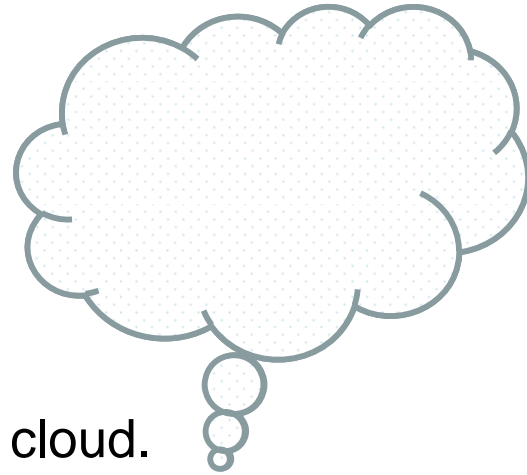




# Identity in the Fog

Open Group SPC, London April '09

# Lost in the Clouds



One thing is true about a cloud.

There is less to it than meets the eye.

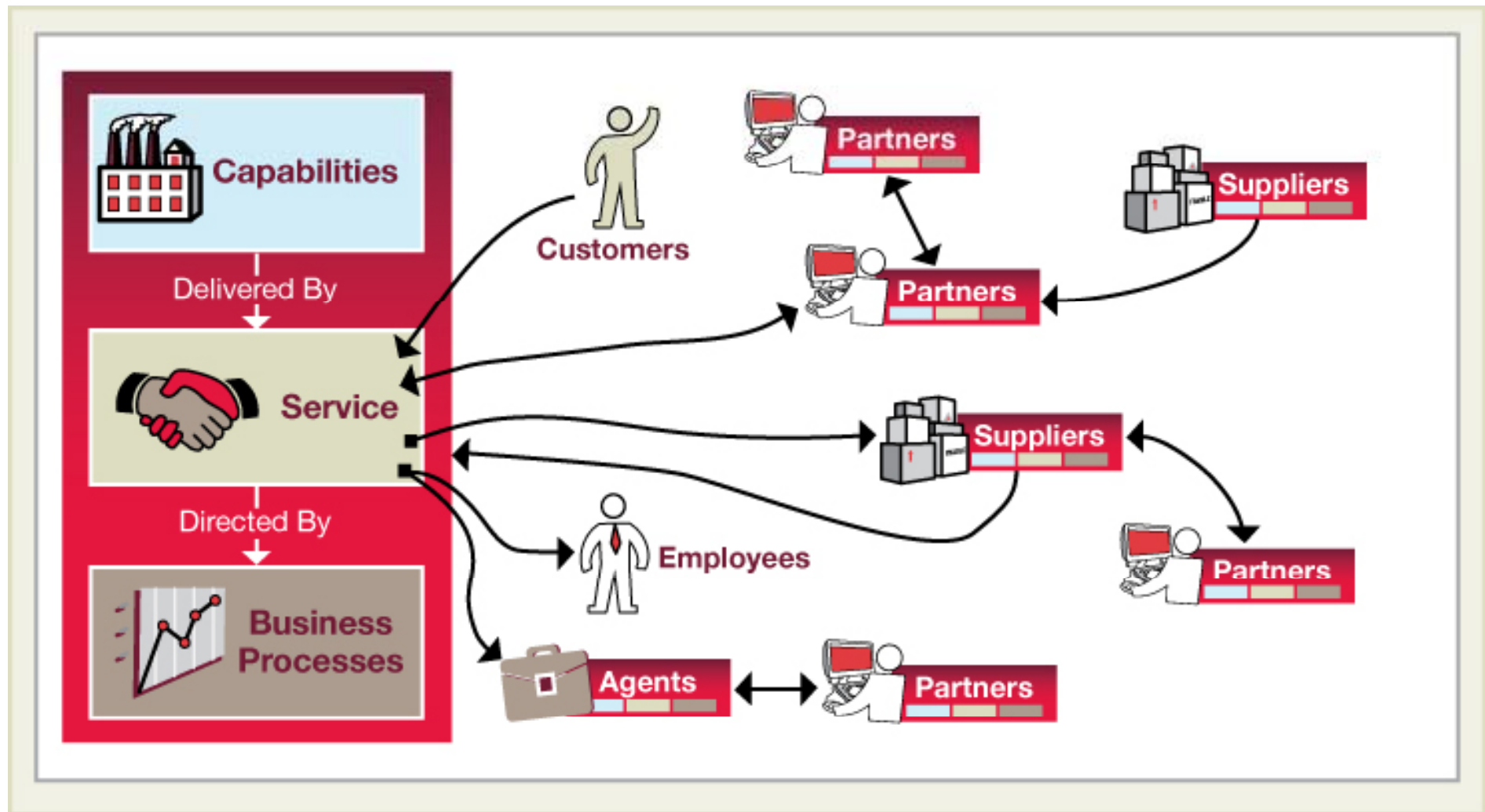
Unless you're in it  
– and then it's fog



# How we see it

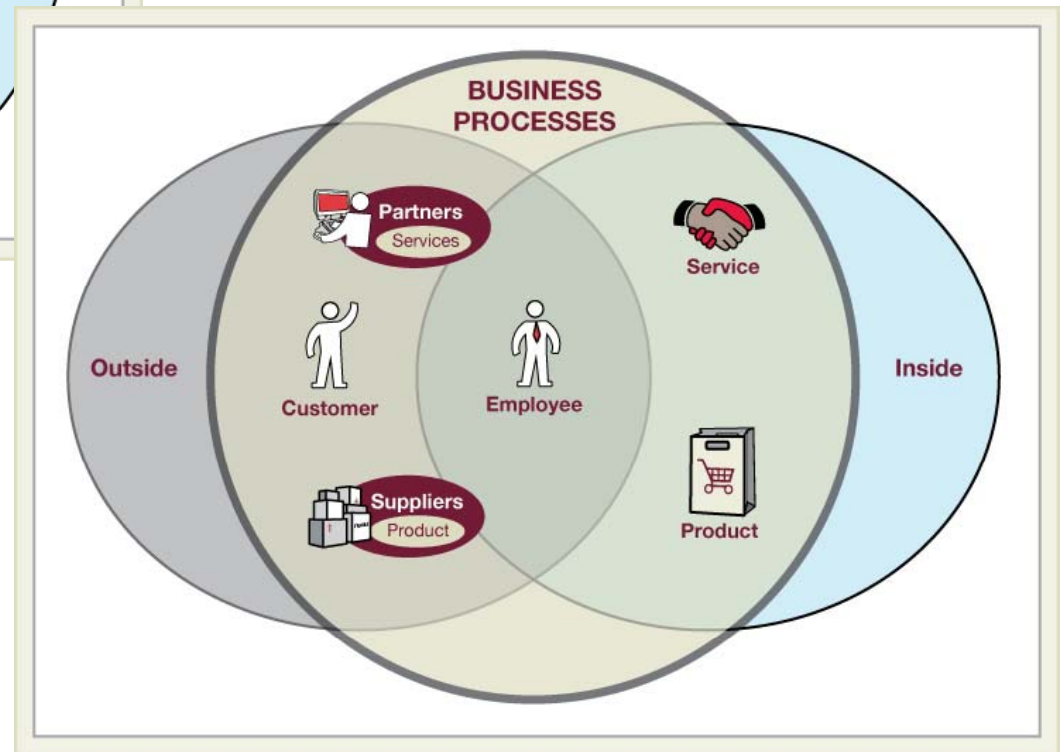
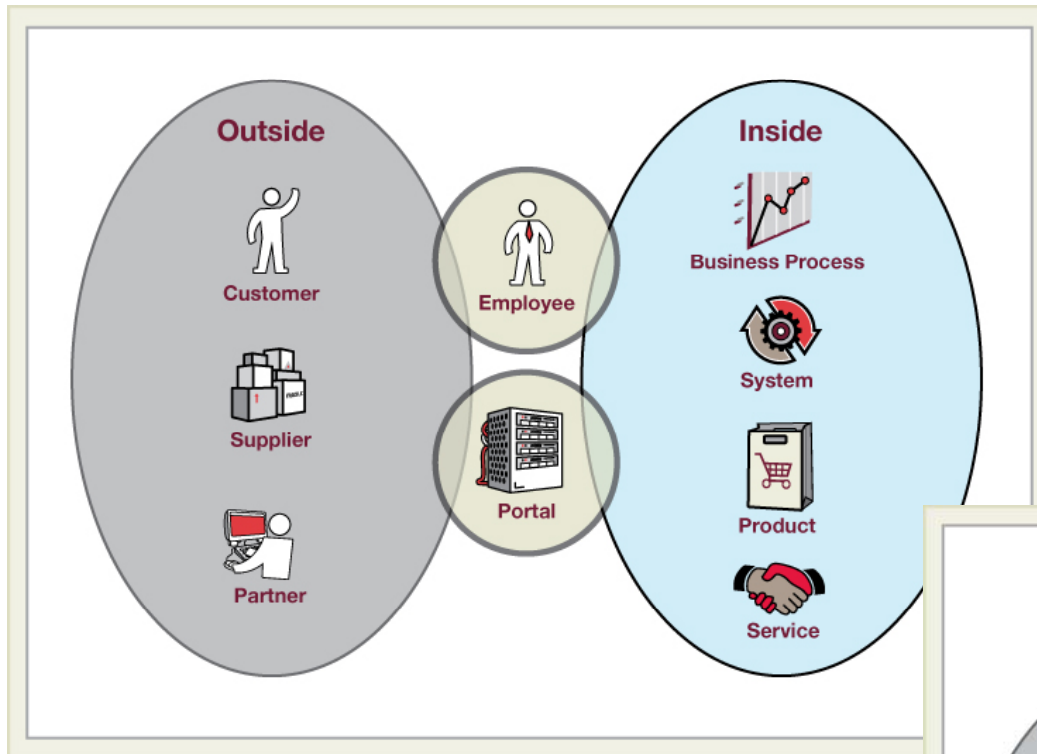
- Cloud is:
  - Extended Enterprise
  - Web 2.0/User-centricity
  - Internet based IT services (Cloud Computing)
- Cloud is:
  - changing how business is conducted via technology
  - requires change in how technology supports business.
- Identity is a fundamental enabler (but also potential threat)
- Getting this right in the Cloud environment matters
  - for security and privacy
  - for usability and agility
- Established and emerging standards
  - How they work
  - Business meaning

# Extended Enterprise



A value network

# The Outside is Inside



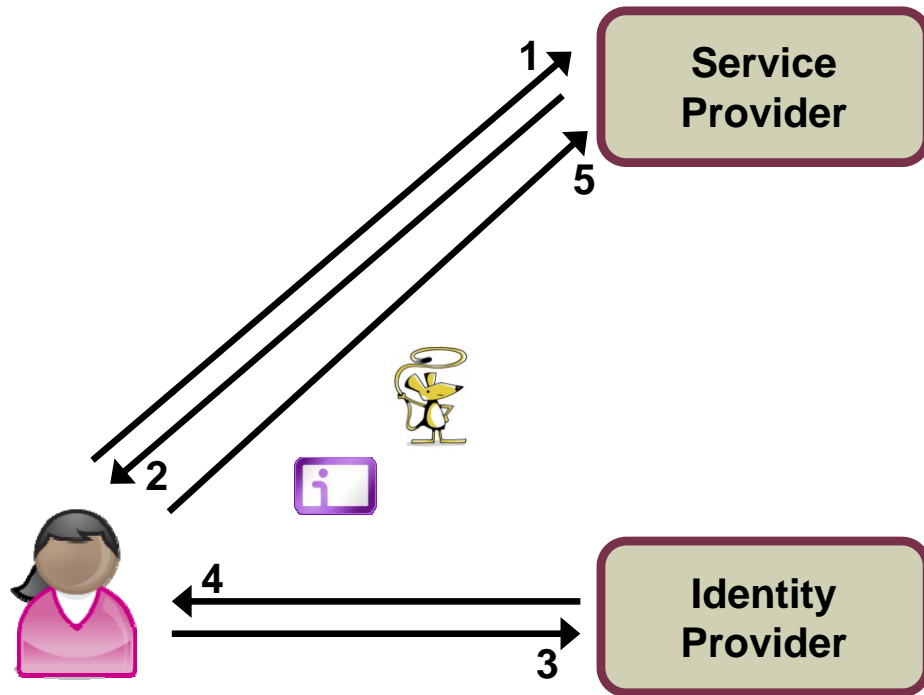
# Effect of Extended Enterprise on IAM

- most obvious consequence is the need for federation
  - cannot maintain user repositories for all individuals (employees of partner enterprises, customers) that may make legitimate use of an enterprise's services.
  - why would they want to manage all these individuals?
  - can delegate or outsource these activities to their partners just as with other services they provide
- SAML, WS-Federation

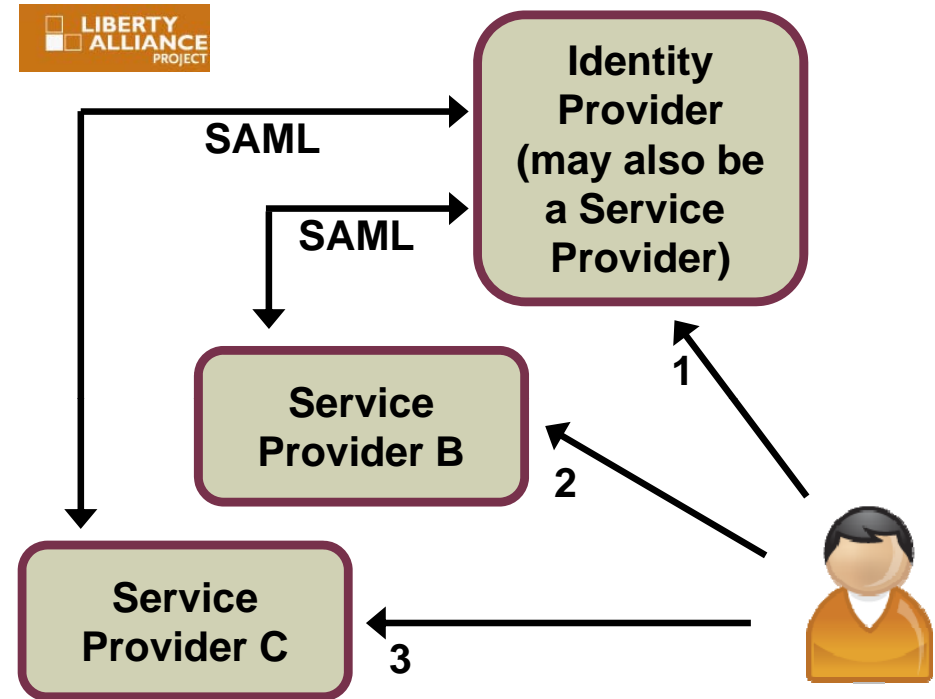
## Web 2.0

- not so much concerned with specific technologies as with the use paradigm
- increasingly pervasive presence of the internet
  - eCommerce, eGovernment
  - social networking, user generated content etc
  - **Collaboration!** (->COA)
  - ubiquitous connectivity
  - personalization and profiles
- Leads to User-Centric Identity
  - Dick Hardt <http://identity20.com/media/OSCON2005/>

# IdP vs Federation



- 1 Request service.
- 2 Provide requirements.
- 3 Select suited Identity Provider.
- 4 Credentials provided.
- 5 Provide card to Service Provider.



- 1 Login (name/pw) at Identity Provider.
- 2 Use Service Provider B without login.
- 3 Use Service Provider C without login.

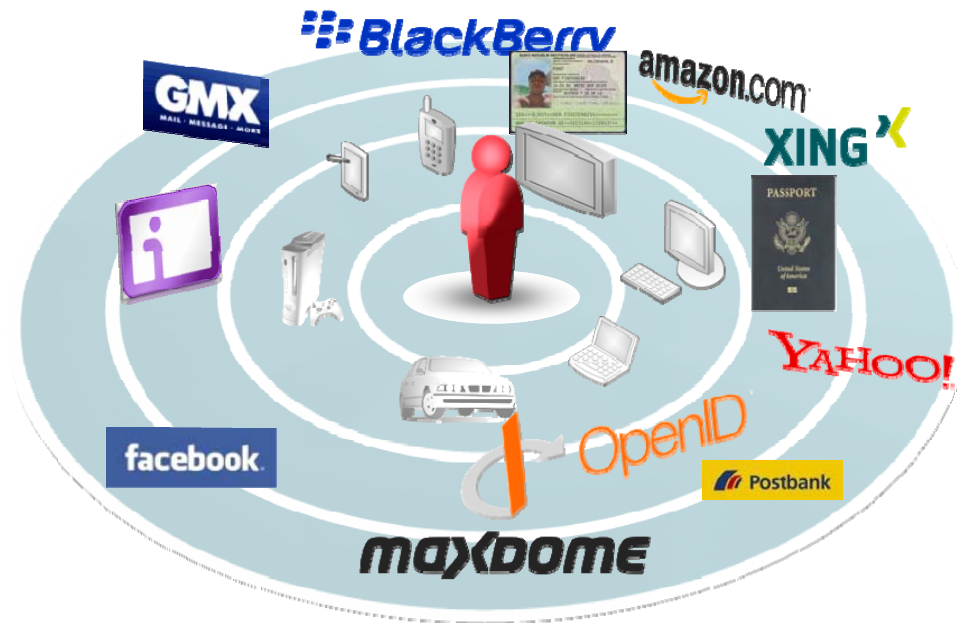
Circle of Trust between Service Providers and Identity Provider on contractual basis.



# IdP, Federation etc.– business meaning

- Federation
  - Really for B2B
  - Known (trusted) *business* partners
  - No use for individuals (consumers/prosumers)
- IdP
  - Oriented to individuals but available to enterprises
  - Good for profiling
  - Not the place for business differentiators
  - Implicit trust - risk
- etc.
  - Tend to consumer solutions

# Ubiquitous connectivity



- Purely mobile identity solution (i.e. a solution for mobile devices) not enough.
- Access and authentication services must not limit access
- have to provide a user experience which is similar and easy on every device.
- A *mobilized* identity is essential
  - accessible without limitations
  - capable of being combined with device specific security behavior.

# Standards in place, summary

	Federation	OpenID	Infocard
Owner	Liberty Alliance OASIS	Open Source	Microsoft / Novell Via Higgins: Open Source
Main Supporter	IT Vendors and Telco provider	Recently: Yahoo, Google, France Telecom	Microsoft, Novell, partly Open Source driven by IBM
Maturity	Stable, proven	Stable	Stable, client dependent
User Experience	Transparent	Technical interaction necessary (URL), medium	Graphical Interaction, easy
Spreading	Wide, de facto standard	Low to medium	Low to Medium (Shipped with Windows Vista)
Security	Easy to strong	Medium	Medium to strong

# What is Cloud Computing ?



IT Infrastructure



Functional Services



Variable Cost



Elastic Capacity



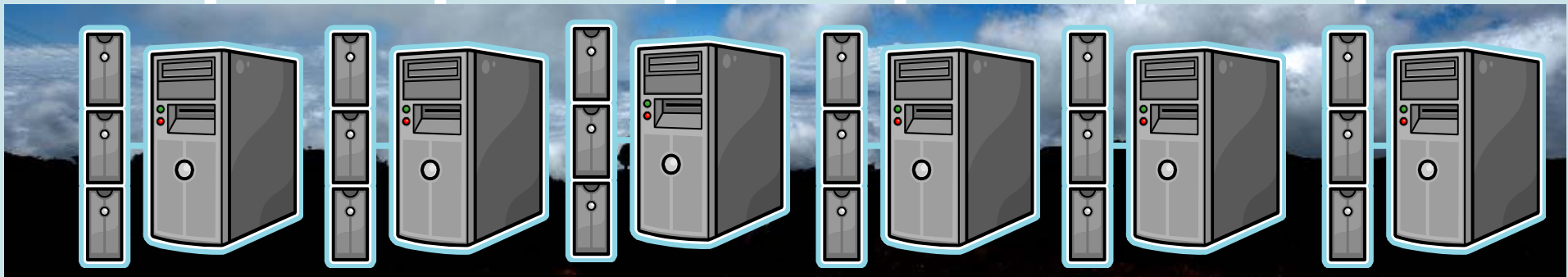
Standards (real or defacto)



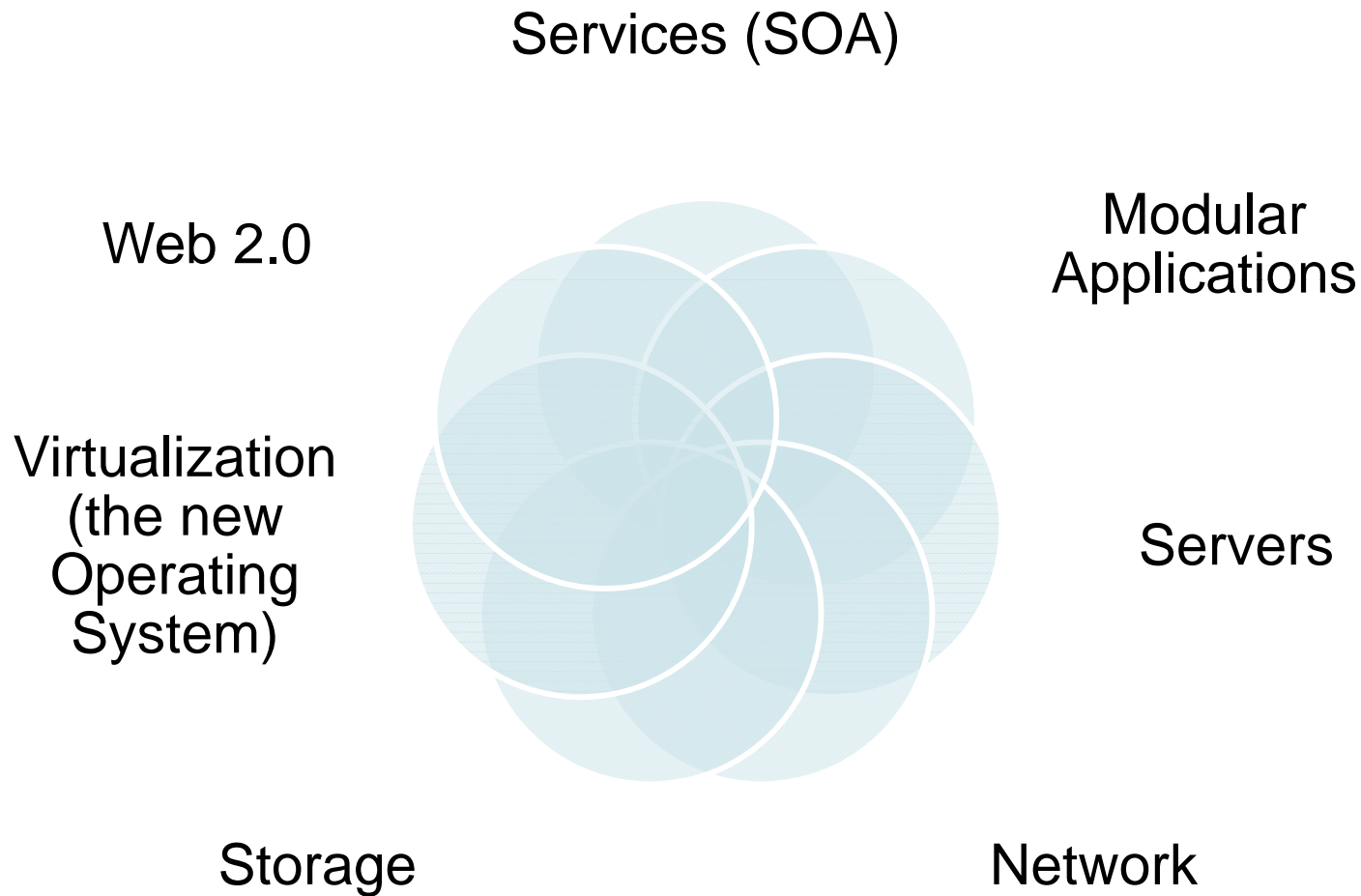
Accelerated Cycles



Business Agility



# Components of the Agile Enterprise



# What will happen ?

Orchestration of  
Business Processes,  
Services, Infrastructure

Services (SOA)

Everything as  
a Service

Web 2.0

Modular Applications

IT Infrastructure  
Virtualization

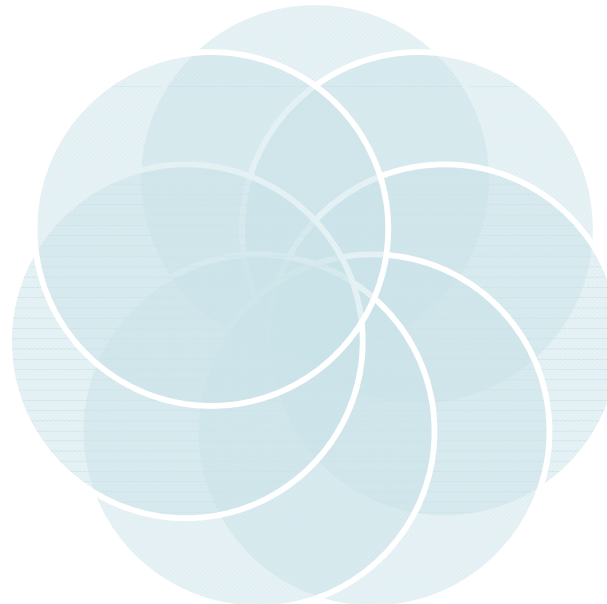
Less Servers

Continued  
Commoditization

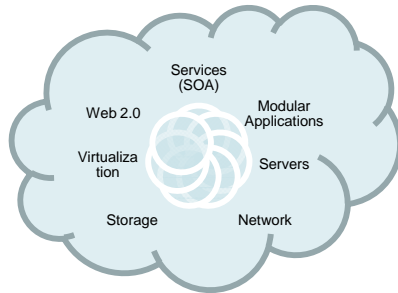
Improved ROI

Consolidated Storage

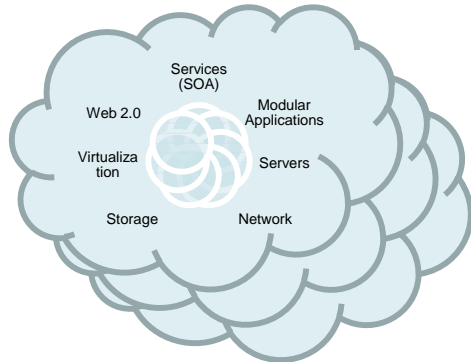
More Network



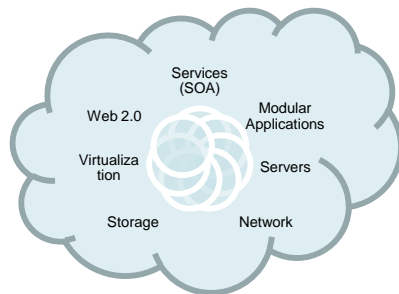
# What do you mean by 'Inside' ?



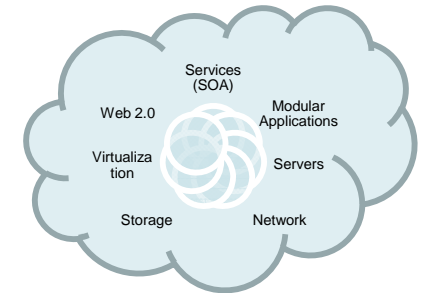
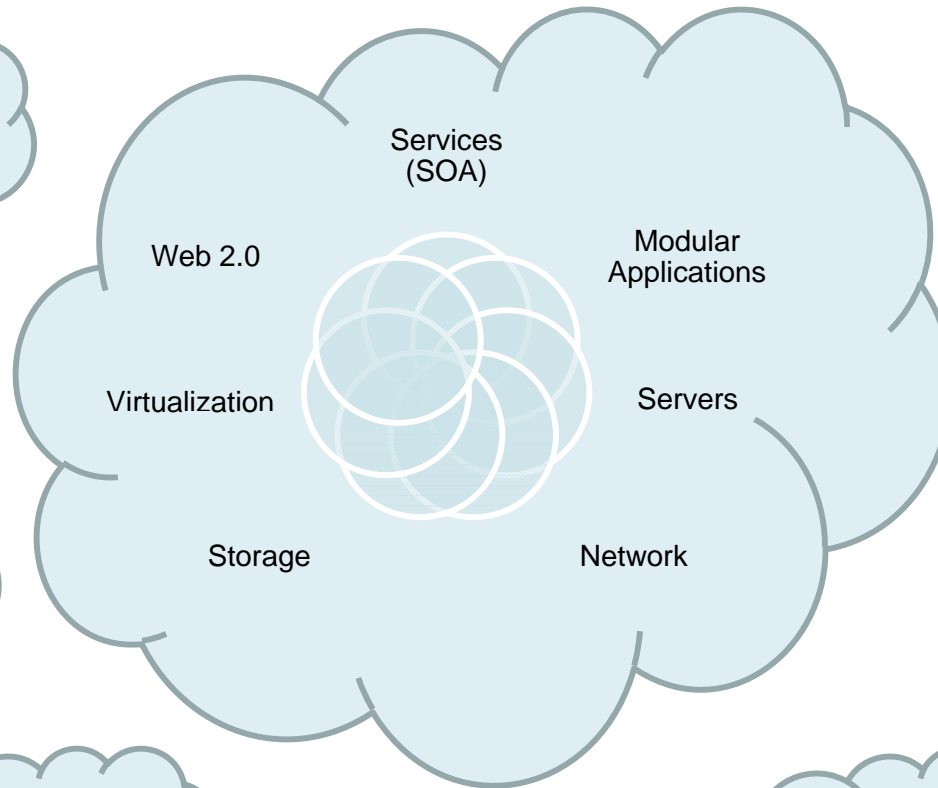
Adaptable Patterns



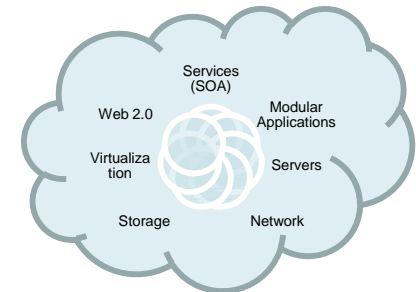
Disaster Recovery /  
Live Load Balancing



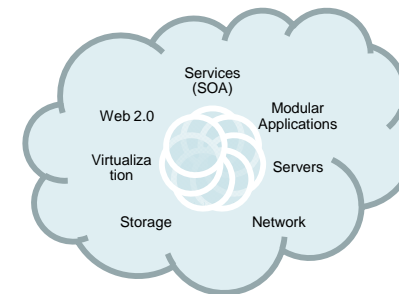
IT Infrastructure Cloud



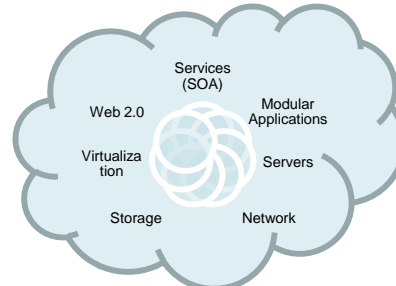
SaaS Solutions



SaaS Components



Development /  
Test Clouds



Solution Specific  
Infrastructure Clouds

# What to monitor ? What may happen ?



open cloud manifesto 

the following companies and groups support the open cloud manifesto






over 175 supporters and growing

- Cisco
- IBM
- National Bank of Greece
- Novell
- Red Hat
- Sun (Oracle)
- VMWare



## Commercial Cloud Formation

Logos include: CYCLECOMPUTING, Appistry, Amazon web services (Amazon Elastic Compute Cloud (Amazon EC2) - Beta), GOGRID beta, Path, VM Ops, 3tera, b-hive, MOSSO the hosting cloud, Citrix, Engine Yard, vmware, Microsoft, Q-layer, Joyent, VERIO, and hp.

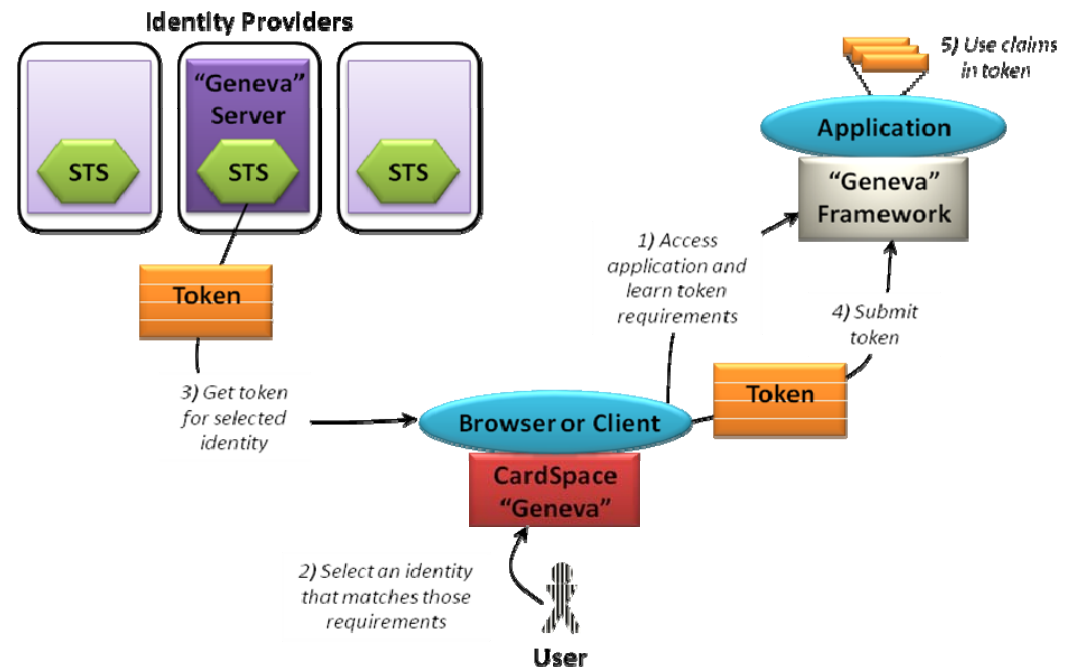
-  Amazon (Machine Images)
-  Google (Python 2.5)
-  Facebook (anatomy/API)
-  Microsoft (Azure & .Net)
-  Salesforce.com (Visual Force & Adobe Flex)



# Related Developments

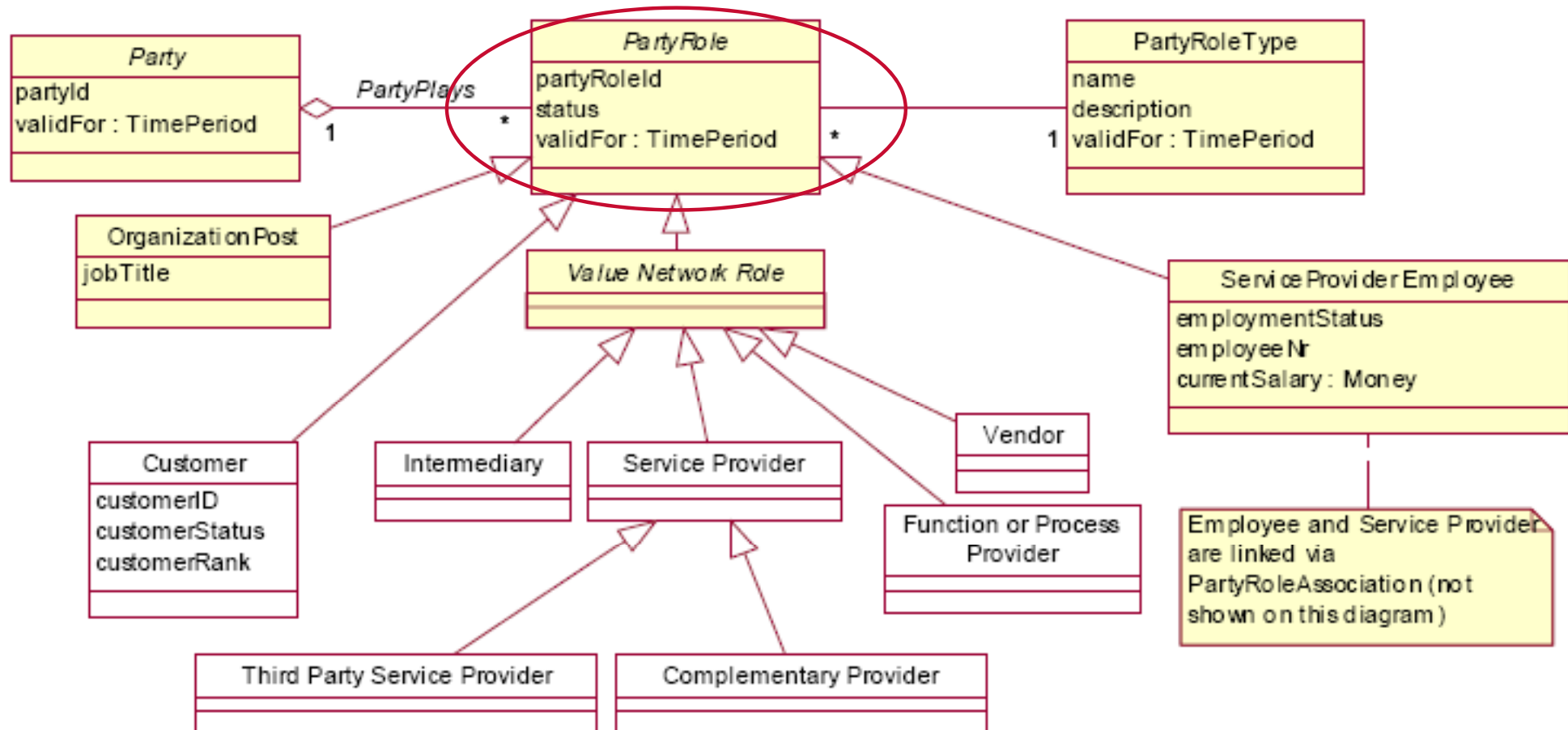
- Claims-based Access Control
  - RBAC overloaded and not dynamic
  - CBAC dynamic and context based
  - InfoCards contain claims (verified & unverified)

MS-Geneva



- Trust frameworks and interoperability (WS-Trust, Liberty Alliance IAF)

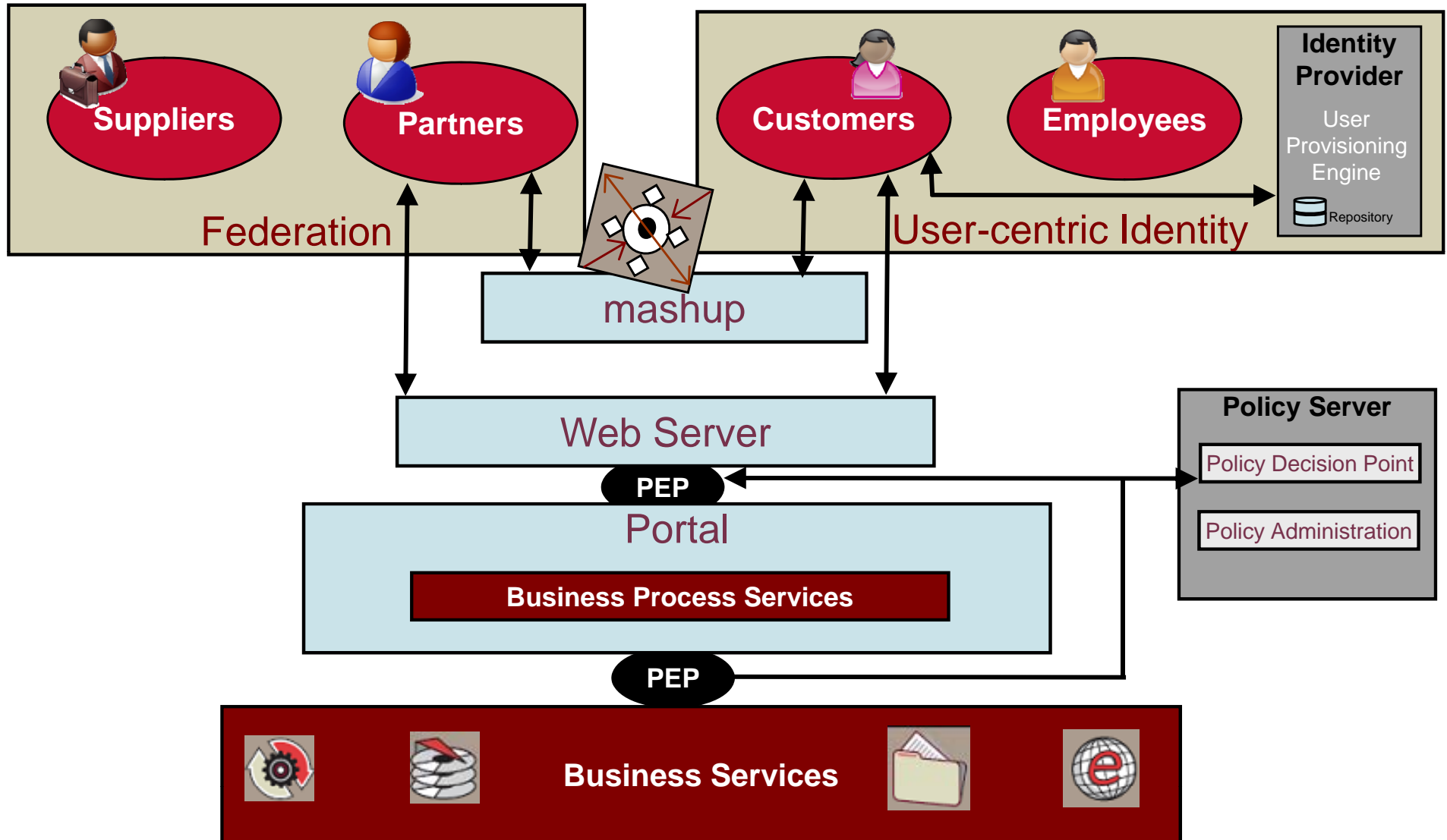
# Identity data is Business Data



# Conclusions

- Increasingly difficult to maintain user identities and assign rights to identities within a single organization
  - little business logic in doing so.
- Identity as a concept far removed from the userid/password simplification.
- How we use identity and ensure privacy and regulatory compliance are business issues.
  - How we address this with our IT solutions can make or break our business objectives
- Move away from isolating “security” concerns into a “non-functional”, infrastructure domain.
- Decouple identity solutions from other applications and locate them in their own business domain.
  - Even if we didn’t want to, the Cloud will force us.

# Elements of a Solution



# Last word - Trust

- trust relationships between providers of identities and services will become even more significant.
- explicit trust agreements between all parties potentially collaboration in the cloud are unthinkable.
- Need:
  - standards supporting dynamic trust relationships
  - network of recognized, trusted providers of identities.
- Government is an example of such a provider active today.
  - Who has an explicit trust relationship with the Government?
  - We simply assume that, if the government says it's true and the credential (e.g. password) looks authentic, then it must be OK.
  - not unreasonable to see how this can be extended but it certainly argues for a limited number of identity providers and a limited set of well accepted standards to underpin that.