



# Attributes Centric Architecture

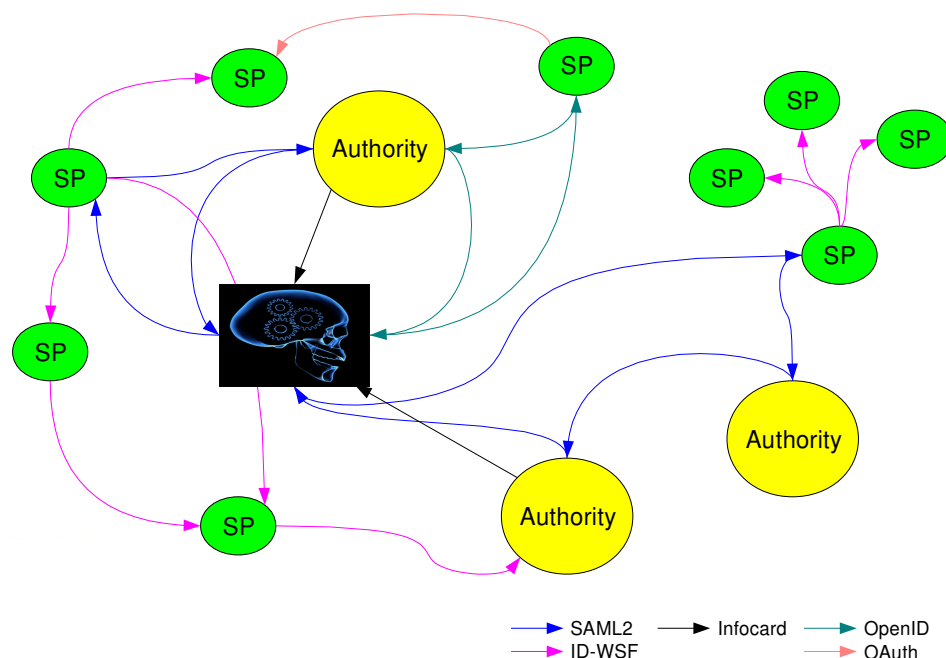
Fulup Ar Foll  
Chief Technology Officer  
Global Software Practice  
[fulup@sun.com](mailto:fulup@sun.com)



**SHIFT**—OUR UNIVERSE. OUR WORLD. YOUR MOVE.

# Authent. protocols armistice

- SAML2: business related services
- OpenID: web2.0 and free services
- InfoCard: user interface, identity selection




**IDManagement.gov**

**Quick Click:**

**Local IDManagement.gov Links:**

- Accessibility Policy
- Calendar
- Contact Us
- Home
- Library
- Links Policy
- Login with your HSPD-12 PIV card
- News
- Open ID Solutions for Open Gov't
- Plug-In Policy
- Privacy Policy
- Sitemap

**Related Federal Government Sites:**

- ECA PKI Program
- Federal PKI Architecture
- Federal PKI Policy Authority
- FIPS 201 Evaluation Program

**Open Identity Solutions for Open Government**

The Open Identity Initiative seeks to leverage existing industry credentials for Federal use. The Initiative approves credentials for government use through our Trust Framework Providers who assess industry Identity Providers (IDPs).

The Trust Framework Provider Adoption Process outlines the process that the ICAM community uses to sanctify organizations that assess commercial identity providers.

**Trust Framework Providers:**

- Open Identity Exchange - Provisional Approval
- Kantara Initiative - Provisional Approval
- InCommon Federation - Draft submission under review

The Scheme Adoption Process outlines the process that the ICAM community uses to develop and/or approve specification profiles for achieving portable identity over the Internet.

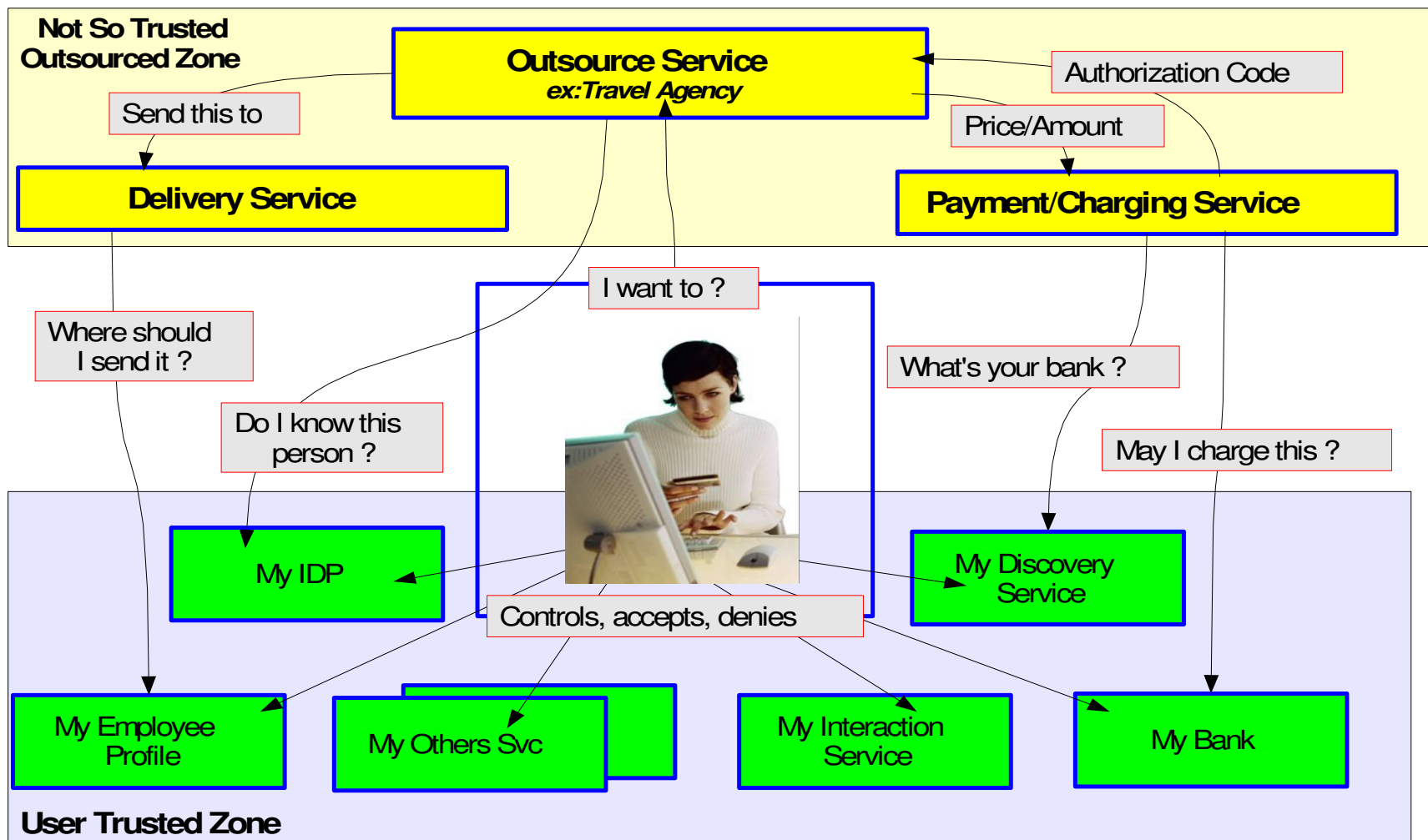
**Adopted Schemes:**

- ICAM OpenID 2.0 Profile - Fully adopted
- Kantara SAML 2.0 eGovernment Profile - Fully adopted
- ICAM IMI 1.0 Profile - Fully adopted
- ICAM WS-Federation - In development

**Identity Providers:**

- Google - OpenID Foundation, Pilot assessment with NIH in progress
- Yahoo - OpenID Foundation, Pilot assessment in progress
- PayPal - OpenID Foundation, InfoCard Foundation, Pilot assessment in progress
- Equifax - InfoCard Foundation
- VeriSign - OpenID Foundation
- Wave

# What about after authentication



# Authentication is not the end goal

- Authentication is only the entry door to your house.
- Authentication enables identity aware applications, but does not provide any added value.
- Authentication is a nothing more than a “*must have feature*” that does not interest end-users.




# Attributes define you

- what you are, what you can do, where you can go.
- Attributes enable personal APIs

## Personal APIs

available for web, mobile web, desktop and mobile applications



## Orange Partner


The Personal APIs consist in a suite of service proposed through APIs that allow you to enable Orange France customers to access their calendar, contacts, messaging, photo and profile information via your website.

Personal APIs also include Payline API for payment, open to all users.

The APIs include...

- Authentication API
- Personal Calendar API
- Personal Contacts API
- Personal Content API
- Personal Favourites API
- Personal Messages API
- Personal Photos API
- Personal Profile API
- Personal RichProfile API \* new \*
- Payline API \* new \*

Use the APIs to develop and enhance your web application.



news and updates

- Personal APIs now available for mobile browsing and mobile applications...












[contact us](#) for more information

Currently, some of the Personal APIs are in beta mode. This means that they're FREE to use with some service limitations (as you would expect). It also means that they're in the early stages of development. We need your feedback!

## API Directory

The following Google services provide APIs that imple

Each API has its own set of guides and resources, incl Developer's Guide for that API should point you in the r

| API Home  |   |
|---|---|
|    | <a href="#">Google Analytics Data Export API</a>  |
|    | <a href="#">Google Apps APIs</a>                  |
|    | <a href="#">Google Base Data API</a>              |
|    | <a href="#">Blogger Data API</a>                  |
|    | <a href="#">Google Booksearch Data API</a>        |
|  | <a href="#">Google Calendar Data API</a>          |
|  | <a href="#">Google Code Search Data API</a>       |
|  | <a href="#">Google Contacts Data API</a>          |
|  | <a href="#">Google Documents List Data API</a>    |
|  | <a href="#">Google Finance Portfolio Data API</a> |
|  | <a href="#">Google Health Data API</a>            |

# Architecture requirements

- Authentication (who are you?)
  - Only a technical MUST HAVE feature
- Attributes (what you are)
  - The real value of identity
- Proof of validity (trustful?)
  - Source of the ID and/or Reputation
  - Assurance framework
- Privacy as a first class citizen
  - Isolation of partial user ID in federated silos
  - Contracts to enable delegation of trust
  - Minimal disclosure, minimal creation of information

# Current situation

- Every service creates its own copy of your personal attributes.
- Still in a very centralized approach, including the ones that pretend themselves open & distributed.
- I'm the center of the world. I control 100% of your identity. Others can use it, if they agree to my conditions.
- Assumption is that user attributes must be attached to the principal of the Identity.

# Where should we go

- Move from copy attributes to retrieve/cache on demand from authoritative source.
- Define & normalize an assurance framework for attributes.
- Move away from fixed location to a by-user discovery model.
- Define meta-data (in-band/out-of-band) to help receivers to apply the right policy on usage/storage/dissemination.



# Advantages [attribute centric model]

- No more gigantic provisioning work-flow.
- Cheaper and more reliable data.
- Better privacy.
- Scale to Internet/Cloud level.

# Constraints [attributes centric model]

- Delegation of trust (*not controlled by me*).
- Performances in some specific cases.
- What about off-line transactions?
- Negotiation of mesh contracts (meta-data for relying parties).

# Existing technologies

- Protocols
  - OAuth
  - ID-WSF
  - XACML
- Assurance framework
  - Kantara
    - ISWG (*Information Sharing Working Group*)
    - UMA (*User Managed Access*)
  - OpenLiberty ArisID

*Fulup@sun.com*



- <http://www.fridu.org/fulup>
- <http://kantarainitiative.org>
- <http://www.openliberty.org> (project aristotle)
- <http://www.oracle.com>

**SHIFT**—OUR UNIVERSE. OUR WORLD. YOUR MOVE.

