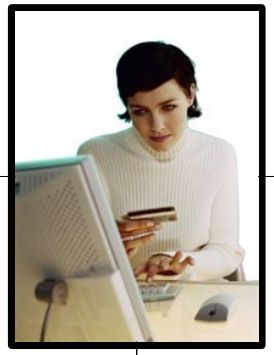
Identity Jungle

Fulup Ar Foll
Liberty Technical Expert Group

Master Architect, Global Software Practice
Sun Microsystems

Identity Legacy

(let's built my own flavor)

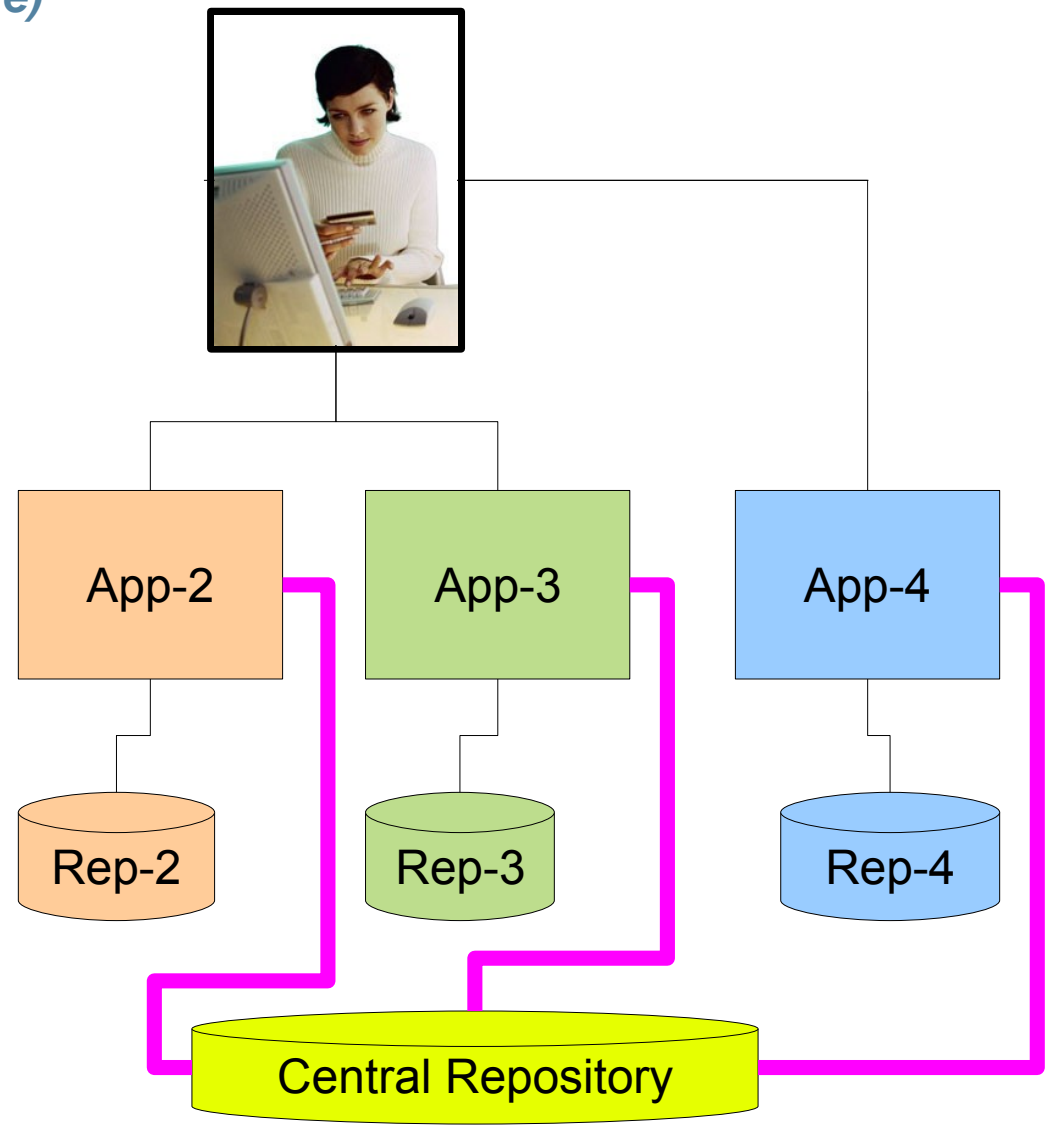


App-1 App-2 App-3 App-4

Rep-1 Rep-2 Rep-3 Rep-4

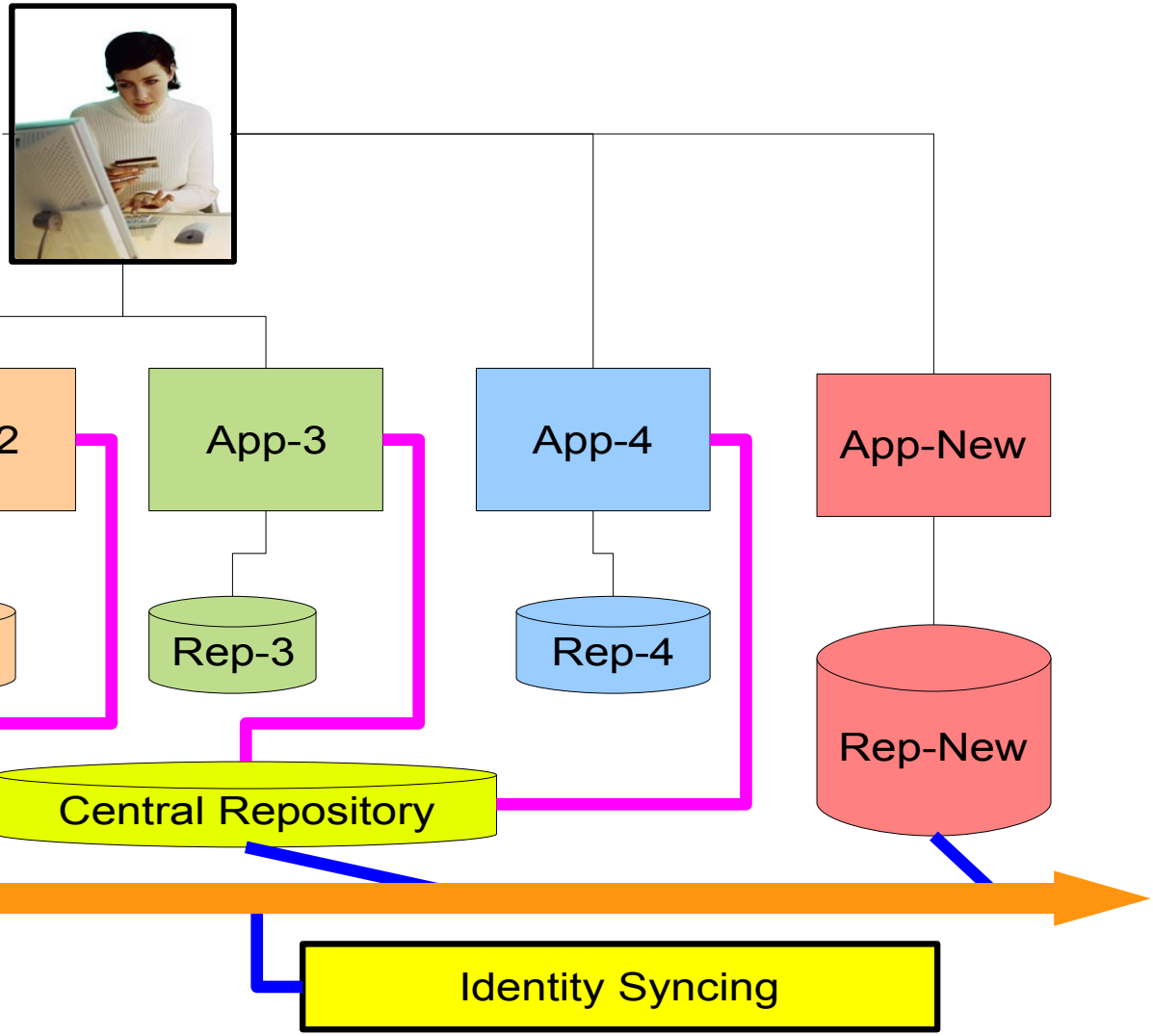
Unique Central repository

(almost unique)



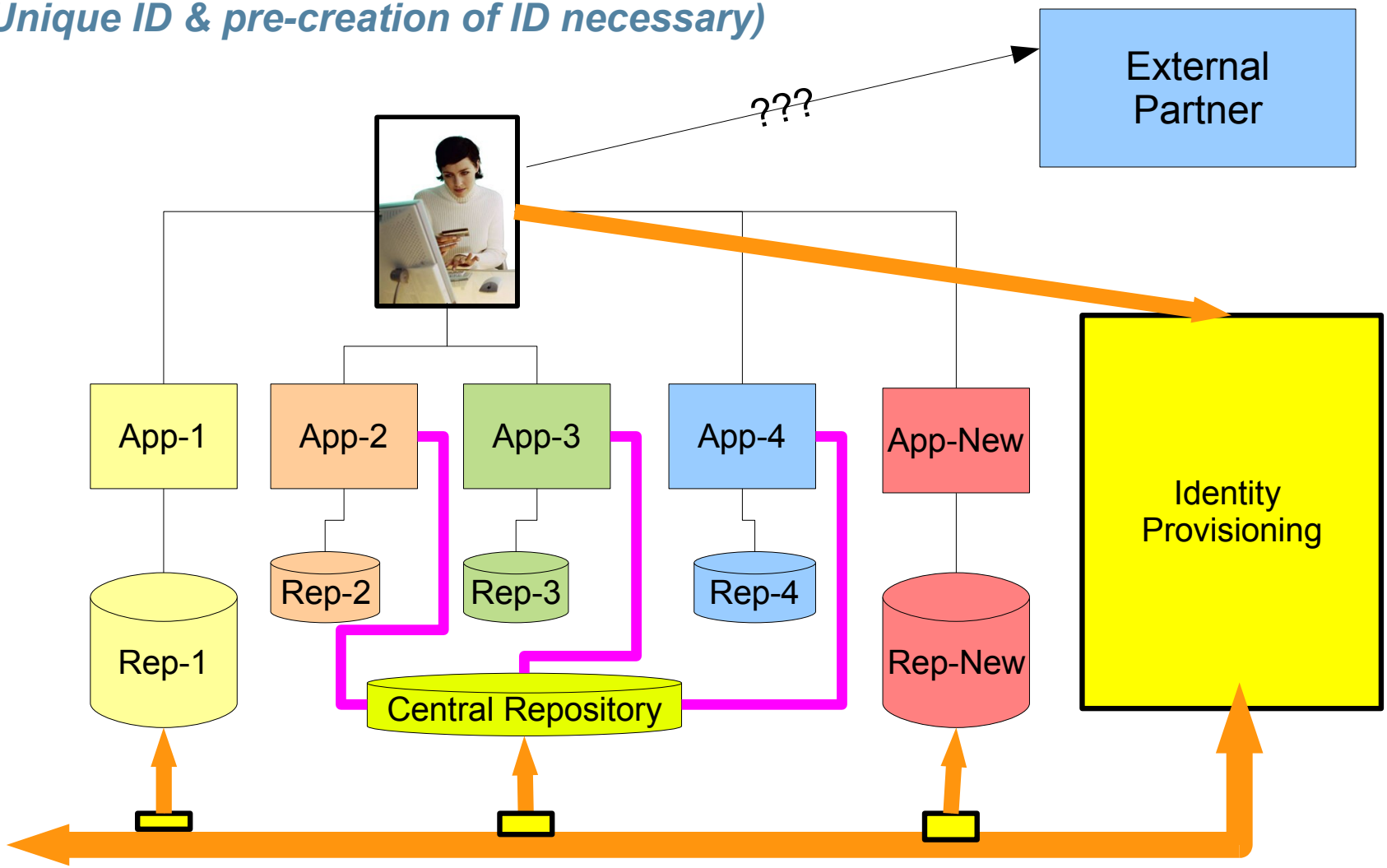
Identity and Password Syncing

(adhoc solution, hero period, do it yourself)



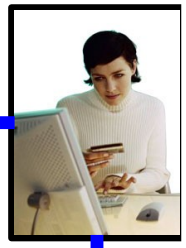
Identity Full Provisioning

(Unique ID & pre-creation of ID necessary)



Portal centric, eSSO, rProxy,

(do not solve the problem, but hide it)



ESSO
R-proxy
Unique Portal entry door

Passwd/Vault
Management

App-1

App-2

App-3

App-4

Rep-1

Rep-2

Rep-3

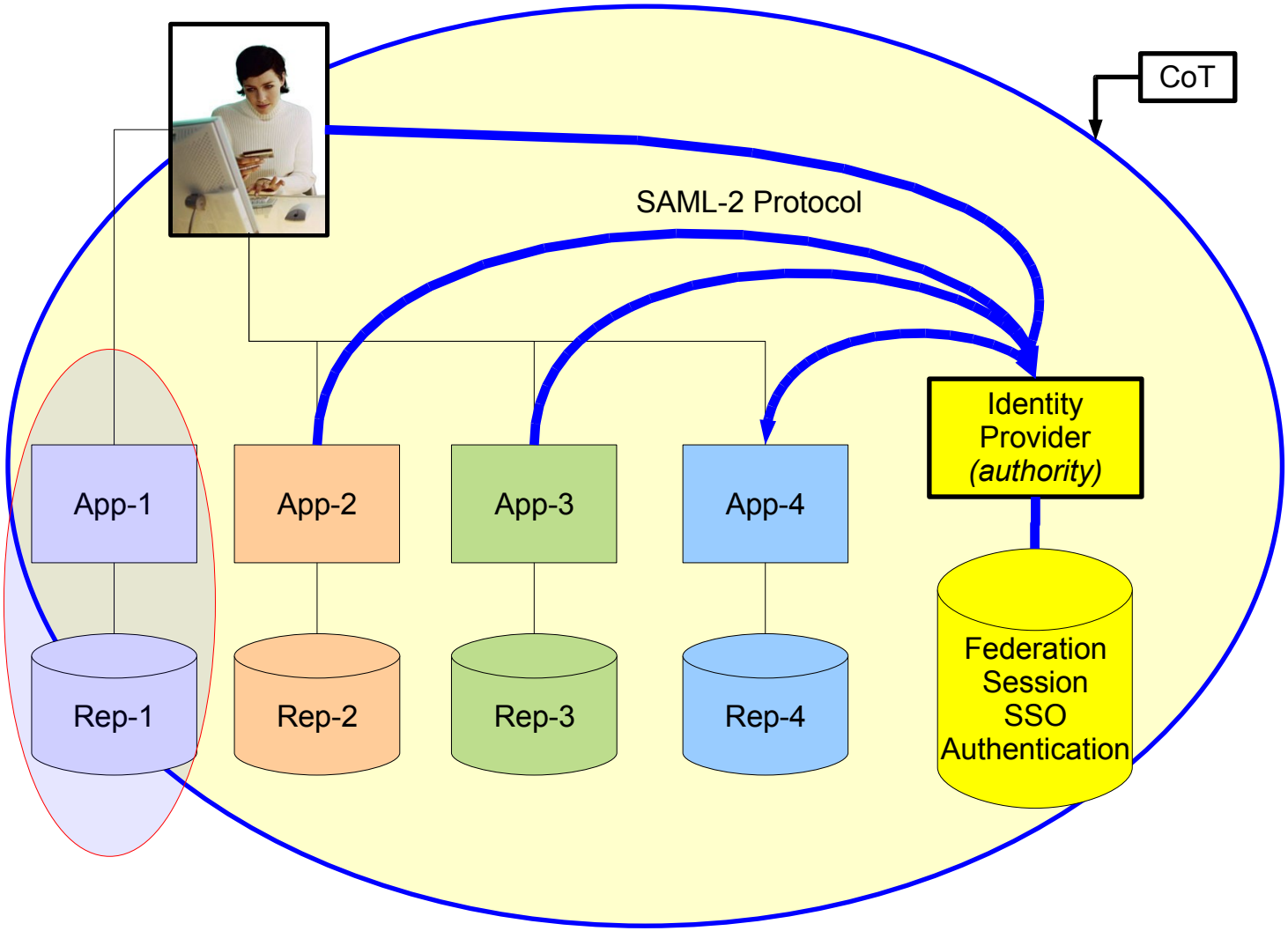
Rep-4

Central Repository

Passwd
Vault

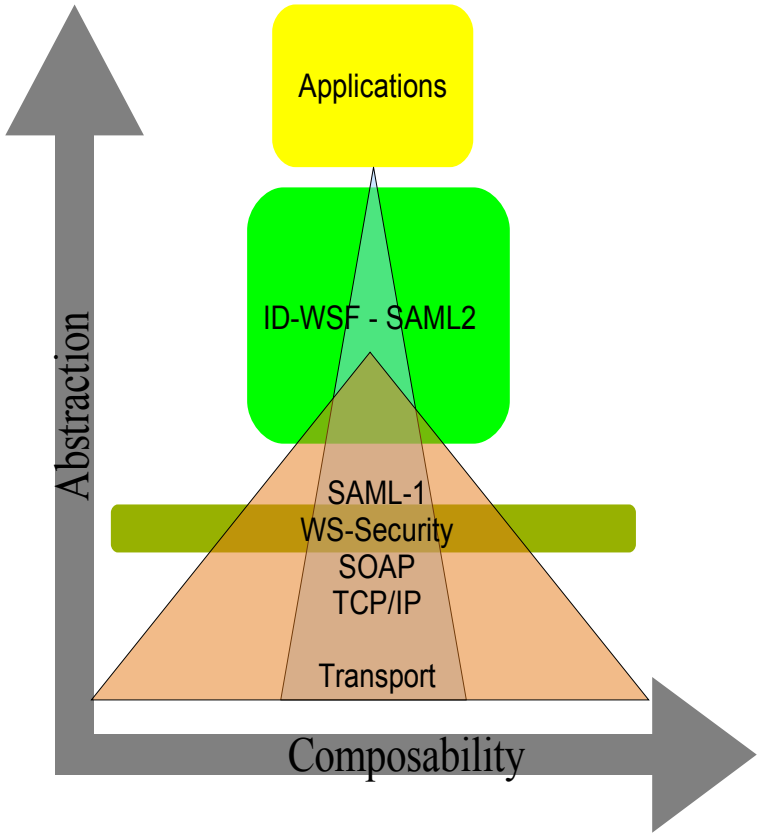
Federation [Liberty-SAML2]

(no unique-ID, Lazy provisioning, Roaming)

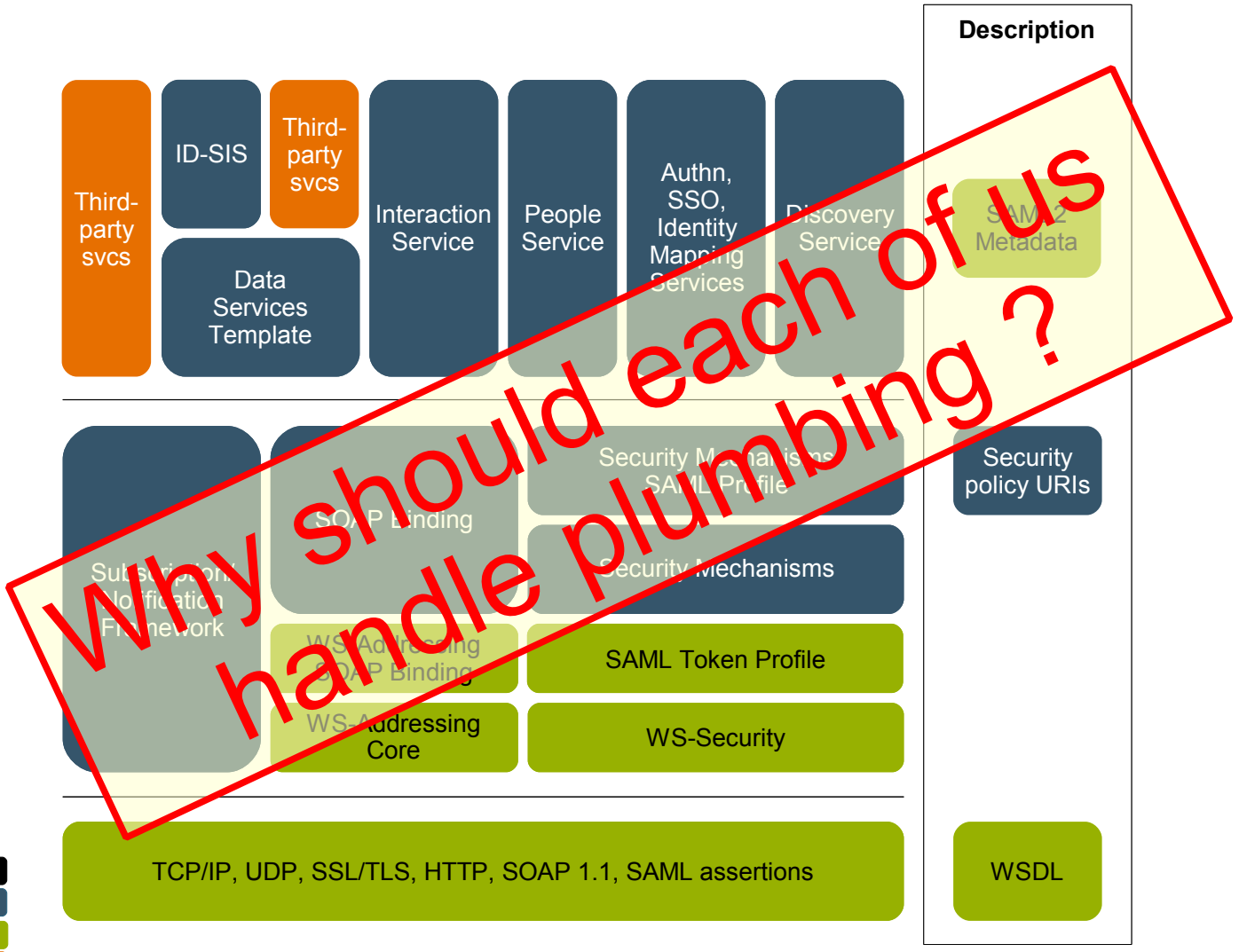


Standards why and what ?

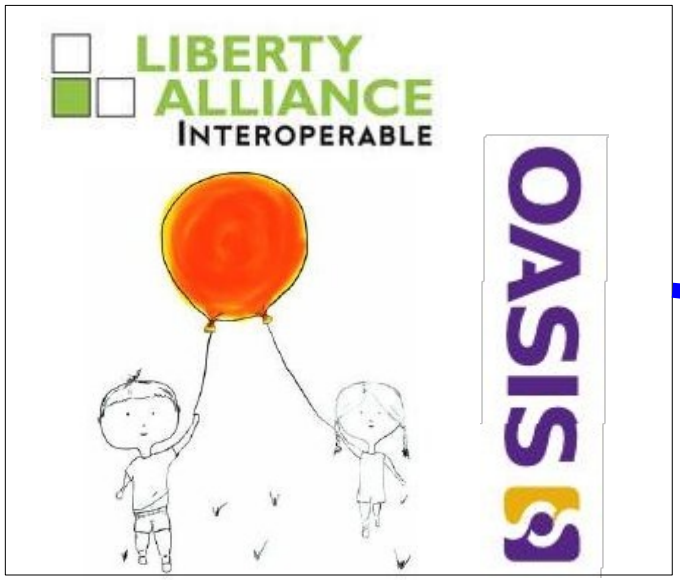
- **Portability versus Interoperability**
  - Posix, Java, PHP,...
  - TCP/IP, HTTP, SOAP,...
- **Cost of adoption**
  - legacy applications
  - end-user adoption
- **Level Services provided**
  - transport: end to end, point to point, stream, broadcast
  - security: encoding, authorization, authentication, legal compliance
  - infrastructure: user schema, group management, discovery mechanism
  - Compliance to legislation
- etc.



Should we even know about this ?



User Centric versus User Control



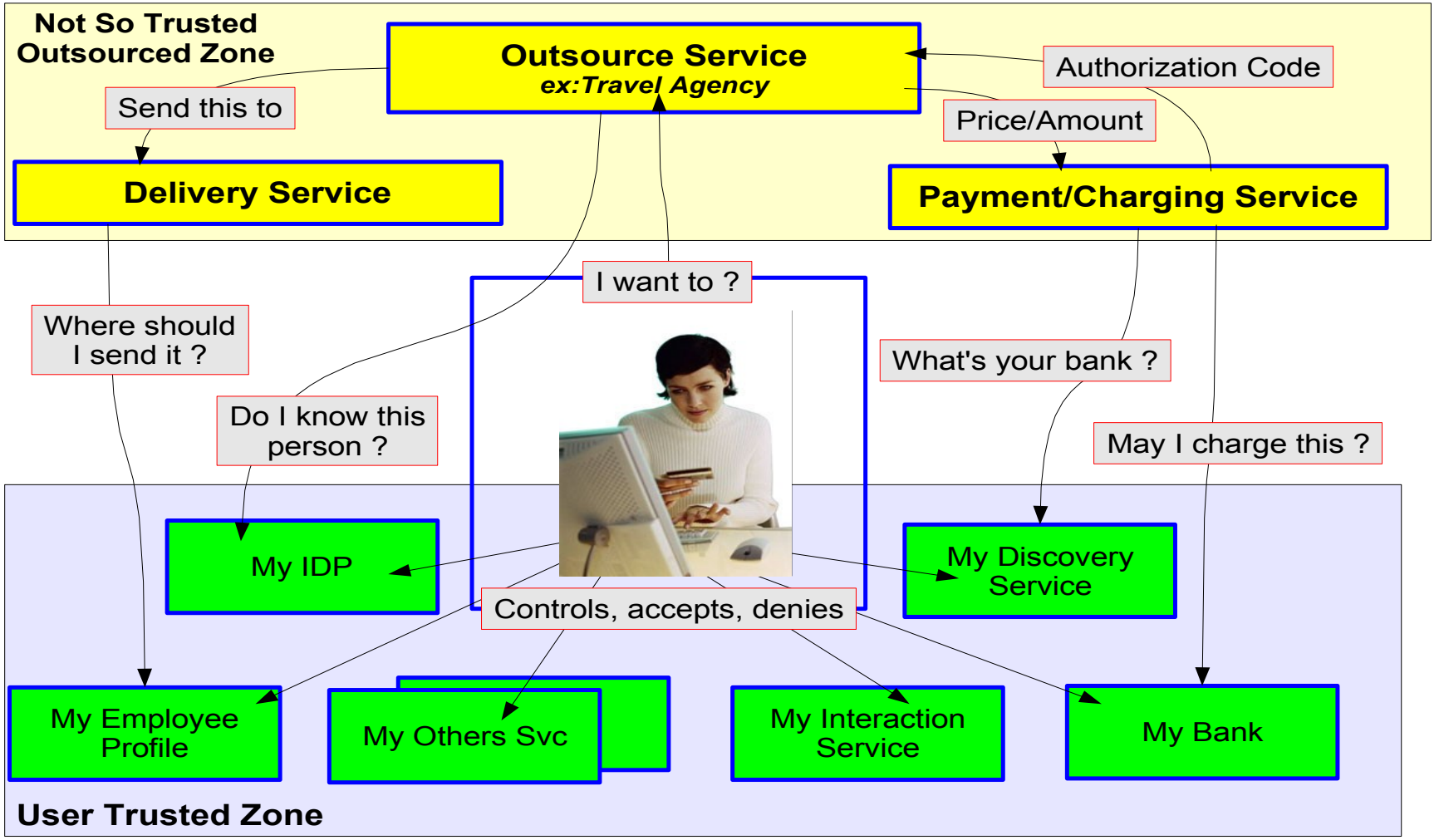
TCP/IP Brain interface

Cardspace / ID selectors

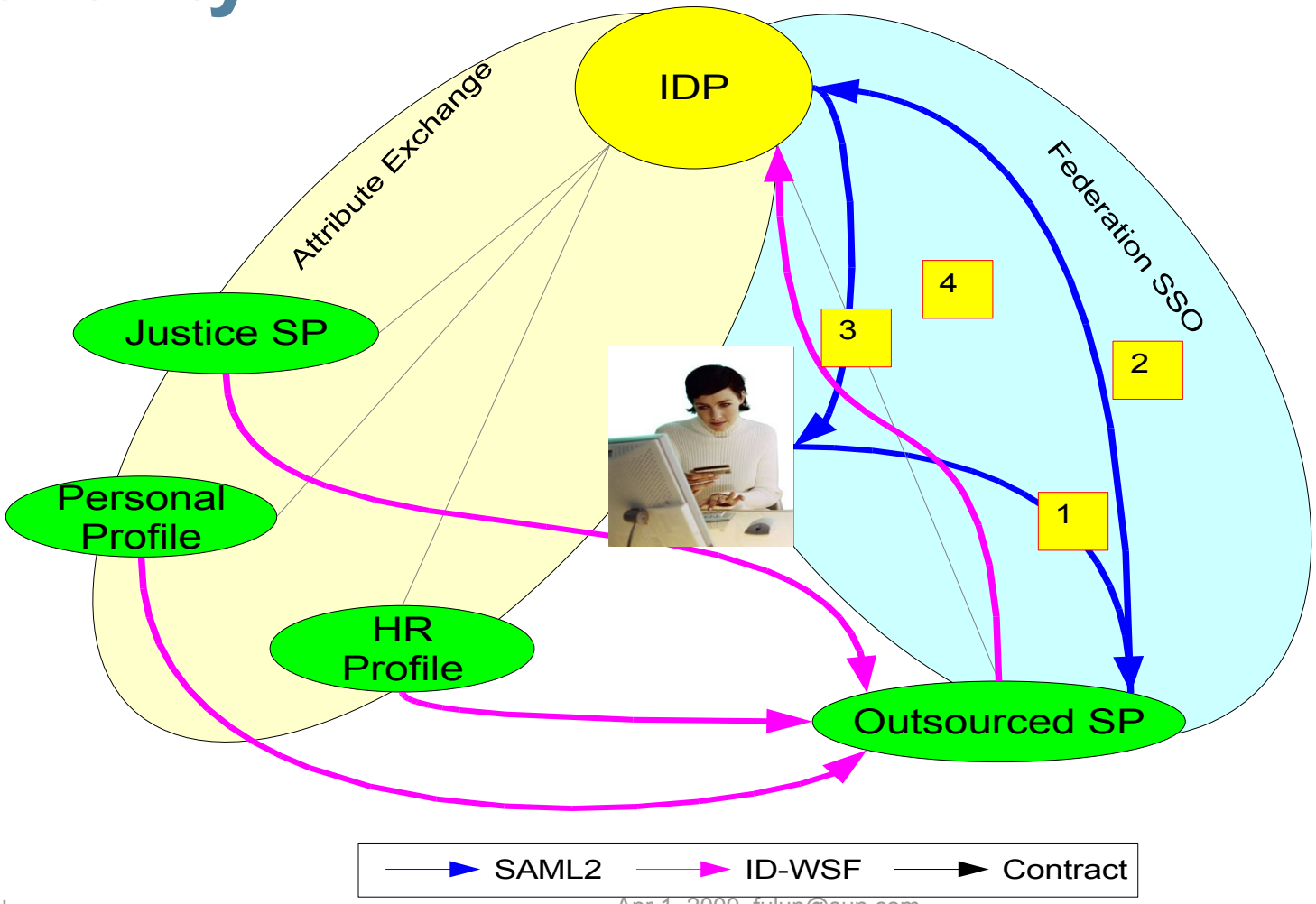
How much user centric ?

- **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

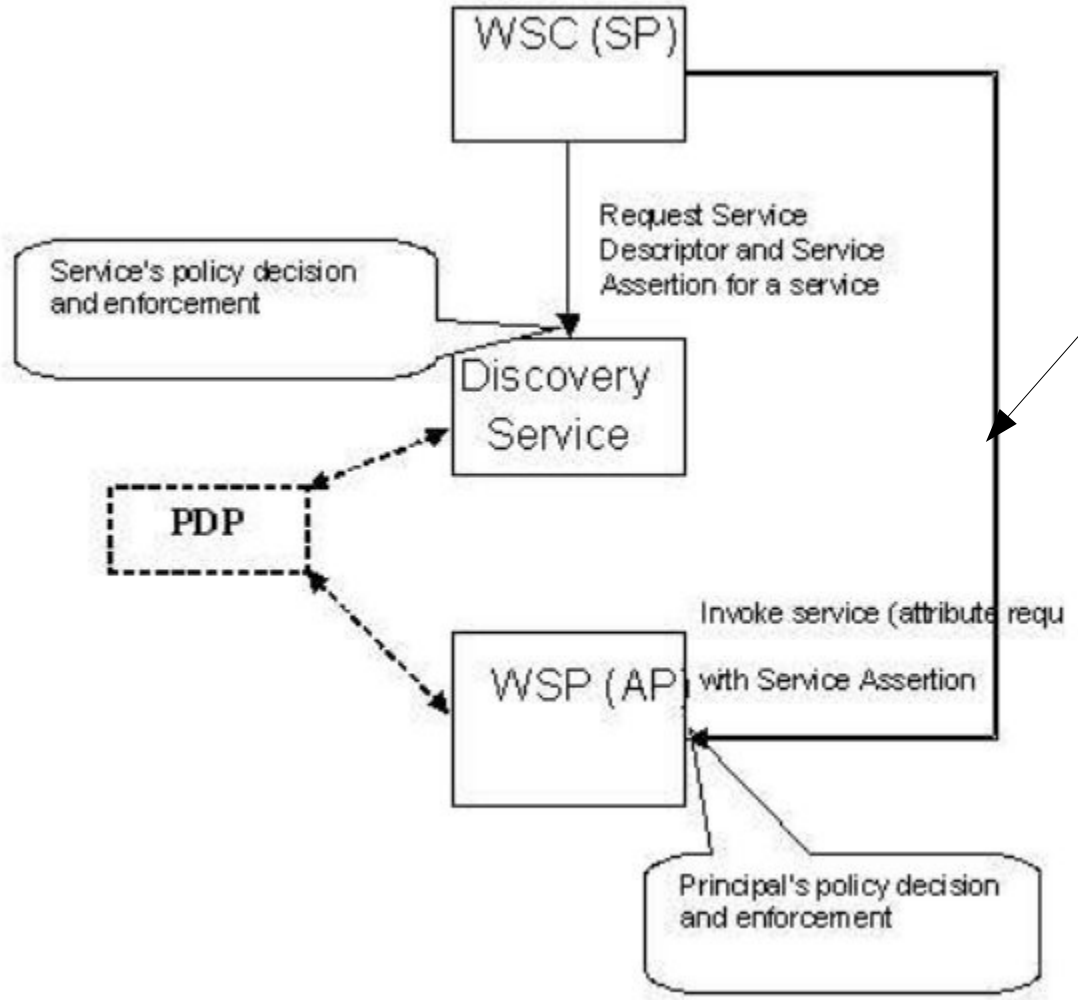
What's about after authentication



How to retrieve attributes bypassing the authentication authority



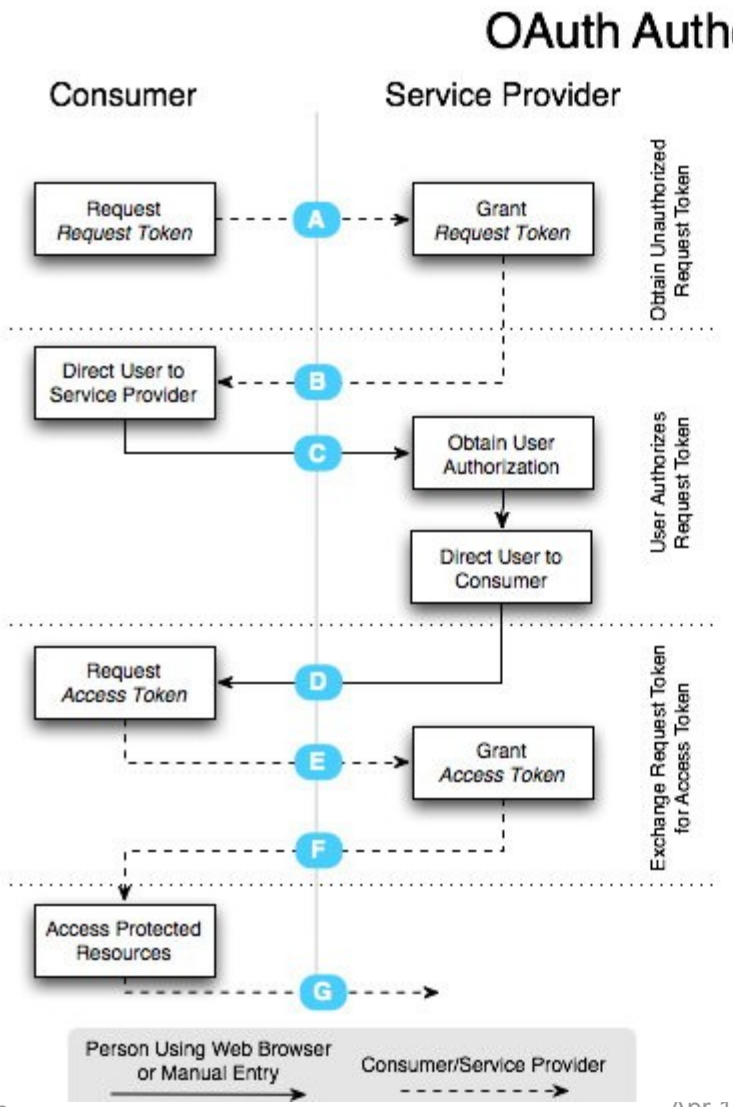
Attributes Exchange (ID-WSF)



Informations provided to invoke the attribute provider

- EndPoint (where is the service)
- NameID (define target user within the service)
- Security Token (authority vision on the transaction)

oAuth (web authentication token)



A Consumer Requests *Request Token*

Request includes
oauth_consumer_key,
oauth_signature_method,
oauth_signature,
oauth_timestamp,
oauth_nonce,
oauth_version (optional).

B Service Provider Grants *Request Token*

Response includes
oauth_token,
oauth_token_secret.

C Consumer Directs User to Service Provider

Request includes
oauth_token (optional),
oauth_callback (optional).

D Service Provider Directs User to Consumer

Request includes
oauth_token (optional).

E Consumer Requests *Access Token*

Request includes
oauth_consumer_key,
oauth_token,
oauth_signature_method,
oauth_signature,
oauth_timestamp,
oauth_nonce,
oauth_version (optional).

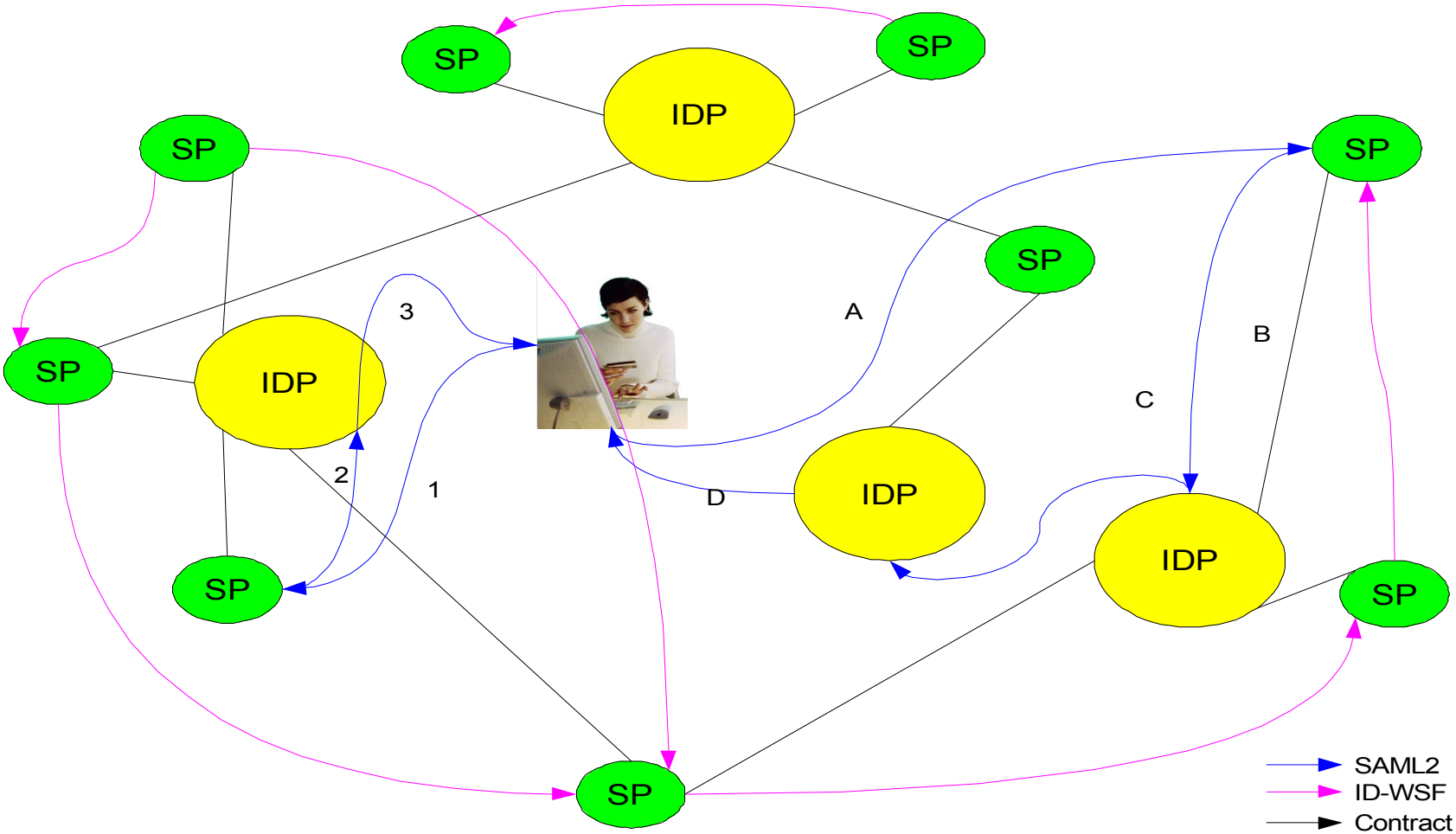
F Service Provider Grants *Access Token*

Response includes
oauth_token,
oauth_token_secret.

G Consumer Accesses Protected Resources

Request includes
oauth_consumer_key,
oauth_token,
oauth_signature_method,
oauth_signature,
oauth_timestamp,
oauth_nonce,
oauth_version (optional).

Web-2.0 Federated Architecture



My 0.1€ predictions

- Authentication
  - SAML2 enterprise, governments, telcos, ...
  - Open-ID2 for blogs, photos sharing services, ...
  - Inforcard for password less authentication GUI
- Attributes exchanges
  - Authentication attributes will continue to be the most common practice
  - ID-WSF2 in government or where ever privacy is enforce by regulation.
  - Oauth for cheap services (with OpenID).
- Convergence
  - Protocol will1st be bridged (ex: ID-WSF on REST, IDP supporting SAML2 & OpenID, ...)

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

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