OpenID

David Recordon
drecordon@verisign.com

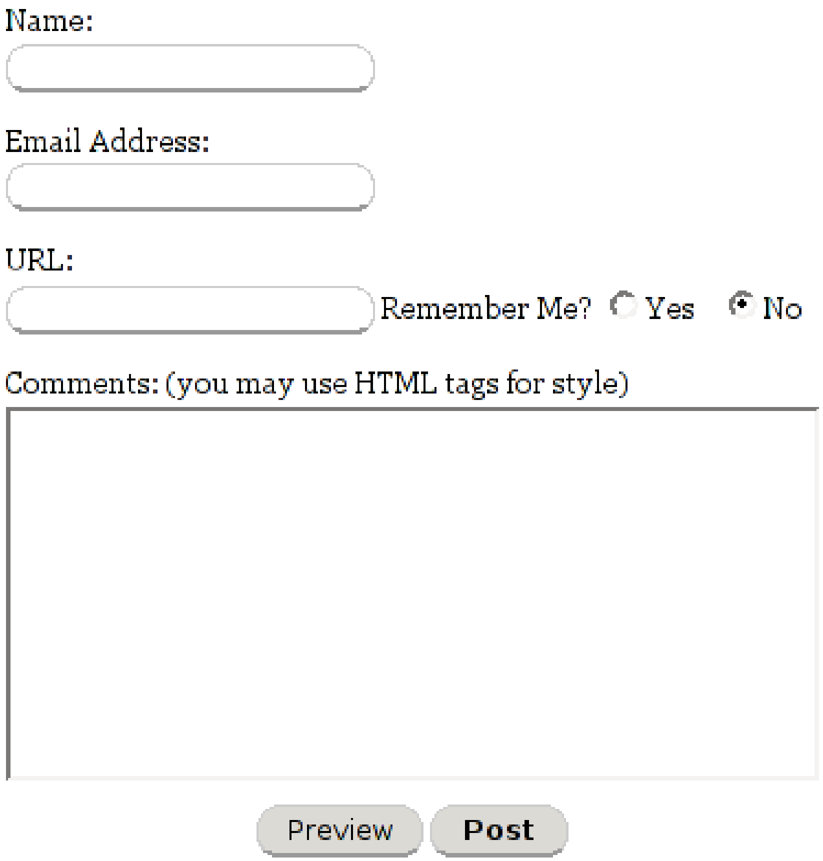
What was OpenID 1.1?

- 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

Why Was It Developed?

- No authentication was way too common
- Comment spam
- Auth interop
  - LiveJournal
  - TypePad
  - Movable Type
  - WordPress
  - DeadJournal

lame



Name:

Email Address:

URL:

Remember Me? ○ Yes ● No

Comments: (you may use HTML tags for style)

Design Goals For Auth

- Low barrier to entry
  - Works with static HTML pages
  - Decentralized
  - Understandable identity (a URL)
    - 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
    - URLs
    - i-names
  - Messaging (DTP)
  - Profile Exchange (Many layered atop DTP)
- Still not a service or company
- Open community development within the Apache Heraldry Podling

How's Auth Work?

- Proves “who” you are
  - You own a URL / i-name
  - One-time assertions w/ digital signature
  - See **openid.net** for specs, libraries, etc
- Not a trust system
  - Spammers can/will/have setup OpenID authentication servers
  - Trust and reputation require authentication
- Trust networks can build atop the framework

Why URLs as identifier?

- Already the convention
  - 03:47, 3 August 2006 Xaosflux (Talk | contribs) m (Protected Elephant: on colbert again)
  - Click to see more about Xaosflux
- Users don't understand public keys
- Users don't understand namespaces
- Users associate email addresses with spam
- Users do understand URLs
  - 10+ years of billboards and TV commercials
- You can click them
  - Tangible

Role of the OpenID IdP

- Provide a URL/i-name which the user “owns”
- Provide a way for users to authenticate to itself
  - Auth mechanism not in OpenID spec
  - Common method is password over SSL
  - OTP, Biometrics, etc
    - By using strong auth in one place, all relying parties benefit
- Asserts to a relying party that the person using the browser owns the given identifier

Deployment

- Relying Parties
  - Six Apart’s blogging properties
  - Zooomr
  - ClaimID
  - Opinity
  - WikiTravel
- Patches / Active Development
  - MediaWiki
  - WordPress
  - MoinMoin
  - Drupal
  - phpBB
- Identity Providers
  - *VeriSign Lab’s Personal Identity Provider*
  - *MyOpenID.com*
  - *GetOpenID.net*

Bounty Program

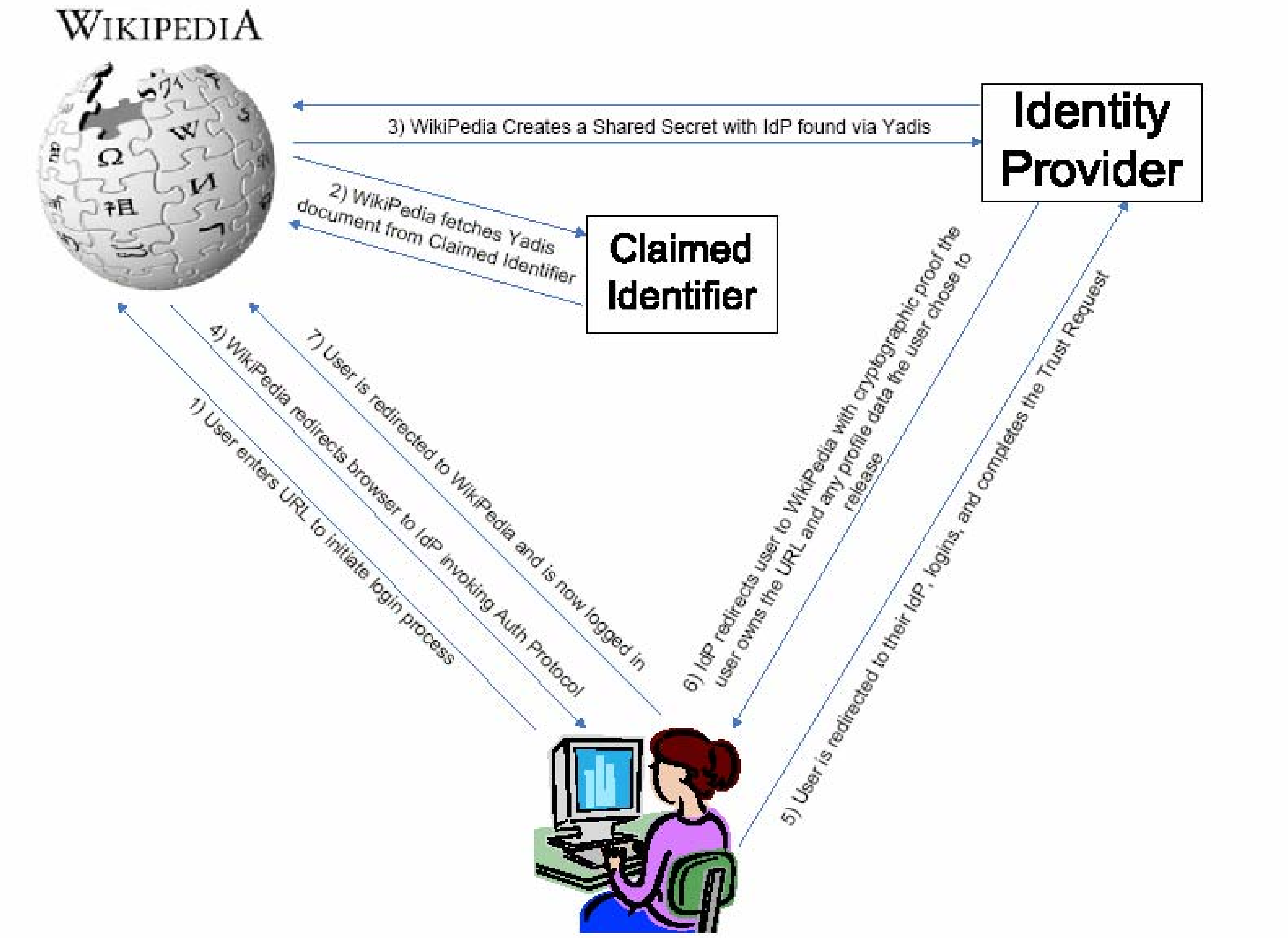
- Ten $5,000 bounties
- Implement OpenID 2.0 support
- We want to see MediaWiki collecting a bounty!
- Here to help make this happen!

IWantMyOpenID.org

Code!

- Free libraries on openid.net (moving into Apache)
  - PHP
  - Perl
  - Python
  - C#
  - Ruby
  - Java
  - C++
- Similar API across languages
- Hides low level details of the protocol

Basic Protocol Flow



1) User enters URL to initiate login process

2) WikiPedia fetches Yadis document from Claimed Identifier

3) WikiPedia Creates a Shared Secret with IdP found via Yadis

4) WikiPedia redirects browser to IdP invoking Auth Protocol

5) User is redirected to their IdP, logins, and completes the Trust Request

6) IdP redirects user to WikiPedia with cryptographic proof the user owns the URL and any profile data the user chose to release

7) User is redirected to WikiPedia and is now logged in

Questions?

www.OpenID.net
www.OpenIDEnabled.com
yadis@lists.danga.com
heraldry-dev@incubator.apache.org

David Recordon (drecordon@verisign.com)