

Identity 2.0

Phillip J. Windley
Brigham Young University

phil@windley.com
www.windley.com

Unmasking Identity Management Architecture (IMA)

Digital Identity



O'REILLY®

Phillip J. Windley

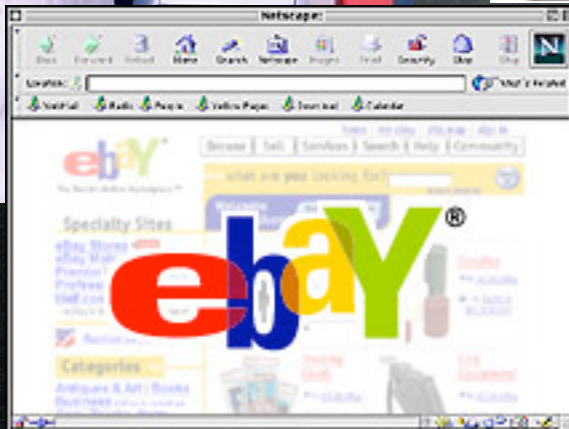
www.windley.com

Does Identity Matter?



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

Does Identity Matter?



What is an Identity?



**METROPOLITAN
PORT AUTHORITY**

**Allen Bishop
Inspector**

I.D. 0006-398-99



PASSPORT



*United States
of America*

 **Bank of New Zealand** CLASSIC CARD

4999 7700 1234 5678
4999

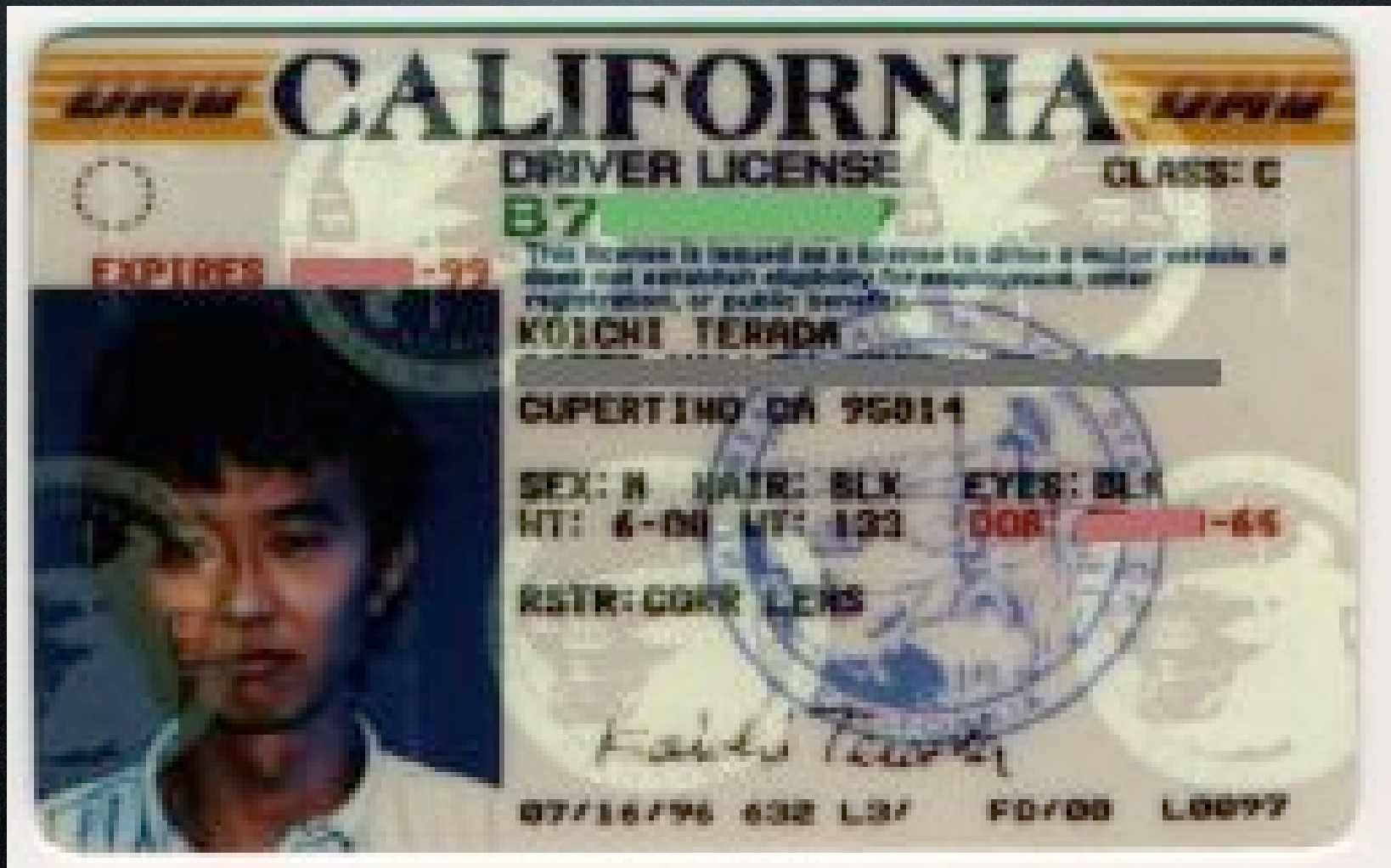
VALID FROM 00/00 MONTH YEAR EXPIRES END OF 00/00 MONTH YEAR

YOUR NAME

VISA



Credentials



Buying Beer



What Happened to the Walls?



What Happened to the Walls?



The Border Patrol



Business Context of Identity



vs



Wide Area Identity

- Federated identity
- Internet identity
- Modalities
 - Tokens
 - Addresses

Credential Context



Credential Context

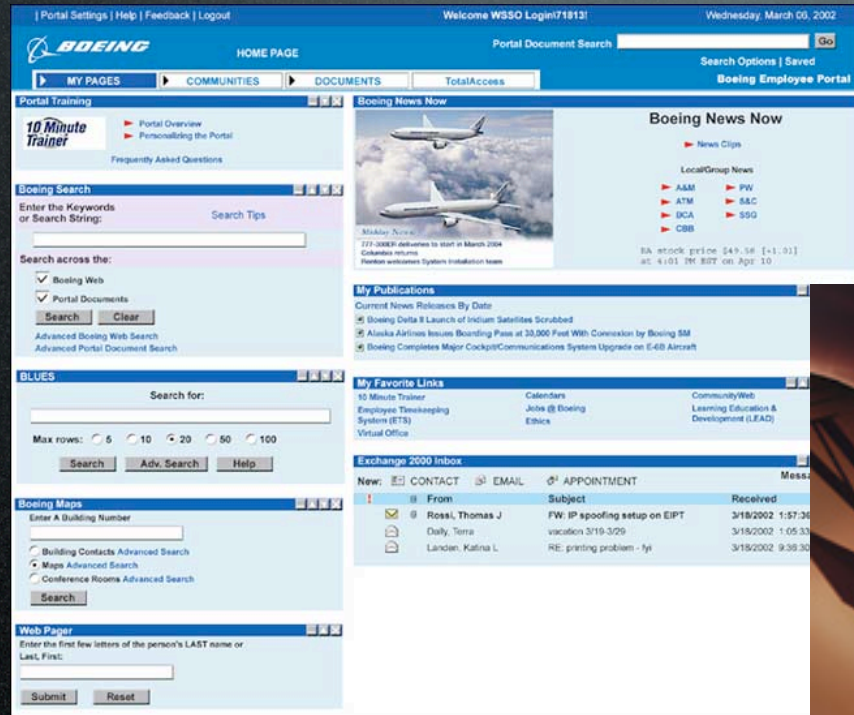


Credential Context



Token Use Case

Linking 401K site
to employee
portals

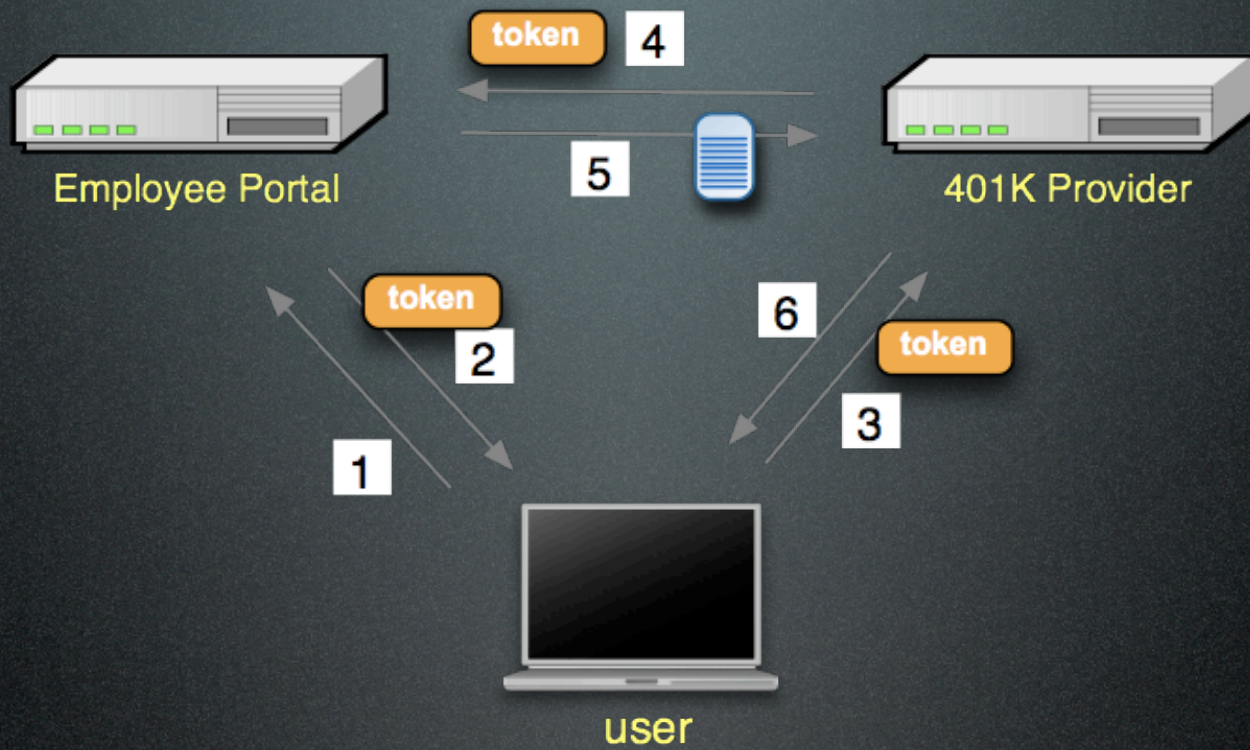


Roles

1. Identity issuer
2. Relying party

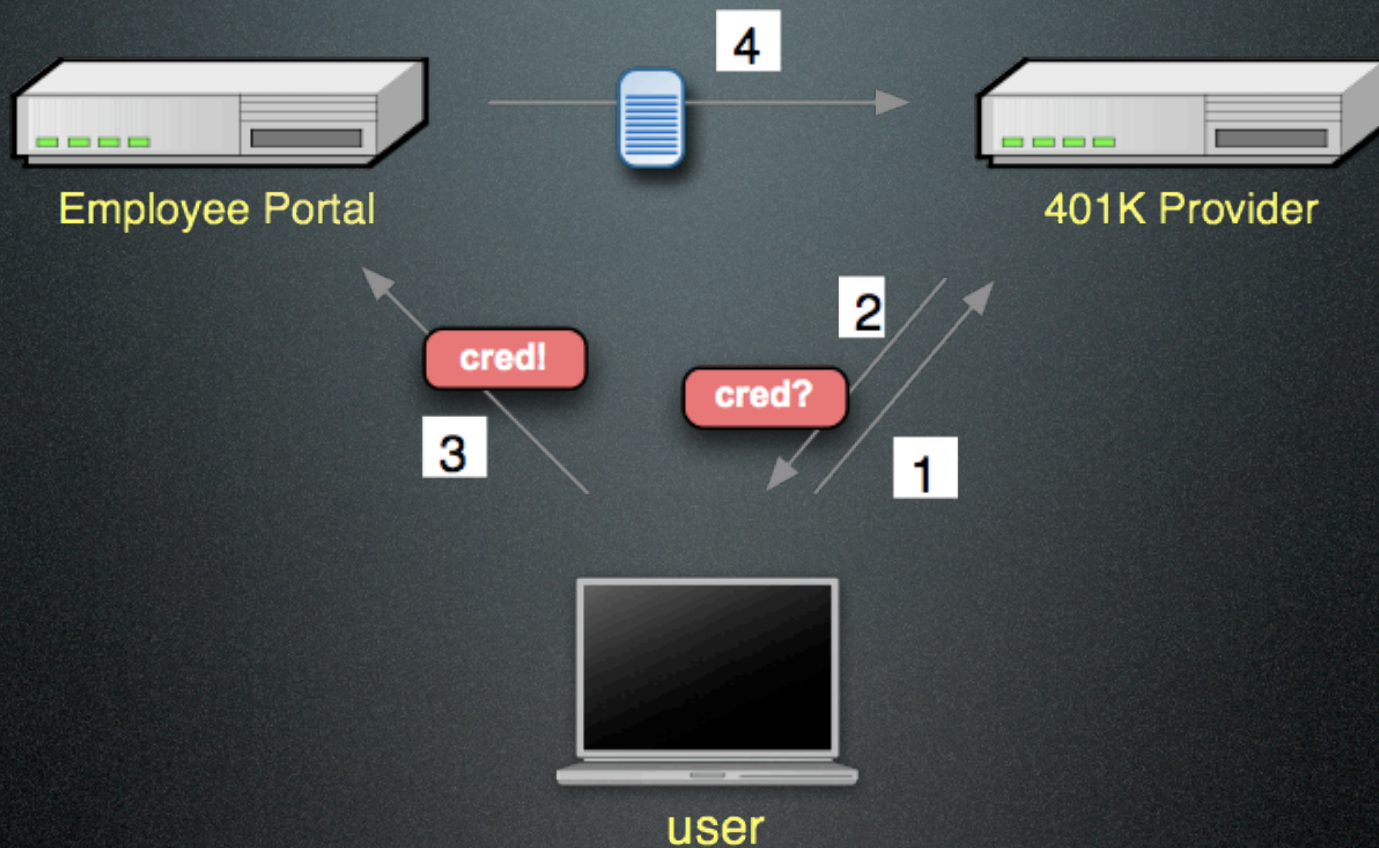
Roles

1. Identity issuer
2. Relying party
3. User



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

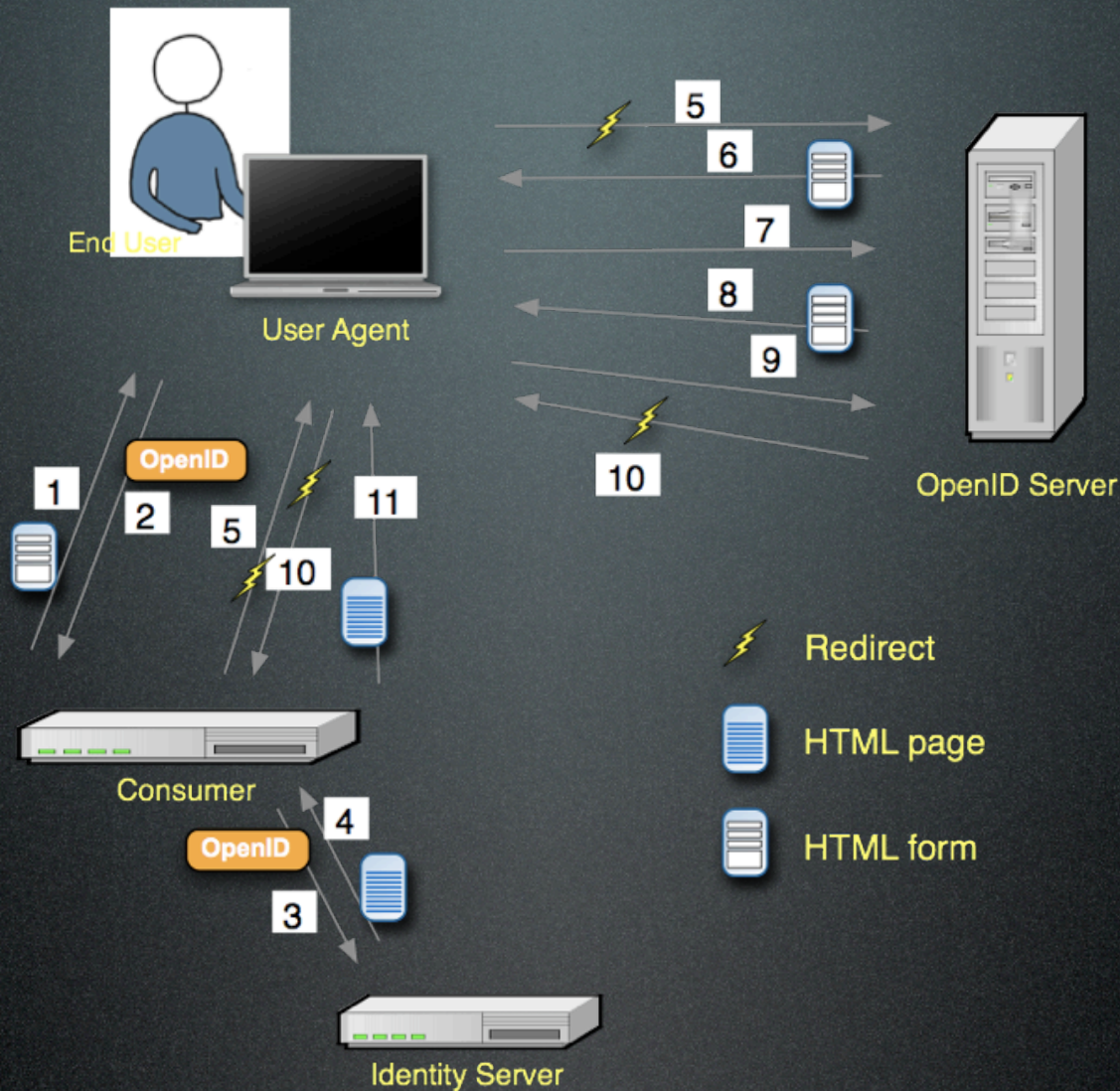
Internet Identity Technologies

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

OSIS Announcement



June 20, 2006, Berkman Identity Mashup



OpenID interactions

Reputation

About the ship, Wendy bravely walked the plank, reached the end, and stepped off.

(WENDY) Oohhh!

And just as she was about to land in the water...

(PAN) Wendy! Wendy!

(JOHN) Look, Michael, it's Peter Pan!

Down swooped Pan, catching Wendy, he brought her to the deck.

(BOYS) Hurry!

Pan drew his dagger and laid the cruel plan.

(PAN) Now, Hook, prepare to die!

(HOOK) Why, you stinked! I'm! My sword will slash you in ribbons!

But Hook was too much for the clever Pan.

(HOOK) Sinner! Help me!

(SMEE) Sorry Cap'n, we're leaving!

Like the cowardly they were, the crew deserted.

(PIRATE) Lower the longboat!

(SMEE) Row for your lives, now!

Now, with a final lunge, Pan threw Hook right through the ship's

rail... And that was the end of Captain Hook. For waiting in the

water was one old friend, the crocodile... who was tamed. E.E.

(TICK-TOCK TICK-TOCK TICK-TOCK)



Your story about me

Principles of Reputation

- Trust based on reputation
- Exists in the context of community
- Reputation *based* on identity
- Reputation is a currency
- Reputation is multi-level

$$r_{id} \approx f(\phi, T_x, \rho)$$

CS601

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

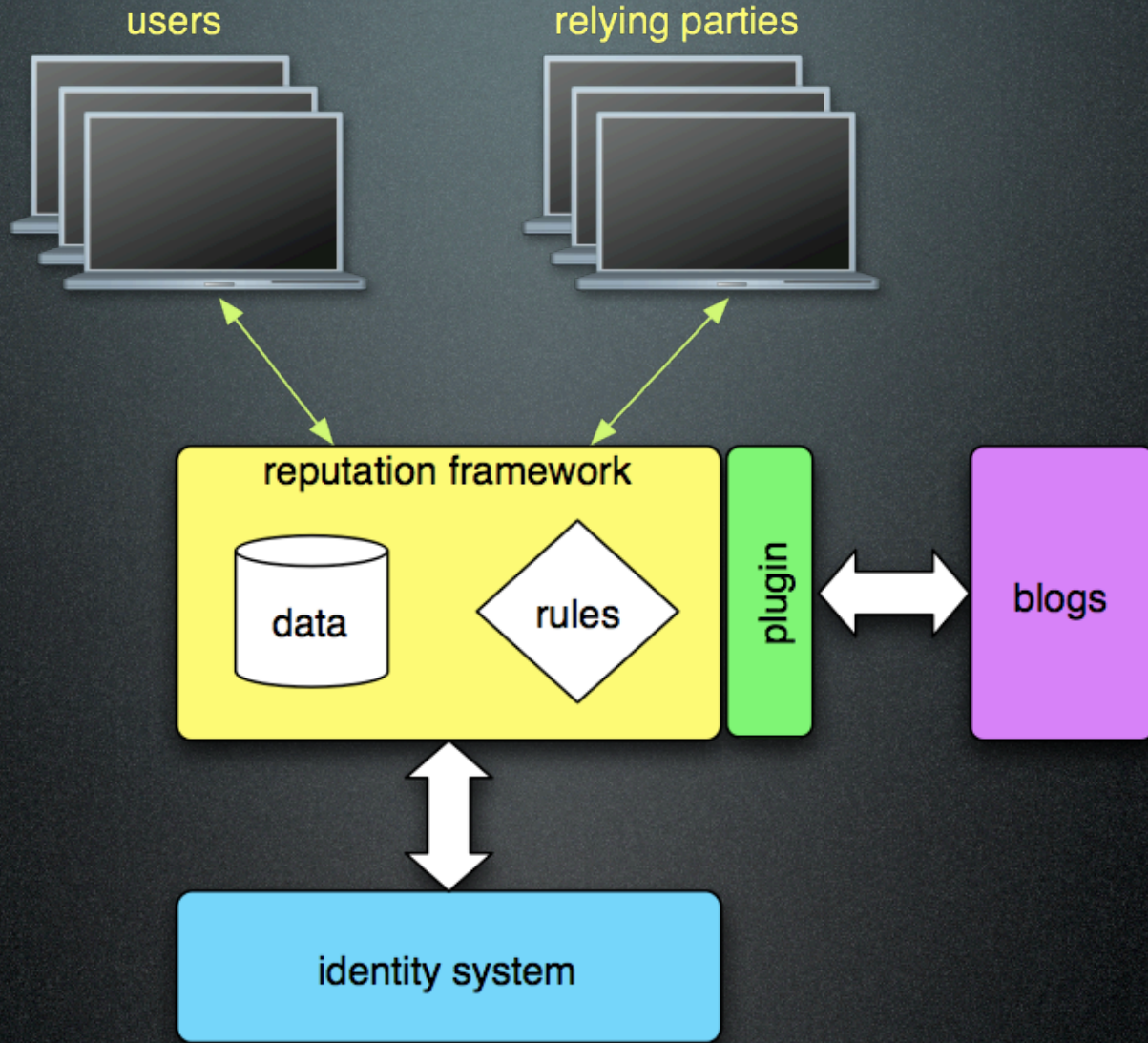
Design Philosophy

- Reputation is a calculated score
- Factors
 - verified facts and credentials
 - transactions
 - 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

You've got to start
somewhere

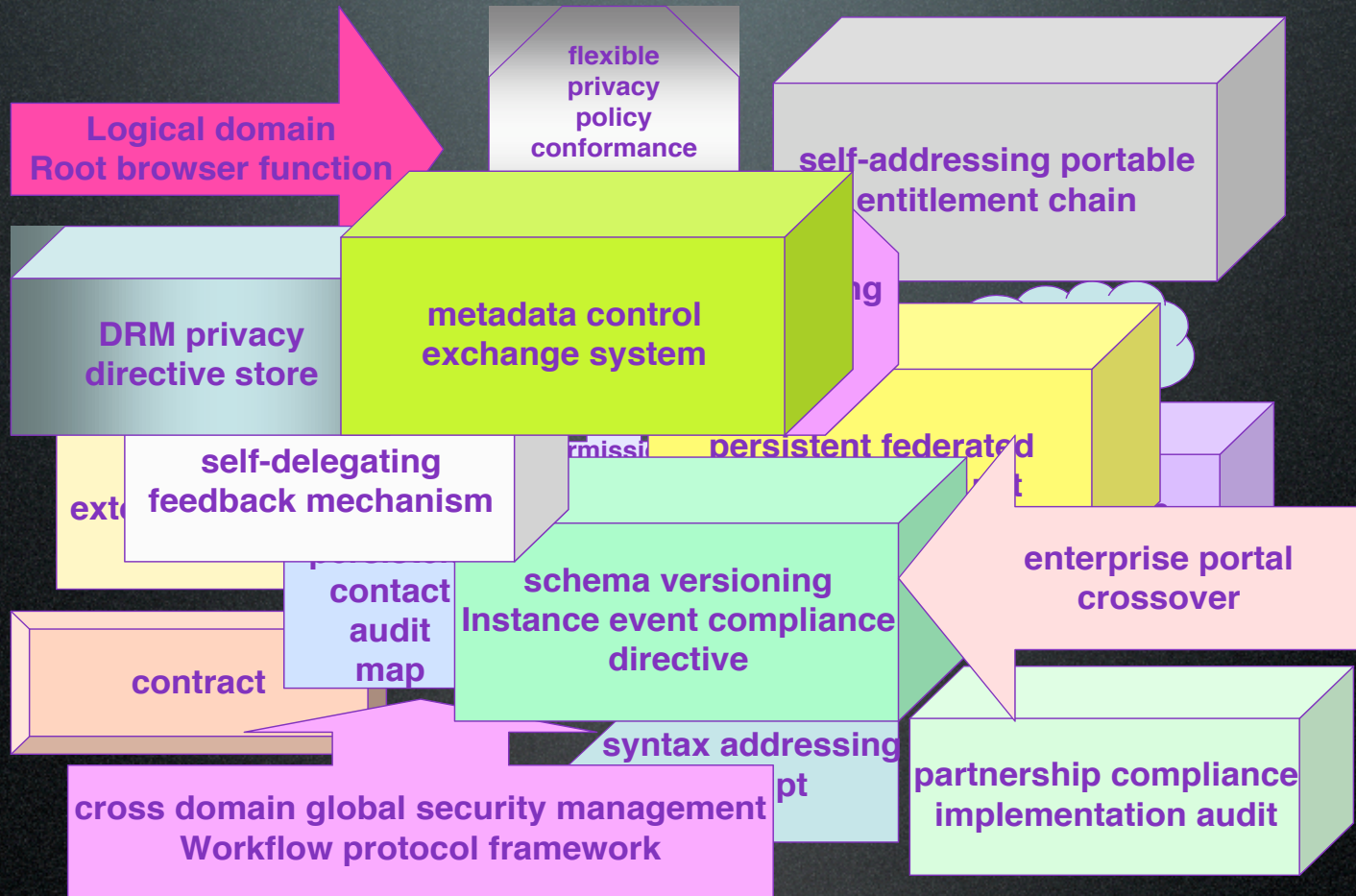


Future Reputation Work

- Ratings and endorsements
- Interuser trust
 - claim bloglines OPML, friends
- Check other network data
- Identity broker
- Credential validation

Identity in the Enterprise

Identity Infrastructure (as built)



Architecture courtesy of Doc Searls

Identity Management Architectures



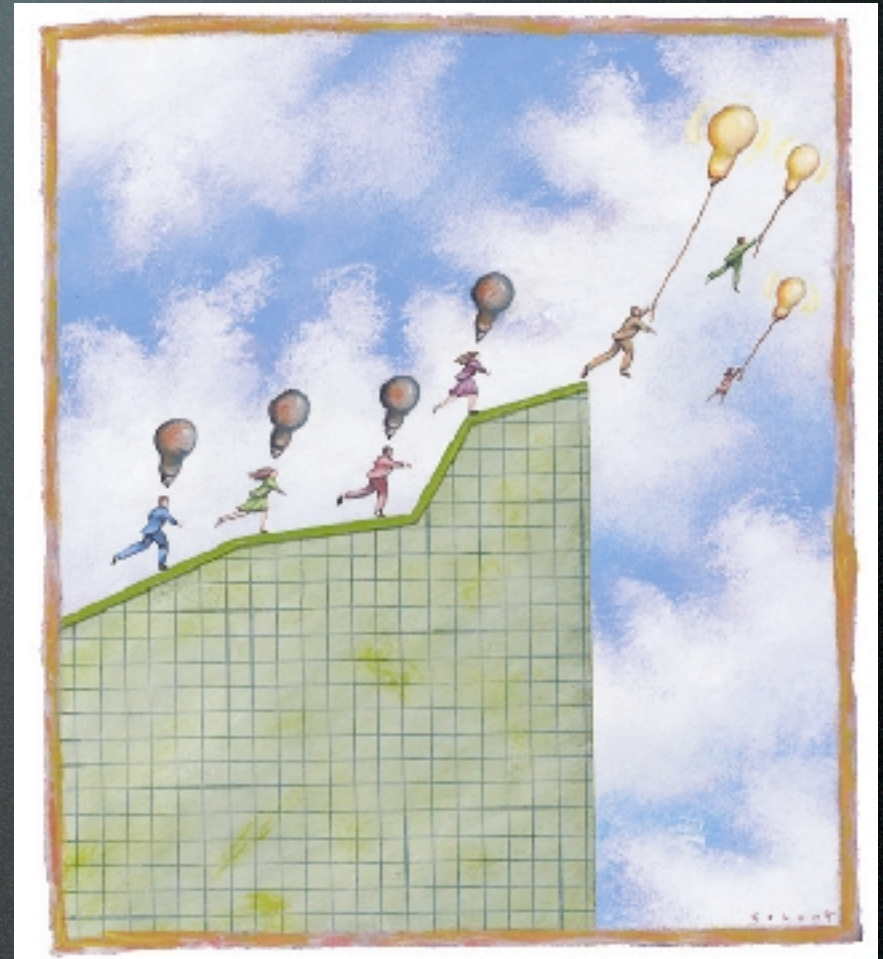
City Planning

- 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



Accountability vs. Enforcement

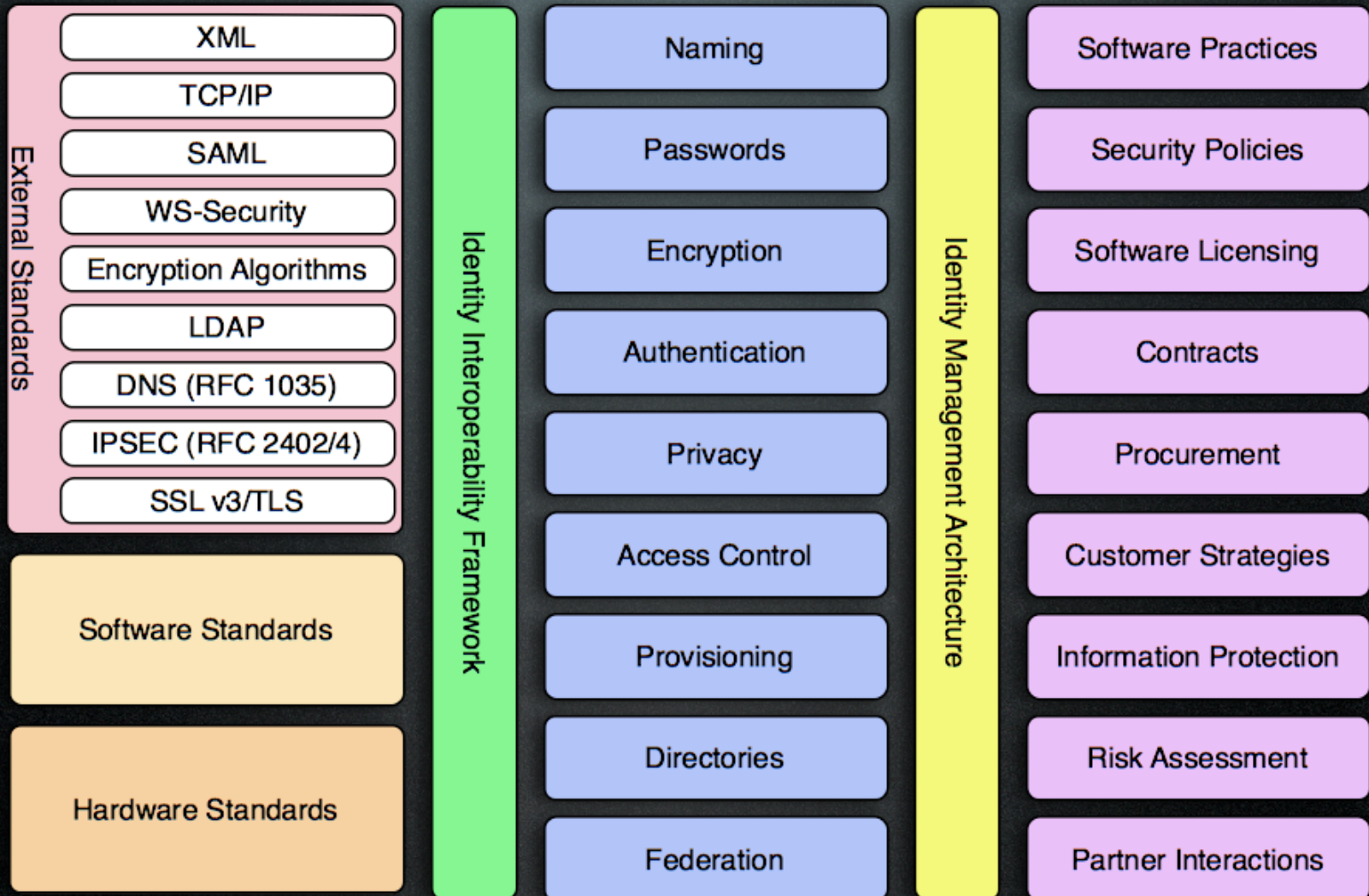


“Accountability is
a log processing
problem”

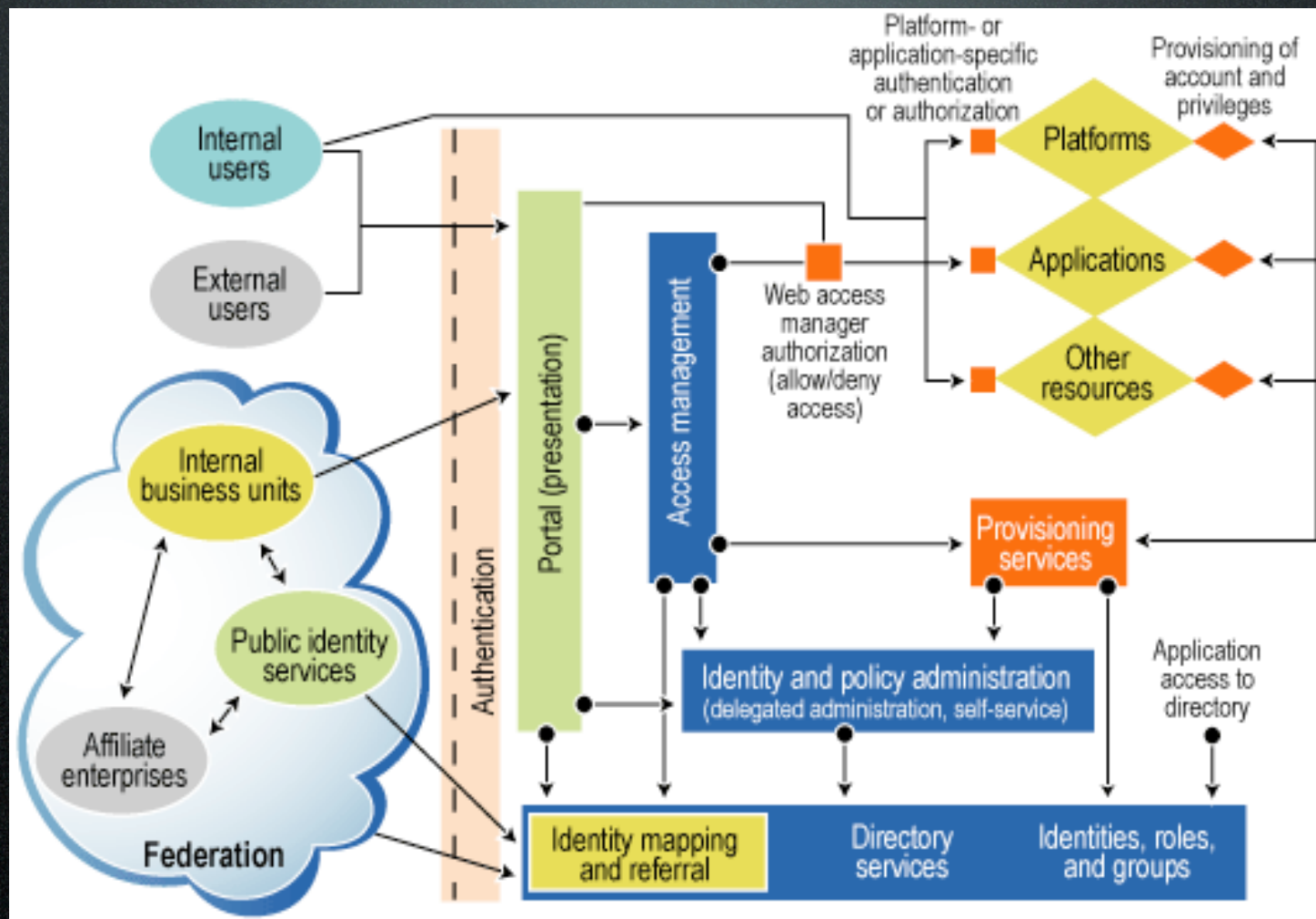
-Dan Geer

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

Identity Policy Stack



Reference Architecture





The End

Contact Information

Contact me

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

Buy the book...

Questions?

