



# New Generation Identity Aware Web 2.0 Architecture

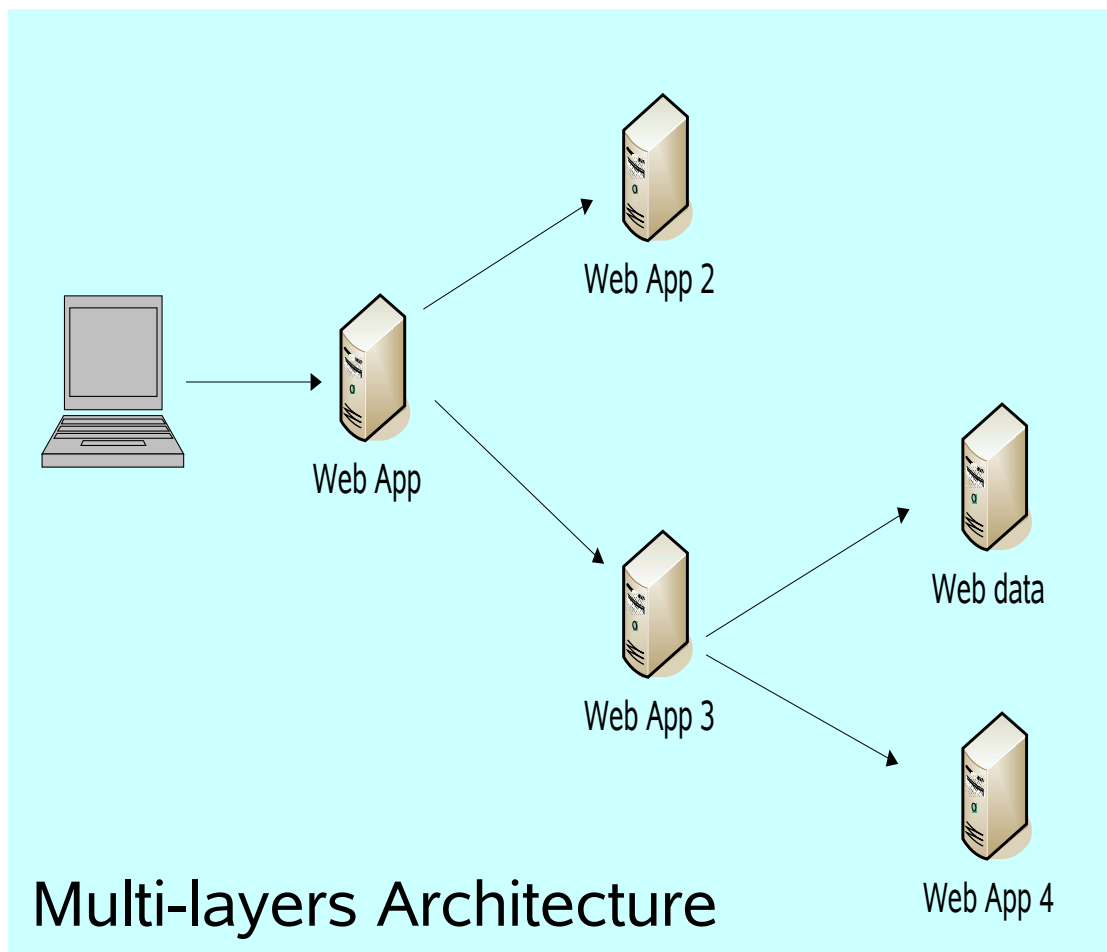
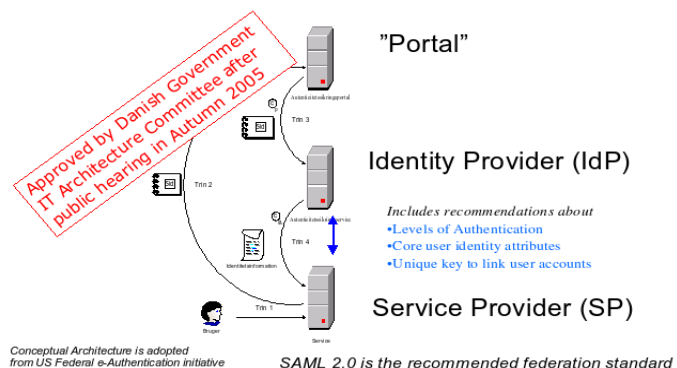
Fulup Ar Foll  
Master Architect  
Sun Microsystems  
Fulup@sun.com



# What's WEB-2.0 behind AJAX GUI



Reference Architecture for Cross-organizational Single Sign On

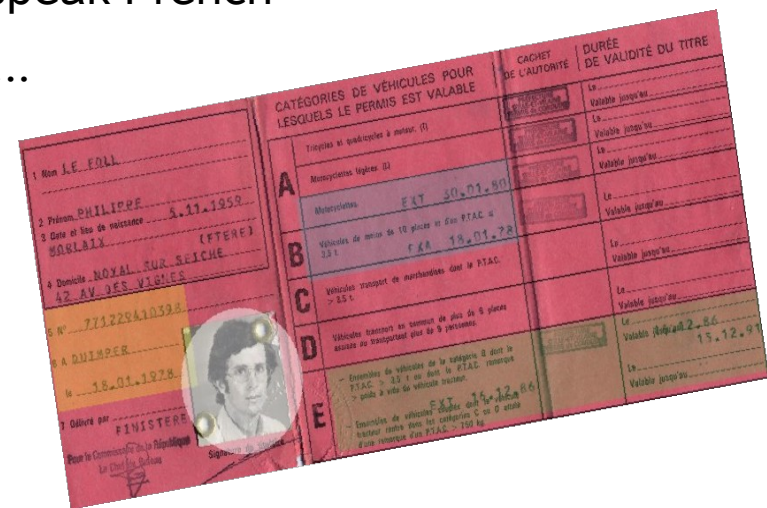


## Multi-layers Architecture



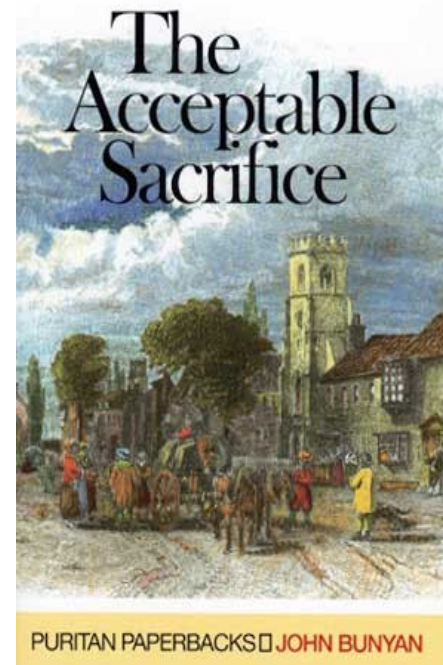
# Inside Technical ID ?

- **Authentication:** *proof you're the one you claim to be*
  - Biometric: picture, fingerprint, voice, ...
  - Secret: login/passwd, certificate, pin code, ...
- **Attributes:** *define what you are*
  - Authorization attributes: allow to drive a motorbike
  - Personalization attributes: preferred color, speak French
  - Group attributes: French citizen, Manager, ...
- **Verification:** *proof this document is valid*
  - Signature + Certificates
  - Date and place of issuance.
  - Validity time stamp.



# Limits toward digital ID?

- **Cost:** cheaper and cheaper every days
- **Legal:** uncompleted or no support.
- **Technology:** constant evolution, wait or not ?
- **Interoperability:** will the other follow me ?
- **Complexity:**
  - level of change user can absorb
  - level of manageability
- **Acceptability**
  - possible versus acceptable



# Standards why and what ?

## •Portability versus Interoperability

- Posix, Java, PHP,...
- TCP/IP, HTTP, SOAP,...

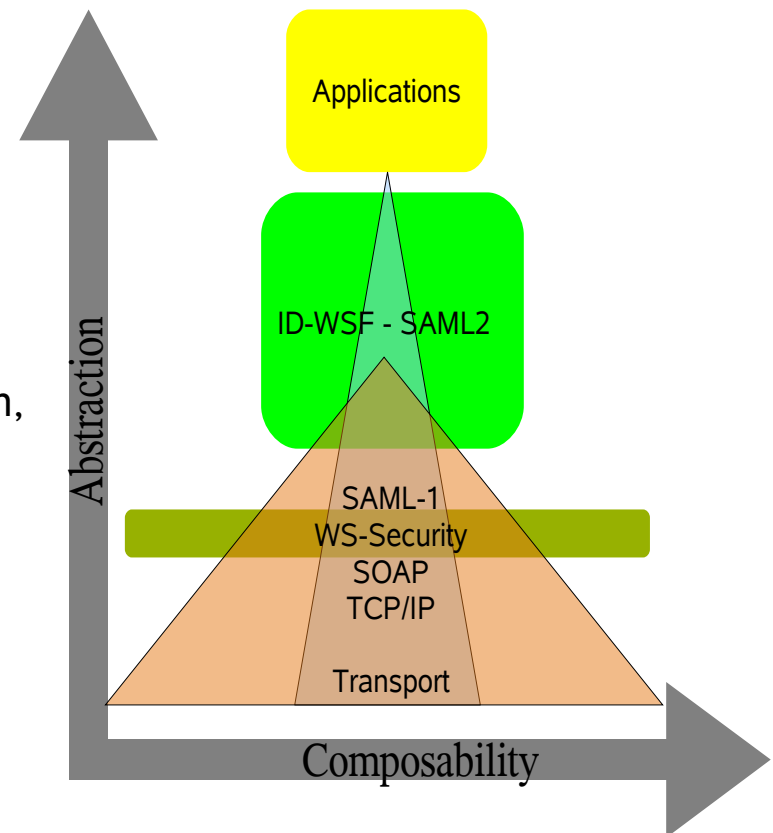
## •Cost of adoption

- legacy applications
- end-user adoption

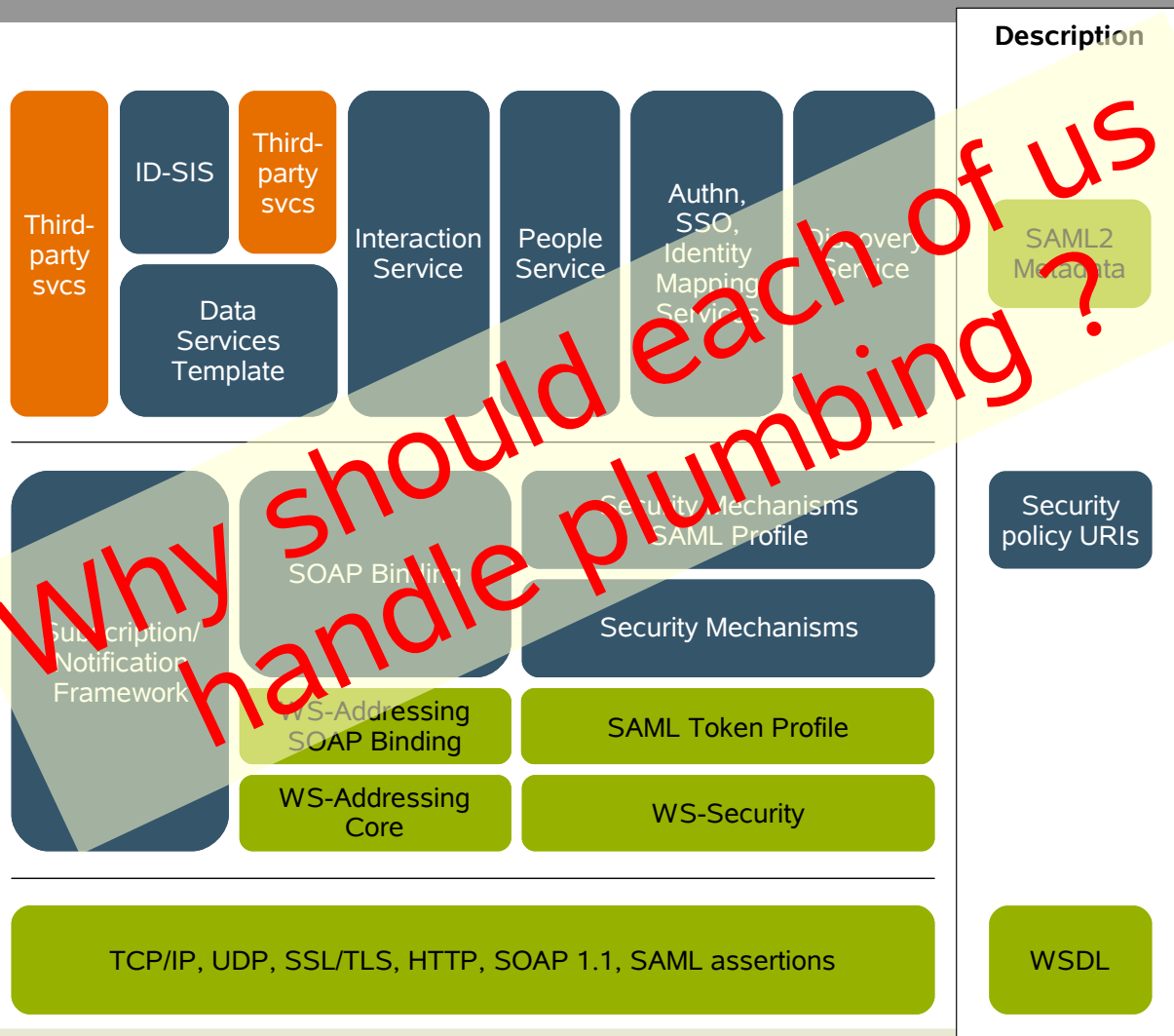
## •Level Services provided

- transport: end to end, point to point, stream, broadcast
- security: encoding, authorization, authentication, legal compliance
- infrastructure: user schema, group management, discovery mechanism
- Compliance to legislation

•etc.

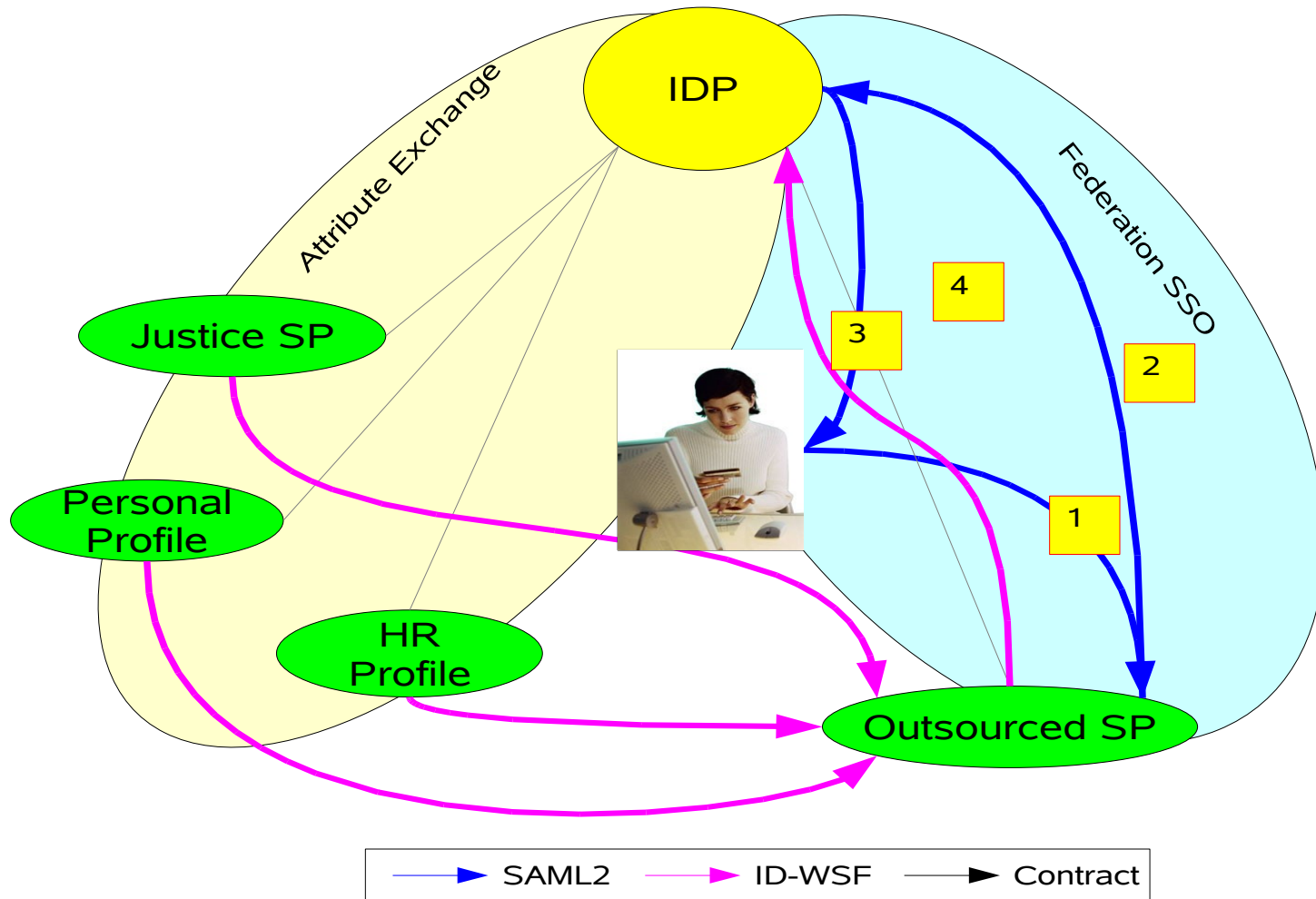


# Should we even know about this ?



- Legend:**
- Liberty Alliance standard
  - External standard
  - Third-party (possibly a standard)

# Outsourced Simplified Flow



# Which Authority's Components

## ■ Basic Authority Services

### ■ Authentication Framework

- Common definition of risk
- Common authentication confidence for a given risk

### ■ Federation framework

- Multi-authority (proxy IDP model)
- Multi-personality

### ■ Discovery Mechanism

- Where to find services (in a user contextual mode)
- Security Mechanism (Attributes shared 1<sup>st</sup> policy decision point)
- Identity mapping (peer to peer in privacy aware mode)

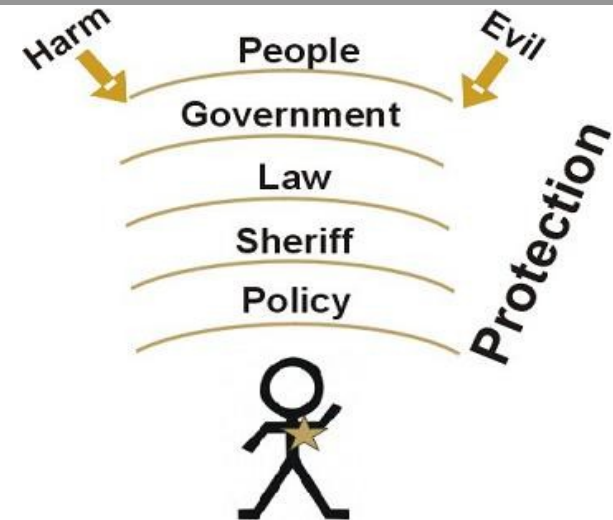
### ■ Social networking

- Should support delegation
- Capability to create informal group of people

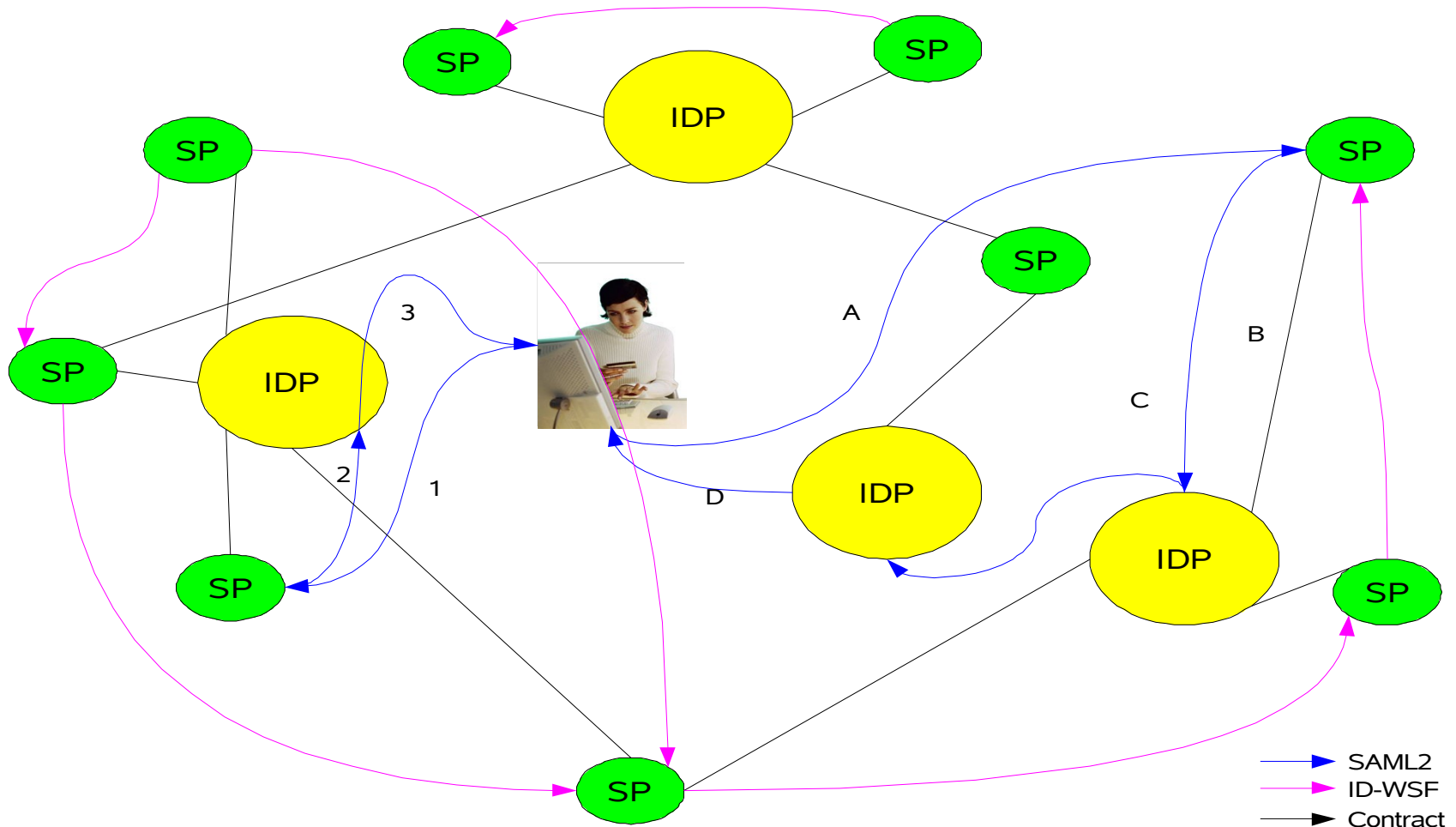
### ■ Interaction Service

- Should allow user to be in control at any time

## ■ Advanced Services: Personal Profile, Document Exchange, Dashboard, ...



# Web-2.0 Federated Architecture





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

<http://www.projectliberty.org>

<http://www.sun.com>

<http://www.telenor.com/telektronikk>