



Simon Josefsson <simon@yubico.com>

<http://www.yubico.com/>

What is OpenID?

**Decentralized
Web-based
Reduced-sign-on
System**

What does that mean?

You can *reduce* the number of username/passwords *sign-in's*

[Prevent Password Theft](#)

Sign in to Yahoo!

Yahoo! ID:

Password:

Keep me signed in
for 2 weeks unless I sign out. **New!**
[Uncheck if on a shared computer]

[Forget your ID or password?](#) | [Help](#)

Sign in to Gmail with your

Google Account

Username:

Password:

Remember me on this computer.

[I cannot access my account](#)

**Web sites doesn't need to
maintain a username and
password database**

Decentralized:

**no central authority in charge of
your credentials**

Cross-site persistent user identity (if user wants that)

without OpenID:

User X on site Y \neq User X on site Z

with OpenID:

OpenID X on site Y $==$ OpenID X on site Z

How do I use it?

**You pick a provider
you trust**

**(like you pick an
e-mail provider today)**

**You can change provider
any time you want**

**You can even run the
server yourself**



C#

C++

Java

PHP

Perl

Python

Ruby

***Too many choices, I'm
lazy.***

<http://openid.yahoo.com/>





[**http://openid.aol.com/<screenname>**](http://openid.aol.com/<screenname>)

***Ok, I have an account,
now what?***


**Find sites that
supports OpenID**

(or better, ask the sites you use to support OpenID)

Pibb: Stay in the Loop - Iceweasel

File Edit View History Bookmarks Tools Help

https://pibb.com/



Pibb for all your communications

Pibb combines the best features of instant messenger, chat, email, and bulletin boards.

- Messages are delivered instantly, or can be retrieved later
- New threads are stored and searchable like email or bulletin board
- Start public channels about your favorite subjects
- Use private channels to communicate with groups or your social network
- Send private messages to your friends
- Pibb will notify you when you have new messages

Who is using Pibb?

JanRain, Inc.
Software company using a secure private channel to keep it's employees connected in a fast paced startup environment.

Ron Paul Supporters
Using a public Pibb channel to *mobilize* and get the vote out.

Ma.gnolia
Social bookmarking site *Ma.gnolia* uses Pibb for real time user support and feedback.

Search the pibb channel directory

Done

Free Worldwide Travel Guides - Wikitravel - Iceweasel

File Edit View History Bookmarks Tools Help

http://wikitravel.org/en/Main_Page

Wikitravel navigation

- Main Page
- Project Home
- Today's log
- Recent changes
- Random page
- Help
- Wikitravel Shared
- Wikitravel Extra

feeds

- Travel news and trivia

search

göteborg

Main Page

Wikitravel is a project to create a free, complete, up-to-date, and reliable **worldwide travel guide**. So far we have 17,164 destination guides and other articles written and edited by Wikitravellers from around the globe. Check out the **Help** page to see how you can edit any page **right now**, or the **Project** page for more information about Wikitravel and getting involved.

- Africa
- Asia
- Australasia & Oceania
- Europe
- Middle East
- North America
- South America
- Central America & Caribbean
- Other destinations
- Travel topics & Phrasebooks

Destination of the month

Angkor Archaeological

Off the beaten path

Rietvel Nature Reserve is a small reserve located in the Gauteng Province of South Africa. Despite 272 bird and 530 plant species, not to mention hippos, rhinos, zebras, ostriches and vast numbers of various antelopes, the reserve is generally not very busy and you will often have a bird hide all to yourself. [\(more...\)](#)

ng Kong, a hotel in the Kowloon district, includes a helicopter


r of the title villain in two movies featuring the vampiric Count

Tor Disabled

Zoomr | Share th

File Edit View History Bookmarks Tools Help

http://www.zoomr.com/



Universally the best way to share, search, store, sort and sell your photos online.

Learn More

[View more photos >](#)

Language: English | Español | Deutsch | Italiano | Polski | Português (BR) | Nederlands | Français | 日本語 | 简体中文 | 繁體中文

Discover: [Last Day](#) | [Last Week](#) | [Last Month](#) | [Public Profile](#) | [Search](#)

Help: [Search](#) | [Help](#) | [Contact](#) | [Feedback](#)

Privacy: [About Zoomr](#) | [Privacy Policy](#) | [Terms of Service](#) | [Privacy Policy](#)

Done

Ma.gnolia.com - Find Web Sites & Build Community Online - Iceweasel

File Edit View History Bookmarks Tools Help

http://ma.gnolia.com/

Sign in | Learn More

over, share and discuss the best of the web. Join Us or More.

Digg Explorer v1.1

Marked in Ma.gnolia by krlwll

Find more about digg tool

Discover sites about

Featured Linker

Michael Biven
Michael Biven is the new admin chief

Art
Online art site

Transferring data from scst.srv.grafa.com...

Tor Disabled



WELCOME TO MYOPENID

NEWS

myOpenID now supports Information Cards. With a self-issued Information Card you can sign-in to myOpenID (as well as sign-up and recover your account) without ever having to remember a password.

Information Cards are supported on Windows (XP/Vista), Linux, and Mac OS X. Learn more on [our blog](#). To set up an Information Card for your account, go to your [Authentication Settings](#) page.

NEW TO OPENID?

[Our tutorial](#) will help you get started using your OpenID.

YOUR PERSONAL ICON

YOUR ACCOUNT

YOUR OPENID:
<http://simonj.myopenid.com/>

Home

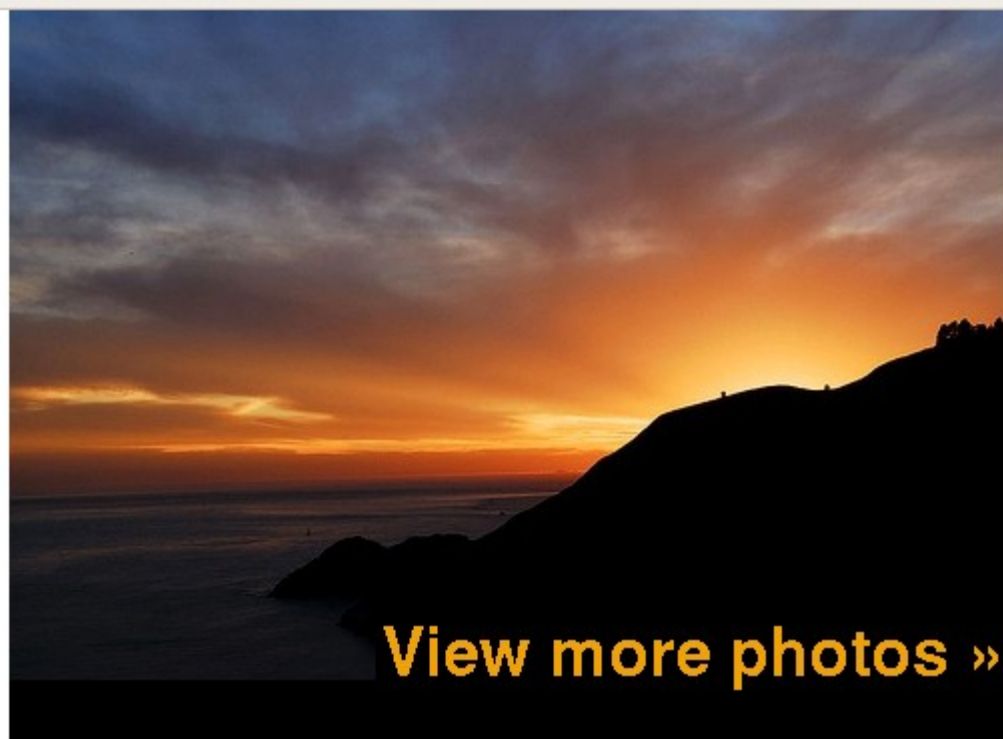
[Registration Personas](#)

[Account Settings](#)

[OpenID Site Directory](#)

[Your Affiliate Sites](#)

[Sign Out](#)



Sign-In ★ Sign-Up

Universally the best way to share, search, store, sort and sell your photos online.

Learn More

Language Select | [English](#) | [Español](#) | [Deutsch](#) | [Italiano](#) | [Polski](#) | [Português](#) | [Português \(BR\)](#) | [Nederlands](#) | [Русский](#) | [日本語](#) | [简体中文](#) | [繁體中文](#)

Discover | [Last Day](#) | [Last Week](#) | [Last Month](#) | [Public Zipline](#) | [Search](#)

Help | [Learn More](#) | [Help Group](#) | [Email Support](#)

Zoomr | [About Zoomr](#) | [Blog](#) | [Zipfox](#) | [Zoomr TV](#) | [Terms Of Service](#) | [Privacy Policy](#)

Copyright © 2006-07 Zoomr Inc. All Rights Reserved.







Sign-In | OpenID What is OpenID?

OpenID Examples:

- VOX:** <http://username.vox.com/>
- myOpenID:** <http://username.myopenid.com/>
- LiveJournal:** <http://username.livejournal.com/>

Language Select | [English](#) | [Español](#) | [Deutsch](#) | [Italiano](#) | [Polski](#) | [Português](#) | [Português \(BR\)](#) | [Nederlands](#) | [Русский](#) | [日本語](#) | [简体中文](#) | [繁體中文](#)

Discover | [Last Day](#) | [Last Week](#) | [Last Month](#) | [Public Zipline](#) | [Search](#)

Help | [Learn More](#) | [Help Group](#) | [EMail Support](#)

Zoomr | [About Zoomr](#) | [Blog](#) | [Zipfox](#) | [Zoomr TV](#) | [Terms Of Service](#) | [Privacy Policy](#)

Copyright © 2006-07 Zoomr Inc. All Rights Reserved.





OPENID VERIFICATION

A site identifying as all sites matching **http://*anything*.zoomr.com/** has asked us for confirmation that **http://simonj.myopenid.com/** is your identity URL.

[What exactly do these buttons do?](#)

YOUR PERSONAL ICON

YOUR ACCOUNT

YOUR OPENID:

<http://simonj.myopenid.com/>

Home

Registration Personas

Account Settings

OpenID Site Directory

Your Affiliate Sites

Sign Out

[Help](#) | [Feedback](#) | [Privacy](#) | Language:
[Not set](#)

[Blog](#) | [About Us](#) | © 2007 [JanRain, Inc.](#)

myOpenID™ and the myOpenID™ website are trademarks of JanRain, Inc.

***I don't want to be
foobar.myopenid.com!***

I'm foobar.com.

Add

```
<link rel="openid.server"  
      href="http://www.myopenid.com/server"/>
```

```
<link rel="openid.delegate"  
      href="http://foobar.myopenid.com/">
```

to <http://foobar.com/> HTML source.



Simon Josefsson Datakonsult

- » [Home](#)
- » [Contact](#)
- » [Consulting](#)

About us

Simon Josefsson Datakonsult (SJD) implement and standardize network security protocols. Our solutions are often used in the wireless and embedded markets. We

Source of: <http://josefsson.org/> - Iceweasel

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
    "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <meta name="generator" content="AsciiDoc 8.2.2" />
    <meta name="description" content="Simon Josefsson Datakonsult" />
    <meta name="keywords" content="network security free software consultant developer programmer standardization" />
    <link rel="stylesheet" href="/xhtml11.css" type="text/css" /><link rel="openid.server" href="http://openid.yubico.com/server.php" />
    <link rel="stylesheet" href="/xhtml11-quirks.css" type="text/css" />
    <link rel="stylesheet" href="/layout1.css" type="text/css" />
    <title>About us</title>
  </head>
  <body>
    <div id="lavout-banner">
```

Line 9, Col 138

» [Projects](#)

We are primarily working with network security and internationalization technologies related to:

- Kerberos,

**Changing provider by
editing two lines of HTML**

**Your OpenID URL
remains the same**

And this is new?



SAML



Higgins



Microsoft

Cardspace



X.509 / eID

***Why chose OpenID
over the rest?***

**“Solve one problem
and do it well”**

**Other standards are
already on-board**

**(alas, eventually, you'll probably
need to support multiple
protocols in the back-end)**

*How does
OpenID work?*

<http://openid.net/developers/specs/>

New! Version 2.0!

1. User enters Identifier at RP

1. User enters Identifier at RP

2. RP locates the OP

- Several mechanisms exists, simplest is to retrieve the URL and look for HTML HEAD link rel nodes

1. User enters Identifier at RP

2. RP locates the OP

- Several mechanisms exists, simplest is to retrieve the URL and look for HTML HEAD link rel nodes

3. RP redirects browser to OP

- HTTP redirect, the new URL contains Diffie-Hellman exchange and parameters for OP

1. User enters Identifier at RP

2. RP locates the OP

- Several mechanisms exists, simplest is to retrieve the URL and look for HTML HEAD link rel nodes

3. RP redirects browser to OP

- HTTP redirect, the new URL contains Diffie-Hellman exchange and parameters for OP

4. OP authenticates user

- The protocol doesn't care how this happens

1. User enters Identifier at RP

2. RP locates the OP

- Several mechanisms exists, simplest is to retrieve the URL and look for HTML HEAD link rel nodes

3. RP redirects browser to OP

- HTTP redirect, the new URL contains Diffie-Hellman exchange and parameters for OP

4. OP authenticates user

- The protocol doesn't care how this happens

5. OP redirect back to RP

- HTTP redirect again, the new URL for RP finishes the DH and provides information

***Can I do more with
OpenID?***

Yes!

“Simple Registration”

**Your OpenID server can send
personal information**

**(after your approval,
of course)**

**Email, nickname,
home address, etc**

**Allows multiple “personas”,
or user profiles**

**You need to trust your OpenID
server to not reveal anything
without your approval**

What's new in OpenID 2.0?

Server-driven identity selection

Old:

type 'simonj.myopenid.com'

New:

type 'myopenid.com'
select identity to use

Assertions without identity

**Prove you are over 18 without
revealing who you are**

Tech improvements

- **HMAC-SHA-256**
- **Uses HTTP POST instead of HTTP GET (to increase maximum size)**
- **Nonce and time stamps**
- **URI Normalization**
- **...**

***Are there security
problems in OpenID?***

**Phishing is a real
security problem**

Solutions?

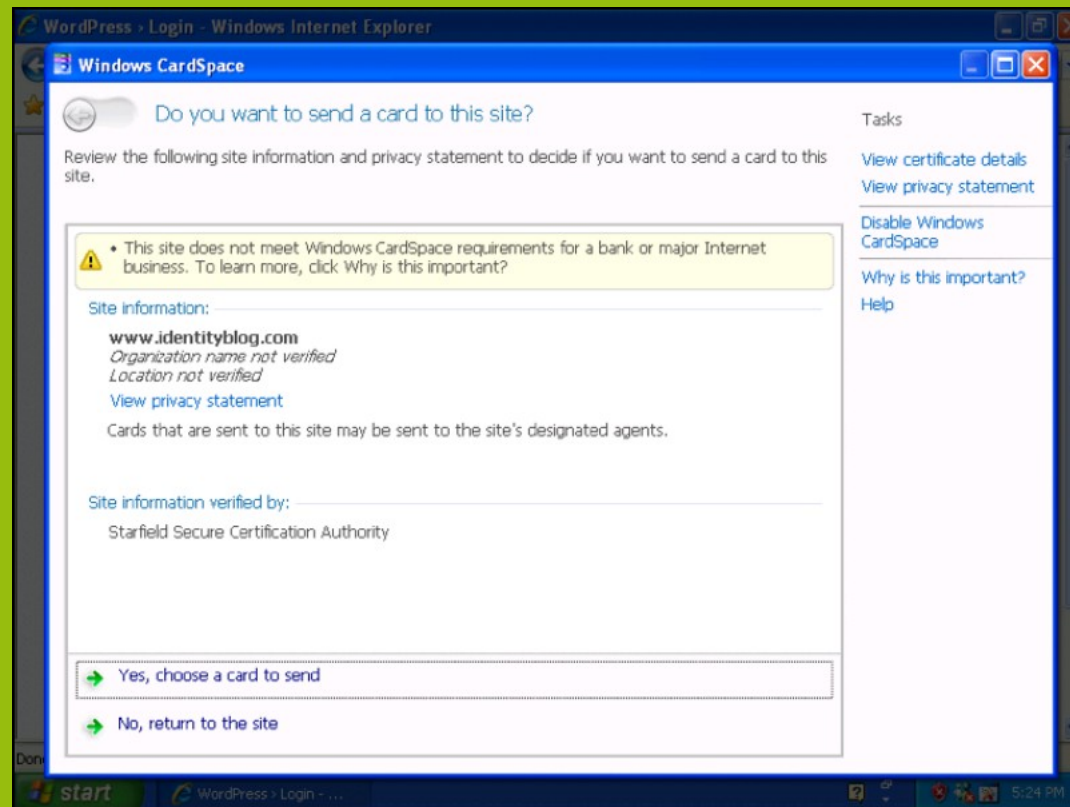
“Never enter passwords in the attackers' control flow”

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.

Microsoft CardSpace



What about flash..?

Better Solutions?

**Protocol changes to OpenID?
(unlikely!)**

Browser integration of OpenID

Just Avoid Passwords!

HTTPS with client- side certificates (complex!)

Hardware authentication devices

yubico

trust the net

Offices in Stockholm and California

Yubico Identity Platform

**OpenID, Java, ASP/.NET/C#, Radius, PAM,
PHP, Perl, Ruby, ...**

Multi-platform USB key without device drivers

Free Worldwide Travel Guides - Wikitravel - Iceweasel

File Edit View History Bookmarks Tools Help

http://wikitravel.org/en/Main_Page

Wikitravel

article discussion view source history

Plunge forward!

Main Page

Login with OpenID - Wikitravel - Iceweasel

File Edit View History Bookmarks Tools Help

http://wikitravel.org/en/Special:OpenIDLogin

Wikitravel

special

Plunge forward!


Login with OpenID

Wikitravel supports the OpenID standard for single signon between Web sites. There are many Public OpenID providers, and you may already have an account with one of them.

Yubico - Trust the net. - Iceweasel

File Edit View History Bookmarks Tools Help

http://openid.yubico.com/server.php?openid.assoc_handle=



Verification succeeded - Wikitravel - Iceweasel

File Edit View History Bookmarks Tools Help

http://wikitravel.org/en/Special:OpenIDFinish?nonce=JaCtI

Wikitravel

special

Plunge forward!

Verification succeeded

Verification succeeded

Return to Main Page.

Confirm login

<http://wikitravel.org/en/Special:OpenIDFinish?nonce=JaCtI>

by pressing

Cancel



***How does the
Yubikey work?***

128-bit AES key

Two factor authentication



Wallet size

No display or batteries

Questions?

Answers?