

October 3<sup>rd</sup> 2008  
IT University  
Copenhagen

# Open Source Days

2008



Simon Josefsson  
Head of R&D  
[simon@yubico.com](mailto:simon@yubico.com)  
<http://www.yubico.com/>

**yubico**

trust the net

***What is...***



***...?***

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

***What does that mean?***

# As User:

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

**Sign in to Yahoo!**

Prevent Password Theft

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

MySpace | People | Web | Music | Music Videos | Blogs

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 | Horoscopes | Music Videos | TV On Demand  
Downloads | Impact

**Exclusive NEVER BEFORE SEEN American Idol Video**

Member Login

E-Mail:   
Password:   
 Remember Me

Forgot your password?

Cool New People

valerie | ash | Roddy

**YouTube** Broadcast Yourself™

Sign Up | My Account | History | Help | Links

Videos | Categories | Channels | Community | Upload Videos

Director Videos

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

**Featured Videos** See More Featured Videos

Lika Barn Avvika Bäst Del 2  
CberendelFarsabla  
Time: 1:05  
Views: 7,043  
★★★★

Cows With Guns  
An epic musical tale about the great cow revolution. A 6 minute claymation by Guru  
From: caraborn  
Views: 26,792  
★★★★

**Most popular CHANNELS this week**

My: Videos - Channels - Profile - Blog - Subscriptions

**COMP USA** 1-800-COMPUSA

Sign Up | Log In | Help

**Create New Account** (See Benefits)

First Name:   
Last Name:   
E-Mail 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

AMERICAN WORKING | SITUATION ROOM | LOW DOBS TONIGHT | PAULA PATTON SHOW | LARRY KING LIVE | ANDERSON COOPER 360 | RANCHO GRACE | SCHEDULE

Feedback | International Edition | CNN (Print)

**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

FDIC ETORADE BANK

QUICK TRANSFER Between E\*TRADE and any institution.

SECURE LOG ON

User ID:  Password:

Start In:

Accounts:

Forgot your User ID or Password?

Set Up Online Account Access

HOME LOANS

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

TRADING

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

INVESTING

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

BANKING

5.05% 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%)

**Quality Foods.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

Register

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

Password:  [forgot your password?](#)

New here? [Sign up](#) | [Create my account](#) | [Take a tour](#)

About | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Sites | Base 2kx

**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

**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!**



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 >

OpenID Login

People add you as their friend, trust your name you're logged in, you'll also be able to

Just enter your journal URL (you don't need an address is. After you do so, you'll be able to trust them once, or forever. You can

Welcome to MyOpenID - Iceweasel

myOpenID  
SECURE OPENID PROVIDER

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
- Ease-of-sign-in on untrusted sites
- Account activity reports
- Ability to manage multiple personas for different sites and a whole lot more!

LEARN SOME MORE

- Learn more about OpenID
- Get some help
- Send us some feedback
- Check out the blog
- Sites that support OpenID

BECOME A MYOPENID AFFILIATE

SIGN UP FOR AN OPENID

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

http://claimid.com/

Welcome to claimID.

claimID Login:  
Password:

Log in to claimID | Need help?

Secure Login

You might also wish to:

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

claimID is the free, easy way to manage your online identity with OpenID.



# *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

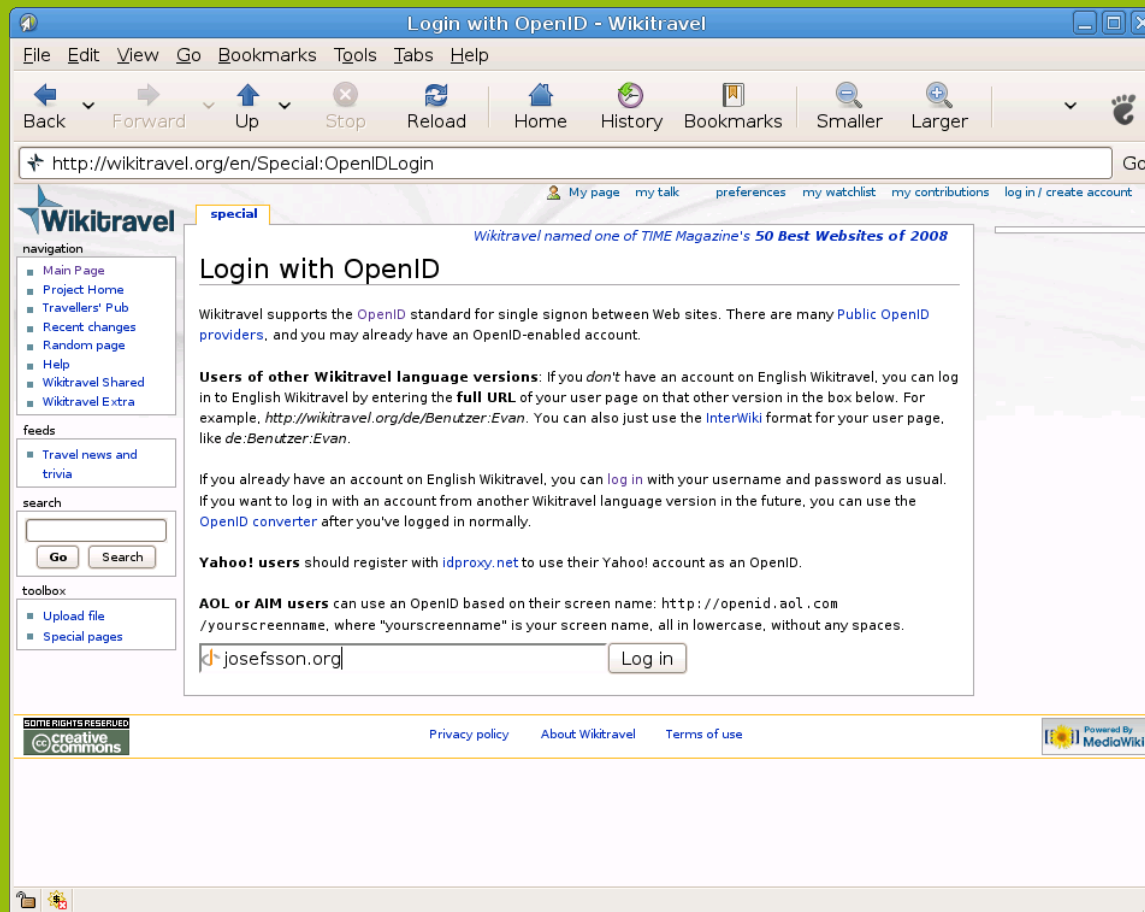
VeriSign PIP

Livejournal

Yubico

***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

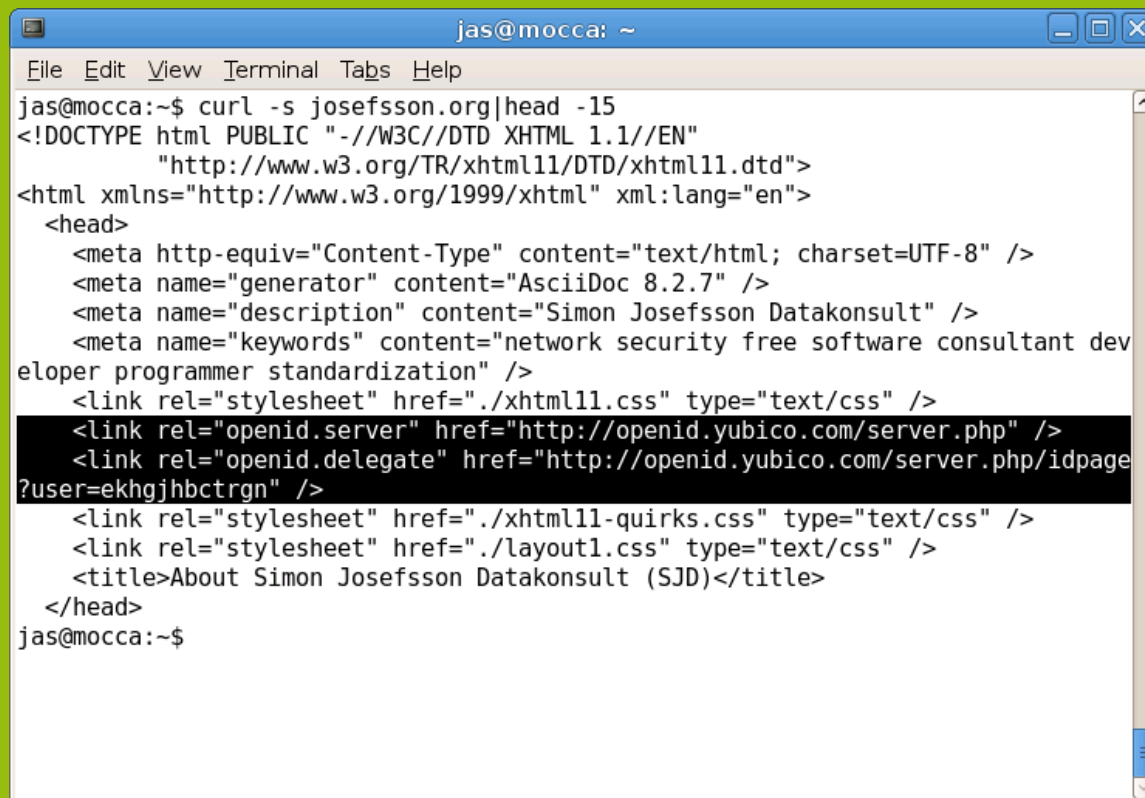




# HTML discovery:

3. RP retrieve identifier URL

4. Extract META link.rel fields



```
jas@mocca: ~  
File Edit View Terminal Tabs Help  
jas@mocca:~$ curl -s josefsson.org|head -15  
<!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 8.2.7" />  
    <meta name="description" content="Simon Josefsson Datakonsult" />  
    <meta name="keywords" content="network security free software consultant dev  
eloper programmer standardization" />  
    <link rel="stylesheet" href="./xhtml11.css" type="text/css" />  
    <link rel="openid.server" href="http://openid.yubico.com/server.php" />  
    <link rel="openid.delegate" href="http://openid.yubico.com/server.php/idpage  
?user=ekhgjhbctrgn" />  
    <link rel="stylesheet" href="./xhtml11-quirks.css" type="text/css" />  
    <link rel="stylesheet" href="./layout1.css" type="text/css" />  
    <title>About Simon Josefsson Datakonsult (SJD)</title>  
  </head>  
jas@mocca:~$
```

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.

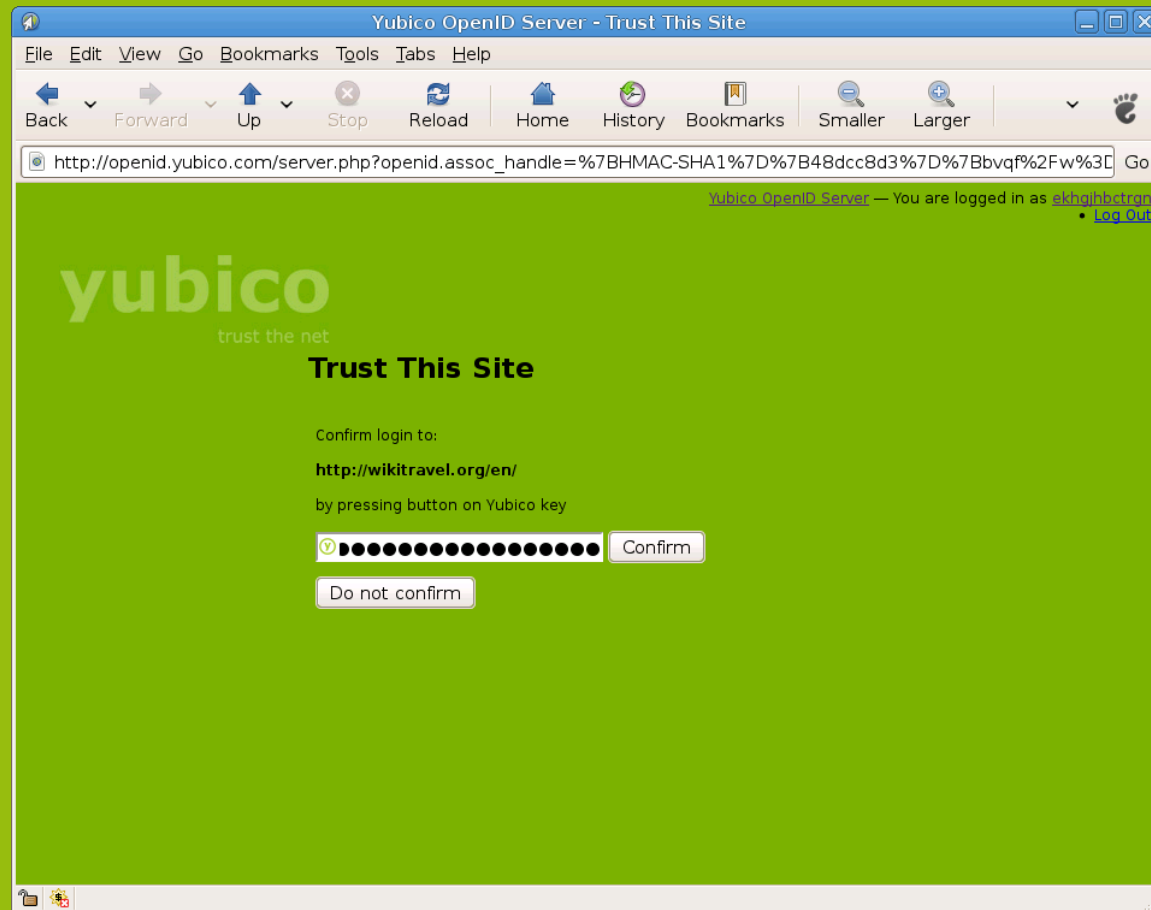
## 5. RP redirects browser to server indicated by *openid.server* – expecting to resume at *openid.return*

```
HTTP/1.0 302 Moved Temporarily
```

```
http://openid.yubico.com/server.php?openid.assoc_handle=
%7B HMAC-SHA1%7D%7B48dcc8d3%7D%7Bbvqf%2Fw%3D%3D
%7D&openid.identity=http%3A%2F%2Fopenid.yubico.com
%2Fserver.php%2Fidpage%3Fuser
%3Dekhgjhbctrgn&openid.mode=checkid_setup&openid.return_
to=http%3A%2F%2Fwikitravel.org%2Fen%2FSpecial
%3AOpenIDFinish%3Fnonce
%3DFJm3Ncp4&openid.sreg.optional=nickname%2Cemail
%2Cfullname%2Clanguage%2Ctimezone&openid.trust_root=http
%3A%2F%2Fwikitravel.org%2Fen%2F
```

6. User-Agent requests the new URL

7. User authenticates and/or accepts,  
HTML form posted back to OP



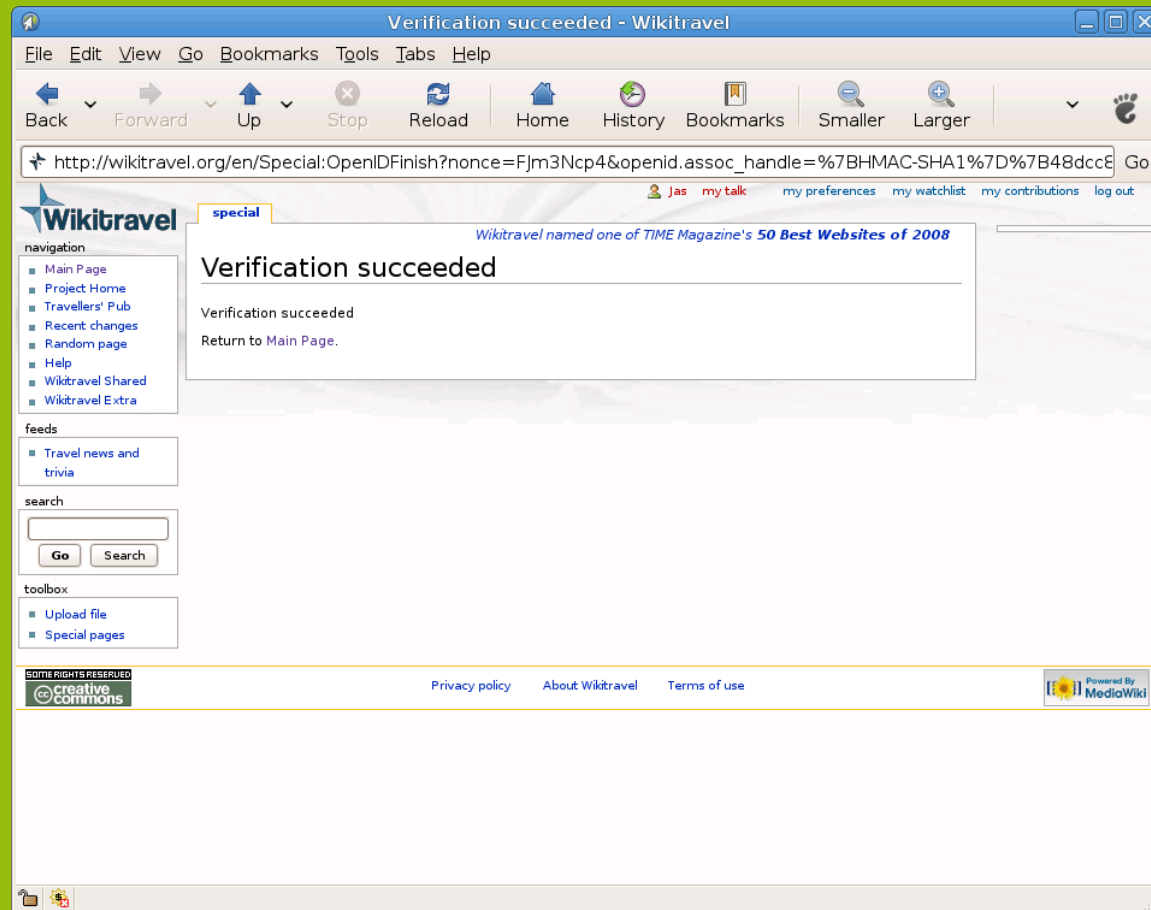
## 8. OpenID Provider redirects browser back to Relying Party

HTTP/1.0 302 Moved Temporarily

```
http://wikitravel.org/en/Special:OpenIDFinish?  
nonce=FJm3Ncp4&openid.assoc_handle=%7B HMAC-SHA1%7D  
%7B48dcc8d3%7D%7Bbvqf%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  
A52ZgcvvcMd&openid.return_to=http%3A%2F%2Fwikitravel.org  
%2Fen%2FSpecial%3AOpenIDFinish%3Fnonce  
%3DFJm3Ncp4&openid.sig=ybS%2BIXKlHulmi3Ukde07r0BS%2Fxy  
%3D&openid.signed=assoc_handle%2Cidentity%2Cmode  
%2Cop_endpoint%2Cresponse_nonce%2Creturn_to%2Csigned
```

9. Browser requests the new URL

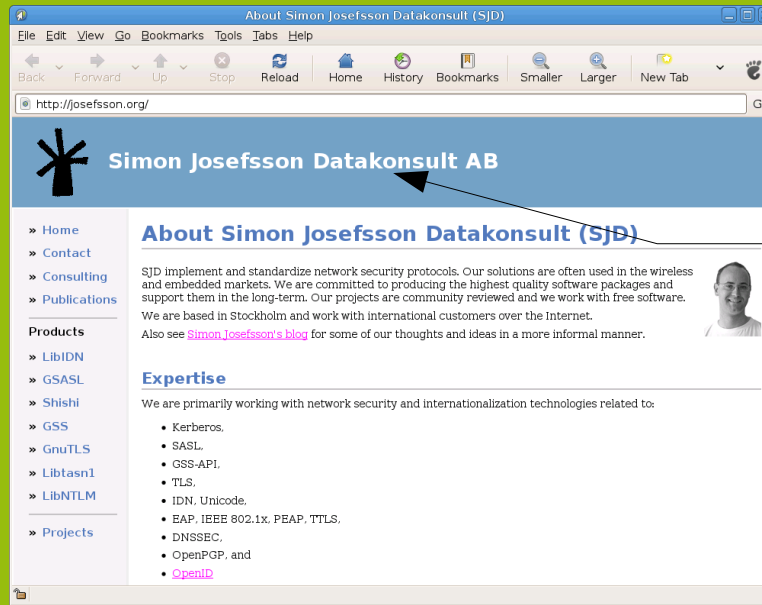
10. After receiving the response, RP verifies the signature



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.

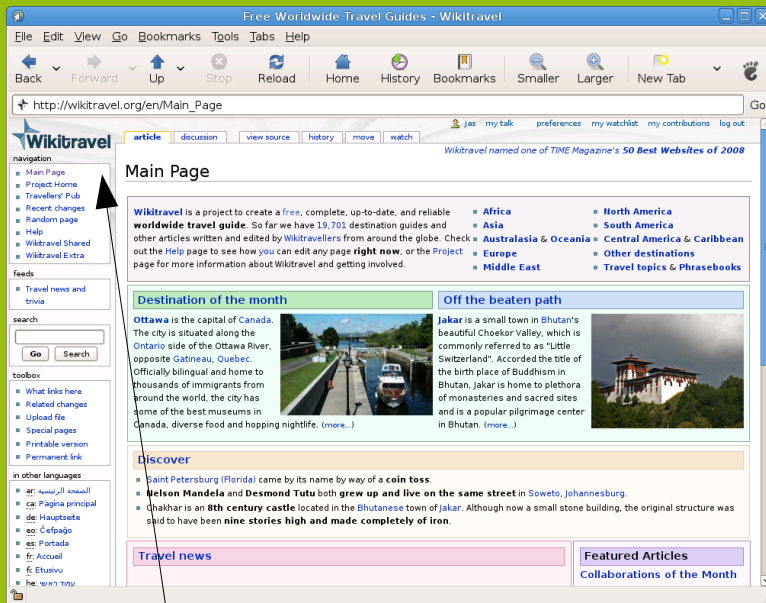
# *OpenID Trust Relationship*



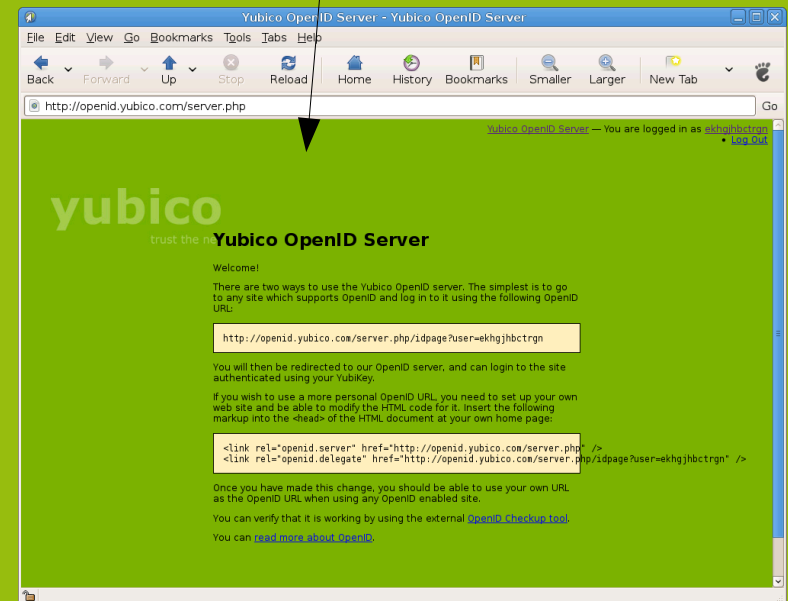


User

OpenID Provider



Relying Party



***And this is new?***



SAML



Higgins



*Microsoft*

Cardspace



Shibboleth.

**X.509 / eID**

***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'  $\neq$  OP and enters long-term credentials
6. Profit

***Solutions?***

***“Never enter passwords in the attackers’ control flow”***

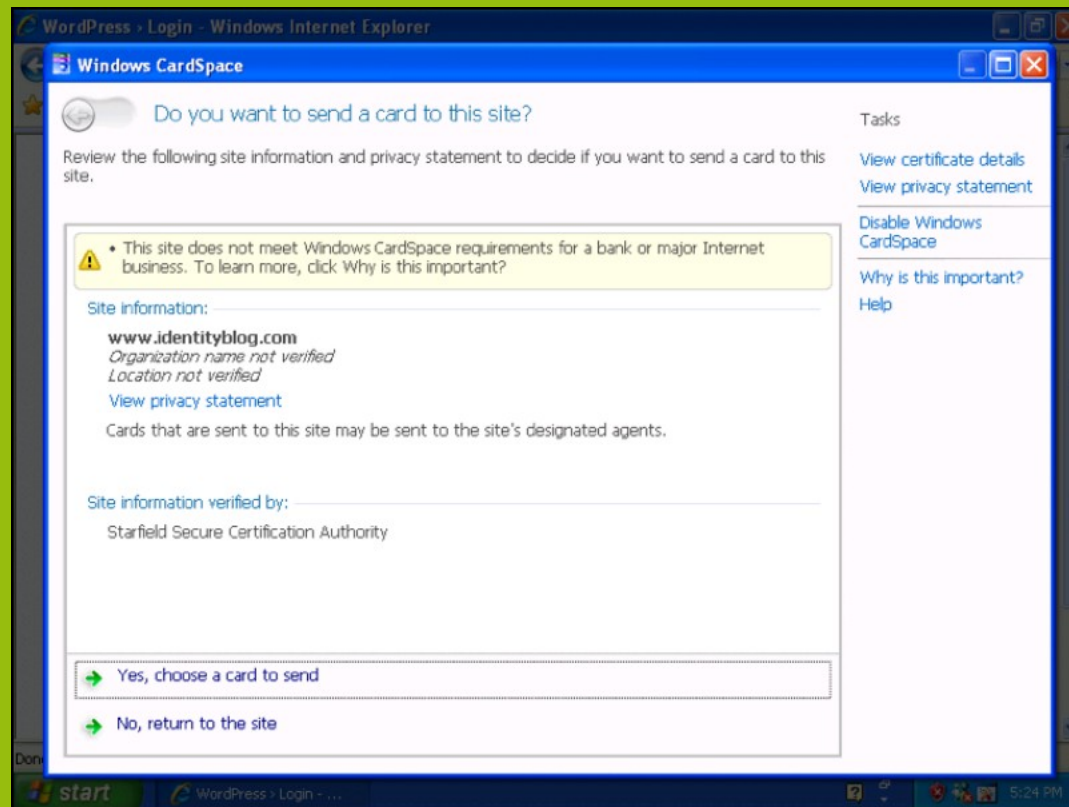
## **You need to sign in**

---

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

**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**



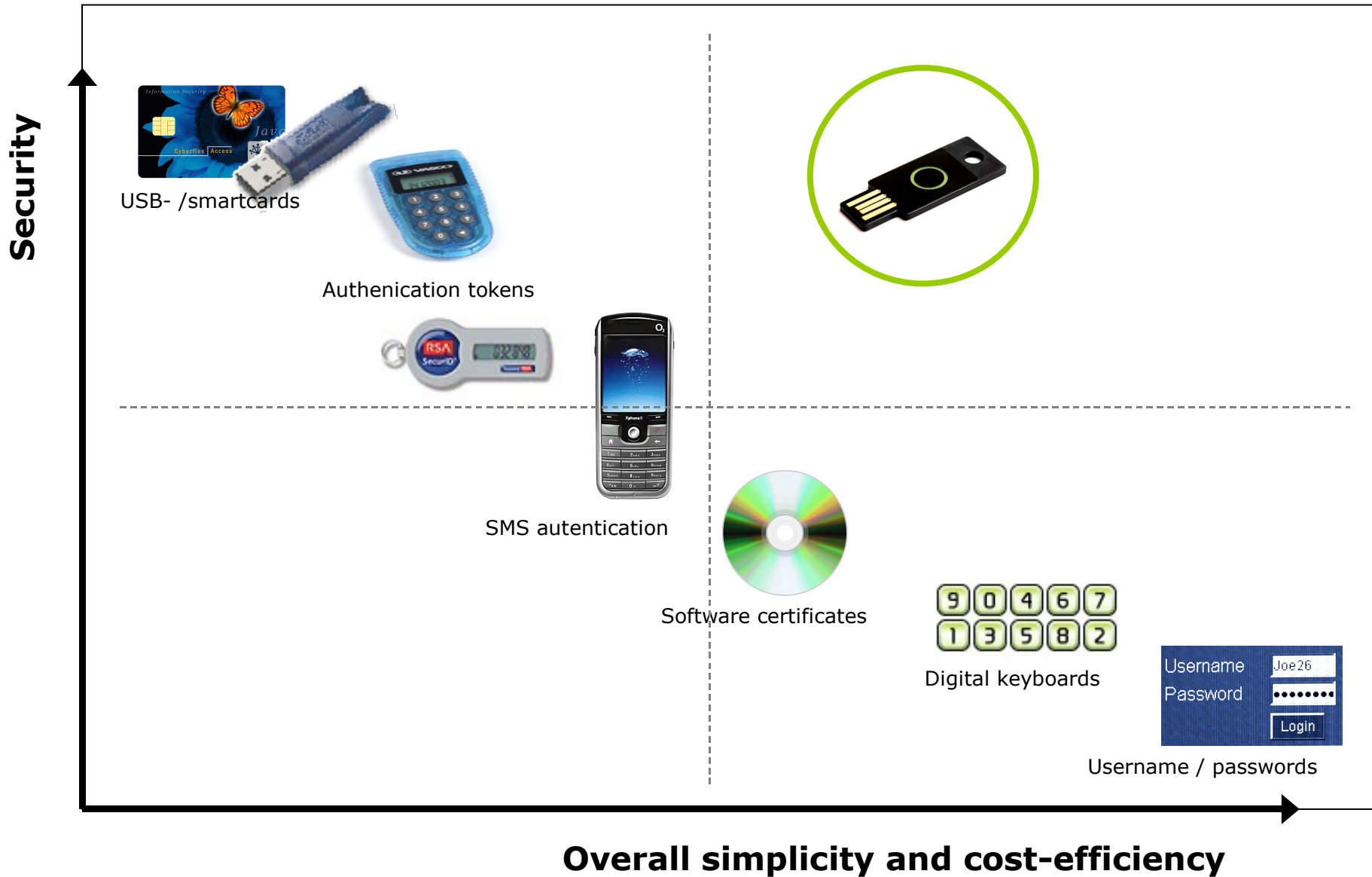
# USB key with pin entry

# USB key with one button



# Ultra-Thin Touch button





USB- /smartcards



Authentication tokens



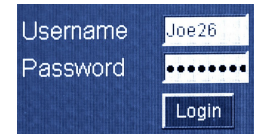
SMS authentication



Software certificates



Digital keyboards



Username / passwords



Overall simplicity and cost-efficiency

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



**128-bit AES key**

# Simulates an USB keyboard



***Unique ID***

***Time variant pass code***

tndrvbtecccunbhkddvclbckjbidjbbftcebjkkhcfle  
tndrvbtecccunvtkkuvblbbbkbcerufuvuckbdhhucid  
tndrvbtecccunclhhvktthctdnclgktdktvnttfcgikic  
tndrvbteccuhjvgrhdvbjlglicchdgvjniglujuvdjl

# **Two-factor authentication**

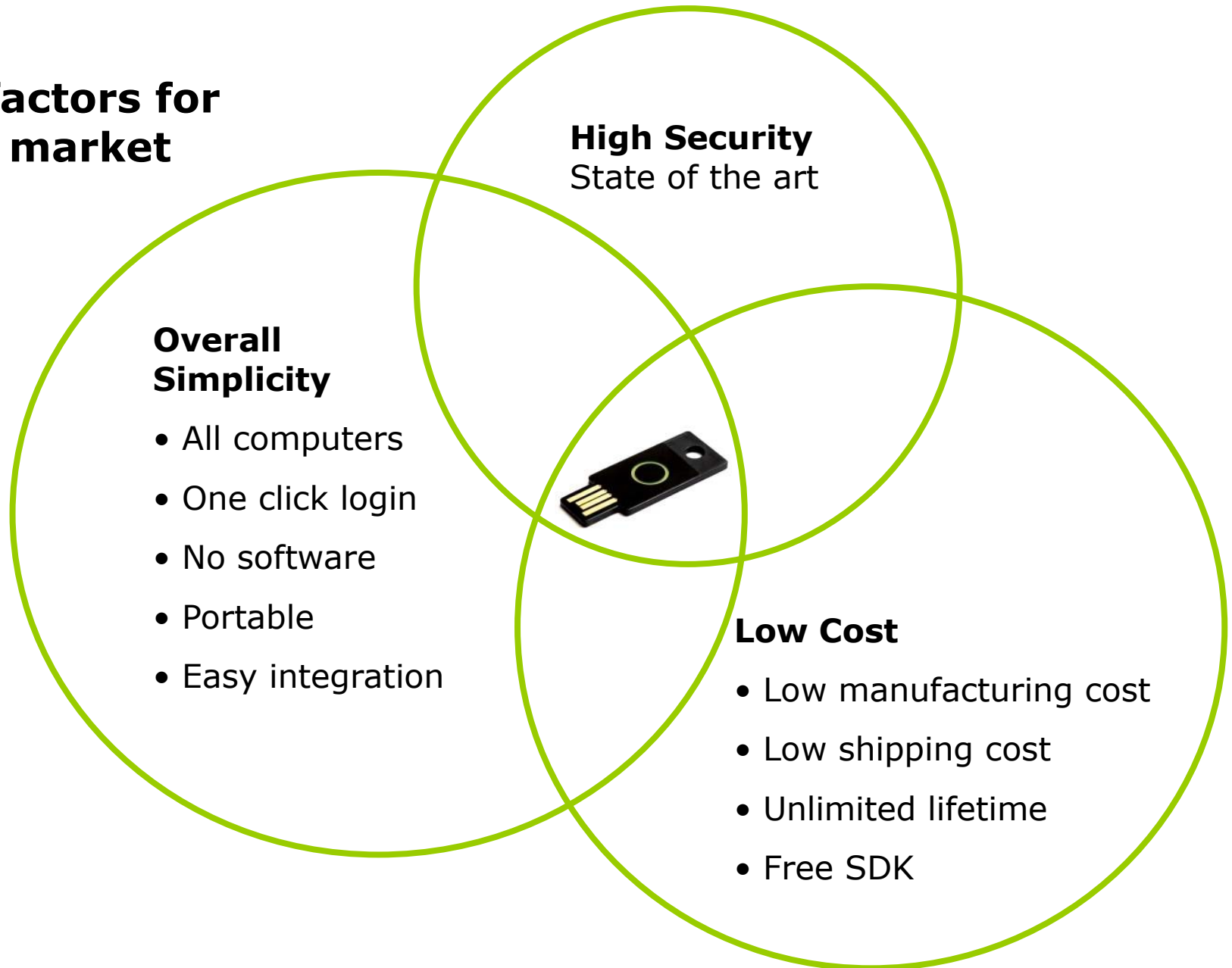


**Wallet size**

**No display or batteries**

**No mechanical parts**

## Success factors for the mass market





***How can I integrate  
the YubiKey?***

**All open source ...**

**Radius**

**.NET**

**C#**

**C++**

**Java**

**PHP**

**Perl**

**Python**

**Ruby**

*Questions?*

**Answers?**

# *How to use your own webpage as an OpenID URL authenticated using YubiKey*

## **Add**

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

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

**to the HTML HEAD section of your webpage.**

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