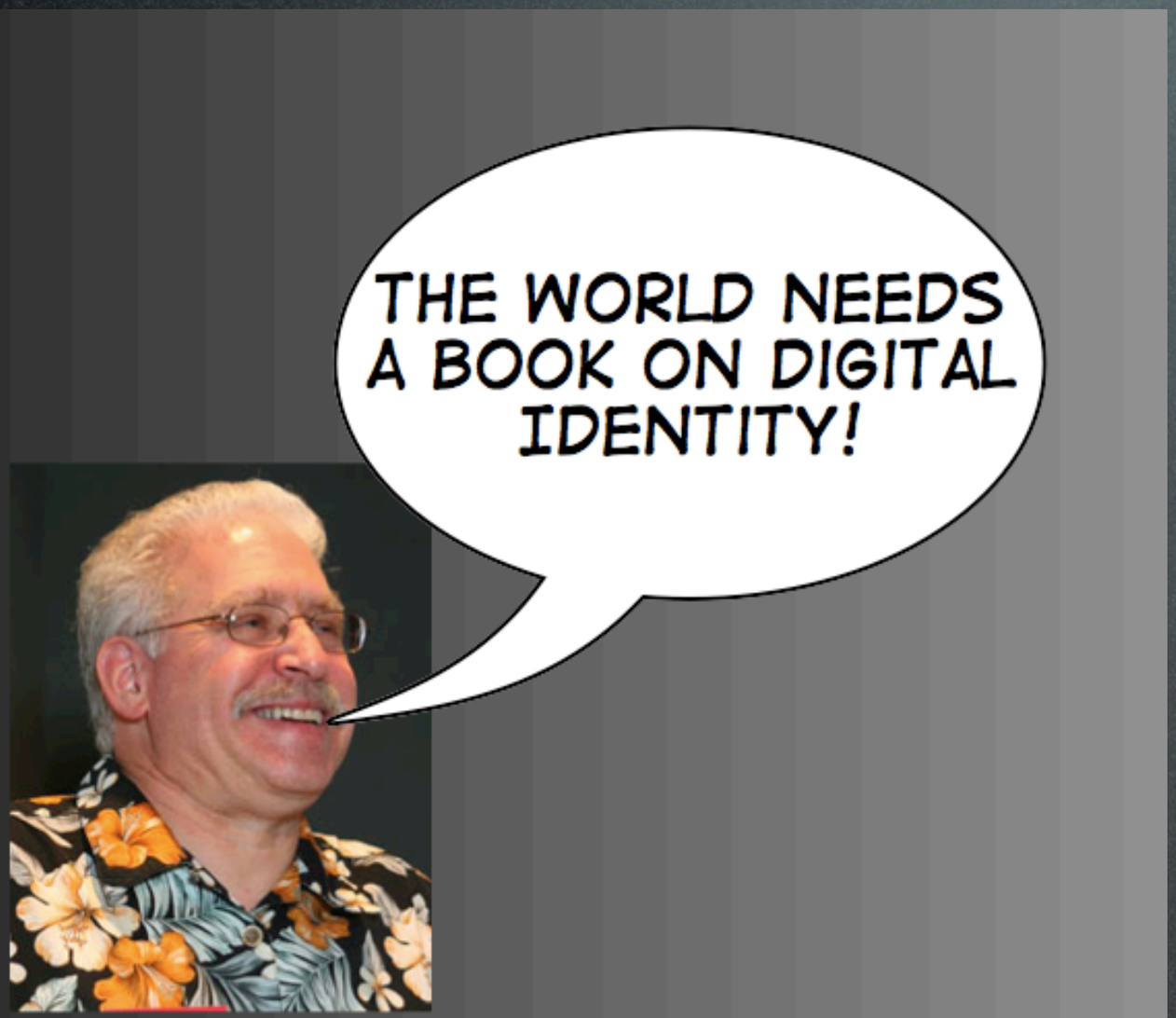
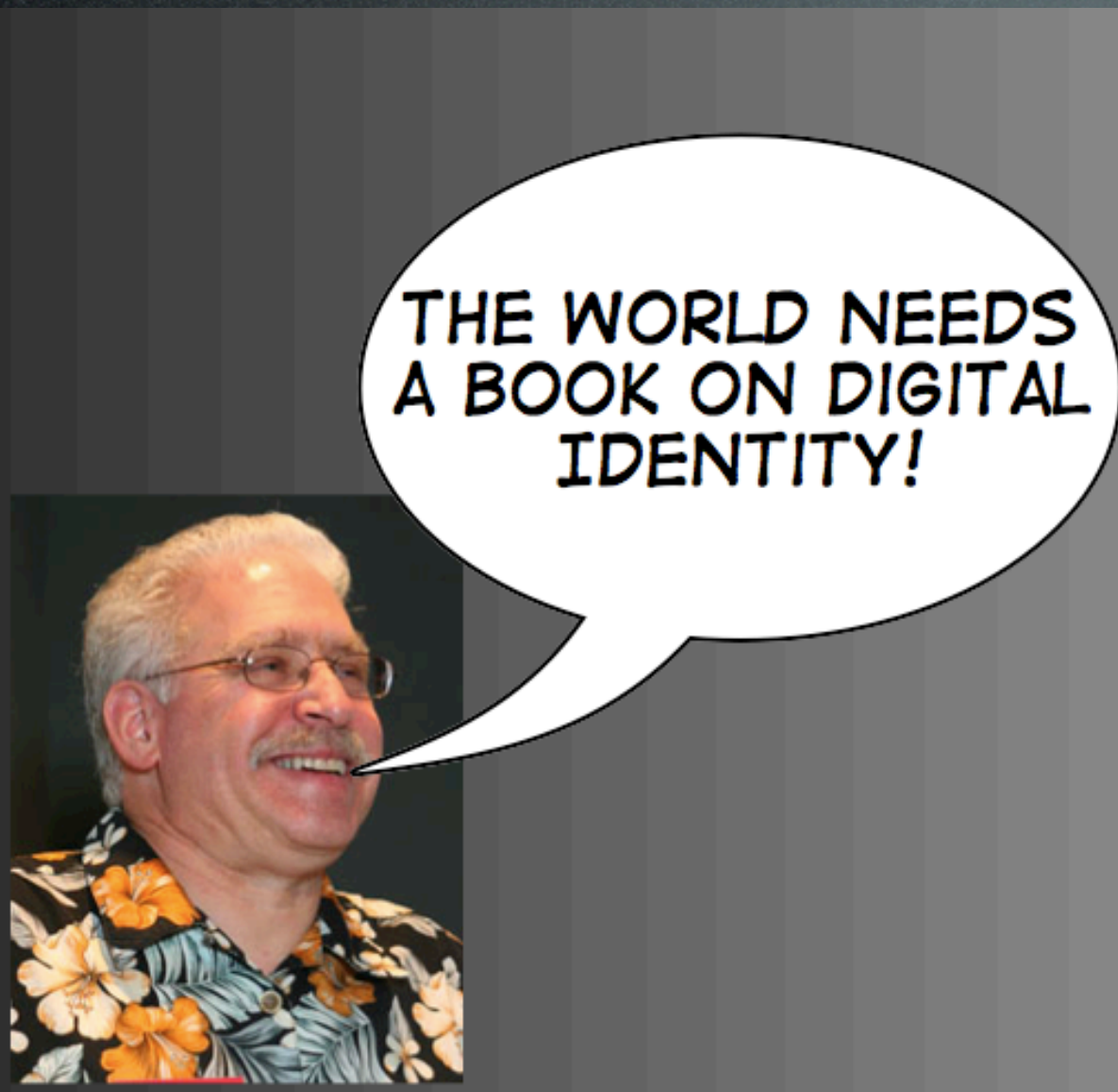
Digital Identity
Tutorial for WWW2007

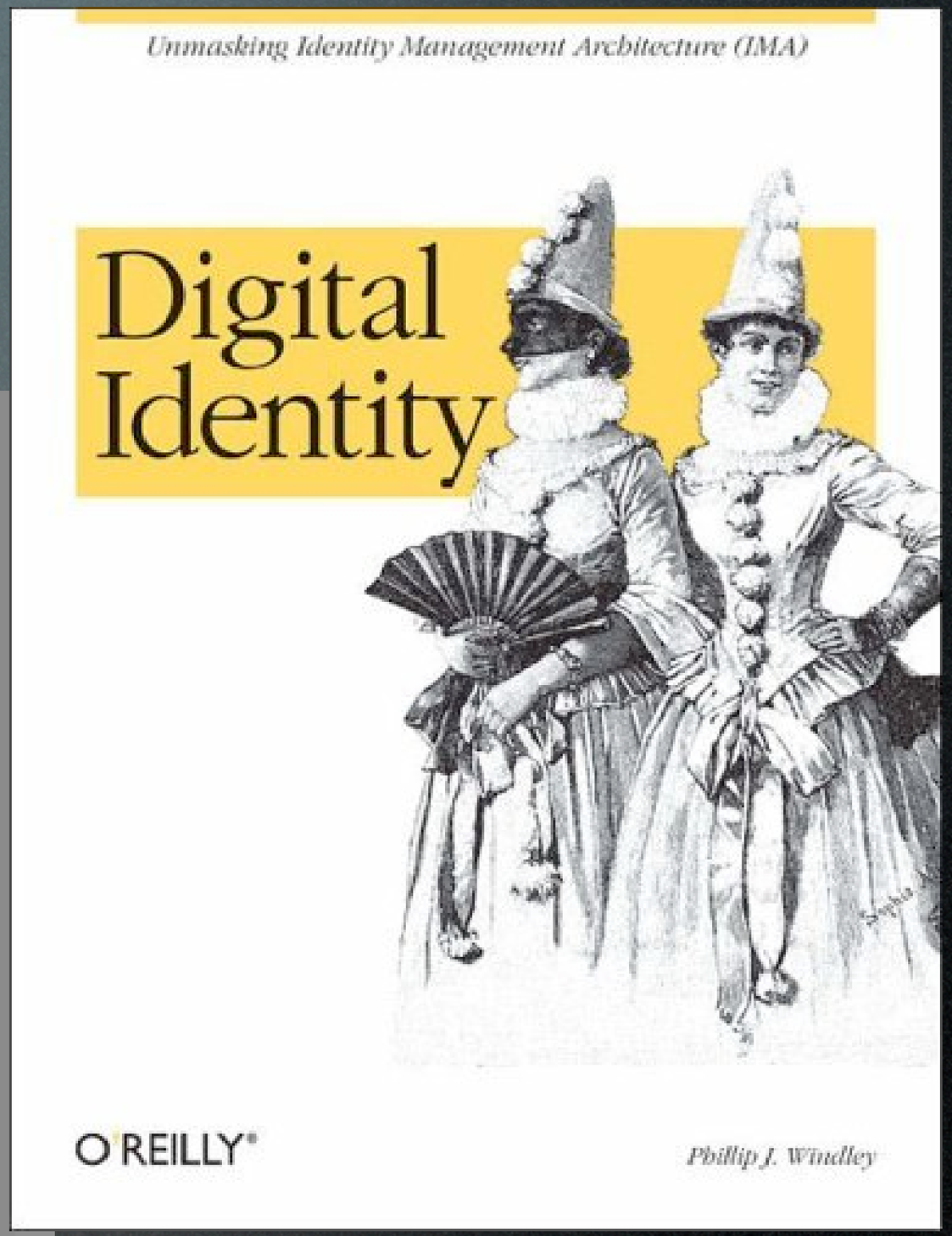
Phillip J. Windley
Brigham Young University

phil@windley.com
www.windley.com

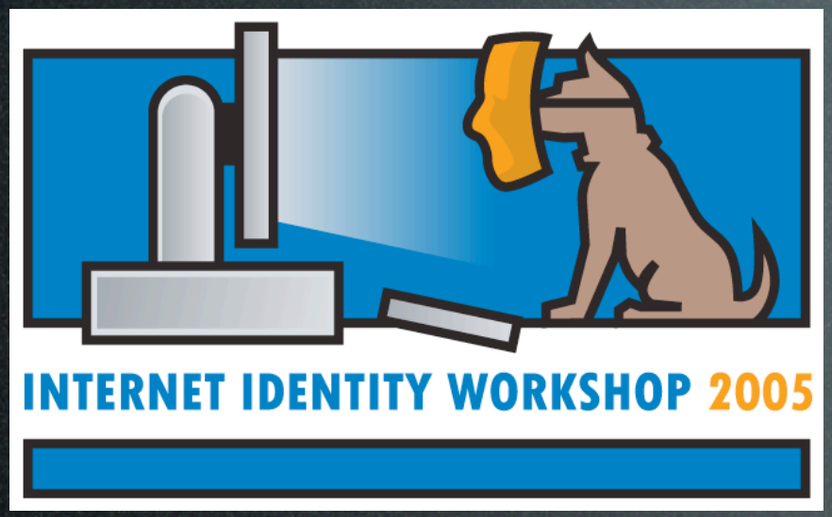


www.windley.com





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:

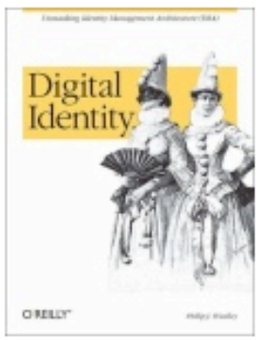
> *Native XmlDB Query Daemon is a client-server version of the Sleepycat native XML database deployed as an Apache module. The client is a pure Java API, supporting XQuery, XPath, and an Xml:DB API layer. It comes with a graphical admin console. Server binaries are provided for Linux x86 and x86-AMD64; 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

the identity of entries

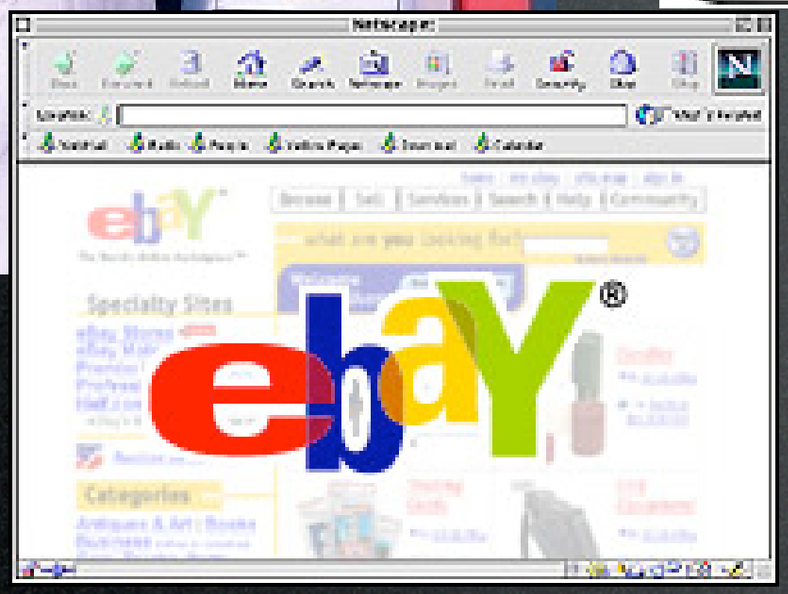
enables conversation

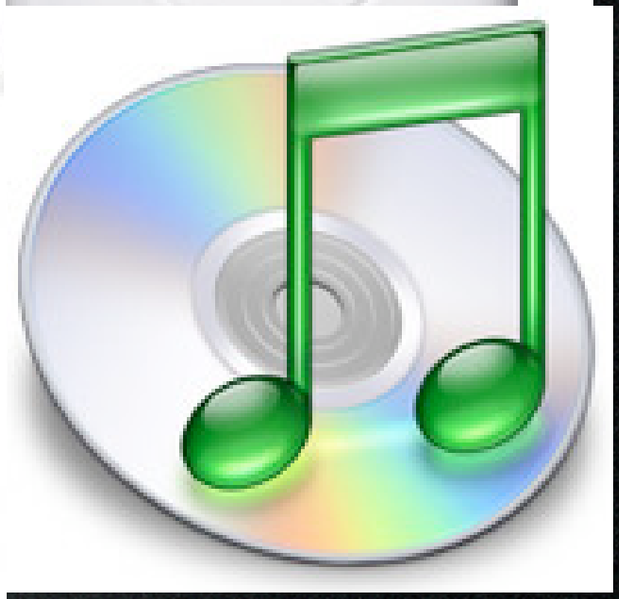
Does Identity Matter?

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?

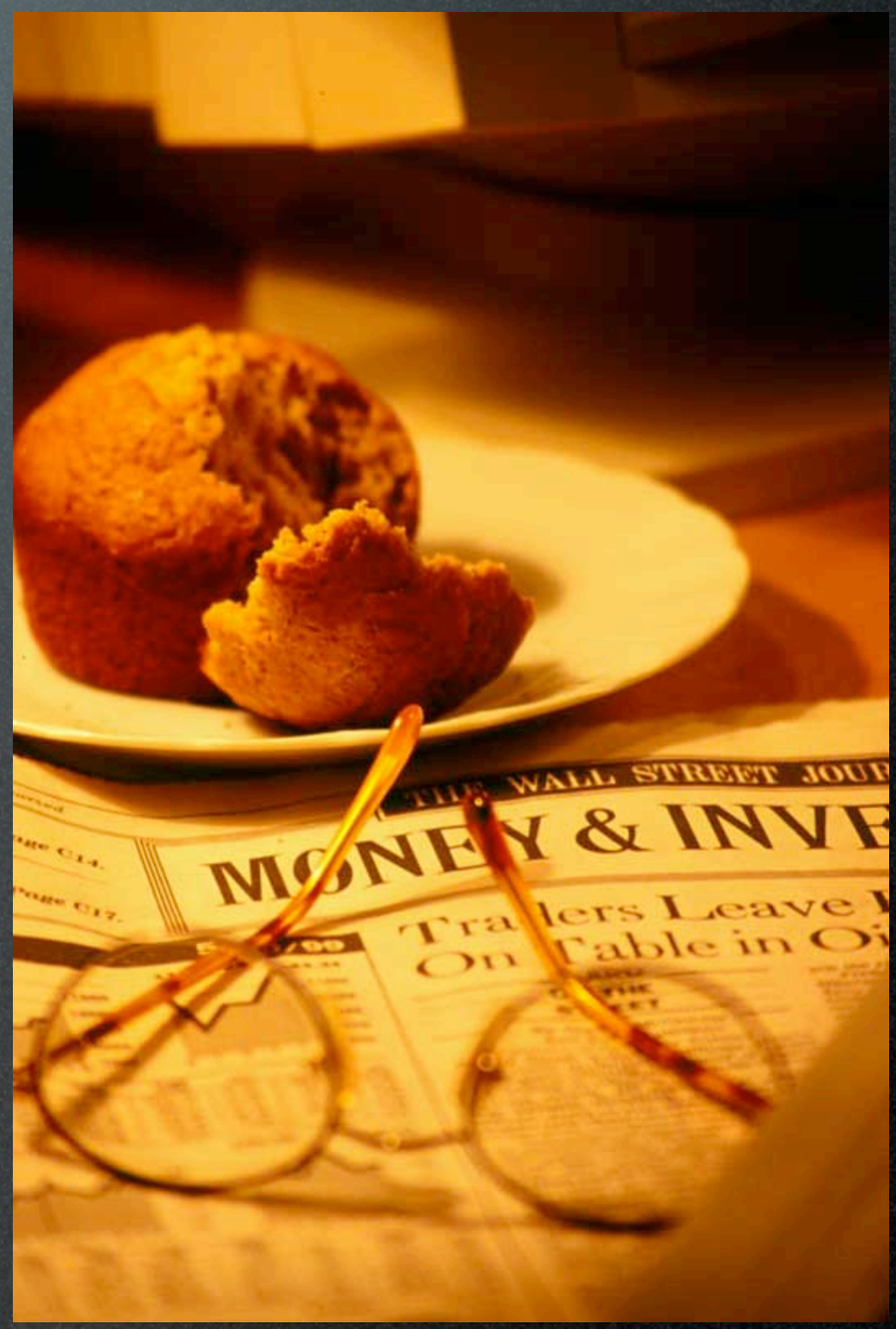
www.windley.com

The Border Patrol

www.windley.com

Business Context of Identity

vs



www.windley.com

identifiers

www.windley.com

what's in a name?

Samantha

Matsuhiro

Fred

Alice

George

Greta

Steve

Cindy

Kristen

Lynne

Betty

Monty

Phil

Tonya

Rumplestiltskin

3 Phillip Windleys

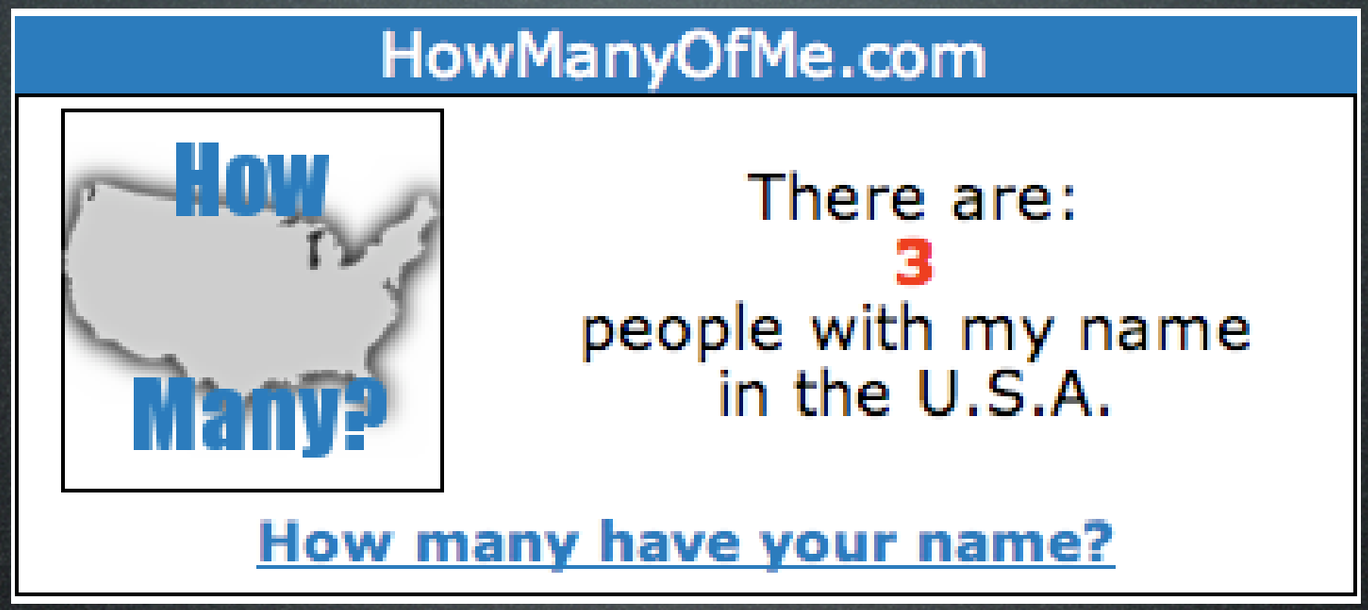
HowManyOfMe.com

There are:
3
people with my name
in the U.S.A.

How many have your name?

www.windley.com

3 Phillip Windleys



50,000 John Smiths

phil@windley.org

windley.com

http://www.windley.com/essays

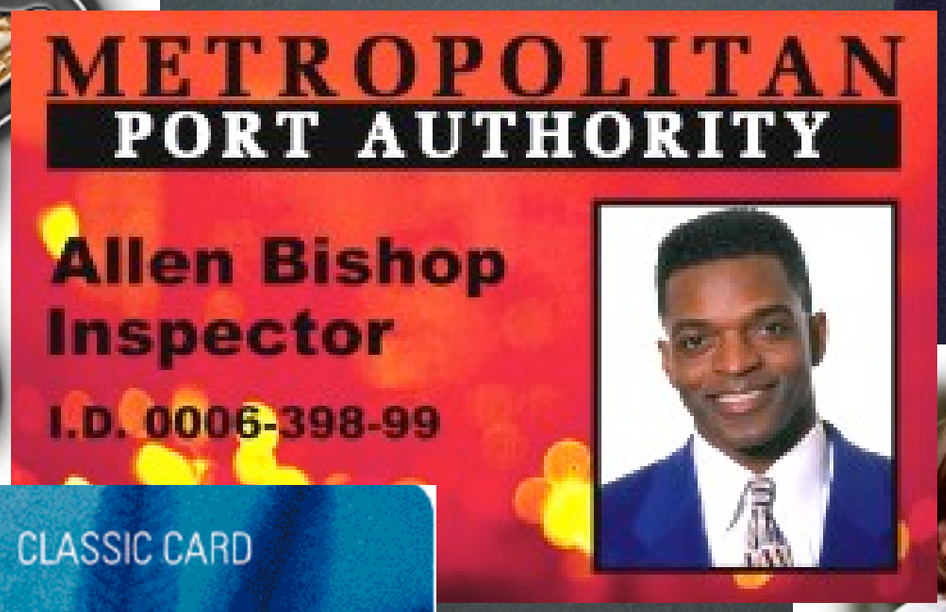
xri://=windley

www.windley.com

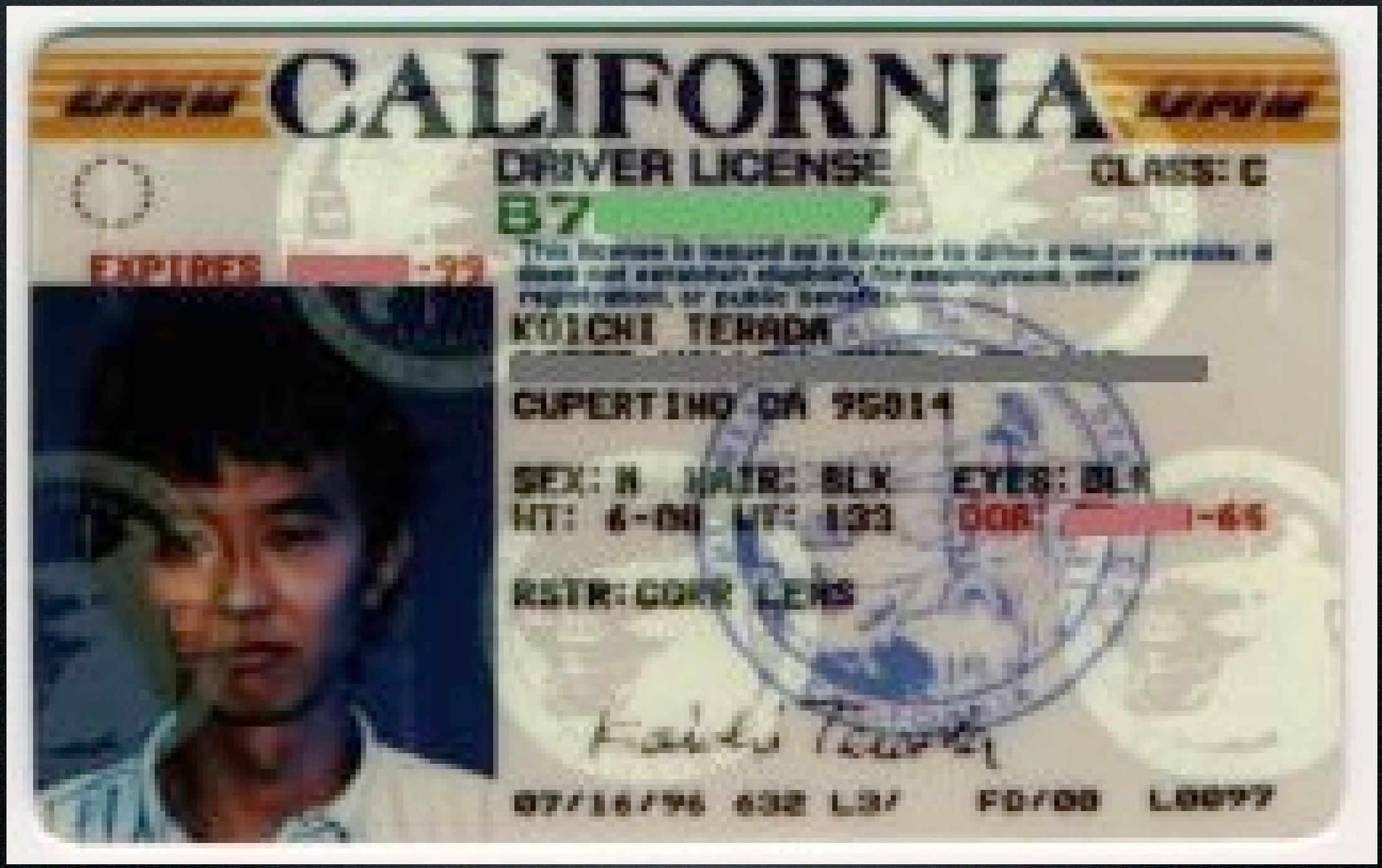
credentials

www.windley.com

One of these things is not like the others!

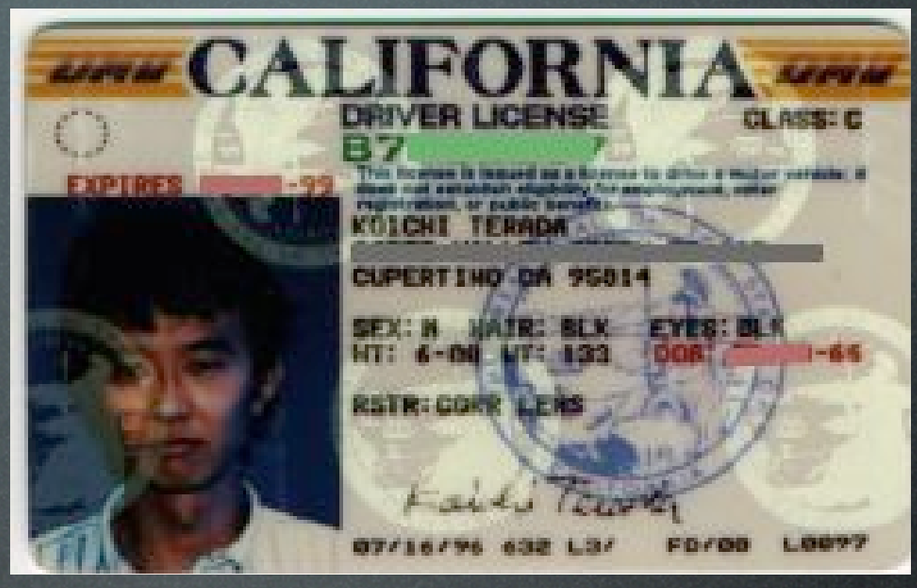


Credentials & Identity



www.windley.com

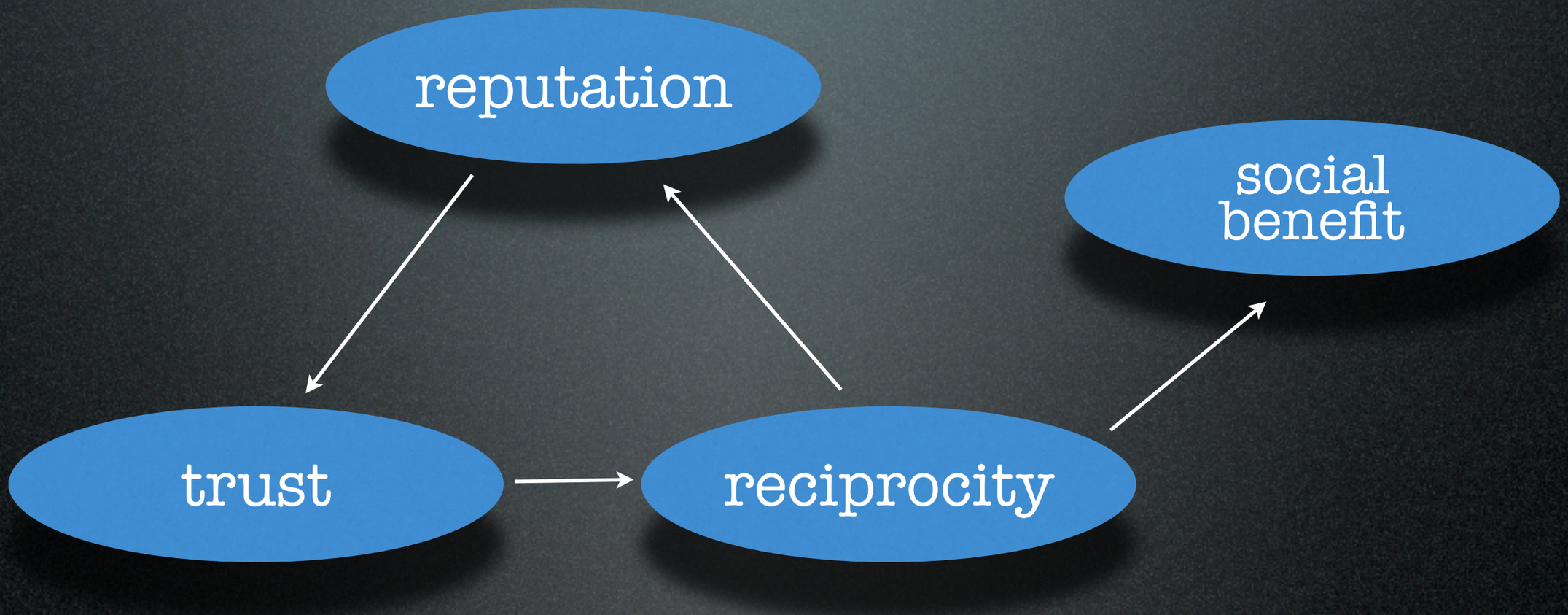
Buying Beer



www.windley.com

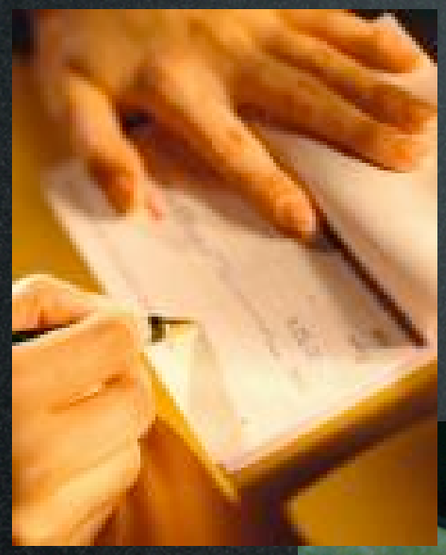
accountability & reputation

www.windley.com

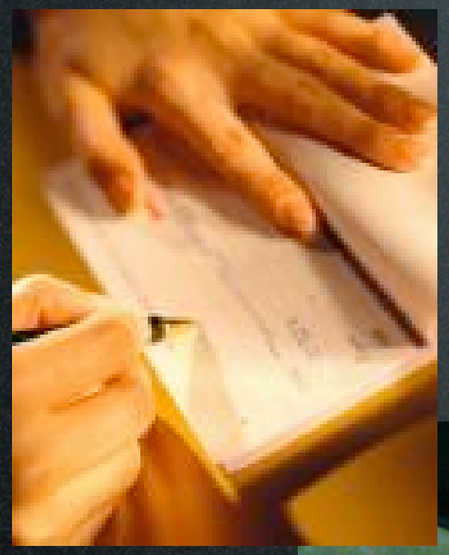


Mui et. al., A Computational Model of Trust and Reputation


STARBUCKS
COFFEE

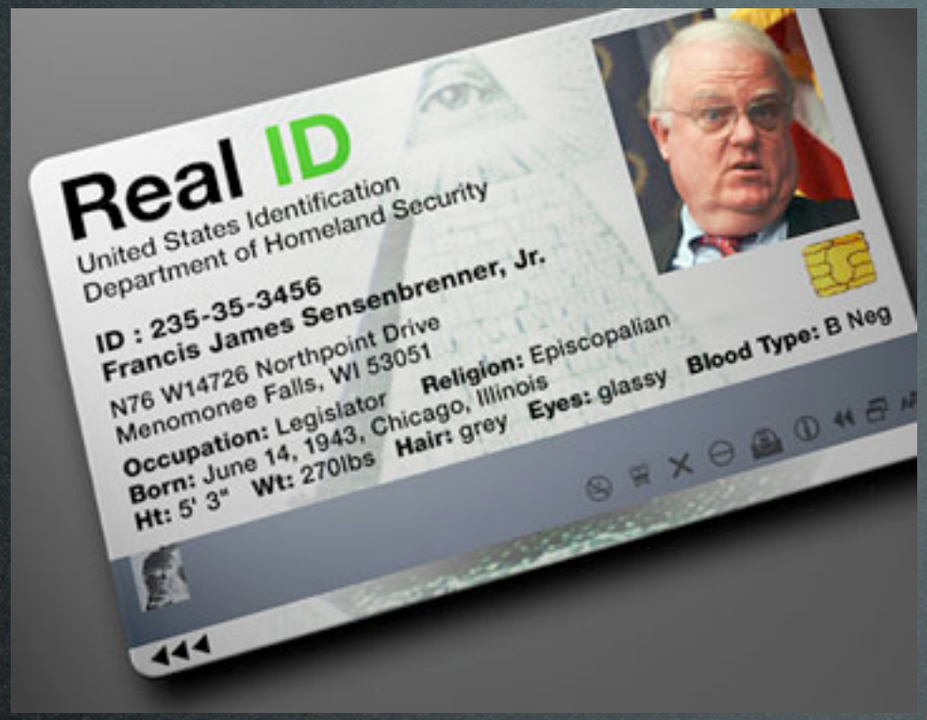


www.windley.com




STARBUCKS
COFFEE


PASSPORT
United States
of America


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

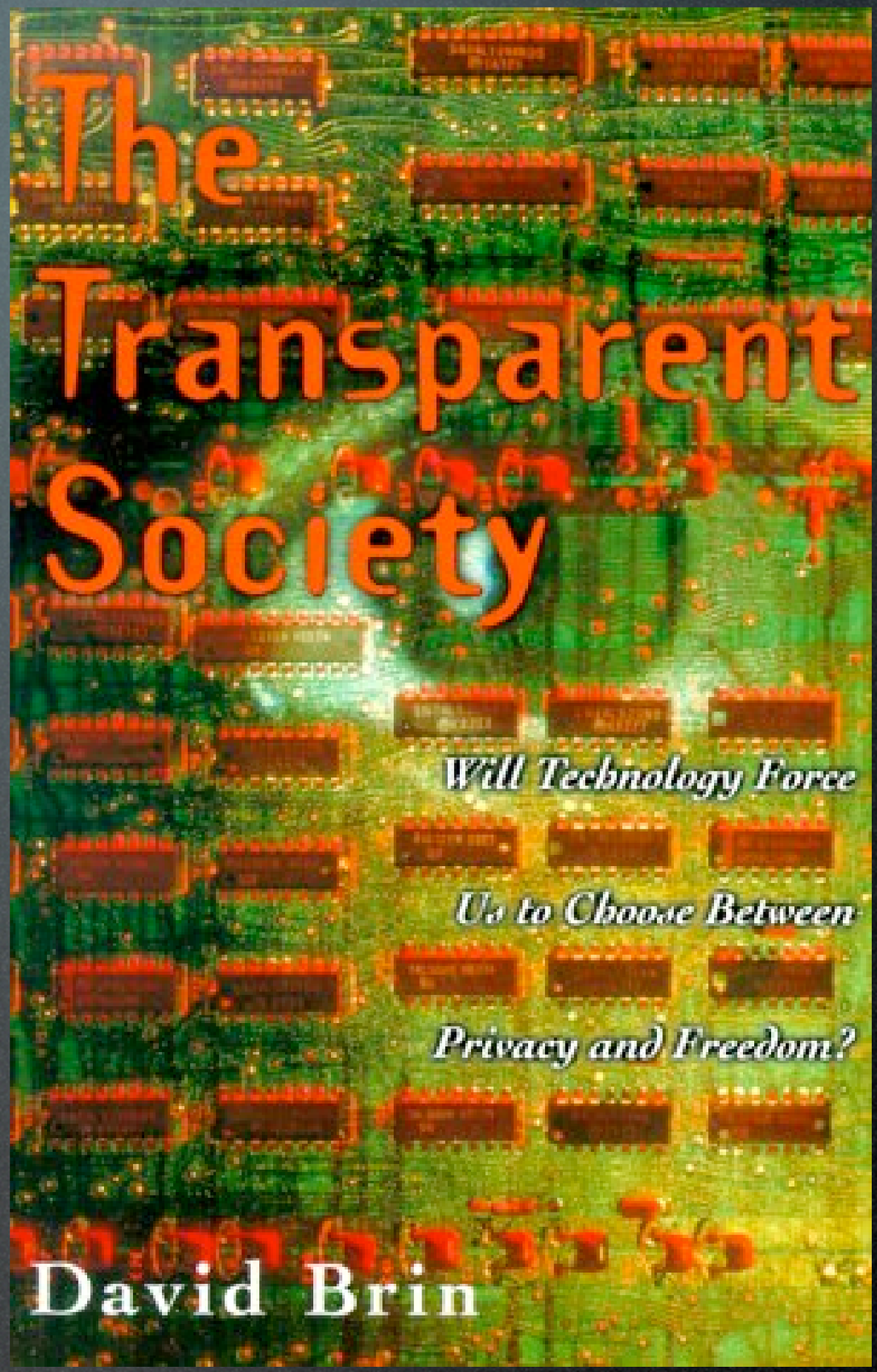
privacy

www.windley.com

YOU HAVE NO PRIVACY ANYWAY. GET OVER IT!

Scott McNealy,
CEO Sun

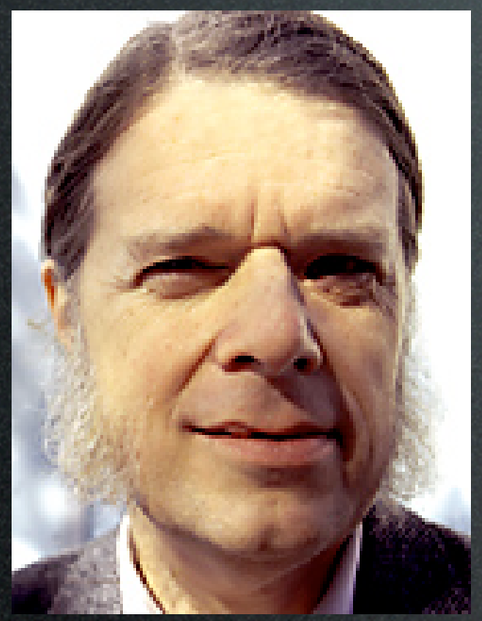
www.windley.com


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

anonymity enables social good

anonyms and pseudonyms

CHEAP!!!

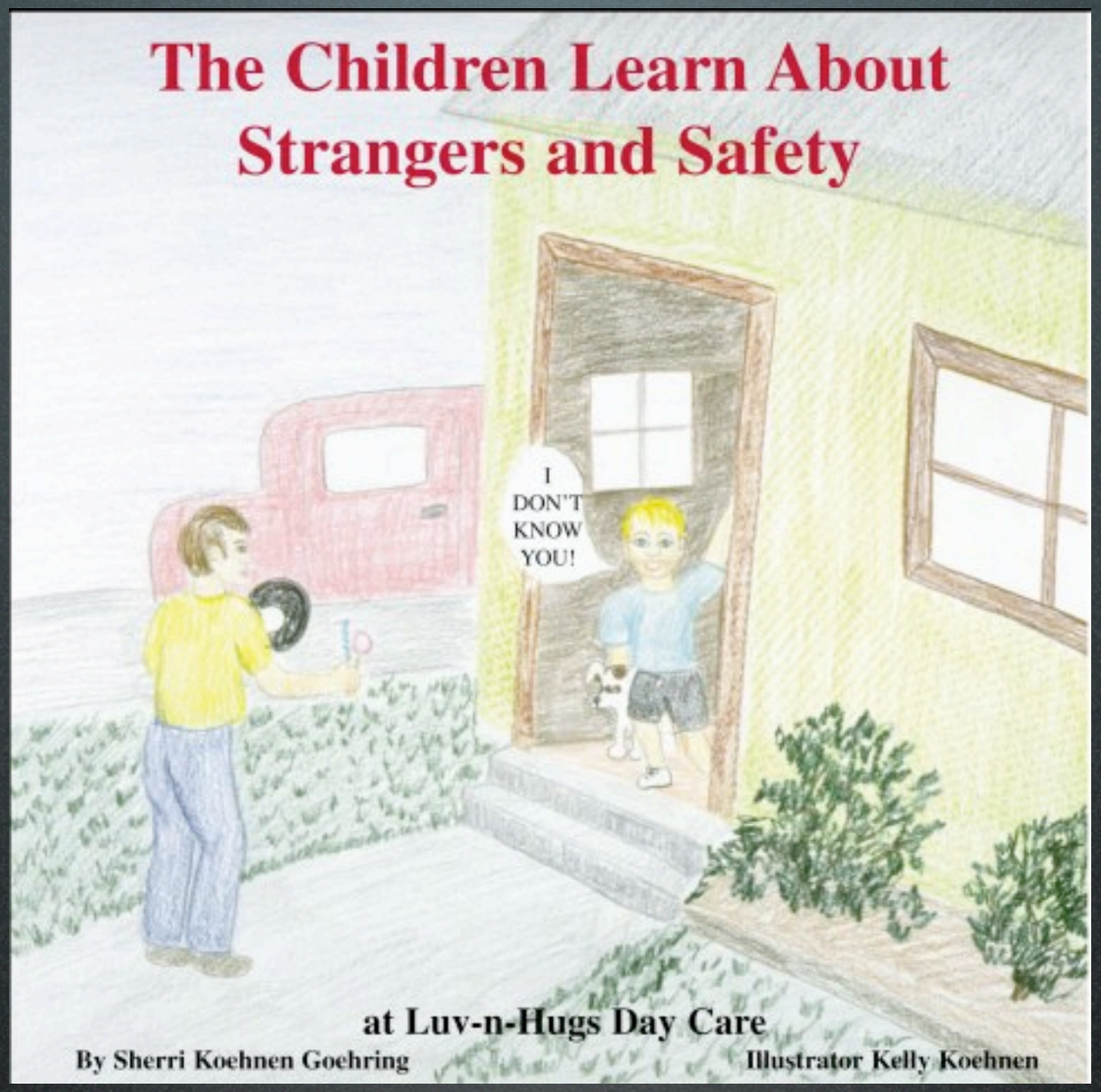
pseudonyms

Today
Only!!

www.windley.com

positive reputations are valuable

negative reputations don't stick...



Distrust Strangers

Stratgies:

- Distrust strangers
  - No strategy does better
- Make name changes more costly
- Commit to name permanence
  - Anonymous

Friedman and Resnick, The Social Cost of Cheap Pseudonyms

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 pseudonyms
- Two ways to scale:
  - Accountability (audits)
  - Reputation

Examples

- eBay
  - Pseudonyms and reputation
- Credit cards
  - simple authorization combined with fraud monitoring

reputation

www.windley.com

your story about me

principles of reputation

- Reputation is personal
- Reputation is a currency
- Reputation is narrative and dynamic
- Reputation is based on identity
- Reputation is based on claims, transactions, and opinions
- Reputation exists within specific contexts
- Reputation quality should be continually assessed

Reputation Components

Reputation Components

1. Verified claims (identifiers)

Reputation Components

1. Verified claims (identifiers)
2. Transaction data

Reputation Components

1. Verified claims (identifiers)
2. Transaction data
3. Opinions, ratings, and endorsements

reputation vs. privacy

CS601 - 2006

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

Design Philosophy

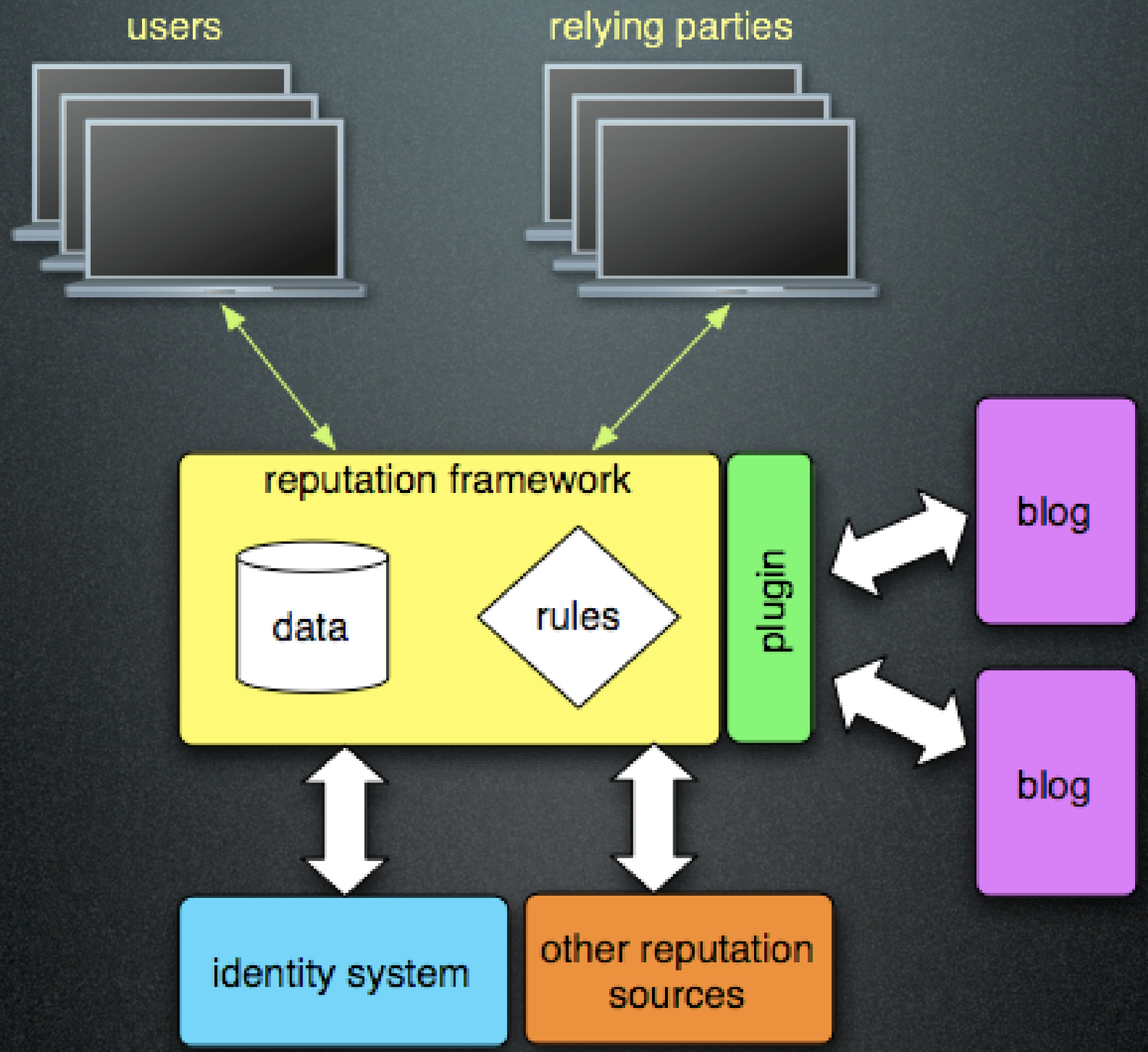
- Reputation is a calculated score
- Multiple computational models supported
- Users have multiple identifiers
- Factors
  - verified facts and credentials
  - transactions
  - opinions, ratings, & endorsements
- Transparency
- Transactions jointly owned and immutable

Architecture

- ID system neutral
- Data model for users and credentials
- Rules engine
- Plug-in architecture
  - adds data model
  - adds rule operations
- Plug outs to online systems

you've got to start somewhere

www.windley.com


users
relying parties
reputation framework
data
rules
plugin
blog
blog
identity system
other reputation sources

2007

www.windley.com

Reputation for OpenID

www.windley.com

CS601 - 2007

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

Use Case One

- George enters his OpenID at a Web site and gets redirected to a Web site that looks like his OpenID provider. Is it really? (protect user)
- Browser bar make automatic query
- Unathenticated or authenticated

Use Case Two

- George enters his OpenID at a Web site. What can the Web site know about George based on the reputation of that OpenID?
  - George doesn't have to be a stranger
  - George can selectively reveal other factors to the Web site

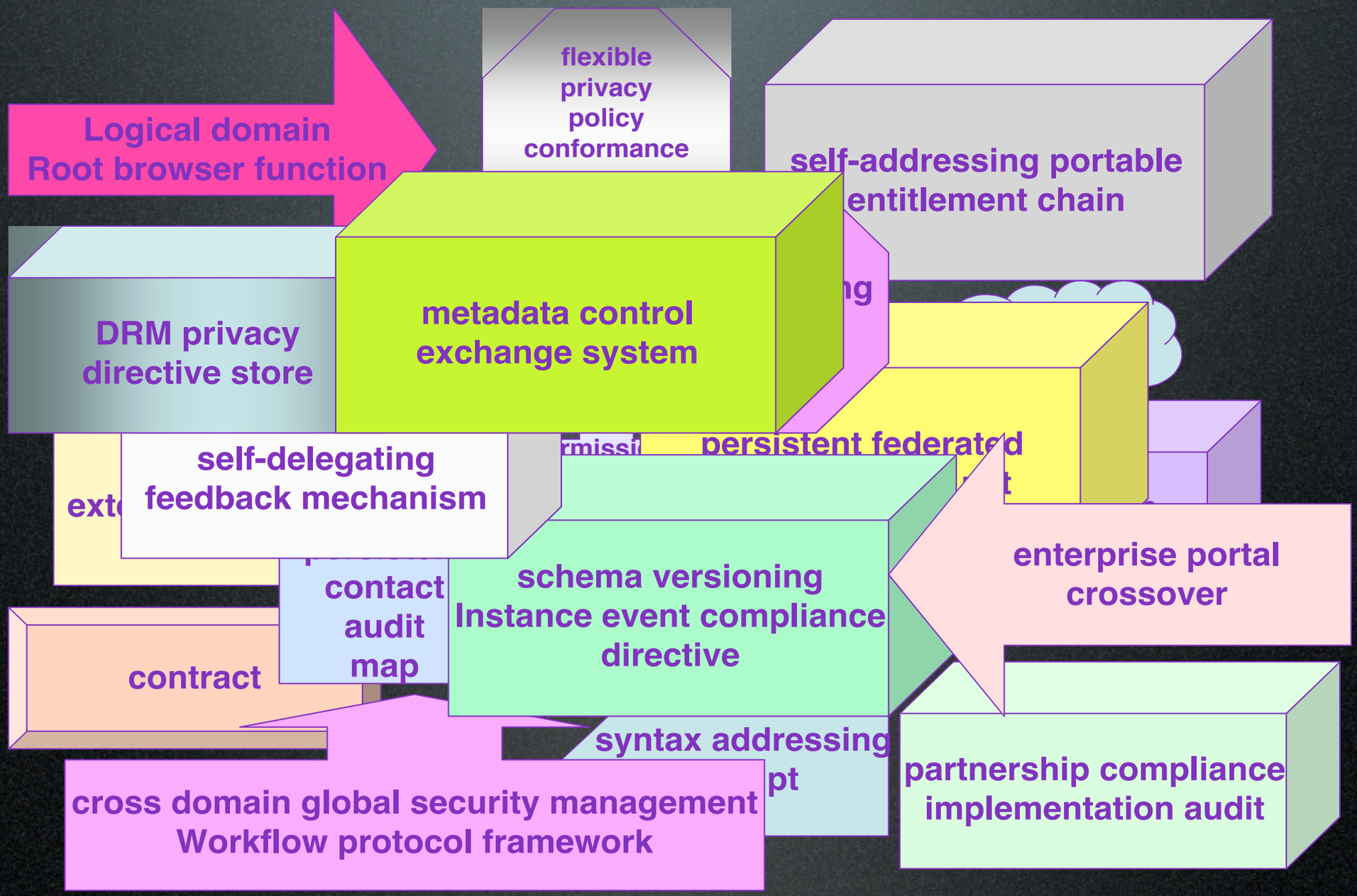
results

www.windley.com

Identity in the Enterprise

www.windley.com

Identity Infrastructure (as built)



Architecture courtesy of Doc Searls

Identity Management Architectures

City Planning

- Standardization
- Certification
- Management
  - Rules
  - Regulation
  - Enforcement

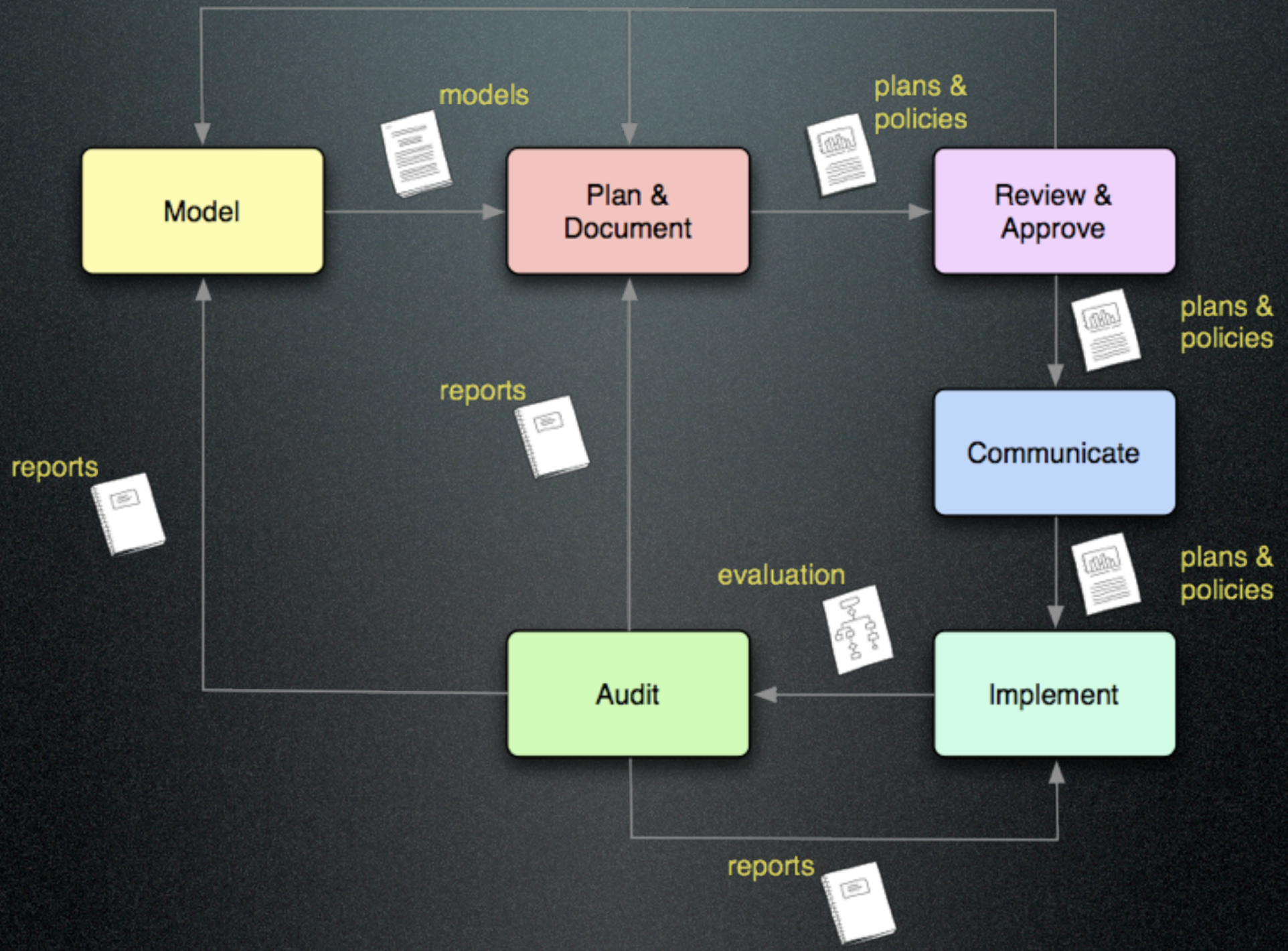
Creating a IMA Strategy

Key Steps

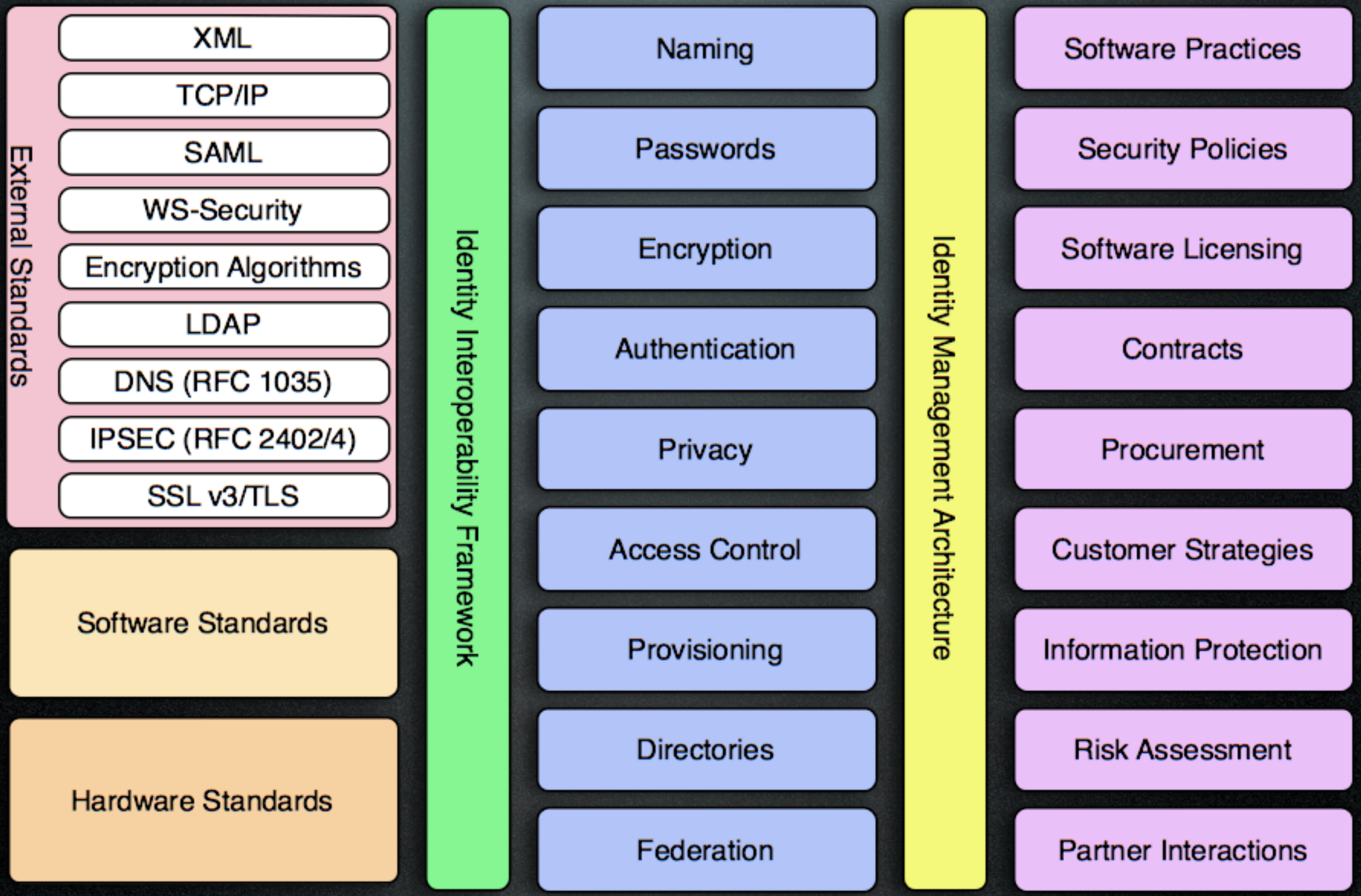
1. Governance
2. Business context
3. Resources
4. Policy
5. Interoperability framework
6. Reference architecture

www.windley.com

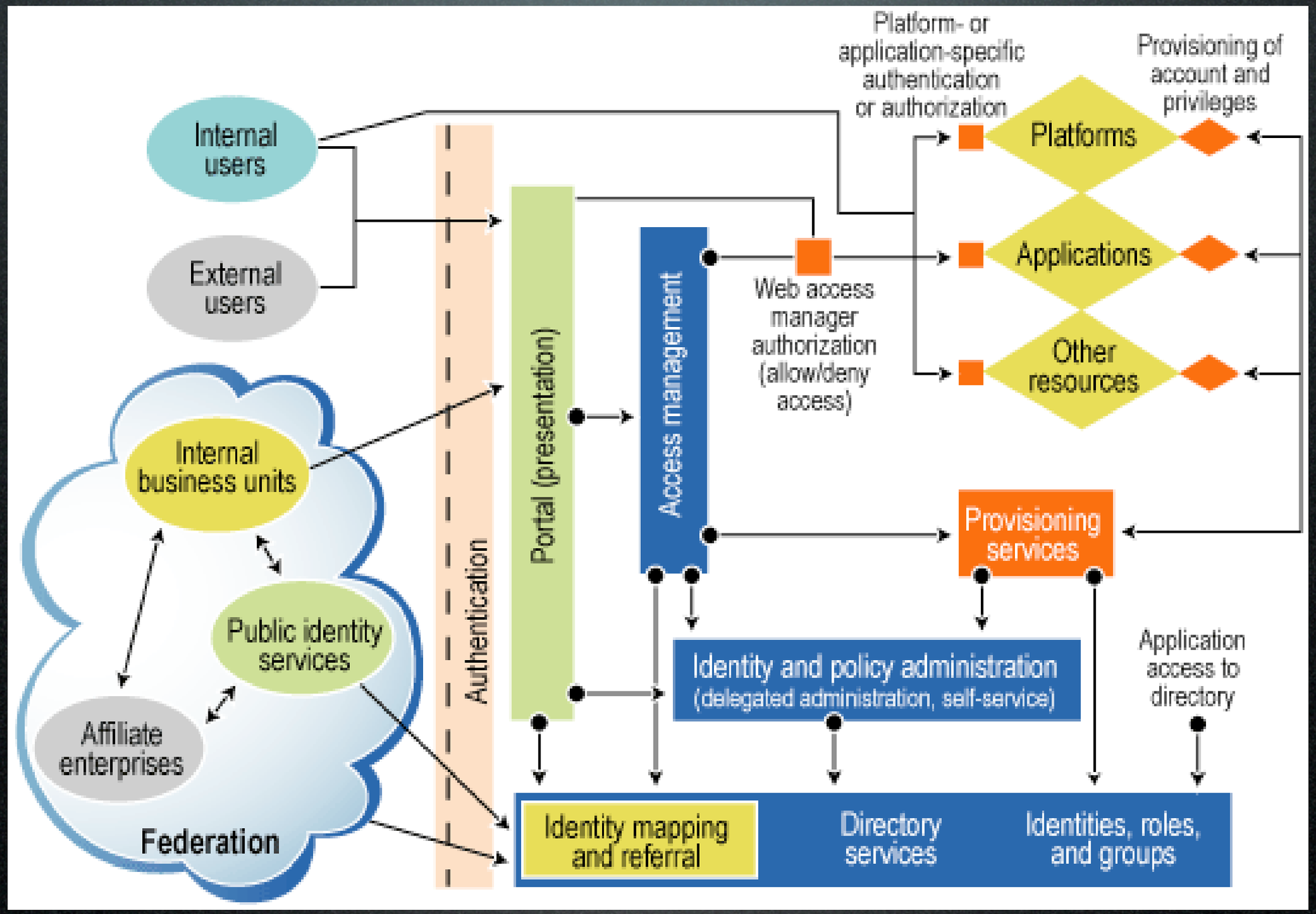
IMA Lifecycle



Identity Policy Stack



Reference Architecture



Courtesy of The Burton Group

break

www.windley.com

federation

www.windley.com

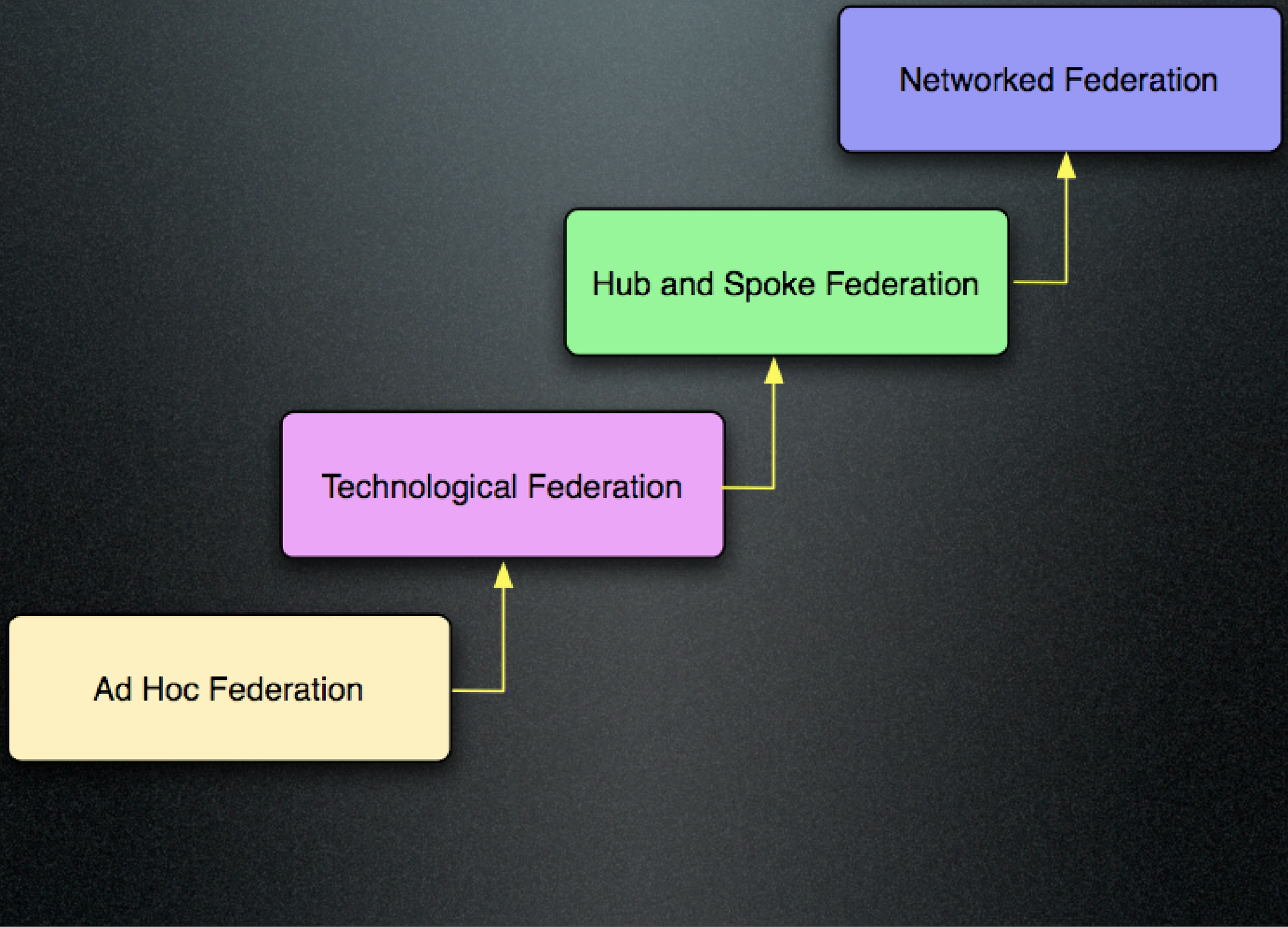
Identity Federation

WS-Federation

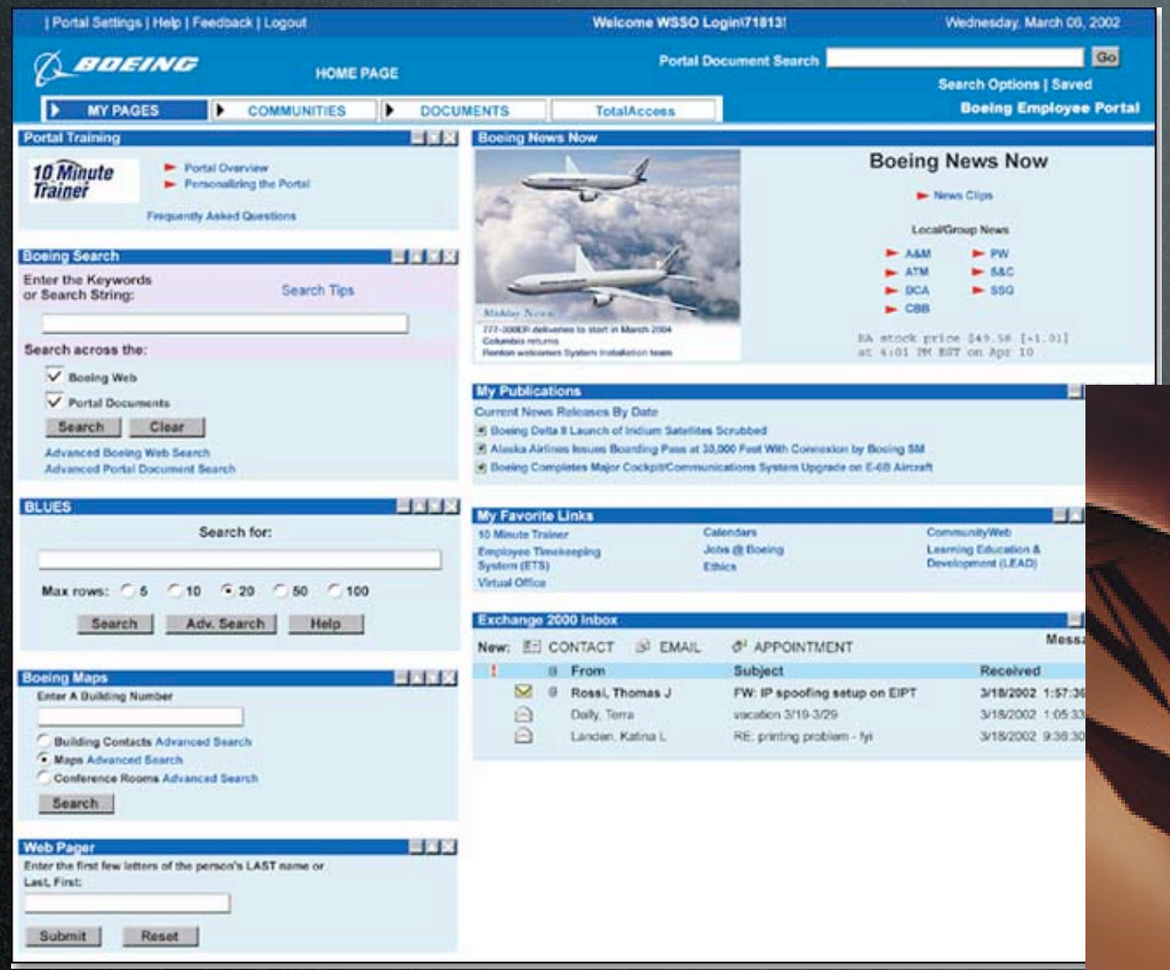
WS-Federation

- Linking identities across organizations
- Sharing attributes and authentication
- Loose coupling
- Goes beyond technology standards
  - Policy
  - Liability
  - Governance
  - Trust

Federation Maturity



Liability and Policy



Linking 401K site to employee portals

www.windley.com

user-centric identity

www.windley.com

An identity layer for the Internet

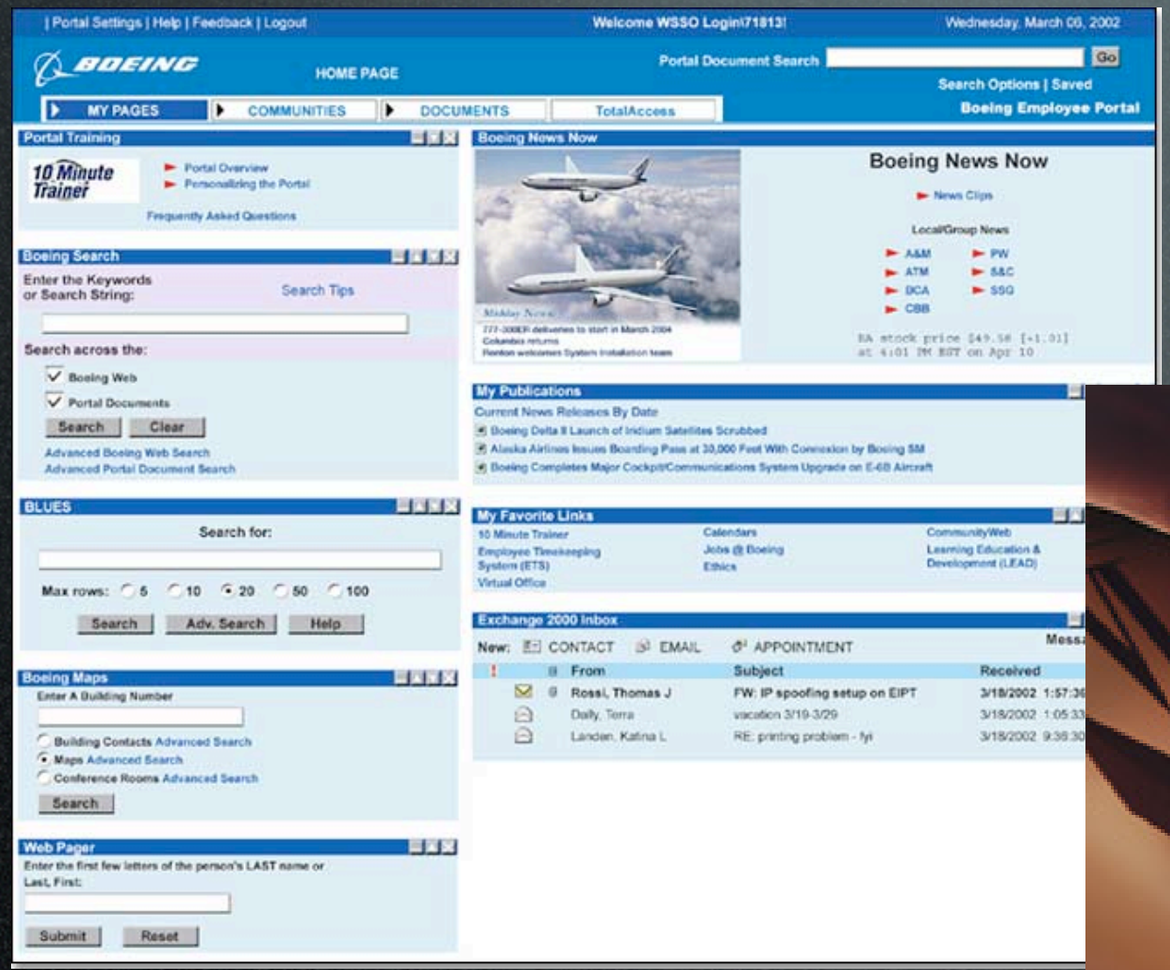
Vint Cerf

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

Federation Problems

Linking 401K site to employee portals



www.windley.com

Roles

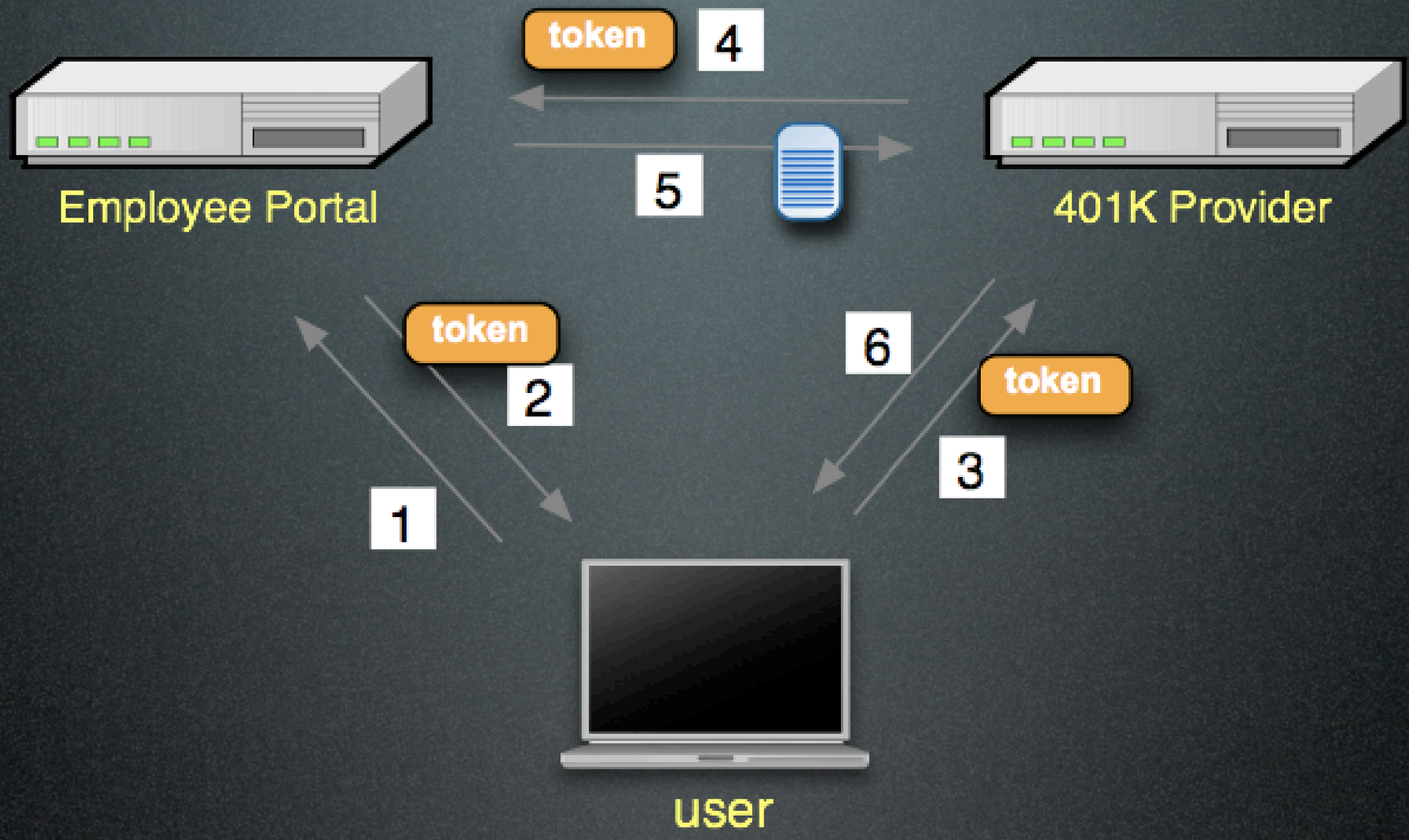
1. Identity Provider
2. Relying party

Roles

1. Identity Provider
2. Relying party
3. User

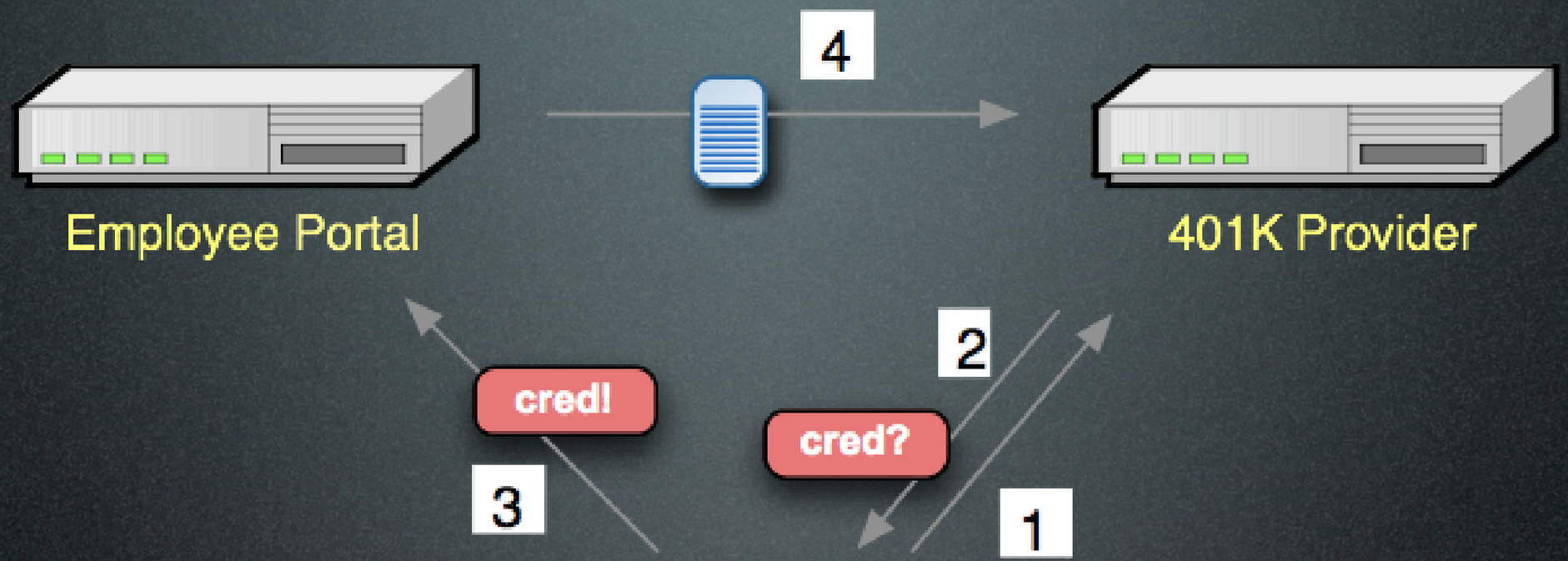
Identity Provider

- 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

www.windley.com

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

User-Centric Identity Technologies

Name	Type	Comments
XRI, i-names	address	URI-like, complete
OpenID	address	URL
LID	address	URL, attributes
CardSpace	token	ubiquity, complete
SXIP	token	complete solution
Higgins	token	interop framework
Liberty	token	enterprise
Shibboleth	token?	higher ed

OSIS Announcement

June 20, 2006, Berkman Identity Mashup

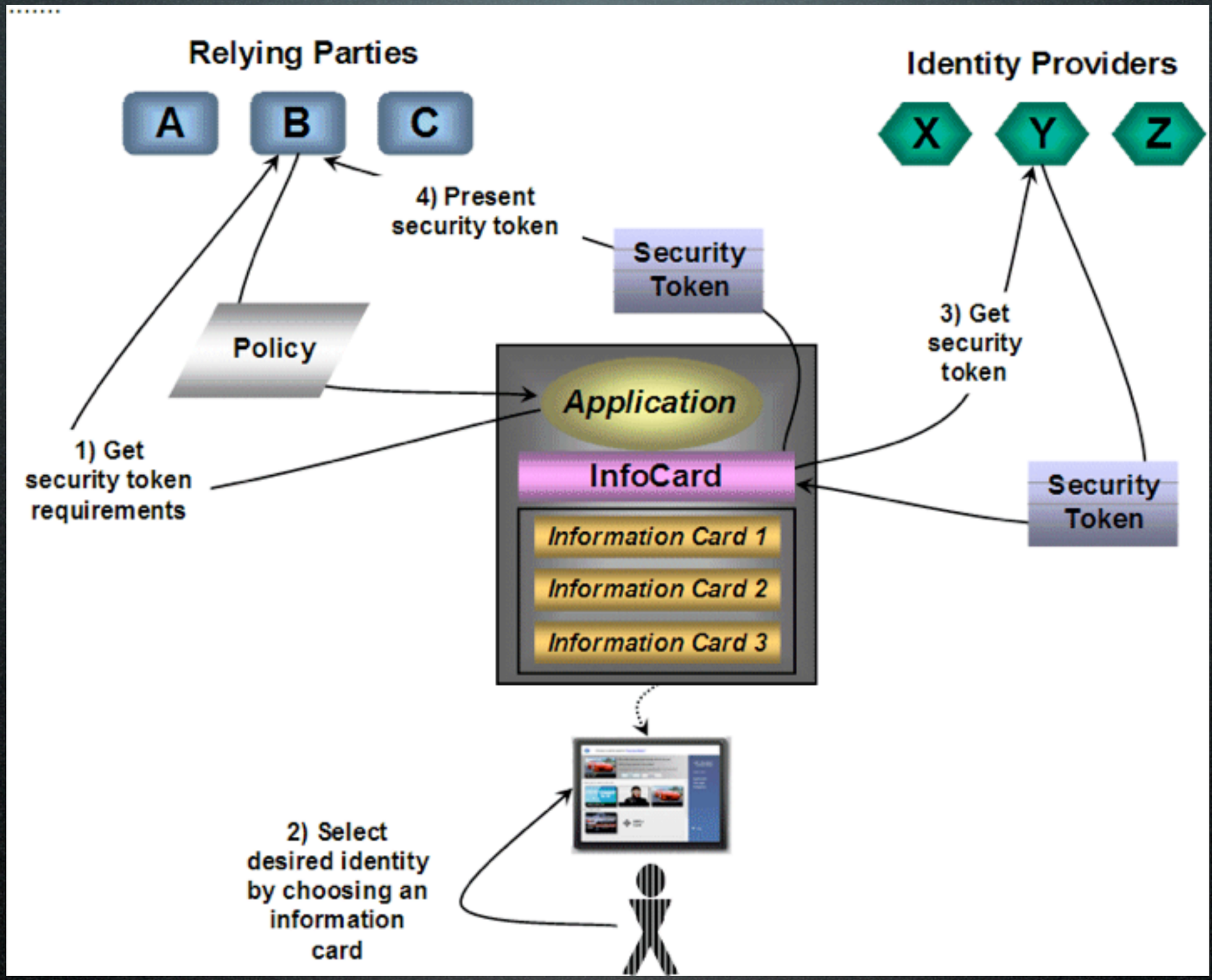
www.windley.com

Interoperable Layer

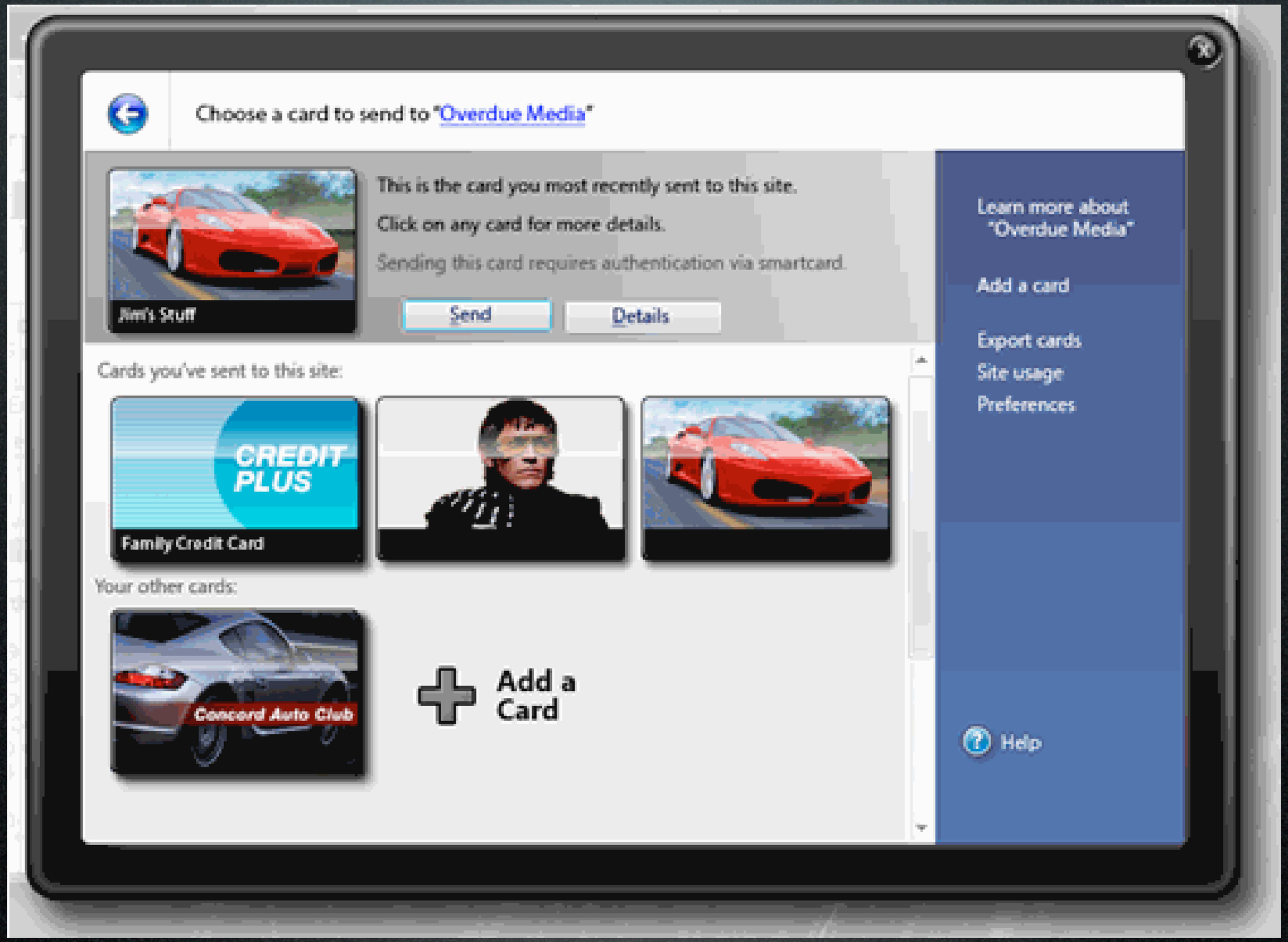
- Cross OS
  - Windows
  - Linux
  - OS X
- Cross Browser

CardSpace

- Open
- Decentralized
- Based on WS-* standards



InfoCard Interactions



CardSpace Identity Selector

CardSpace demo

www.windley.com

www.windley.com

http://openid.aol.com/pjwindley

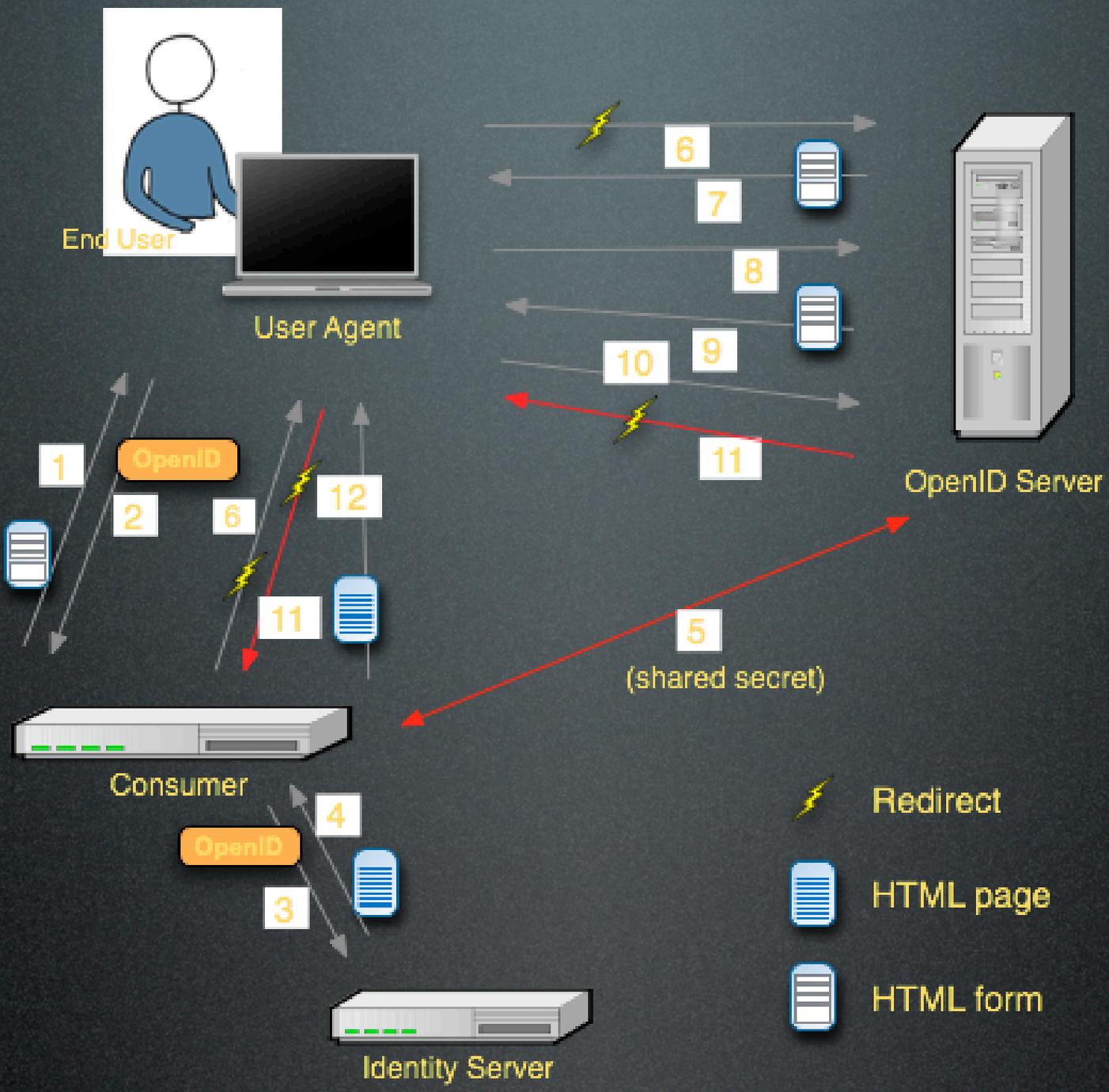
www.windley.com

http://www.windley.com

delegation

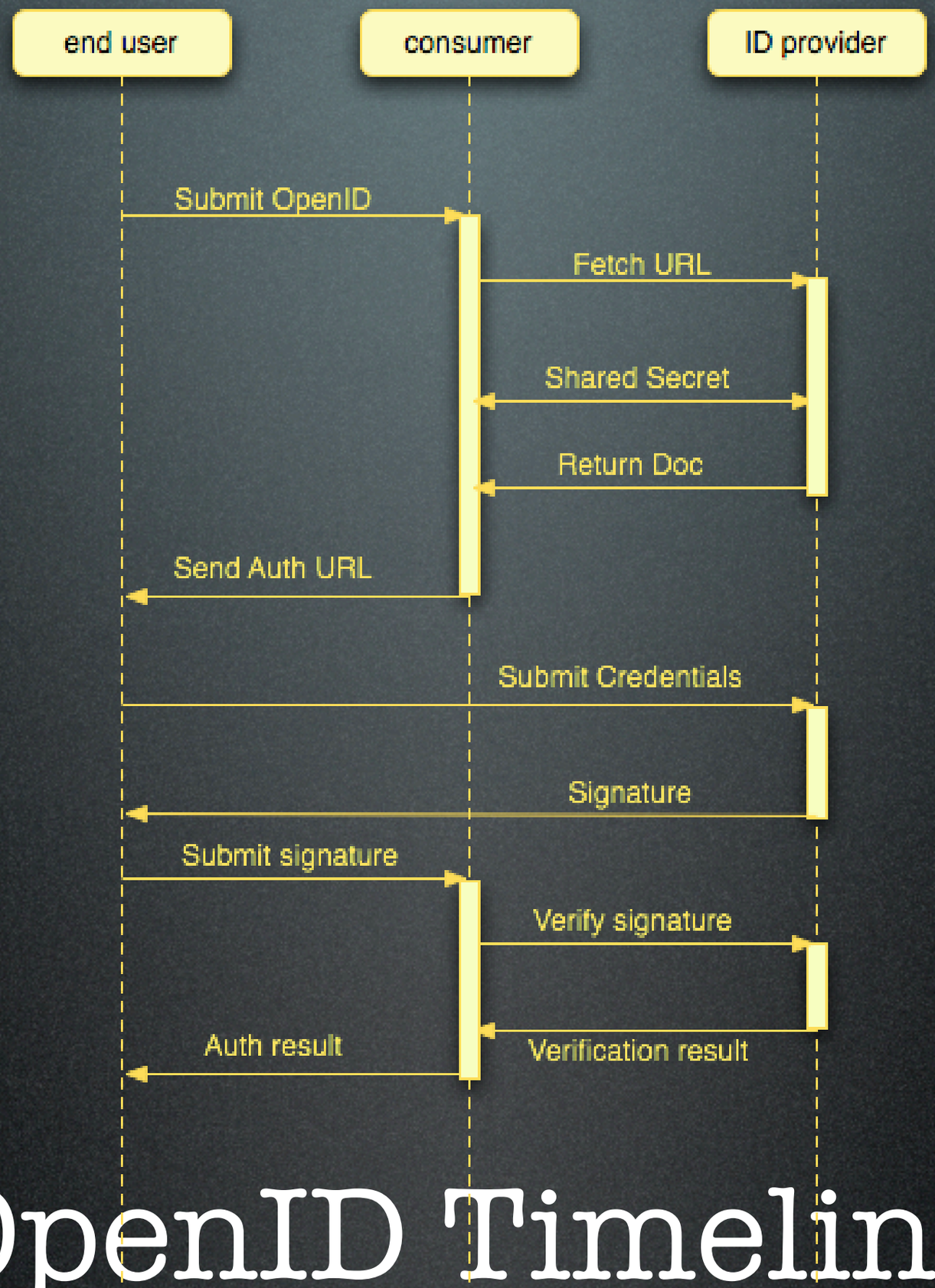
www.windley.com

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



OpenID Interactions

www.windley.com



OpenID Timeline

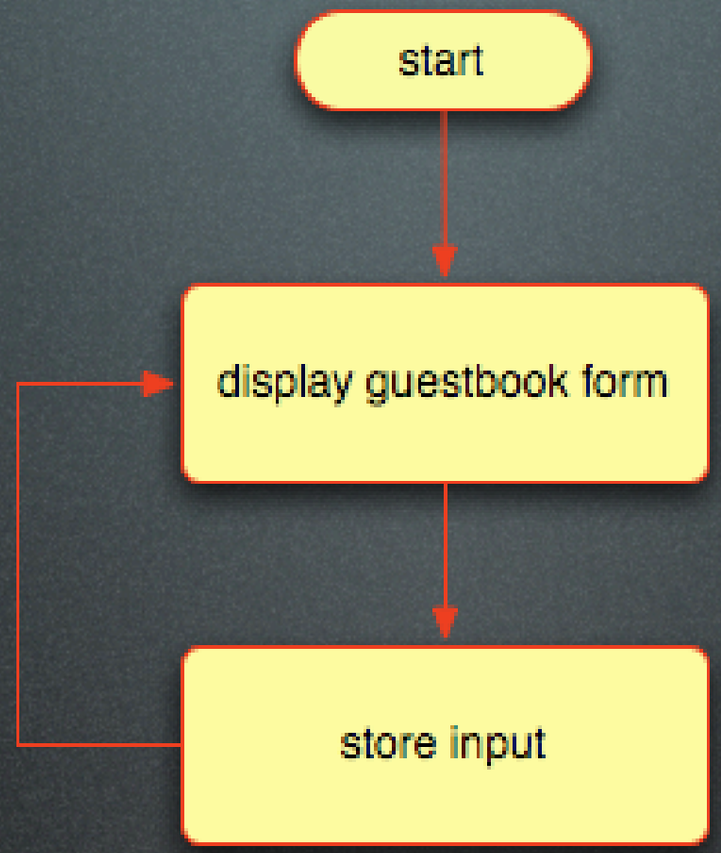
www.windley.com

OpenID Demo

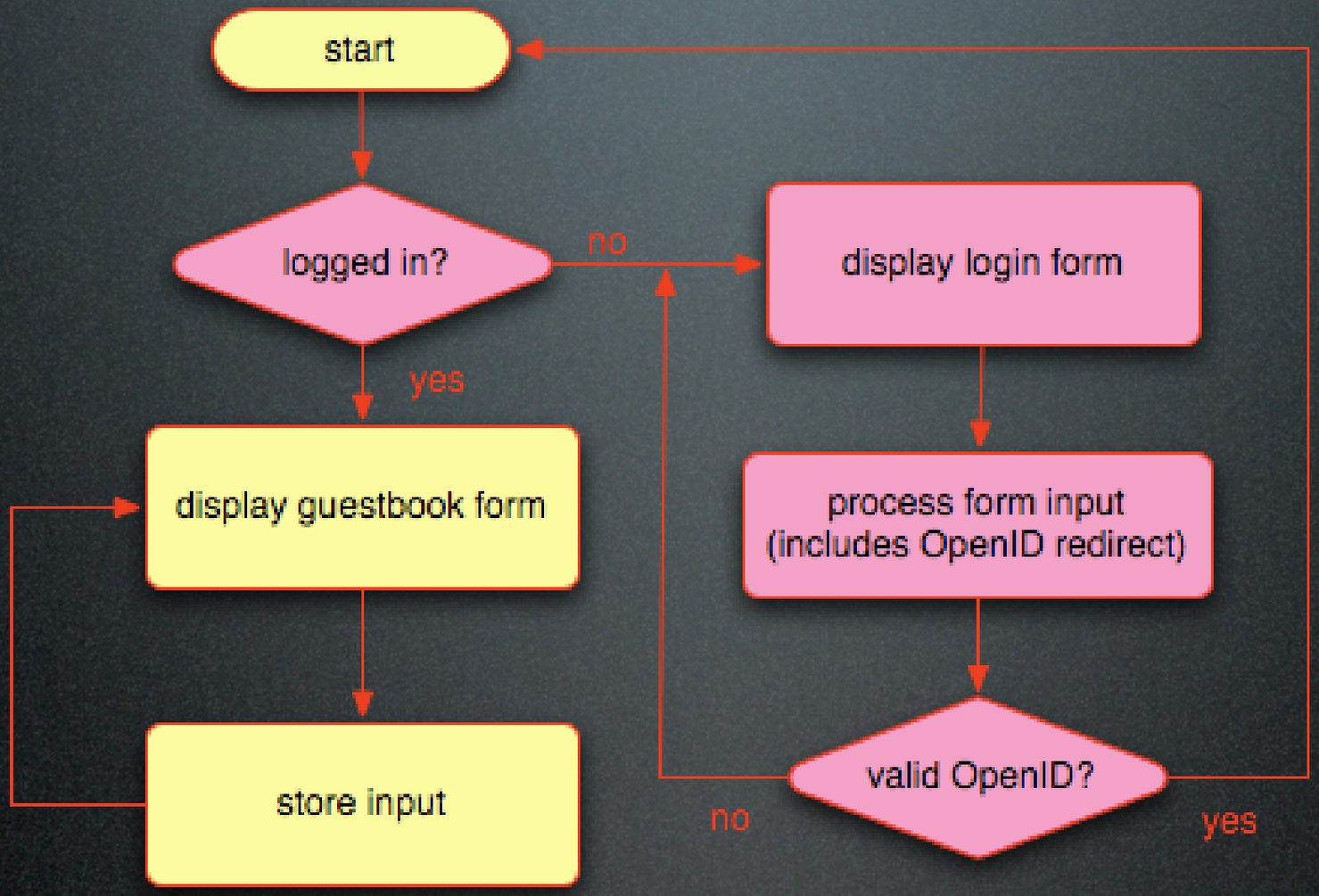
www.windley.com

guestbook example: factoring out authentication

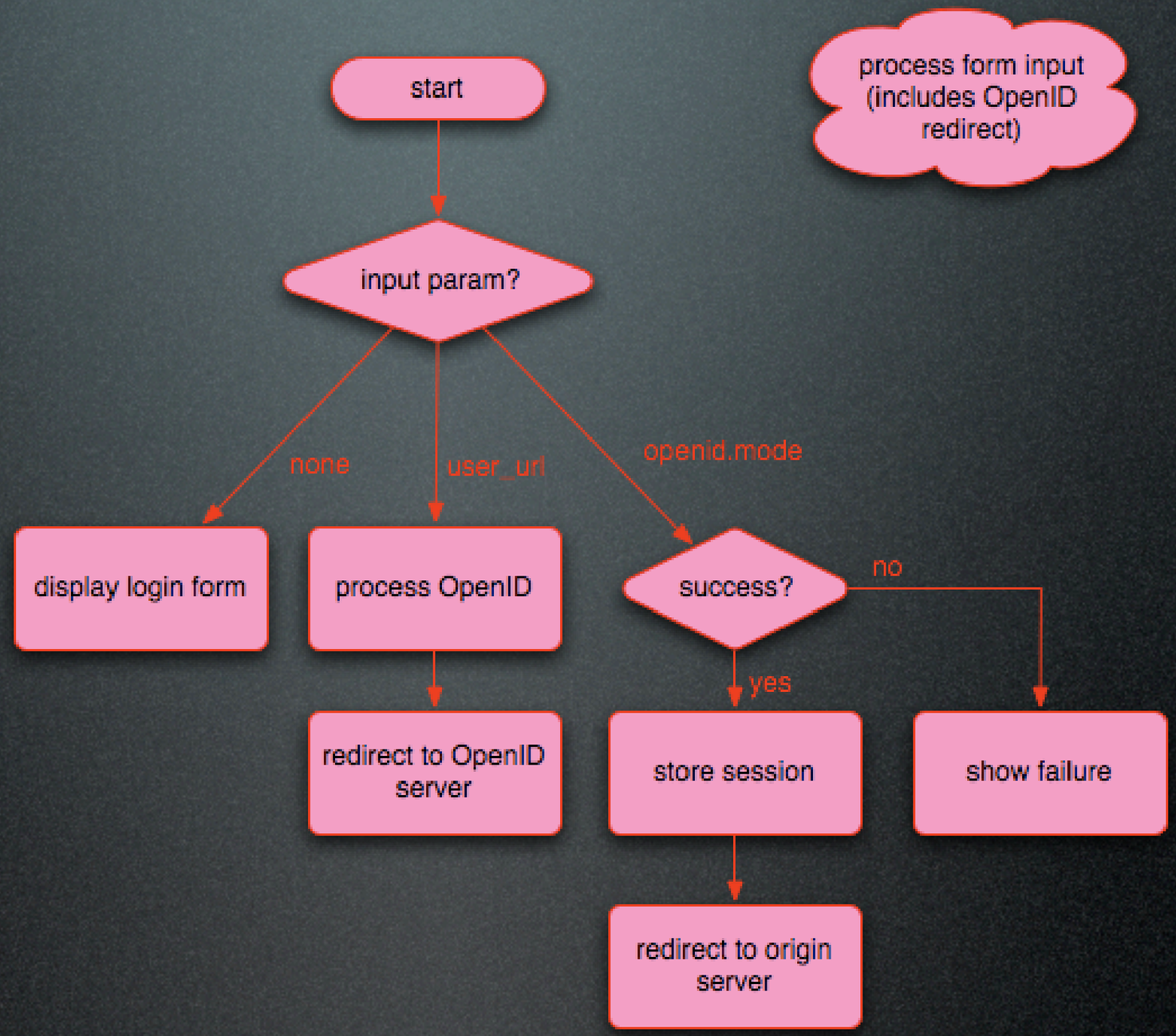
Simple Flow



Adding Authentication



More Detail


start
process form input (includes OpenID redirect)
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

assurance

www.windley.com

trust basis

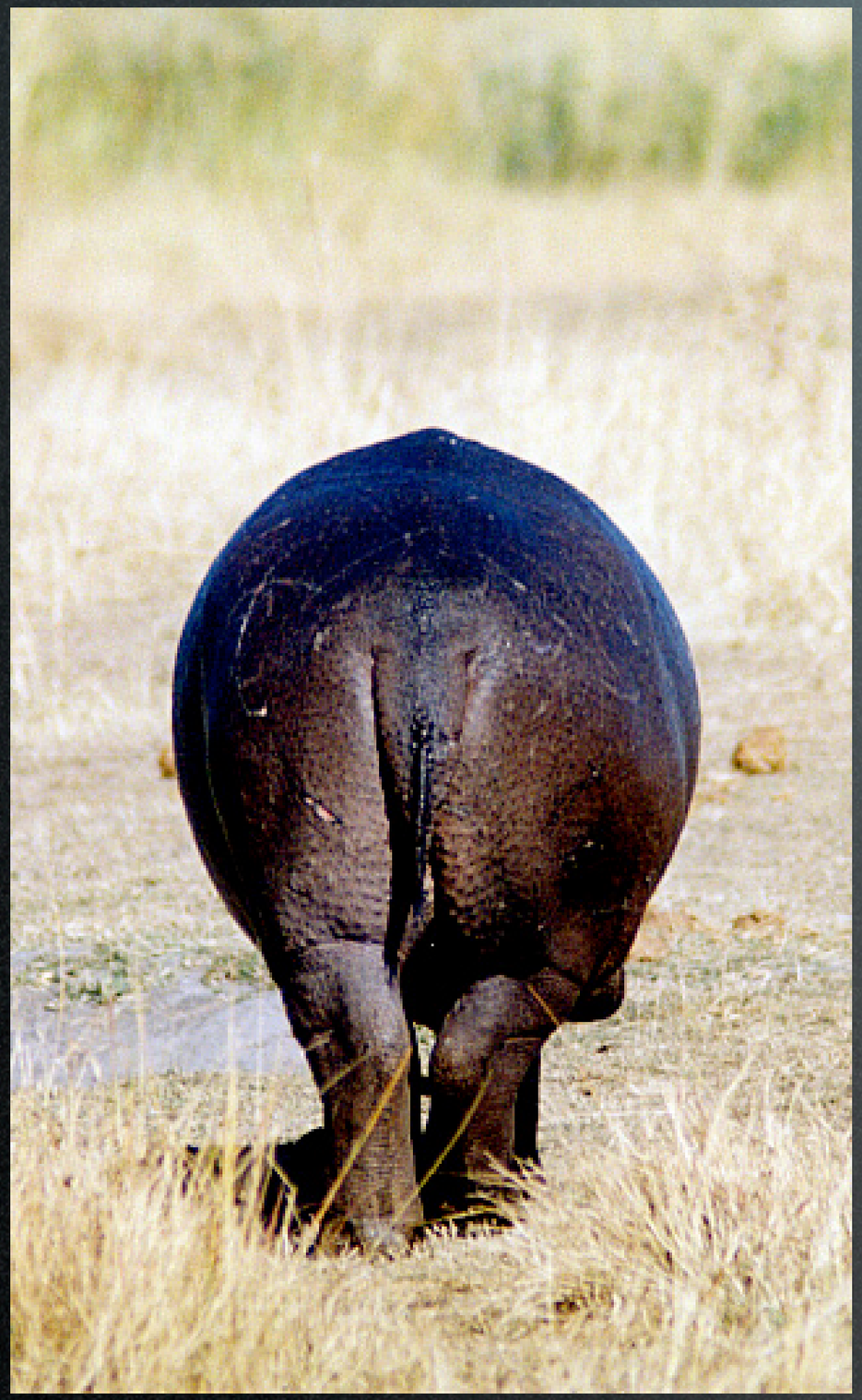
www.windley.com

user-centric economics

www.windley.com

threats

www.windley.com



the end

Contact Information

Contact me

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

Buy the book!!!

Questions?