LIBERTY ALLIANCE PROJECT

Moving Digital Identity to the Cloud,
a Fundamental Shift in rethinking the enterprise collaborative model.

Fulup Ar Foll
Master Architect
Sun Microsystems
Fulup@sun.com

What is the cloud ?

LIBERTY ALLIANCE PROJECT

From a middle age castle to super-market

Same Goal

Different architecture

What are we looking for ?

- Move from anonymous to identity enabled
  - Most transactions on the Internet today are anonymous
  - Value transactions are identity based
- Enable Identity while protecting privacy
  - Issuer and target ID do not have to know each other
  - Enable the right to forget
  - Provide an identity dashboard for user to keep control of its own digital ID
- Enable audit and policy enforcement.

Old success in digital IDs

- Phone Number, Email,Credit card, ...
  - No need for pre-registration
  - Based on some form of contract
  - Proven to scale toward hundreds of millions of users
  - Does not protect privacy
  - Subject to random attack (phishing, spam, …)
- *Do you call your mobile operation to warn them about your vacation destination ?*
- *Do you have to register for someone to use your email ?*

Inside digital ID

- Authentication (who are you ?)
  - Only a technical MUST HAVE feature
- Attributes (what are you ?)
  - The real value of identity
- Proof of validity (trustful ?)
  - Source of the ID and/or Reputation

- *Isolation of partial user ID in silos enables privacy.*
- *Contracts enable trust.*
- *Best way to protect information leak, is by not creating the information*

LIBERTY ALLIANCE PROJECT

Which Identity for which cloud ?

- Which Cloud ?
  - GRID, Virtualisation
  - SAS, Service provider, Service Consumer
  - Full Internet, or Partner Internet
- Which Identity
  - Exporting internal Identity
  - Consuming external Identity
  - Being an identity proxy/broker
- Access control
  - Based on external data
  - Based on internal data

Cloud Identity Enabled Transaction

Anonymous Discovery of an Acceptable authority

Identity Authentication Assurance Framework

Identity enable Discovery

Access Control

Action toward Arbitrary data

Weaknesses of traditional security

- Rarely stick to reality
  - Password enforcement versus reset through email
  - Roles turnover/distribution versus employees.
  - Centralized fine-grained control
  - Audit, Alarm, Logs, ...
- Too many systems work because people choose to close their eyes
  - Public passwords
  - Shared accounts
  - Signed contract, that everyone knows to be ignored

Keep complexity close to usage

- Relocating complexity to a central point is not free:
  - Distribution by itself adds complexity
  - Significant impact on performances
  - Loss of understanding (especially when handled by different teams)
  - Synchronization dependencies.
- Only useful when:
  - Complexity is reused enough to obtain economies of scale
  - Central authority enforcements are kept at a very high level.

Limits of traditional approach

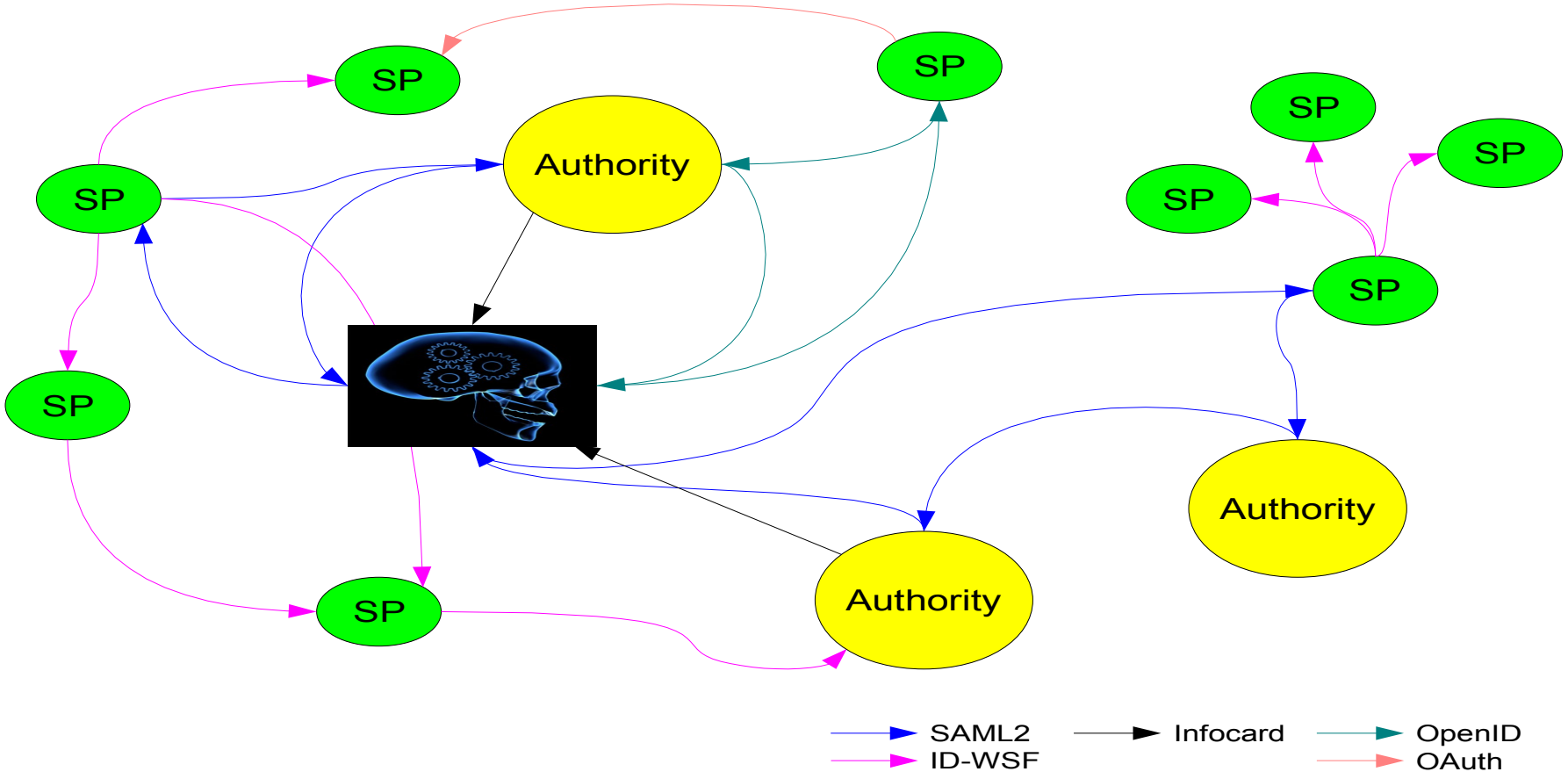
- Centralization
  - Creates a lot of dependencies, and limits functionalities
  - Increase 1st step cost of any new concept/application, eventually prevents innovation.
  - Treats privacy as a 3rd class citizen.
- Back channel pre-provisioning
  - Cannot scale at Internet level like GSM.
  - Incompatible with on the fly decision (click & buy)
  - Identity attributes usage (best case only expensive, worse case provides obsolete values)
- Russian doll layer design (legacy remodeling)
  - Impact both functionalities and performances.

Loosely coupled and Lazy synchronization

- Available: federation & claims *(full spec, FCS products)*
  - Loosely coupled session management
  - Identity attributes discovery and retrieval from authentic sources
  - Privacy as a 1st class citizen
- Partially available *(draft spec, early implementation)*
  - Authentication assurance Framework (Liberty IAF)
  - Identity governance framework (Liberty IGF)
  - Identity roaming (proxy authentication, attributes broker,...)
- Still waiting *(mostly thoughts and ideas)*
  - Initial Authority discovery
  - Transfer of attribute ownership
  - Erase/forget functionality
  - Identity dashboard

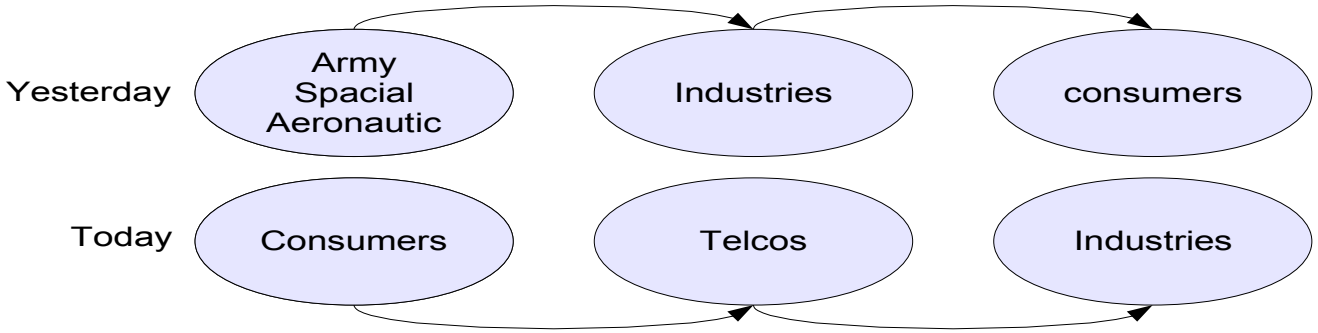
LIBERTY ALLIANCE PROJECT

Fully distributed, partially Heterogeneous



Which ID provider(s) for your cloud

- Change in evolution model



- But a limited number of potential authorities.
  - Bank, Telecoms operators, post office, Government
  - Equipment manufacturer (Microsoft, Apple, Nokia, …)
  - New players (google, yahoo, facebook, ...)

Furthermore user need to know his ID credentials

LIBERTY ALLIANCE PROJECT

Let's imagine the future

- Identity enabled search (seamless SSO for any proposed link)
- Smart discovery of acceptable authorities
- Dashboard for user to keep control of its digital ID usage.
- Distribution of my ID attributes through chosen authoritative sources.
- Identity governance enforced independently of service provider (producer/consumer)

My 0.1€ predictions for next 18/36 months

- **Authentication**
  - SAML2: enterprise, governments, telcos, …
  - Open-ID2: blogs, photos sharing services, …
  - Infocard: password less authentication GUI
- **Attribute exchanges**
  - Authentication attributes will continue to be the most common practice for some time.
  - ID-WSF2 in government or where ever privacy is enforced by regulation.
  - OAuth for “cheap” services, in conjunction with OpenID.
- **Convergence**
  - Protocol will first be bridged (ex: ID-WSF on REST, IDP supporting SAML2 & OpenID, SAML2/SIP, ...)

Fulup Ar Foll
Master Architect
Sun Microsystems
Fulup@sun.com

http://www.projectliberty.org
http://www.opensso.org
http://www.fridu.org/fulup-publications