By Prabath Siriwardena, WSO2
Why OpenID???
Too many passwords
Duplicated profiles everywhere
Oops..!!! My favorite user name... GONE...!!!
Why OpenID???
OpenID solves them all...!!!
Single user name/password
Single user profile
Claim your URL as your user name
What is OpenID???
OpenID is a URL or an XRI
http://prabath.myopenid.com
http://www.prabathsririwardena.com
=prabath
Who gives me an OpenID???
OpenID Providers [OP] issue OpenIDs and maintain user profiles
JOIN THE CLUB

SIGN UP FOR YOUR OPENID
Get your own OpenID and start using the last username and password you'll ever need. Signing up with myOpenID gets you:
- Secure control of your digital identity
- Easy sign-in on enabled sites
- Account activity reports
- Ability to manage multiple personas for different sites, and a whole lot more!

LEARN SOME MORE
- Learn more about OpenID
- Check out the blog
- OpenID website directory
- Read our blog
- Services for website operators

GET MYOPENID FOR YOUR DOMAIN
Do you own a domain? With myOpenID For Domains, you can issue OpenIDs to your employees, family, or organization with your own URL. It's easy to set up and manage your users.
Start now!

BECOME A MYOPENID AFFILIATE
Do you run an OpenID-enabled web site? With the myOpenID Affiliate Program, you can help users get OpenIDs quickly and easily with a customized sign-up page. Become an affiliate now!
Yahoo! meets OpenID
Log in to websites with your Yahoo! account

Why OpenID?
Are you tired of creating a new account on every website you use? Do you avoid new websites because they come with yet another username and password? Do you paste stickies with password hints all over your computer monitor?

OpenID is an open technology standard that solves all of these problems. The OpenID technology will allow you to use your Yahoo! account to sign in to hundreds of websites! And this list is growing every day...

Once you enable your Yahoo! account for OpenID access, you can simply tell any OpenID enabled website that you are a Yahoo! user. You will be sent to Yahoo! to verify your Yahoo! ID and password and then signed in to the website. Its that easy!

Still not convinced?
Take our handy-dandy OpenID tour to learn more or visit the OpenID homepage

Why Yahoo!?
You already enjoy a bunch of great services with your Yahoo! account. The Yahoo! OpenID (http://openid.yahoo.com) service lets you take your account beyond Yahoo!. Plus, the free Yahoo! Sign-In Seal will help protect you from password theft, also known as phishing.
What’s a blog?

- Publish thoughts
- Get feedback
- Post photos
- Go mobile

Create a blog in 3 easy steps:
1. Create an account
2. Name your blog
3. Choose a template

A blog is your easy-to-use web site, where you can quickly post thoughts, interact with people, and more. All for FREE.

CREATE YOUR BLOG NOW
Who accepts my OpenID???
Any web site can accept OpenIDs for sign in
13,196 unique web sites seen by myOpenID.com to accept OpenID, by May 2008
Leave your comment

You can use some HTML tags, such as <b>, <i>, <a>

WORD VERIFICATION
Type the characters you see in the picture above.

Choose an identity
- Google/Blogger
- OpenID

OpenID

- Name/URL
- Anonymous

PUBLISH YOUR COMMENT  PREVIEW
Log in with a SourceForge account

Username: 
Password: 

Log in

Forgot your username/password?

Need an account on SourceForge.net?
Create Account

Log in with an OpenID

http://

Via these Identity Providers:

Log in

Problems logging in with OpenID?

OpenID eliminates the need for multiple usernames across different websites, simplifying your online experience.
Learn more - Get an OpenID
OpenID

What is OpenID?
LiveJournal.com supports the OpenID distributed identity system, letting you bring your LiveJournal.com identity to other sites, and letting non-LiveJournal.com users bring their identity here. After all, not everybody uses the same websites, but you should still be able to play together.

Using your OpenID here.
If you're not a member of LiveJournal.com but want to leave authenticated comments and let people add you as their friend, trust your comments, etc., then you can login either in the form below, or from any comment entry form. Once you're logged in, you'll also be able to read friends-only posts that LiveJournal.com users have indicated you're allowed to read.
With OpenID we simply maintain a single user name/password pair.....
OpenID

What is OpenID?

LiveJournal.com supports the OpenID distributed identity system, letting you bring your LiveJournal.com identity to other sites, and letting non-LiveJournal.com users bring their identity here. After all, not everybody uses the same websites, but you should still be able to play together.

Using your OpenID here.

If you're not a member of LiveJournal.com but want to leave authenticated comments and let people add you as their friend, trust your comments, etc., then you can login either in the form below, or from any comment entry form. Once you're logged in, you'll also be able to read friends-only posts that LiveJournal.com users have indicated you're allowed to read.

Your OpenID URL: [http://prabath.myopenid.com](http://prabath.myopenid.com)
For example: melody.smehblog.com (if your host supports OpenID)

Username: http://prabath.myopenid.com/
Password: **************

Stay signed in

Sign in with an Information Card
Sign in with an SSL certificate
I cannot access my account
myOpenID
SECURE OPENID PROVIDER

OPENID VERIFICATION

A site identifying itself as

http://www.livejournal.com/

has asked us for confirmation that

http://prabath.myopenid.com/

is your identity URL.

Allow Forever  Allow Once  Deny

What exactly do these buttons do?
Welcome back to LiveJournal!

You're logged in as prabath.myopenid.com. Go have fun. Here are some suggestions...

- **Update your Journal**
  Did you know you can now easily add a photo?

- **Read your friends page**
  See the latest updates to your friends' journals.

**Change log-in options**

- Remember me
  Log in automatically on this computer

- Bind cookie to IP address
  Learn more about this option

[Save] [Log out]
Log in with a SourceForge account

Username: [Field]
Password: [Field]
Log in

Forgot your username/password?

Need an account on SourceForge.net?
Create Account

Log in with OpenID

http://prabath.myopenid.com

Via these Identity Providers:

Log in

Problems logging in with OpenID?

OpenID eliminates the need for multiple usernames across different websites, simplifying your online experience.
Learn more - Get an OpenID
OPENID VERIFICATION

A site identifying itself as

https://sourceforge.net

has asked us for confirmation that

http://prabath.myopenid.com/
is your identity URL.

The site also asked for additional information. You can find their policy about the data it collected on this page

This is the persona we're going to send to sourceforge.net:

---

**Prabath**

<table>
<thead>
<tr>
<th><strong>Full Name</strong></th>
<th>Prabath Siriwardena</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nickname</strong></td>
<td>Prabath</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td>Male</td>
</tr>
<tr>
<td><strong>E-mail</strong></td>
<td><a href="mailto:prabathsiriwardena@yahoo.com">prabathsiriwardena@yahoo.com</a></td>
</tr>
<tr>
<td><strong>Postal Code</strong></td>
<td>0094</td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td>Sri Lanka</td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>English</td>
</tr>
<tr>
<td><strong>Time Zone</strong></td>
<td>Asia/Colombo</td>
</tr>
</tbody>
</table>

---

Edit this persona
Delete this persona

---

Allow Forever  Allow Once  Deny

What exactly do these buttons do?
OpenID verified! Please associate your identity
Check our site doc for more information on OpenID.

Existing SourceForge Account

Username: 
Password: 
Log in

New SourceForge Account

Create SF Account

Registration fields will be pre-populated from your Identity Provider, if possible.
With OpenID we authenticate once at the OP and sign in to rest of the OpenID relying party web sites....
That is Single Sign On
OpenID facilitates decentralized single sign on
What is “decentralized”???
NOT - centralized
No central server – or authority
Remember Microsoft Passport: That is centralized – there is a central server
With OpenID any body can be an OpenID Provider
Once again – What is OpenID???
OpenID is a URL or an XRI which facilitates decentralized single sign on
I enter my OpenID at the RP – how come the RP knows who is my OpenID Provider???
The process of getting to know about the corresponding OpenID Provider from a given OpenID is known as ‘Discovery’.
Just type your OpenID on the browser
http://prabath.myopenid.com
HTTP://PRABATH.MYOPENID.COM/

This is the OpenID Identity Page for http://prabath.myopenid.com/.

(This user has not chosen to share any information on their Identity Page.)

Learn more about OpenID or Sign up for a free OpenID now
BUT... that is not what we wanted – just ‘view source’
<link rel="openid.server" href="http://www.myopenid.com/server" />

<link rel="openid2.provider" href="http://www.myopenid.com/server" />
Why there are two tags pointing to the same OpenID Provider URL???
openid.server → OpenID 1.1
openid2.provider → OpenID 2.0
This form of discovery is known as ‘HTML Based Discovery’
What is ‘HTML Based Discovery’ ???
Under HTML-Based discovery, an HTML document MUST be available at the URL of the Claimed Identifier and RP retrieves the document with an HTTP GET.
Within the HEAD element of the document a LINK element MUST be included with attributes "rel" set to "openid2.provider" and "href" set to an OP Endpoint URL
That is what we noticed earlier.
Any other forms of Discovery other than HTML-Based??
XRDS-Based discovery
[will be covered later...]
My OpenID is http://prabath.myopenid.com. BUT…
I do NOT own that URL… it’s under the control of myOpenID – not mine
This type of Identifiers are known as OP-Local Identifiers
What is an OP-Local Identifier???
An alternate Identifier for an end user that is local to a particular OP and thus not necessarily under the end user's control.
Can I use my own URL as my OpenID???
Of course you can – and that is known as the “Claimed Identifier”
What is a Claimed Identifier ??
An Identifier that the end user claims to own
I own a URL – but I am not an OpenID Provider – can I still use my URL as my OpenID???
YES – you can
Say, the URL I own or my claimed identifier is
http://www.prabathsiriwardena.com
I also have an account with myOpenID and my OP Local identifier is http://prabath.myopenid.com
I can use my claimed identifier as my OpenID – by delegating the OpenID Provider functionality to myOpenID
<link href='http://www.myopenid.com/server' rel='openid2.provider openid.server'/>

<link href='http://prabath.myopenid.com/' rel='openid2.local_id openid.delegate'/>
With this approach we never limited to a single OpenID Provider.
If we lost faith on the OpenID Provider we can move to another – but, still keeping the original OpenID
I have maintain a single user name/password pair for all my relying party web sites... will OpenID make a difference for me ???
Of course in two ways.
Even you have the same user name/password for all the relying party web sites – still you need to maintain your profile data in different places.
Also, what if you lose your password? You will lose access to all your relying party web sites.
But, isn’t it the case under OpenID as well. If you lose your password to the OpenID Provider you lose access to all relying party web sites depend on the OpenID.
No – it’s not.
With OpenID – if it is a claimed identifier - you never lose your password.
I own a URL – and I use it as my OpenID Claimed Identifier. What if I could not renew my domain name ???

Now somebody else owns it.....
You own an OpenID until you can claim the ownership of the URL behind it.
You lose the ownership of the URL – you lose your OpenID as well
BUT...
XRI based OpenIDs solve this issue
You never lose the ownership of the i-number behind an XRI – so, you never lose your XRI based OpenID
What is an XRI ??? What is an i-number ???
eXtensible Resource Identifier
A Global Unique Identifier
[just as Domain Names]
URL, Phone Number, Email are concrete identifiers
XRI is an *abstract* identifier
Concrete identifiers represent actual resources in a network
Abstract identifiers are used to find concrete identifiers
XRI is an abstract identifier which can be mapped to concrete identifiers [e.g.: URL, email]
XRI syntax defines two forms of XRIs
i-names and i-numbers
i-names are human-friendly identifiers
=prabath
i-numbers are typically machine-friendly identifiers
i-names, are intended to be re-assignable identifiers just like domain names
i-numbers are intended to be persistent
If your OpenID is your i-number – you never lose it
How an OpenID RP discovers an XRI based OpenID ???
XRDS based discovery
[which we did not cover earlier]
HTML based discovery returns an HTML page [discussed earlier]
XRDS based discovery returns an XRDS document
eXtensible Resource Descriptor Sequence
<?xml version="1.0" encoding="UTF-8"?>
<xrd:XRDS xmlns:xrd="xri://$xrd" xmlns="xri://$xrd*($v*2.0)"
xmlns:openid="http://openid.net/xmlns/1.0">

<XRD ref="xri://=example">

<!-- service section -->

<!-- XRI resolution service -->
<Service>
</Service>

<!-- OpenID 2.0 login service -->
<Service priority="10">
</Service>

<!-- OpenID 1.1 login service -->
<Service priority="20">
</Service>

</XRD>

XRDS based discovery – NOT just for XRI based OpenIDs
XRDS based discovery – can also be used for URL based OpenID discovery
If an URL – XRDS based discovery will use Yadis protocol for discovery
If an XRI – XRDS based discovery will use XRI resolution
A given XRDS document can define multiple services
<!-- XRI resolution service -->
<Service>
  <ProviderID>xri://=!F83.62B1.44F.2813</ProviderID>
  <Type>xri://$res*auth*($v*2.0)</Type>

  <MediaType>application/xrds+xml</MediaType>
  <URI priority="10">http://resolve.example.com</URI>
  <URI priority="15">http://resolve2.example.com</URI>
  <URI>https://resolve.example.com</URI>
</Service>
<!-- OpenID 2.0 login service -->
<Service priority="10">
  <Type>http://specs.openid.net/auth/2.0/sign on</Type>  <URI>http://www.myopenid.com/server</URI>
  <LocalID>http://example.myopenid.com/</LocalID>
</Service>
<!-- OpenID 1.0 login service -->
<Service priority="20">
  <Type>http://openid.net/server/1.0</Type>
  <URI>http://www.livejournal.com/openid/server.bml</URI>
  <openid:Delegate>
    http://www.livejournal.com/users/example/
  </openid:Delegate>
</Service>
What attributes can my RP get from the OpenID Provider???
Under OpenID; attribute flow is defined under two main extensions
OpenID Simple Attribute Registration [SReg]
OpenID Attribute Exchange [Ax]
OpenID Simple Registration allows for very light-weight profile exchange
It is designed to pass nine commonly requested pieces of information when an End User goes to register a new account with a web service
RP can request the required/optional attributes from the OP with the Authentication request
nickname, email, fullname, dob, gender, postcode, country, language, timezone
OpenID Attribute Exchange is for exchanging identity information between endpoints
Not limited for a predefined set of attributes
With AX: not just fetch attributes from the OP – but also can store attributes at the OP
Ax defines messages for retrieval [fetch] and storage [store] of identity information
“fetch” : retrieves attribute information from an OpenID Provider
“store” : saves or updates attribute information on the OpenID Provider
Both messages are originated from the RP as an indirect message
Under Ax each attribute is identified by an URI
There are two popular schemas which define subject identifiers to attributes
http://schema.openid.net
&
http://www.axschema.org
Under http://schema.openid.net the attribute “email” is identified as “http://schema.openid.net/contact/email”
Under http://www.axschema.org the attribute “email” is identified as “http://axschema.org/contact/email”
myOpenID.com supports http://schema.openid.net
RP can request the required/optional attributes from the OP with the Authentication request
[Demo]: Attribute flow with WSO2 OpenID Demo RP
https://is.test.wso2.org/javarp
Why Yahoo does NOT trust my RP – while all the other OpenID Providers ???
“This web site has not confirmed it’s identity with Yahoo! and might be fraudulent. Do not share any personal information with this website unless you certain it is legitimate.”
Yahoo supports OpenID 2 and it does OpenID Relying Party Discovery
With OpenID RP Discovery, RPs should publish their valid return_to URLs in an XRDS document.
To get rid of Yahoo! warning the RP needs to publish this XRDS at the return_to URL.
RP discovery also allows any software agent to discover sites that support OpenID.
Am I correct to say that OpenID is a phishing heaven ???
Not really...!!!
OpenID does NOT address the problem of phishing
To the same extent any of the web sites are exposed to phishing – OpenID too exposed to phishing.
There are many approaches taken individually by OpenID Providers to protect their users against phishing.
Yahoo Sign In Seal
Why OpenID?

- No need to create a new account on websites that support the OpenID technology. No more forgotten passwords when you try new websites.
- Just tell websites that you are a Yahoo! user, sign in to Yahoo!, and you will be on your way.
- Hundreds of websites support the OpenID technology. And this list is growing every day.
SeatBelt plugin for Firefox
Settings

General Settings | OpenID Providers | OpenID Delegation

Installed Providers

- VeriSign Personal Identity Provider  1.0.00
  Manage your online identity without compromising your privacy.

- myOpenID  2007.05.07.01
  The free, secure OpenID server

Add Provider

https://

[Enable] [Remove] [Add] [OK] [Cancel]
**OpenID**

**What is OpenID?**

LiveJournal.com supports the OpenID distributed identity system, letting you bring your LiveJournal.com identity to other sites, and letting non-LiveJournal.com users bring their identity here. After all, not everybody uses the same websites, but you should still be able to play together.

**Using your OpenID here.**

If you're not a member of LiveJournal.com but want to leave authenticated comments, links, or use their file storage system, you can login either in the form below, or from any comment entry form. Once you're logged in, you'll also be allowed to read.

**Using your OpenID on another site.**

If another site says it supports OpenID and you want to use your LiveJournal.com OpenID, you can login to it. For example, just enter melody.livejournal.com, or whatever your address is. After you do so, you'll be able to log into that site using your LiveJournal identity. You can either trust them once, or forever. You can change your OpenID settings and trust at any time.

---

**BETA:**

Our OpenID consumer support is very new. That is, external users logging in with their identity here will find some rough edges while we work on smoothing it all out.

Our server support is relatively complete, though.
Information Card based login


SIGN IN

Username

Password

Stay signed in

- Sign in with an Information Card
- Sign in with an SSL certificate
- I cannot access my account

Sign In  Cancel
Please sign in to authenticate to https://is.test.wso2.org/javarp/openidloggedin.jsp?login=true as https://is.test.wso2.org/user/prabath.

Login with your OpenID password

- Password [password input field]
- Remember me on this computer [checkbox]
- Login [button]

OR

Login with your self-issued Information Card

You can only login with a personal information card that you have already registered. If you have not registered a personal information card please first login with your username and password and register a card.
Login to OpenID Provider with a bookmark
You need to sign in

You need to log in to idproxy.net to complete this process.

You should use a bookmark or type in the address to do this. This page does not contain any links, to protect you from phishing.
Can OpenID RPs request OpenID Providers to authenticate users in a phishing resistant manner ??
YES – they can
OpenID Provider Authentication Policy Extension [PAPE]
[Demo]: PAPE demo with WSO2 OpenID
Demo RP
https://is.test.wso2.org/javarp
How strong OpenID against Man-in-the-Middle attacks ??
This requires explaining what ‘OpenID Association’ is...
A given OpenID relying party can be either Dumb or Smart
Smart relying parties maintain a shared secret key with the OpenID Provider – while Dumb relying parties maintain no state.
We talk about ‘OpenID Associations’ only for ‘Smart’ RPs
‘OpenID Association’ takes place just after ‘Discovery’ and establishes ‘Shared Secret Key” between OpenID Relying Party and the OpenID Provider
OpenID uses Diffie-Hellman key-exchange to establish the shared secret
Diffie-Hellman key-exchange allows two parties to jointly establish a shared secret key over an insecure communications channel
‘Shared Secret Key’ is used to sign subsequent messages exchanged in between OpenID Relying Party and the OpenID Provider
‘OpenID Association’ is a direct communication between OpenID Provider and the RP
Under OpenID, HTTP POST is used for all Direct Communications
Still we have NOT answered the original question...
How strong OpenID against Man-in-the-Middle attacks ???
Associations prevent tampering of signed fields by a man in the middle except during discovery, association sessions
BUT... if DNS resolution or the transport layer is compromised; signatures on messages are not adequate
How do we handle Man-in-the-Middle attacks for discovery and association sessions ??
One solution is to build a white-list of OpenID Providers and maintain their public key certificates at the RP end.
RP performs an XRDS-based discovery and OP returns a digitally signed XRDS document
RP verifies the signature
During an ‘Association’ OP can sign the field ‘assoc_handle’ by it’s private key and RP verifies it once received
How good OpenID at handling DoS attacks??
Within the protocol there are places where a rogue RP could launch a denial of service attack against an OP.
This can be done by the RP repeatedly requesting associations, authentication, or verification of a signature
There is nothing in OpenID protocol messages that allows the OP to quickly check that it is a genuine request.
White-listing RPs is not a good solution
OpenID Providers can easily use generic IP based rate-limiting and banning techniques to help combat these sorts of attacks and black list RPs.
It’s hard to remember a whole URL as an OpenID ??
"Do you remember my OpenID URI? It was either dog.pets.com, =dog, snowclone/dog, ..."
ID Selector

Sign In

You must sign in to create an ID selector for your website.

Click to Sign In

Sign in with OpenID using

- Yahoo!
- Vidooop
- OpenID By Card
- Blogger
- Other OpenID

Get an OpenID

- myOpenID
- Clickpass
- claimID
- Livejournal
- Technorati

- Verisign
- Flickr
- AOL

Sign in
ID Selector

Sign In

You must sign in to create an ID selector for your website.

http://prabath.myopenid.com/

Sign in with OpenID using

- Yahoo!
- Vidoop
- OpenID By Card
- Blogger
- Other OpenID

myOpenID

Get an OpenID

- myOpenID
- Clickpass
- claimID
- Livejournal

Verisign

Flickr

AOL

Technorati

Help

myOpenID username: prabath
Finally....
The complete OpenID Protocol flow...
The end user initiates authentication (Initiation) by presenting a User-Supplied Identifier to the Relying Party via their User-Agent.
The Relying Party performs discovery (Discovery) on the identifier and establishes the OP Endpoint URL that the end user uses for authentication.
(optional) The Relying Party and the OP establish an association
(Establishing Associations)
The OP uses an association to sign subsequent messages and the Relying Party to verify those messages.
The Relying Party redirects the end user's User-Agent to the OP with an OpenID Authentication request (Requesting Authentication)
End user authenticates to the OP
The OP redirects the end user's User-Agent back to the Relying Party with either an assertion that authentication is approved (Positive Assertions) or a message that authentication failed (Negative Assertions).
The Relying Party verifies (Verifying Assertions) the information received from the OP
Useful Links

6. OpenID mailing list:
   http://openid.net/mailman/listinfo/general
7. AxShema mail group:
   http://groups.google.com/group/axschema
10. WSO2 Identity Solution download page:
    http://wso2.org/projects/solutions/identity
11. WSO2 OpenID Demo OP: https://is.test.wso2.org
12. WSO2 OpenID Demo RP:
    https://is.test.wso2.org/javarp
Next Webinar…. On 17th June

Introducing WSO2 ESB 1.7

Now open for registration...
http://wso2.com/about/news/esb-webinar-june-17/
Questions...

you...!

Thank you...!