Why Federation

- External Employee
- Internal Employee
- External IDP
- External Private Services
- External Shared Services
- Internal Shared Services
- Internal Private Services
- Attributes Exchange
- Public Owned Service
- Public Shared Service
- Anonymous Customer
- Account Owner
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 wherever customer want

<table>
<thead>
<tr>
<th>Actor</th>
<th>Must have relation with</th>
<th>Must know Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customer:</strong></td>
<td>vendor, shipping, bank</td>
<td>products(choose), price(accept), delivery address (choose/select)</td>
</tr>
<tr>
<td><strong>Shop:</strong></td>
<td>payment, shipping</td>
<td>price (own), product (from customer)</td>
</tr>
<tr>
<td><strong>Shipping:</strong></td>
<td>shop</td>
<td>delivery address (from customer)</td>
</tr>
<tr>
<td><strong>Payment:</strong></td>
<td>shop, bank</td>
<td>price(from shop), bank(from customer)</td>
</tr>
<tr>
<td><strong>Bank:</strong></td>
<td>payment, customer</td>
<td>price (from payment), bank account(own)</td>
</tr>
</tbody>
</table>
Liberty Self Contain Circle of Trust

Service Provider (outsourced)

Service Provider (internal)

Attribute Provider (outsourced)

Attribute Provider (Internal)

Authority
IDP + DS

Repository

User to Application
(Federation zone)

Application to Application
(Identity WebService zone)

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

Service Provider

Authority IDP + DS

User

Service Provider

Authority IDP + DS

User

Service Provider

Authority IDP + DS

Federal Level

Regional Level

Provincial Level
Social Networking & Cross ID

Social Circle of Trust

Service Provider

Authority IDP + DS

Service Provider

Authority IDP + DS
Technology is Mature

Liberty Alliance ID-WSF 1.1

Nokia 3250  Nokia 5500  Nokia E290  Nokia E50

Nokia E61  Nokia E62  Nokia E70  Nokia N71

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)

SAML 2.0 is the recommended federation standard

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

Fulup Ar Foll
fulup@sun.com