



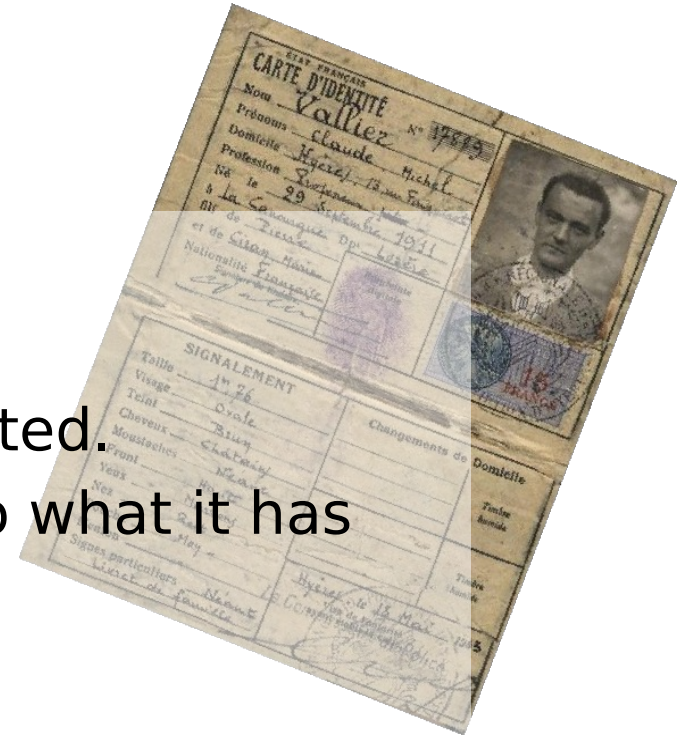
Identity 2.0 Enabled Architecture

Fulup Ar Foll
Liberty Technical Expert Group

Master Architect, Global Software Practice
Sun Microsystems

Digital versus Paper

- Same fundamentals
 - usually not so many secrets.
 - when collected usually never deleted.
 - want to keep information usage to what it has been collected for.
- Key differentiators
 - easy & cheap mass analysis simple correlation research
 - lack of stability: change too fast for basic human brain and legal framework.
 - unlimited capabilities: Moving from what we can, to what is acceptable.



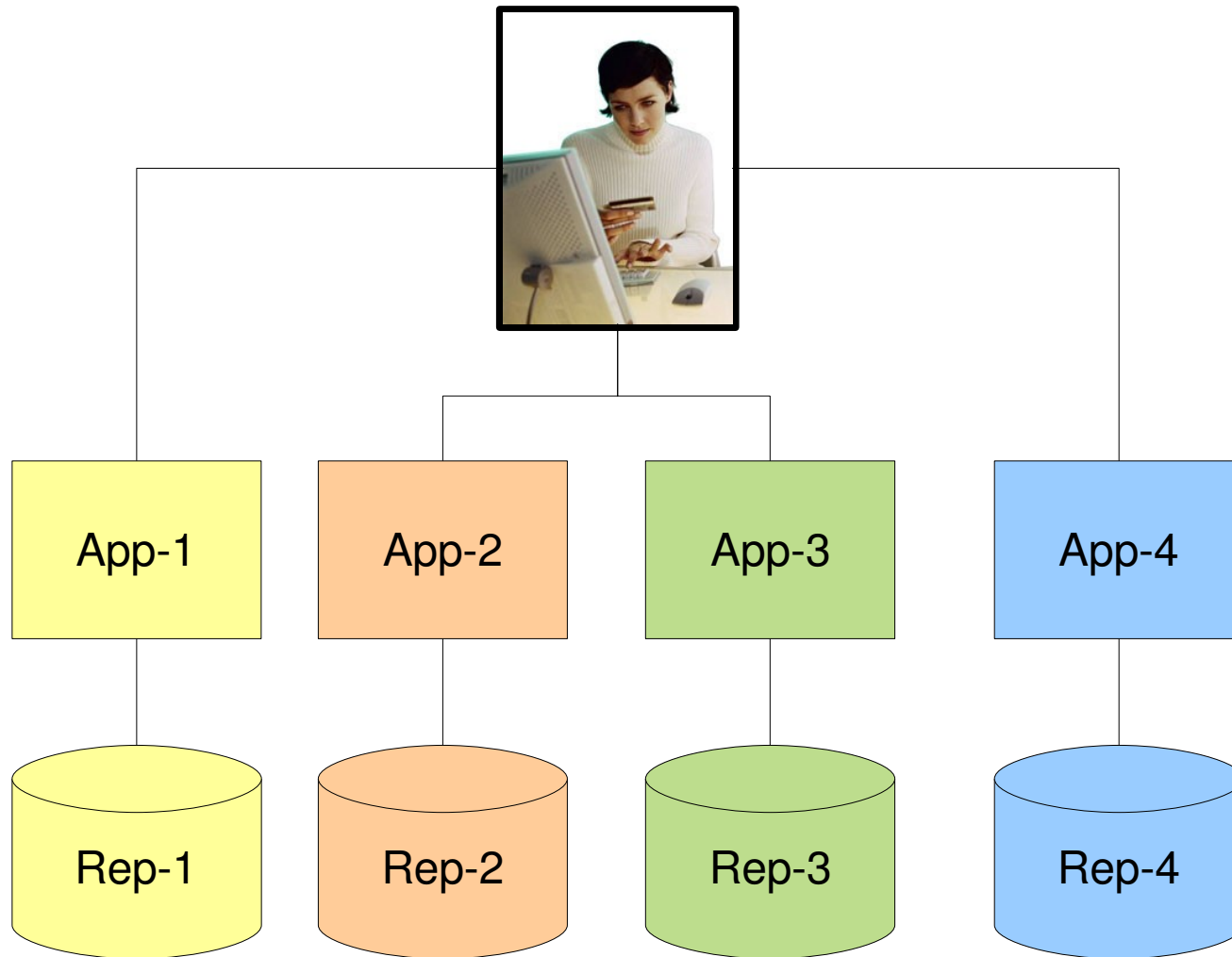
Inside Technical ID ?

- **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.



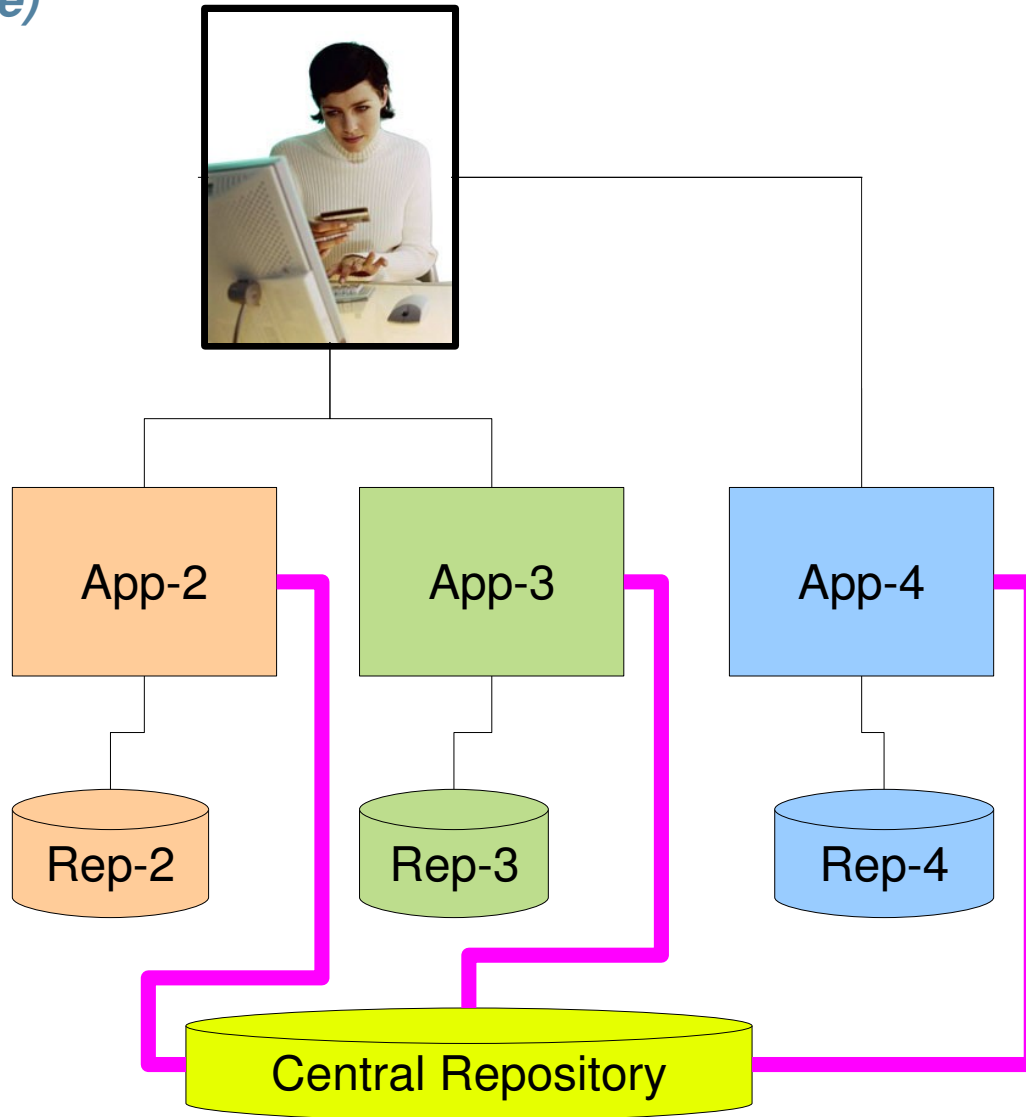
Identity Legacy

(let's built my own flavor)



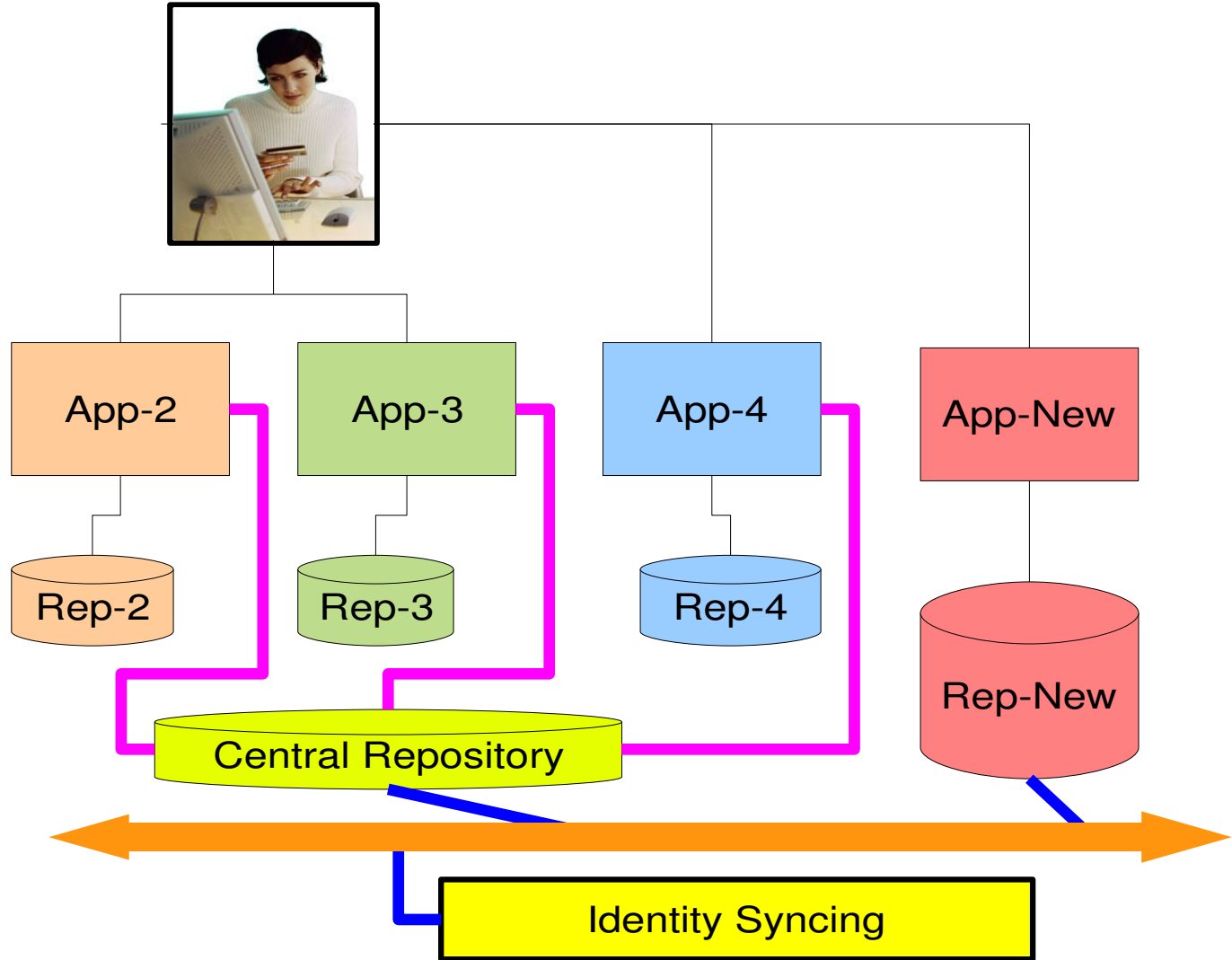
Unique Central repository

(almost unique)



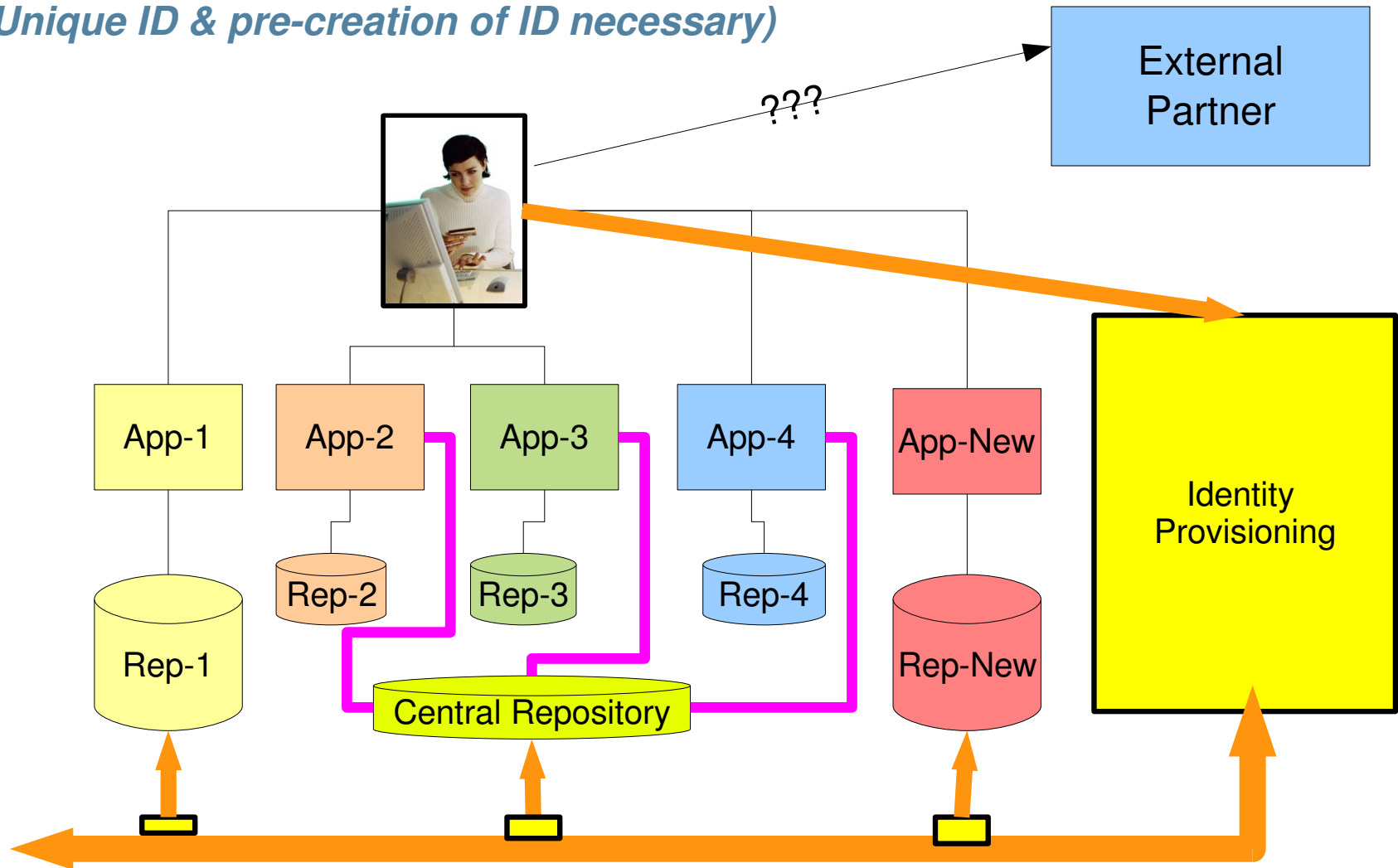
Identity and Password Syncing

(adhoc solution, hero period, do it yourself)



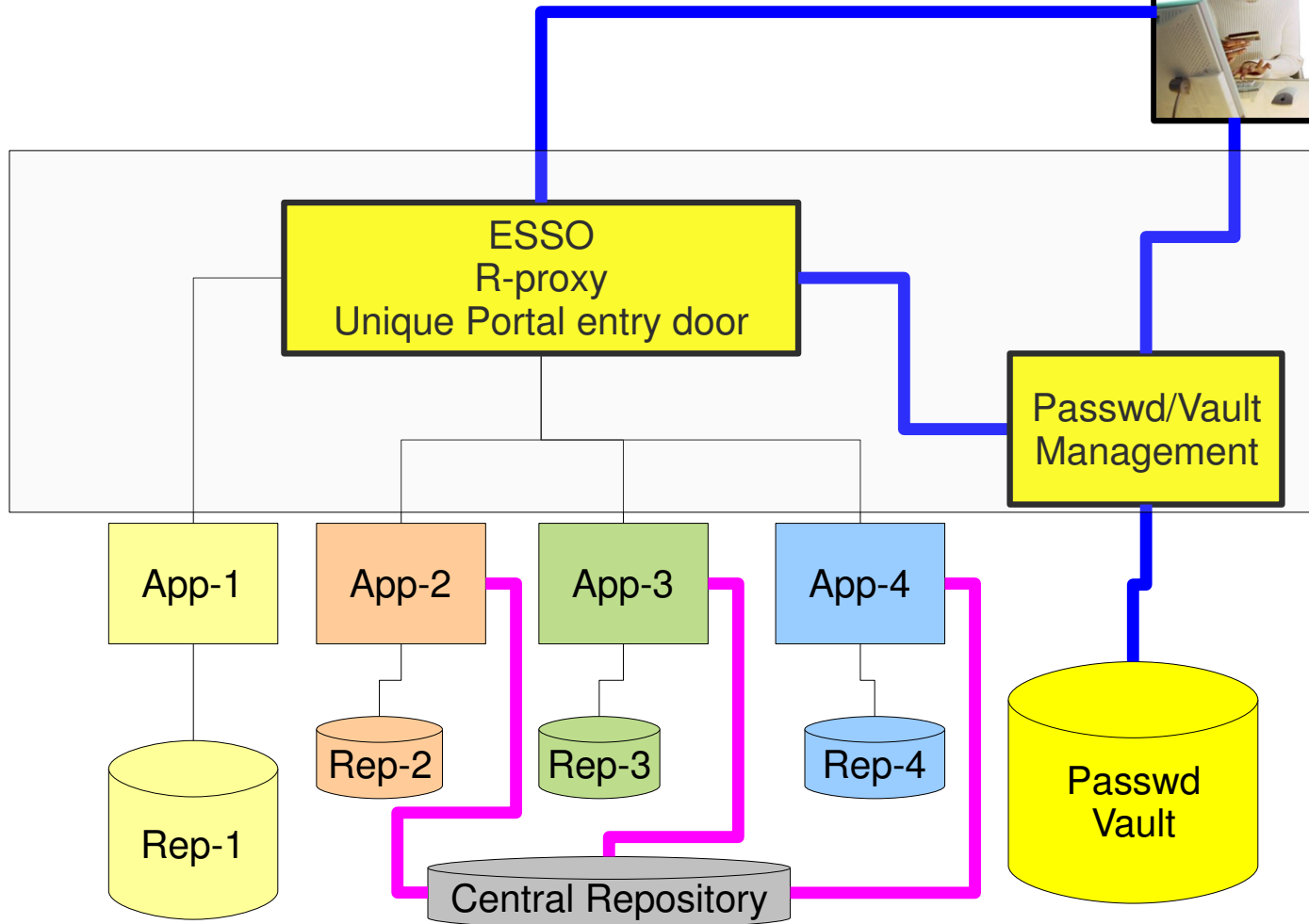
Identity Full Provisioning

(Unique ID & pre-creation of ID necessary)



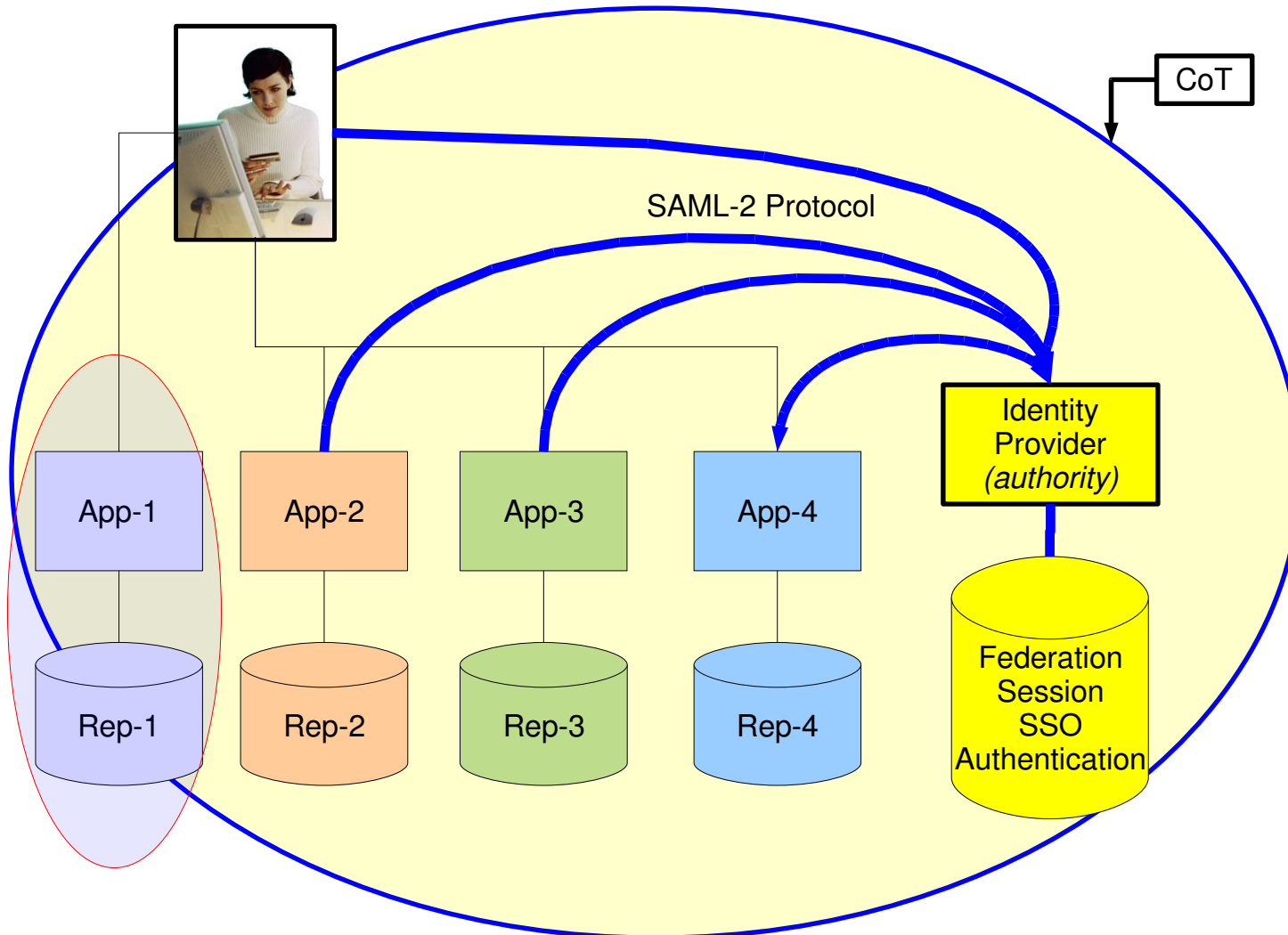
Portal centric, eSSO, rProxy,

(do not solve the problem, but hide it)



Federation [Liberty-SAML2]

(no unique-ID, Lazy provisioning, Roaming)



Should we even know about this ?



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

Identity Framework problematic

User

- Seamless (nothing is too simple)
- Consent (nothing without my consent)
- Multiple personalities
- Delegation

User Secure/Trust ?

Authentication/Authorization

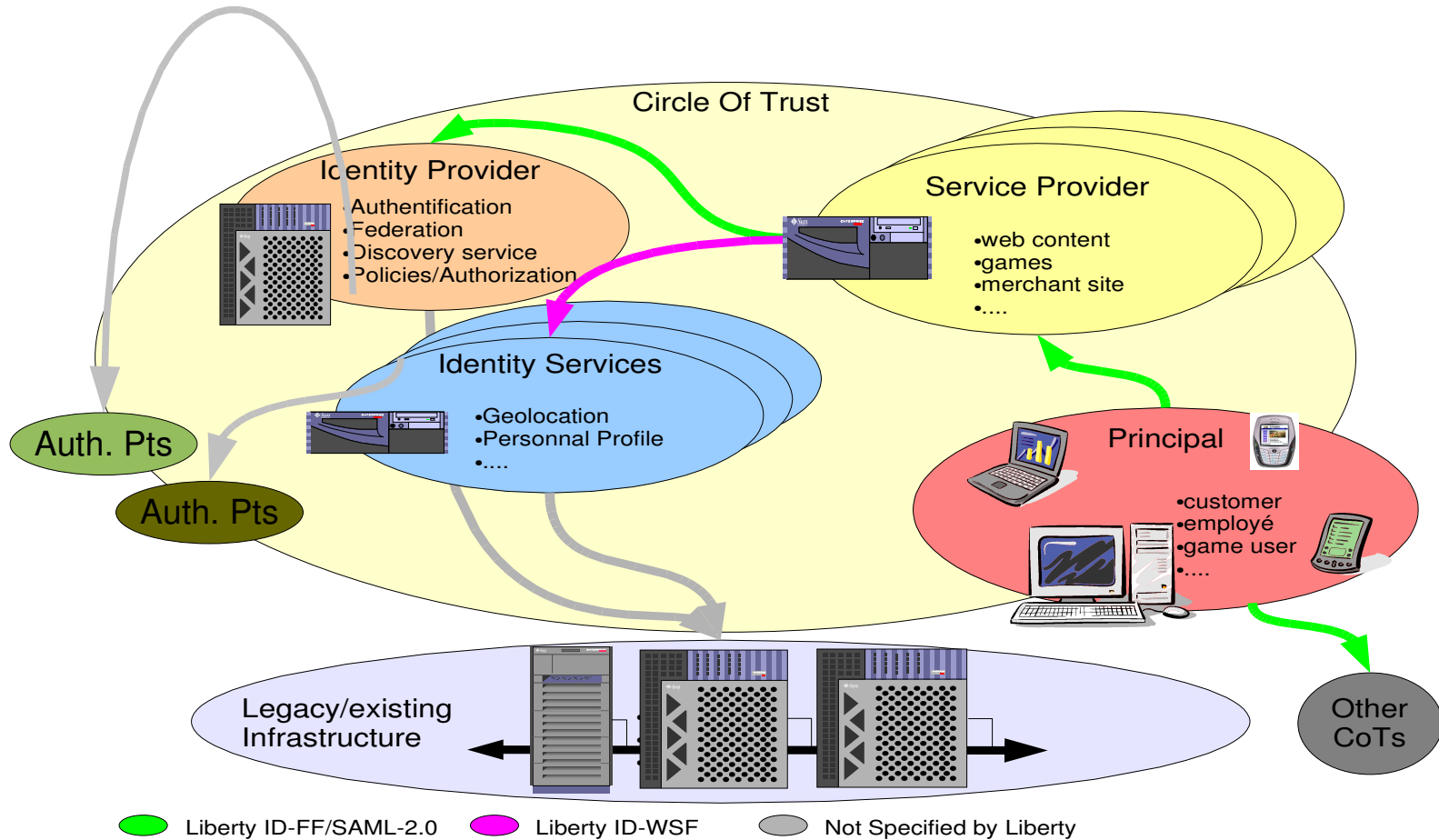
- Shared/Compatible risk levels
 - Common Authentication trust
 - Cross Border/CoT (roaming user)
- Multiple Identity (issuerID/targetID)

CoT

Attributes Exchange

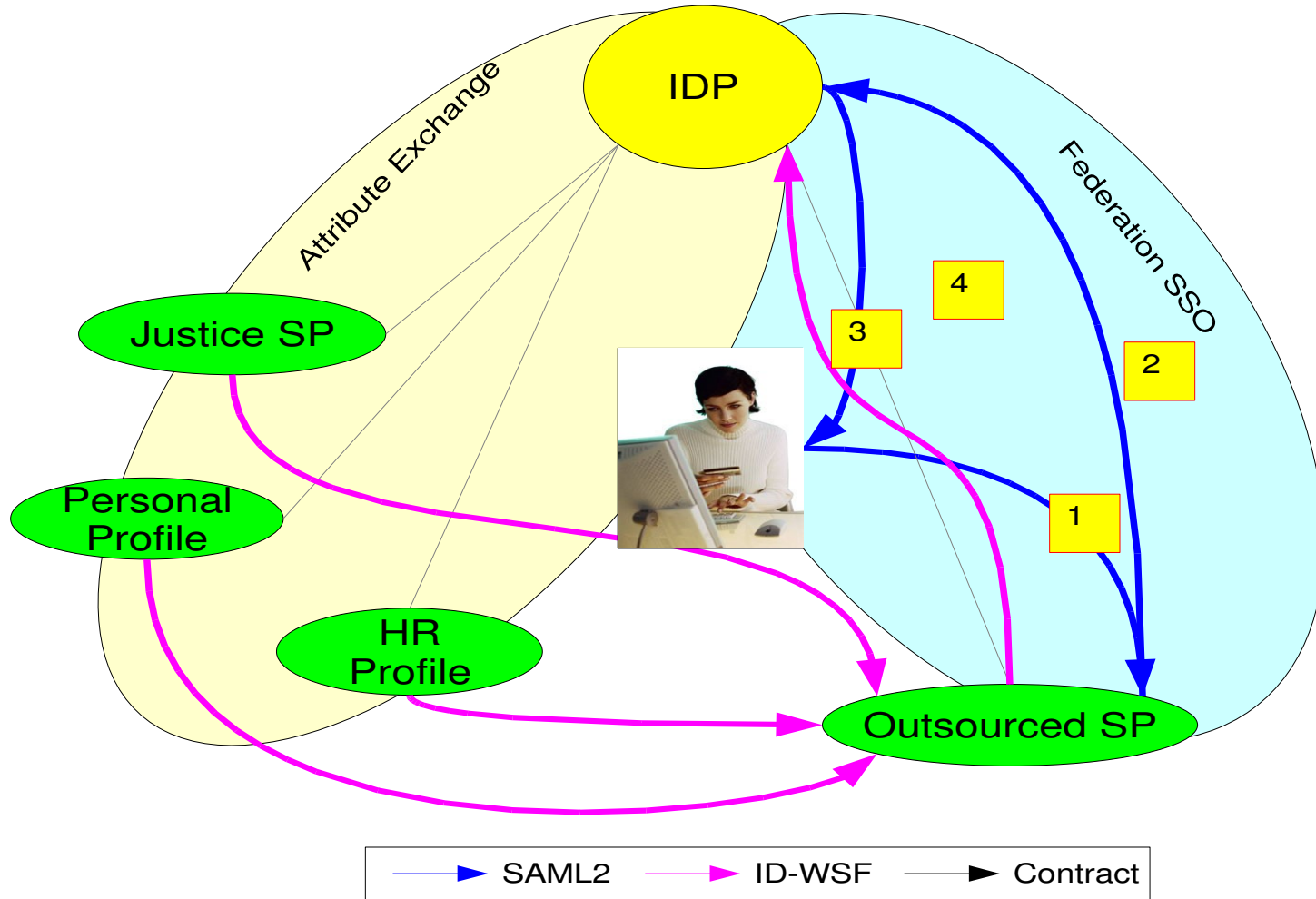
- Authoritative source
 - Level of validation of the information
 - Policy to release/store/receive
 - Big Brother Danger
 - Duplication/Depreciation
- Right to correct

Global Liberty Architecture



Simplified Federated Flow

(Liberty-SAML2 and ID-WSF)



How much user centric ?

- **Dick Hart & Kim Cameron**

- Protocol passed through end user terminal
- Because SP/RP must trust user terminal, no contract in between IDP and SP/RP is required.
- Self defined or when needed ID can be signed/store by a trusted authority

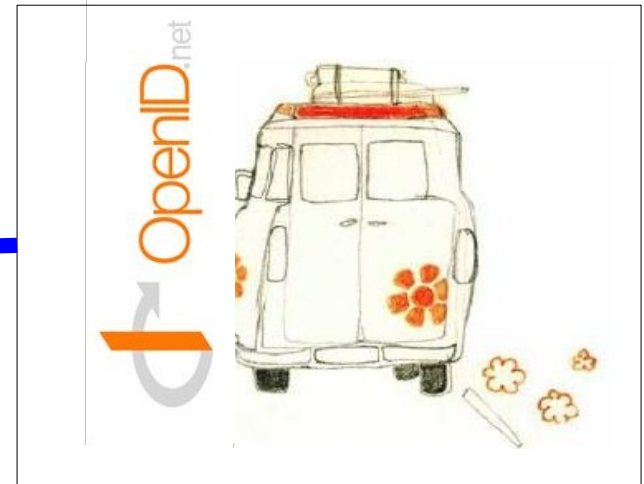
- **Open-ID**

- “Nobody should own this” (*Brad Fitzpatrick*)
- User as full freedom of choosing its ID and IDP
- User can delegate or handle its own authority

- **Liberty-SAML2**

- Protocol with built-in privacy
- User as to consent, when ever needed
- Relation based on a contractual trust

User Centric versus User Control



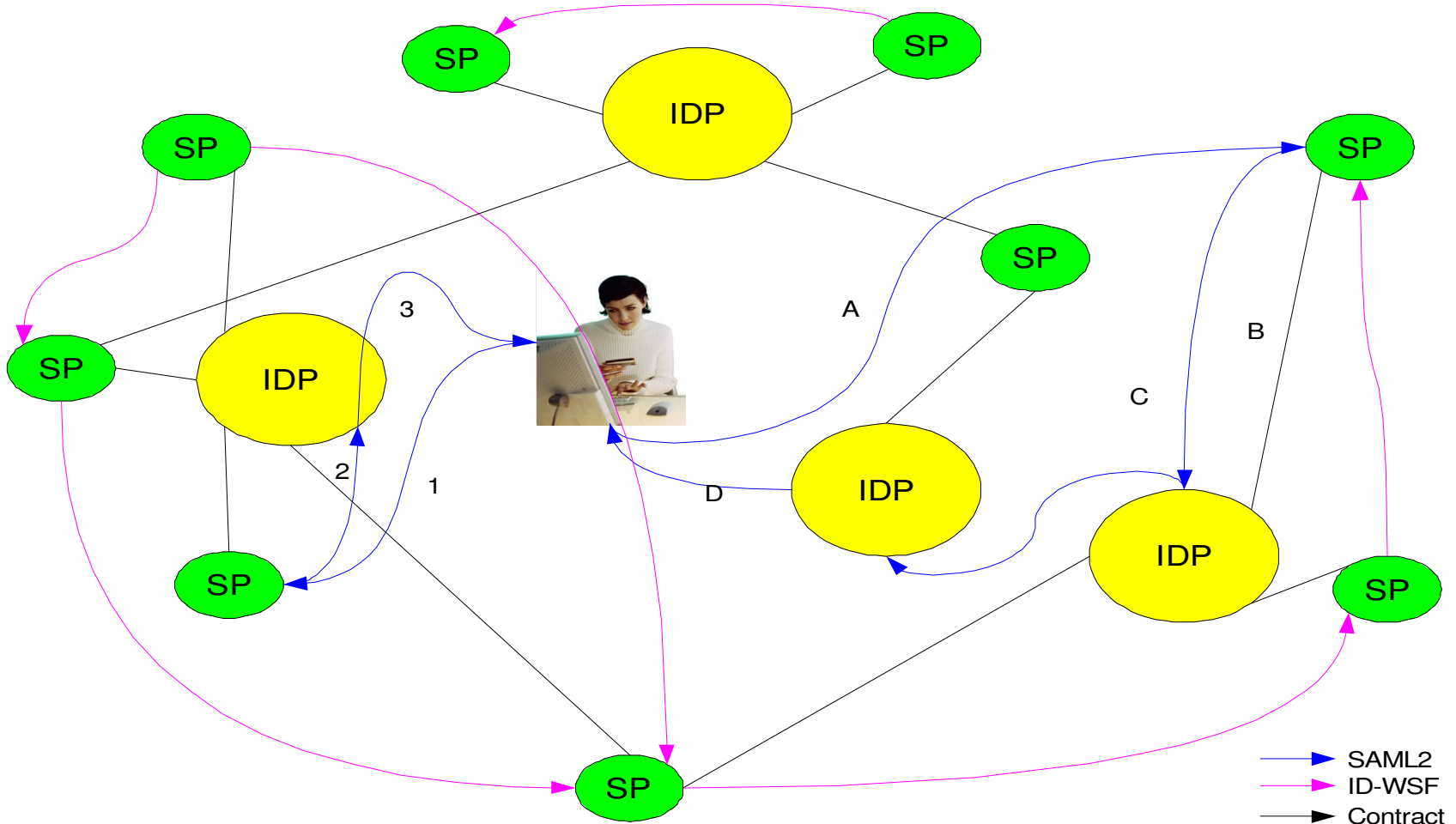
Cardspace / ID selectors



TCP/IP Brain interface



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>