What is...

OpenID

...?
Decentralized web-based authentication system
What does that mean?
As User:

You can reduce the number of username and passwords you need to remember.
As Developer:

You don't need to maintain a username and password database for your web site
aka: out-source the authentication service to someone else!
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
Zooomr
LiveJournal
“OpenID Provider” (OP)

Web site that you rely on for authentication services

myOpenID
VeriSign PIP
Livejournal
Yubico
How does OpenID work technically?
1. User browse to Relying Party (RP)

2. Enters User-Supplied Identifier in a HTML form, posted back to RP
HTML discovery:

3. RP retrieve identifier URL

4. Extract META link.rel fields
RP can create a Diffie-Hellman association with the OP at this point. The goal is to set up a shared secret between RP and OP.

Optional step! Not discussed here.
5. RP redirects browser to server indicated by `openid.server` – expecting to resume at `openid.return`

HTTP/1.0 302 Moved Temporarily

6. User-Agent requests the new URL

7. User authenticates and/or accepts, HTML form posted back to OP
8. OpenID Provider redirects browser back to Relying Party

HTTP/1.0 302 Moved Temporarily

http://wikitravel.org/en/Special:OpenIDFinish?
nonce=FJm3Ncp4&openid.assoc_handle=%7B7BHMAC-SHA1%7D
%7B48dce8d3%7D%7Bbqvf%2Fw%3D%3D%7D&openid.identity=http
%3A%2F%2Fopenid.yubico.com%2Fserver.php%2Fidpage%3Fuser
%3Dekhgjhbctrgn&openid.mode=id_res&openid.op_endpoint=ht
tp%3A%2F%2Fopenid.yubico.com
%2Fserver.php&openid.response_nonce=2008-09-26T12%3A42%3
A52ZgcvcMd&openid.return_to=http%3A%2F%2Fwikitravel.org
%2Fen%2FSpecial%3AOpenIDFinish%3Fnonce
%3DFJm3Ncp4&openid.sig=ybS%2BIXK1HU1mi3UkdeO7r0BS%2FxY
%3D&openid.signed=assoc_handle%2Cidentity%2Cmode
%2Cop_endpoint%2Cresponse_nonce%2Creturn_to%2Cssigned
9. Browser requests the new URL

10. After receiving the response, RP verifies the signature
The RP verifies the signature in the response by using the shared secret key established via D-H or using a direct HTTP call to the OP.
OpenID Trust Relationship
User

OpenID Provider

Relying Party
And this is new?
Why chose OpenID over the rest?
“Solve one problem and do it well”
Few of the other technologies are optimized for web applications
Disadvantage: OpenID is only for web applications

(...although some people are trying to use it for other purposes...)
Other standards are already on-board
Trend to use OpenID as the user and browser interface, but use other technology in the backend (e.g., SAML) and between RP and OP
Are there security problems in OpenID?
Phishing is a real problem
OpenID Phishing Attack

1. User browses to Evil-RP
2. Instead of redirecting user to OP, Evil-RP redirects user to OP'
3. OP' is controlled by Evil-RP and looks the same as OP
4. OP' asks for user's credentials
5. User doesn't notice he is talking to OP' != OP and enters long-term credentials
6. Profit
Solutions?
“Never enter passwords in the attackers' control flow”
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
Company started in May 2007
9 people in Stockholm and California
Invention: USB-based one-time-password generator
Product History:
Version 0, Version 1, ...
RFID card with buttons, card reader and proprietary device drivers
USB key with pin entry
USB key with one button
Ultra-Thin Touch button
Market positioning

Overall simplicity and cost-efficiency

- USB- /smartcards
- Authentication tokens
- SMS authentication
- Software certificates
- Digital keyboards
- Username / passwords
How does the Yubikey work?
128-bit AES key
Simulates an USB keyboard

Unique ID      Time variant pass code

`tndrvbteccunbhkddvclbckjbidjbbftcebjkkhcfl`e
`tndrvbteccunvtkkuvblbbbkbcerefuvuckbdhhucid`
`tndrvbteccuncclhhvkthctdnclgktdktvnttfcgikic`
`tndrvbteccuhjvgrhdvbjlgllicchdgvjnigluuvdjl`
Two-factor authentication
Wallet size
No display or batteries
No mechanical parts
Success factors for the mass market

High Security
State of the art

Overall Simplicity
- All computers
- One click login
- No software
- Portable
- Easy integration

Low Cost
- Low manufacturing cost
- Low shipping cost
- Unlimited lifetime
- Free SDK
How can I integrate the YubiKey?
All open source ...
Questions?

Answers?
How to use your own webpage as an OpenID URL authenticated using YubiKey

Add

```html
<link rel="openid.server" href="http://openid.yubico.com/server.php" />
<link rel="openid.delegate" href="http://openid.yubico.com/user/?id=ljitnbjbcujvh" />
```

to the HTML HEAD section of your webpage.

Replace `ljitnbjbcujvh` with the identity string of your YubiKey, i.e., the first 12 characters printed by the key when you touch the button