

# Digital Identity Tutorial

Phillip J. Windley  
Brigham Young University

[phil@windley.com](mailto:phil@windley.com)  
[www.windley.com](http://www.windley.com)



Do you really need to understand enterprise rights management before you undertake a directory virtualization project?









**THE WORLD NEEDS  
A BOOK ON DIGITAL  
IDENTITY!**



*Unmasking Identity Management Architecture (IMA)*

# Digital Identity



O'REILLY®

*Phillip J. Windley*

THE WORLD NEEDS  
A BOOK ON DIGITAL  
IDENTITY!







October, 2005



May and  
Dec, 2006



May 14-16, 2007  
Mountain View, CA



# Coming Up



IIW07b, Dec 3-5  
Mountain View, CA

Come to the IOS event on Wed afternoon!



WINDLEY'S

# TECHNOMETRIA

ORGANIZATIONS GET THE IT THEY DESERVE



## TECHNOMETRIA

[Home](#)

[Why Technometria?](#)

RSS **XML**

Atom **XML**

Podcasts **XML**

[add to MyYAHOO!](#)

[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

[\(Find out more...\)](#)

## SEARCH

Search this site:

## UPCOMING EVENTS

[Dell Briefing](#)

September 18 - September 18

[Broadband Cities](#)

September 19 - September 19



permalink



September 11, 2006

---

## **Vitamins, Pain-killers, and Viagra**

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.



Dick Hardt  
(click to enlarge)

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!**



# Does Identity Matter?



**YAHOO!**

PR 無料でアドレス取得、メール送受

✉ 新着メッセージ1件

📅 02/19(木) 16:00 定例会

🌞 ☀ 東京-東京

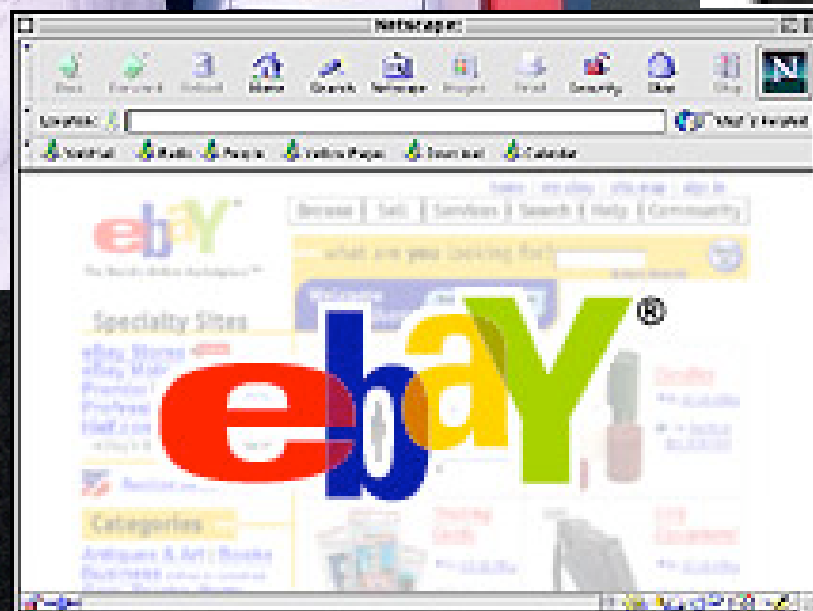
👤 いて座:総合運60点

📈 ×××(株) 1,680,000

🛒 📺 📺 📺 📺 📺 📺 📺

2004/02/19 12:13 更新 🔄

📧 [02/19 10:52] 女子テニスの心







identity is the foundation for  
commerce



# What Happened to the Walls?





# What Happened to the Walls?





# The Border Patrol

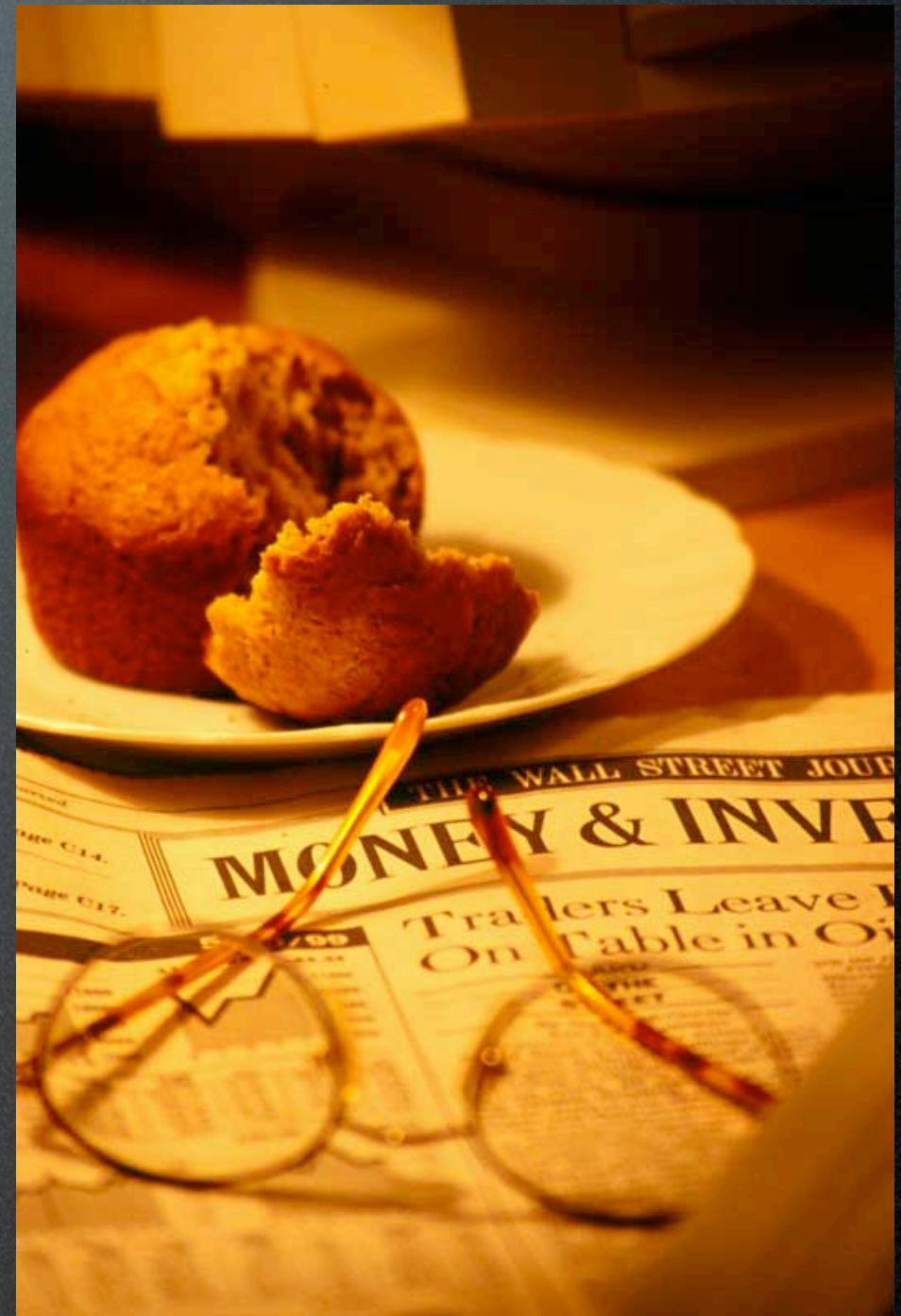




# Business Context of Identity



VS





identifiers



what's in a name?





Samantha

Matsuhiko

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?](#)



# 3 Phillip Windleys

HowManyOfMe.com



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

How many have your name?

50,000 John Smiths



128-56-7567



phil@windley.org



windley.com



<http://www.windley.com/essays>



xri:///windley



credentials

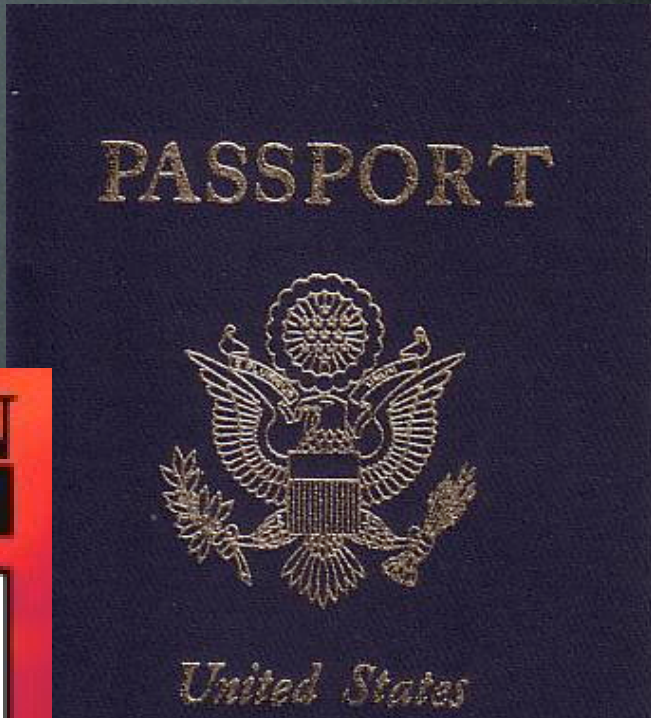


One of these things is not like the others!



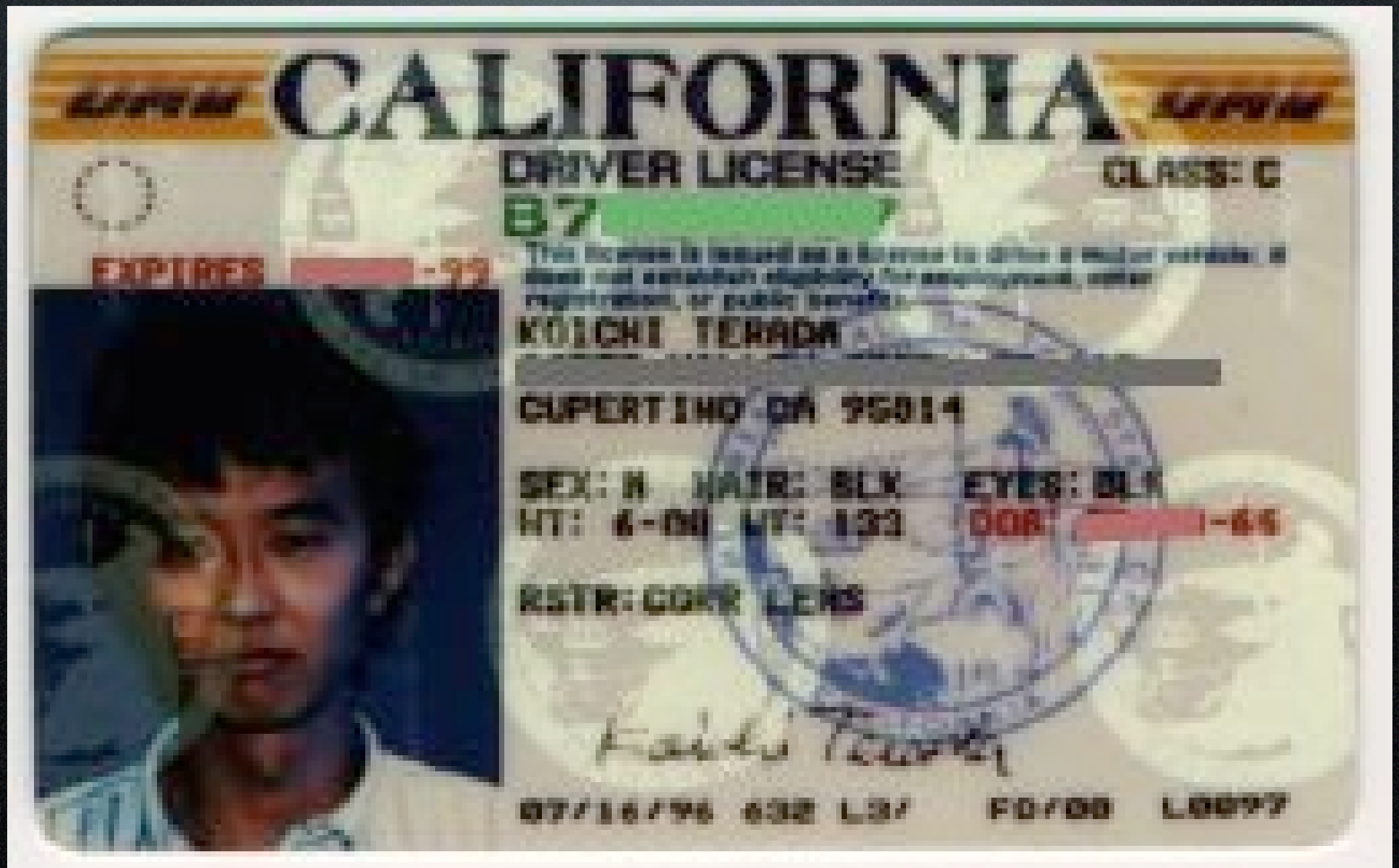
**METROPOLITAN  
PORT AUTHORITY**

**Allen Bishop  
Inspector**  
I.D. 0006-398-99



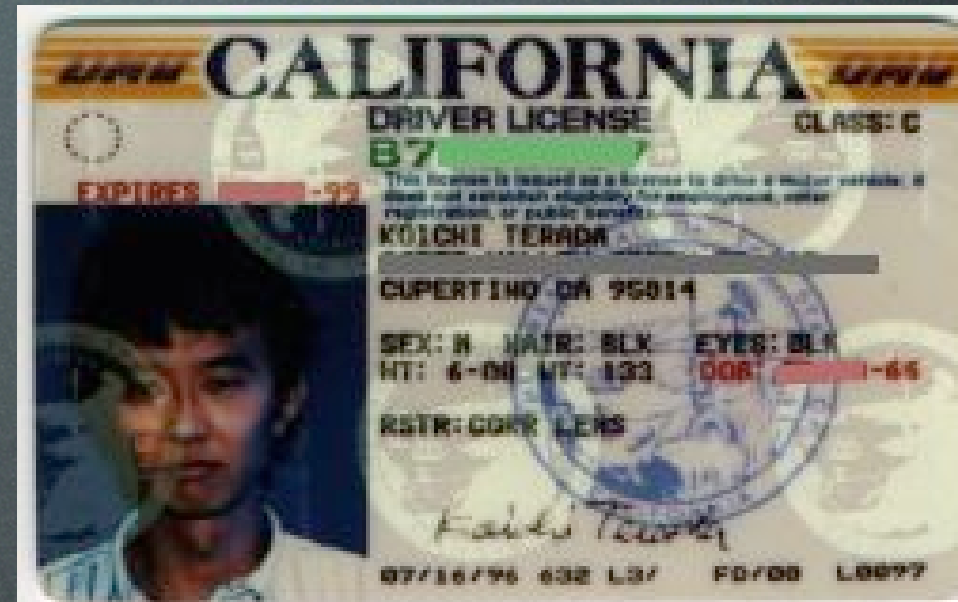


# Credentials & Identity





# Buying Beer







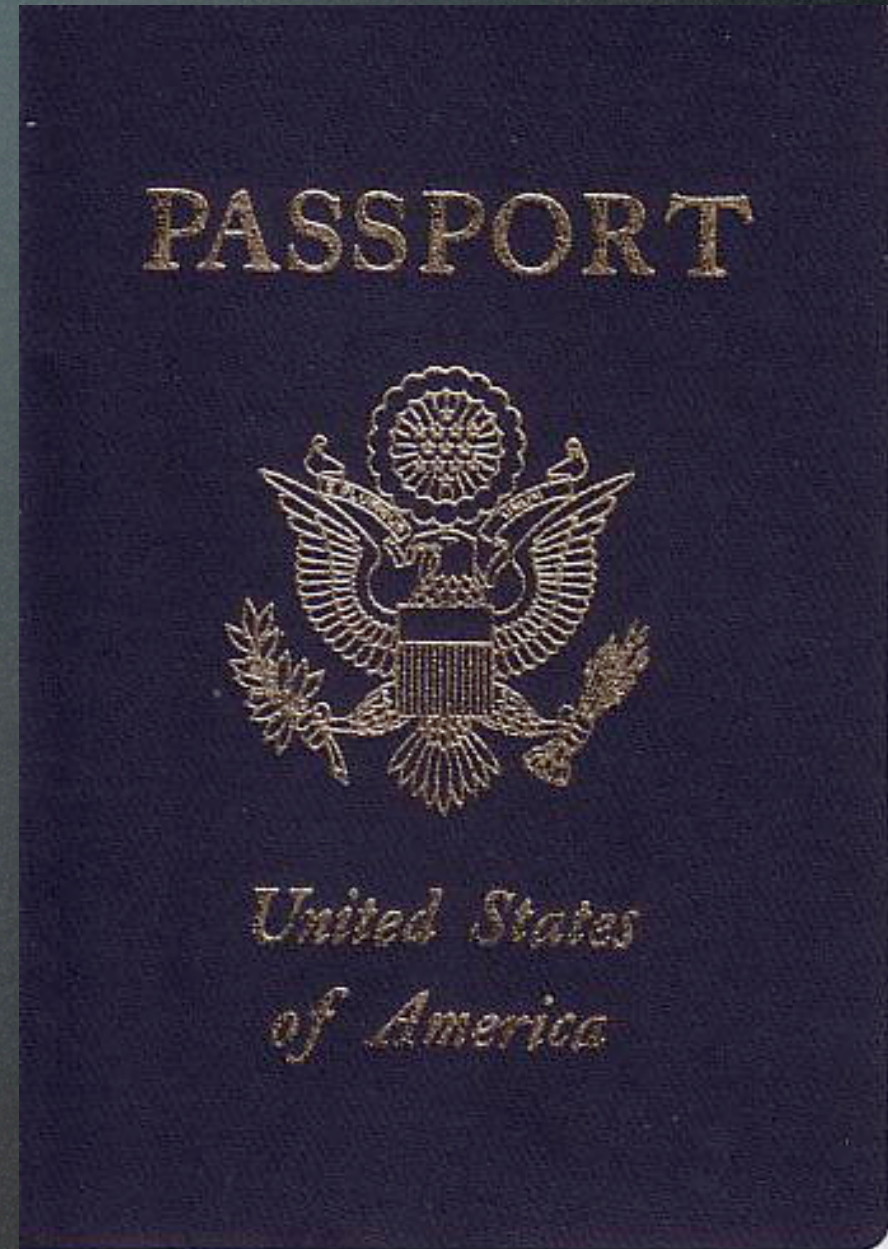
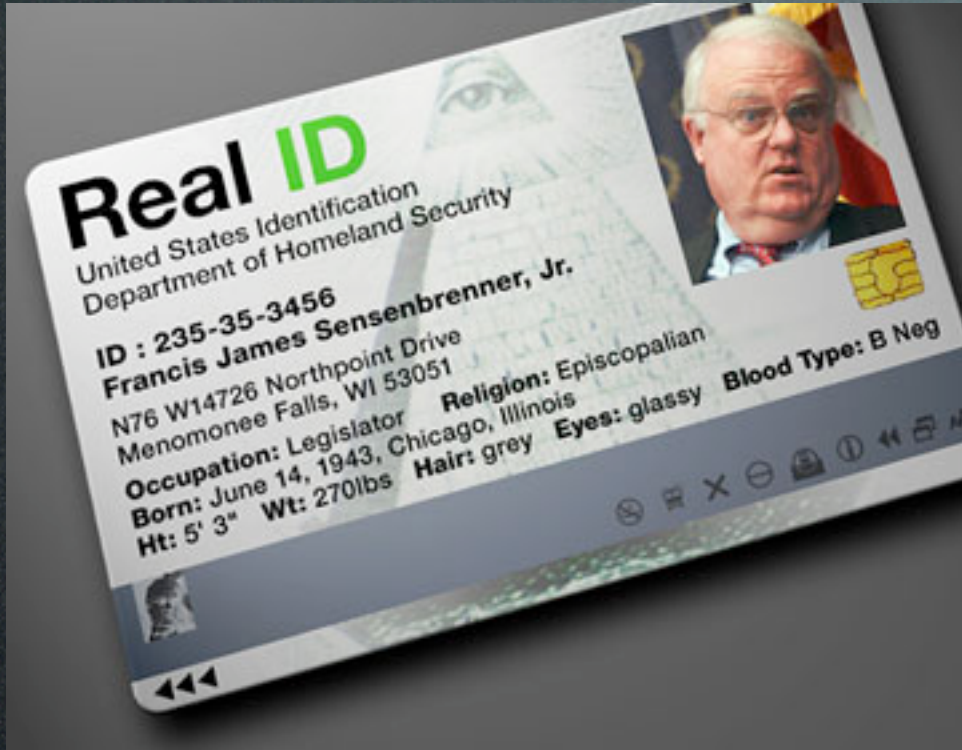


















Accountability,  
Reputation,  
Privacy &  
Authorization



privacy



privacy





privacy



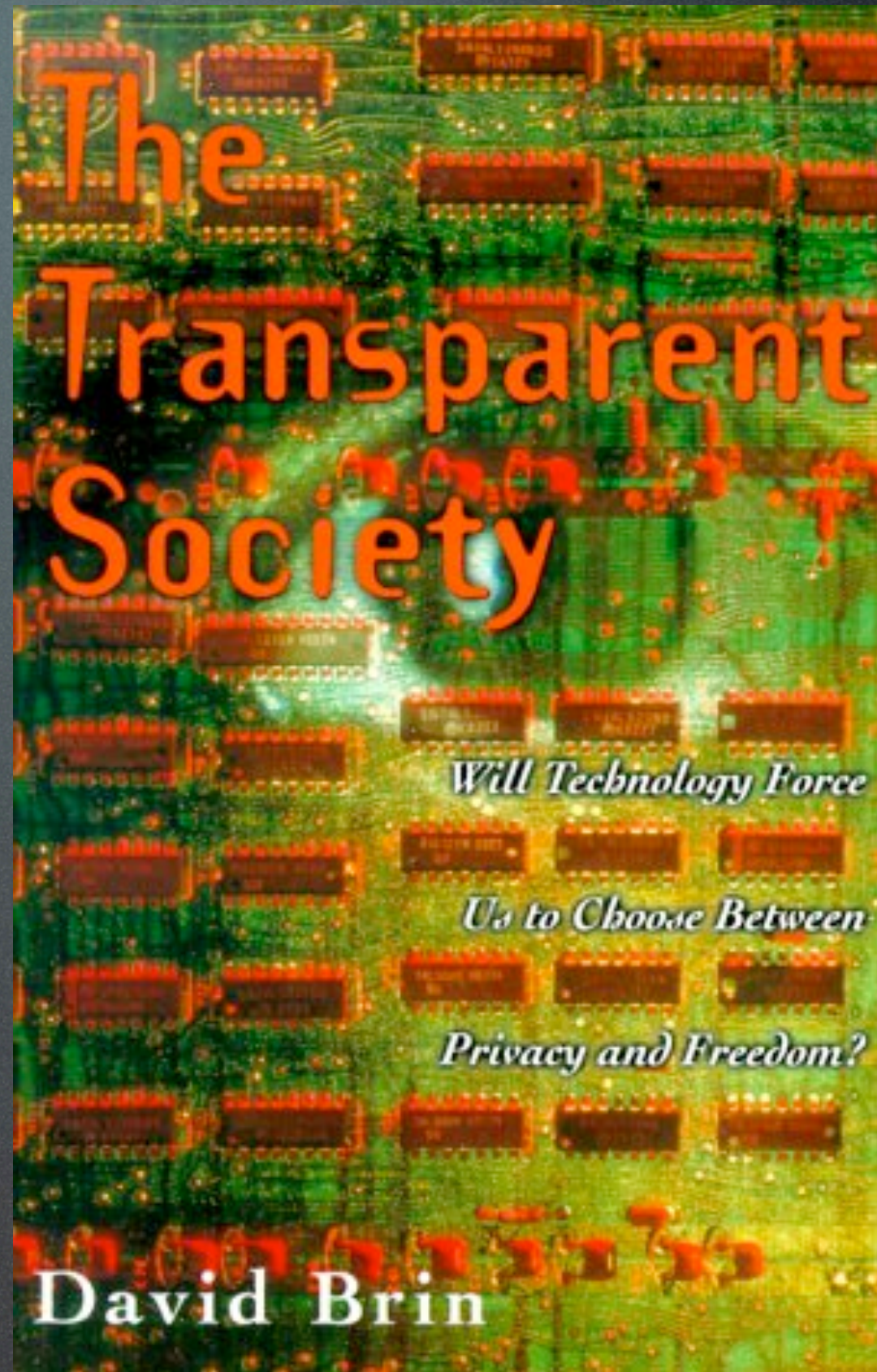


**YOU HAVE NO  
PRIVACY ANYWAY.  
GET OVER IT!**



Scott McNealy,  
CEO Sun







# 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



A bright yellow starburst graphic with multiple points, containing the text 'CHEAP!!!'.

CHEAP!!!

pseudonyms

A bright red starburst graphic with multiple points, containing the text 'Today Only!!'.

Today  
Only!!





positive reputations are  
valuable



negative reputations don't stick...



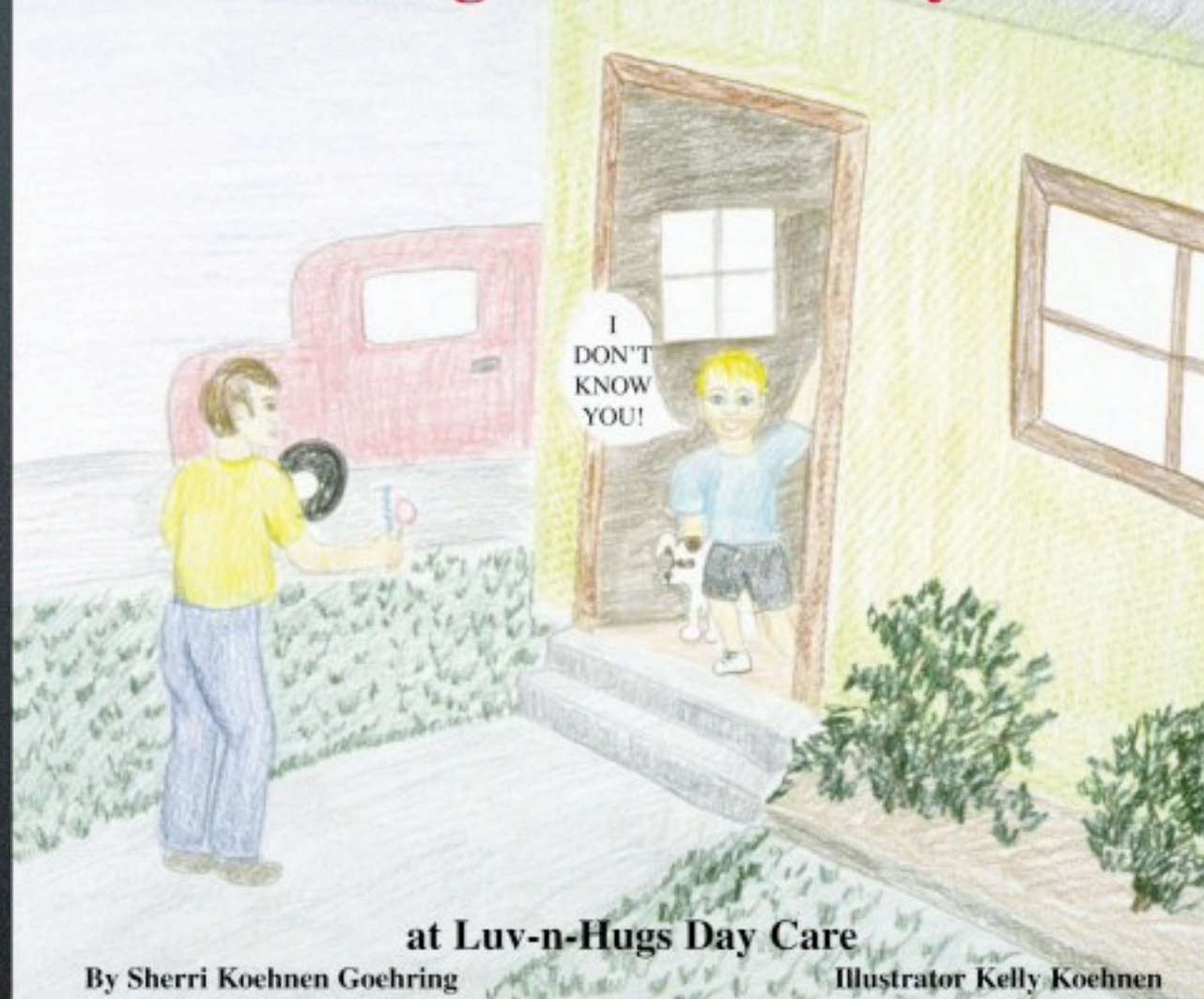


# Pseudonym Strategies

Friedman and Resnick,  
The Social Cost of Cheap Pseudonyms



# The Children Learn About Strangers and Safety



at Luv-n-Hugs Day Care

By Sherri Koehnen Goehring

Illustrator Kelly Koehnen

# Distrust Strangers





Make name changes  
costly





Commit to permanent  
names



anonymity enables  
social good



# Authorization



# Traditional View

- Enforcement
- $U \times R \times A$  table
  - $U \Rightarrow$  Users
  - $R \Rightarrow$  Resources
  - $A \Rightarrow$  Actions



# Authorization Problems

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



# Examples

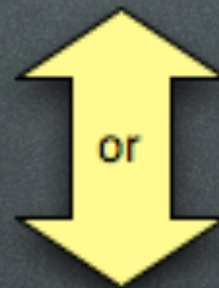




# Authorization

## The Traditional View

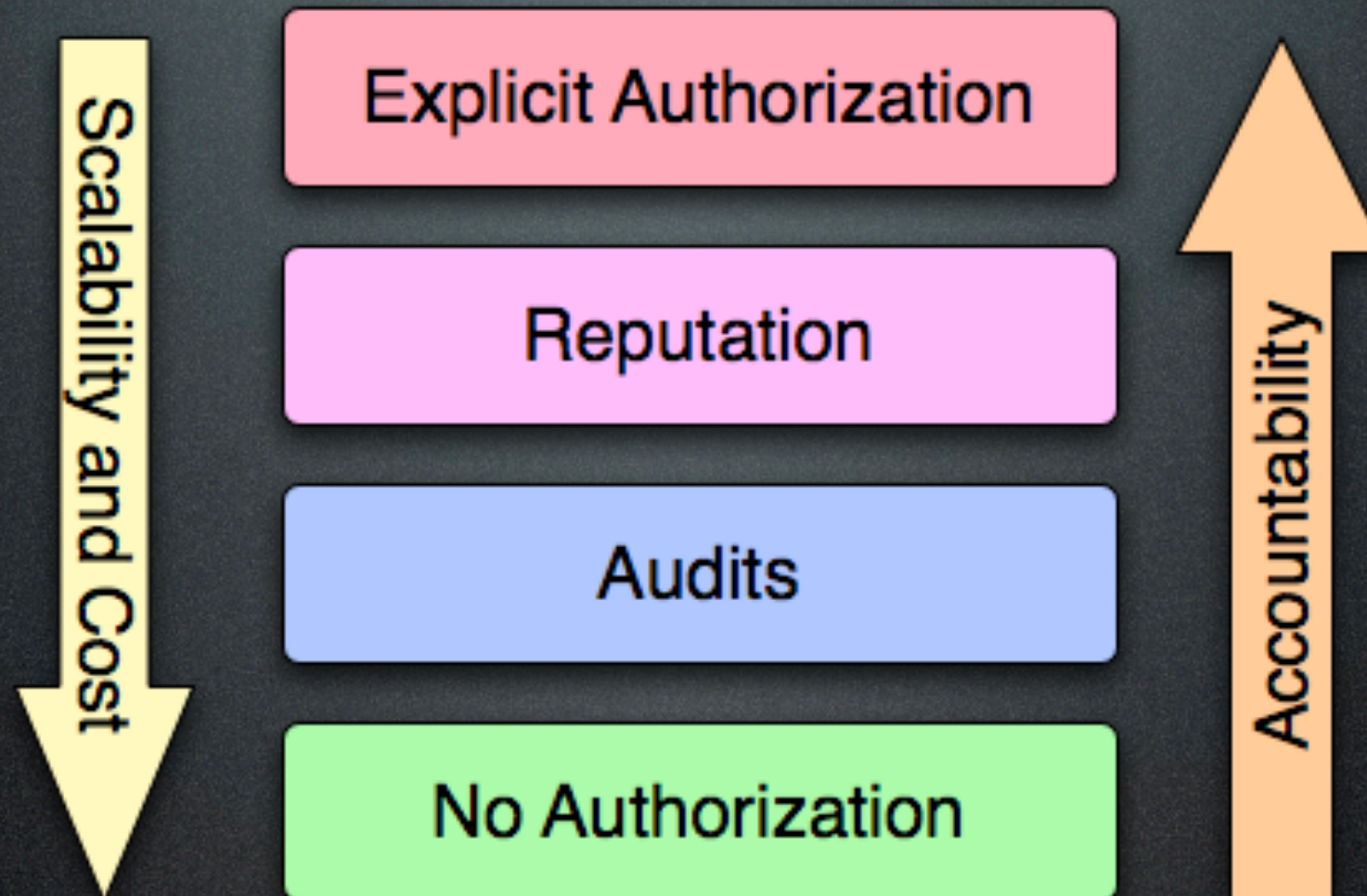
Explicit Authorization



No Authorization



# Authorization Hierarchy





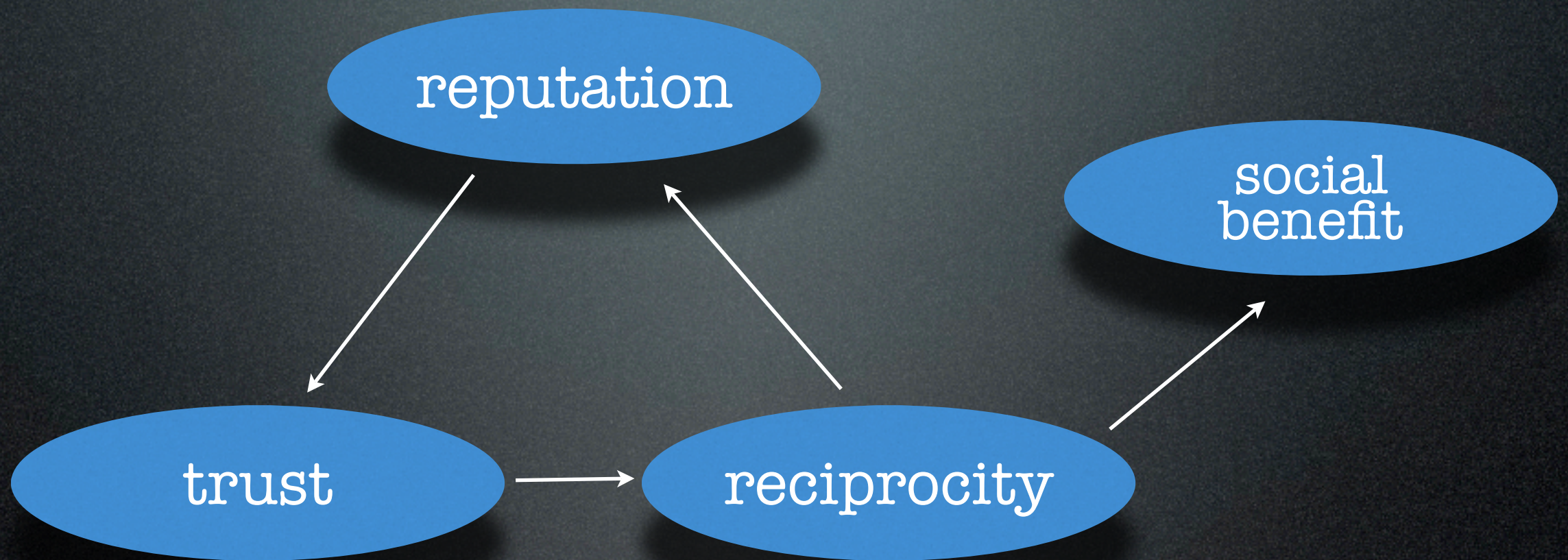
# Reputation





your story about me





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



# Principles of Reputation



Reputation should be  
user-centric



Reputation has value



Reputation is  
narrative and  
dynamic



Reputation is based on  
identity



Reputation is based on  
claims, transactions &  
opinions



Reputation exists  
within **specific**  
**contexts**



Reputation **quality** is  
an important  
metavalue





reputation vs. privacy





Linking Identifiers



- 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



# Reputation as a substitute for authorization



# 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



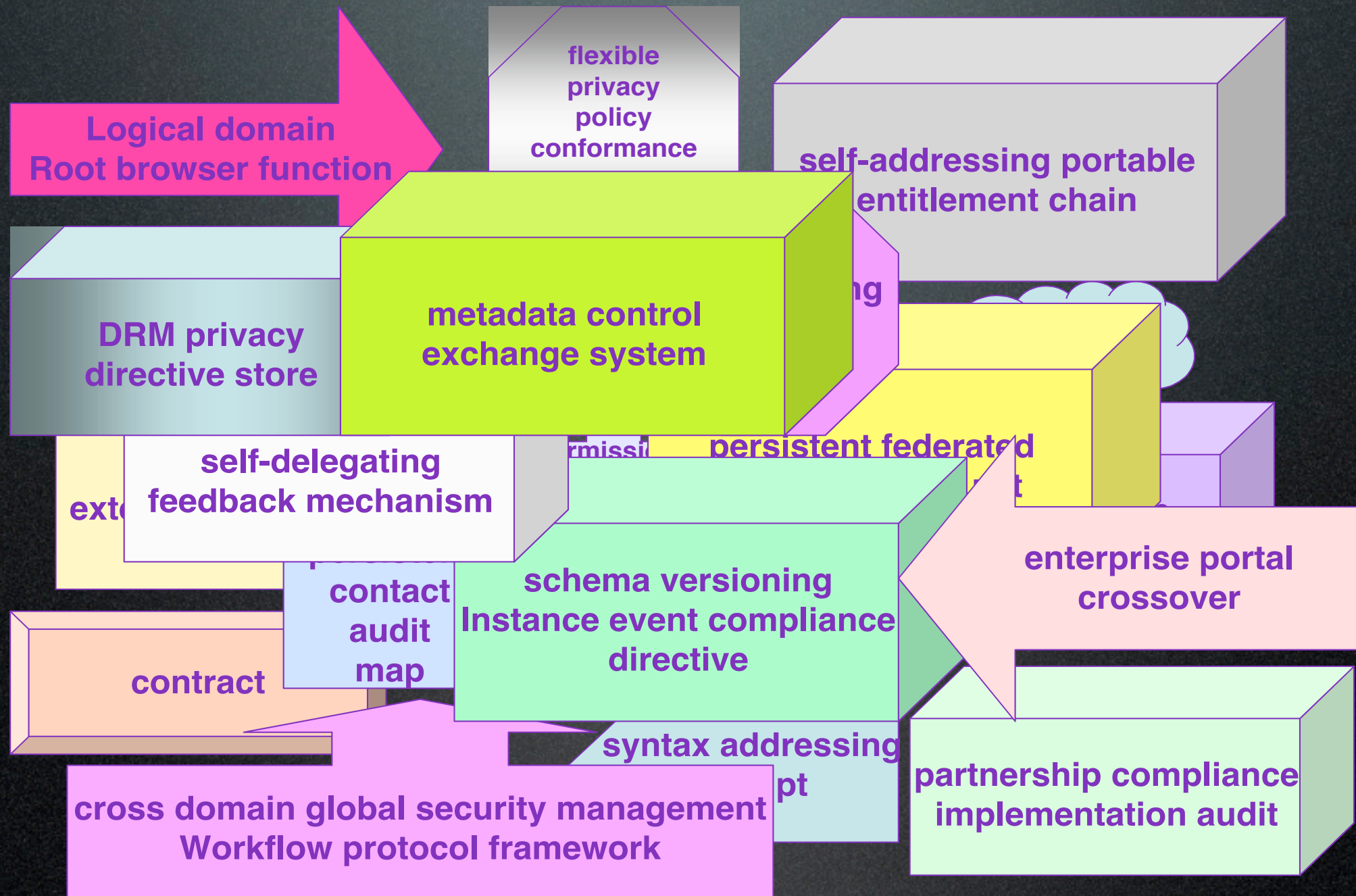
# Blogs and MediaWiki



enterprise identity  
governance



# Identity Infrastructure (as built)



Architecture courtesy of Doc Searls



# Identity Management Architectures



## City Planning

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



# Creating a IMA Strategy

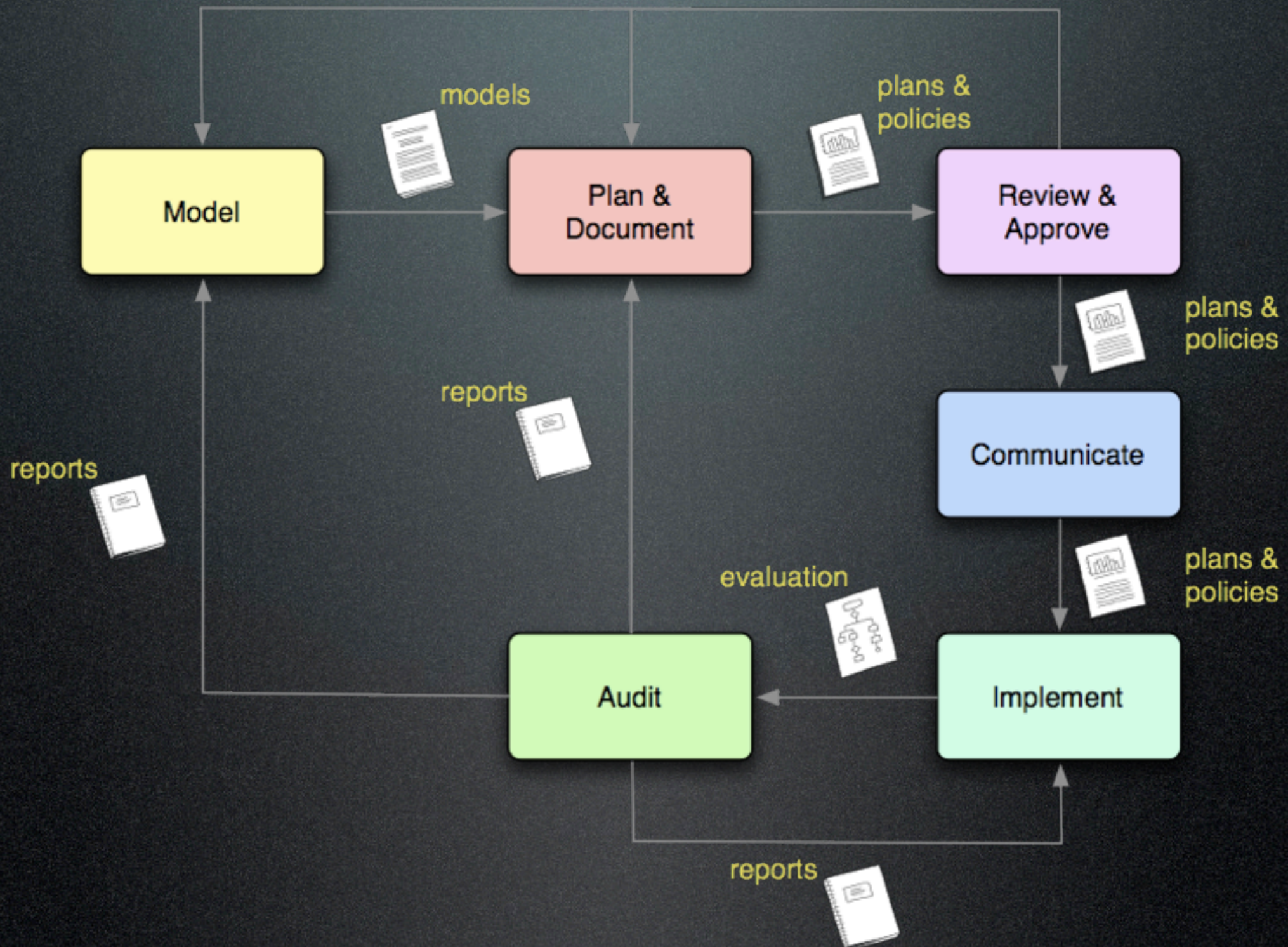
## Key Steps

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



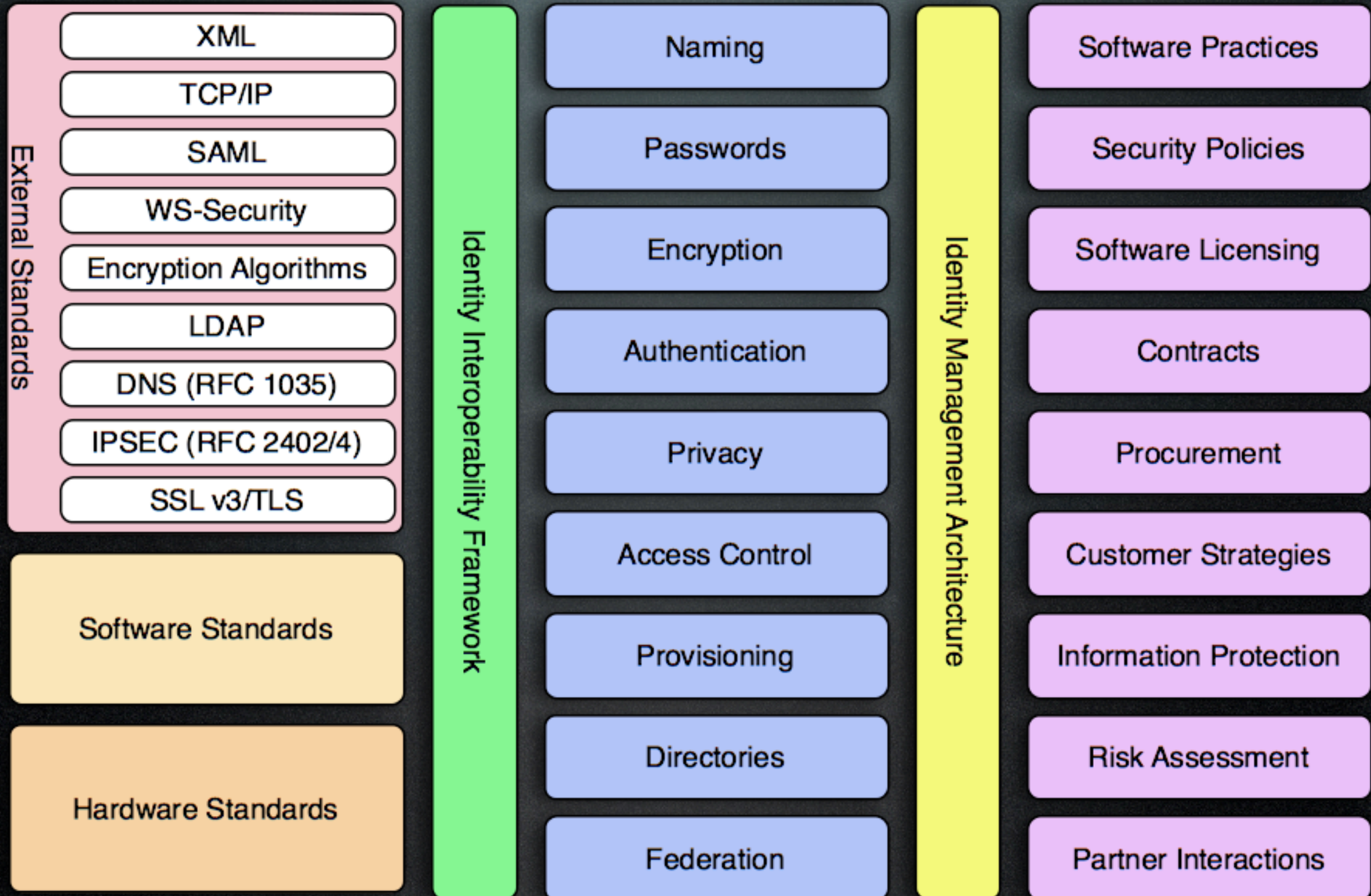


# IMA Lifecycle





# Identity Policy Stack





federation



# Identity Federation



*SourceID*

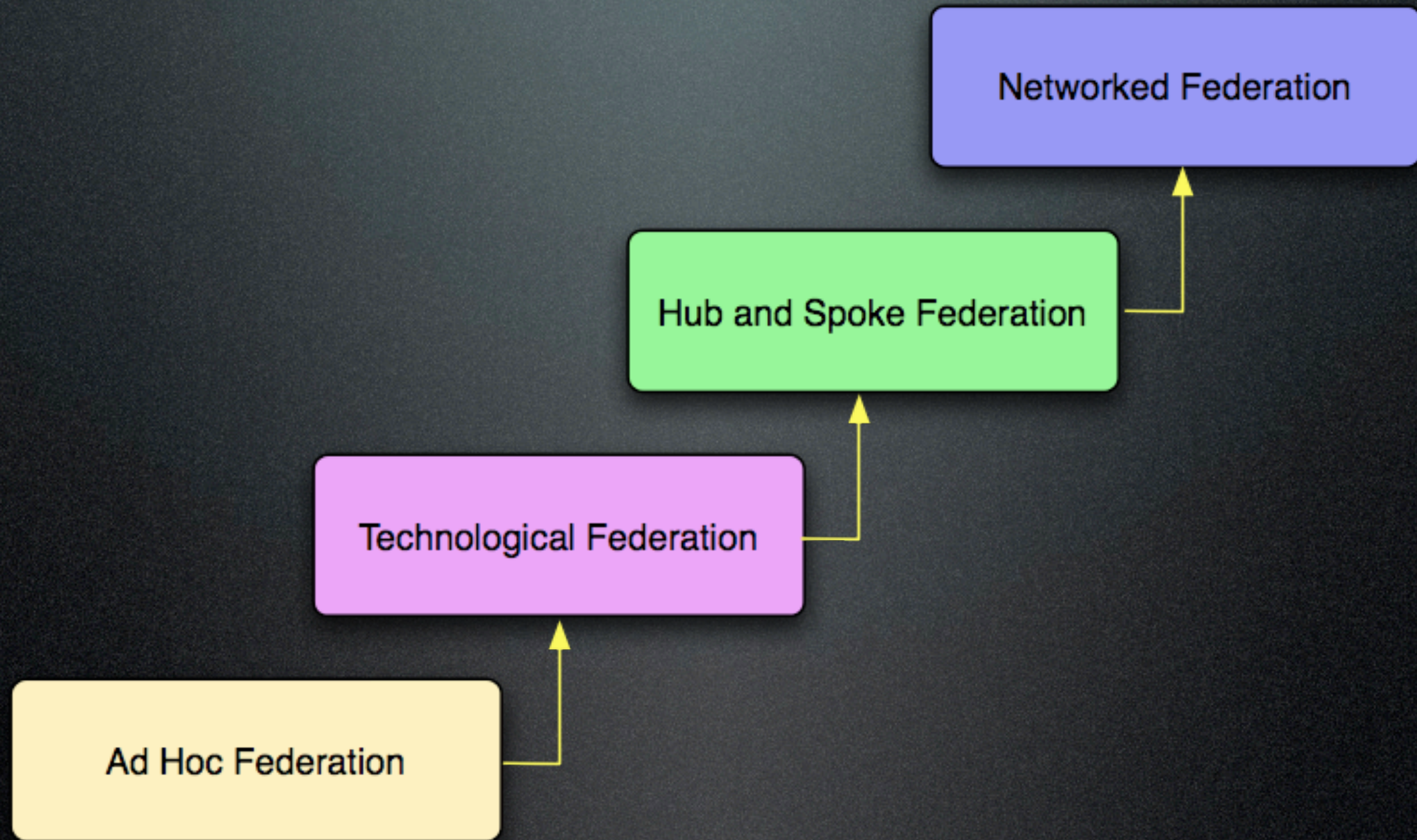


WS-Federation  
**WS-Federation**

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



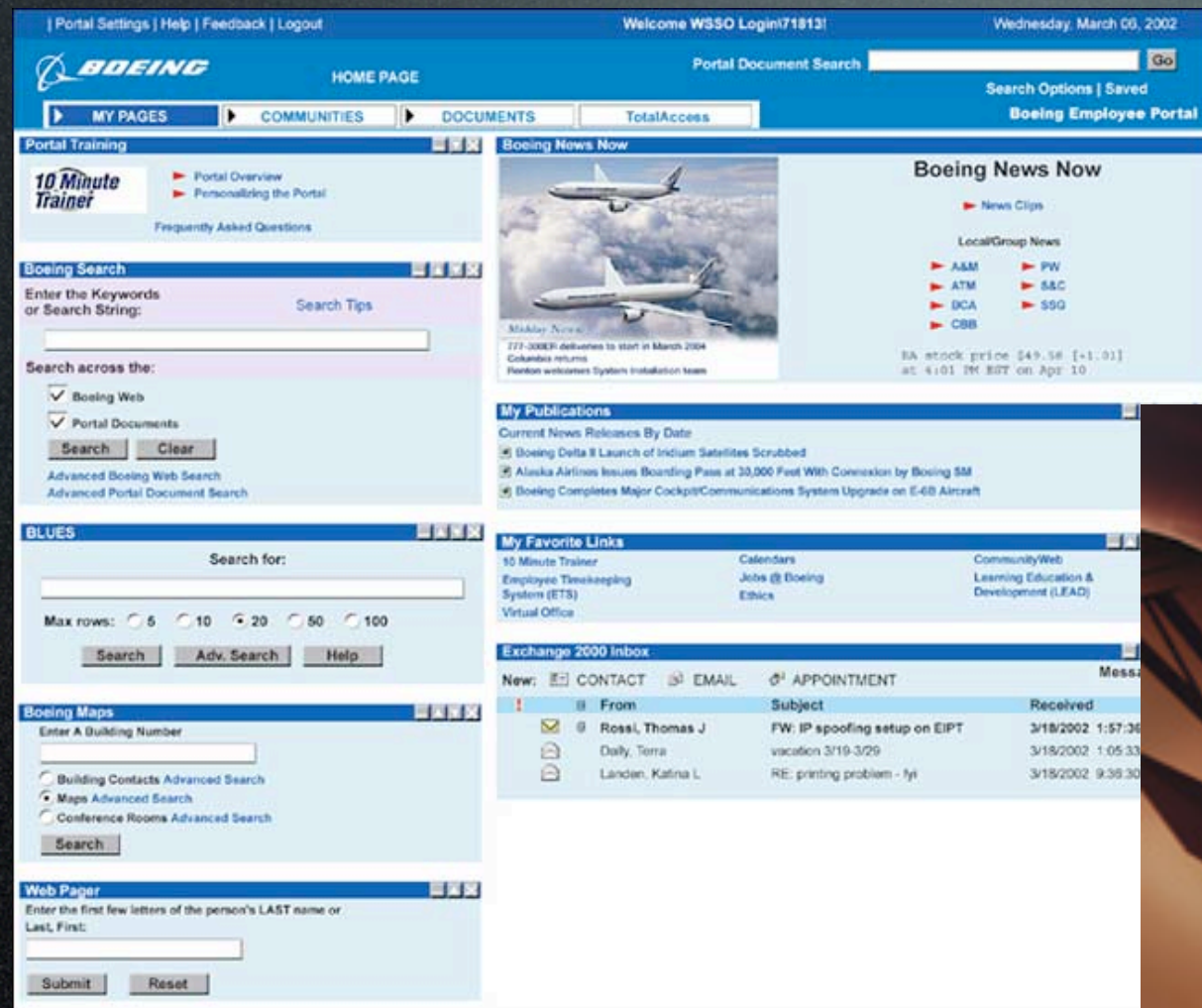
# Federation Maturity





# Liability and Policy

Linking 401K site  
to employee  
portals





user-centric identity



# An identity layer for the Internet



Vint Cerf



# Cameron's Laws of Identity

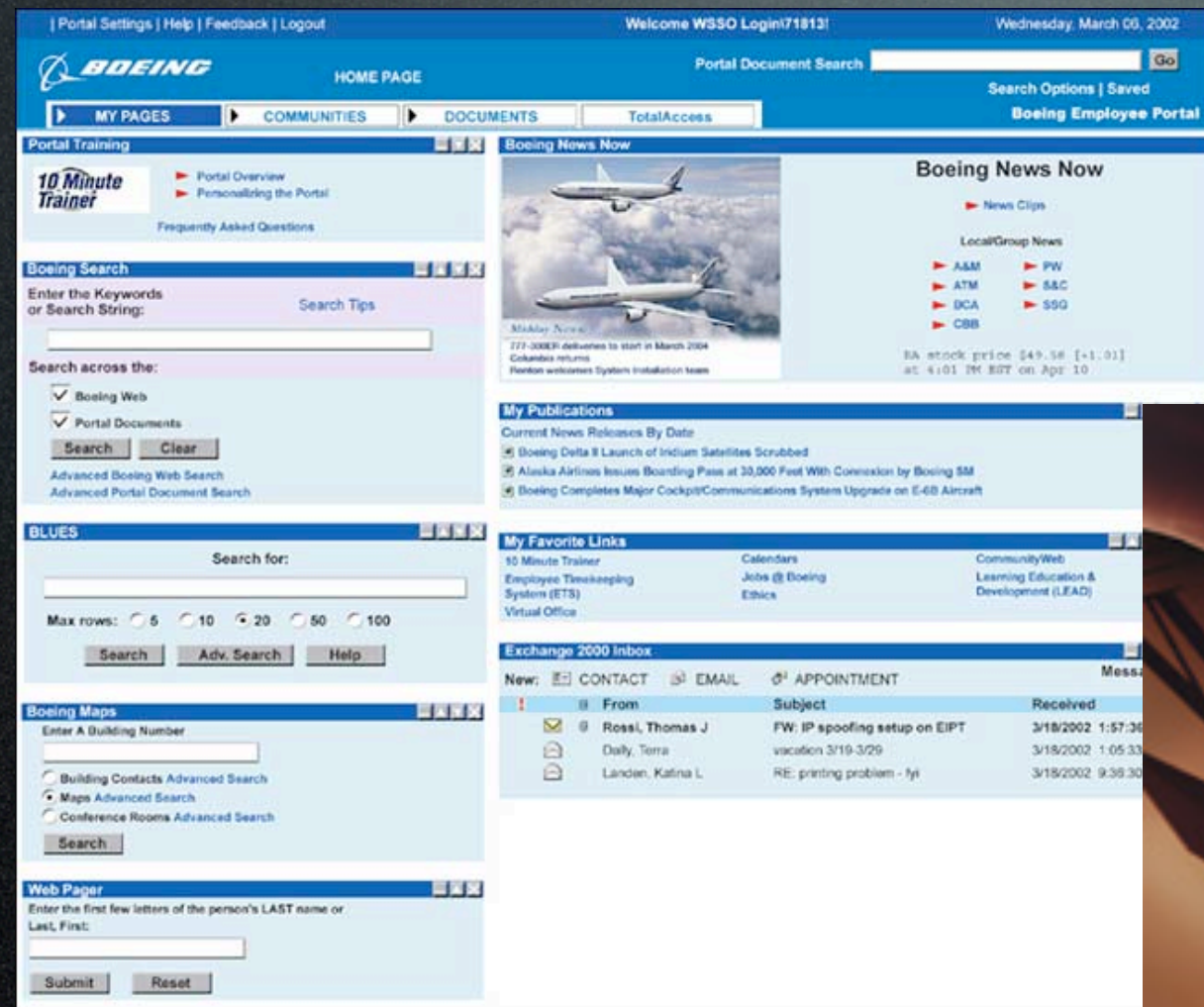
1. User consent and control
2. Minimal disclosure
3. Justifiable parties
4. Directed identity
5. Pluralism
6. Human integration
7. Consistent experience across contexts





# Federation Problems

Linking 401K site  
to employee  
portals





# Roles

1. Identity Provider
2. Relying party



# Roles

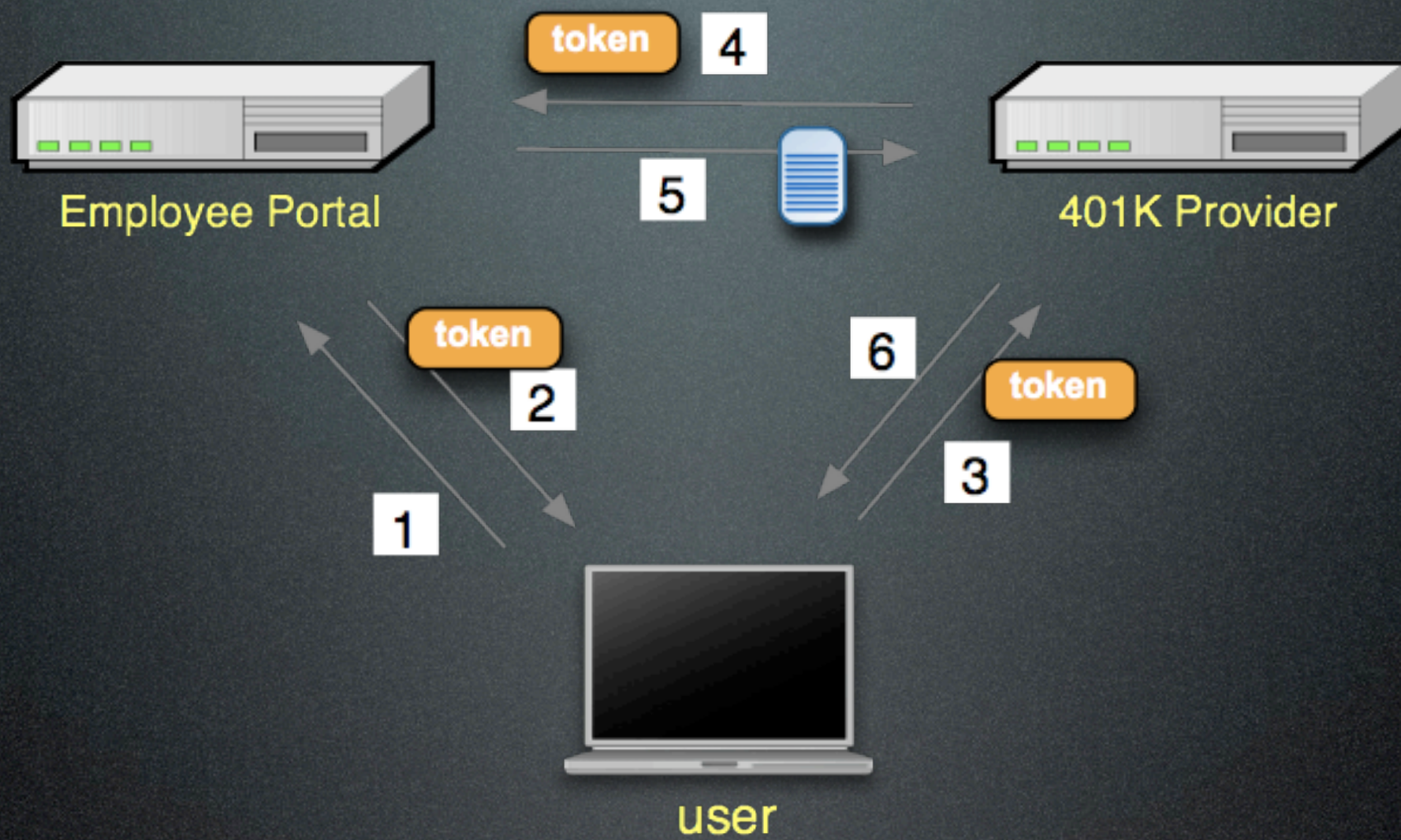
1. Identity Provider
2. Relying party
3. User



# 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



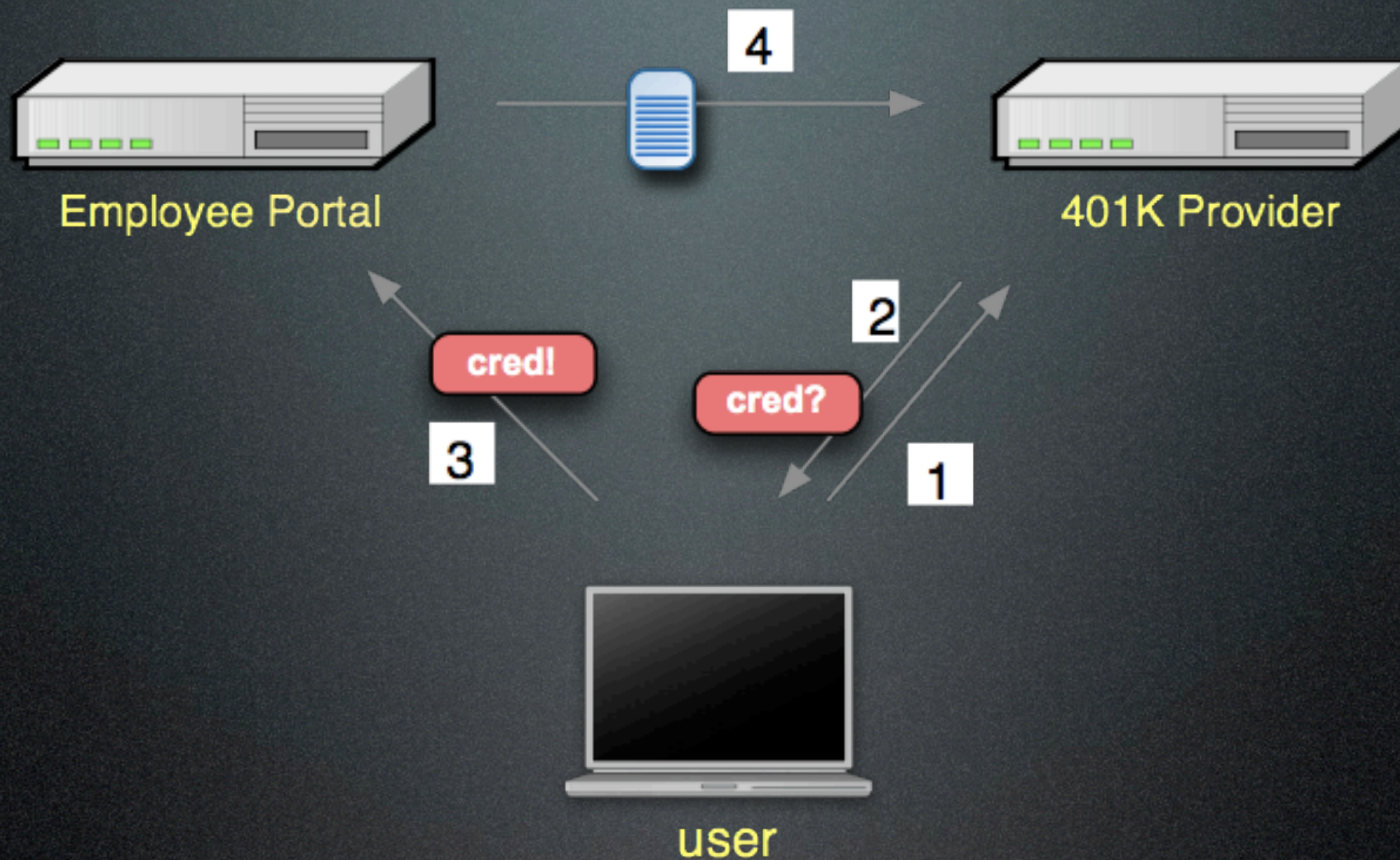


scenario one



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





# scenario two

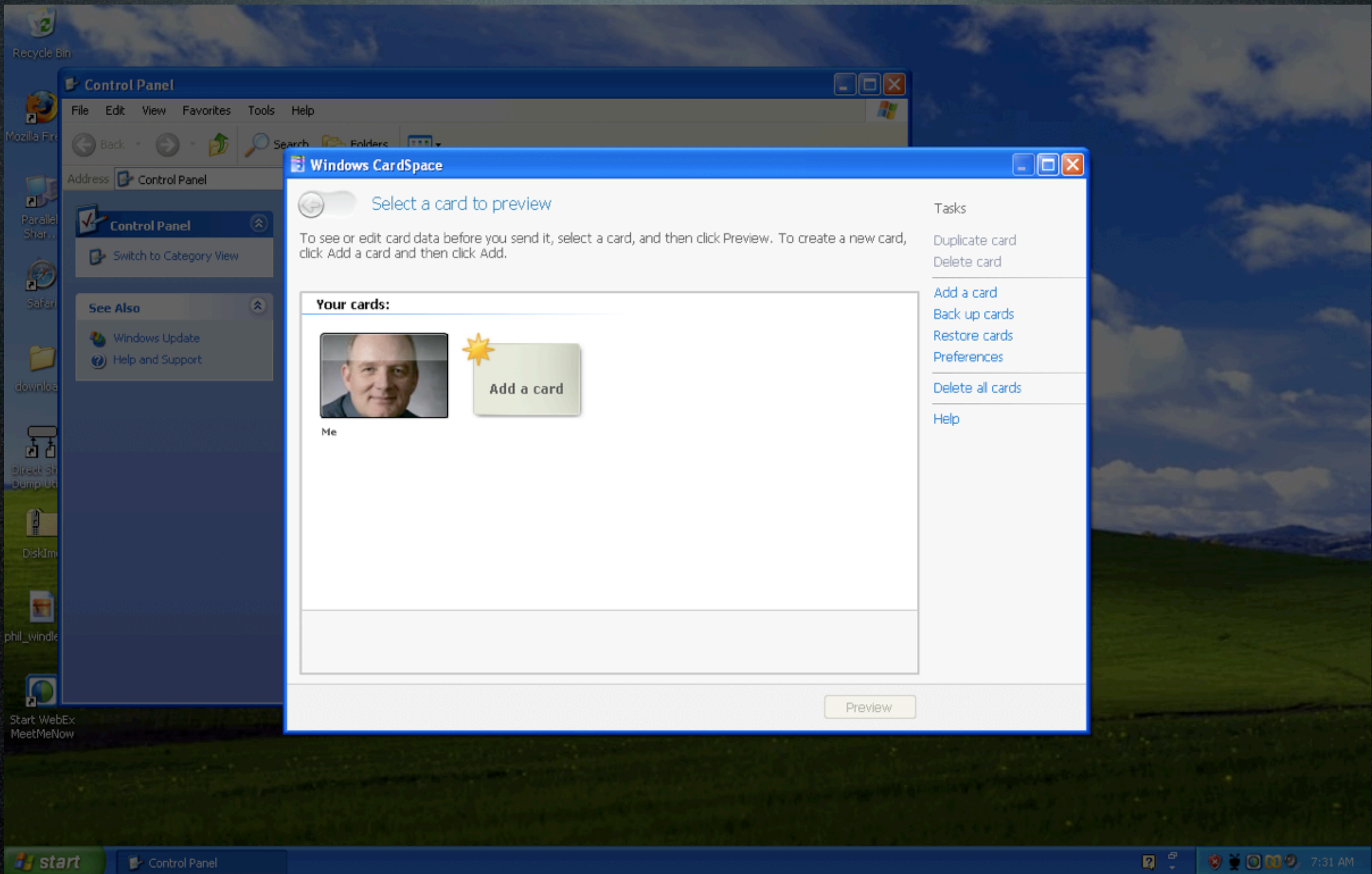


- ID issuer and relying party need no prior agreement
- User involved structurally



# CardSpace





# CardSpace Identity Selector







<http://openid.aol.com/pjwindley>



<http://www.windley.com>



delegation



```
<head>
```

```
...
```

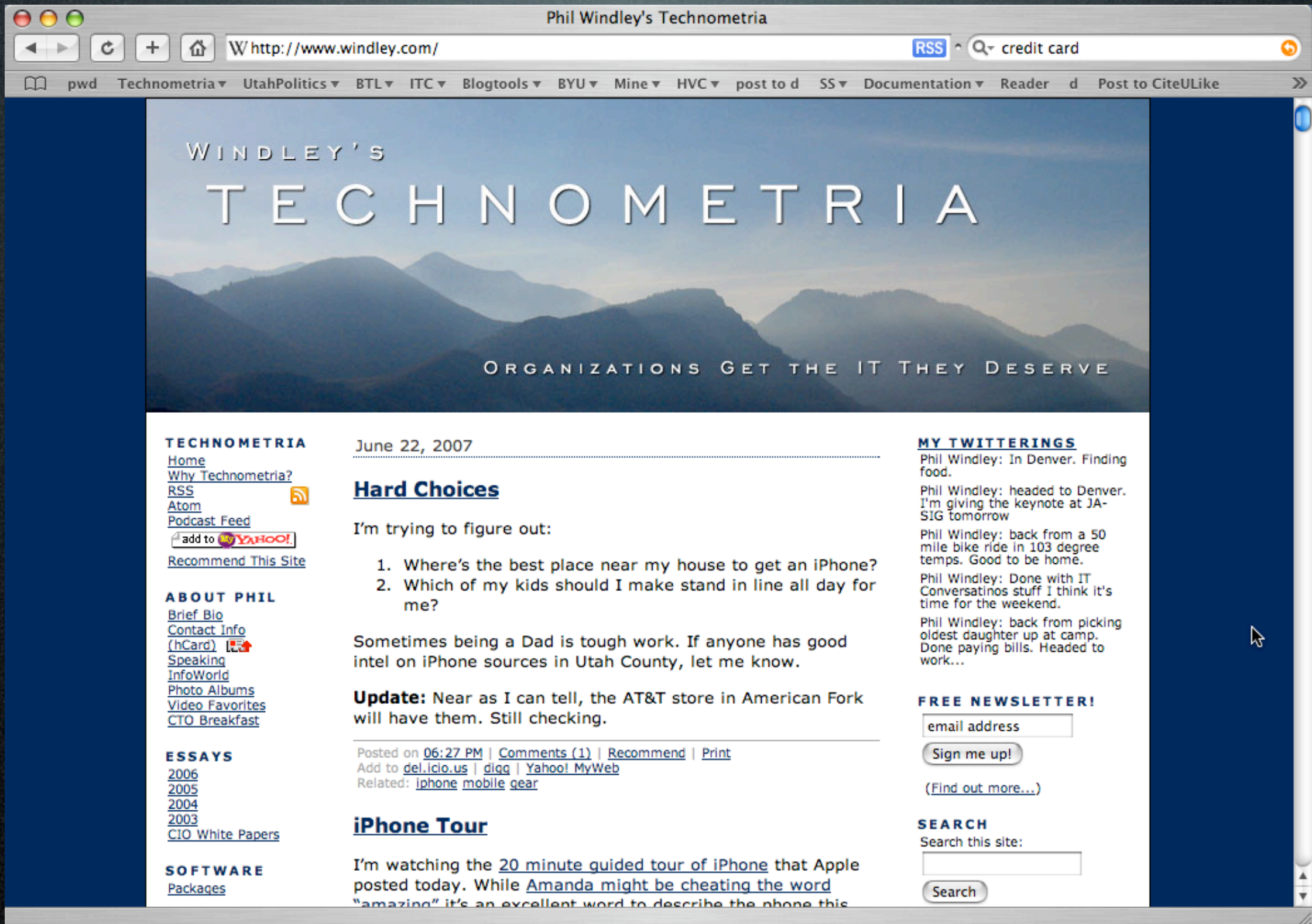
```
<link rel="openid.server"  
      href="https://www.myopenid.com/server" />
```

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

```
...
```

```
</head>
```





OpenID Screenshot



# Using OpenID



Internal deployments  
useful for loosely  
coupled organizations



Wide-area  
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 relying party
- Novell is building identity selectors for Cardspace



# 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





the end



# Contact Information

## Contact me

- [phil@windley.com](mailto:phil@windley.com)
- [www.windley.com](http://www.windley.com)

## Questions?



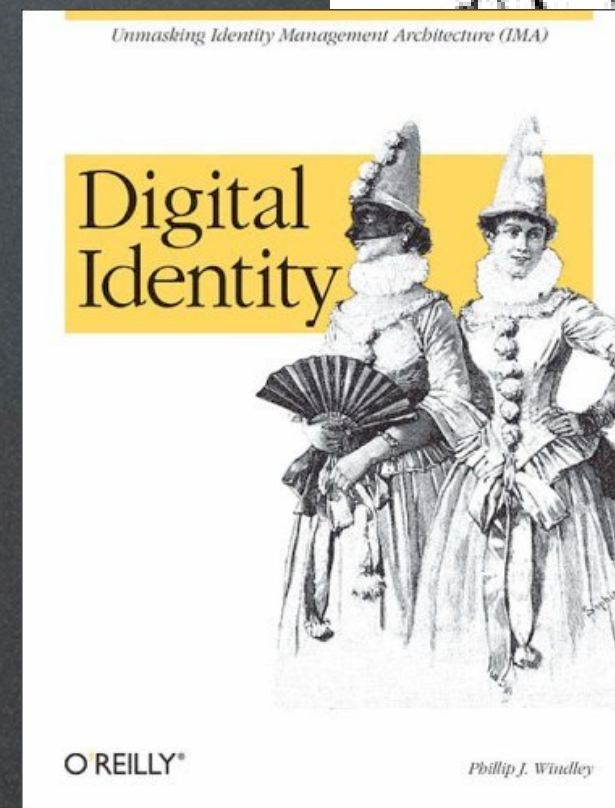


# Contact Information

## Contact me

- [phil@windley.com](mailto:phil@windley.com)
- [www.windley.com](http://www.windley.com)

## Questions?





# Contact Information

## Contact me

- [phil@windley.com](mailto:phil@windley.com)
- [www.windley.com](http://www.windley.com)

## Questions?

**Buy the book!!!**

