

« Gestion et fédération des identités »

Fédération de cercles de confiance

Solution Linux 2008 – 30 janvier 2008



AVEC VOUS l'administration
SE MODERNISE
www.modernisation.gouv.fr



Contexte et enjeux

■ Une volonté politique :

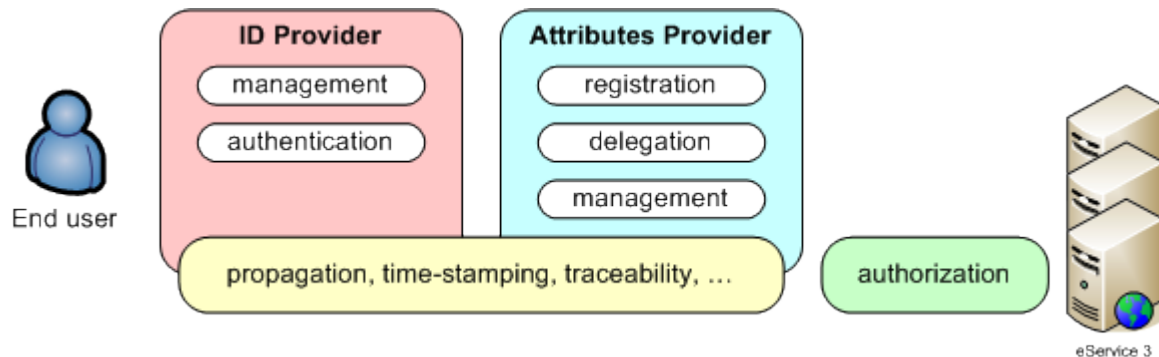
- « *Simplifier la vie des usagers* » en standardisant les modes d'accès et la gestion des droits d'accès
- « *Valoriser les missions des Agents* » en encourageant la polyvalence par un enrichissant des périmètres d'intervention
- « *Améliorer l'efficacité des services publics* » en mutualisant les investissements et en réduisant les délais de mise en œuvre

■ Mais l'accès aux SI reste à simplifier :

- (Re)Connaître les usagers de services en ligne
- Limiter l'accès aux seuls services en ligne autorisés
- Garantir l'accès avec des conditions adaptées de sécurité et de légitimité, de confidentialité et de traçabilité *code pénal et la loi du 6 Janvier 1978 et décret du 24 mars 2006 du code des postes et des communications électroniques*

Au delà de l'authentification ...

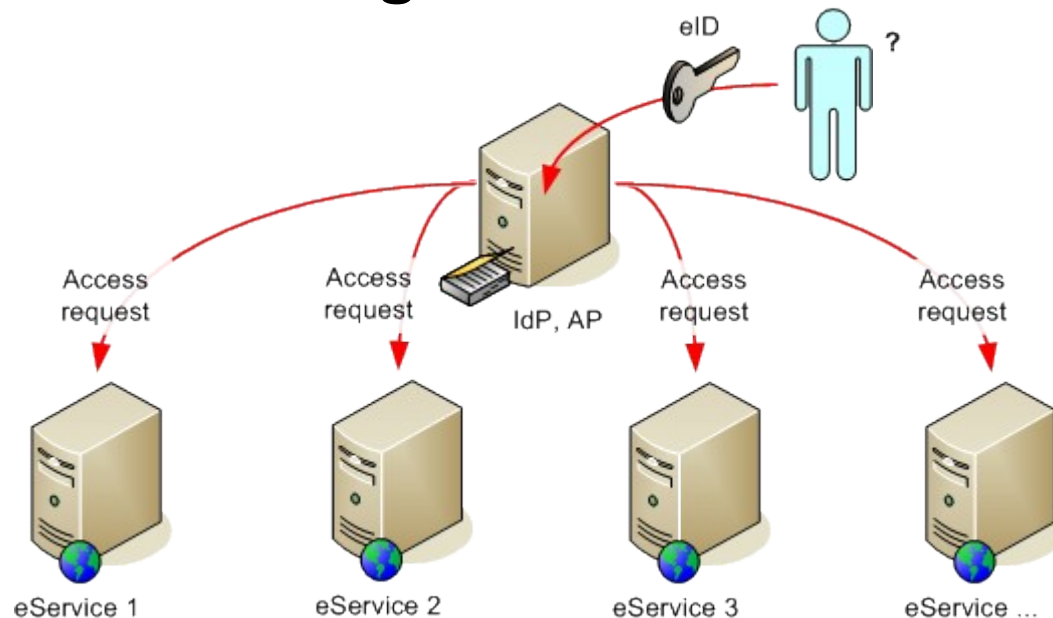
- **Un principe** « *un usager utilise un service, pour son propre compte ou celui d'un tiers, selon certaines modalités* »
- **Qui se résume par** « *[qui][quoi][pour qui][comment]* »
- **Une véritable offre de services pour l'utilisateur qui s'appuie sur une infrastructure :**
 - De gestion de comptes utilisateur *[qui][pour qui]*
 - De gestion de droits d'accès aux services en ligne *[pour qui][comment]*
 - De contrôle d'accès aux services en ligne *[quoi]*
 - Assurant la traçabilité des actes



La volonté d'abandonner les multiples points d'accès est principalement orientée vers l'utilisateur personne physique

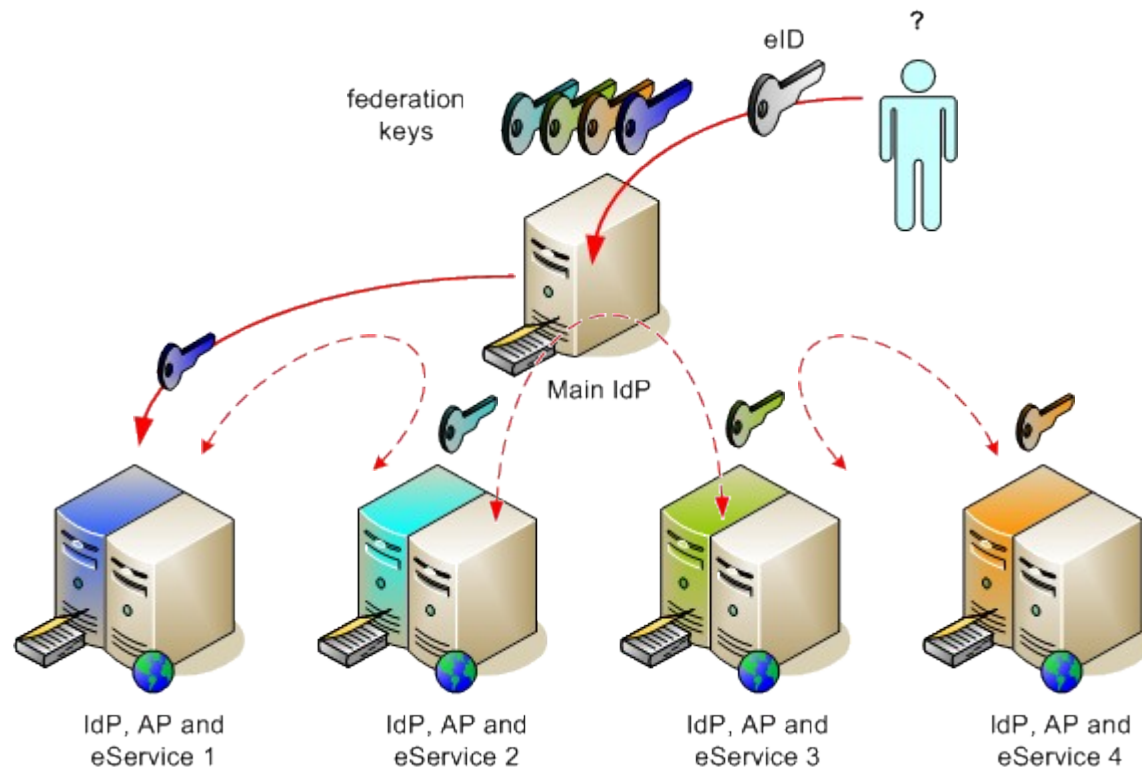
Un point d'accès unique ... le mode SSO

- Le fournisseur de services héberge les *Espaces de Confiance*
- Inscription auprès de l'offreur de services en ligne ou enrôlement SIRH par sa structure d'appartenance
- Possibilité de déléguer ses droits d'accès



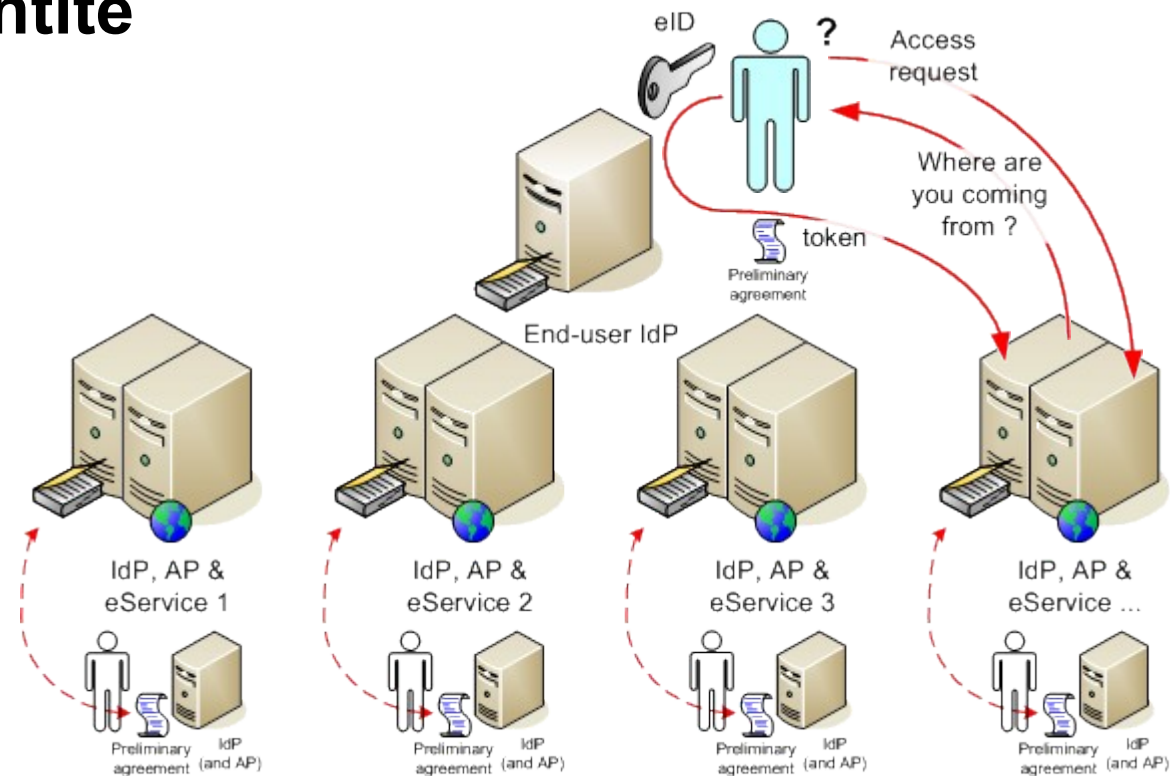
Fédération d'Identités

- Le fournisseur d'identités principal héberge les clés de fédération ... fédération initiée par l'utilisateur
- Anonymat et respect des identifiants sectoriels



Reconnaissance auprès de son IdP favori

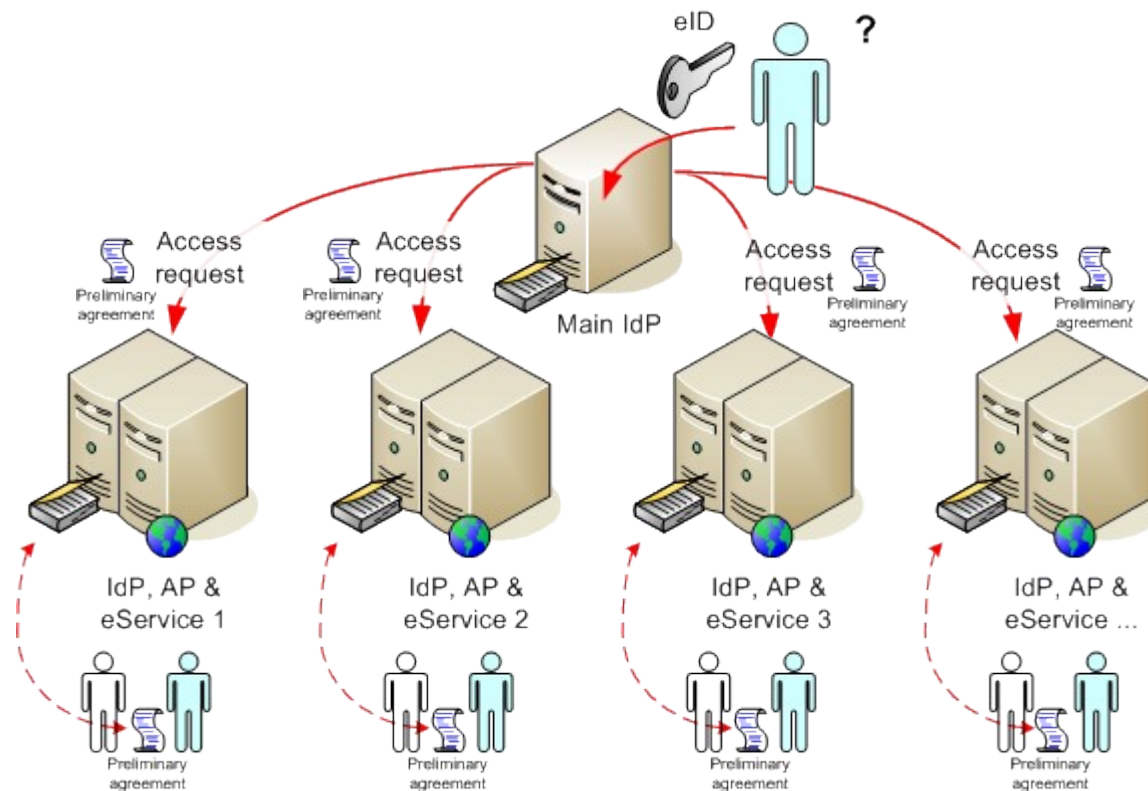
- Une convention décrit les modalités techniques, fonctionnelles et organisationnelles d'accès aux services en ligne
- L'utilisateur s'authentifie auprès de son fournisseur d'identité



**Et l'ouverture des SI par la
reconnaissance mutuelle
entre organismes ?!!!**

Reconnaissance mutuelle entre organismes

- Une convention décrit les modalités techniques, fonctionnelles et organisationnelles d'accès aux services en ligne
- L'utilisateur est authentifié par son organisme



Les modalités ...

- **Les modalités techniques :**
 - Serveur : d'où vient l'assertion ?!!
 - Certificats ... de chiffrage / de signature
 - Durée de vie de l'assertion ... Serveur d'horodatage
- **Les modalités fonctionnelles :**
 - Schéma de l'assertion et version de l'assertion
 - Attribut(s) reconnus
 - Niveau d'authentification requis
- **Les modalités organisationnelles :**
 - Signature de la convention entre services juridiques
 - Périodicité des audits
 - Cadre juridique d'accès aux traces

Les traces ...

- **Traçabilité** : « aptitude à retrouver l'historique d'un événement » (définition ISO)
- **Une obligation légale** :
 - texte du 24 mars 2006 du code des postes et des communications électroniques
- **Mise en œuvre de** :
 - traces côté « consommateur de services »
 - traces côté « fournisseur de services »
- **Un cadre contractuel permettant de savoir et précisant** :
 - Qui a demandé à faire « quoi / pour qui » côté « consommateur de services »
 - Les accès « à quoi / pour qui » côté « fournisseur de services »
 - Les modalités d'audit (fréquence, sur alerte, ...)

Standards, bonnes pratiques et solutions

- **SAML** <http://www.oasis-open.org/home/index.php>
- **Un point d'accès unique ... le mode SSO**
 - **lemonLDAP** <http://wiki.lemonldap.objectweb.org>
- **Fédération d'identités**
 - <http://www.projectliberty.org>
 - **federID** <http://federid.objectweb.org>
- **Reconnaissance auprès de son IdP favori**
 - **openID** : <http://openid.net>
 - **Shibboleth** : <http://shibboleth.internet2.edu>
- **Reconnaissance mutuelle entre organismes**
 - **INTEROPS** http://synergies.modernisation.gouv.fr/article.php?id_article=508

Merci ...

« Gestion et fédération des identités »

Fédération de cercles de confiance

Solution Linux 2008 – 30 janvier 2008

contact : bruno.deschemps@finances.gouv.fr

