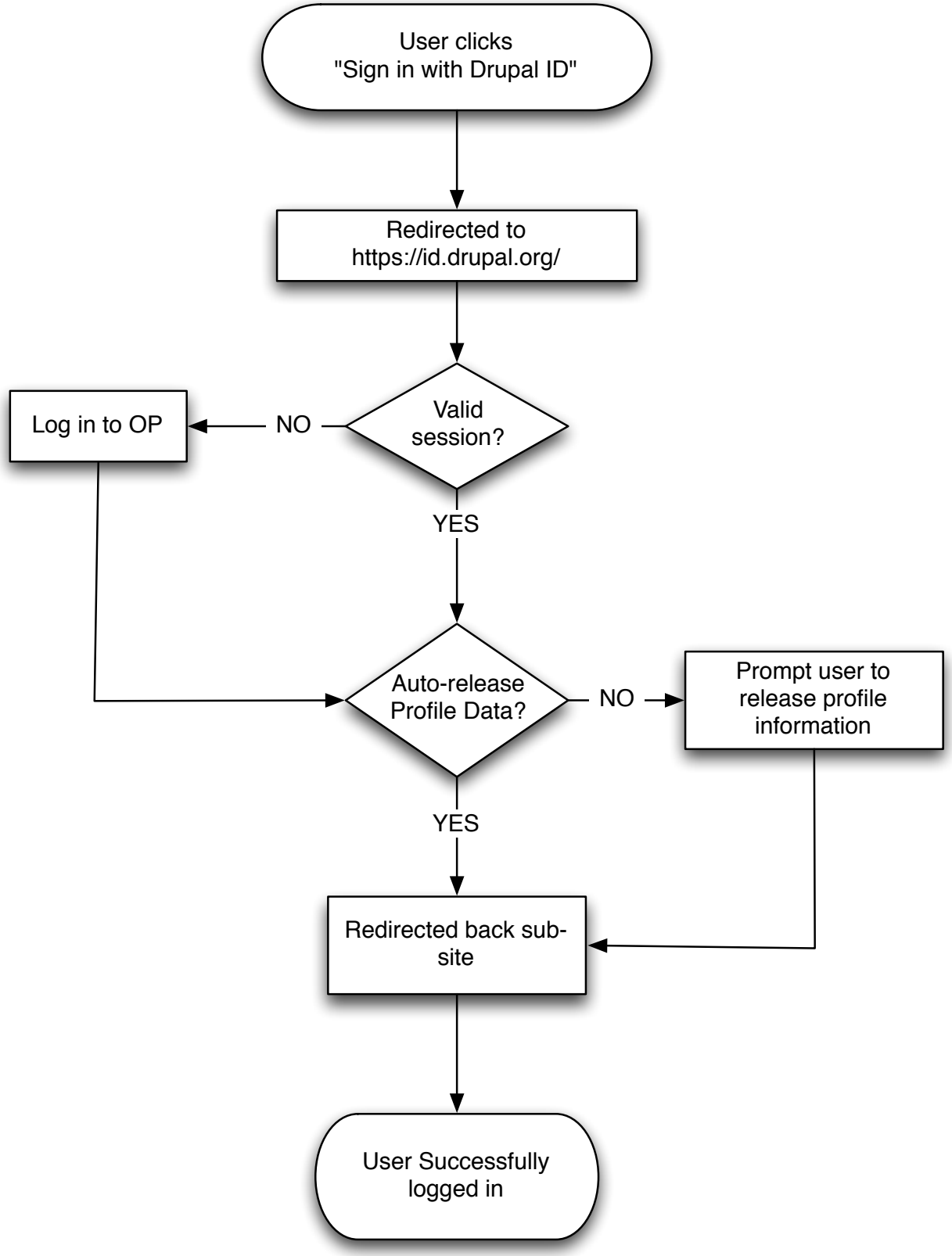
- The OP can be completely decoupled from the rest of the infrastructure (for scalability).
- The design for the OP should be “generic” from a design perspective, but offers a chance for promotions, notices, etc if so desired.

Key Feature: “Drupal ID”

With one of the key points being simplicity and usability, the introduction of a new identity system must be seamless. OpenID uses URLs as identifiers (i.e. http://walkah.myopenid.com/). while this has several benefits, and is in fact essential to the operation of OpenID, “URLs as usernames” can be confusing for users. The recent release of OpenID 2.0 (http://openid.net/2007/12/05/openid-2_0-final-ly/) offers a new feature known as “directed identity” to help alleviate this issue. Directed identity (or “anonymous login”) simplifies the user experience by no longer requiring the user to even know their OpenID URL with the provider, they merely need to know the URL of their provider (i.e. myopenid.com).

This implementation can take this concept a step further and introduce a “Drupal ID” which can simplify the process by constraining authentication against the Drupal OP. Thus, by clicking a single ‘log in now’ button, the user would be redirected to the Drupal OP where their session and/or credentials would be verified and they would be redirected back to the site and logged in - in a single click.

Below is a diagram of the intended user flow:



For more information on “directed identity” see:

http://pezra.barelyenough.org/blog/2007/12/openid-20s-killer-feature/

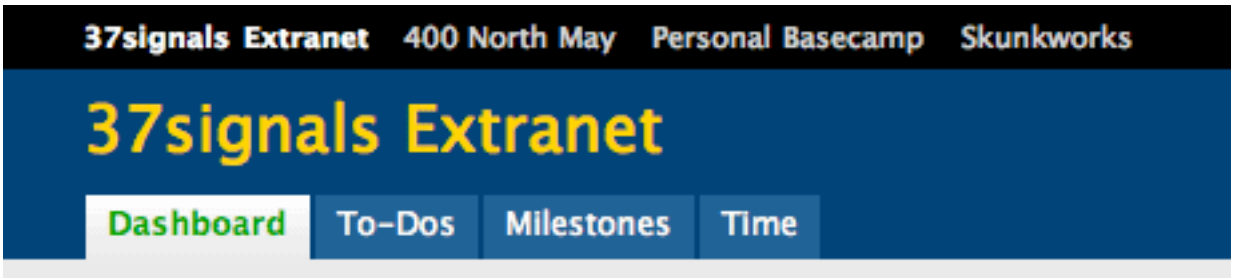
http://blogs.gnome.org/jamesh/2007/10/23/openid-20/

Key Feature: "Drupal Bar"

One excellent feature made possible by a digital identity system is the ability properly recognize accounts across sites. This would allow an interface for users to easily switch between the Drupal sites where they actively participate.

37signals, creators of Basecamp, have implemented a similar feature based on OpenID. For more information see:

http://www.37signals.com/svn/posts/479-basecamp-gets-openid-and-open-bar



Key Feature: Profile updates

In addition to too many user names and passwords, users are often repeatedly faced with lengthy registration screens asking for the same personal information again and again. In the interest of growing adoption, limiting the time investment required for registration and login is important. Keeping this same user data in sync across several sites is also a challenge.

OpenID 2.0 was released along with an extension known as "Attribute eXchange" (AX) which provides a standardized protocol for fetching and storing profile data from and to the OP. By implementing AX for Drupal, we can allow users to update their profile on each subsite centrally. Attribute Exchange is also fully extensible, so the profile data can include any fields including ones that may, perhaps, be unique to Drupal sites.

Existing modules

openid.module : currently in core.

openid_provider.module : currently in an alpha - basic authentication is working. Required for Drupal OP (http://id.drupal.org/)

openid_ax.module : Was a Google SoC project this summer - needs some work still on the RP (client) side.

Custom modules

openid_bar : this module would provide the bar on top of all sites, and allow switching between *.drupal sites and simple SSO features.

openid_login : simple module that provides a URL (openid/login) that will initiate the auth process (i.e. the endpoint that openid_bar links will point to). *This module is already in progress, but not yet submitted.*