

An Experimental Active Client for OpenID

Mike Jones, Ariel Gordon, Oren Melzer, Chuck Reeves
(with help from several of you!)

November 2, 2009

Goals

- Evolving OpenID together to address known issues
 - To improve both its usability and security
 - While providing a smooth migration path
- Prototype meant to stimulate discussion about possible futures for OpenID
 - Intended as starting point – not the destination

What are we going to show you?

- A prototype identity selector for OpenID
- That remembers your identities for you
 - Instead of the site having to guess what they are
 - One manner of mitigating phishing attacks
- That contacts the OP on your behalf
 - Instead of the RP doing so directly
 - Another means of mitigating phishing attacks

What changes and doesn't change?

- OPs are unchanged
- RPs augmented to pass OpenID authentication parameters to the identity selector
 - Using Information Card object tag
 - Scriptable detection via capabilities
- I chose my OpenID in the selector
 - Rather than at the RP
- Selector contacts the selected OP
 - Rather than the RP

What steps occur?

- RP detects selector and invokes it
- RP passes request parameters to selector via an object tag
- Selector enables user to choose an OP
- Selector performs discovery on the OP
- Selector vets OP against user's saved list and OP white list
 - Asking for user confirmation if OP not known to be trusted
- Selector constructs OpenID Authentication Request on behalf of the RP and redirects to OP
- Selector closes
- OP interaction unchanged
- OP redirects back to RP, without selector involvement
 - Sending an unsolicited positive assertion


The OP White List Issue

- Our prototype postulates a white list of “known trustworthy” OPs
 - No user trust decision in UX when interacting with white-listed OPs
 - In this prototype, Yahoo, Google, MyOpenID
 - Versus explicit user trust decision when interacting with unknown OPs
 - Such as self-issued.info
- This is one basis for phishing protection
 - (Another is the selector remembering my OpenIDs!)
- We need to be discussing the white list question

Demonstration

- (Live demonstration, as follows)
- Start with an empty selector
- Associate account at Plaxo with Yahoo OpenID
- Sign out and sign back in
- Go to interscope.com or citysearch.com or pibb.com (RPX sites) and use Google OpenID
- Go to test-id.org and use self-issued.info
 - Highlight trust dialog for provider not on white list

Issues that Arose while Prototyping

- Spec for OPs to advertize their friendly name and logo
 - Such as “Yahoo!” and 
 - Could be displayed by selectors, RPs
 - In discussion with Allen Tom, Luke Shepard, Dave Recordon, about possibly adding this to the UX extension
- OP-specific parameters such as association handles (and more)
- Unsolicited positive assertions
- Determining identity equivalence
 - Compare post-discovery endpoints?
- Use of i-frames and knowing who the RP really is

We'd like to thank!

- Joseph Smarr of Plaxo for RP work
- Carl Howells, Larry Drebes, and Brian Kissel of JanRain for RP work
- Andrew Arnott of DotNetOpenAuth for RP work
- Allen Tom, Luke Shepard, and Dave Recordon for ideas about OPs publishing their names and logos
- Eric Sachs, Ben Laurie, Allen Tom, Raj Mata, Andrew Nash, Don Thibeau, Drummond Reed, Paul Trevithick, Mary Ruddy, John Bradley, Axel Nennker, Craig Burton, Arun Nanda, Kim Cameron, and many of the rest of you for your thoughts and encouragement

Possible Futures

- Interacting with OP in window other than RP's browser window
- Interacting with OP in a security context not controlled by the RP
- Enable OpenID to be used at higher levels of assurance
- Provide an attribute selection user experience
- Solving existing post/redirect problem from OP
- Non-browser applications
- Roaming your identities and use at kiosks
- Smart cards and/or other second factor devices
- Tokens with proof-of-possession
- Minimal disclosure tokens
- Mobile phones, other OSs, browsers, etc.
- *Plus I'm sure many other things you're already thinking of!*
- ***It's up to all of us together to decide which of these to pursue and why***

For More Information

- We'll all be here at the Summit and IIW
 - Mike Jones <http://self-issued.info/> and mbj@microsoft.com
 - Ariel Gordon Ariel.Gordon@microsoft.com
 - Oren Melzer oremel@microsoft.com
 - Chuck Reeves creeves@microsoft.com
- Plus speak with those we thanked as well
- ***Let's talk!***

Backup Slides

Object Tag Syntax Example

```
<object type="application/x-informationCard" id="infoCardObjectTag">
  <param name="protocol" value="http://specs.openid.net/auth/2.0" />
  <param name="tokenType" value="http://specs.openid.net/auth/2.0" />
  <param name="issuer" value="Google.com/accounts/o8/id Yahoo.com myOpenID.com" />
  <param name="issuerExclusive" value="false" />
  <param name="OpenIDAuthParameters" value=
"openid.ns:http://specs.openid.net/auth/2.0
openid.return_to:http://www.plaxo.com/openid?actionType=complete
openid.realm:http://*.plaxo.com/
openid.ns.sreg:http://openid.net/extensions/sreg/1.1
openid.sreg.required:email
openid.sreg.optional:fullname,nickname,dob,gender,postcode,country,language,timezone
openid.sreg.policy_url:http://www.plaxo.com/about/privacy_policy
" />
</object>
```

Prototype OpenID Selector Diagram

