LIBERTY ALLIANCE PROJECT

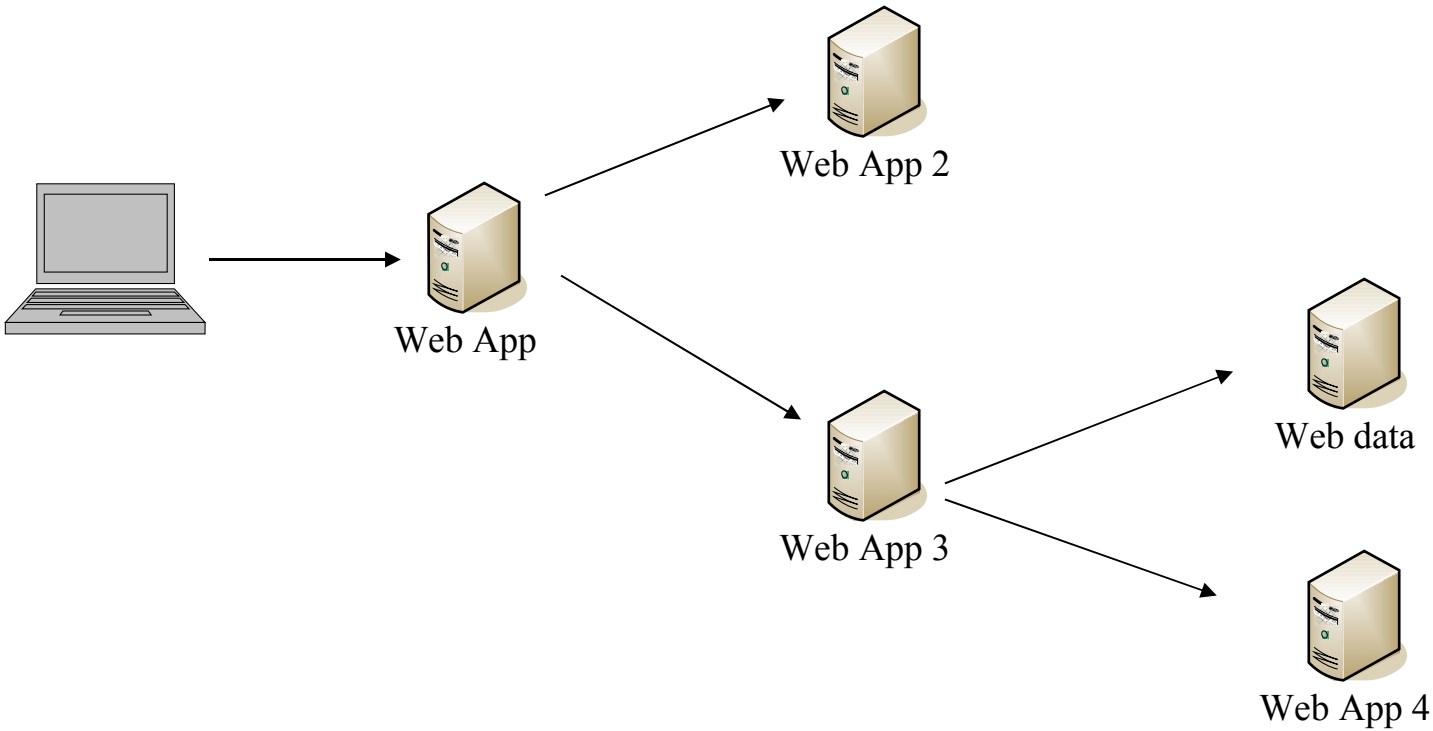
New Generation of Identity Aware Web Applications

Fulup Ar Foll, Sun Microsystems
fulup@sun.com

LIBERTY ALLIANCE PROJECT

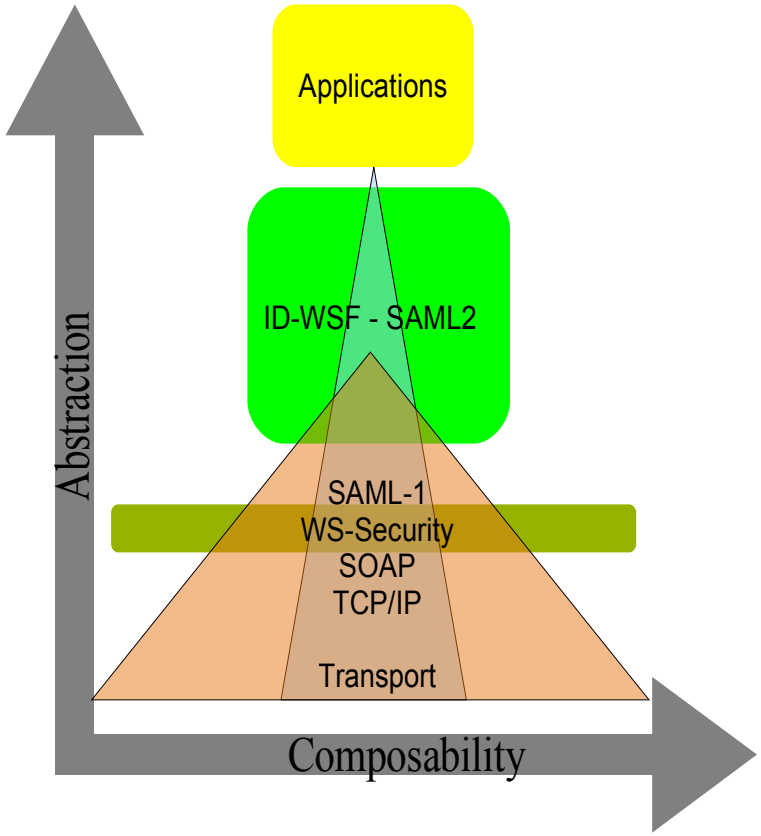
What's WEB-2.0 behind AJAX GUI

WEB-2.0 layered WEB architecture

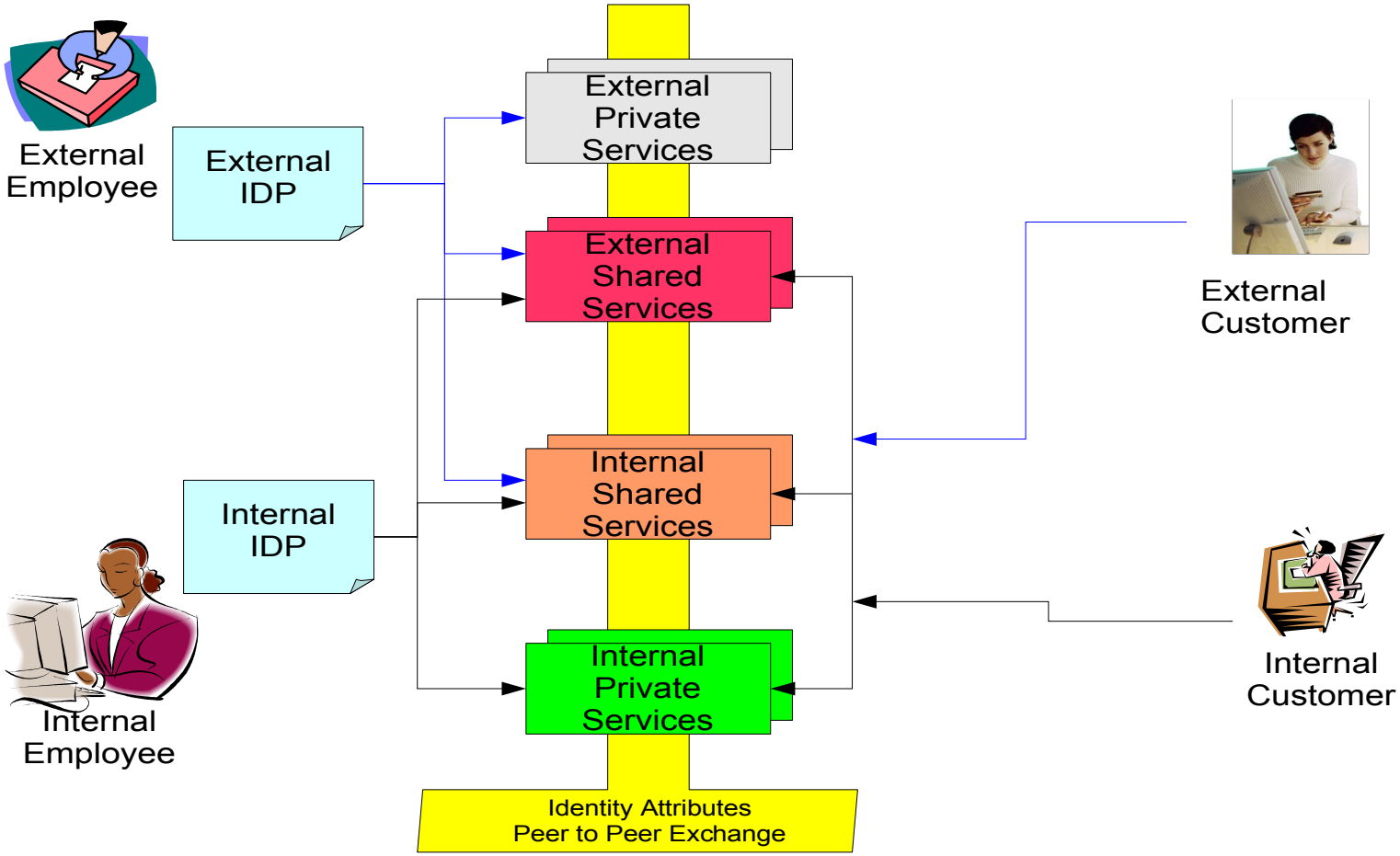


A hight level Inter-operable standard

- **Global Connectivity**
  - Across repository, domain, ...
  - Seamless to User (complexity advert)
  - Want to be both consumer and provider
- **Increasing Demand for ID**
  - Every one want your Identity, but does users want it ?
  - Need adequate privacy mechanisms before exposing it.
- **Heterogeneous world**
  - Multi vendors, services provider and consumers are heterogeneous.
  - Multi channel, cross devices, cross networks, ...
- **...**



Why Federation & Attributes Exchange



LIBERTY ALLIANCE PROJECT

Next Generation Design goals

- A standards-based architecture for Federation & identity web services
  - Ecosystems of services that expose interfaces on behalf of individual users' identities
- Privacy and Security as a 1st class citizen
  - Identity information requests access-controlled
  - Minimal disclosure of identity information
  - Protection against disclosure of identifiers
- Flexible foundation for application development
  - Across security domains and computing platforms
  - Across time, allowing for service location flexibility

Privacy is a MUST

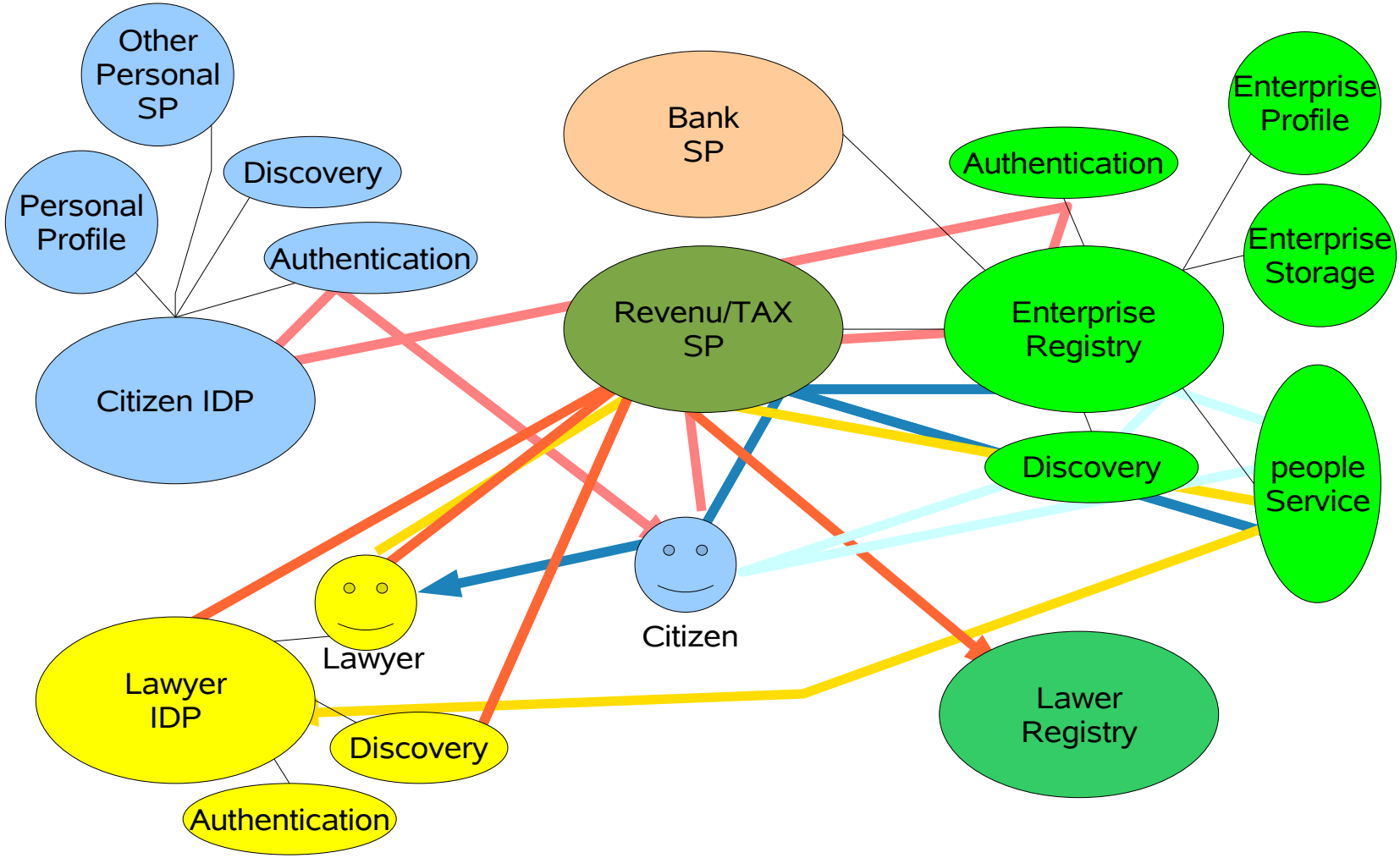
- Ensuring that your data is shared on your terms by:
  - Capturing your usage directives and consent status in service messages
  - Allowing for interaction with you at critical junctures to obtain your consent and privacy policies
    - Interaction Service, Interaction Redirect
- Inhibiting correlation of your activities by:
  - Offering different pseudonyms to different parties
    - Identity Mapping Service
- Protecting your data in transit
  - WS-Security for confidentiality

LIBERTY ALLIANCE PROJECT

Delegation Scenario

- You Create a company (SmallComp)
  - Govt gives you a SmallComp-ID
  - As Citizen & Owner you act on behalf of SmallComp,
  - SmallComp-ID is federable (ex: with MyBank)
- You sign a contract with an MyLayer SP
  - You allow your layer to act on behalf of SmallComp
  - You can control who can act on SmallComp behalf
  - eGovt service can assert MyLayer as a layer
- You sell SmallComp to BigComp
  - BigComp can now act on behalf of SmallComp
  - BigComp can break MyLayer delegation

People Service Delegation Flow



LIBERTY ALLIANCE PROJECT

Major benefits of ID-WSF's design

- Peer to Peer (no big brother)
- Authentication, authorization, and application of usage policy against consumers of identity data
- User privacy through use of pseudonyms
- Dynamic service discovery and addressing
- Common web services transport mechanisms to apply identity-aware message security
- Abstractions and optimizations to allow anything – including client devices – to host identity services
- Unified data access/management model for developers
- Flexibility to develop arbitrary new services
- Identity model for social network & cross users (ID-WSF2)

What does Web 2.0 need?

- SSO at the service level (as opposed to browser session level)
  - *Liberty ID-WSF provides this*
- An identity model to identify parties in txns
  - *Liberty ID-WSF provides this*
- An identity model that supports chained txns
  - *Liberty ID-WSF provides this*
- An interaction model that supports backend interactions
  - *Liberty ID-WSF provides this*
- A discovery model that allows per-user discovery
  - *Liberty ID-WSF provides this*
- A token management model that allows context translation
  - *Liberty ID-WSF provides this*

LIBERTY ALLIANCE PROJECT

C'est Fini

Fulup Ar Foll
fulup@sun.com