Liberty Alliance concepts
applied to
Mon Service Public

Liberty Alliance Deployment Workshop

December 7th, 2005
Agenda

1. What is Mon Service Public?
   • Key features

2. Mon Service Public & Liberty Alliance
   • How it works
   • How it will work
   • How it should work

3. Next steps
   • Proof of Concept
   • Full service
What is Mon Service Public ?
The personalized service “Mon service-public” will be accessible from the service-public.fr portal. It will enable every citizen to set up his or her own home page to access all the online public services of concern to him or her. Users will thus be able to access all their official paperwork.

"Mon service-public" will incorporate the services developed by the administrations (taxes account, family benefits, etc…) and those developed by the ADAE (change of address, applications for certificates from the civil register, etc…).

A "personal space" (briefcase / e-safe) can be used for storage of personal data and dematerialized official documents (diplomas, civil register certificates, etc…) which the user can obtain from the civil service and submit to the authorities to complete other procedures.
What is Mon Service Public?

Key features
What does it really mean?

To set up an Identity Management Architecture for all eGov services

Redesign the communication and interaction between citizens and administration
Audience of the service

- **The Mon Service-Public portal is dedicated to**
  - **Users, that will use this service for their interactions with Government**
    - Citizen (all of them *may* use the service, nobody *has to*)
    - Companies (especially small businesses)
    - Associations
  - **MSP partners, providing users with services**
    - Ministries
    - Social services
    - Local administrations (Counties, towns)
Building and using one’s eIdentity & Sharing one’s attributes
Créer mon espace emploi

Mes coordonnées

Ces données sont confidentielles. Elles sont uniquement consultables par les agents de l'ANPE pour faciliter vos démarches. Conformément aux dispositions de la loi Informatique et Libertés du 6 janvier 1978, vous disposez d'un droit d'accès, de modification, de rectification et de suppression des données qui vous concernent. En validant cet état, vous vous engagez à respecter les conditions d'utilisation du site.

Je saisir mon espace emploi

* Obligatoire

Je saisir mes coordonnées

* Célibataire

* Madame

* Mademoiselle

* Monsieur

Nom

Prénom

Mes coordonnées postales

* Pays FRANCE

* Adresse

Complément d'adresse

(ex. tour Mirabelle)

Code postal

Commune

Acheminement postal

(ex. boîte postale, cedex)

Mes autres modes de contacts

Merci de préciser un ou plusieurs moyens de contact (la saisie d'un numéro de téléphone est nécessaire pour les télecandidatures)

* Telephone portable

* Téléphone fixe

Je choisis :

Adresse e-mail

Je souhaite recevoir mes informations dans mon Service Public

Je veux associer ce compte à mon Service Public

Pour + d'information

Abandonner Valider
Créer mon espace emploi
Mes coordonnées

Ces données sont confidentielles. Elles sont uniquement consultables par les agents de l'ANPE pour faciliter vos démarches. Conformément aux dispositions de la loi Informatique et Libertés du 6 janvier 1978, vous disposez d'un droit d'accès, de modification, de rectification et de suppression des données qui vous concernent. En validant cet écran, vous vous engagez à respecter les conditions d'utilisation du site.

Pour accéder à votre espace de données, vous devez préalablement vous authentifier :

Identifiant
Mot de passe

Autres moyens d'accès

Je choisis :
- Adresse e-mail
- Je souhaite recevoir mes informations dans mon Service-Public

Je veux associer ce compte à mon Service-Public

Pour + d'information

Abandonner | Valider
Créer mon espace emploi

Mes coordonnées


* Obligatoire

Je saisir mes coordonnées

* Civi*late ✓ Madame ○ Mademoiselle ○ Monsieur

* Nom  [ ] [ ] [ ] [ ] [ ]

* Prénom  [ ] [ ] [ ] [ ] [ ] [ ] [ ]

Mes coordonnées postales

* Pays  FRANCE

* Adresse  [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] rue [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ }
Mon Service Public and Liberty Alliance
Why Liberty Alliance?

- Mon Service Public may give access to all services provided by Administrations.
  - Need SSO based on federated identity
  - Need shared authentication

- Main constraints
  - Respect for Privacy
  - Free choice of how to identify oneself
  - CNIL (National Commission for Data Protection) and French law considerations
  - User control of personal data
  - Open specifications and infrastructure (impact on all public services)
Identity Federation Use Cases

Authentication

One MSP account / several authentication ways (user / pwd, SMS challenge, smartcard)

One authentication way can be used for only one MSP account

Federation with different kinds of eGov accounts

Several MSP accounts can federate the same identity on the same service

Services provided by administrations

Assurance maladie
- Personal account M Dupont- N° 85651
- Personal account Mme Durand- N° 65482

Remboursements
- Personal account Mme Durand- N° 88888

Formulaires
- Personal account Mme Durand- N° 88888

URSSAF
- Cotisations sociales
  - Business account Société 1-N° 15646746

Impôts
- Compte fiscal
  - Family account Durand Dupont- N° 654832

ADAE
- Changement d'adresse
  - Procedure Id N° 694125
Dealing with multiple CoTs

Sharing one’s identity at both national and local levels

- Multiple portals will coexist. MSP will only be one of them. And yet, the users need simplified access to both national and local services, whichever Circle of Trust (CoT) they belong to:
  - How many IdPs? How many CoTs?

- We challenged several possible models:

  **Dealing with multiple CoTs**

  **Multiple portals will coexist. MSP will only be one of them. And yet, the users need simplified access to both national and local services, whichever Circle of Trust (CoT) they belong to:**
  - How many IdPs? How many CoTs?

  **We challenged several possible models:**

  **General architecture:**
  - One Service Provider only belongs to one CoT
  - There will be “gateways” between CoTs so that user identity can be shared between different CoTs
What needs to be solved
What still needs to be defined

- Creating **Groups** and sharing attributes between them
  - Shared documents within an user’s eSafe

- Ergonomics – Early users feedback
  - “I don’t understand who you will give my documents to! Why should I leave all my personal information to you?” or “You know me, why isn’t this all automatic?”
  - Does the user really **have to** deal with identity concerns?
  - Does the user have to know who is in charge of managing his identity?
  - How can we explain these concepts to the average user of our systems!
  - Simplifying means Provisioning

- Ways to use federation for **communicating** with the user
  - Email address = new UID?
  - The administrations may send information to the user (through MSP) without knowing his address or MSP identity
  - How federation keys could provide an indirection in the communication between citizen and administration?
  - Consistency with LA messaging workgroup

- Interconnecting CoTs
  - Need of a standardized architecture
Next steps – Deployment issues
From a strategic view to a live system

- **Q1 2004**: Defining the strategy
  - First MSP “big picture”

- **Q4 2005 - Q1 2006**: Testing the POC
  - Operational system (LA implemented on 2 IdPs and 5 SPs)
  - Tested by 500 users

- **Q2 2007**: MSP 1.0
  - Live system connected to several SPs
  - Real data and transactions

- **2007 and beyond**: MSP used by millions of people
  - Extending the CoT; partnerships. Increasing the number of users
Deployment

- It takes a long time to define an identity management architecture
  - which will be available for a large number of citizens
  - which will involve a large number of organizations and legacy systems
- Proof of Concept is crucial
  - to test users’ appetite and reactions
  - to test ergonomics
  - to test the implementation of the concepts

- The way we worked / work
  - Pilot (POC)
    - Main contractor: France Telecom (involving R&D)
    - Using two open source / free LA frameworks: SourceID, LASSO (ID-FF1.2, ID-WSF)
    - We provide the SPs with a LA “toolkit” in order to ease integration
  - Live System
    - We managed multiple workgroups with representatives of ministries, civil services, CNIL…
    - Either at a technical and organizational scale
    - Contract and technical choices to be defined Q1 2006
    - Currently designing the services list, building the CoTs
Want to know more?
→ Contact ADAE

:: Benoît BOUTE ::
Project Leader, Mon Service Public

+33 (0)1 42 75 82 56
benoit.boute@pm.gouv.fr