Open your Identity to the world

Fulup Ar Foll
Master Architect & CTO

Global Software Practice
Sun Microsystems

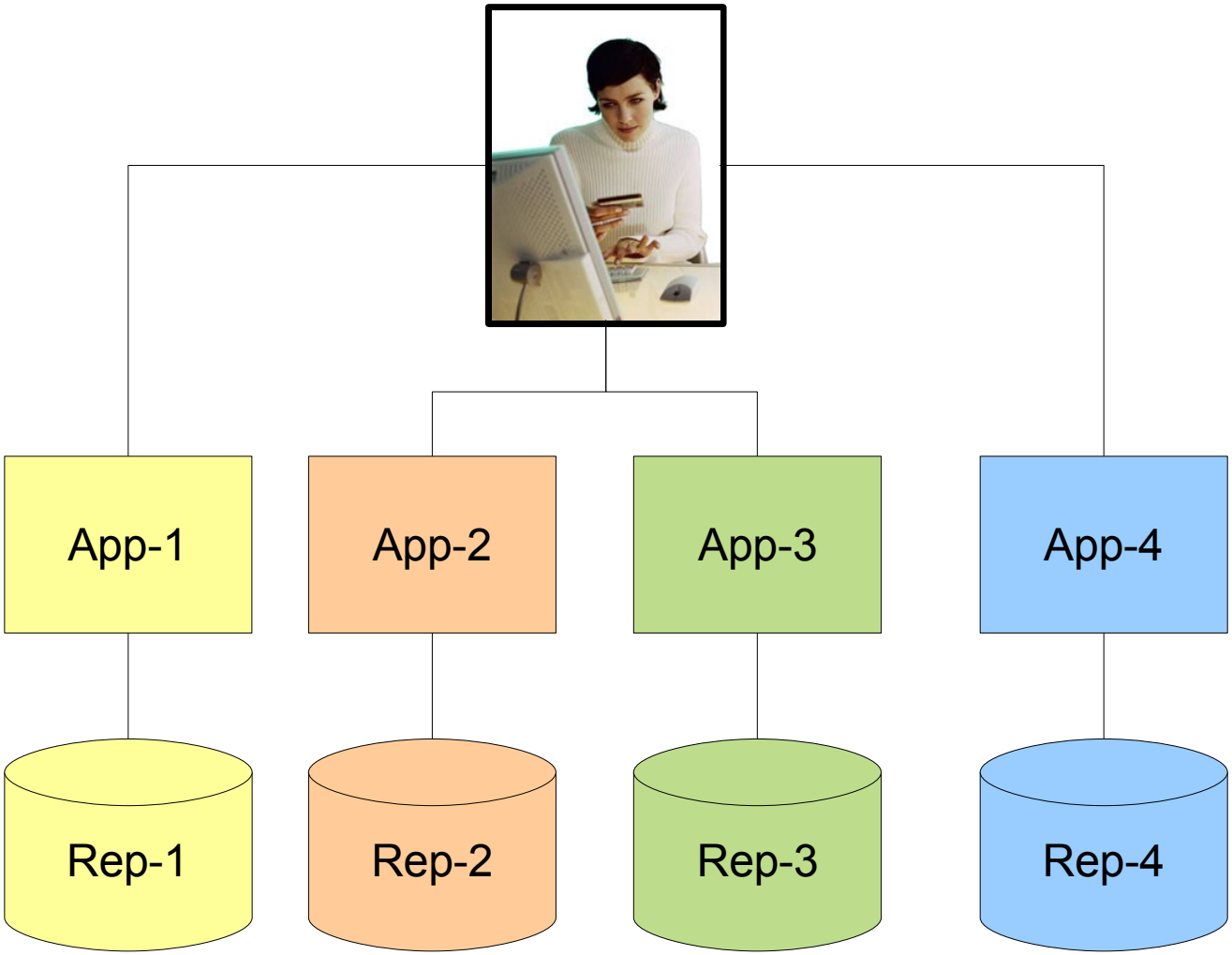
Middle age castle are not working any more.

Old security architectures are bases on multi-layer walls and security zones.

New architecture should be compliant with today business model.

Identity Legacy

(let's built my own flavor)



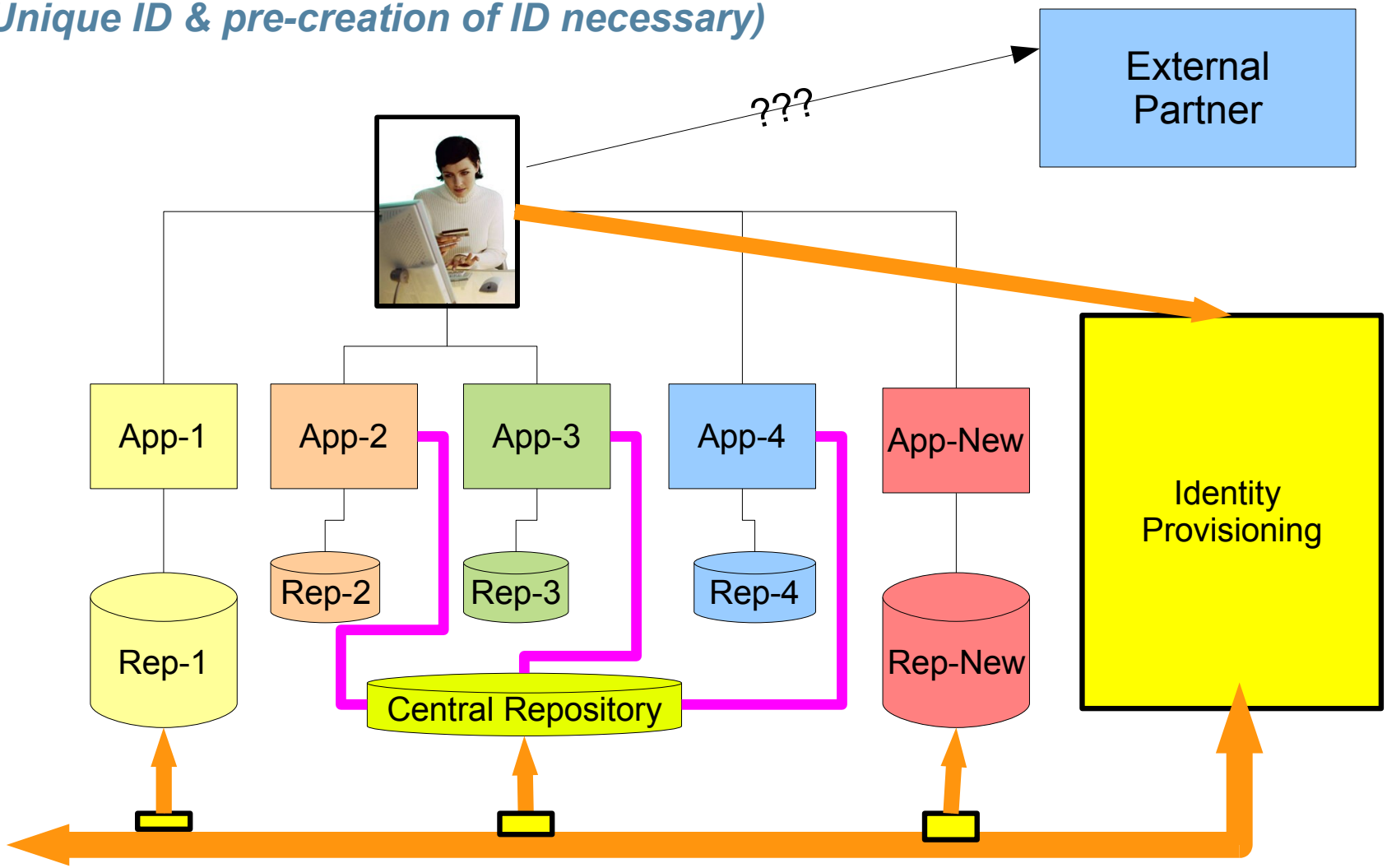
Next Generation in the cloud ?

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.

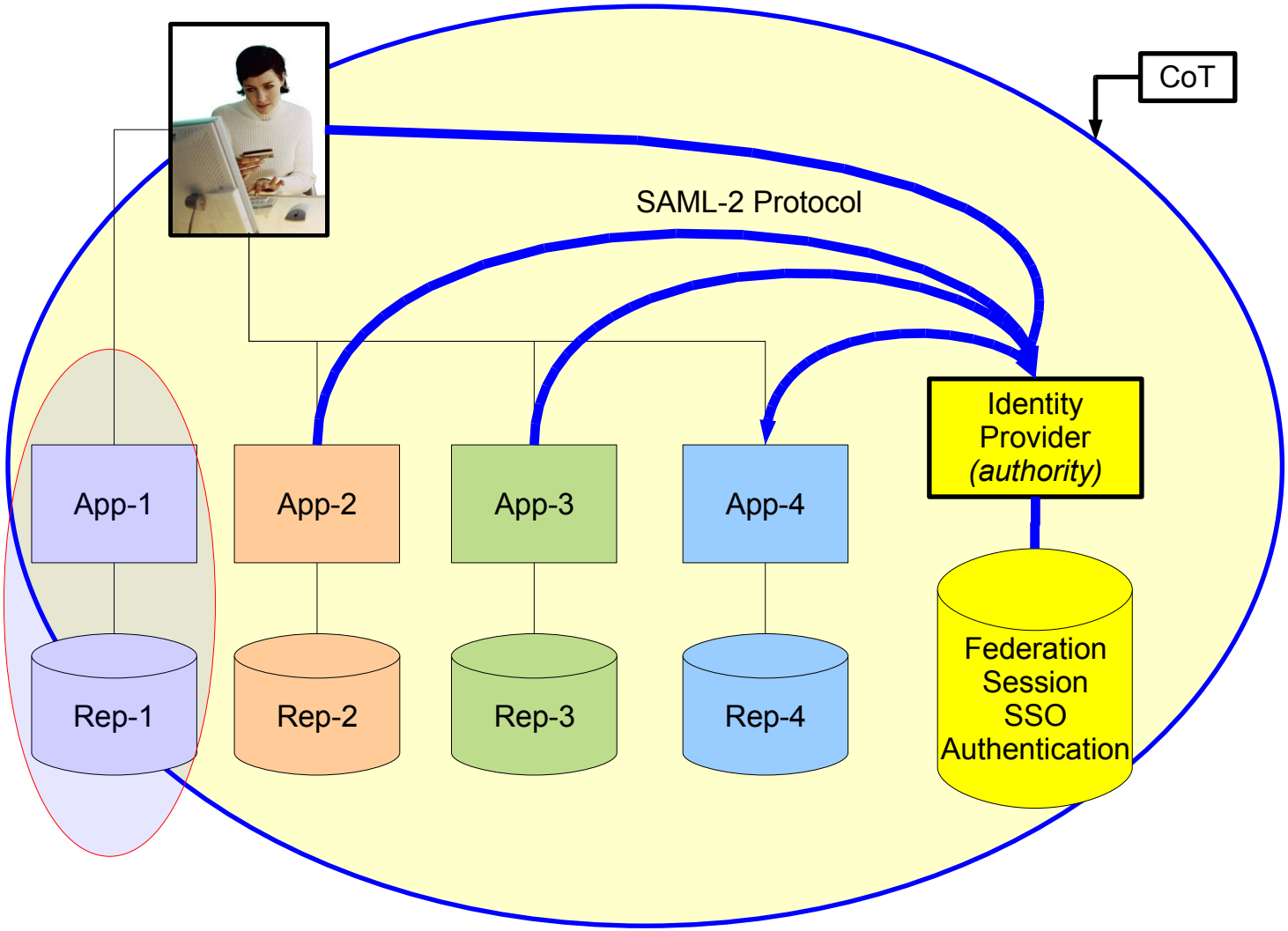
Identity Full Provisioning

(Unique ID & pre-creation of ID necessary)



Federation [Liberty-SAML2]

(no unique-ID, Lazy provisioning, Roaming)

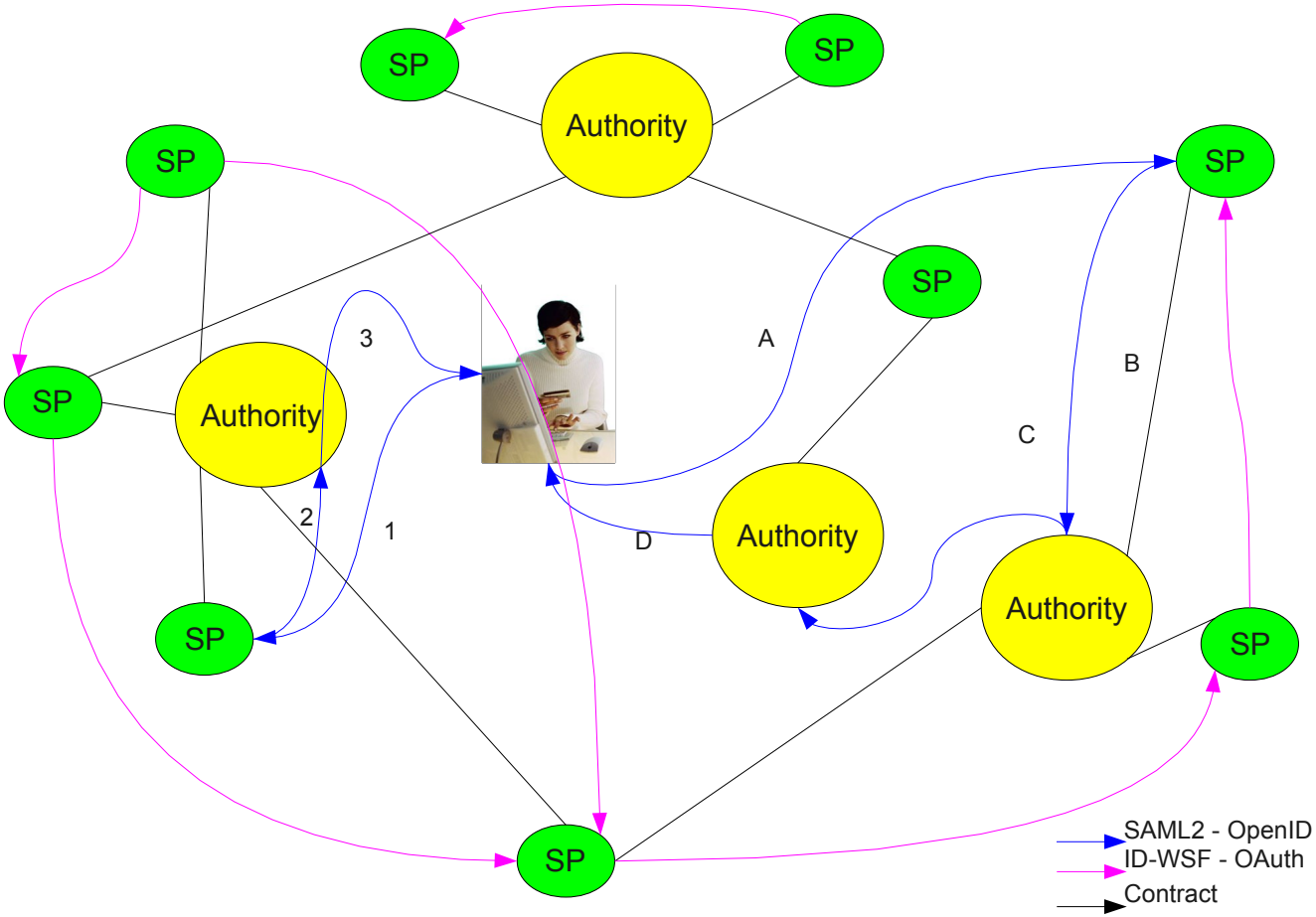


What we need to take decisions ?

- 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

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

Fully distributed, partially Heterogeneous



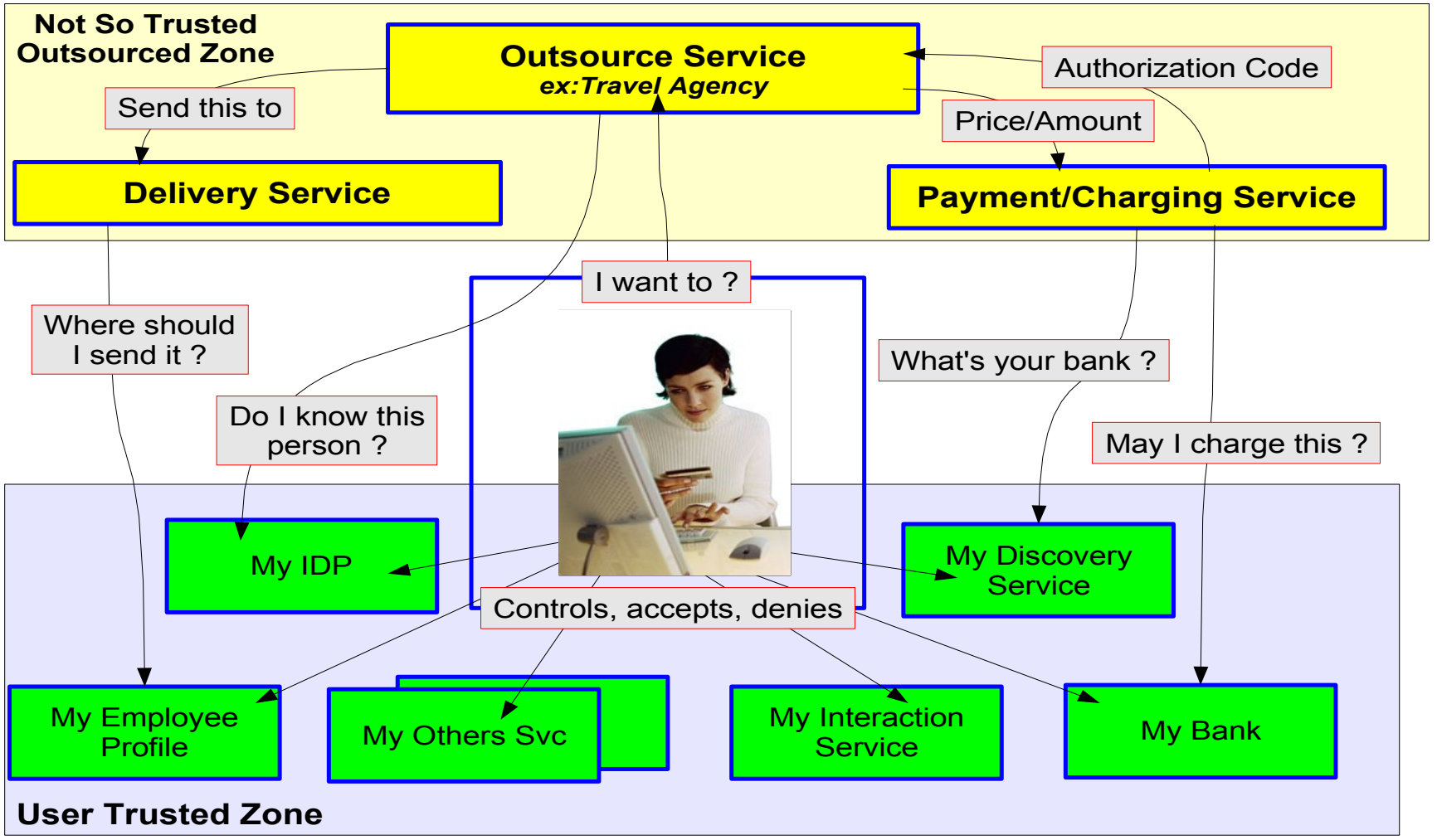
Weaknesses of traditional security

- 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

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
  - Impact both functionalities and performances.

Reality is somehow complex

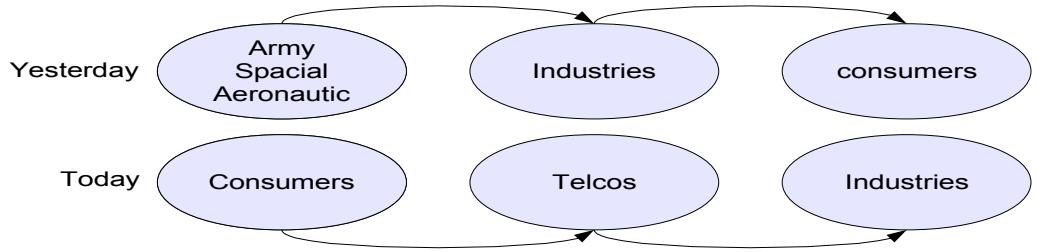


Let's imagine the future

- 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)

Which Identity Authorities ?

- 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

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 & CTO
Global Software Practice
Sun Microsystems
Fulup@sun.com

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