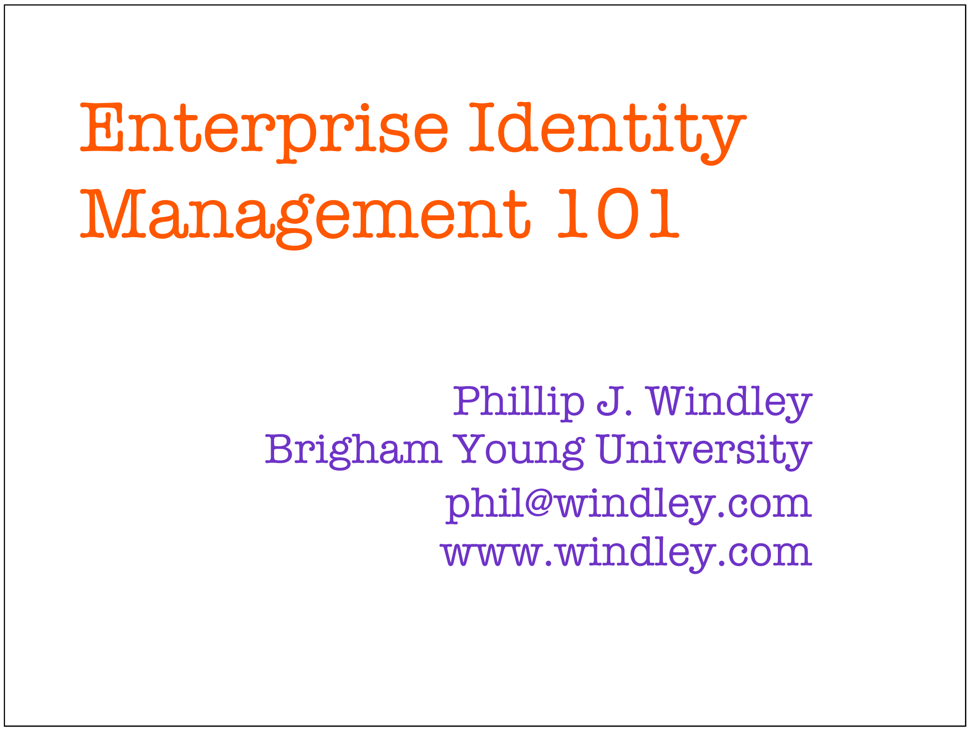


Enterprise Identity Management 101

Phillip J. Windley
Brigham Young University
phil@windley.com
www.windley.com

Digital Identity Matters

Rifkin on service economy and what it portends for identity: commercial transactions based on property can be relatively anonymous, not services. This raises the burden of authentication

Trends:

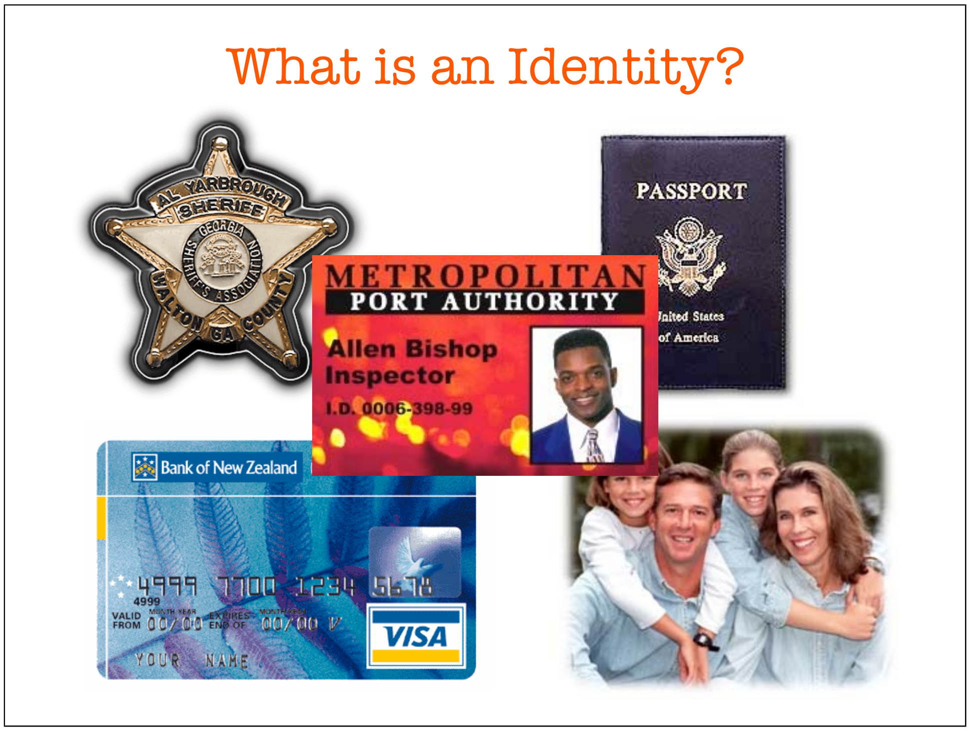
Service economy

Reduced anonymity

Electronic delivery

Result:

Digital identity matters!



What is an Identity?

An **Identity** is a set of:

Attributes - medical history, past purchasing behavior, bank balance

Preferences - currency used, what brand of hot dog you like, blue background on the screen

Traits - eye color, where a business was incorporated

About a **subject**

Subjects make requests relative to a **resource**

Outside looking in or inside looking out. Inside looking out is more holistic. Concentrate on that, even if you're outside. Iit drives user behavior and attitudes.

Credentials

Evidence of the right to an identity

Transfer of trust

Policy enforcement point (**PEP**) **authenticates** credentials

Policy decision point (**PDP**)

- determines **permissions** and **entitlements**
- In accordance with an **access policy**

PDP communicates a **authorization decision assertion** to the PEP

Buying Beer

Coors
CALIFORNIA
DRIVER LICENSE
Bank of New Zealand CLASSIC CARD
4999 7700 1234 5678
VALID FROM 00/00 EXPIRES END OF 00/00
YOUR NAME
VISA

Driver’s license

Identity

Attributes

Preferences

Traits

Authentication

Authorization

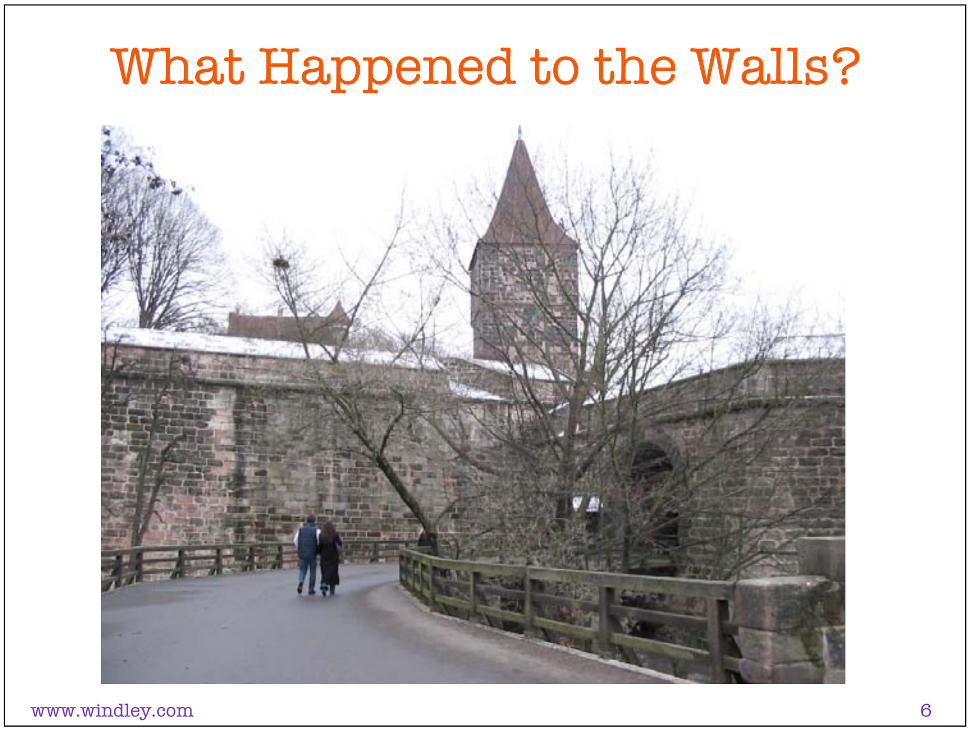
Credit card

Signed credential

External PDP

When a person (i.e. the subject) wants to buy beer (i.e. perform an action on a resource), the clerk (i.e. security authority) examines the license to see if it looks real (i.e. determines the validity of the credential) and uses the picture (i.e. embedded biometric device) to see if the person presenting the license is the same person who owns it (i.e. authenticates the credential). Once certain that the license is authentic, the clerk, reads the birth date (i.e. attribute) from the license and determines whether the person is over 21 (i.e. consults a security policy determined by the state and makes a policy decision about permissions associated with the identity).

The credit card (a separate identity credential) is presented to the



What Happened to the Walls?

www.windley.com

6

City defenses were based on walls.

Limits commerce

Trebuchet made city walls obsolete

The Border Patrol

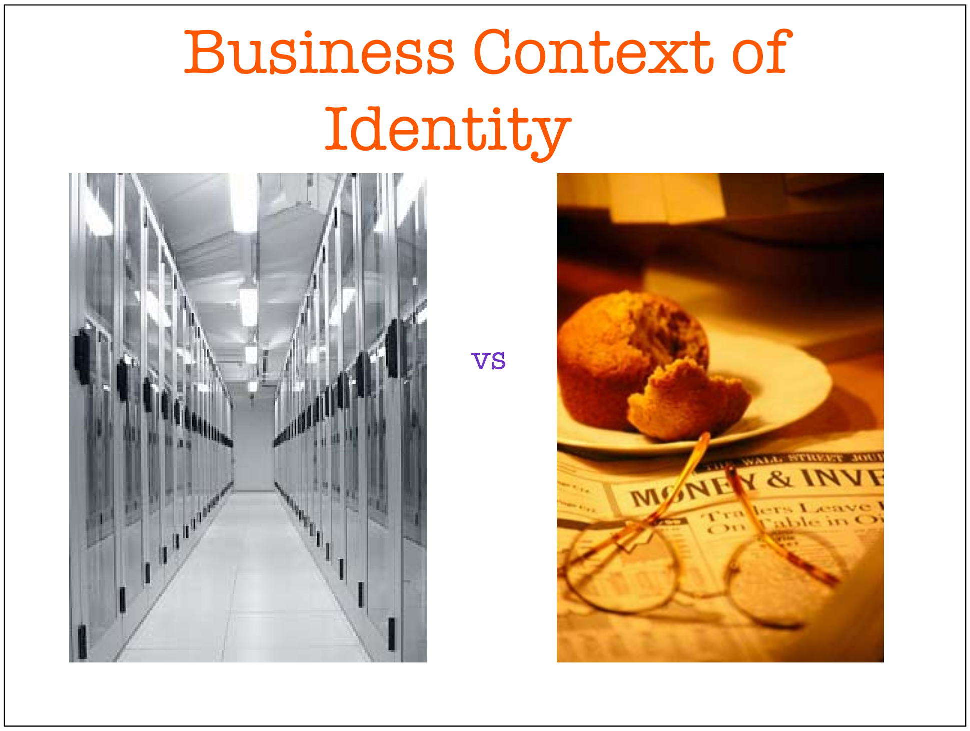
Corporate security is likewise based on a perimeter strategy.

Limits commercial activity, but has been driven by IT based on a security analysis.

Recent trends reduce this strategy to rubble. Examples:

VPNs and Wi-Fi

Web Services



Business Context of Identity

vs

Traditionally focused on machines and networks

Business needs will drive security policies

Policies need to talk about

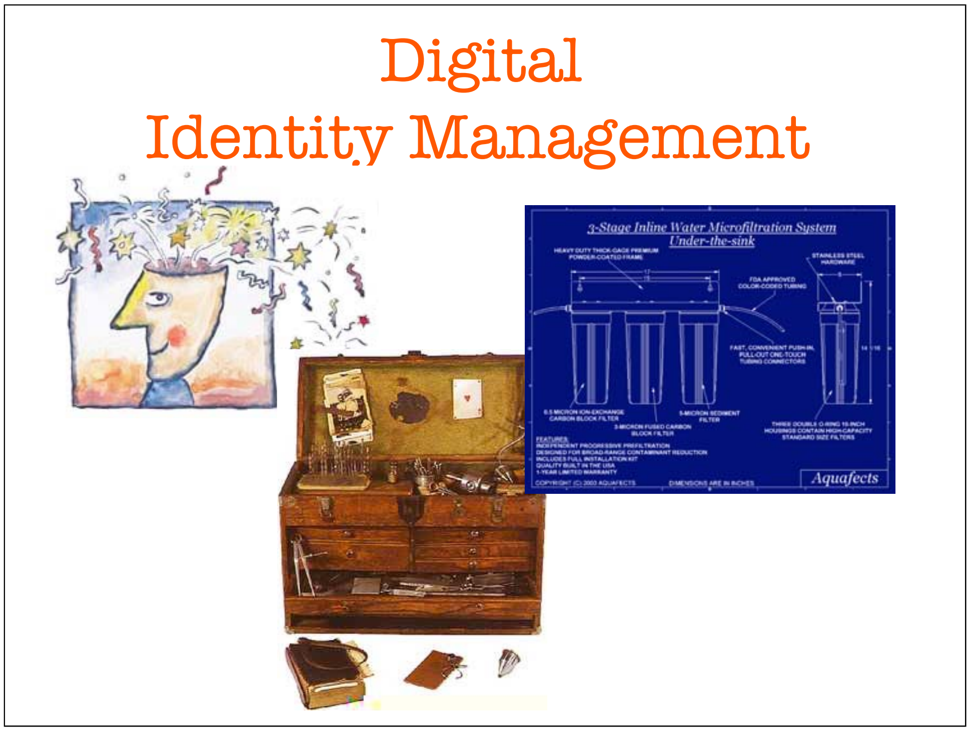
- Documents
- Actions
- Data
- People

Security has been focused on defense

Digital identity is focused on opportunity:

- Employees
- Partners
- Customers

Properly implemented digital ID strategy is an enabler for other strategic initiatives



Digital Identity Management

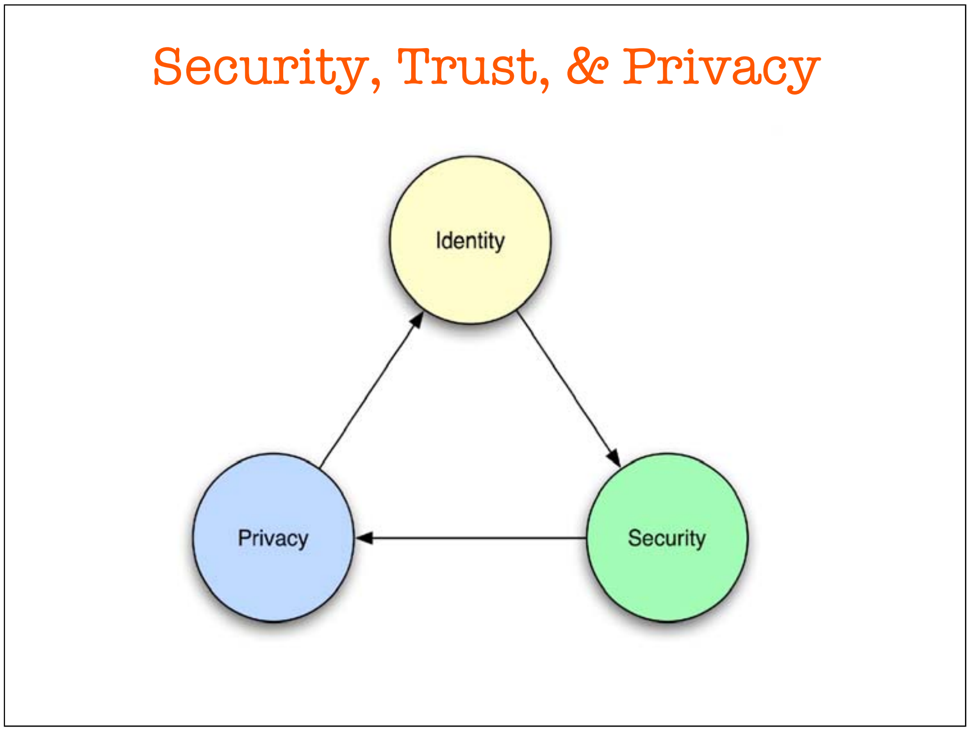
3-Stage Inline Water Microfiltration System
Under-the-sink
HEAVY DUTY THICK-GAGE PREMIUM POWDER-COATED FRAME
STAINLESS STEEL HARDWARE
FDA APPROVED COLOR-CODED TUBING
FAST, CONVENIENT PUSH-IN, PULL-OUT ONE-TOUCH TUBING CONNECTORS
0.5 MICRON ION-EXCHANGE CARBON BLOCK FILTER
5-MICRON SEDIMENT FILTER
3-MICRON FUSED CARBON BLOCK FILTER
THREE DOUBLE O-RING 10-INCH HOUSINGS CONTAIN HIGH-CAPACITY STANDARD SIZE FILTERS
FEATURES:
INDEPENDENT PROGRESSIVE PREFILTRATION
DESIGNED FOR BROAD-RANGE CONTAMINANT REDUCTION
INCLUDES FULL INSTALLATION KIT
QUALITY BUILT IN THE USA
1-YEAR LIMITED WARRANTY
COPYRIGHT (C) 2003 AQUAFECTS
DIMENSIONS ARE IN INCHES
Aquafects

Concepts, tools, ways to plan

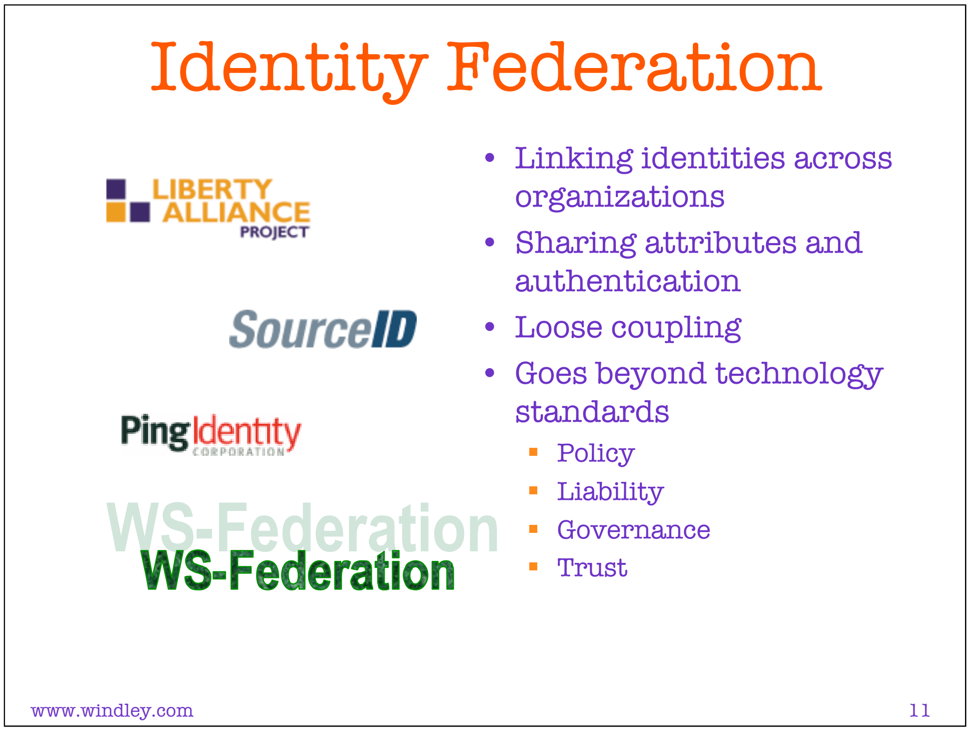
How to manage:

- Thousands of resources
- Thousands of subjects
- Hundreds of systems

Fine-grained access control



Security, Trust, & Privacy



LIBERTY ALLIANCE PROJECT
SourceID
PingIdentity CORPORATION
WS-Federation
WS-Federation

Identity Federation

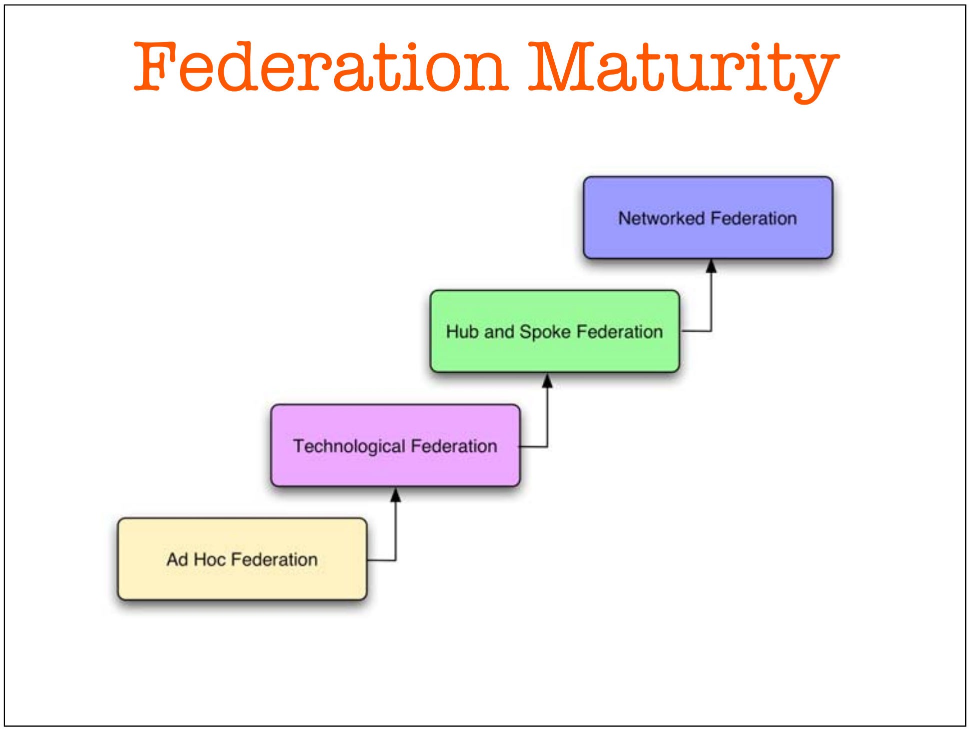
- Linking identities across organizations
- Sharing attributes and authentication
- Loose coupling
- Goes beyond technology standards
  - Policy
  - Liability
  - Governance
  - Trust

www.windley.com 11

Single sign-on between organizations

Goes beyond technology standards

- Policy
- Politics
- Governance
- Legal issues



Federation Maturity

Networked Federation

Hub and Spoke Federation

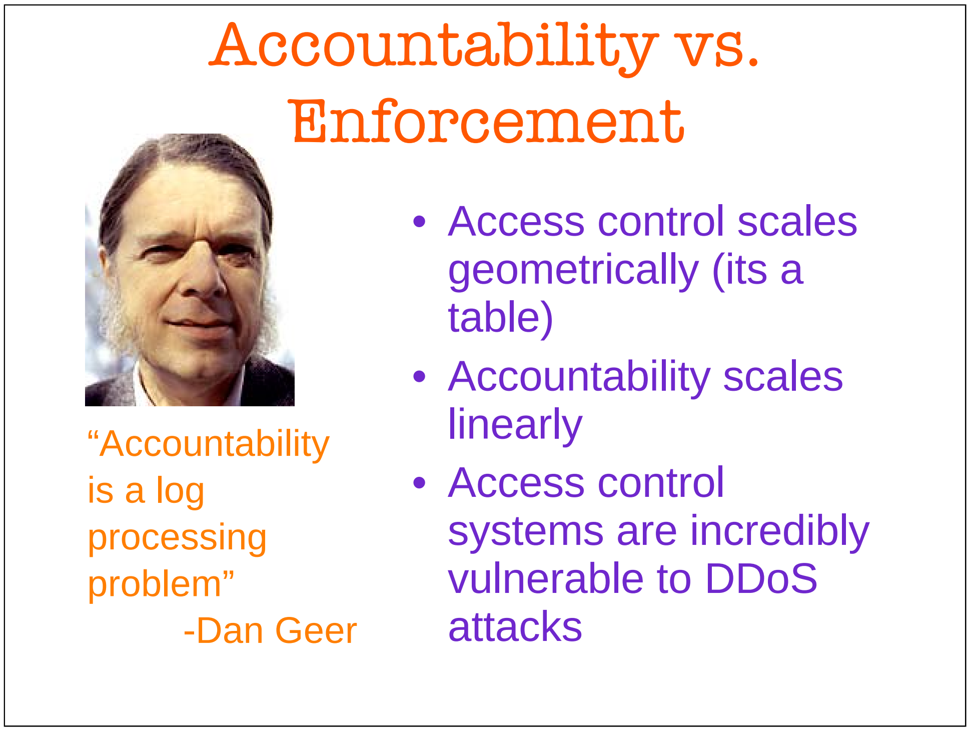
Technological Federation

Ad Hoc Federation

Story of iMall and Verio: ad hoc

Hub and spoke federation driven by large central players in a market

Story of Bank of America, BankAmericard, Visa

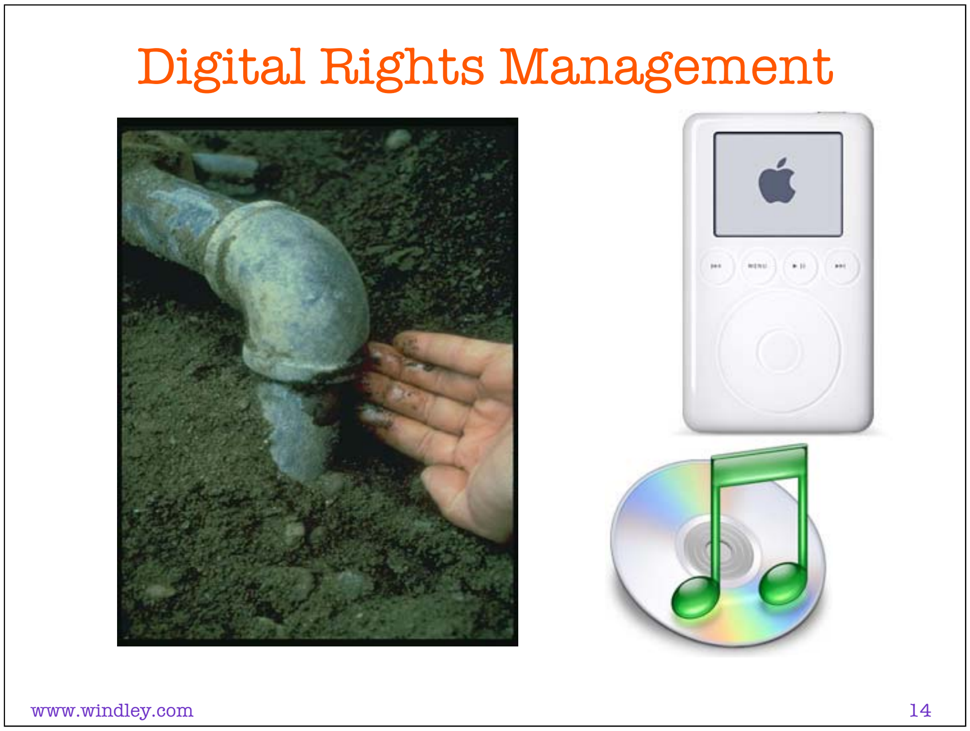


Accountability vs. Enforcement

"Accountability is a log processing problem"
-Dan Geer

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

Controlling access to everything is very hard. Maybe impossible.



Digital Rights Management

www.windley.com

14

Digital leakage

DRM is about controlling access beyond the corporate border.

Controlling data or controlling customers?

Restricting rights costs money.

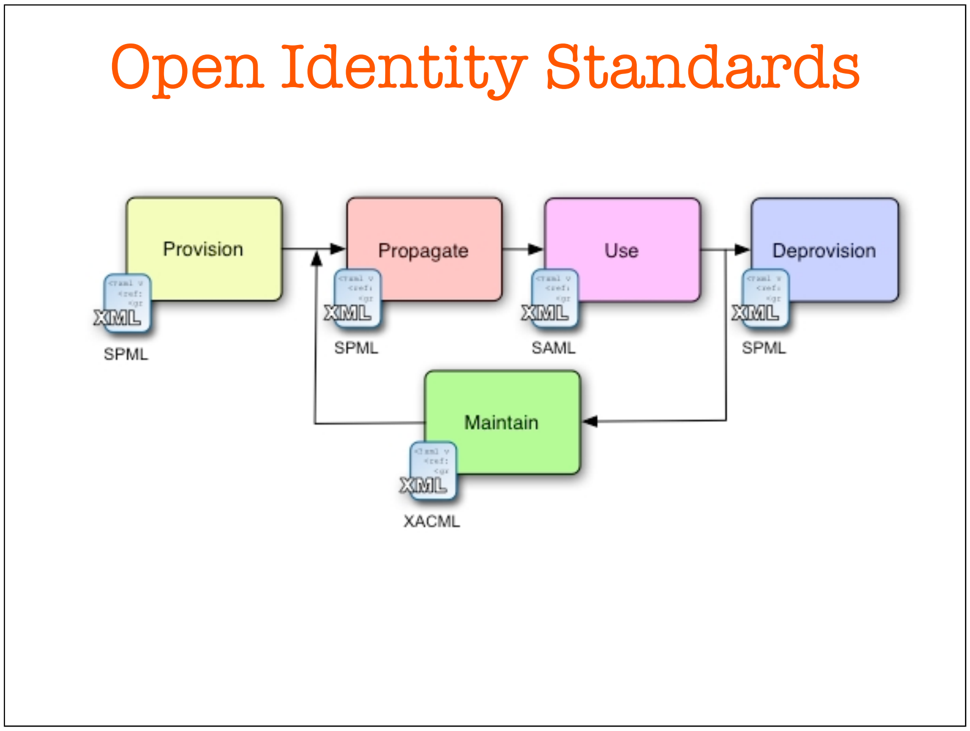
Apple itunes as a cautionary tale

•Balance rights with price

•Heavy administrative burden

•Upset customers

Trusted computing



Open Identity Standards

Provides scaffolding for building identity systems

Starts simple and builds in complexity

•Integrity & Non-repudiation: *XML Signature*

•Confidentiality: *XML Encryption*

•Authentication and authorization: *SAML*

•Identity provisioning: *SPML*

•Managing access control policies: *XACML*

SAML

Linking ticket purchases to car rental

Assertions about authentication, attributes

The language of the PEP and PDP

This is about FEDERATION!!

Issuer ID and issuance timestamp

Assertion ID

Subject

Name and security domain

Subject's authentication data (optional)

Advice (optional additional information provided by the issuing authority)

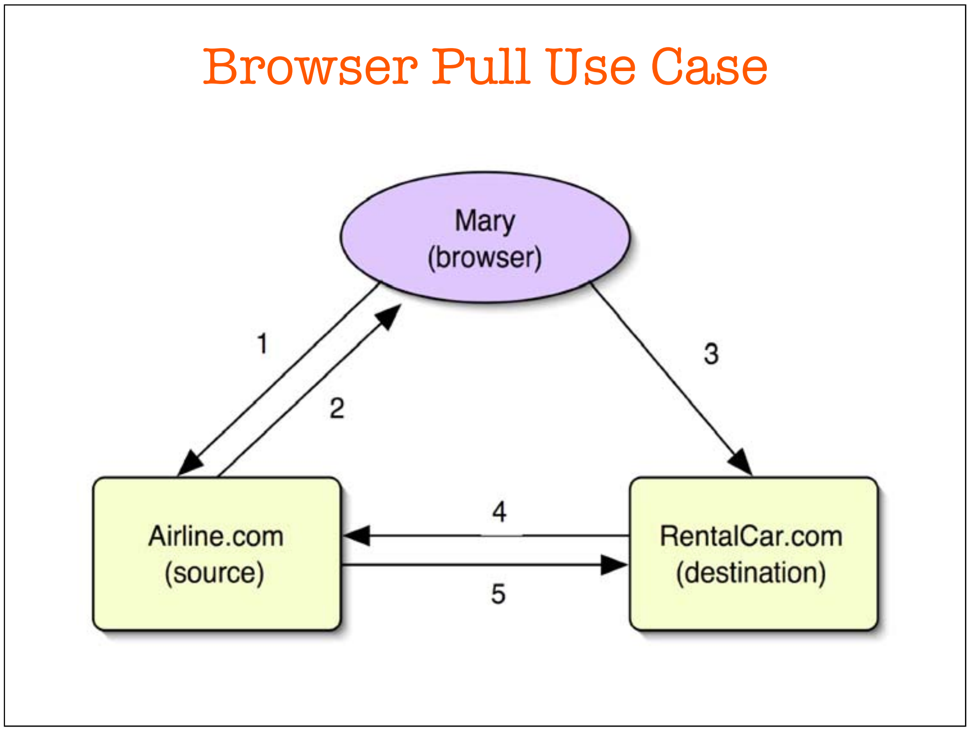
Conditions under which the assertion is valid

Assertion validity period (e.g. NotBefore and NotOnOrAfter)

Audience restrictions

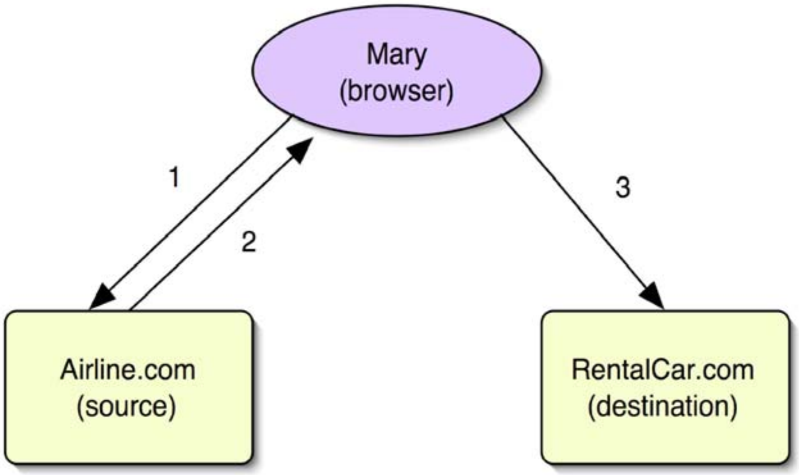
Target restrictions (intended URLs for the assertion)

Application specific conditions

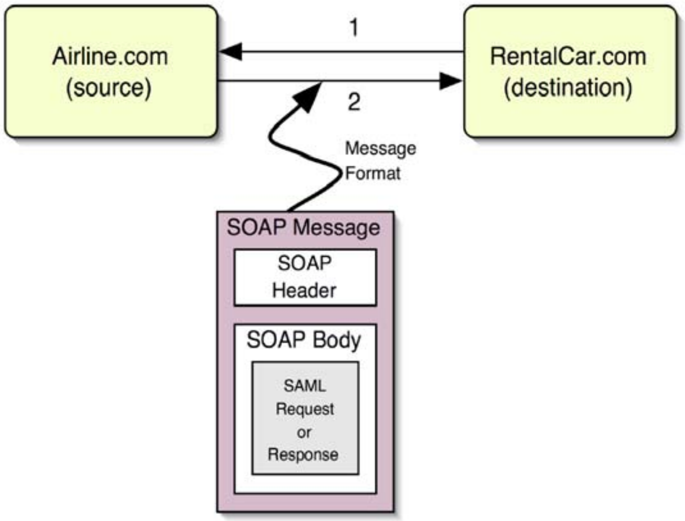


Browser Pull Use Case

Browser Push Use Case



Direct Request Use Case



Airline.com (source)

1

2

RentalCar.com (destination)

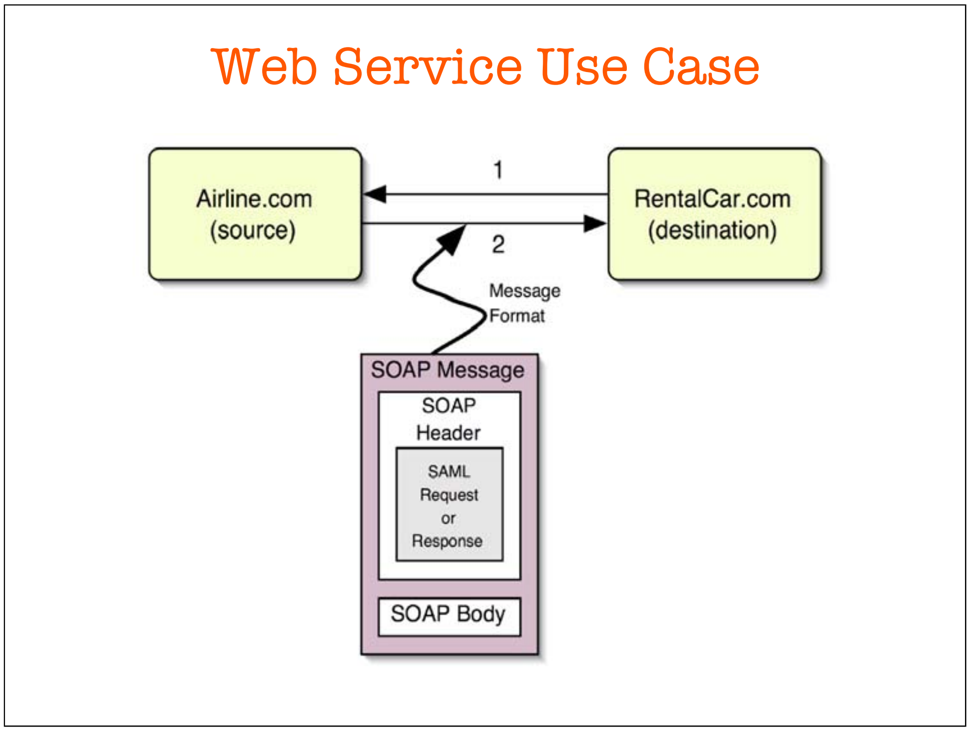
Message Format

SOAP Message

SOAP Header

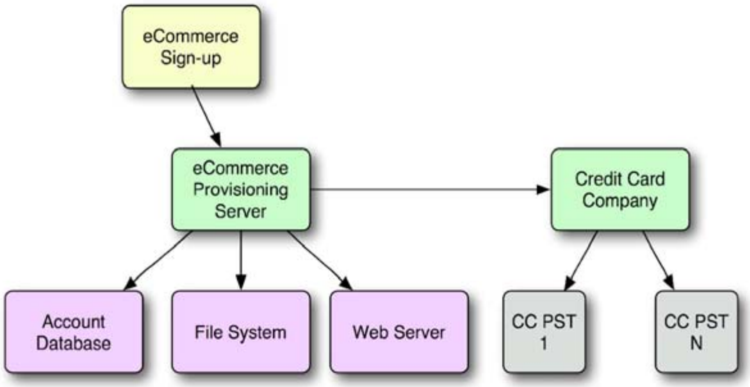
SOAP Body

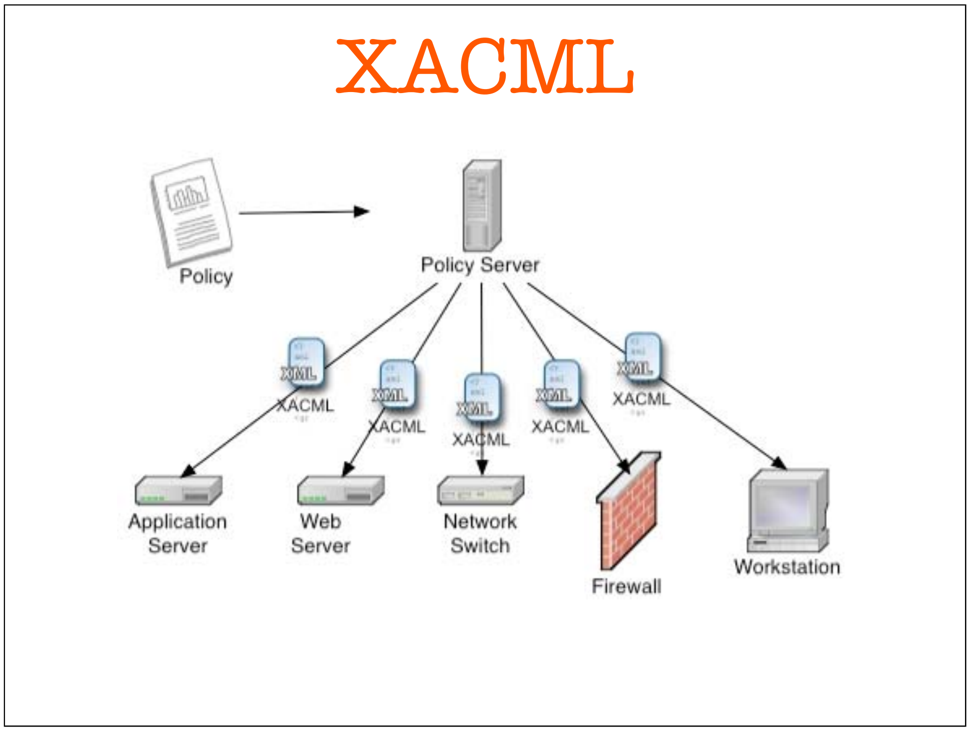
SAML Request or Response



Web Service Use Case

SPML Example





XACML

Policies, and getting them to the right place at the right time.

eXtensible Access Control Mark-up Language

XML standards for storing, sharing, representing, and processing access control policies

Language of the Policy Decision Point (PDP)

SAML is about credentials

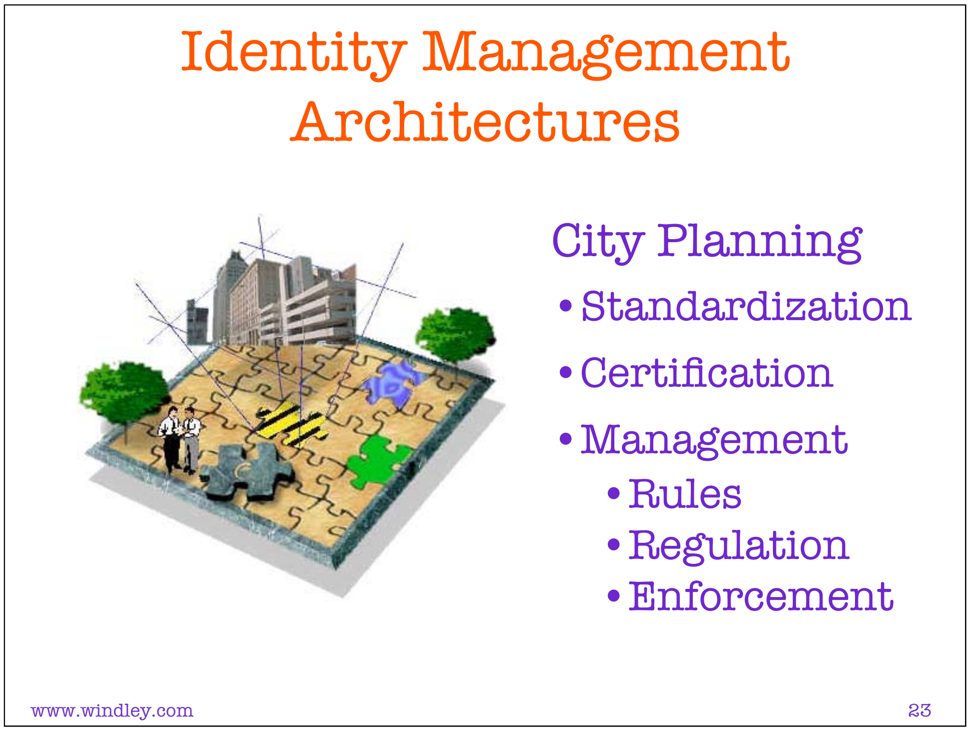
XACML is about processing credentials

XACML is more than a data standard

XACML is a programming language of sorts

Rules can be based on

- Subject attributes
- Action to be taken
- Time of day
- Authentication mechanism
- Transport protocol
- Connectors

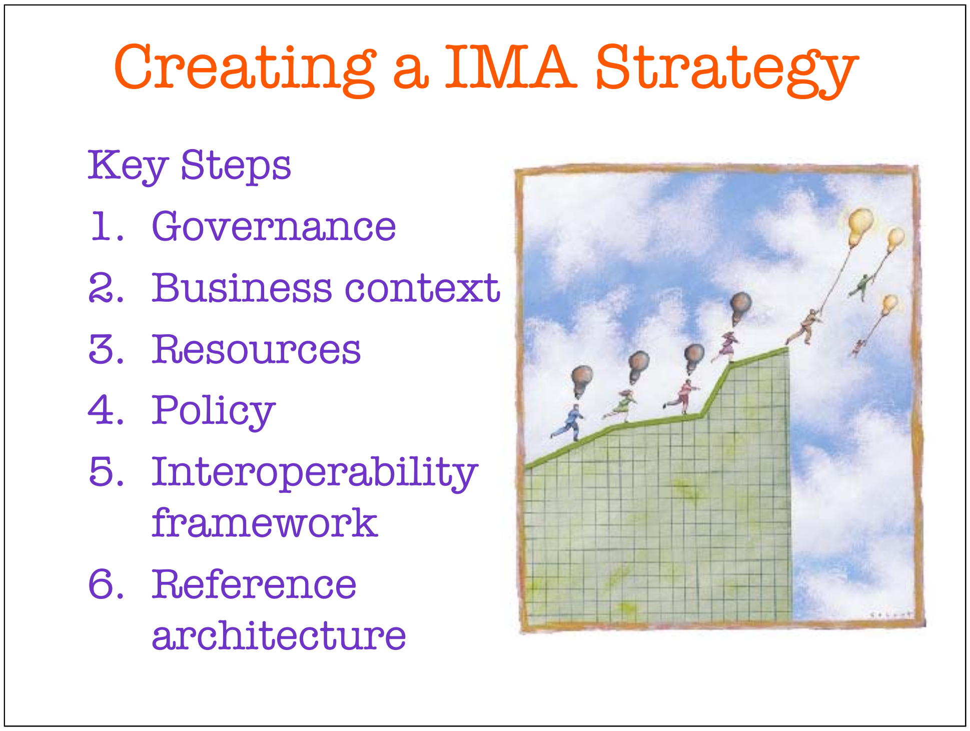


Identity Management Architectures

City Planning

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

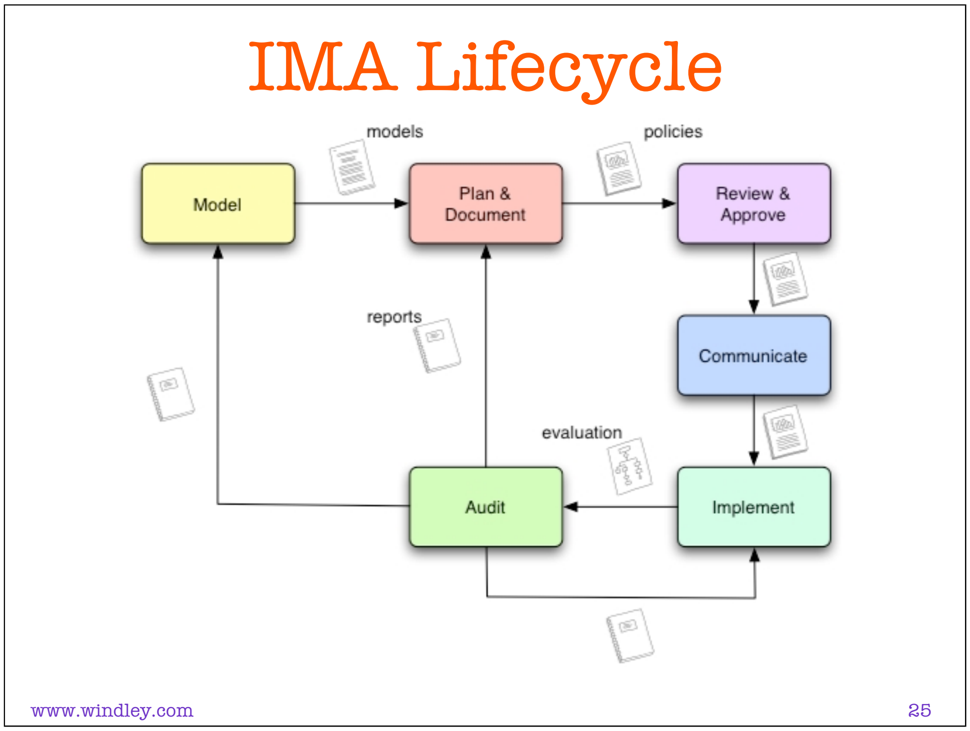
IMAs are like city planning. They provide context for other system activities and ensure interoperability.



Creating a IMA Strategy

Key Steps

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



IMA Lifecycle

models

policies

Model

Plan & Document

Review & Approve

Communicate

reports

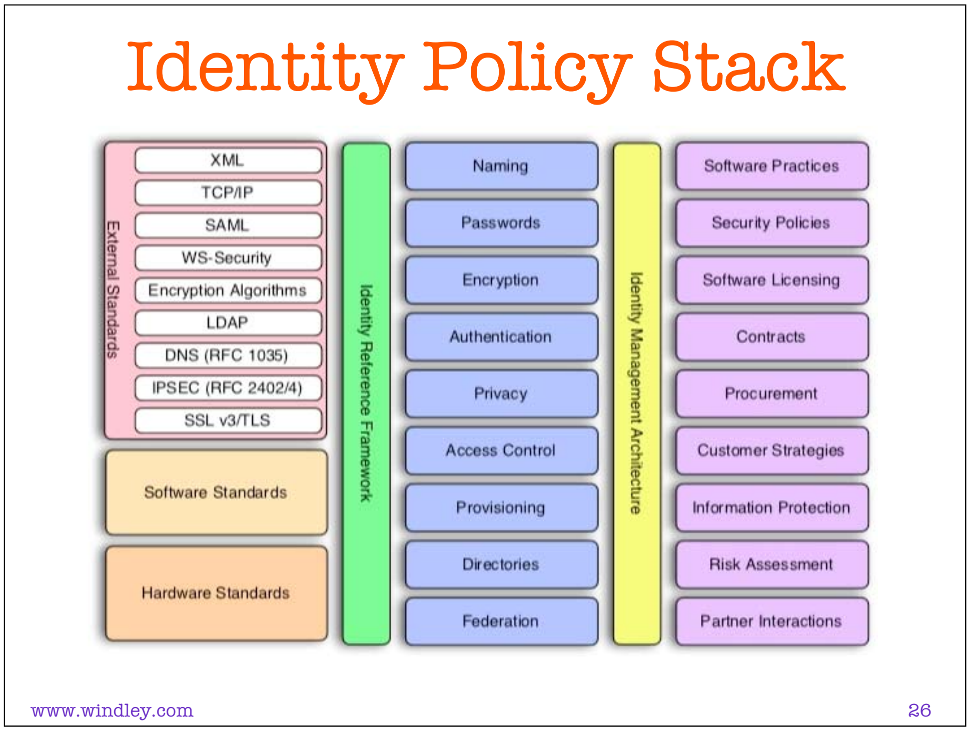
evaluation

Audit

Implement

www.windley.com 25

Governance formalizes this lifecycle



Identity Policy Stack

External Standards

- XML
- TCP/IP
- SAML
- WS-Security
- Encryption Algorithms
- LDAP
- DNS (RFC 1035)
- IPSEC (RFC 2402/4)
- SSL v3/TLS

Software Standards

Hardware Standards

Identity Reference Framework

- Naming
- Passwords
- Encryption
- Authentication
- Privacy
- Access Control
- Provisioning
- Directories
- Federation

Identity Management Architecture

- Software Practices
- Security Policies
- Software Licensing
- Contracts
- Procurement
- Customer Strategies
- Information Protection
- Risk Assessment
- Partner Interactions

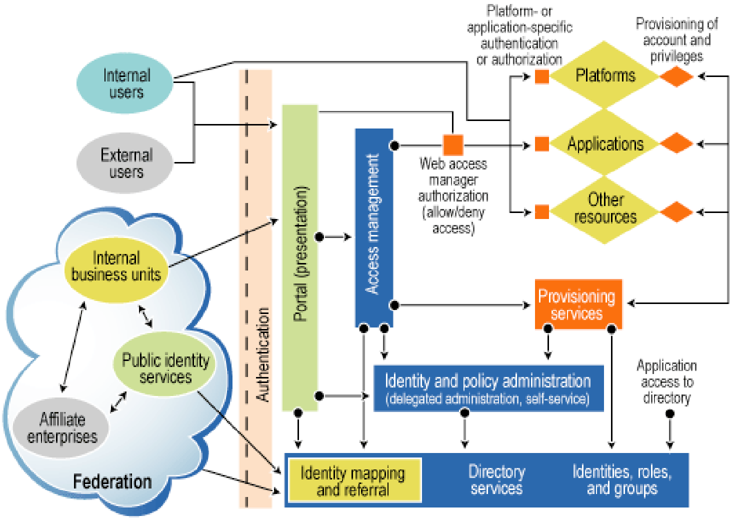
Many geeks don't like policies. We have an anarchist bent. Good policies create freedom.

The problem with most policies is they're ad hoc and reactionary

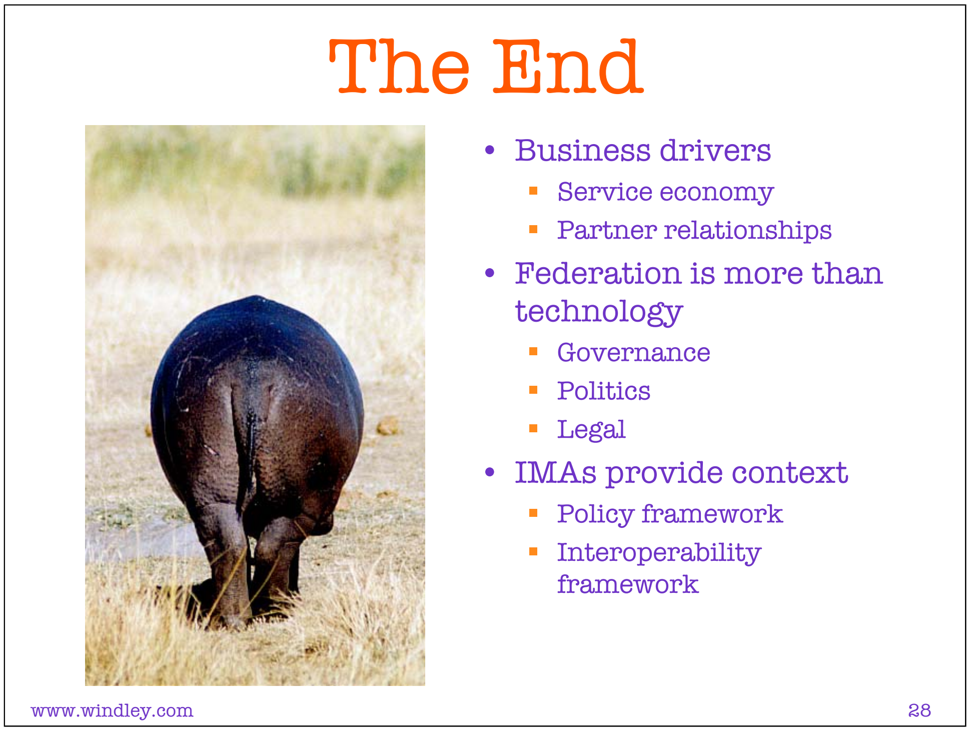
Policies provide a framework for building interoperability

Talk about stack.

IDMa Reference Architecture


Platform- or application-specific authentication or authorization
Provisioning of account and privileges
Internal users
External users
Platforms
Applications
Other resources
Web access manager authorization (allow/deny access)
Access management
Portal (presentation)
Authentication
Internal business units
Public identity services
Affiliate enterprises
Federation
Provisioning services
Application access to directory
Identity and policy administration (delegated administration, self-service)
Identity mapping and referral
Directory services
Identities, roles, and groups

Courtesy of The Burton Group



The End

- Business drivers
  - Service economy
  - Partner relationships
- Federation is more than technology
  - Governance
  - Politics
  - Legal
- IMAs provide context
  - Policy framework
  - Interoperability framework

www.windley.com 28

My book is about building IMAs

Contact Information

Contact me

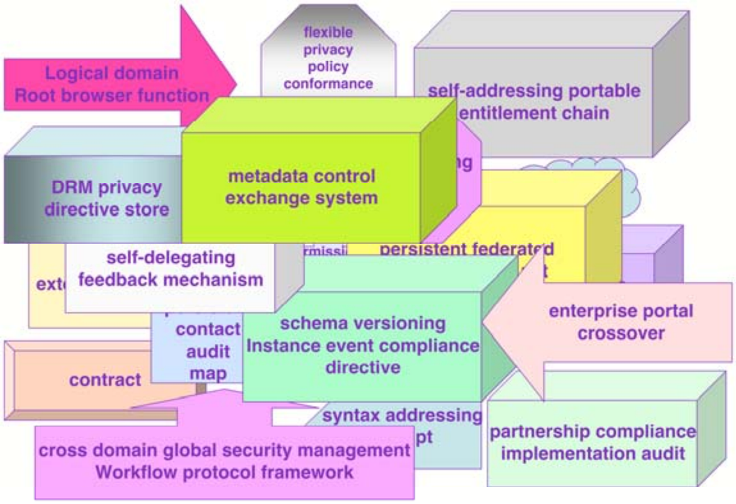
- phil@windley.com
- www.windley.com
- www.eclab.byu.edu

Buy the book…

Get the paper…

Questions?

Identity Infrastructure (as built)



Architecture courtesy of Doc Searls