

# New Generation of Liberty Federated Architecture for Enterprise

Fulup Ar Foll, Sun Microsystems  
[fulup@sun.com](mailto:fulup@sun.com)



# 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

# Next Generation Design Goal

- User Centric, nothing without my consent
- Information collected, maintained once by the most appropriate source.
- Information verified to the adequate level.
- Information available electronically through a vendor neutral long-term standard.
- Information exchange securely to whomever requires it, in a privacy-aware manner.
- Significant benefit for people, businesses, government, enterprises, ...

# Which standard for what

## •Global Connectivity

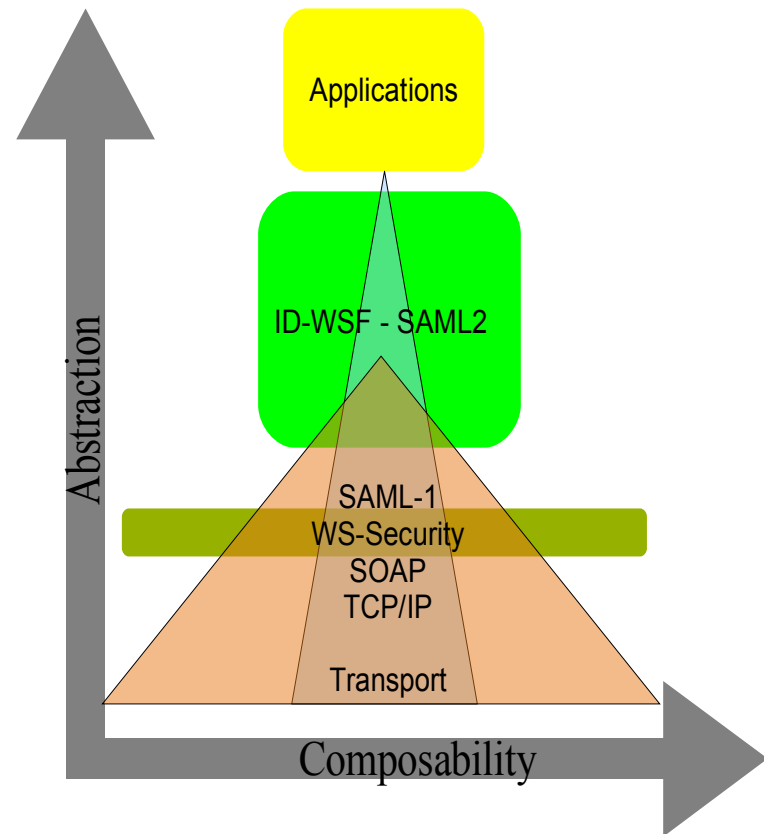
- Across repository, domain, ...
- Seamless to User (complexity advert)
- Want to be both consumer and provider

## •Increasing Demand for ID

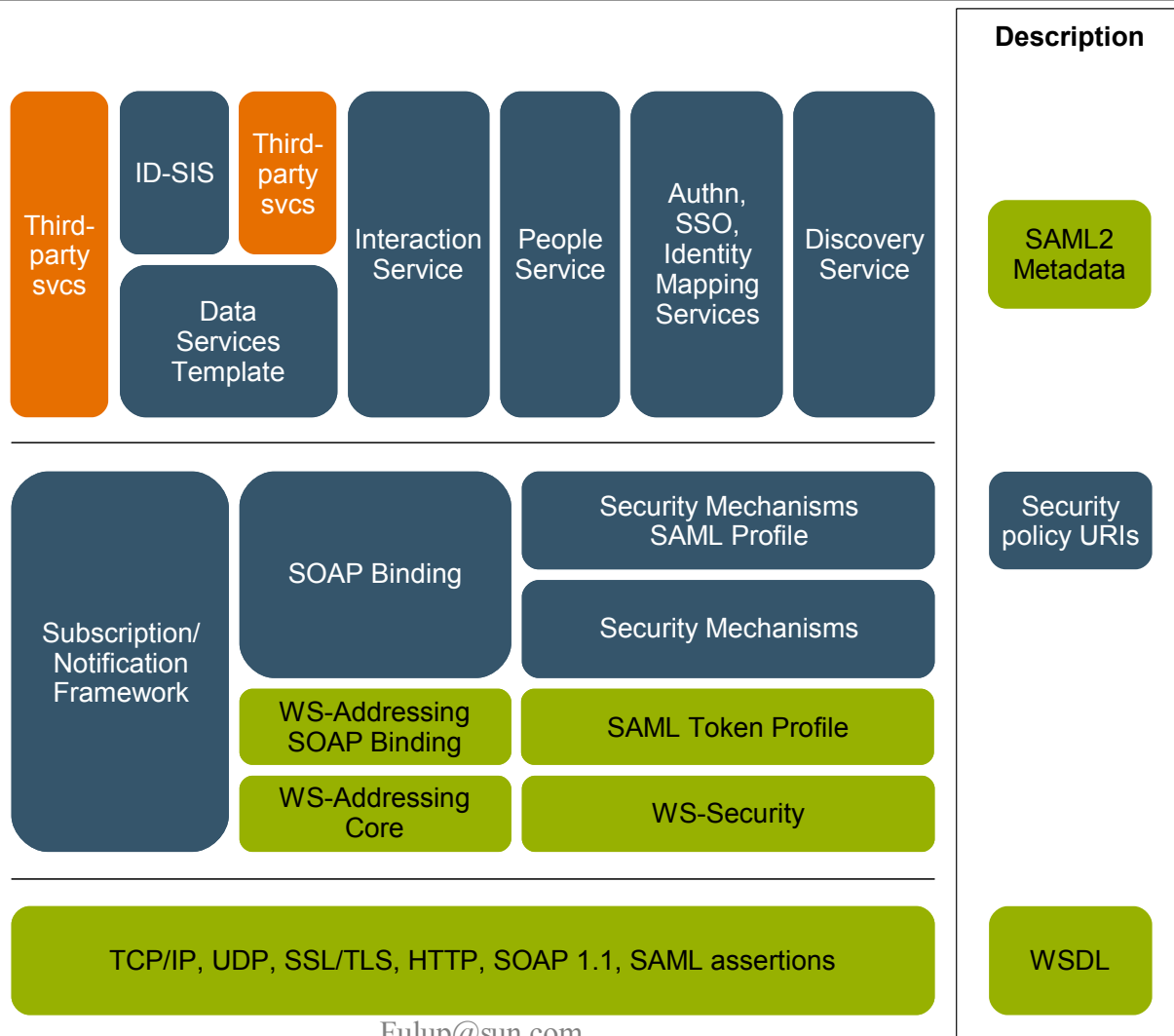
- Everyone wants your identity but do you want it?
- Need adequate privacy mechanisms before exposing it.

## •Heterogeneous world

- Multi vendors, services providers and consumers are heterogeneous.
- Multi-channel, cross devices, cross networks, ...
- ...

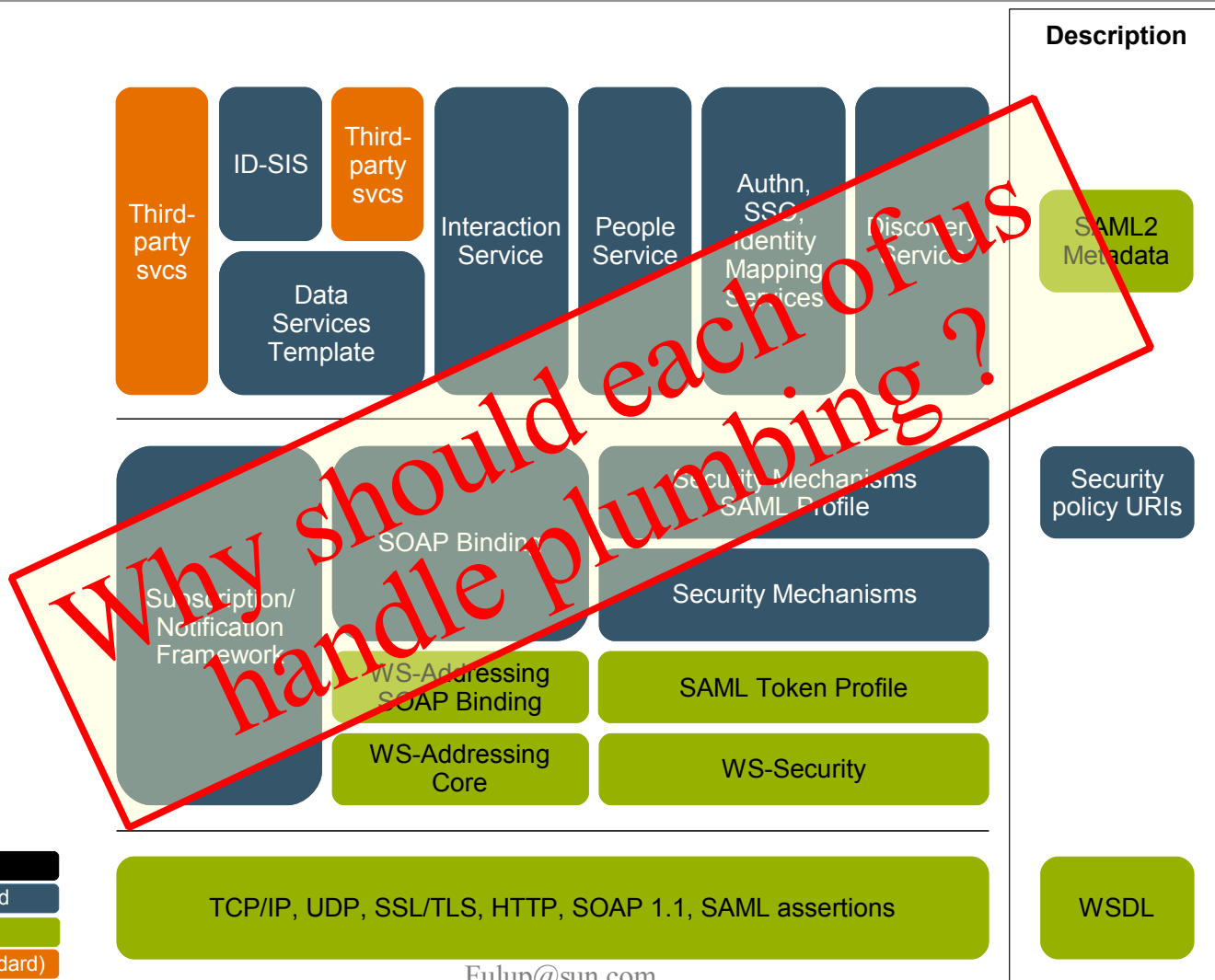


# Protocol architecture piece-parts



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

# Should we even know about this ?



**Legend:**

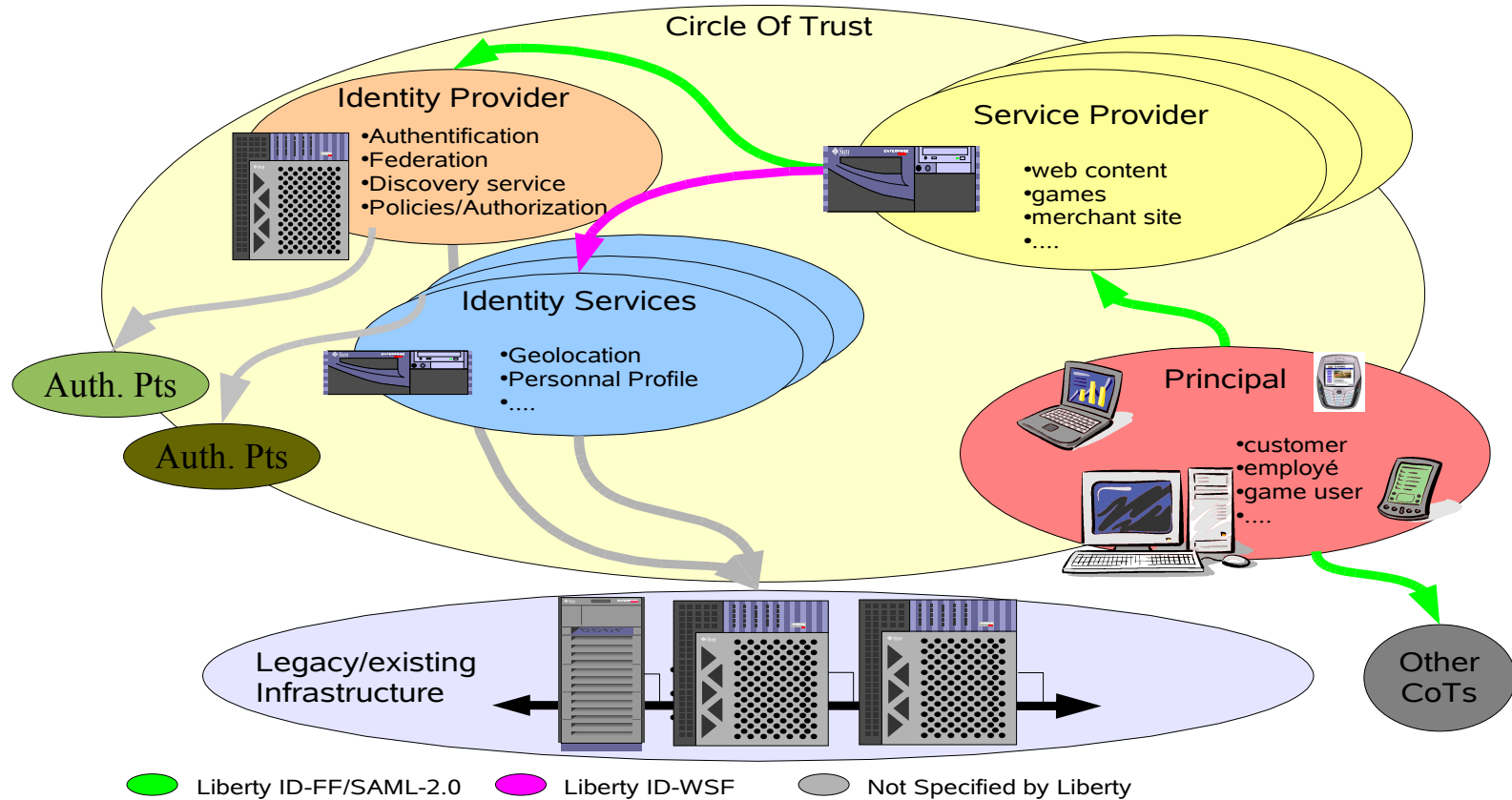
Liberty Alliance standard

External standard

Third-party (possibly a standard)

June 2007

# Global Liberty Architecture



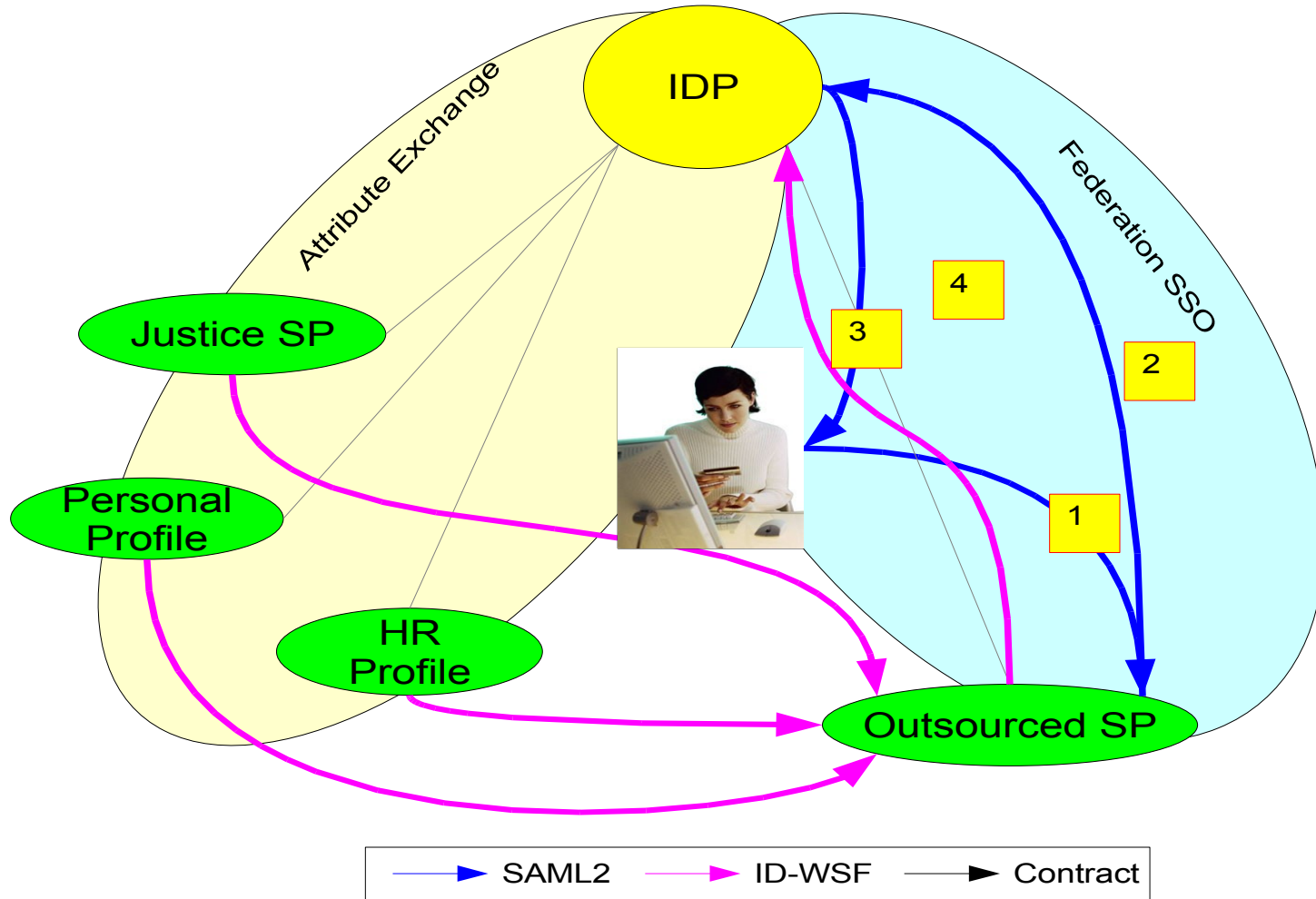
# Liberty Technical Framework

- **ID-FF (Identity Federation Framework)**
  - Federation/Defederation
  - SSO (*single & simplified Sign On*) / SLO (*single logout*)
  - Authentication context & Attributes
  - Metadata
- **ID-WSF (Identity Web Service Framework)**
  - Authentication Service
  - Discovery Service
  - DST (Data Service Template)
  - Interaction Service
  - People Services
- **ID-SIS (Identity Service Interface)**
  - Personal profile, Geoloc, Presence, Contact Book, ...
  - *Tomorrow HR-SiS ???*

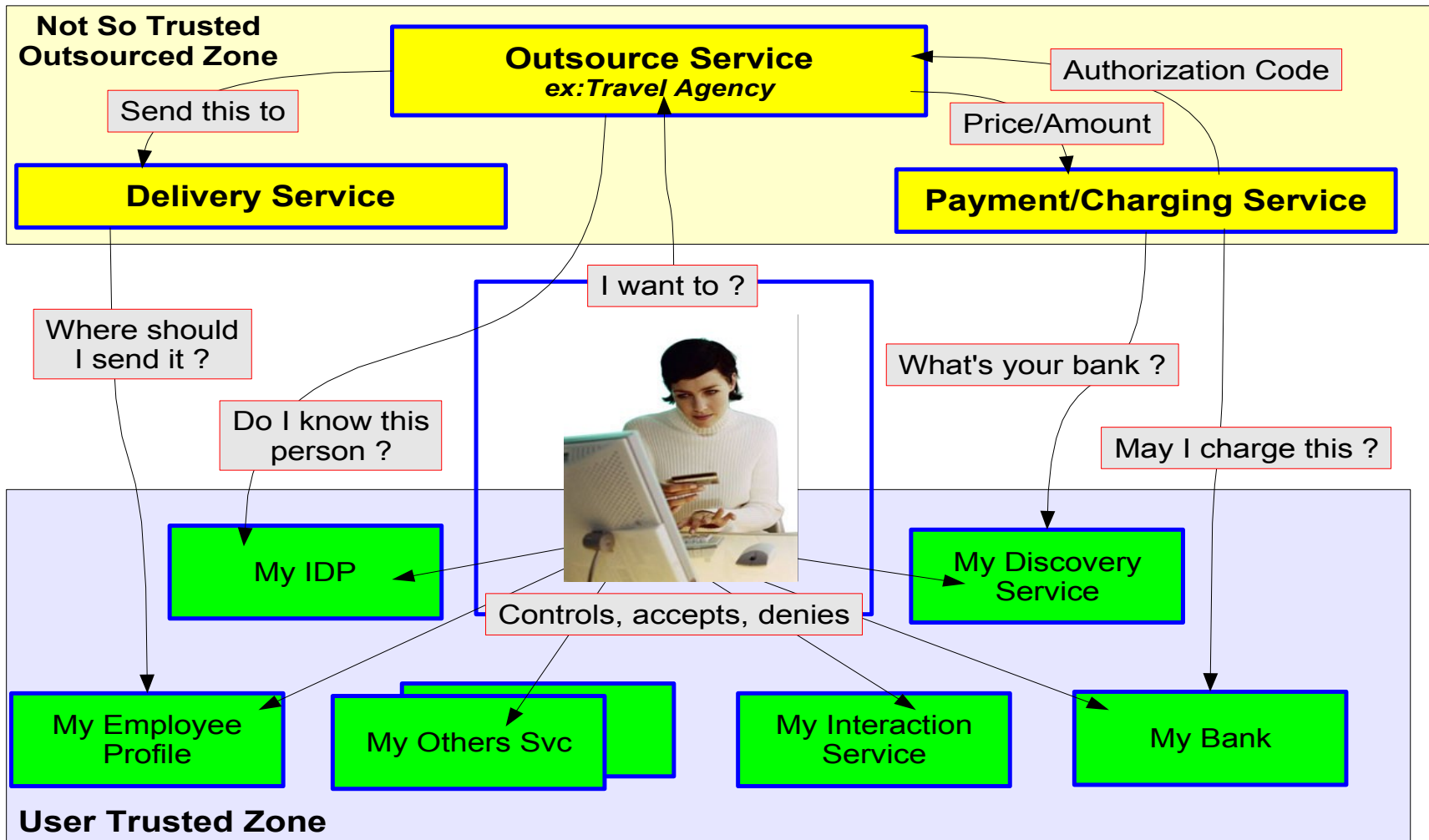
# Outsourcing Scenario

- **Service Constraints**
  - Must be a valid employee from XYZ
  - Must not have the right to request this service
  - Need to know some attributes (ex: department, addr,...)
  - Need to be able to store local preferences
  - ...
- **Citizen Constraints**
  - Need to protect customer/employees
  - Make sure that only valid & authorized people can use it.
  - Log, Tracking, Audit, ...

# Outsourced Simplified Flow



# Outsourcing Big Picture



# Delegation Scenario

- **You create a company (QuickMoney)**
  - Govt gives you a QuickMoney-ID
  - As citizen & owner, you act on behalf of QuickMoney
  - QuickMoney-ID is federateable (ex: with MyBank)
- **You sign a contract with a MyLawyer SP**
  - You allow MyLawyer to act on behalf of QuickMoney
  - You can control who can act on QuickMoney's behalf
  - eGovt service asserts MyLawyer as “authorized lawyer”
- **You sell QuickMoney to BigComp**
  - BigComp can now act on behalf of QuickMoney
  - BigComp can establish new delegations

# 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 students, citizens, employees, companies
  - 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 (nothing without my consent)
  - Strong privacy & security
  - Simple & intuitive

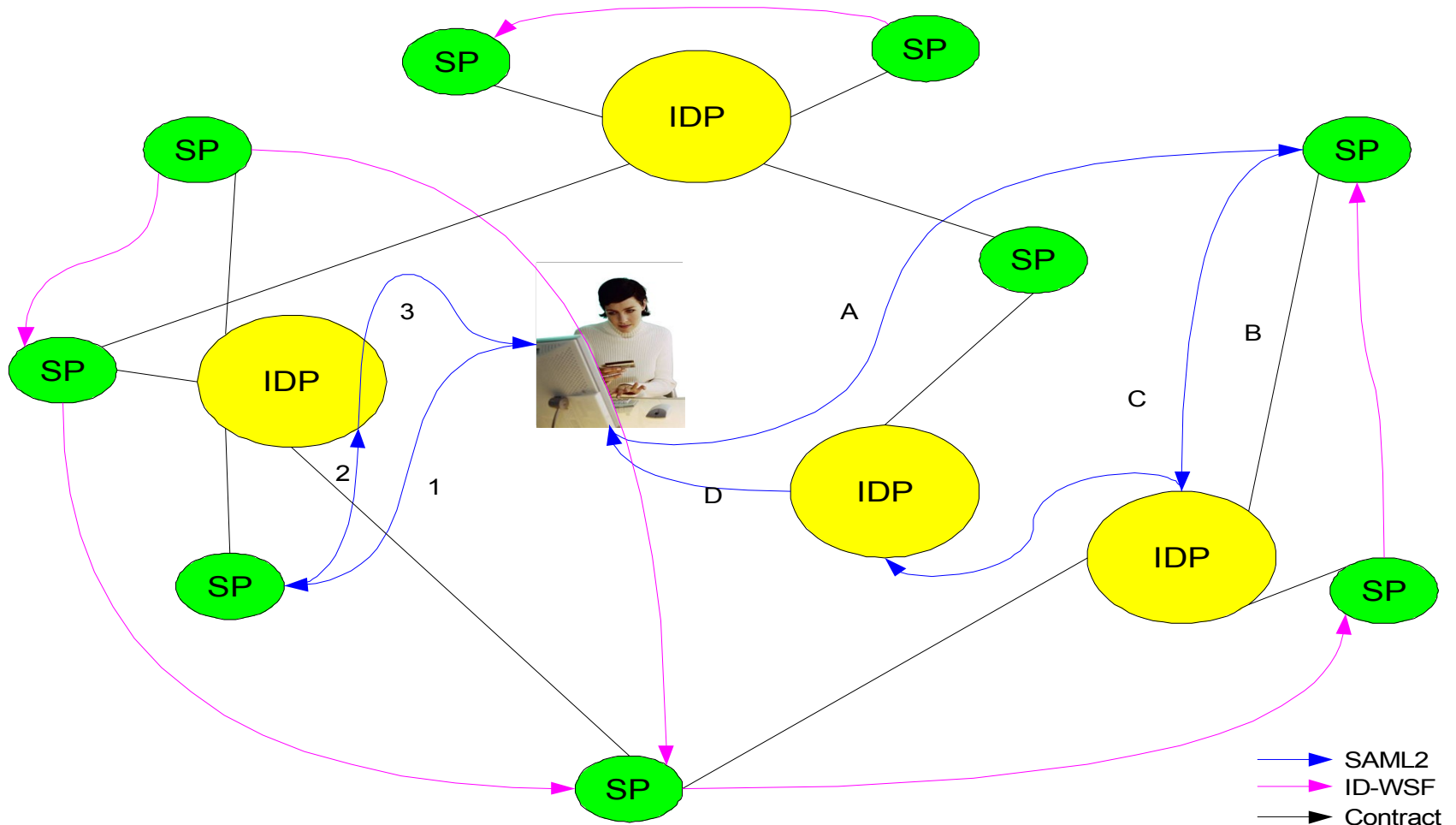
# Federated Authority

- **Should be:**
  - a shield to allow employee/customer to interact with “untrusted” parties.
  - a trusted intermediary to find and exchange attributes in a peer to peer mode with a high level of confidence.
  - a friend that diminishes process complexity.
  - a referent that guarantees user to keep control of its own identity.
- **Should not be:** a new “super homepage”, a Big Brother, a new problem for users, something expensive, ....

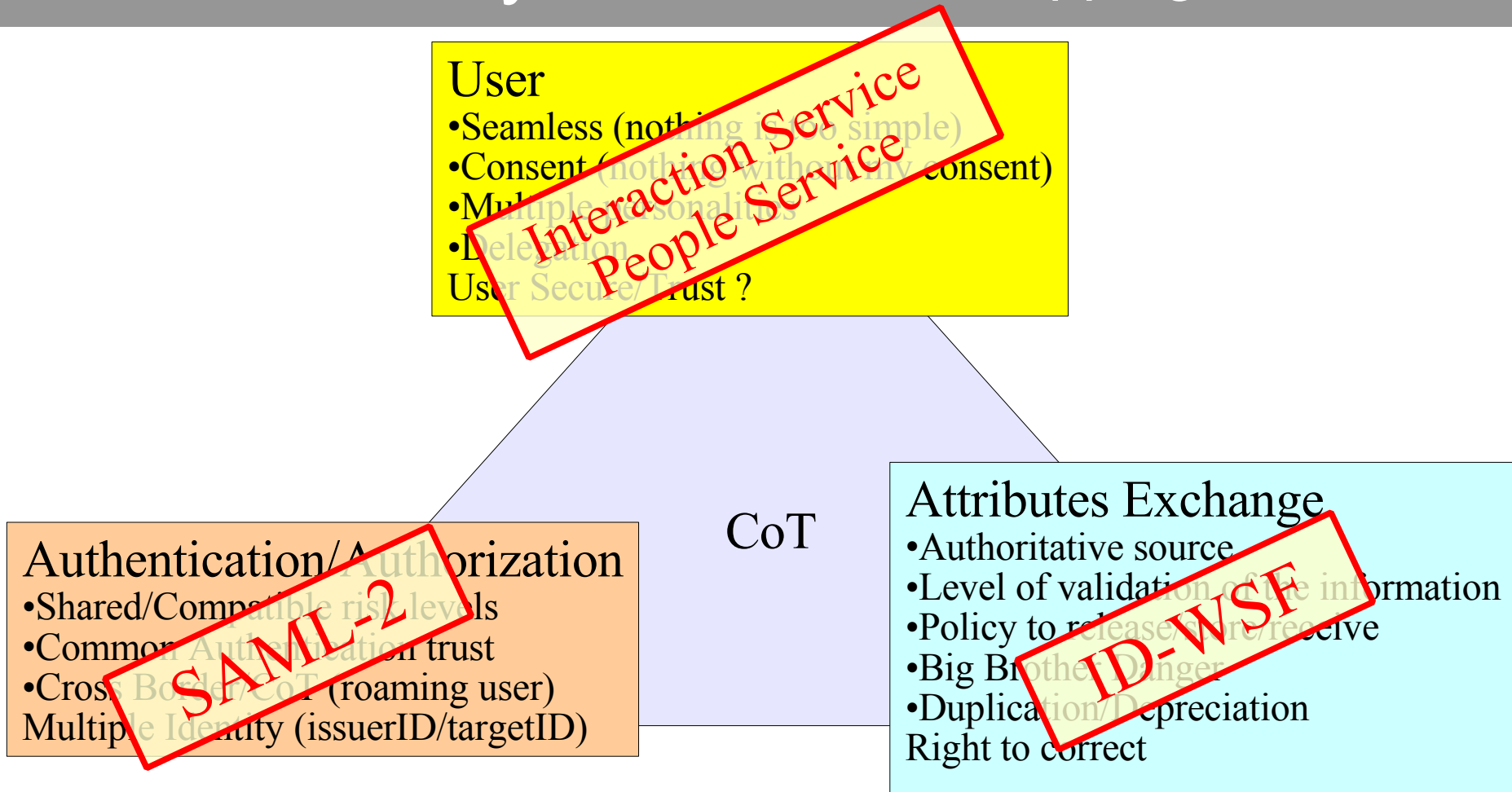
# Which Authority's Components

- **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, ...

# General Federated Architecture

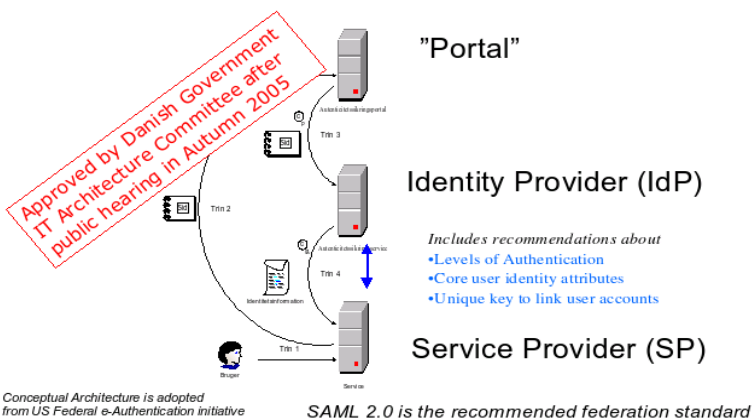


# Liberty Framework Mapping



# Mature and Evolving

## Reference Architecture for Cross-organizational Single Sign On



## Felles innglogging for offentlige tjenester



Du har valgt en offentlig tjeneste som krever at du identifiserer deg. Første steg består i å oppgi fødselsnummeret ditt i feltet nedenfor.

Velg språk: Bokmål | Nynorsk | Sámeigiella | English

Steg 1 av 2: Vennligst tast inn ditt fødselsnummer

Fødselsnummer (11 siffer)

NESTE

- [Hjelp til innglogging](#)
- [Personvern og sikkerhet](#)
- [Bestill PIN-koder](#)
- [Sperr PIN-koder](#)

Versjon 1.0.15.4 - 20.12.2006

Norge.no | Tlf: 800 30 300 | [Kontakt Norge.no](#) | Ansvarlig redaktør: Ove Nyland



Le projet de portail Mon.Service-Public.fr doit permettre à l'utilisateur - personne physique ou morale - l'accès à une gamme cohérente et étendue de services dans un environnement personnalisé, et ce dans des conditions permettant de créer la confiance. Une version pilote a été développée et testée par 500 usagers mi 2006. Après des conclusions plutôt positives sur cette expérimentation et l'intérêt du service, la phase de réalisation du système "grand public" a été lancée.

