



Simon Josefsson
simon@yubico.com

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

What is OpenID?

***Decentralized
web-based
authentication system***

What does that mean?

You can reduce the number of username and passwords you need to remember

[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](#)

myspace.com a place for friends

Home | Browse | Search | Profile | Mail | Blog | Favorites | Forum | Groups | Events | Videos | Music | Connect | Statistics

Cool New Videos 46,956 uploaded today!

4-Year-Old Drummer
Top Gun on Ice
Dog vs. Cat
PC Domino

Books | Events | Jobs | Profile Editor
Blogs | Filmmakers | Movies | Ringtones
ChatRooms | Groups | Music | Screens
Comedy | Downloads | Impact | Music Videos
TV On Demand
MySpaceIM

Exclusive NEVER BEFORE SEEN American Idol Video

Member Login

E-Mail:
Password:
 Remember Me

Forgot your password?

Cool New People

valencia | ash | Roddy

YouTube Broadcast Yourself™

Videos | Categories | Channels | Community | Upload Videos

Director Videos

WIA TV Top 10, Nov 14 (USA)
Cotton Suspension... (Baltimore)
GODS2 (Greece)
Tim 12 Days of Chika... (Zambia)

Featured Videos See More Featured Videos

Featured Videos selected by:

Lika Barn Avvika Bläst Del 2
Obernordfästade
From: [Lika Barn](#)
Views: 7,043
★★★★★
More in [Music](#)

Cows With Guns
An epic musical tale about the great cow revolution. A 6 minute claymation by Guro
From: [Capehorn](#)
Views: 26,792
★★★★★

How to rate videos
From: [apple](#)
Comments: 225
★★★★★
2237 ratings

COMP USA 1-800-COMPUSA

New Account (See Benefits)

First Name:
Last Name:
Address:
Password:
Repeat Password:
 Remember my login (What's this?)
 Sign me up for your email list

my login (What's this?)

Outlook Web Access

Connect to outlook.office.com

Outlook Web Access

Outlook Web Access

Outlook Web Access

Cisco E-Mail Manager Administration

Log In

Username:
Password:

CNN.com Member Card | Sign In | Register

SEARCH THE WEB CNN.COM

Home | World | U.S. | Weather | Business | Sports | Analysis | Politics | Law | Tech | Science | Health | Entertainment | Offbeat | Travel | Education | Specials | Autos | Reports

E*TRADE FINANCIAL

WELCOME

- Open An Account
- Employee Stock Plans
- Why Choose E*TRADE?
- Complete Protection Guarantee
- Futures & Applications

INVESTING & TRADING
ACTIVE TRADING
TOOLS & RESEARCH
RETIREMENT PLANNING
ADVICE & EDUCATION
BANKING
MORTGAGES & HOME EQUITY
PRICING & RATES

Customer Service

CALL 1-800-ETRADE-1 (1-800-367-2331)

EMAIL US OR VISIT ONLINE CUSTOMER SERVICE

COMPLETE SAVINGS ACCOUNT

MAX-RATE SAVINGS

5.05% APY No minimums. No account fees.

OVER 6X THE NATIONAL AVERAGE

OPEN AN ACCOUNT

SECURE LOG ON

User ID: Password:
Start In:
Accounts:

Forgot your User ID or Password?

Set Up Online Account Access

HOME LOANS **TRADING** **INVESTING** **BANKING**

NEW LOW MORTGAGE RATES exclusively for qualified E*TRADE customers.

100 NO COMMISSION FREE TRADES \$0.39-\$0.99 stock & options trades for active traders.

\$500 ROLL OVER TO AN E*TRADE IRA Get up to \$500 in your account.

5.05% APY COMPLETE SAVINGS ACCOUNT No minimums. No account fees.

Markets Overview

Enter Symbol(s): GO Symbol Lookup

E*TRADE Bank & Mortgage Rates

MORTGAGE	RATE	APR	See All Rates	
30 Yr. Fixed	no points	6.375%	6.582%	Learn More >
5 Yr. Int Only	no points	6.250%	7.353%	Learn More >
Line of Credit		6.996%	7.259%	Learn More >

DOW 13558.53 +79.85 (0.59%)

QualityFoods.com Quality Food Items Online Grocery Shopping

ALL CATEGORIES: [Grocery](#) | [Produce](#) | [Deli](#) | [Bakery](#) | [Dairy](#) | [Frozen](#) | [Meat](#)

Welcome to Quality Foods

Welcome to our NEW online grocery shopping website! We've made it easier than ever for Vancouver Island residents to shop online!

Already Registered? Click here to login!
If you have already registered to shop online, simply enter your username and password on the following page. Click here.

Need a username/password? Register Online!
If this is your first visit inside our online store, click here to proceed to our online registration email.

How does it work?
For answers to the most common online shopping questions, click here to visit our Frequently Asked Questions area.

PayPal Sign Up | Log In | Help

Welcome | Send Money | Request Money | Merchant Tools | Auction Tools

Member Log In Secure Log In

Registered? Not Registered?

Email Address: [forgot your email address?](#)

Password: [forgot your password?](#)

New here? [Sign up](#) | [Create Account](#) | [Take a Tour](#)

[About](#) | [Accounts](#) | [Fees](#) | [Privacy](#) | [Security Center](#) | [User Agreement](#) | [Developers](#) | [Referrals](#) | [Stats](#) | [Help Desk](#)

an eBay Company

Copyright © 1999-2006 PayPal. All rights reserved.
[Information about FDIC pass-through insurance](#)

FT.com FINANCIAL TIMES

Lunch with the FT
Gore Vidal talks politics and pleasure over oysters and sole
Plus: Chechnya, adultery and kickboxing geishas

Saturday May 19 2007
All times are London time

SEARCH GO QUOTES GO

Home Europe

SUBSCRIBE

Sign up now or Take a Tour

Username:
Password:
 Remember me

**You don't need to maintain
a username and password
database for your web site**

How do I use it?

**You pick a provider
you trust**

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

WordPress.com » Get a Free Blog Here - Iceweasel

Express yourself. Start a blog.
See our free features »

1,932,247 BLOGS WITH 44,707 NEW POSTS TODAY.

214 - The Blonde Map of Europe
[Image] Q: How do you get a blonde out of a tree? A: Wave
According to this map -- and if you really believe that blondes have less brains -- a nasty fall like that is more likely to happen in the c

Sign Up Now!

OpenID - Iceweasel

LiveJOURNAL

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

Our server support is relatively complete, though.

Personal Identity Provider (PIP) - Sign In - Iceweasel

VeriSign Labs Personal Identity Provider Beta

Take Control of Your Identity...
Manage your online identity without compromising your privacy with PIP, the free Personal Identity Provider from VeriSign

Get Started Now >

myOpenID

JOIN THE CLUB

SIGN UP FOR YOUR OPENID

LEARN SOME MORE

SIGN IN TO YOUR ACCOUNT

Welcome to MyOpenID - Iceweasel

myOpenID

YOUR PERSONAL ICON

GOT ONE? GOOD.

SIGN UP FOR YOUR OPENID

LEARN SOME MORE

SIGN IN TO YOUR ACCOUNT

Yubico - Trust the net. - Iceweasel

yubico trust the net

Confirm login to
<http://www.livejournal.com/>
by pressing button on Yubico key

Cancel

FSFE OpenID Server - Iceweasel

http://black.fsfeurope.org/

FSFE OpenID Server

Welcome!

This is the OpenID server of the Fellowship of FSFE.

claimID.com - Manage your online identity - Iceweasel

claimID

Welcome to claimID.

claimID Login:

Secure Login

You might also wish to:

- Create a new account
- Recover your password
- Log in with your claimID
- Log in with your OpenID

**You can even run the
server yourself**



C#

C++

Java

PHP

Perl

Python

Ruby

<http://wiki.openid.net/Libraries>

Too many choices, I'm lazy.



33k employees

YAHOO!

username



idproxy.net

Click below to get started:

YAHOO! Sign In

[Home](#) - [About this site](#)



LIVE JOURNAL™

Zoom

magnolia

claimID



10m users



65m users

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



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](#)

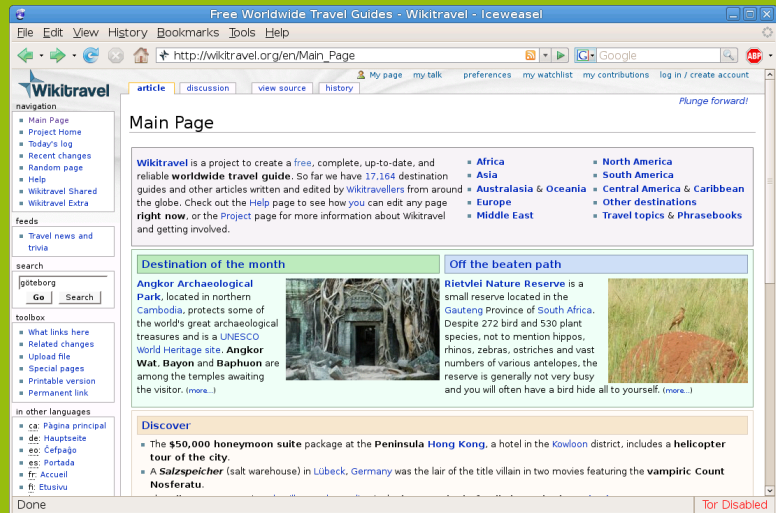
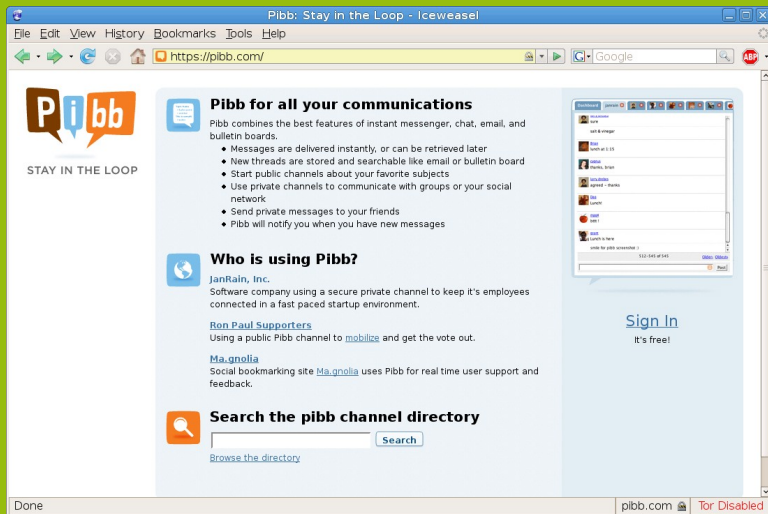
[OpenID Site Directory](#)

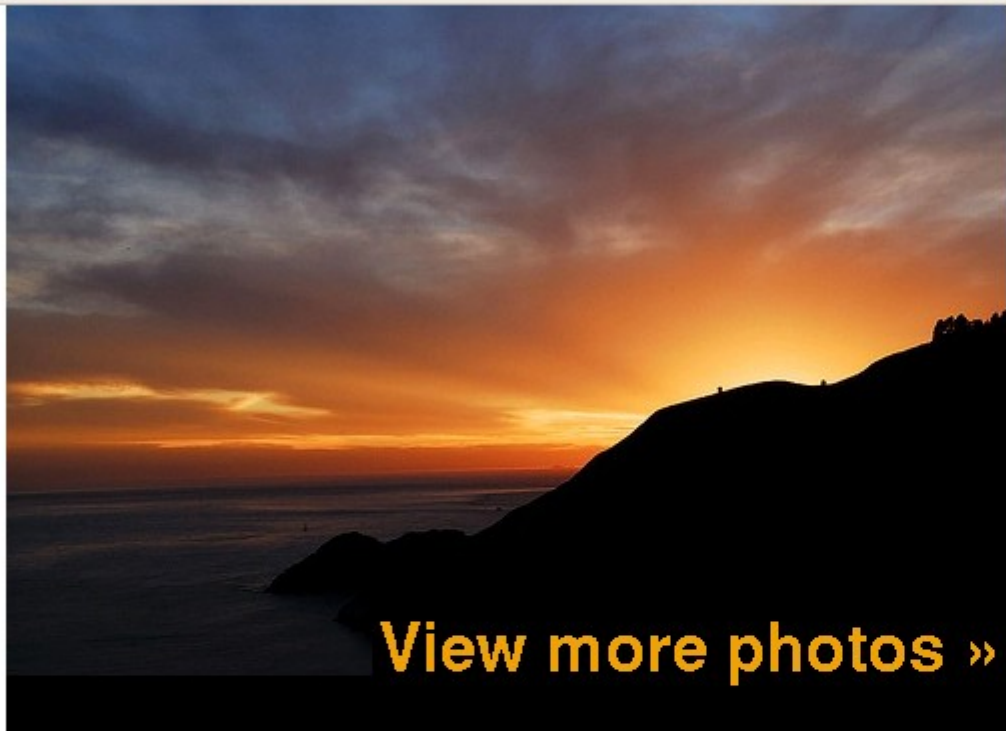
[Your Affiliate Sites](#)

[Sign Out](#)

**Find sites that
supports OpenID**

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





[View more photos »](#)

[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.





Find Friends! OR Sign-In Join Zoomr!

Sign-In | OpenID What is OpenID?

simonj.myopenid.com

Let's Go Exploring!

Cancel

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.

And this is new?



SAML



Higgins



Microsoft

Cardspace



X.509 / eID

***How does
OpenID work?***

RTFM

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

New! Version 2.0!

OpenID Terminology..?

“User-Supplied Identifier”

**What you type at the
OpenID URL prompt**

simonj.myopenid.com

josefsson.org

“Relying Party” (RP) aka “Consumer”

**Web site that wants
proof of who you are**

WikiTravel

Zoomr

LiveJournal

“OpenID Provider” (OP)

Web site that you rely on for authentication services

myOpenID

VeriSign PIP

Livejournal

Yubico

Protocol flow...?

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 OpenID do more?

Yes!

“Simple Registration”

**Your OpenID server can send
personal information to the
web site**

**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**

***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**

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

**Phishing is a real security
problem for OpenID**

Solutions?

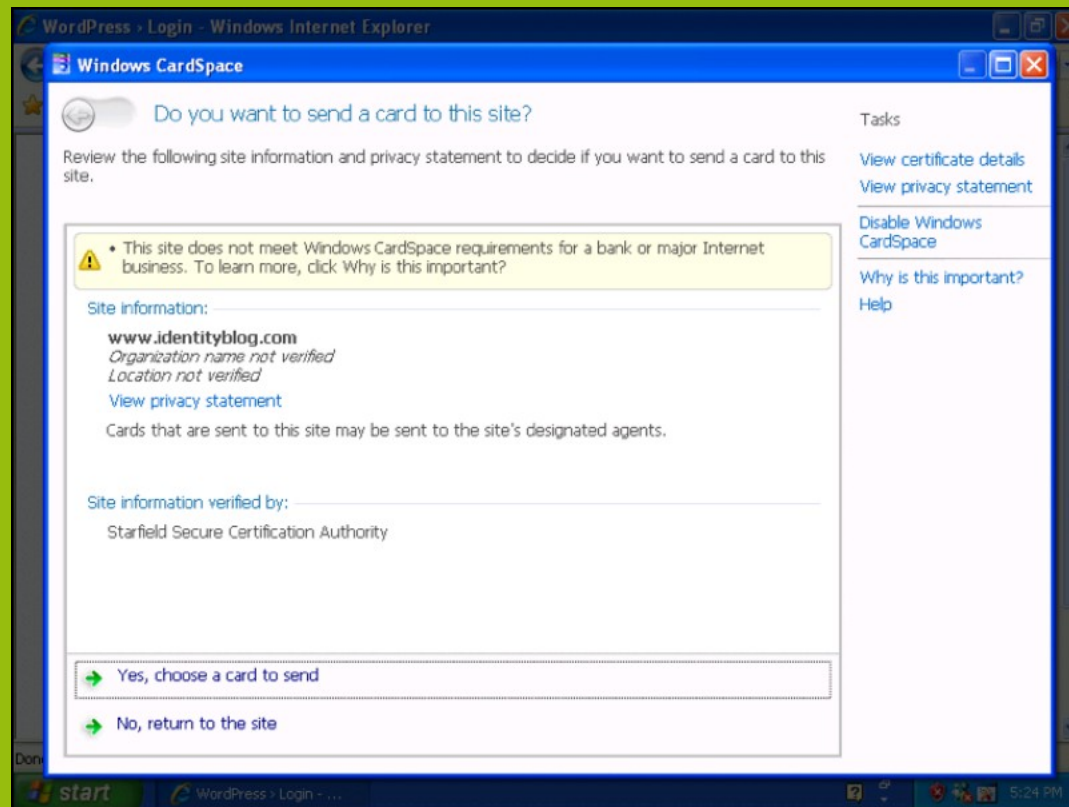
“Never enter passwords in the attackers' control flow”

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!)**

**Generally, just avoid
using passwords**

HTTPS with client- side certificates (complex!)

Hardware authentication devices

yubico

trust the net

**Company started
in May 2007**

**6 people in Stockholm
and California**

Yubico Identity Platform

OpenID, Radius, PAM, PHP, Perl, ...

Developing a multi- platform USB key with no device drivers



**RFID card with
buttons, card reader
and proprietary
device drivers**



USB key with pin entry

USB key with one button



Ultra-Thin



Demo!

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

navigation

- Main Page
- Project Home
- Today's log
- Recent changes

Main Page

Login with OpenID - Wikitravel - Iceweasel

File Edit View History Bookmarks Tools Help

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

Wikitravel

special

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.

Users of other sites can use their existing account to log in to Wikitravel by using their OpenID URL, such as `http://wikitravel.org/en/`.

If you already have an account with an account normally.

Yahoo! users can use their existing account to log in to Wikitravel by using their screen name, such as `http://wikitravel.org/en/yourscreenname`.


AOL or AIM users can use their existing account to log in to Wikitravel by using their screen name, such as `http://wikitravel.org/en/yourscreenname`.

Confirm log in by pressing or

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

Verification succeeded

Verification succeeded

Return to Main Page.

Done

Tor Disabled



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

128-bit AES key

Two factor authentication



Wallet size

No display or batteries

Questions?

Answers?

How to use Yubikey via your own homepage

Add

```
<link rel="openid.server"  
      href="http://openid.yubico.com/server.php" />
```

```
<link rel="openid.delegate"  
      href="http://openid.yubico.com/user/?id=ljitnjbcbujvh">
```

Replace *ljitnjbcbujvh* with your Yubikey's identity string: the first 12 characters printed by the key when you press the button