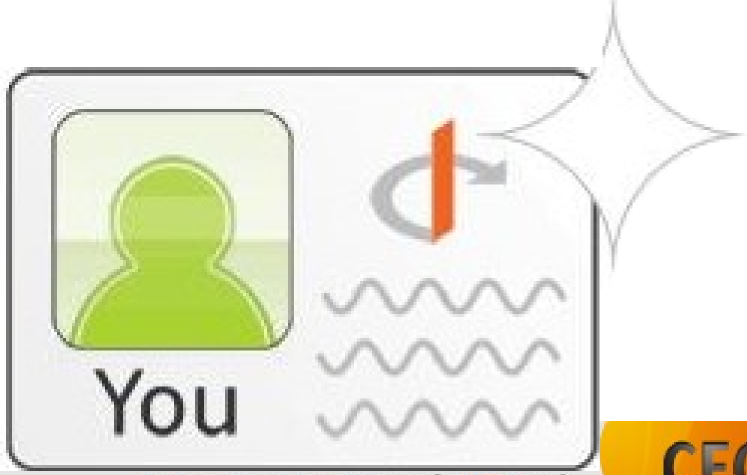
Understanding Identity Jungle

Fulup Ar Foll
Liberty Technical Expert Group

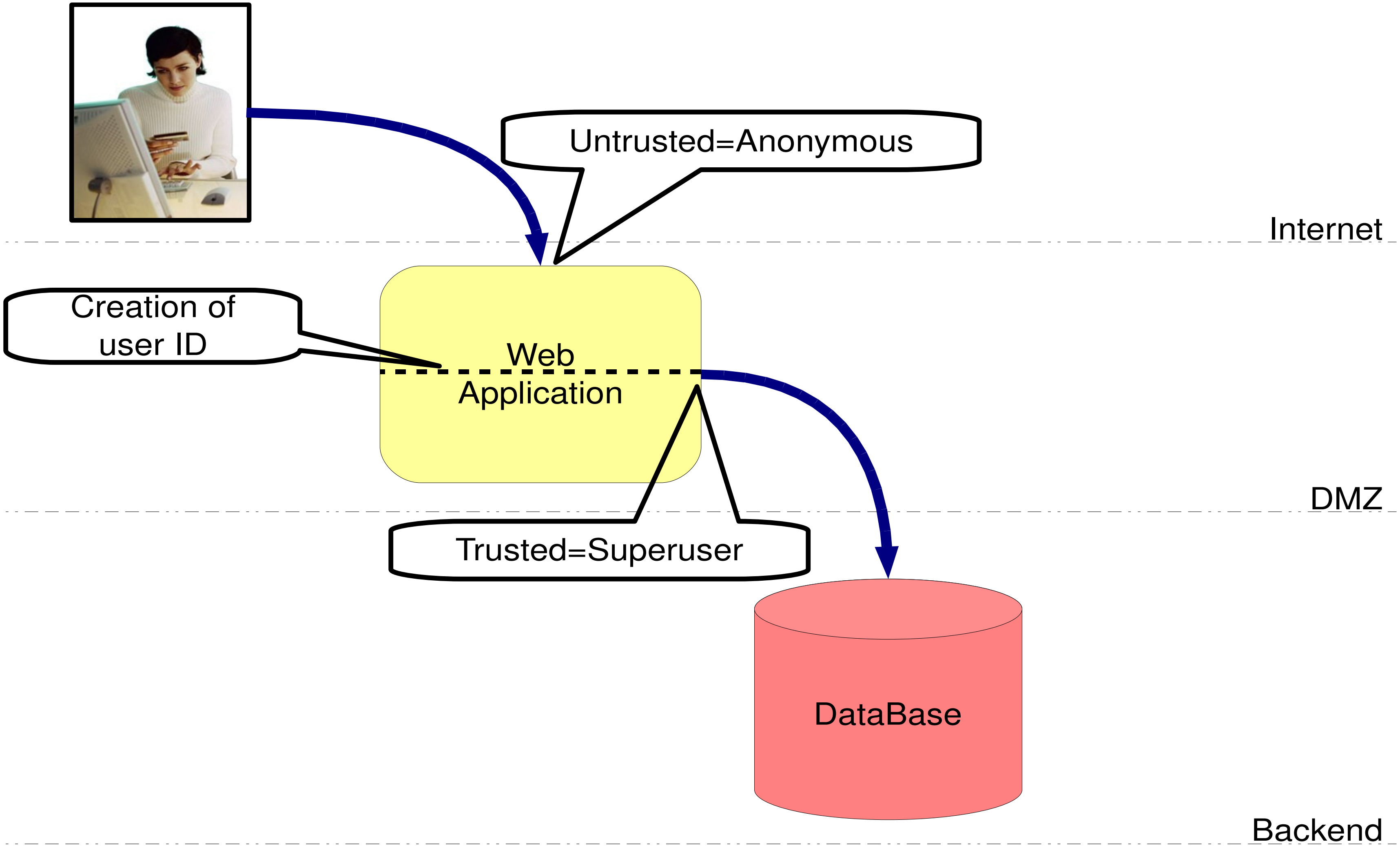
Master Architect, Global Software Practice
Sun Microsystems

What's a digital identity ?

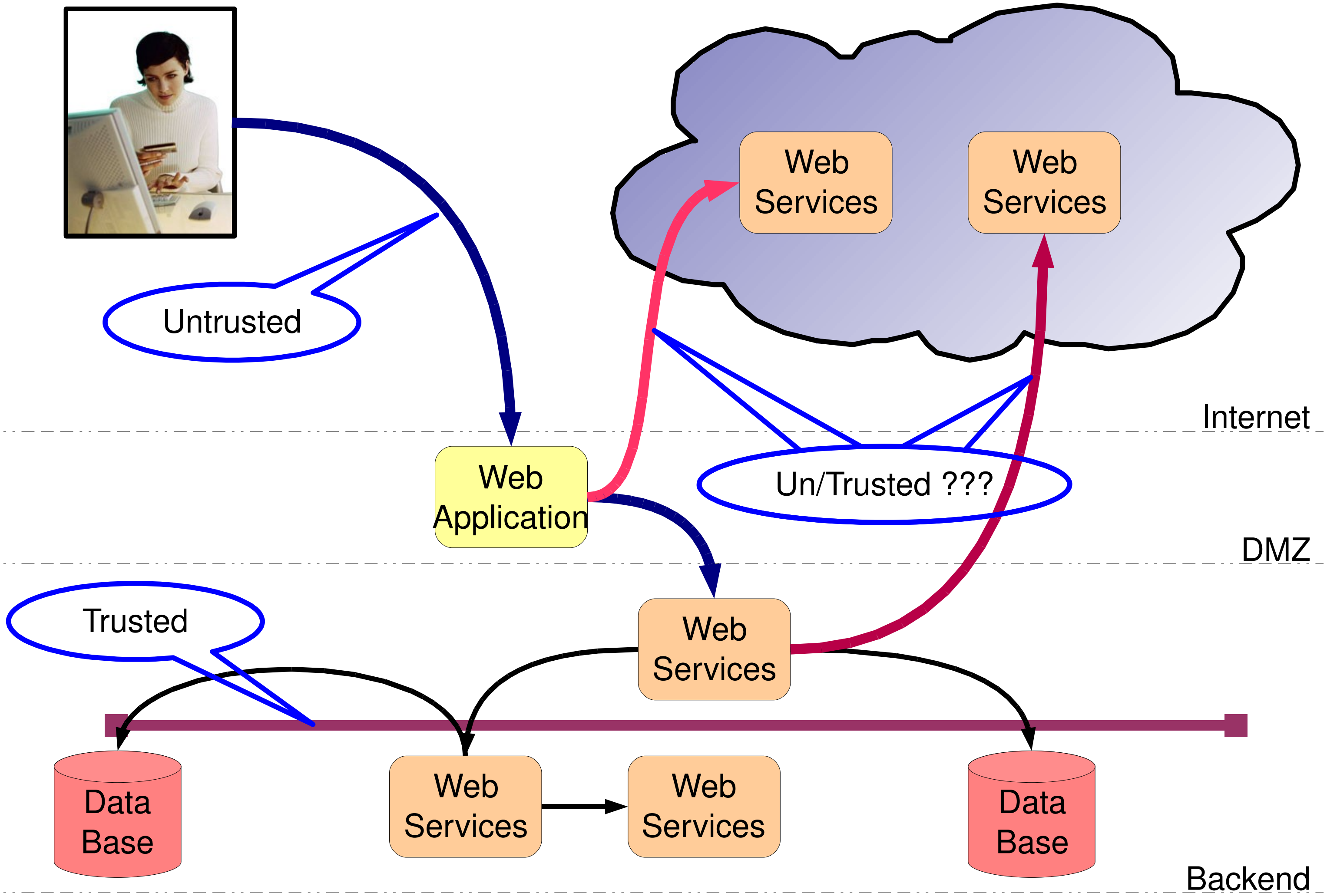
- **Authentication**: *proof you're the one you claim to be*
  - Biometric: picture, fingerprint, voice, ...
  - Secret: login/passwd, certificate, pin code, ...
- **Attributes**: *define what you are*
  - Authorization attributes: allow to drive a motorbike
  - Personalization attributes: preferred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



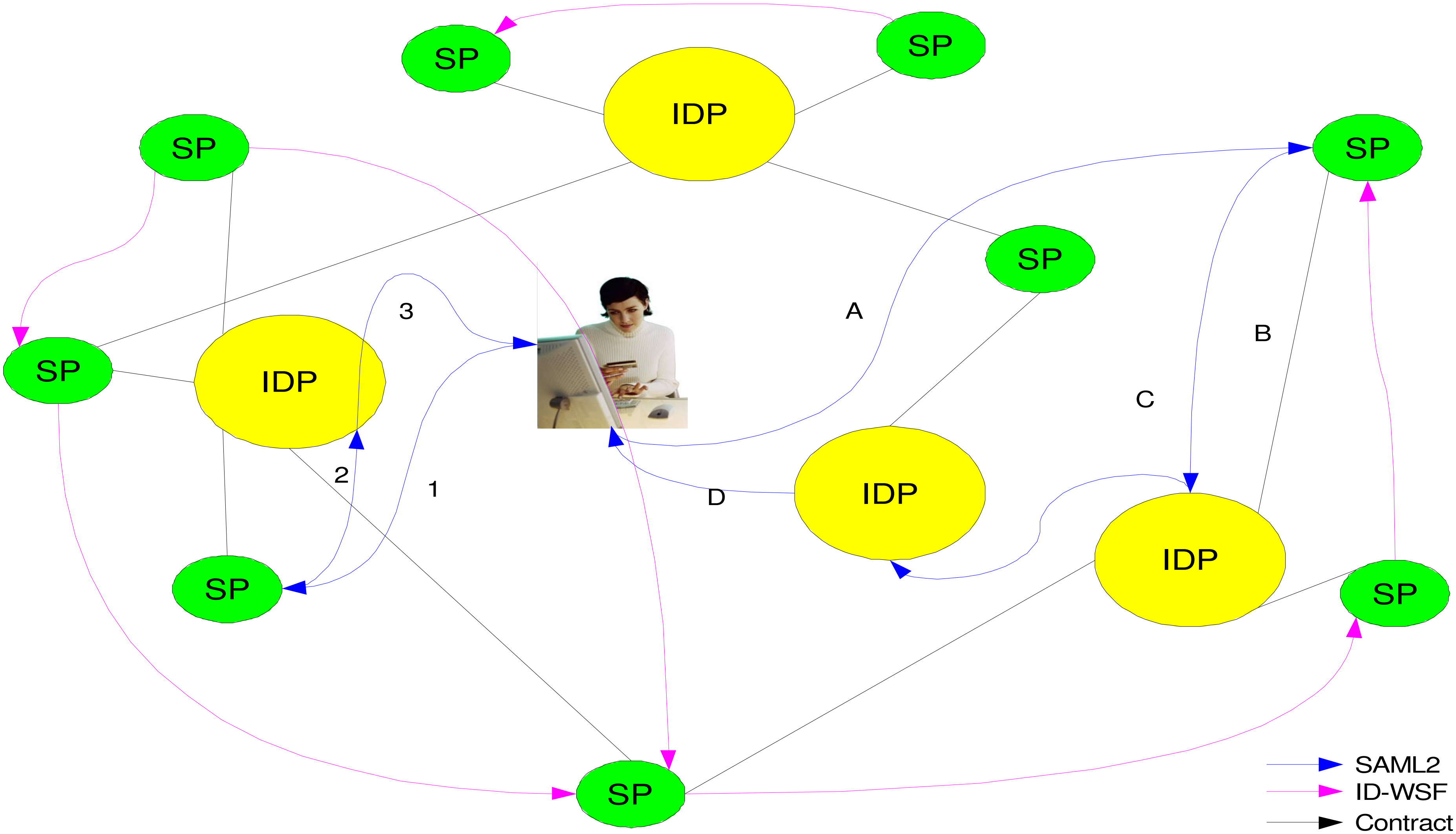
Cold war generated simple security model



Web2.0 security architecture is a mess :(

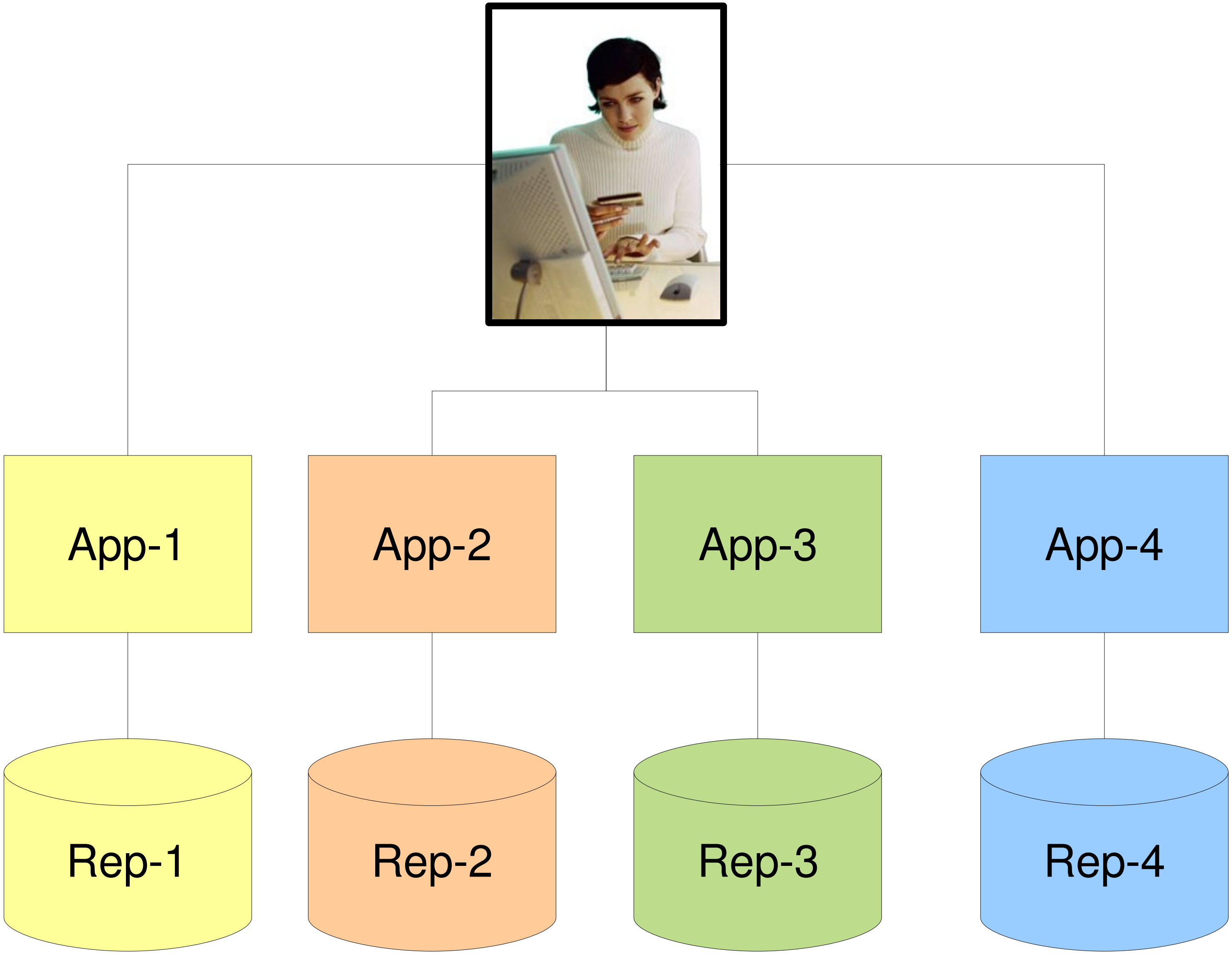


Web-2.0 Federated Architecture even better



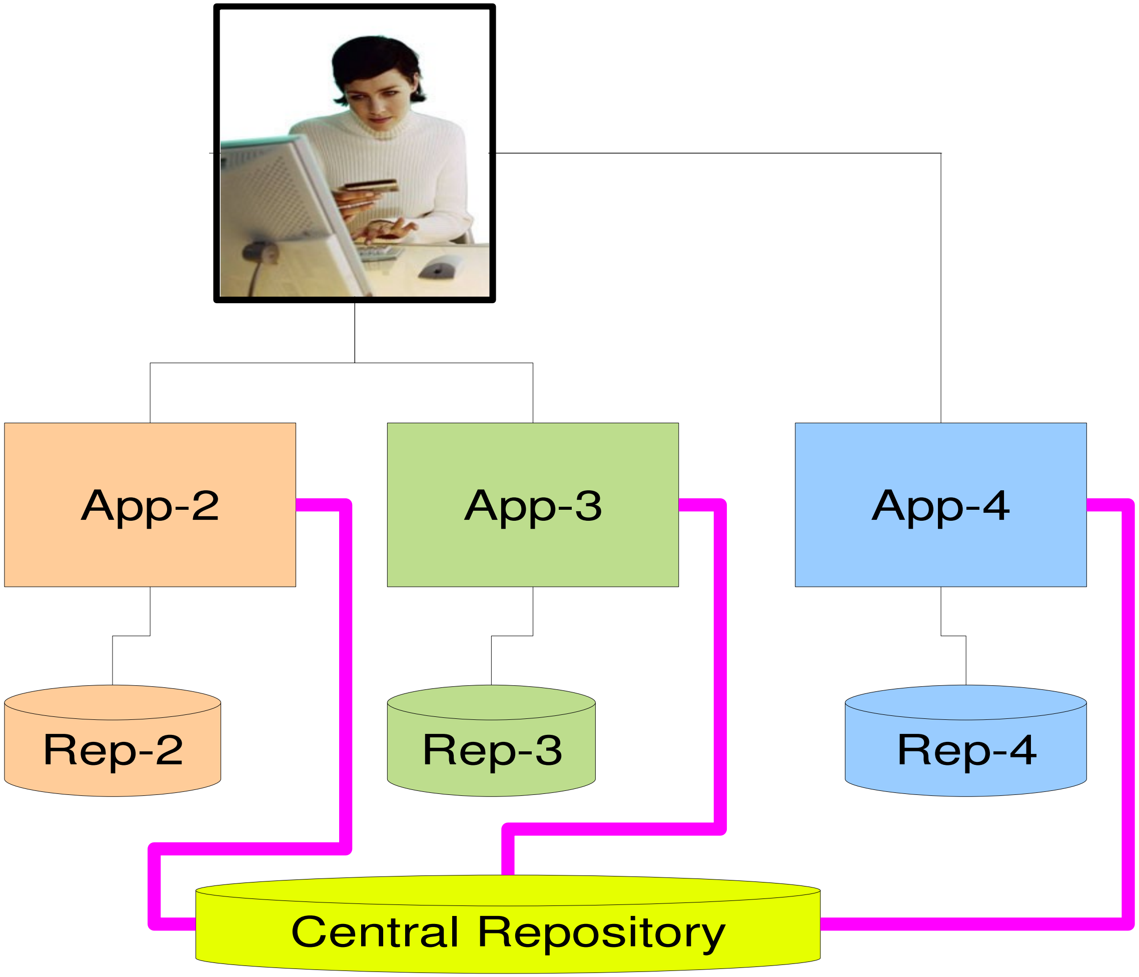
Identity Legacy

(let's built my own flavor)



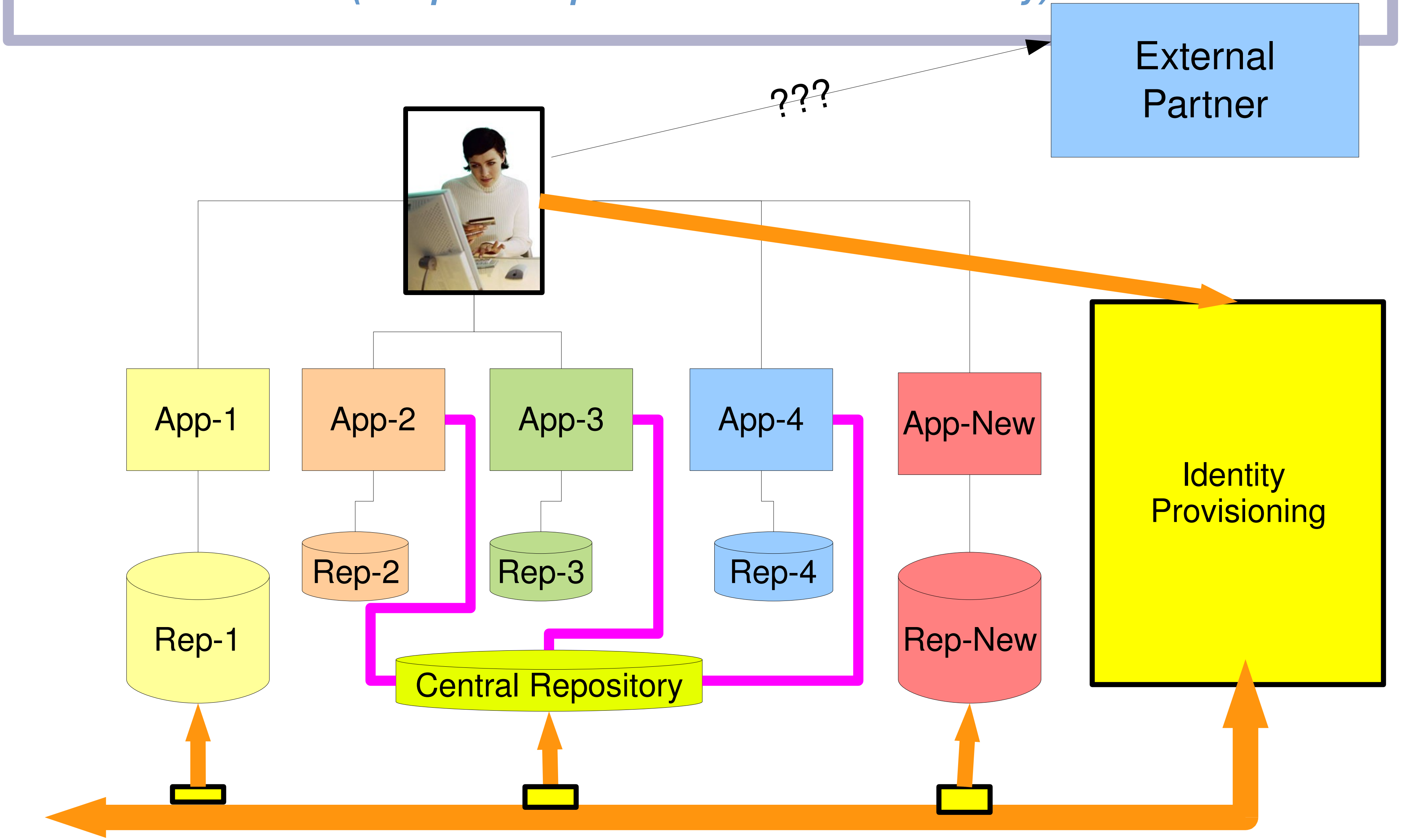
Unique Central repository

(almost unique)



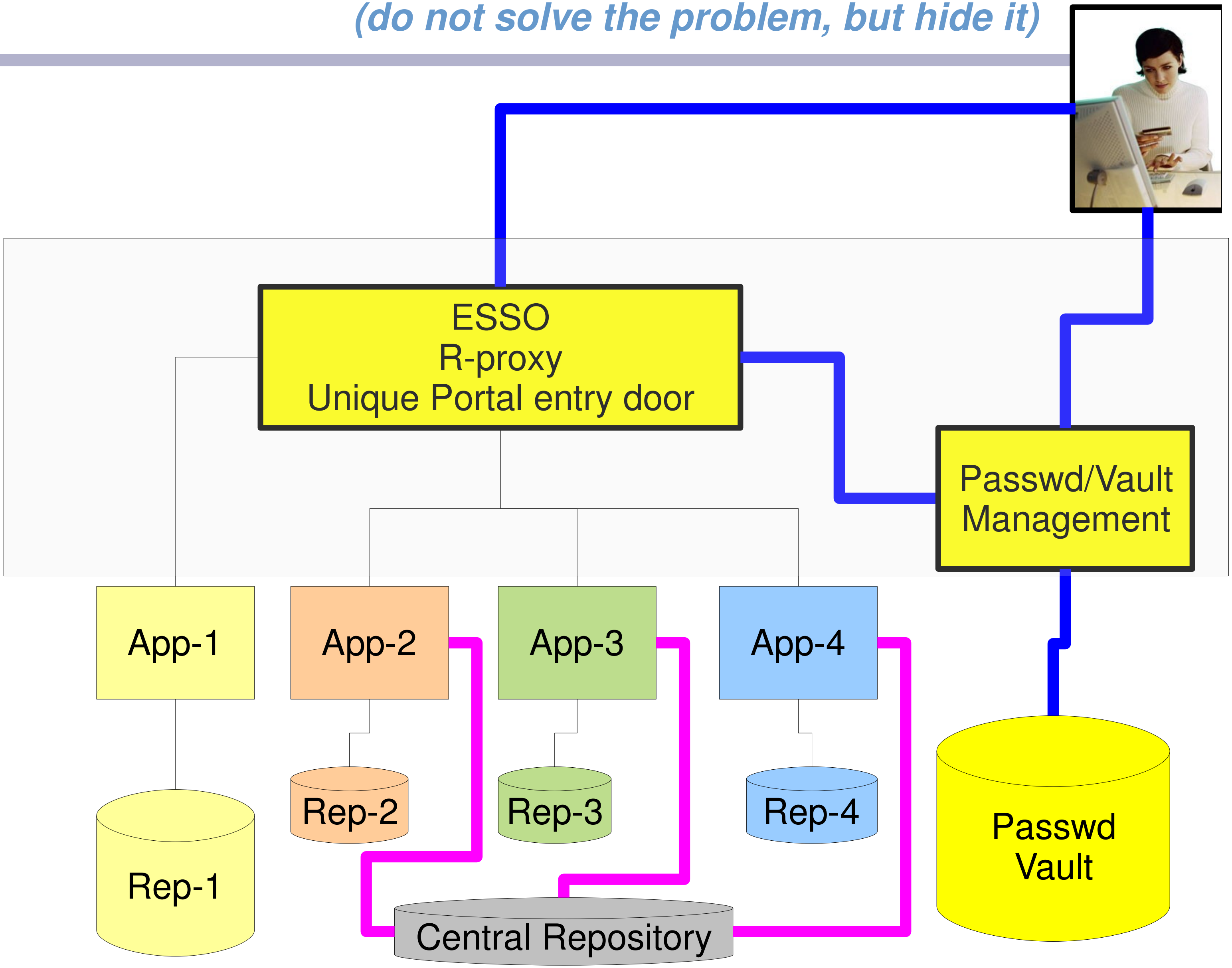
Identity Full Provisioning

(Unique ID & pre-creation of ID necessary)



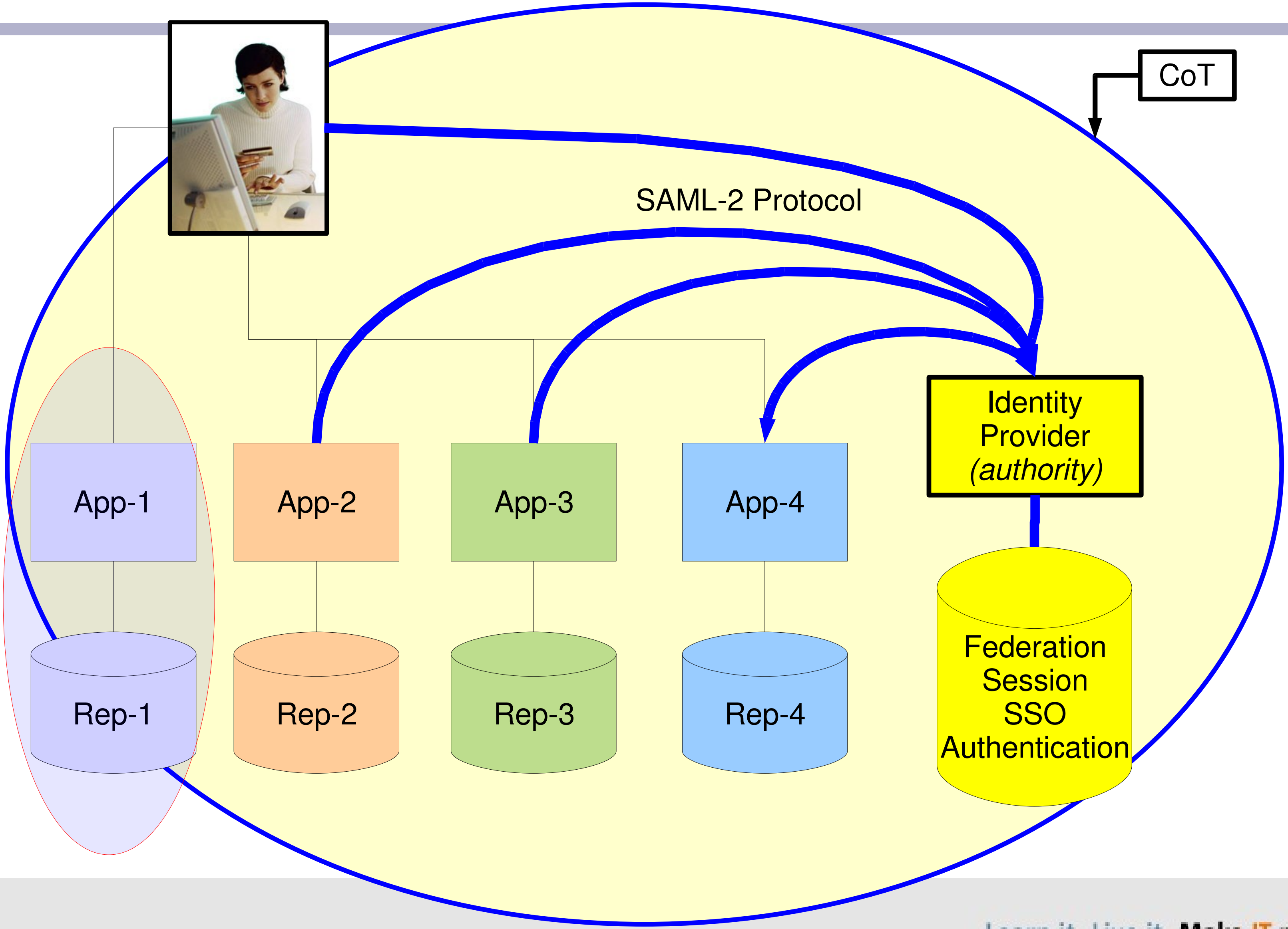
Portal centric, eSSO, rProxy,

(do not solve the problem, but hide it)



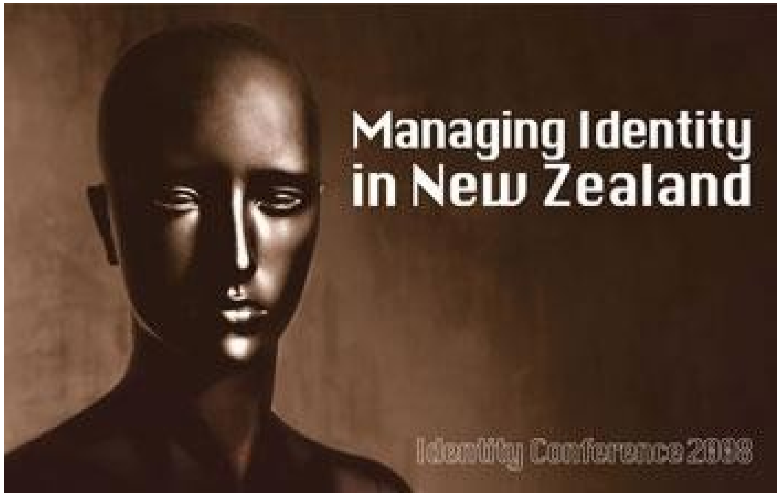
Federation [Liberty-SAML2]

(no unique-ID, Lazy provisioning, Roaming)


CoT
SAML-2 Protocol
Identity Provider *(authority)*
App-1
App-2
App-3
App-4
Rep-1
Rep-2
Rep-3
Rep-4
Federation Session SSO Authentication

Architecture Requirements

- **Internet-Centric**
  - Cheap, fast moving (no special network, like it or trash it, ...)
  - Based on current Internet “day to day” user experience
  - No difference between customers, citizens, employees, parterns,...)
  - Peer-to-Peer (scalable, efficient, data directly from source, ...)
  - Distributed (multiple authority, discovery, flexible, ...)
  - No central system, no “Big Brother”
- **User-Centric**
  - User in control of his global identity
  - Multiple personalities
  - Consent aware
  - Strong privacy & security
  - Simple & intuitive



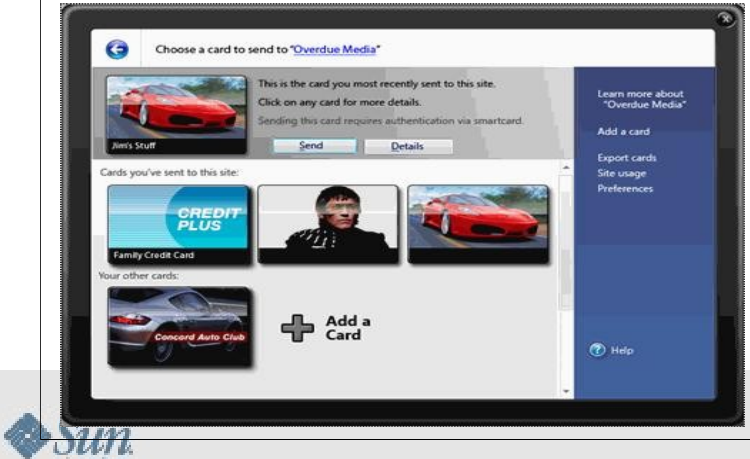
How much user centric ?

- **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

TCP/IP Brain interface

Cardspace / ID selectors



Choose a card to send to "Overdue Media"

This is the card you most recently sent to this site.

Click on any card for more details.

Sending this card requires authentication via smartcard.

Cards you've sent to this site:

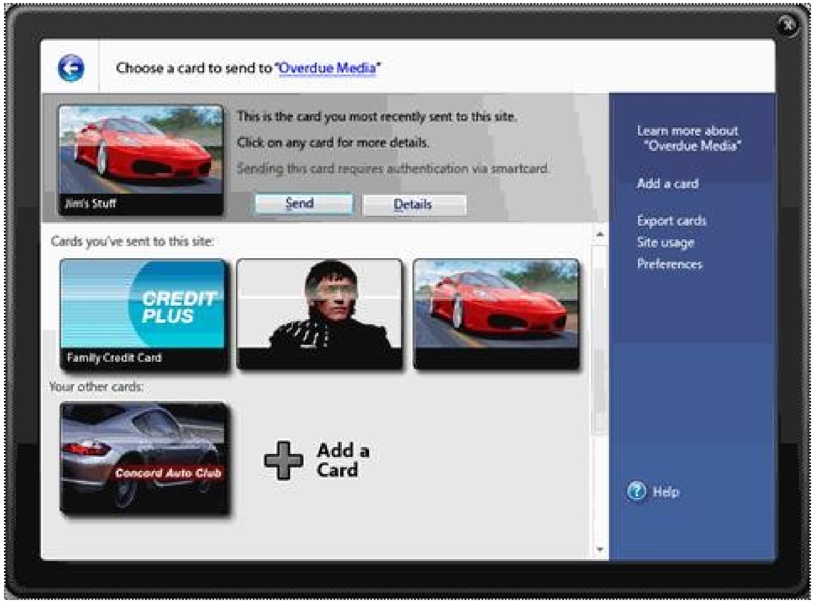
Your other cards:

OpenID [simple but limited]

- **Good**
  - Easy to implement (simple protocol)
  - Universal (no contact needed)
- **Bad**
  - User experience (need to understand URI)
  - Limited to social web (blog, photo-sharing, ...)
  - http://developer.yahoo.com/openid/bestpractices.html
- **To be proven**
  - Security model (better in 2.0, but also much more complex)
  - Business model (OpenID as an self asserted ID as limited value for commercial service providers)

Card-space / Identity Selector

- **Good**
  - Nice user interaction
  - Easy concept to explain
  - Good anti-phishing authentication
- **Bad**
  - Does not really handle privacy
  - Pushed security/privacy to the user
  - Commercial impact of removed authentication dance from IDP.
- **To be proven**
  - When do we need user to self select an ID ?
  - No server for signed ID available



Choose a card to send to "Overdue Media"

This is the card you most recently sent to this site.

Click on any card for more details.

Sending this card requires authentication via smartcard.

Cards you've sent to this site:

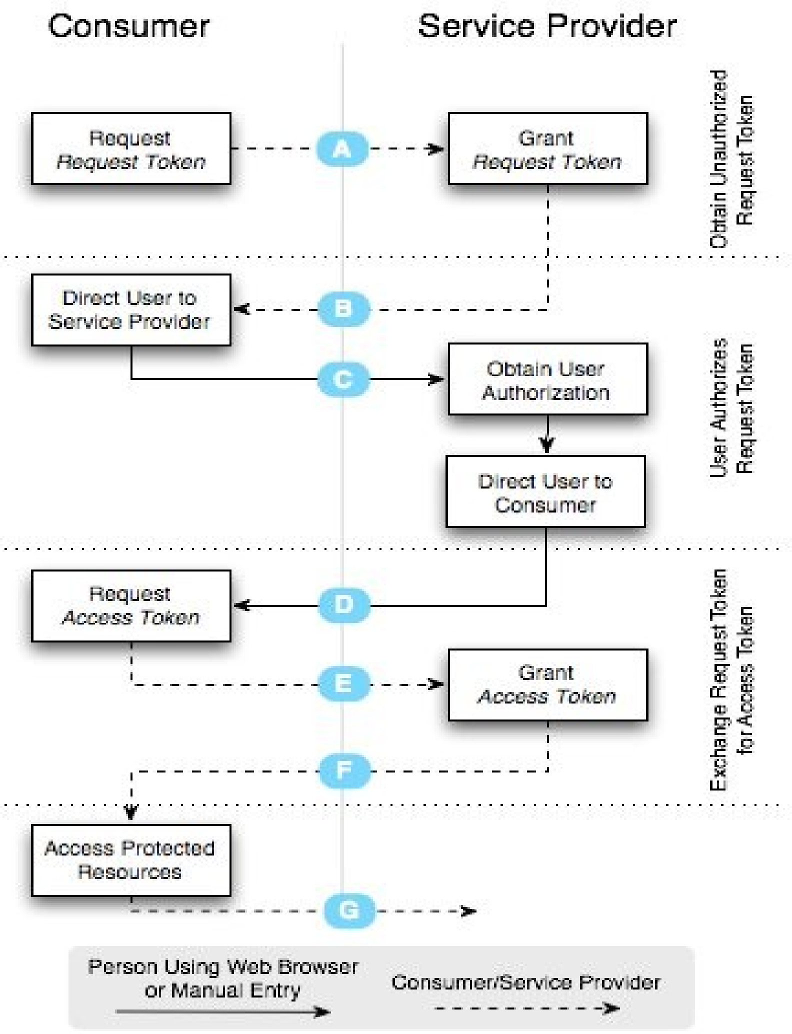
Your other cards:

Liberty/SAML2

- **Good**
  - User experience
  - Privacy built in
  - Rich protocol adapted to mobile, government,banks, ...
- **Bad**
  - Need to convince partners one per one
- **To be proven**
  - SOAP/XML versus REST ?
  - Large scale interoperability (ex: country to country)
  - Capacity to integrate with other world (ex: SIP, SMTP, ...)

oAuth *(yet an other one !!!)*

- Protocol for delegated authorization, not another authentication protocol.
- Attempts to provide a standard way for developers to offer their services via an API without forcing users to expose credentials.
- Not bind to a specific authentication protocol, it can be used with any (SAML2, OpenID, Google, ..etc.)
- Doesn't enforce Service Provider and API provider to share the same Identity provider.


Consumer
Service Provider
Request Request Token
A
Grant Request Token
Obtain Unauthorized Request Token
Direct User to Service Provider
B
C
Obtain User Authorization
Direct User to Consumer
User Authorizes Request Token
Request Access Token
D
E
Grant Access Token
F
Exchange Request Token for Access Token
Access Protected Resources
G
Person Using Web Browser or Manual Entry
Consumer/Service Provider

One less: WS-FED

SAML 2.0 Protocol Support in “Geneva” Server. As Don Schmidt wrote this morning, Microsoft’s “Geneva” Identity Server product will support the SAML 2.0 protocol. Specifically, we will be supporting the SAML 2.0 IdP Lite and SP Lite profiles and the US Government GSA profile.

Customers had told us that these SAML profiles are important to them and we’re responding to that feedback by implementing them in “Geneva” Server. Those of you who were at Kim Cameron’s “Identity Roadmap for Software + Services” presentation at the PDC got to see Vittorio Bertocci demonstrate SAML federation with “Geneva” Server to a site running IBM’s Tivoli Federated Identity Manager.

http://www.kuppingercole.com/articles/fg_micro_gen_271008

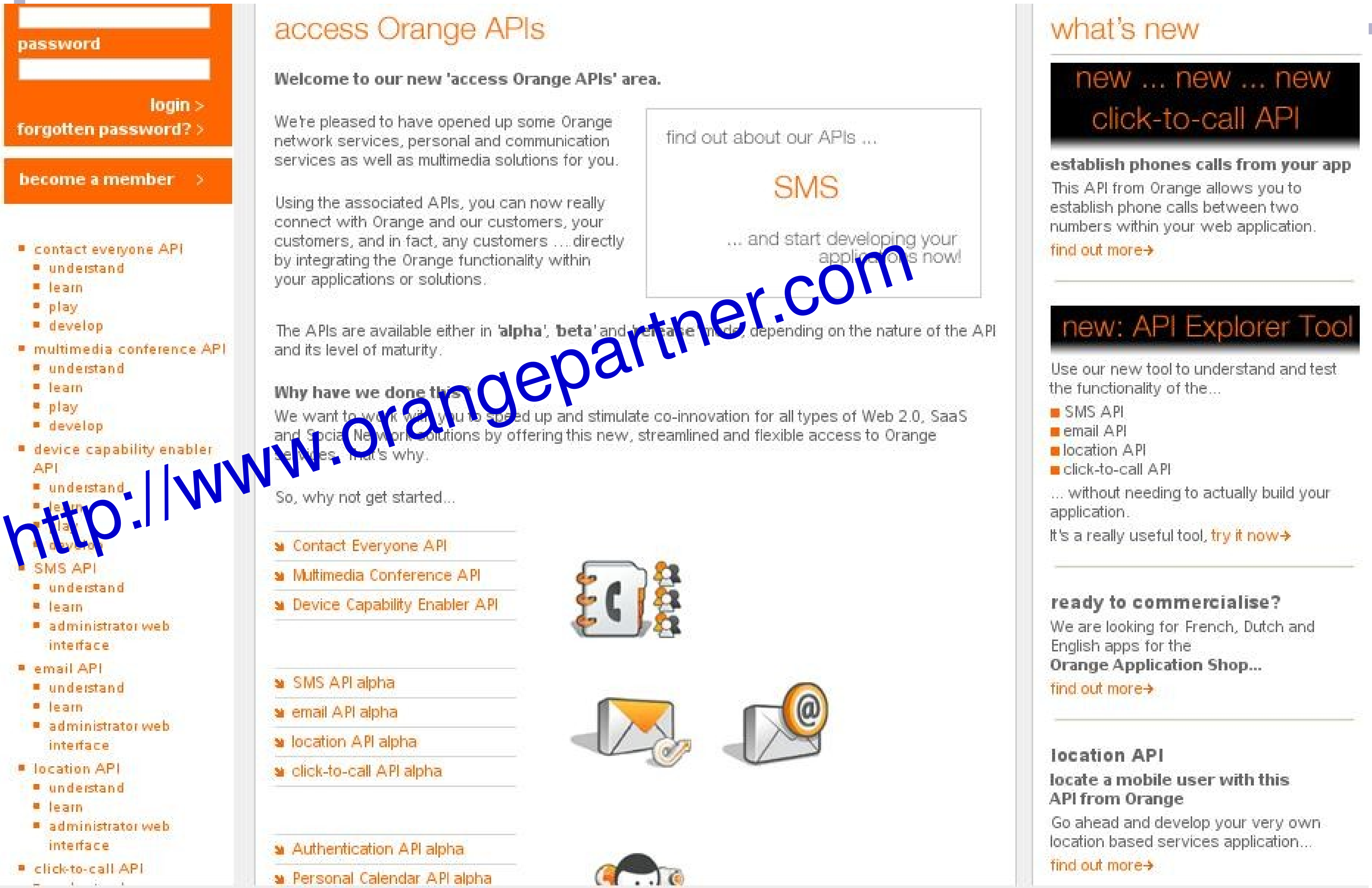
User centric technical requirements

- Privacy and Security as a 1st class citizen
  - Identity information requests access-controlled
  - Minimal disclosure of identity information
  - Protection against disclosure of identifiers
  - User consent when needed.
- Flexible foundation for applications
  - Across security domains and computing platforms
  - Across location, allowing for service location flexibility
- Standards-based Federated identity enable web services
  - Ecosystems of services that expose interfaces on behalf of individual users' identities

Let's predict the future :)

- SAML2 won for eGovt, Telcos, Banks. IAF (Identity Assurance Framework) enable architecture will become the reference.
- OpenID/oAUTH as non SOAP protocol will continue to develop, for social, blogs and low security consumer services.
- ID-WSF2 (Identity enable Web Service) is best placed to win, but mostly in its simplified form *(as proposed by Danish government)* and by opening to WStrust token service, and other binding (oAuth/Rest).
- Some form of card selection and IDP discovery should come, but its to early to predict how/when. Card could also be extended to handle consent management, but IDP selection is the most urgent issue.
- IDP will act as authentication gateway for multiple protocols, mostly to enable alien user to activate services.

Identity-2.0 winder of the day



password

login >

forgotten password? >

become a member >

- contact everyone API
  - understand
  - learn
  - play
  - develop
- multimedia conference API
  - understand
  - learn
  - play
  - develop
- device capability enabler API
  - understand
  - learn
  - play
  - develop
- SMS API
  - understand
  - learn
  - administrator web interface
- email API
  - understand
  - learn
  - administrator web interface
- location API
  - understand
  - learn
  - administrator web interface
- click-to-call API

access Orange APIs

Welcome to our new 'access Orange APIs' area.

We're pleased to have opened up some Orange network services, personal and communication services as well as multimedia solutions for you.

Using the associated APIs, you can now really connect with Orange and our customers, your customers, and in fact, any customers ....directly by integrating the Orange functionality within your applications or solutions.

find out about our APIs ...

SMS

... and start developing your applications now!

The APIs are available either in **'alpha'**, **'beta'** and **'release'** mode, depending on the nature of the API and its level of maturity.

Why have we done this?

We want to work with you to speed up and stimulate co-innovation for all types of Web 2.0, SaaS and Social Network solutions by offering this new, streamlined and flexible access to Orange services. That's why.

So, why not get started...

- Contact Everyone API
- Multimedia Conference API
- Device Capability Enabler API

- SMS API alpha
- email API alpha
- location API alpha
- click-to-call API alpha

- Authentication API alpha
- Personal Calendar API alpha

what's new

new ... new ... new click-to-call API

establish phones calls from your app

This API from Orange allows you to establish phone calls between two numbers within your web application.

find out more→

new: API Explorer Tool

Use our new tool to understand and test the functionality of the...

- SMS API
- email API
- location API
- click-to-call API

... without needing to actually build your application.

It's a really useful tool, try it now→

ready to commercialise?

We are looking for French, Dutch and English apps for the **Orange Application Shop...**

find out more→

location API

locate a mobile user with this API from Orange

Go ahead and develop your very own location based services application...

find out more→

http://www.orangepartner.com

Europe versus North America

Same requirement

Different Implementation

Thank you

CEC 2008

Learn it. Live it.
Make IT real.

Fulup@sun.com
http://www.fridu.org/fulup

November 9-14, 2008 Las Vegas, NV