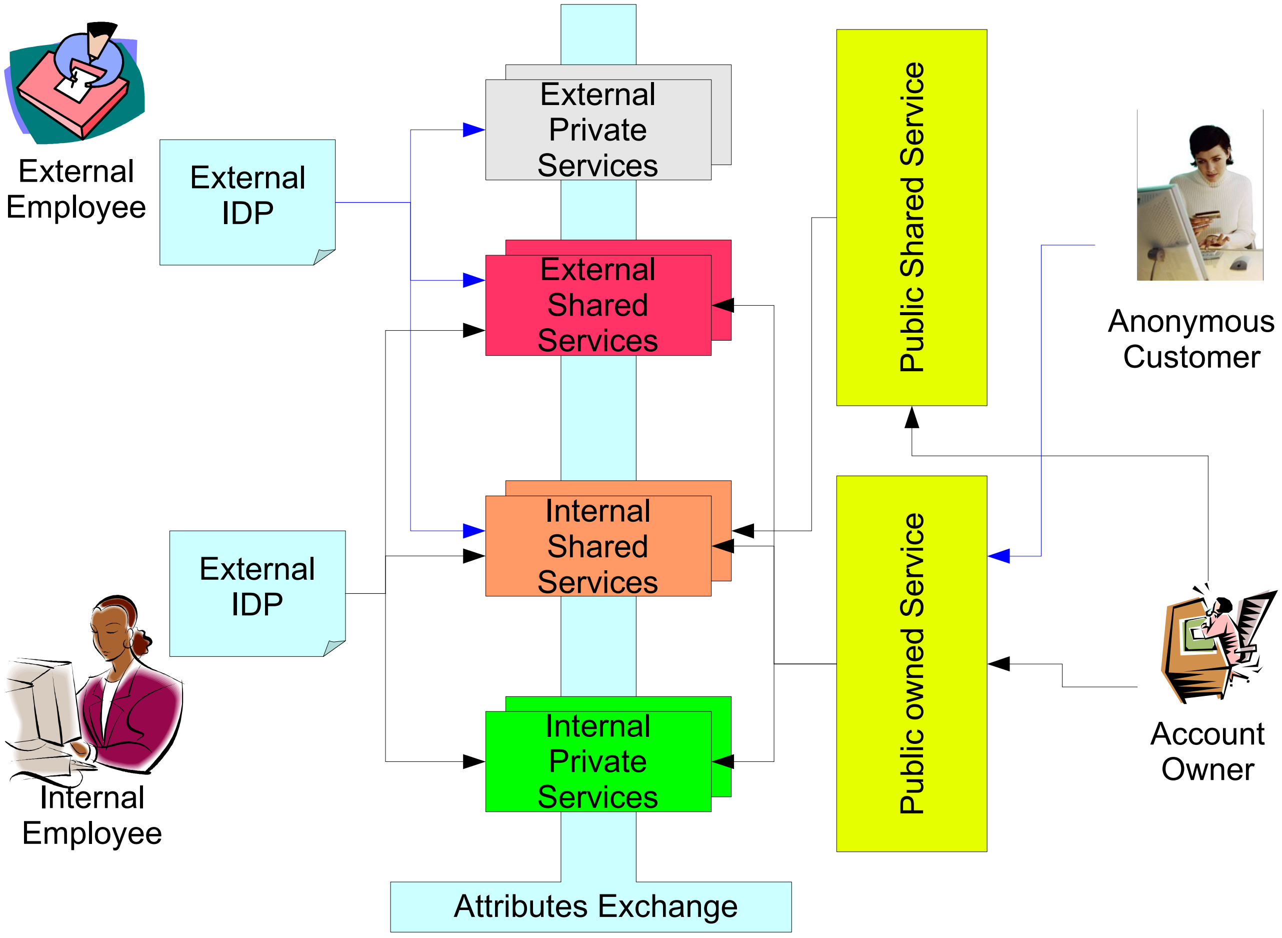
Liberty Alliance
From Usecases to Specifications

Fulup Ar Foll
Master Architect
Global Software Practice
Sun Microsystems

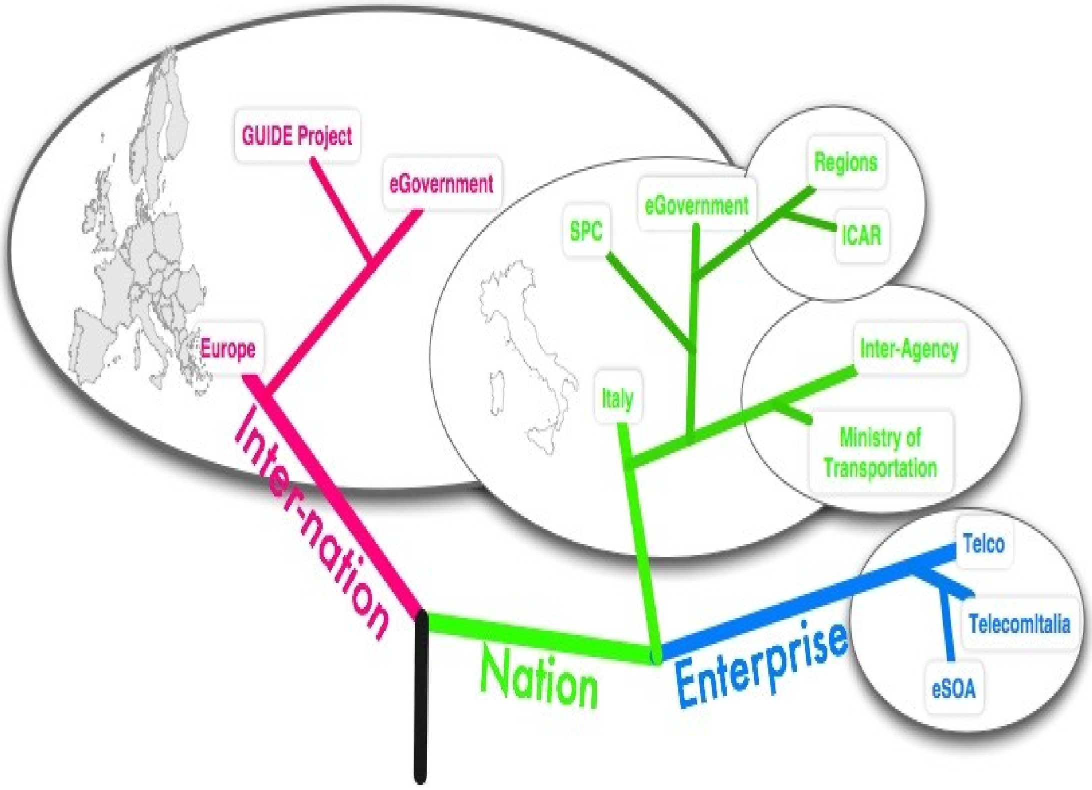
Why Federation

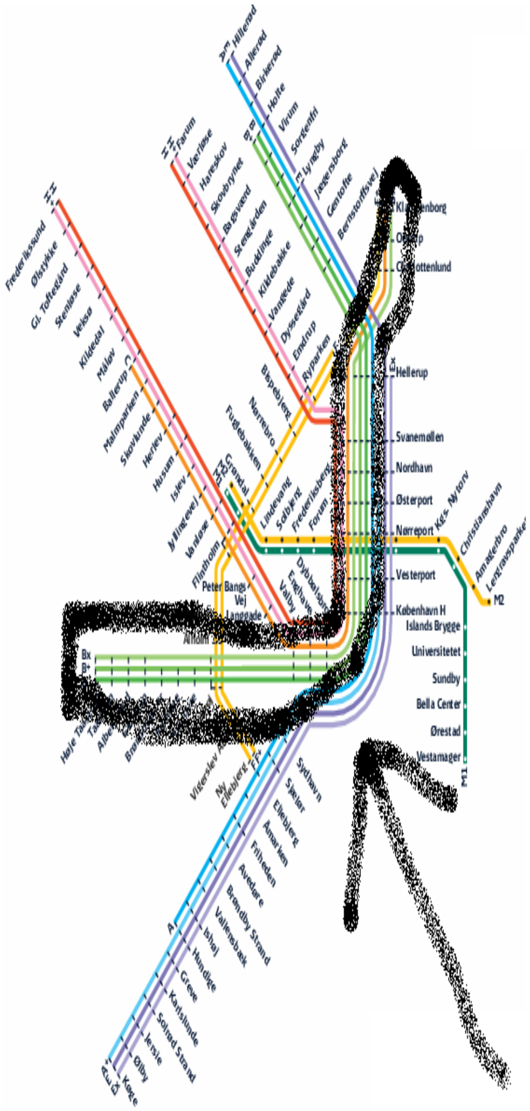


What's About Federation

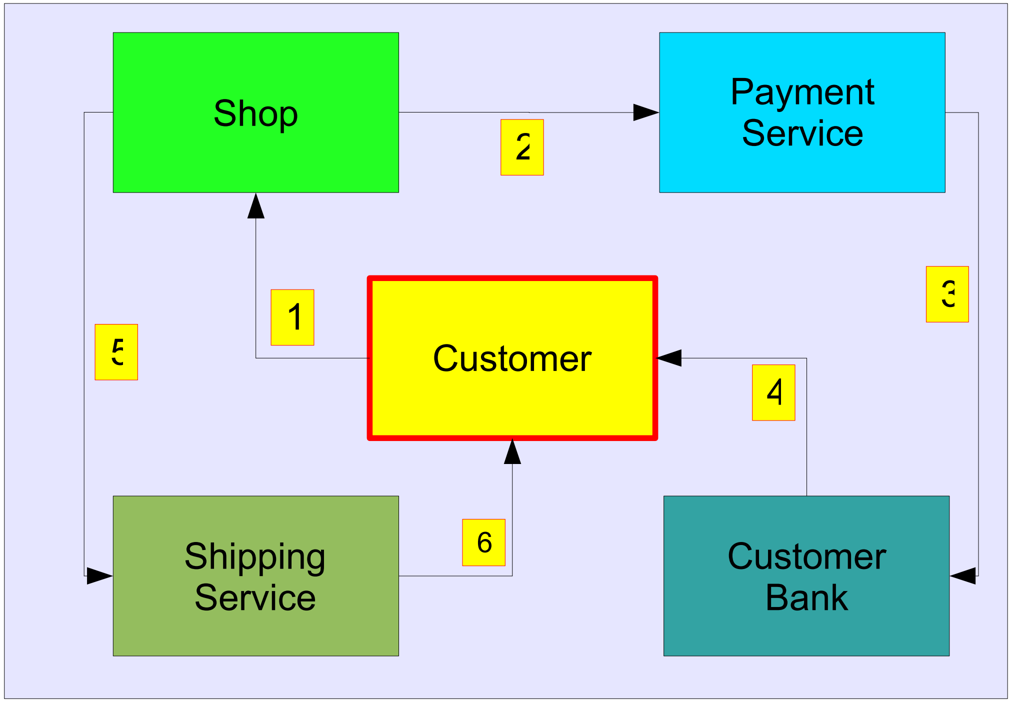
- Federation of providers (CoT), a group of entities providing services who signed agreement, in order to make life of shared customers/users *(Principal)* more simple.
  - *accept Principal identity authentication to be done once per session (SSO) and by a shared authority (IDP)*
  - *Accept to provide service knowing only an “avatar” of principal identity (Opaque Handle/Federation Key). This non significant pointer on principal identity allowing service provider (SP) to know that “it is him” without knowing “who he is”.*
- Federation: a weak link that allow to map a principal avatar identity used by a service provider to the effective principal identity know only from the authority of authentication (IDP).
- Federated Identity: The data/attributes at the service provider attached to a principal identity avatar.

Think Big / Start Small





Don't Forget Privacy



1) User buy something

2) Shop check payment service (Visa, Amex, Paypal, ...)

3)Payment Service check customer bank

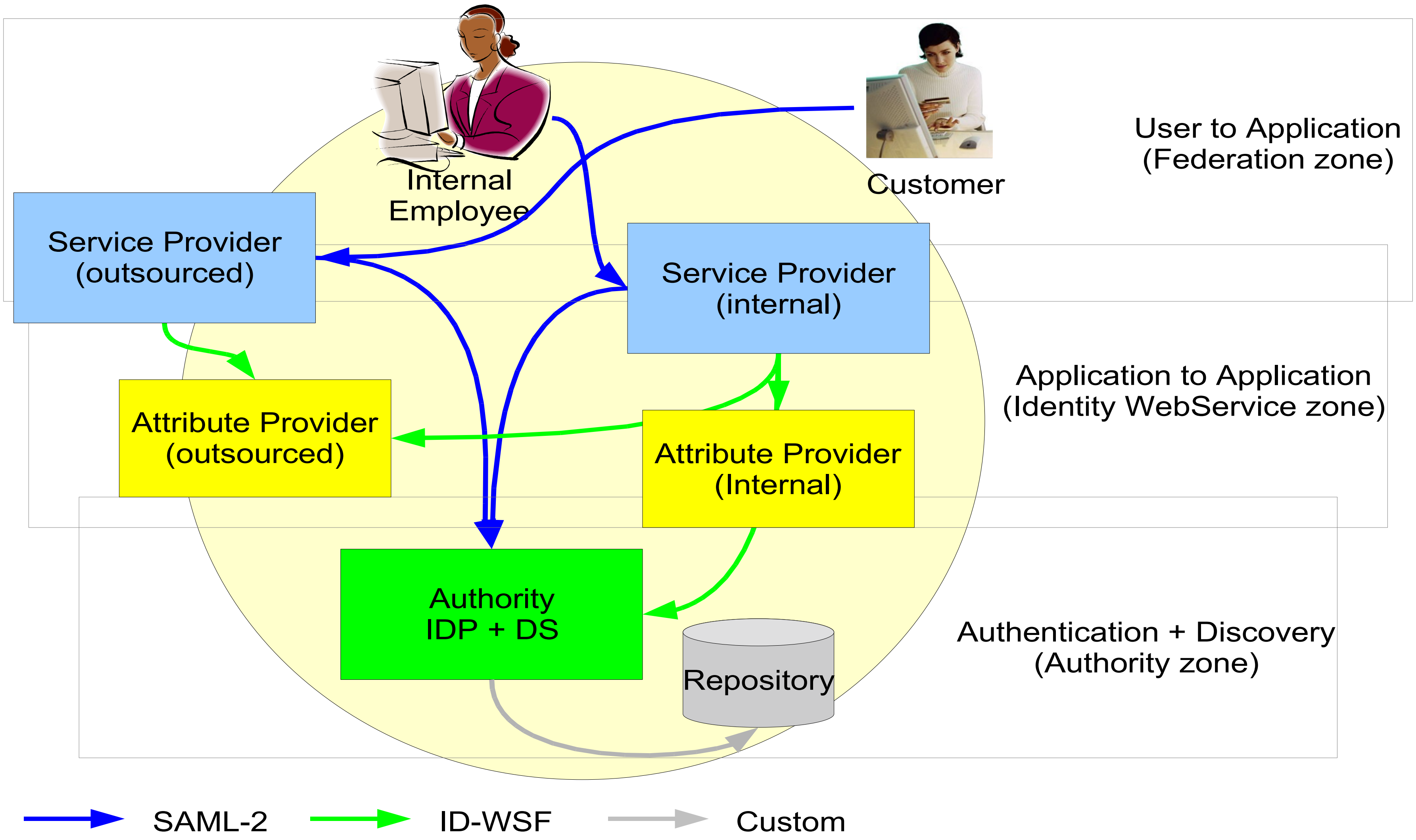
4)Bank check user consent

5)Shop give packet to shipping service

6)Good is deliver where ever customer want

Actor	Must have relation with	Must know Attributes
•**Customer**:	vendor, shipping, bank	products(choose), price(accept), delivery address (choose/select)
•**Shop**:	payment, shipping	price (own), product (from customer)
•**Shipping**:	shop	delivery address (from customer)
•**Payment**	shop, bank	price(from shop), bank(from customer)
•**Bank**:	payment, customer	price (from payment), bank account(own)

Liberty Self Contain Circle of Trust



Internal Employee

Customer

User to Application (Federation zone)

Service Provider (outsourced)

Service Provider (internal)

Application to Application (Identity WebService zone)

Attribute Provider (outsourced)

Attribute Provider (Internal)

Authority IDP + DS

Repository

Authentication + Discovery (Authority zone)

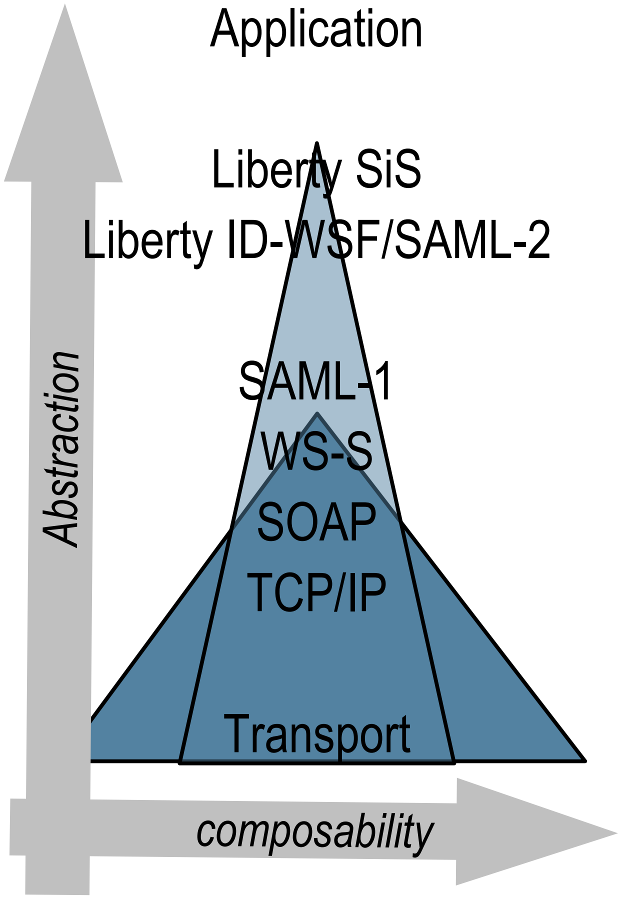
SAML-2

ID-WSF

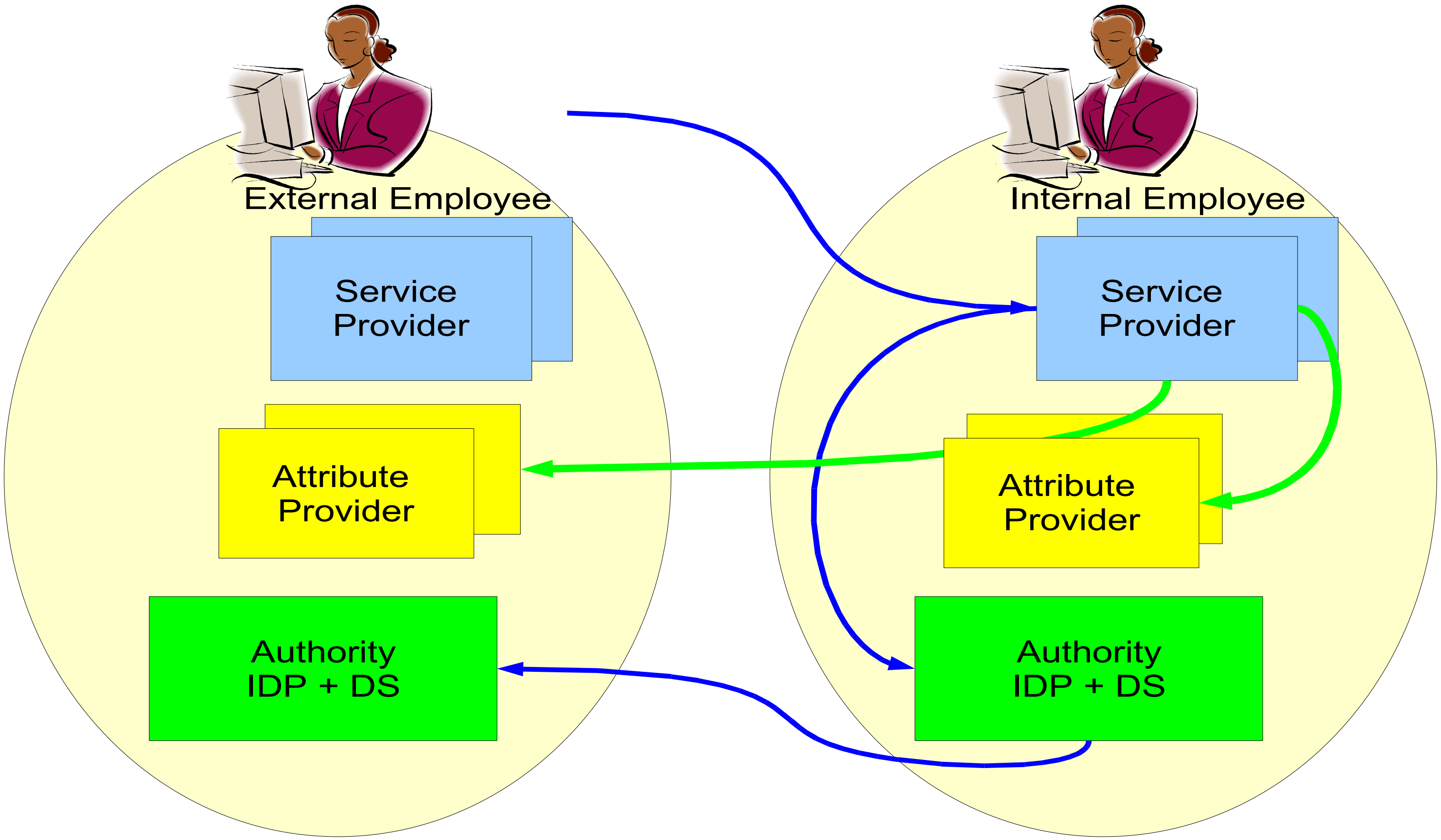
Custom

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
- ID-SIS (Identity Service Interface)
  - Personal profile, Geoloc, Presence, Contact Book, ...



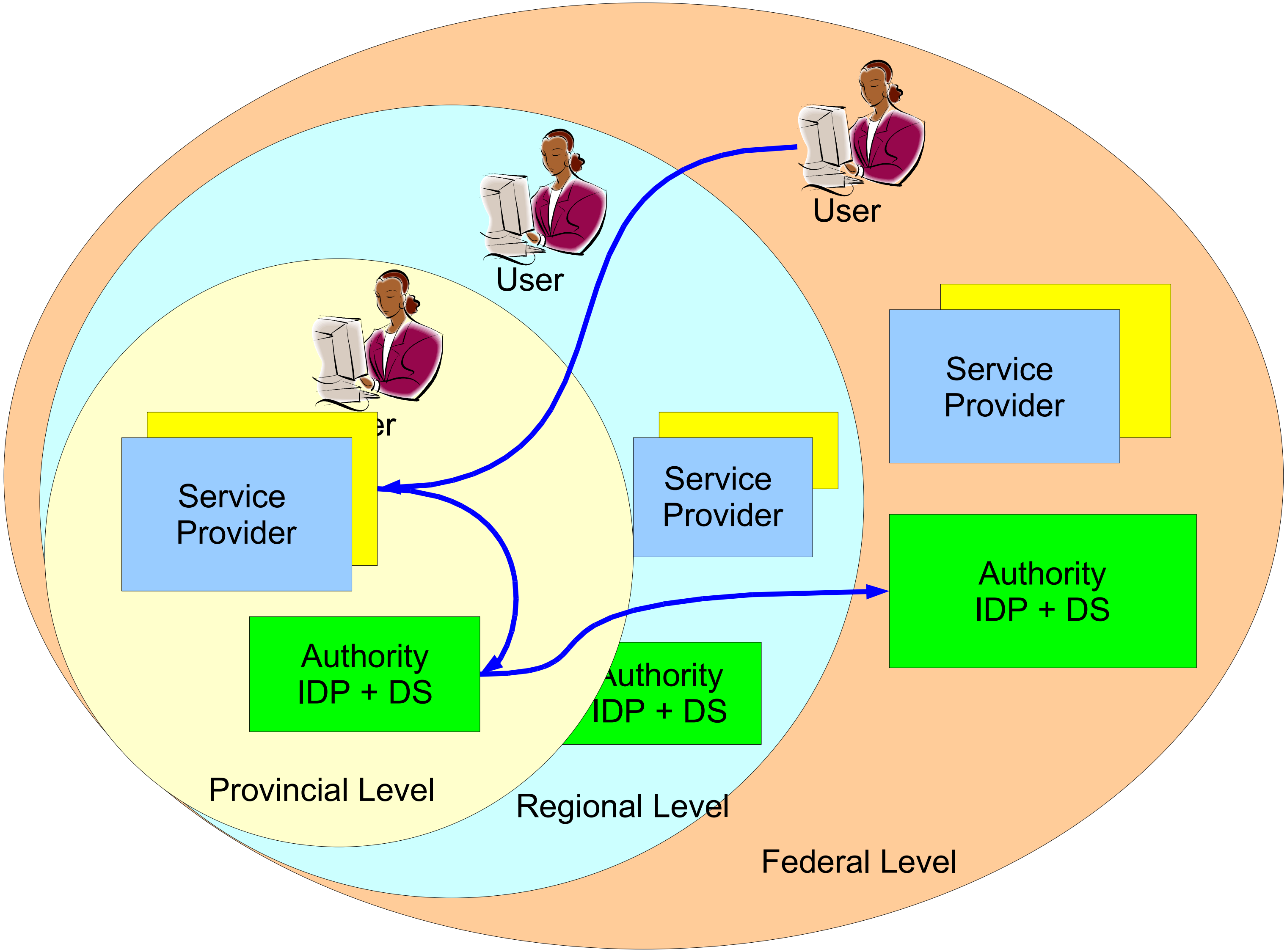
CoT Peering (Roaming user/service)



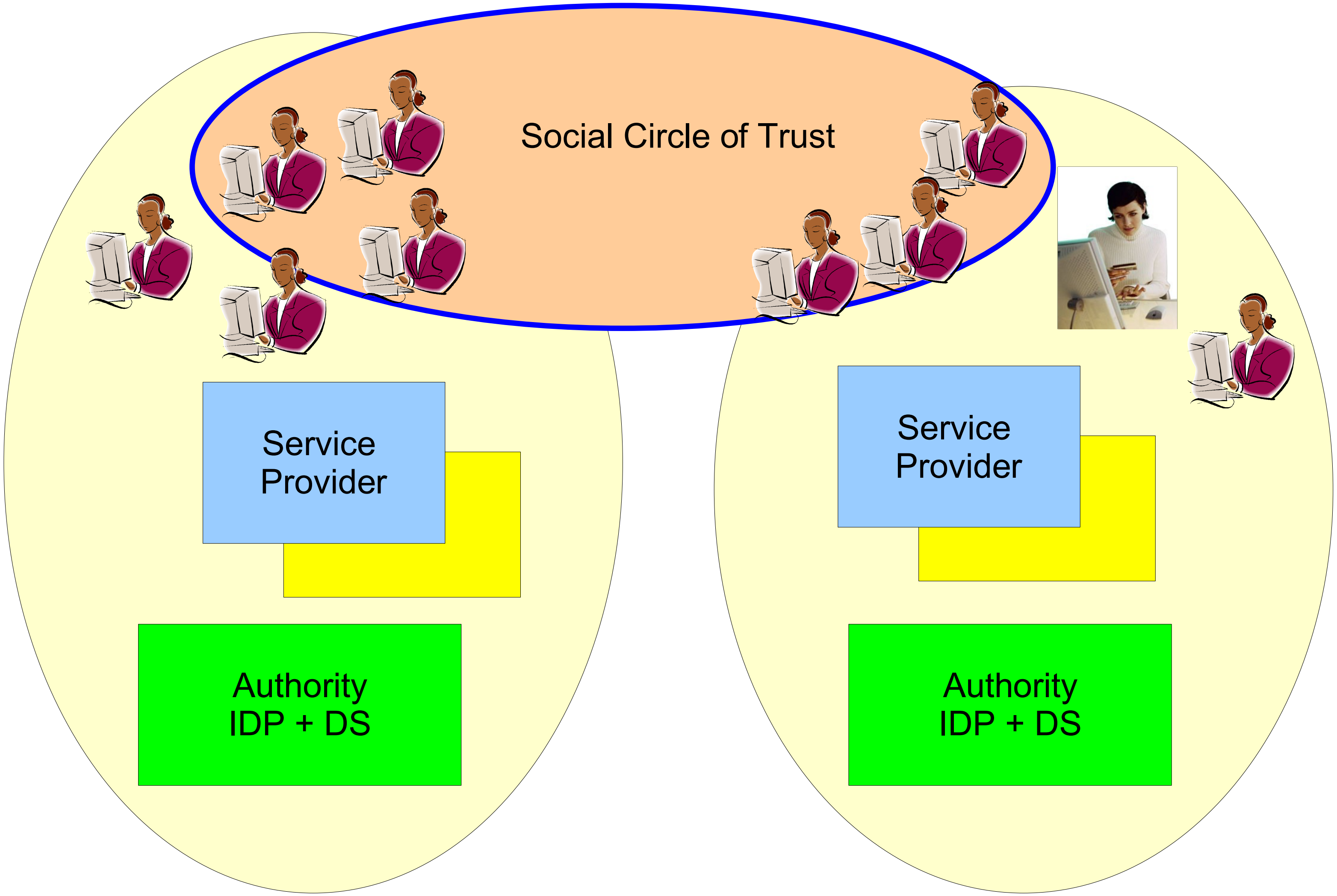
Partner CoT

My CoT

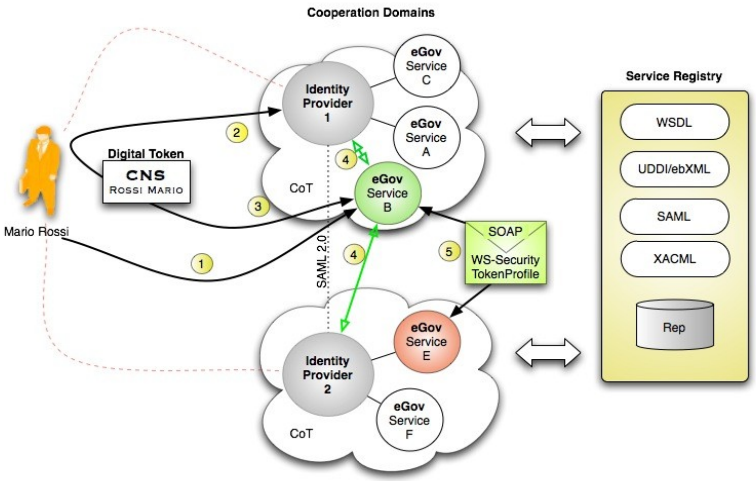
Hierarchies of CoT



Social Networking & Cross ID



Technology is Mature



mon.Service-Public.fr

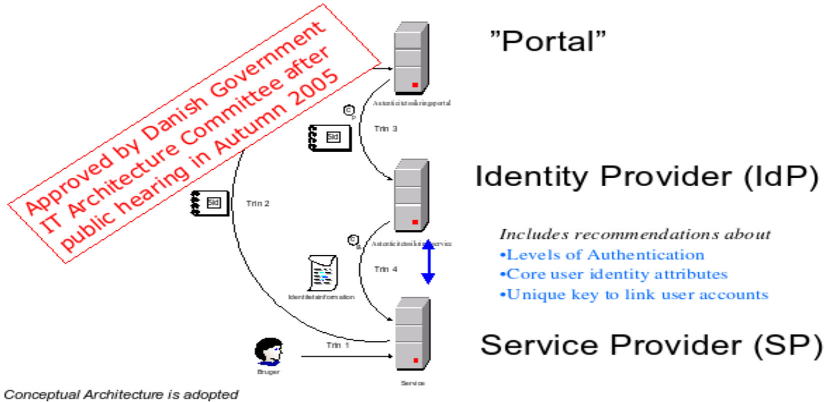
Le projet de portail Mon.Service-Public.fr doit permettre à l'usager - personne physique ou morale - l'accès à une gamme cohérente et étendue de services dans un environnement personnalisé, et ce dans des conditions permettant de créer la confiance.
Une version pilote a été développée et testée par 500 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 ID-WSF 1.1

Nokia 3250 Nokia 5500 Nokia 6290 Nokia E50

Nokia E61 Nokia E62 Nokia E70 Nokia N71

Reference Architecture for Cross-organizational Single Sign On


Approved by Danish Government IT Architecture Committee after public hearing in Autumn 2005
"Portal"
Identity Provider (IdP)
Service Provider (SP)
Trin 1
Trin 2
Trin 3
Trin 4
Bruger
Service

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

Conceptual Architecture is adopted from US Federal e-Authentication initiative

SAML 2.0 is the recommended federation standard

Liberty Alliance

Fulup Ar Foll

fulup@sun.com