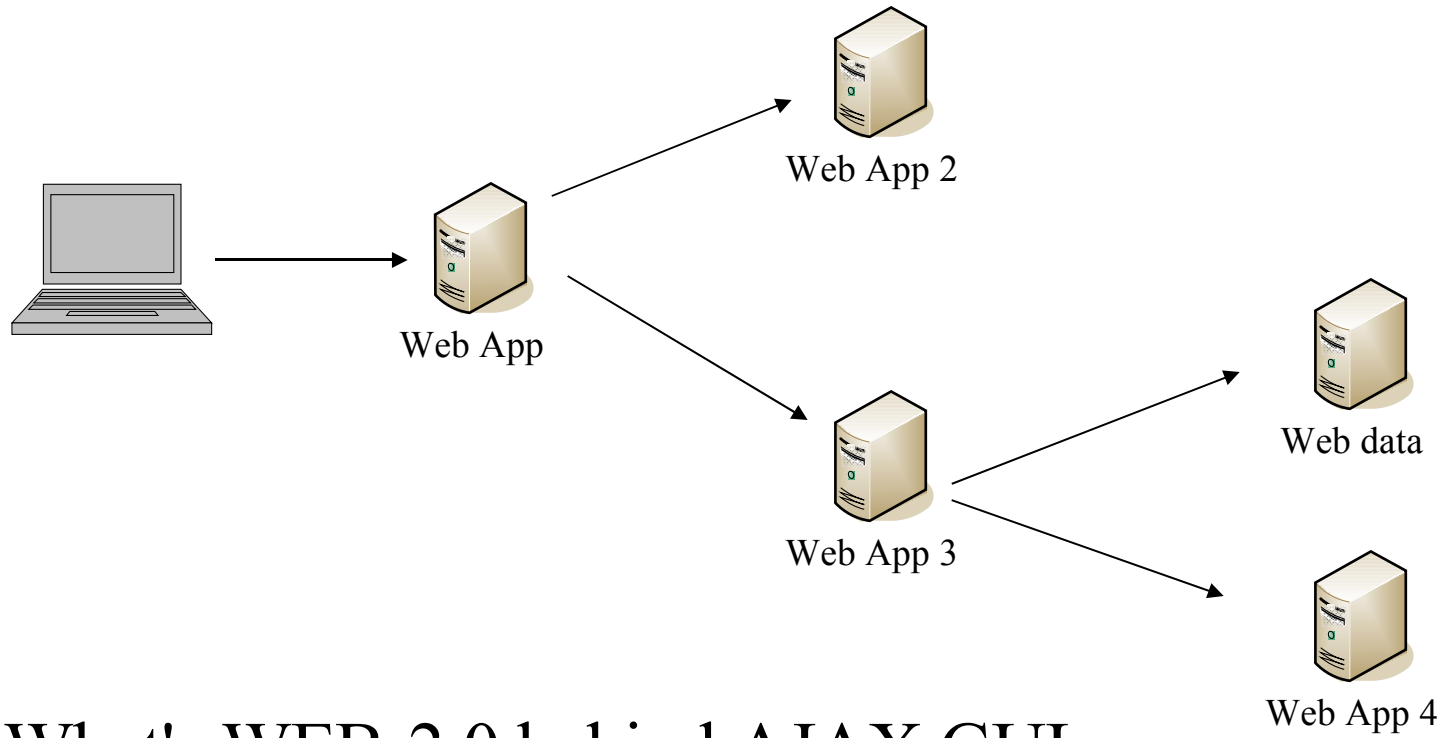
LIBERTY ALLIANCE PROJECT

New Generation of Liberty Federated Architecture

Fulup Ar Foll, Sun Microsystems
fulup@sun.com

WEB-2.0 problematic



What's WEB-2.0 behind AJAX GUI

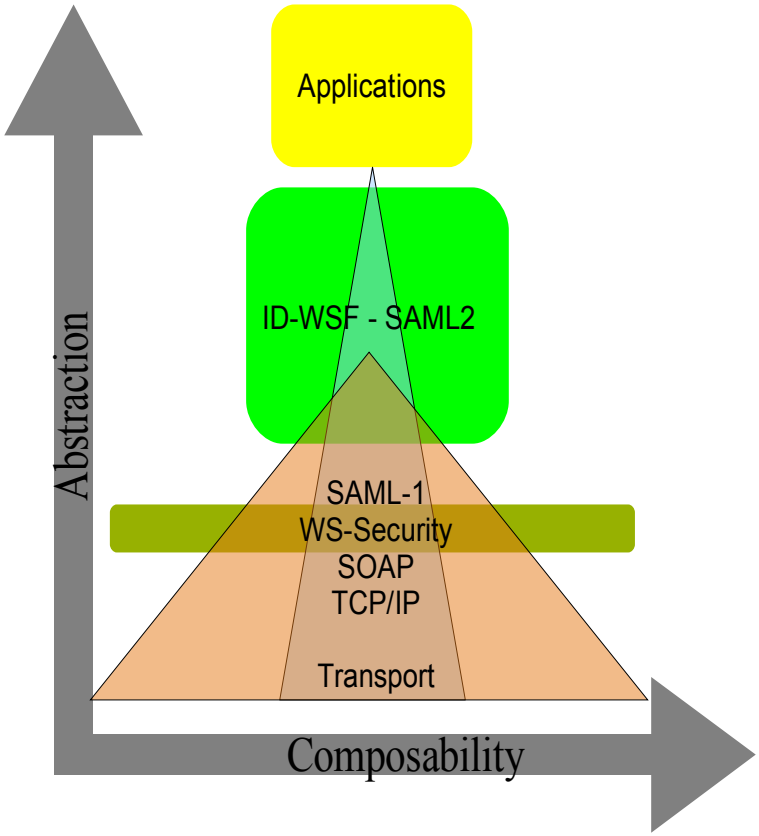
LIBERTY ALLIANCE PROJECT

Next Generation Design Goal

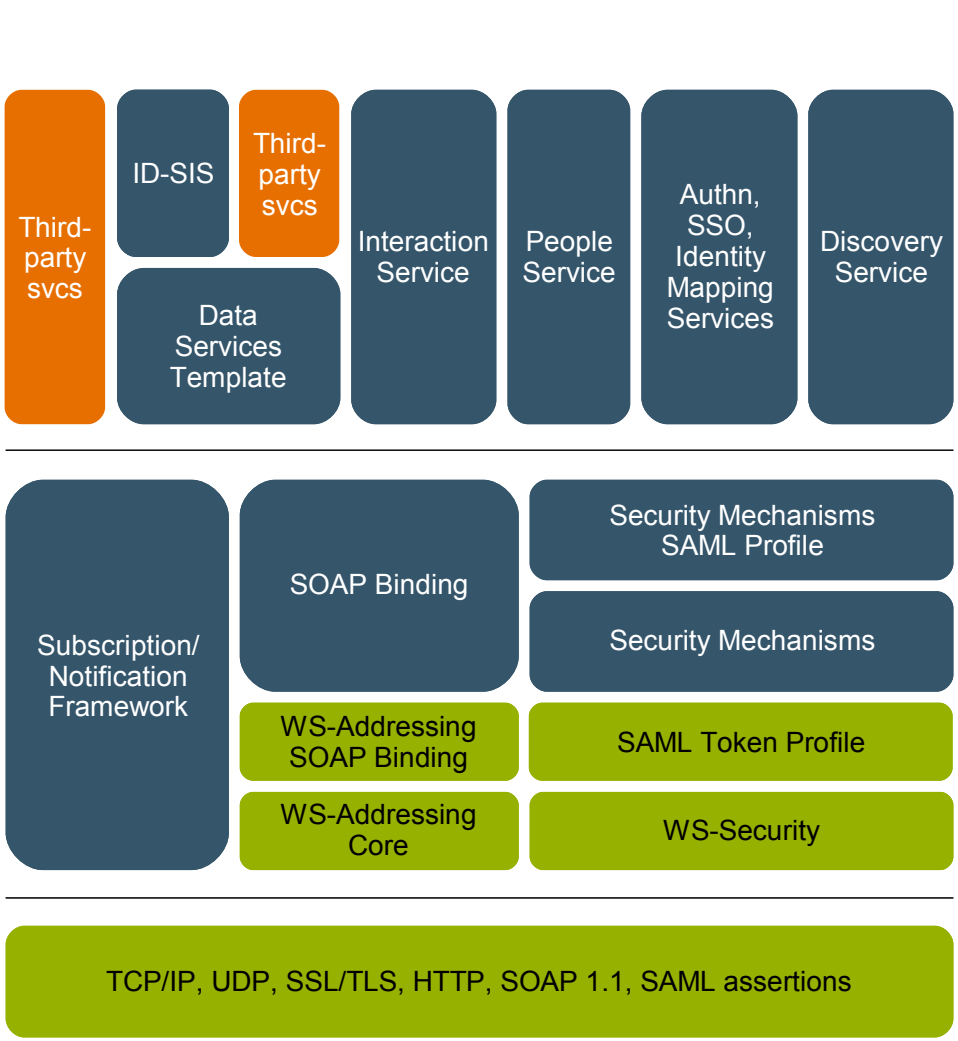
- User Centric, nothing without my consent
- Information collected, maintained once by the most appropriate source.
- Information verified to the adequate level.
- Information available electronically through a vendor neutral long-term standard.
- Information exchange securely to whomever requires it,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

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 —the user—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

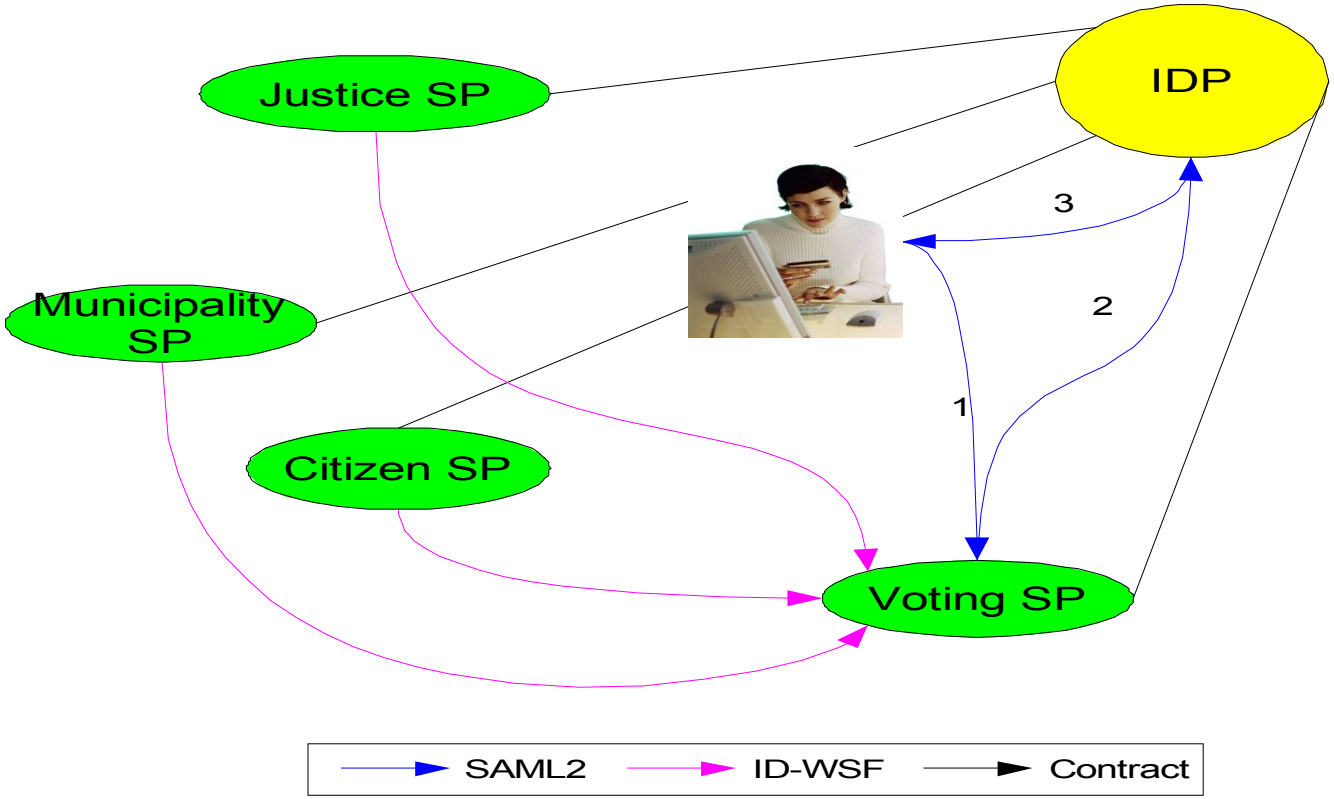


LIBERTY ALLIANCE PROJECT

Anonymous Vote Scenario

- **Government Constraints**
  - Must be 18+
  - Must not have any criminal record
  - Must be a citizen of “Lichtenstein”
  - Must only vote once
  - ...
- **Citizen Constraints**
  - Government should not know what you vote for
  - Voting SP should not know who you are

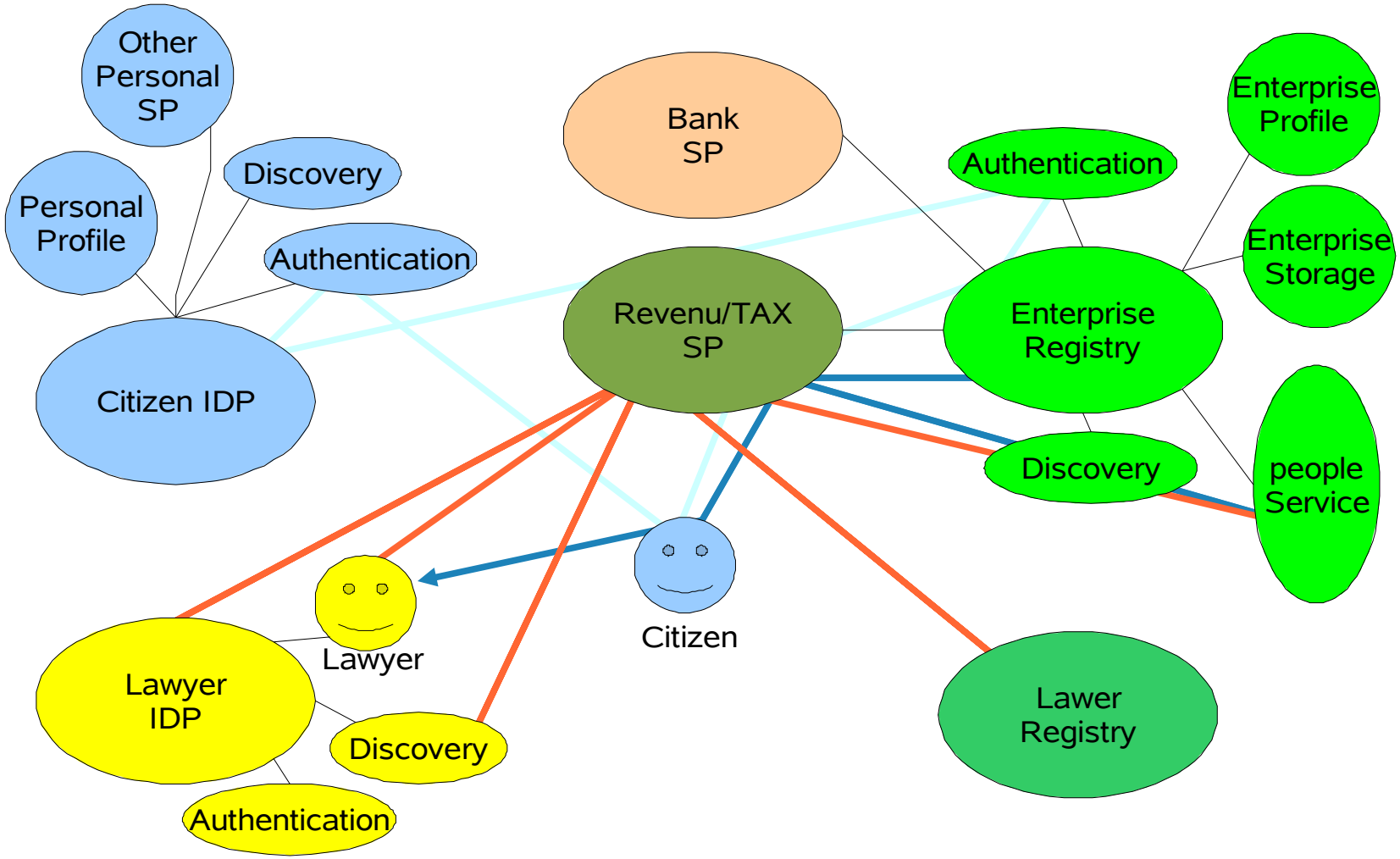
Anonymous Vote Flow



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

People Service Delegation Flow



LIBERTY ALLIANCE PROJECT

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 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

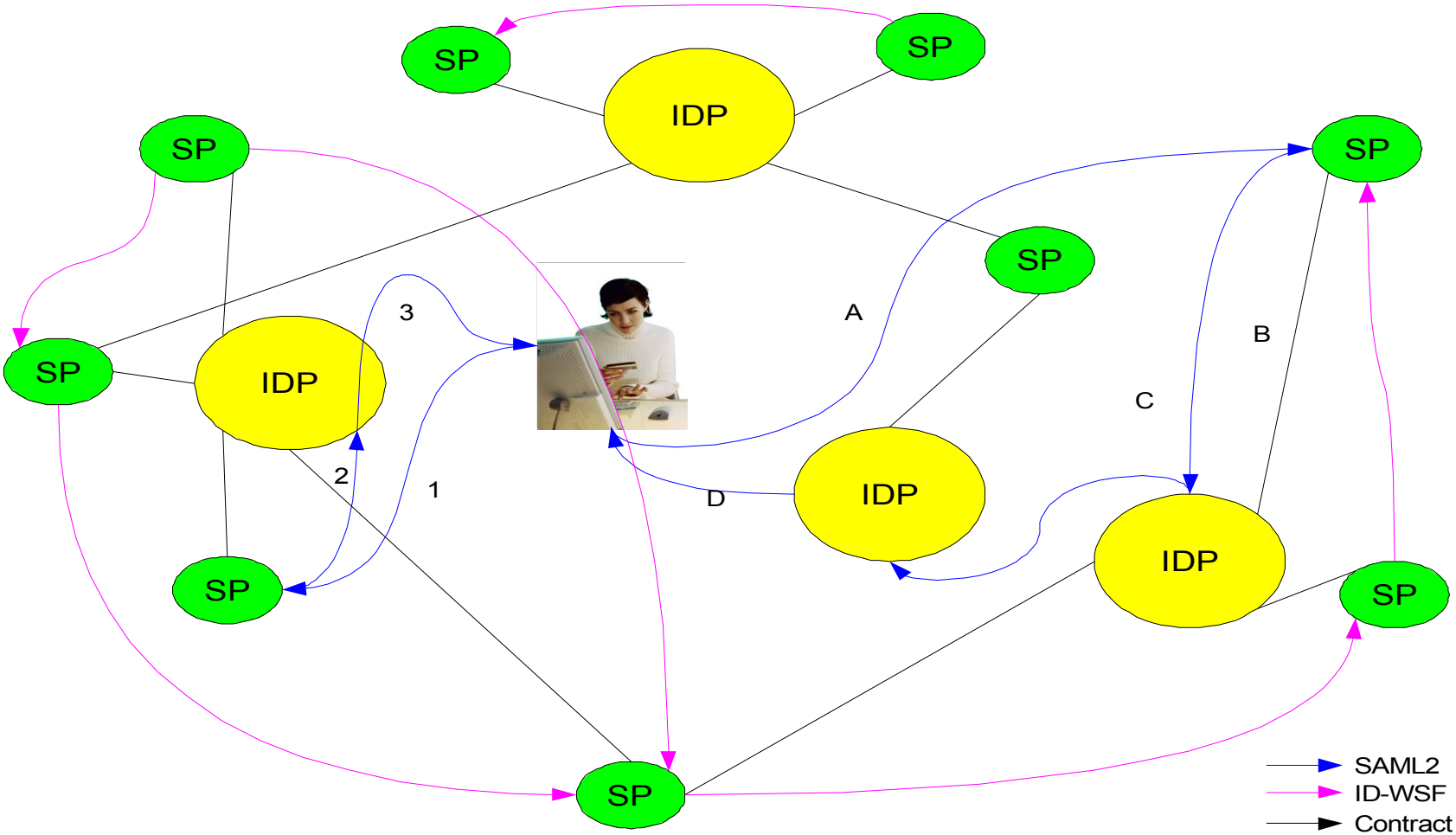
Federated Authority

- **Should be:**
  - a shield to allow citizen 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 government 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

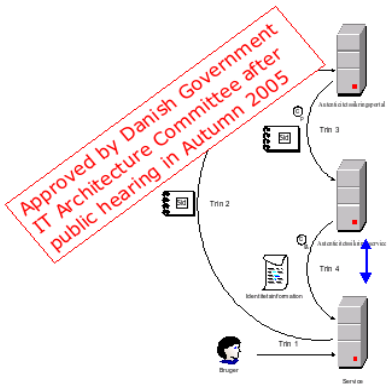
- Basic Authority Services
  - **Authentication Framework**
    - Common definition of risk
    - Common authentication confidence for a given risk
  - **Federation framework**
    - Multi-authority (proxy IDP model)
    - Multi-personality
  - **Discovery Mechanism**
    - Where to find services (in a user contextual mode)
    - Security Mechanism (Attributes shared 1st 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



Mature and Evolving

Reference Architecture for Cross-organizational Single Sign On



"Portal"

Identity Provider (IdP)

Includes recommendations about
- Levels of Authentication
- Core user identity attributes
- Unique key to link user accounts

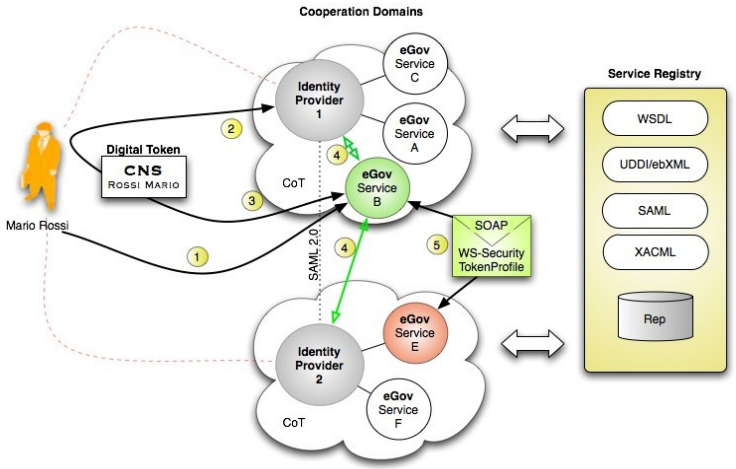
Service Provider (SP)

Conceptual Architecture is adopted from US Federal e-Authentication initiative

SAML 2.0 is the recommended federation standard

mon.Service-Public.fr

Le projet de portail Mon.Service-Public.fr doit permettre à l'usager - 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.



LIBERTY ALLIANCE PROJECT

Pa zo Echu, Echu eo(1) !

Disclaimer: I won't claim the ideas presented in this presentation to be exclusively personal or even original. Here are a few names of people I somehow trust(2) and from whom I stole one or more ideas that appear directly or indirectly in this presentation:

Andreas.Hamnes(Norway) Britta.Glade(USA) Colin.Wallis(New-Zealand) Conor.P.Cahil(USA) Efjestad.Dag(Norway) Eve.L.Maler(USA) George.Fletcher(USA) Hubert.Le-Van-Gong(France) Ignacio Alamillo(Spain) Ingrid.Melve(Norway) Jean-Severin.Lair(France) Lasse.Andresen(Norway) Lauren.Wood(Canada) Louise.Thiboutot (Canada) Mira.Nivala(Finland) Myriam.Cyr(Canada) Orhan.Alkan(Turquie) Ovidiu.Constantin(Italy) Paul.Madsen(Canada) Paul.Zeef(Netherland) Sampo.Kellomaki(Portugal) Søren.Peter-Nielsen(Danemark)Tanguy.Mercier(France) Tisserant.Alexandre(France) Victor.Ake(Finland)

Fulup@sun.com

(1) “When it is finish, Finish it is” in Breton Language
(2) Which does not mean they would agree with me