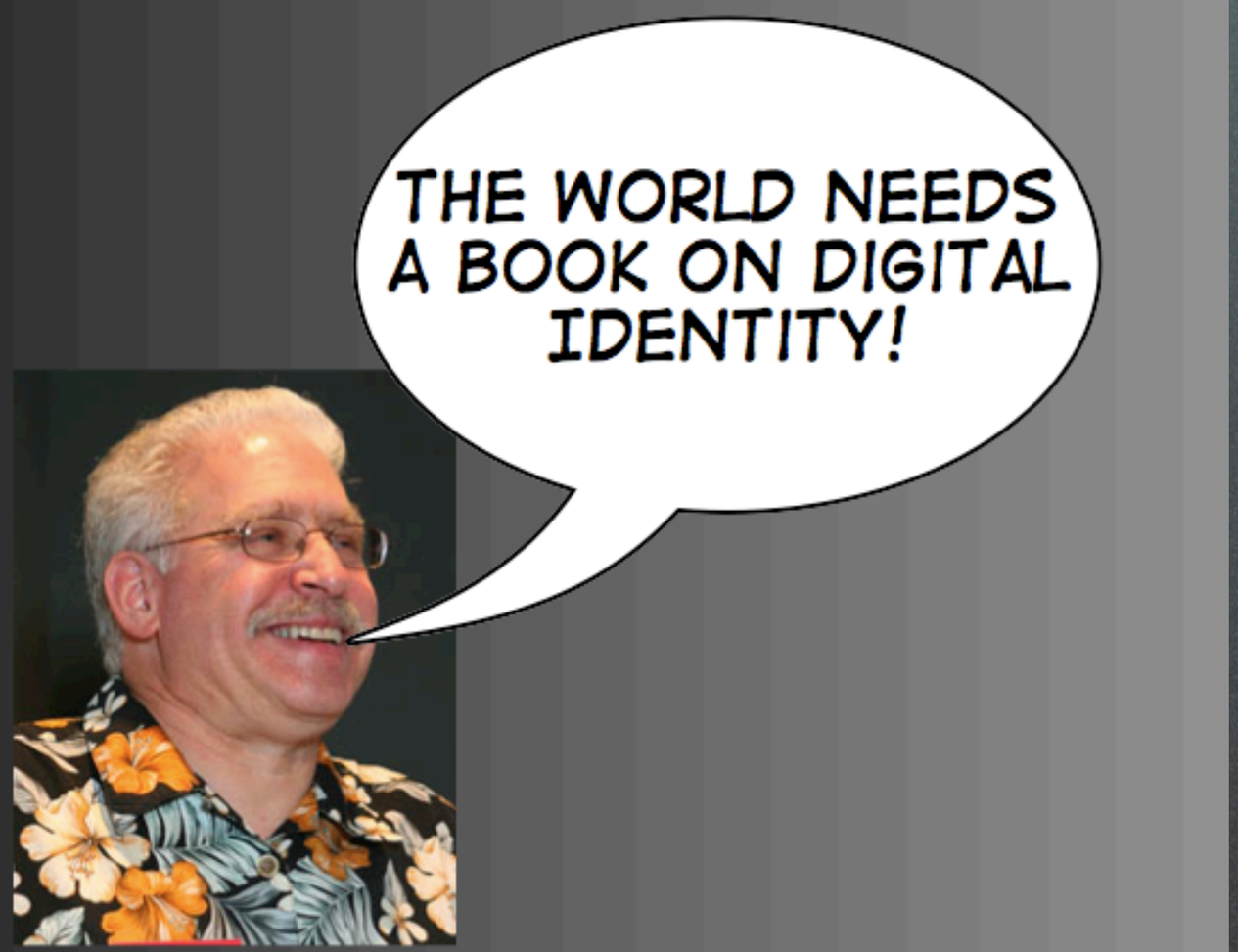
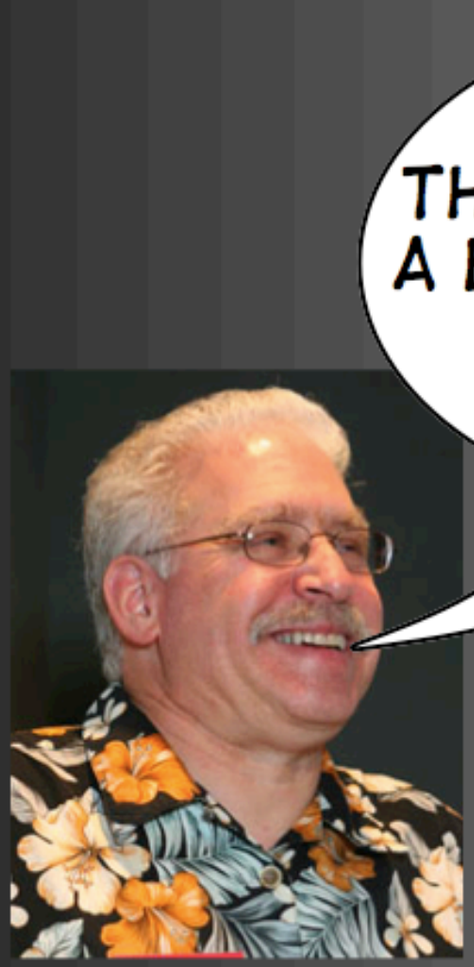
Digital Identity
Tutorial for WWW2007

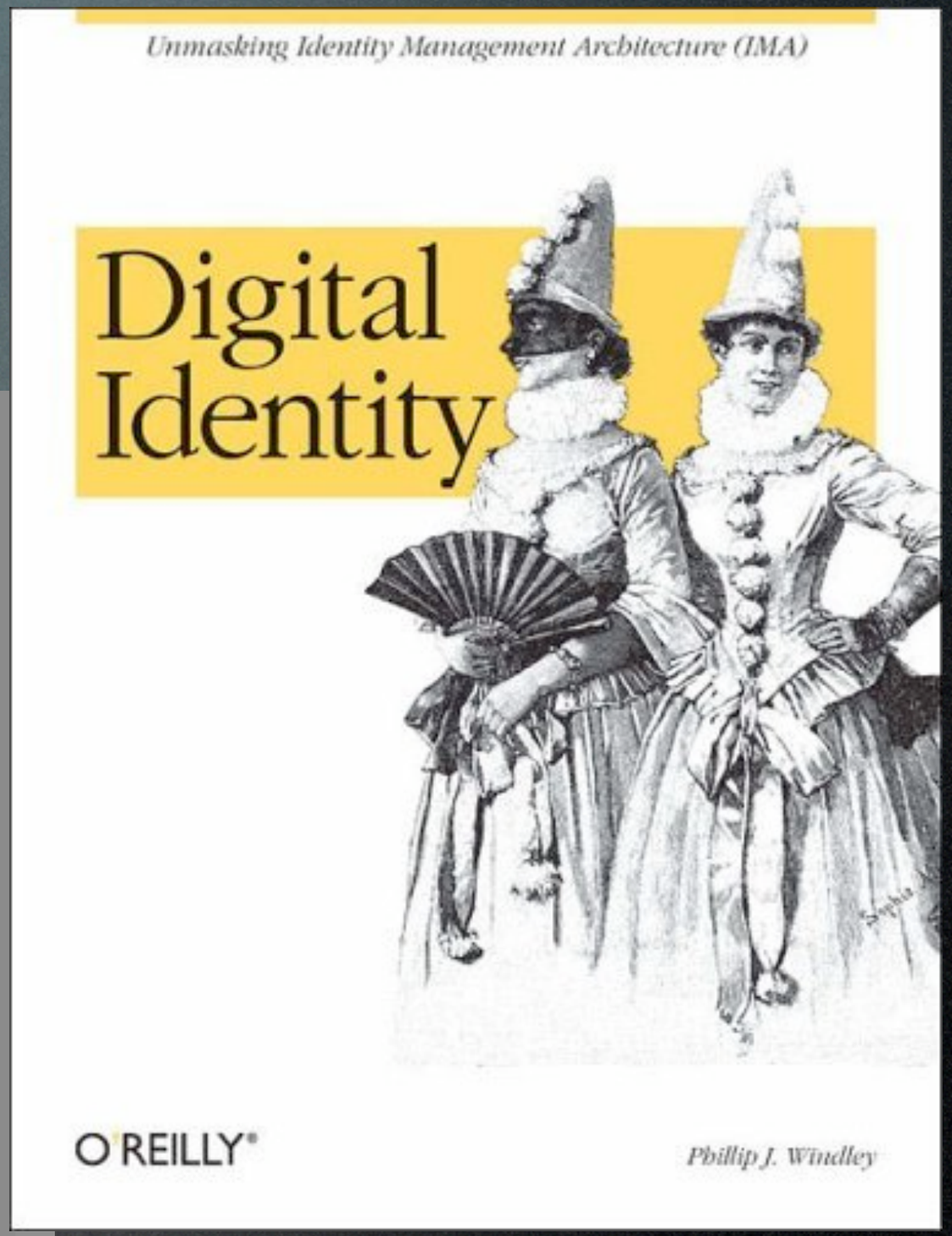
Phillip J. Windley
Brigham Young University

phil@windley.com
www.windley.com

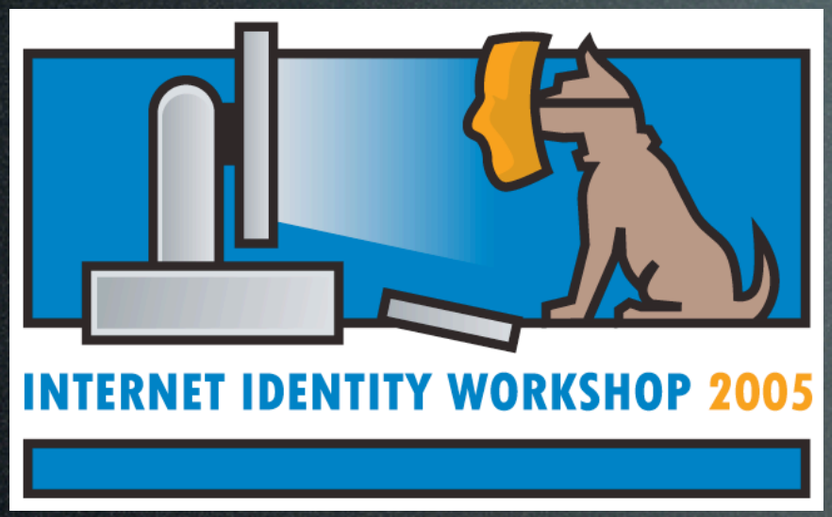


www.windley.com





www.windley.com



October, 2005

May and
Dec, 2006

May 14-16, 2007
Mountain View, CA

www.windley.com

WINDLEY'S TECHNOMETRIA

ORGANIZATIONS GET THE IT THEY DESERVE

TECHNOMETRIA

Home
Why Technometria?
RSS XML
Atom XML
Podcasts XML
add to My YAHOO!
Recommend This Site

ABOUT PHIL

Brief Bio
My hCard
Contact Me
My i-name: =windley
(what's an i-name?)
Speaking
InfoWorld
Photo Albums
CTO Breakfast

ESSAYS

2005
2004
2003
CIO White Papers

TOPIC GUIDES

Understanding RSS
Digital ID Policies
Understanding VoIP
Internet Application Performance

September 09, 2005

Identity 2.0: The Movie

If you missed Dick Hardt's presentation on Identity 2.0 at OSCON this year, he's turned it into a movie. This is well worth viewing if you've got any interest in identity.

02:42 PM | Comments (0) | Recommend | Post to del.icio.us | Print

XQuery Apache Module

From Freshmeat:

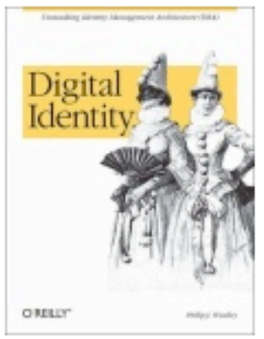
> *Native XmlDB Query Daemon is a client-server version of the Sleepycat native XML database deployed as an Apache module. The client is a pure Java API, supporting XQuery, XPath, and an Xml:DB API layer. It comes with a graphical admin console. Server binaries are provided for Linux x86 and x86-AMD64; for other platforms, compile from source.*
>
> ***From freshmeat.net: Project details for Native XmlDB Query Daemon***
> ***Referenced Fri Sep 09 2005 09:54:31 GMT-0600 (MDT)***

09:53 AM | Comments (0) | Recommend | Post to del.icio.us | Print

September 08, 2005

IIW2005: Hotels and Wiki

Digital Identity



Buy the book!

FREE NEWSLETTER!

email address
Sign me up!

(Find out more...)

SEARCH

Search this site:
Search

UPCOMING EVENTS

Dell Briefing
September 18 - September 18
Broadband Cities
September 19 - September 19

permalink

www.windley.com

September 11, 2006

Vitamins, Pain-killers, and Viagra

Dick Hardt
(click to enlarge)

Dick Hardt intro'd a panel on identity at big sites (meaning eBay, Yahoo!, Google, MSN, and so on). He used a great analogy of vitamins, pain-killers, and Viagra. We've been selling ID Management as vitamins. Everyone knows that they're good for you, but there's no urgency. With pain-killers, there's urgency. Viagra, on the other hand lets people do things they couldn't do before. User-centric identity is a pain-killer for users, but only a vitamin for big sites.

How do you turn user centric identity into Viagra? He uses eBay as an example. By using a user-centric, federated identity system, they could allow other sites to use their reputation system and charge for the privilege. That's a good example of enabling behavior from shared identity.

Posted on 05:57 PM | Comments (1) | Recommend | Print
Add to del.icio.us | digg | Yahoo! MyWeb
Related: didw06 identity reputation

permalink

www.windley.com

www.windley.com

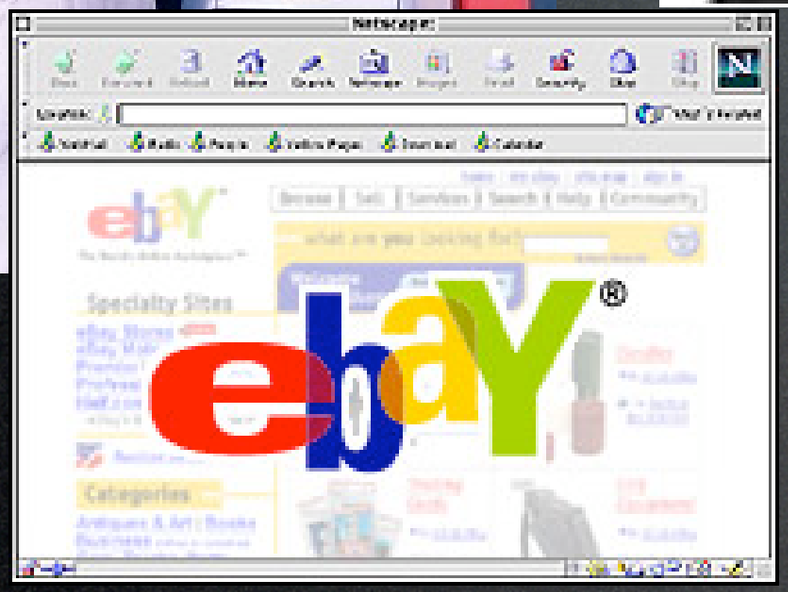
the identity of entries enables conversation

Does Identity Matter?

Inside. Lots and lots of....HARDWARE!

www.windley.com

Does Identity Matter?



www.windley.com

identity is the foundation for commerce

www.windley.com

What Happened to the Walls?

www.windley.com

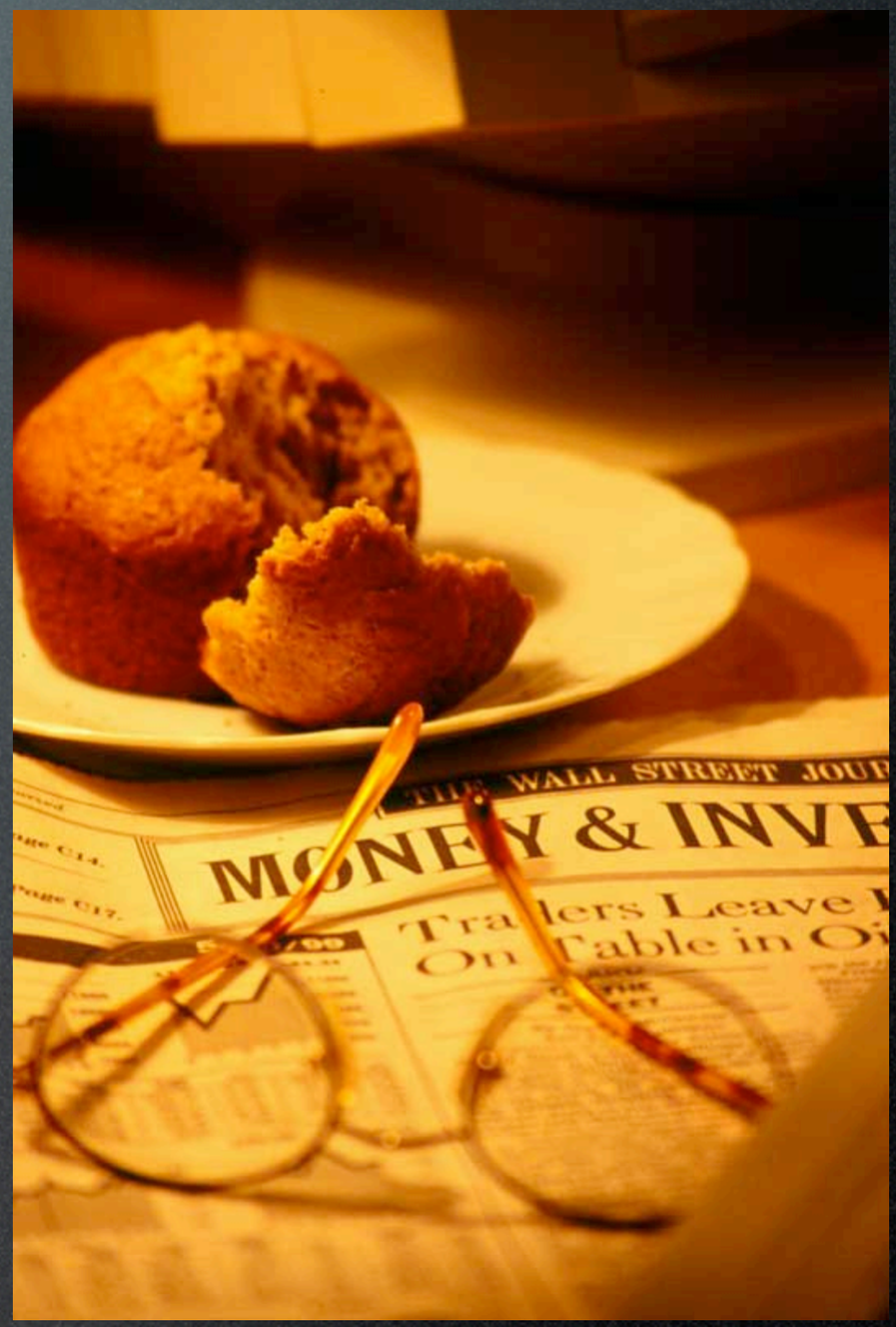
What Happened to the Walls?

www.windley.com

The Border Patrol

Business Context of Identity

vs



www.windley.com

identifiers

what's in a name?

Samantha

Matsuhiro

Fred

Alice

George

Greta

Steve

Cindy

Kristen

Lynne

Betty

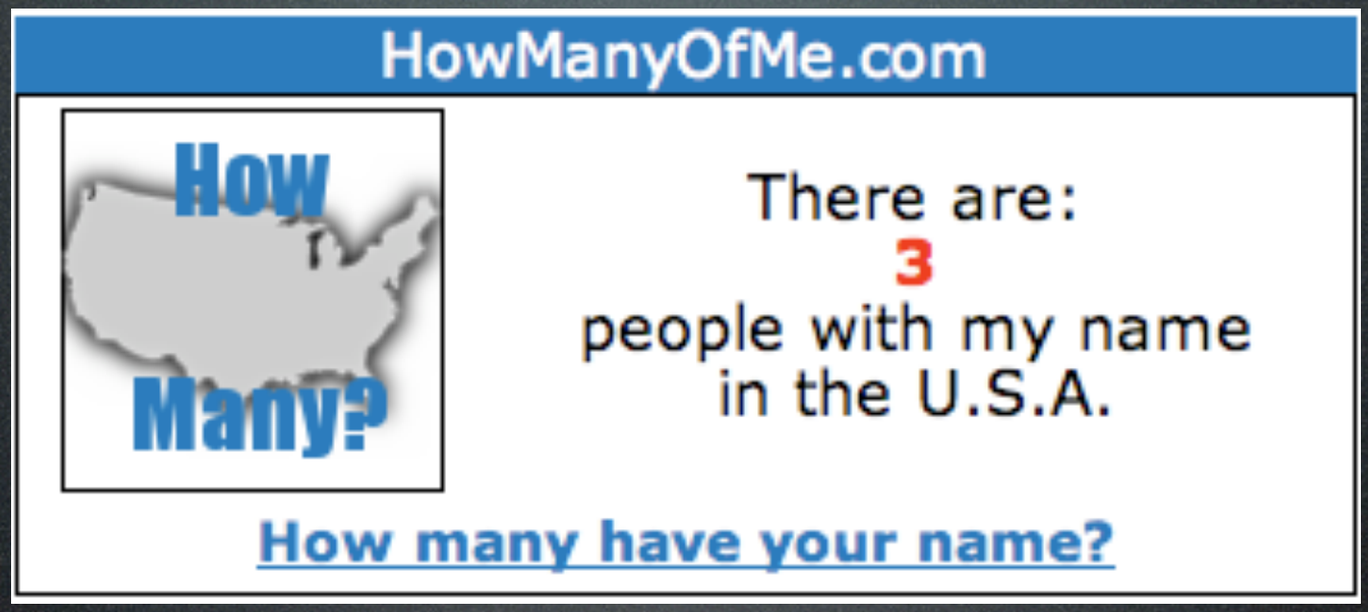
Monty

Phil

Tonya

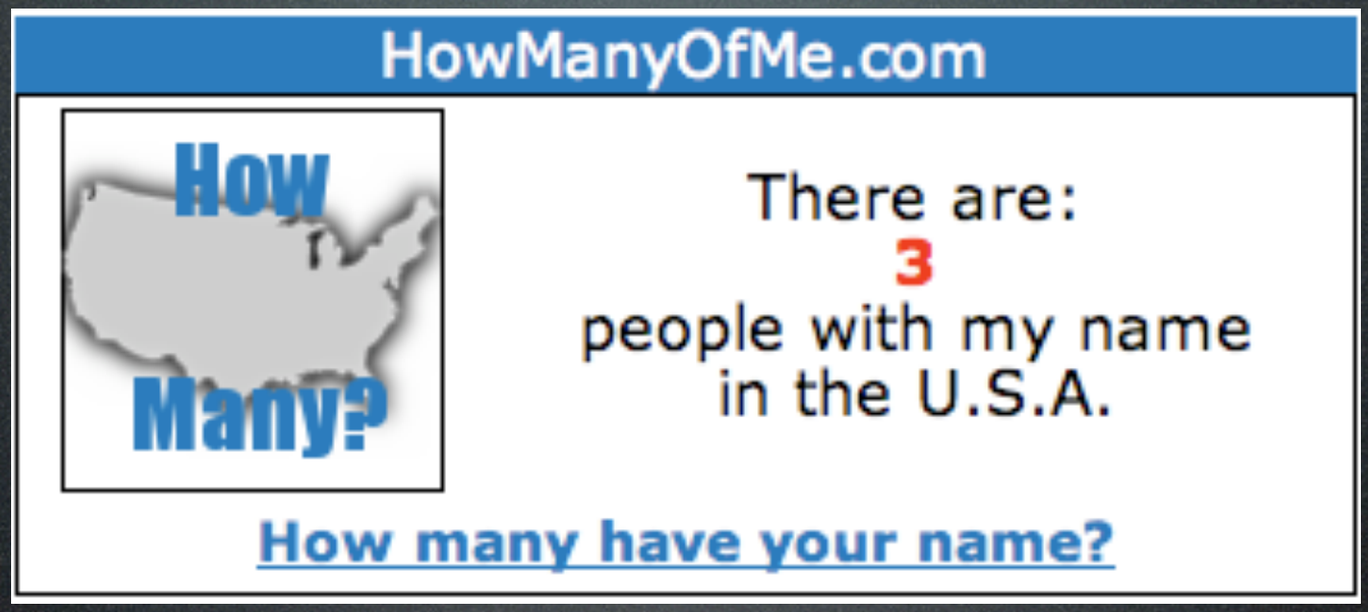
Rumplestiltskin

3 Phillip Windleys



www.windley.com

3 Phillip Windleys



50,000 John Smiths

phil@windley.org

windley.com

http://www.windley.com/essays

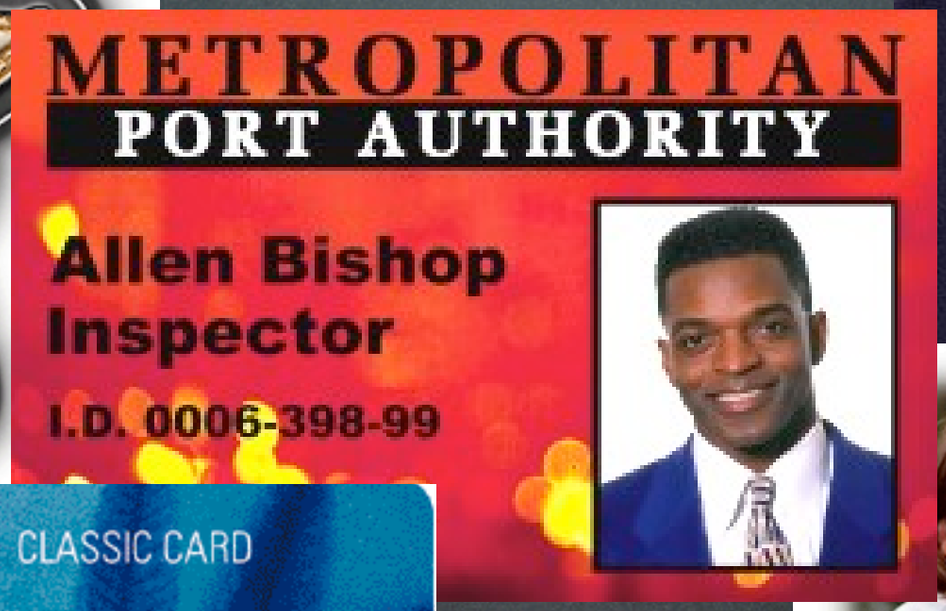
xri://=windley

www.windley.com

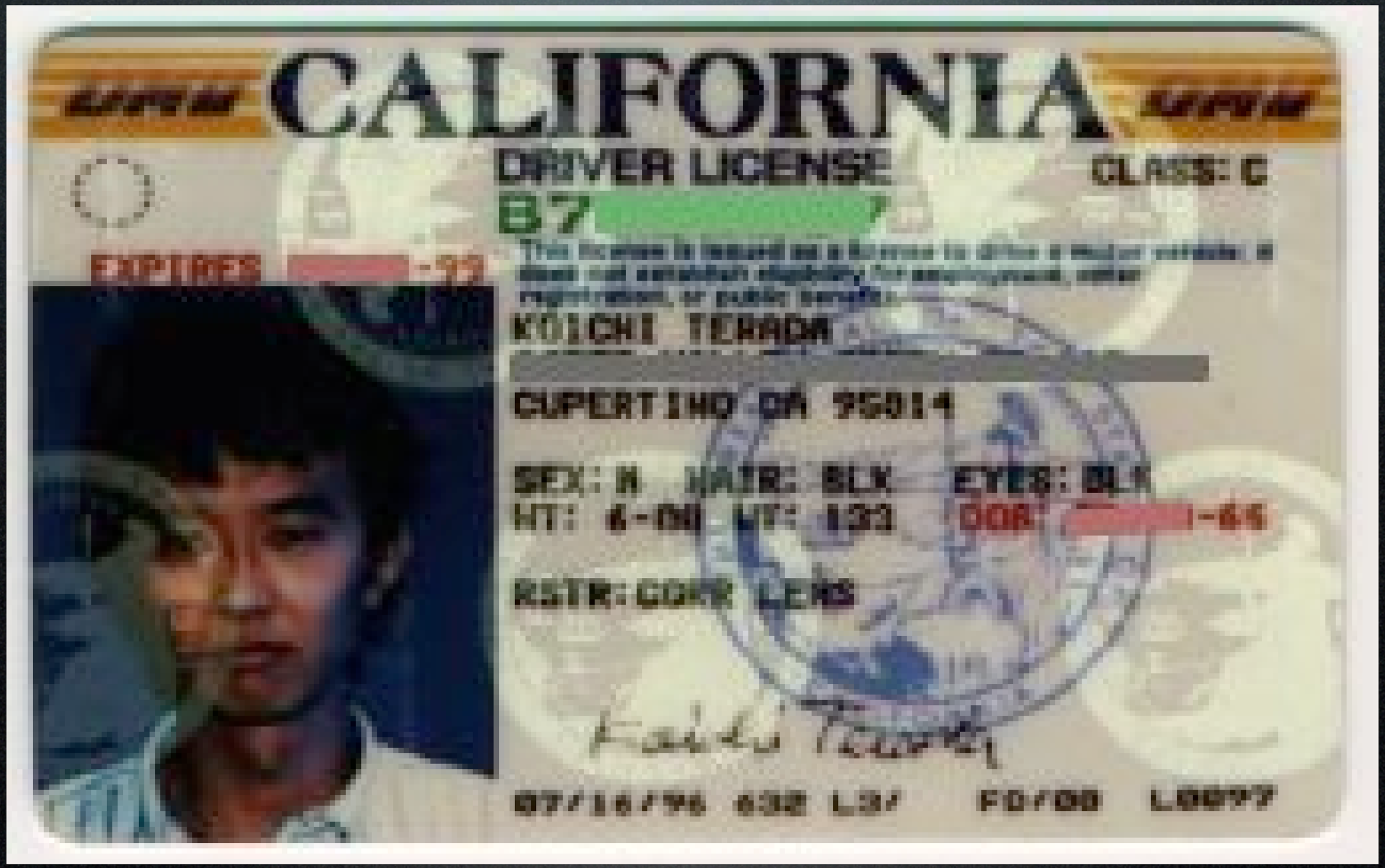
credentials

www.windley.com

One of these things is not like the others!

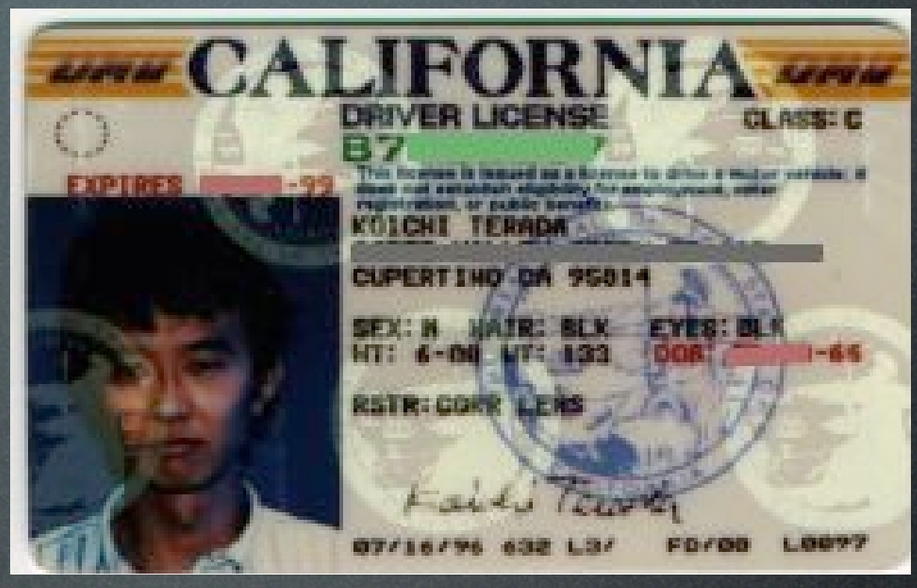


Credentials & Identity



www.windley.com

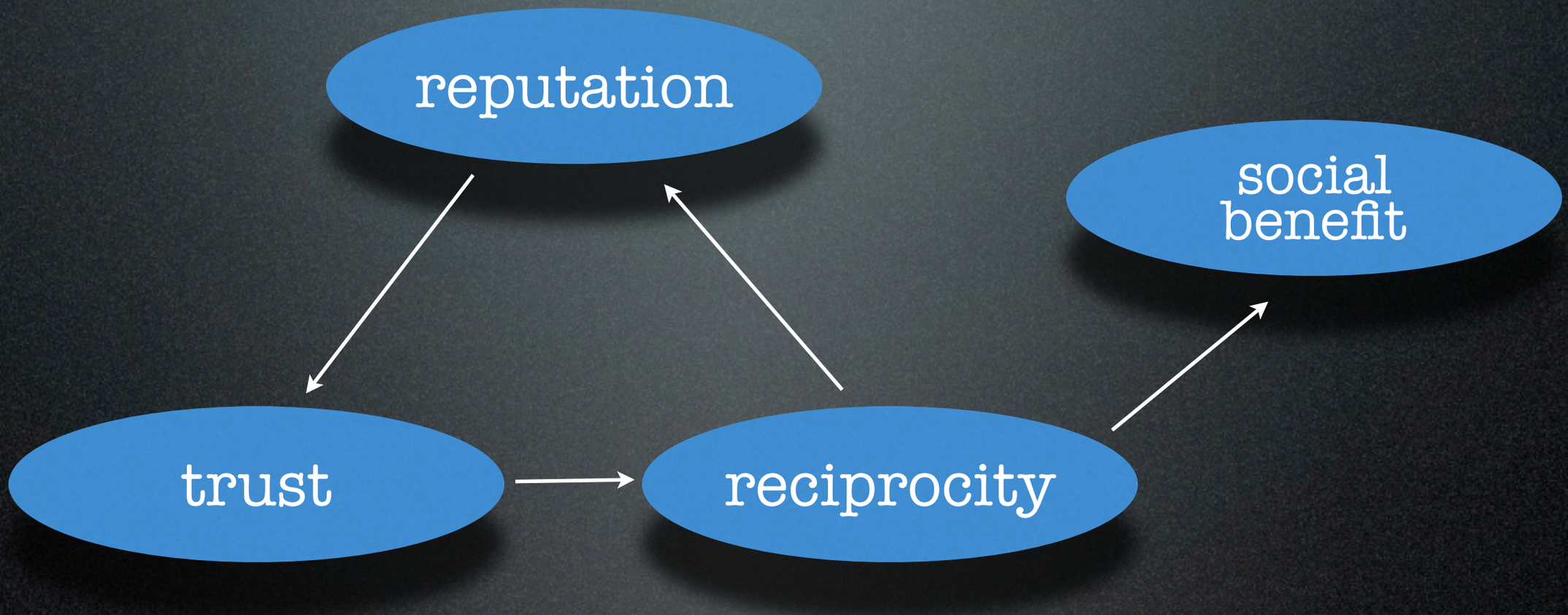
Buying Beer



www.windley.com

Accountability, Reputation, Privacy & Authorization

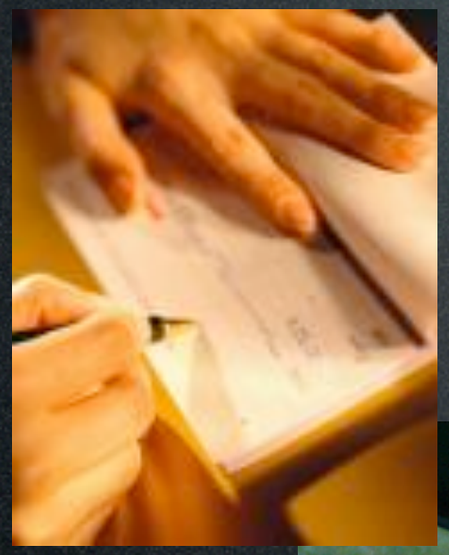
www.windley.com



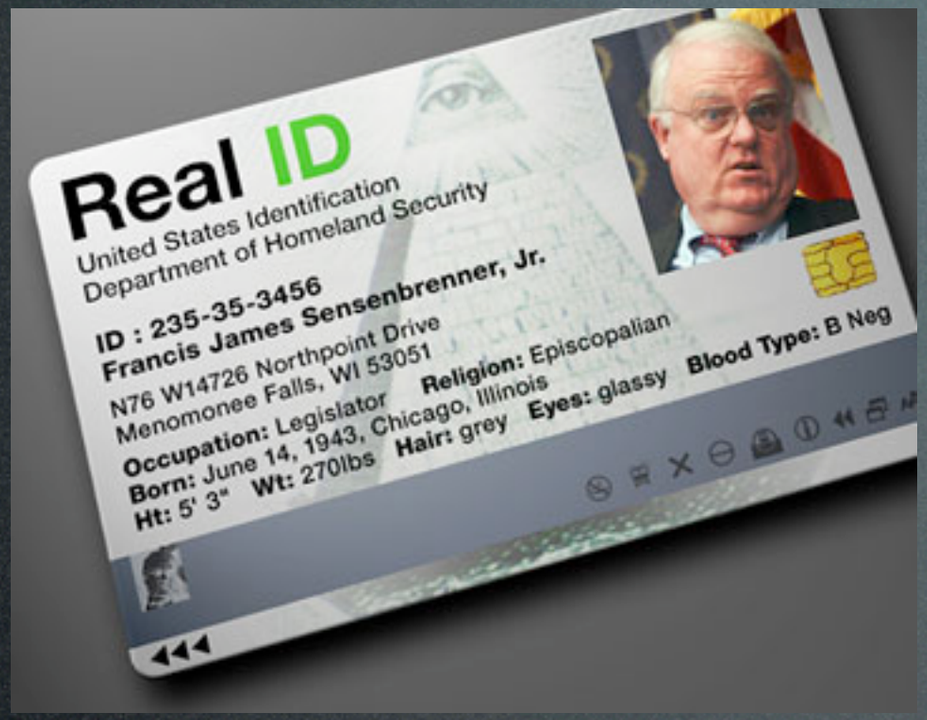
Mui et. al., A Computational Model of Trust and Reputation


STARBUCKS
COFFEE


STARBUCKS
COFFEE



www.windley.com


Real ID
United States Identification
Department of Homeland Security
ID : 235-35-3456
Francis James Sensenbrenner, Jr.
N76 W14726 Northpoint Drive
Menomonee Falls, WI 53051
Occupation: Legislator
Religion: Episcopalian
Born: June 14, 1943, Chicago, Illinois
Ht: 5' 3" Wt: 270lbs Hair: grey Eyes: glassy Blood Type: B Neg


PASSPORT
United States
of America

privacy

www.windley.com

privacy

www.windley.com

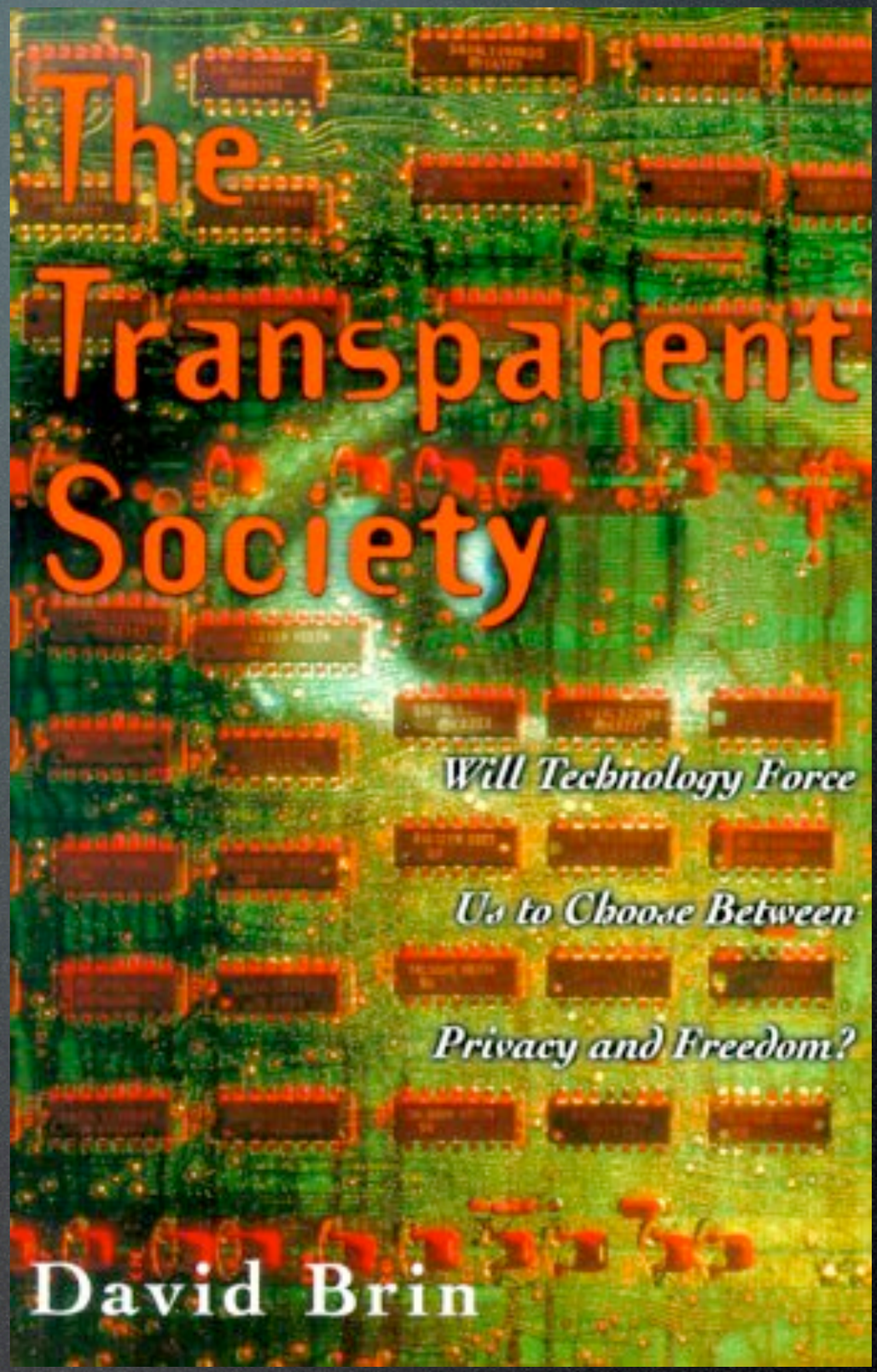
privacy

www.windley.com

YOU HAVE NO PRIVACY ANYWAY. GET OVER IT!

Scott McNealy,
CEO Sun

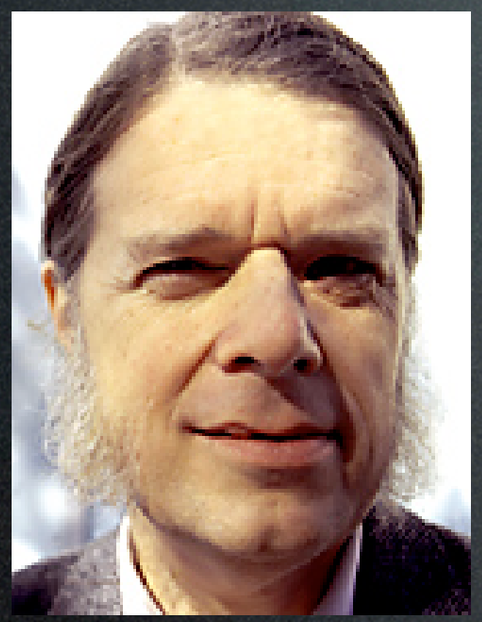
www.windley.com


The Transparent Society
Will Technology Force
Us to Choose Between
Privacy and Freedom?
David Brin

Accountability: Pick Two

1. Tools that help me see what others are up to.	2. Tools that prevent others from seeing what I am up to.
3. Tools that help others see what I am up to.	4. Tools that prevent me from seeing what others are up to.

Accountability vs. Enforcement



"Accountability is a log processing problem"

-Dan Geer

- Access control scales geometrically (its a multi-dimensional table)
- Accountability scales linearly
- Access control systems are incredibly vulnerable to DDoS attacks

anonyms and pseudonyms

CHEAP!!!

pseudonyms

Today
Only!!

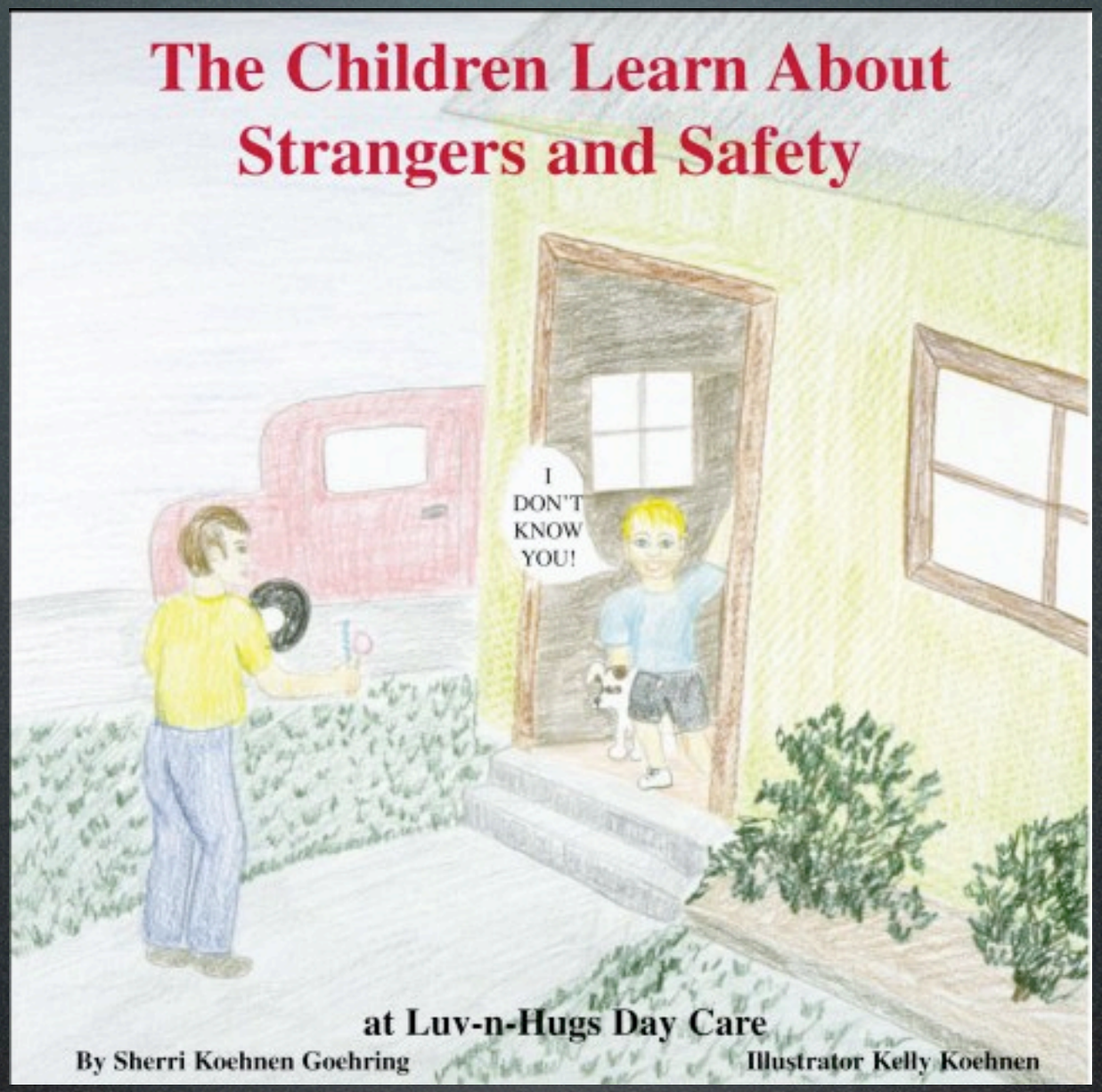
www.windley.com

positive reputations are valuable

negative reputations don't stick...

Pseudonym Strategies

Friedman and Resnick,
The Social Cost of Cheap Pseudonyms



Distrust Strangers

Make name changes costly

Commit to permanent names

www.windley.com

anonymity enables social good

Authorization

www.windley.com

Traditional View

- Enforcement
- U x R x A table
  - U => Users
  - R => Resources
  - A => Actions

Authorization Problems

- Scaling
  - Roles help
- Control of identities
  - Cheap pseudonym problem again
- Two ways to scale:
  - Accountability (audits)
  - Reputation

Examples

Authorization

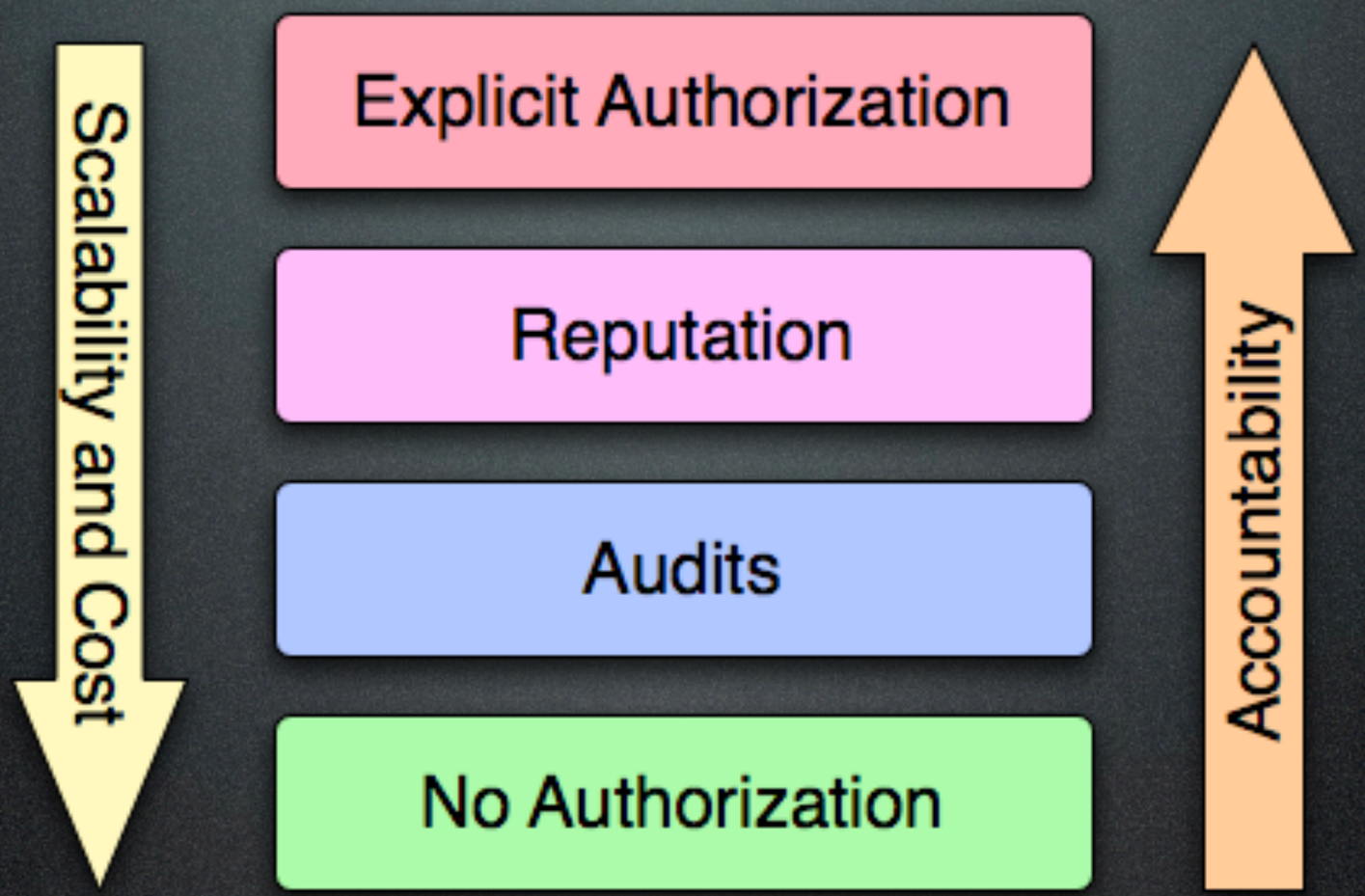
The Traditional View

Explicit Authorization

or

No Authorization

Authorization Hierarchy



Reputation

www.windley.com

your story about me

Principles of Reputation

Reputation should be user-centric

www.windley.com

Reputation has value

www.windley.com

Reputation is narrative and dynamic

www.windley.com

Reputation is based on identity

Reputation is based on claims, transactions & opinions

www.windley.com

Reputation exists within specific contexts

Reputation quality is an important metavalue

reputation vs. privacy

Linking Identifiers

Reputation context

www.windley.com

What are the semantics of the context and how are they expressed?

Plug-in

www.windley.com

Tags

Algorithm Design

www.windley.com

Can everyone really build their own algorithm?

Bootstrapping

www.windley.com

Recovery

www.windley.com

In real life people control their personal algorithm

Pythia is a vehicle for exploring reputation systems

www.windley.com

CS601

- Reputation theme
- Reviewed dozens of papers*
- Class project
- Agile methodology
- 3 two-week sprints
- 9 students

* Bibliography available on request

www.windley.com

Design Philosophy

www.windley.com

Reputation is a calculated score

www.windley.com

Support for multiple computational models

Support linking identifiers

Factors

- Verified claims and facts
- Direct and indirect transactions
- Opinions from third party network sources
  - No direct user opinions

Transparency

www.windley.com

- Important to give feedback
  - privacy & selective disclosure
- User can see
  - All transactions
    - All queries and results
- Aids user in determining what to disclose
- Future: Better feedback

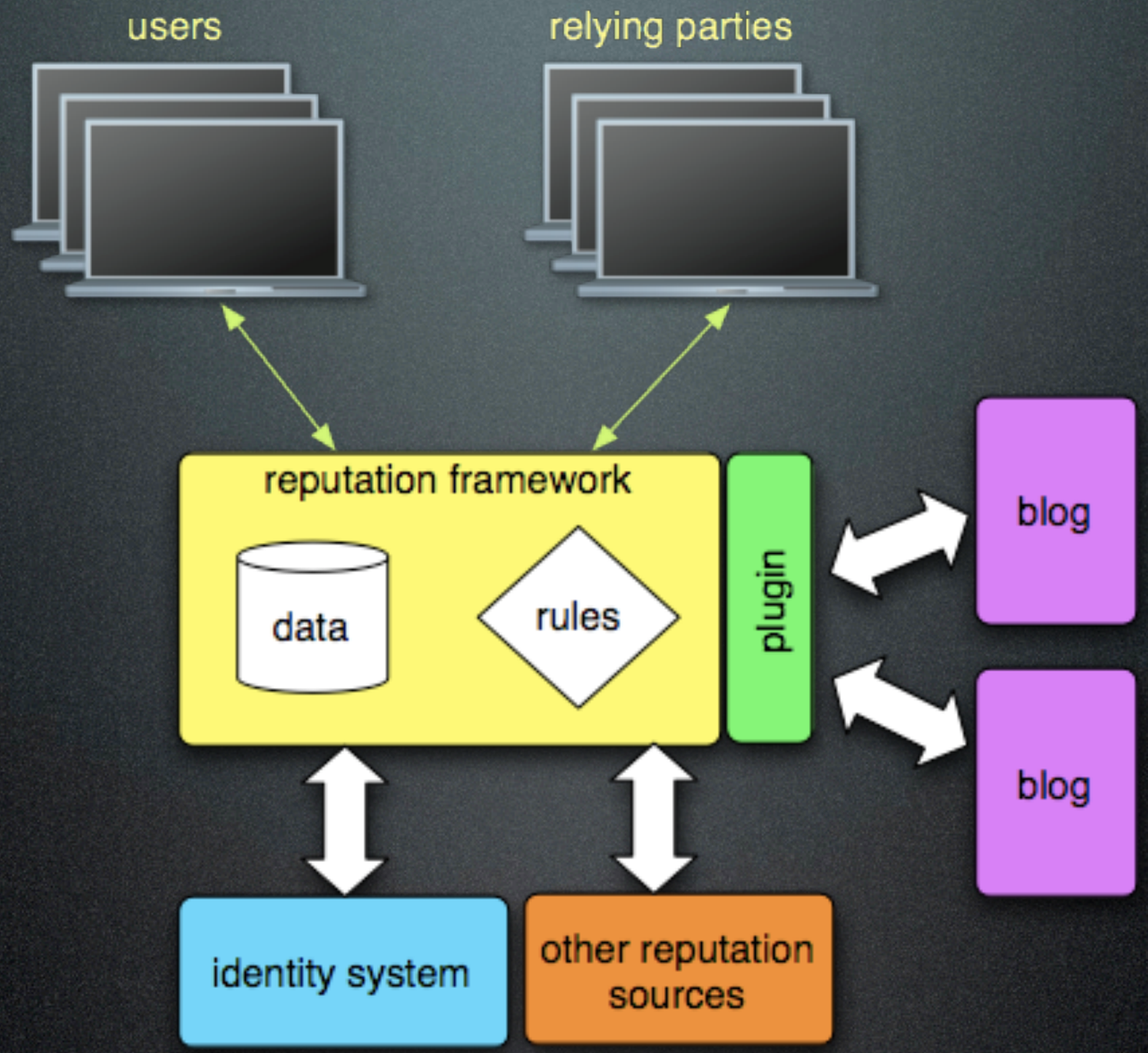
Transactions jointly

owned & immutable

www.windley.com

Current Architecture

- ID system neutral
  - Linking identifiers
- Data model for users and credentials
- Rules engine
- Tags (folksonomy) for transaction semantics
- Plug outs to online systems
  - Whois, Akismet for example
- Centralized



www.windley.com

Reputation as a substitute for authorization

www.windley.com

Why?

- Explicit authorization may not scale
- Explicit authorization may be too costly
- Explicit authorization may not be possible
- Explicit authorization may not suit product requirements

Blogs and MediaWiki

www.windley.com

user-centric identity

www.windley.com

An identity layer for the Internet

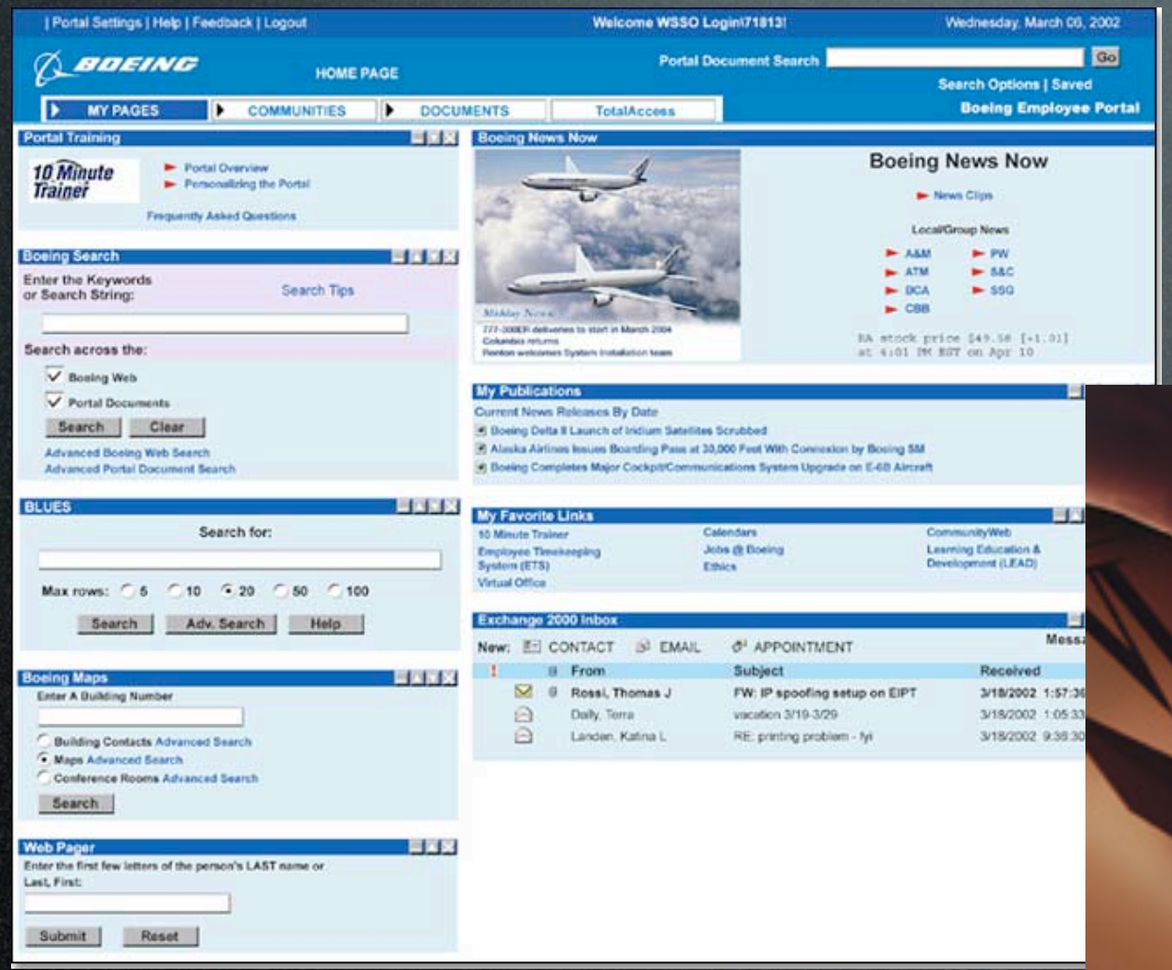
Vint Cerf

Cameron's Laws of Identity

1. User consent and control
2. Minimal disclosure
3. Justifiable parties
4. Directed identity
5. Pluralism
6. Human integration
7. Consistent experience across contexts

www.windley.com

Federation Problems



Linking 401K site to employee portals

www.windley.com

Roles

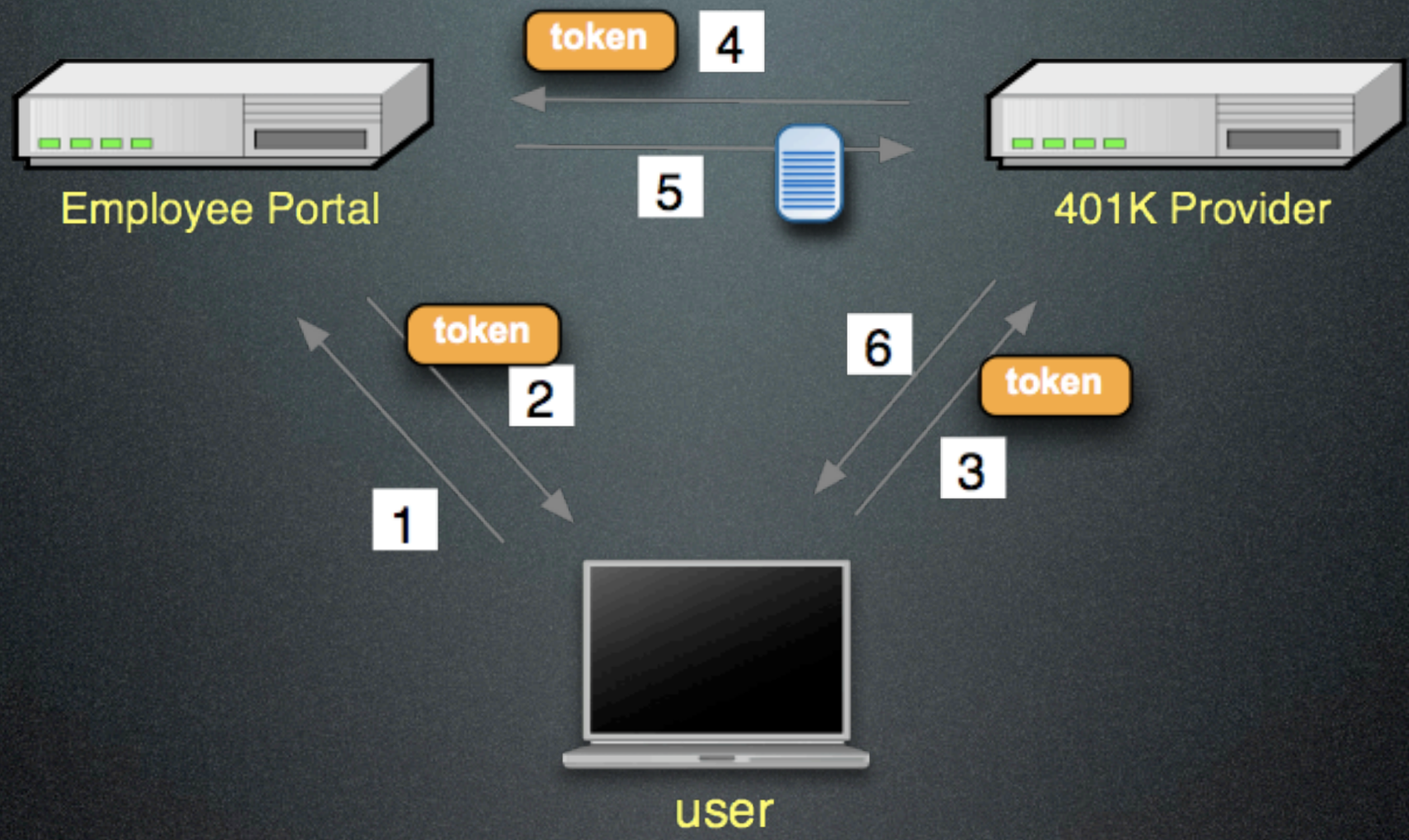
1. Identity Provider
2. Relying party

Roles

1. Identity Provider
2. Relying party
3. User

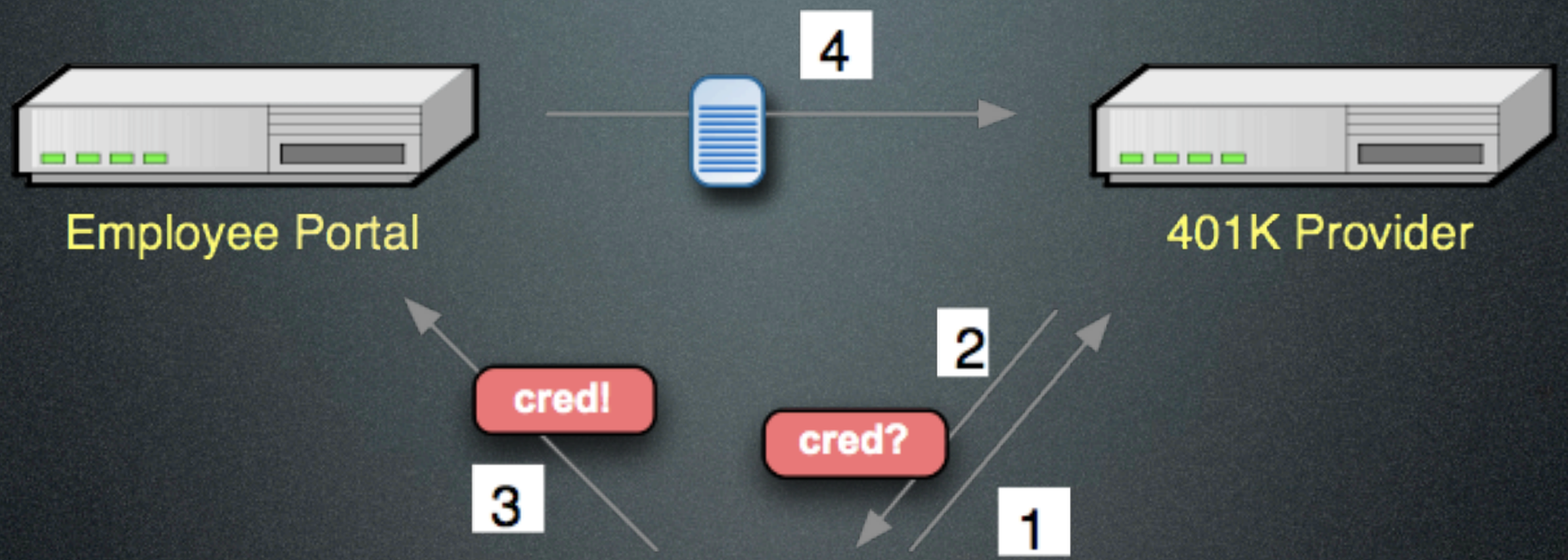
Identity Provider

- Provides testimony regarding the accuracy of claims
  - maintains records about a user
  - maintains account with the user
    - may assume liability
- Provides registration process for account establishment
- Provides authentication services
- User may act as their own identity provider



scenario one

- ID issuer and relying party have prior arrangement
- User is only involved peripherally and because of policy



scenario two

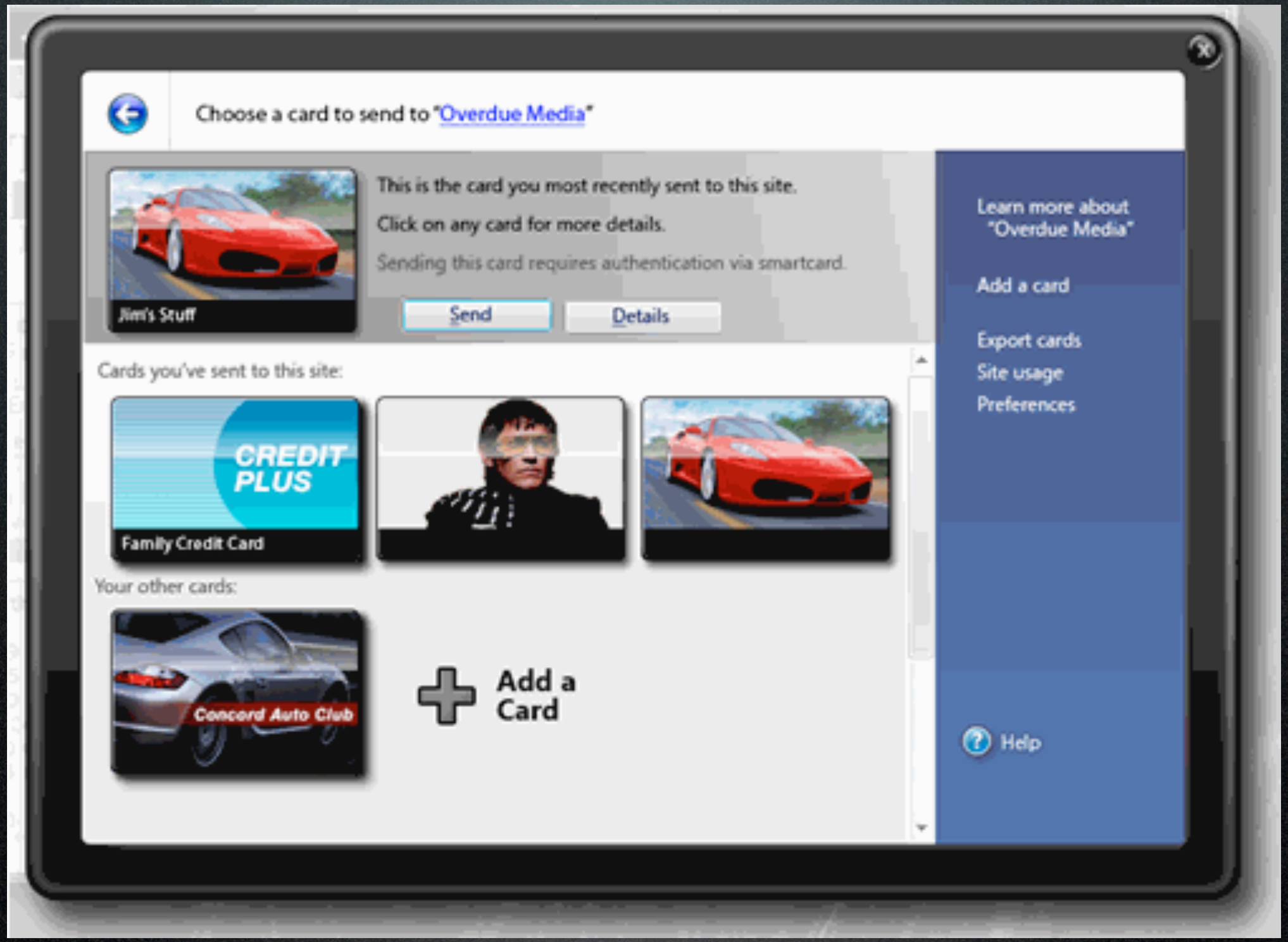
- ID issuer and relying party need no prior agreement
- User involved structurally

CardSpace

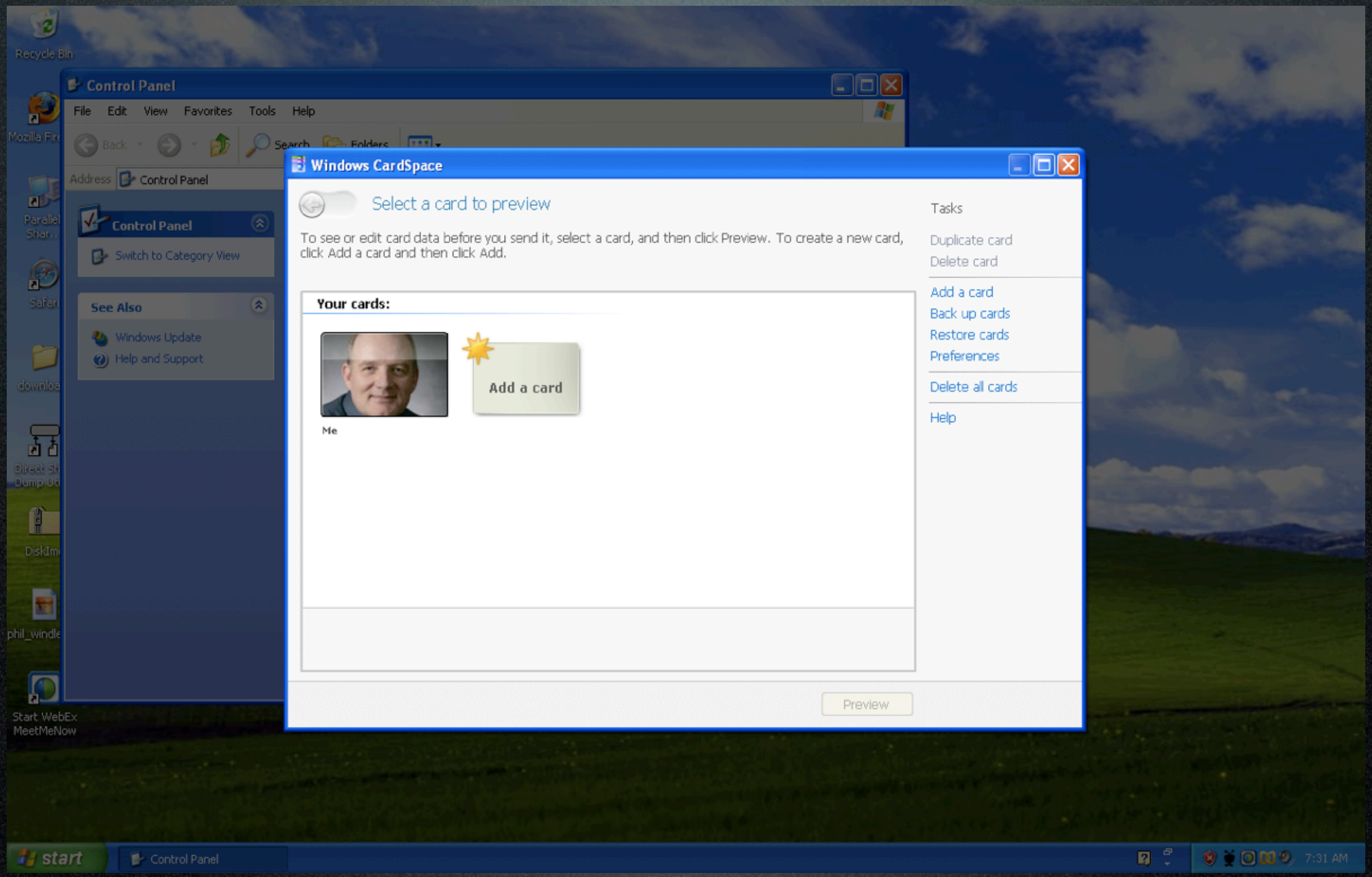
www.windley.com

CardSpace

- Open
- Decentralized
- Based on WS-* standards



CardSpace Identity Selector



CardSpace Identity Selector

CardSpace Screencast

www.windley.com

http://openid.aol.com/pjwindley

www.windley.com

http://www.windley.com

delegation

www.windley.com

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

Phil Windley's Technometria

http://www.windley.com/ RSS credit card

pwd Technometria UtahPolitics BTL ITC Blogtools BYU Mine HVC post to d SS Documentation Reader d Post to CiteULike

WINDLEY'S

TECHNOMETRIA

ORGANIZATIONS GET THE IT THEY DESERVE

TECHNOMETRIA
Home
Why Technometria?
RSS
Atom
Podcast Feed
add to MY YAHOO!
Recommend This Site

ABOUT PHIL
Brief Bio
Contact Info
(hCard)
Speaking
InfoWorld
Photo Albums
Video Favorites
CTO Breakfast

ESSAYS
2006
2005
2004
2003
CIO White Papers

SOFTWARE
Packages

June 22, 2007

Hard Choices

I'm trying to figure out:

1. Where's the best place near my house to get an iPhone?
2. Which of my kids should I make stand in line all day for me?

Sometimes being a Dad is tough work. If anyone has good intel on iPhone sources in Utah County, let me know.

Update: Near as I can tell, the AT&T store in American Fork will have them. Still checking.

Posted on 06:27 PM | Comments (1) | Recommend | Print
Add to del.icio.us | digg | Yahoo! MyWeb
Related: iphone mobile gear

iPhone Tour

I'm watching the 20 minute guided tour of iPhone that Apple posted today. While Amanda might be cheating the word "amazing" it's an excellent word to describe the phone this

MY TWITTERINGS

Phil Windley: In Denver. Finding food.

Phil Windley: headed to Denver. I'm giving the keynote at JA-SIG tomorrow

Phil Windley: back from a 50 mile bike ride in 103 degree temps. Good to be home.

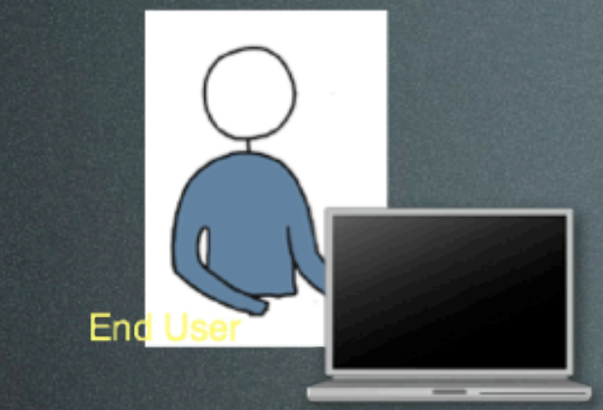
Phil Windley: Done with IT Conversatinos stuff I think it's time for the weekend.

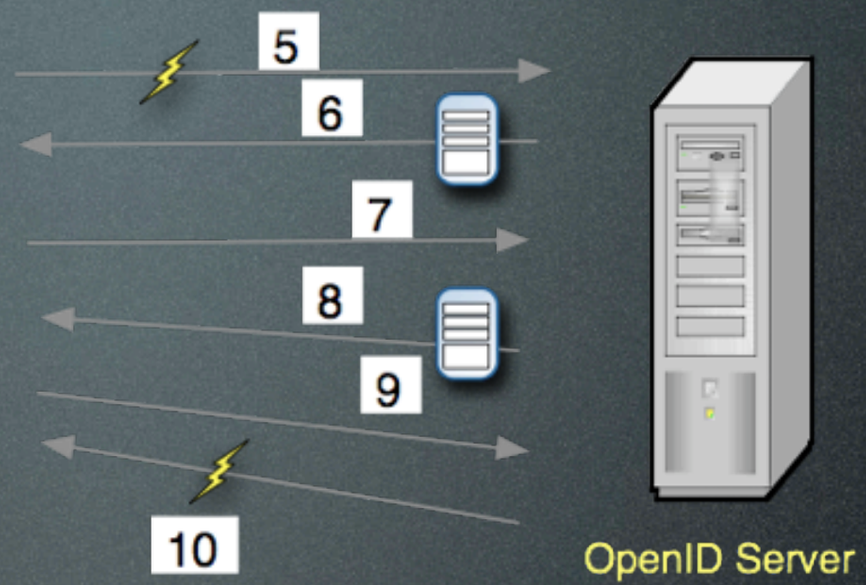
Phil Windley: back from picking oldest daughter up at camp. Done paying bills. Headed to work...

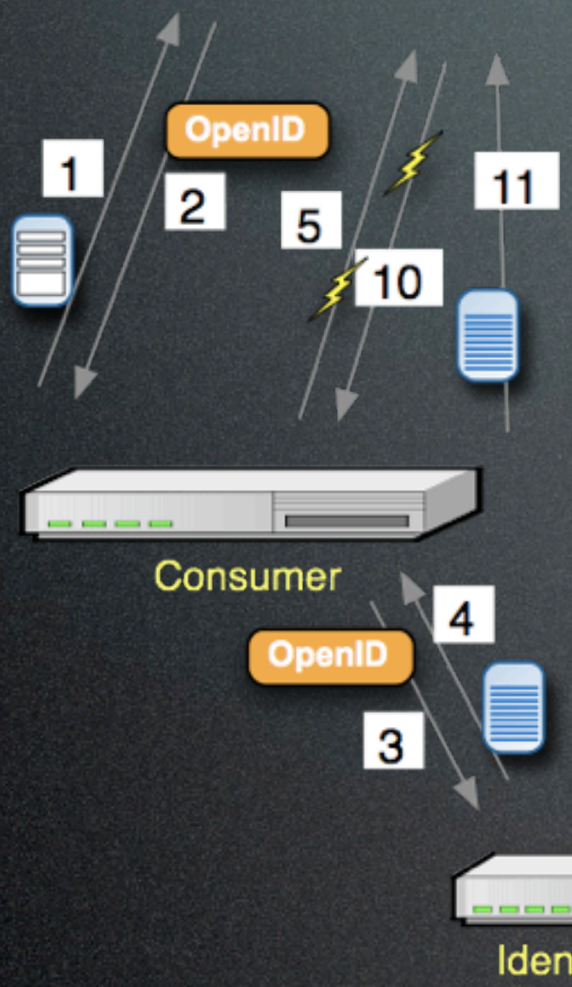
FREE NEWSLETTER!
email address
Sign me up!
(Find out more...)

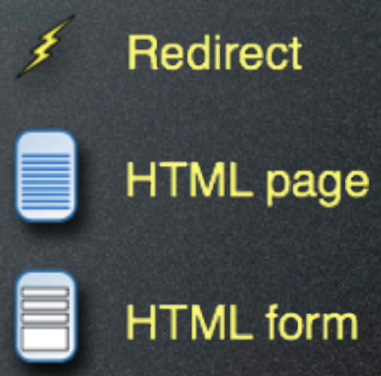
SEARCH
Search this site:
Search

OpenID Screencast



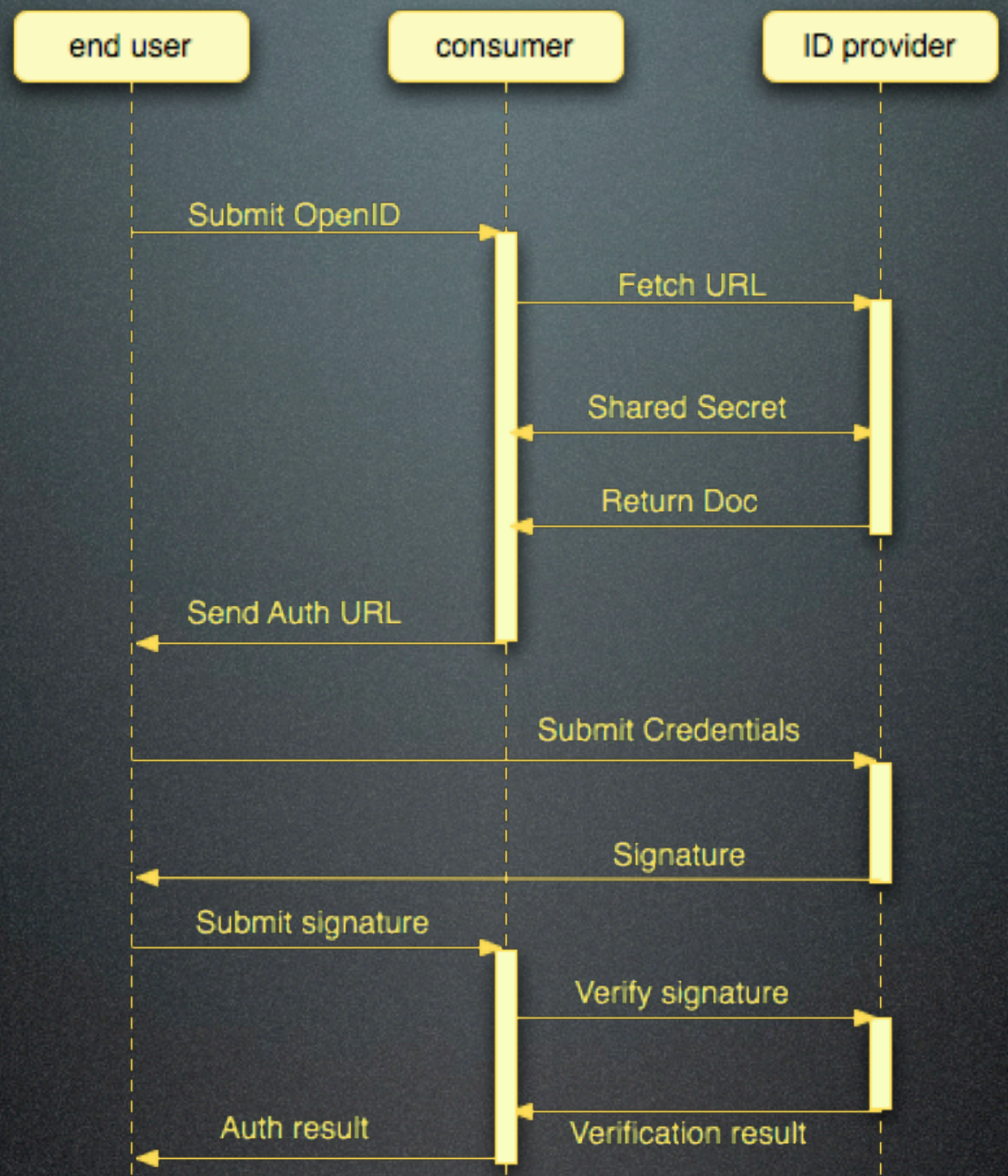






OpenID interactions

www.windley.com



OpenID Timeline

www.windley.com

Using OpenID

www.windley.com

Internal deployments useful for loosely coupled organizations

Authentication services prevent promiscuous password passing

User involvement mitigates trust issues

The Lay of the Land

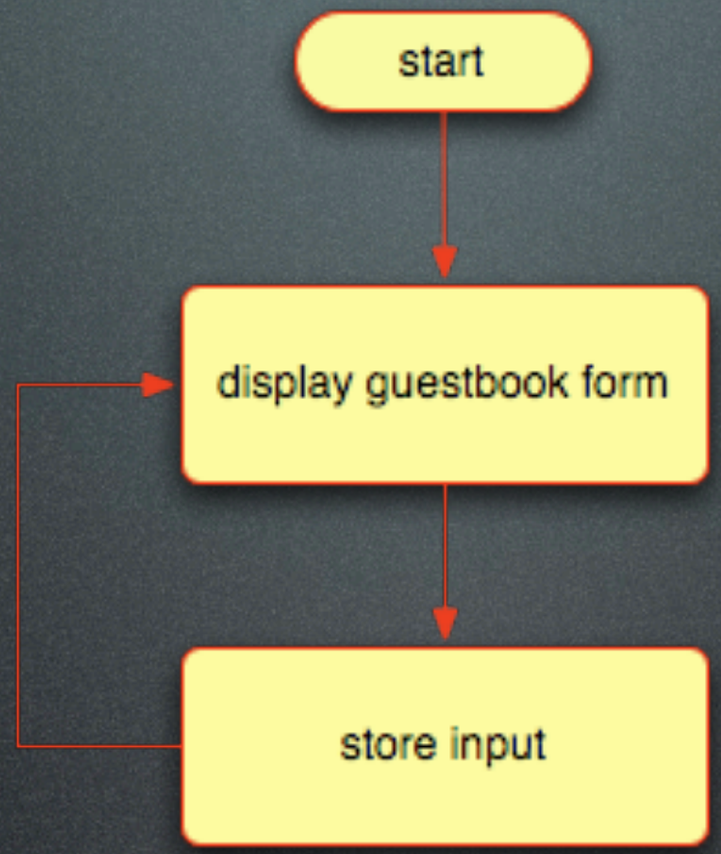
- AOL has become an OpenID provider
- AOL has NOT become an OpenID replying party

Who Pays?

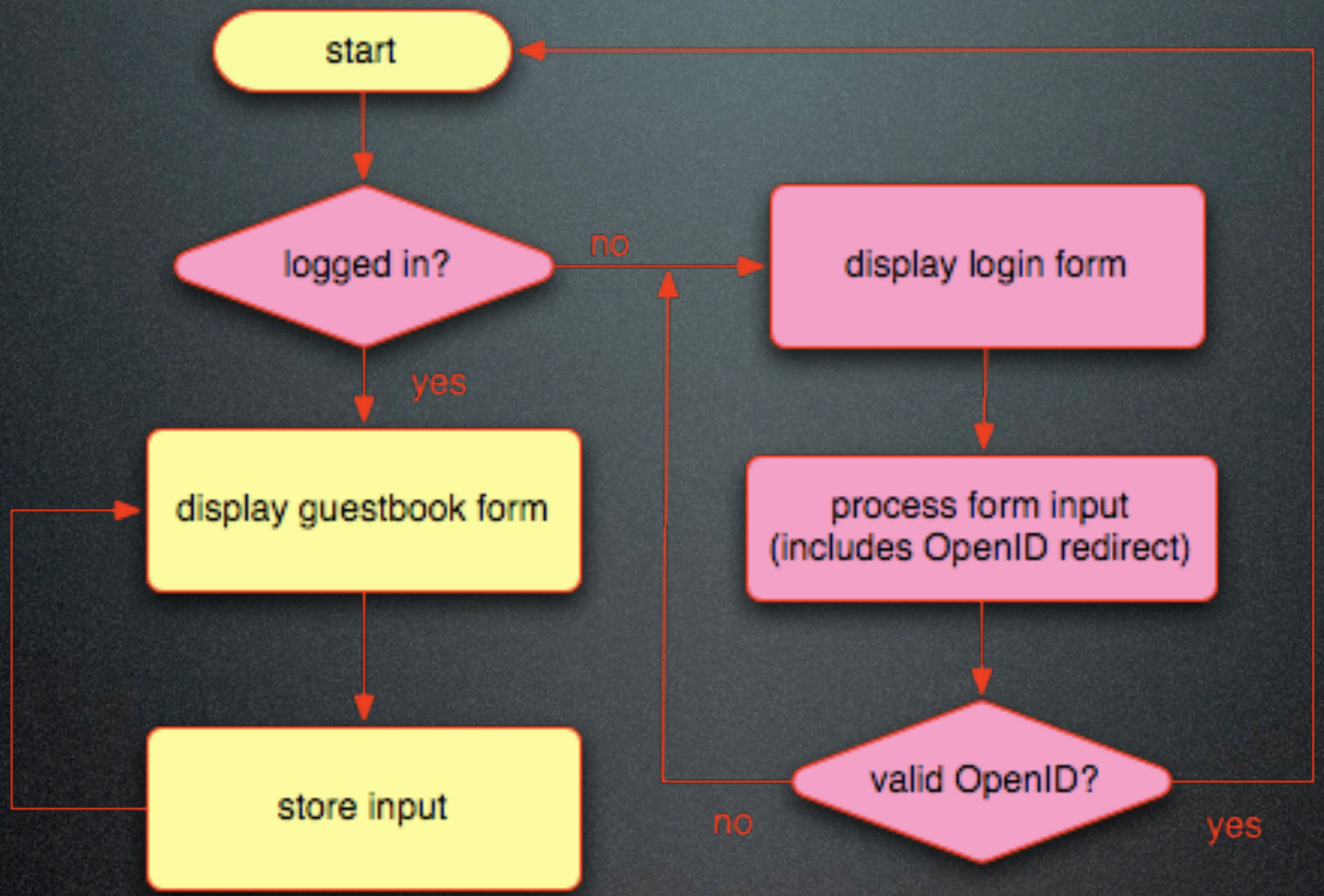
- Authentication will be free (mostly)
- Users will almost never pay
  - Notary services
- Relying parties will pay for
  - Advanced authentication services
  - Authorization, reputation, audits
  - Access to attributes

guestbook example: factoring out authentication

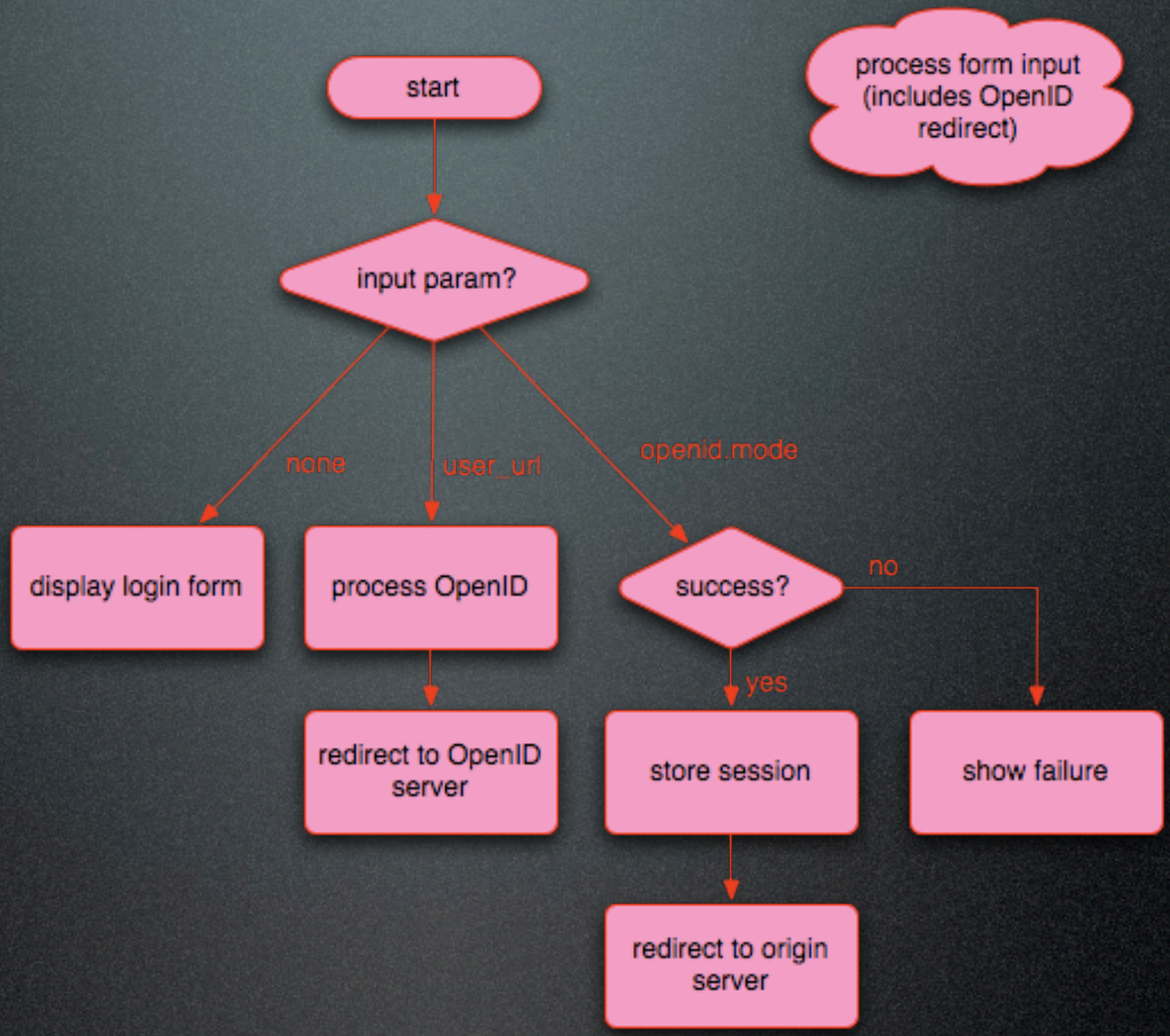
Simple Flow



Adding Authentication

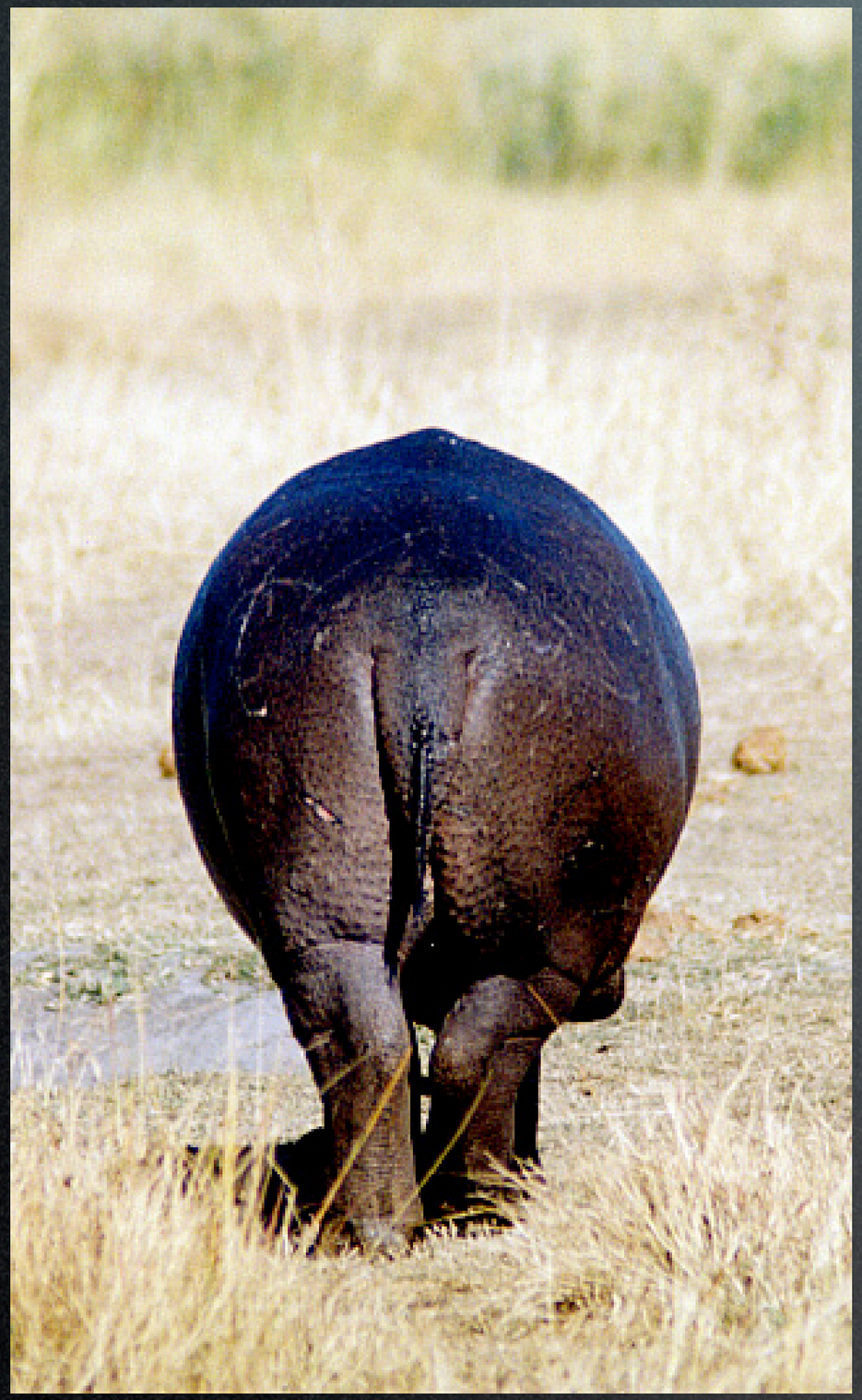


More Detail


process form input (includes OpenID redirect)
start
input param?
none
user_url
openid.mode
display login form
process OpenID
success?
no
yes
redirect to OpenID server
store session
show failure
redirect to origin server

demo time

www.windley.com



the end

Contact Information

Contact me

- phil@windley.com
- www.windley.com

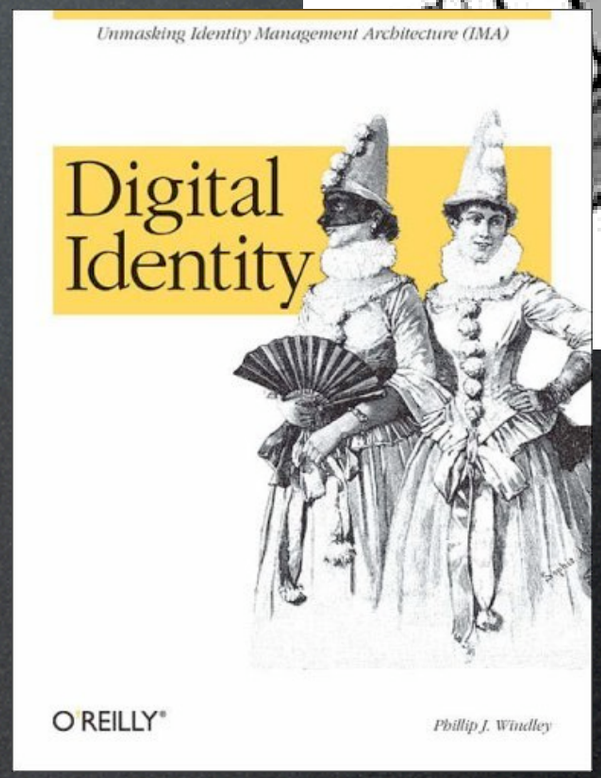
Questions?

Contact Information

Contact me

- phil@windley.com
- www.windley.com

Questions?



Contact Information

Contact me

- phil@windley.com
- www.windley.com

Questions?

Buy the book!!!