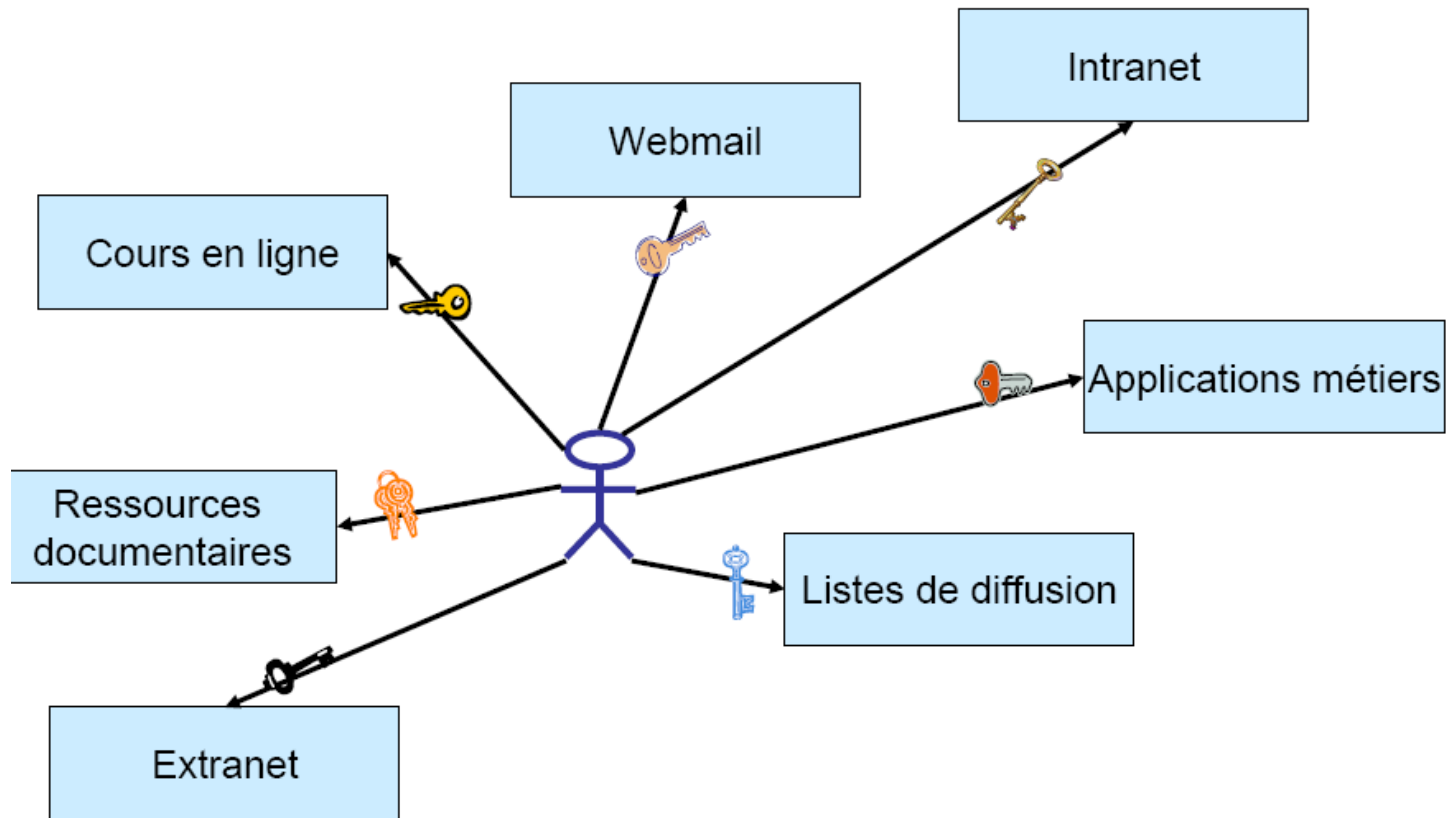


# Journée Shibboleth CRU – 25/01/07

- **Matin 9h30 - 12h30 :**
  - **Présentation de Shibboleth** : intérêts, fonctionnement, intégration dans un SI d'établissement
  - **Présentation de la fédération du CRU** : fonctionnement, responsabilités des membres, utilisation dans le cadre UNR
  - **Le fournisseur d'identités virtuel**
  - **Évolutions techniques de la fédération du CRU** : attributs, ergonomie, interopérabilité Liberty Alliance et Shibboleth + relation avec *eduroam*
- **Après-midi 14h - 17h :**
  - **Déploiement de Shibboleth dans les universités bordelaises**
  - **Fédération d'identités à l'Université de Bretagne & Salles carrefour**
  - **Retour sur l'expérimentation Couperin-SDB-ABES-CRU**
  - **Utilisation de la fédération du CRU pour le portail Sudoc et les services de l'ABES**
  - **Opérations MIPE**

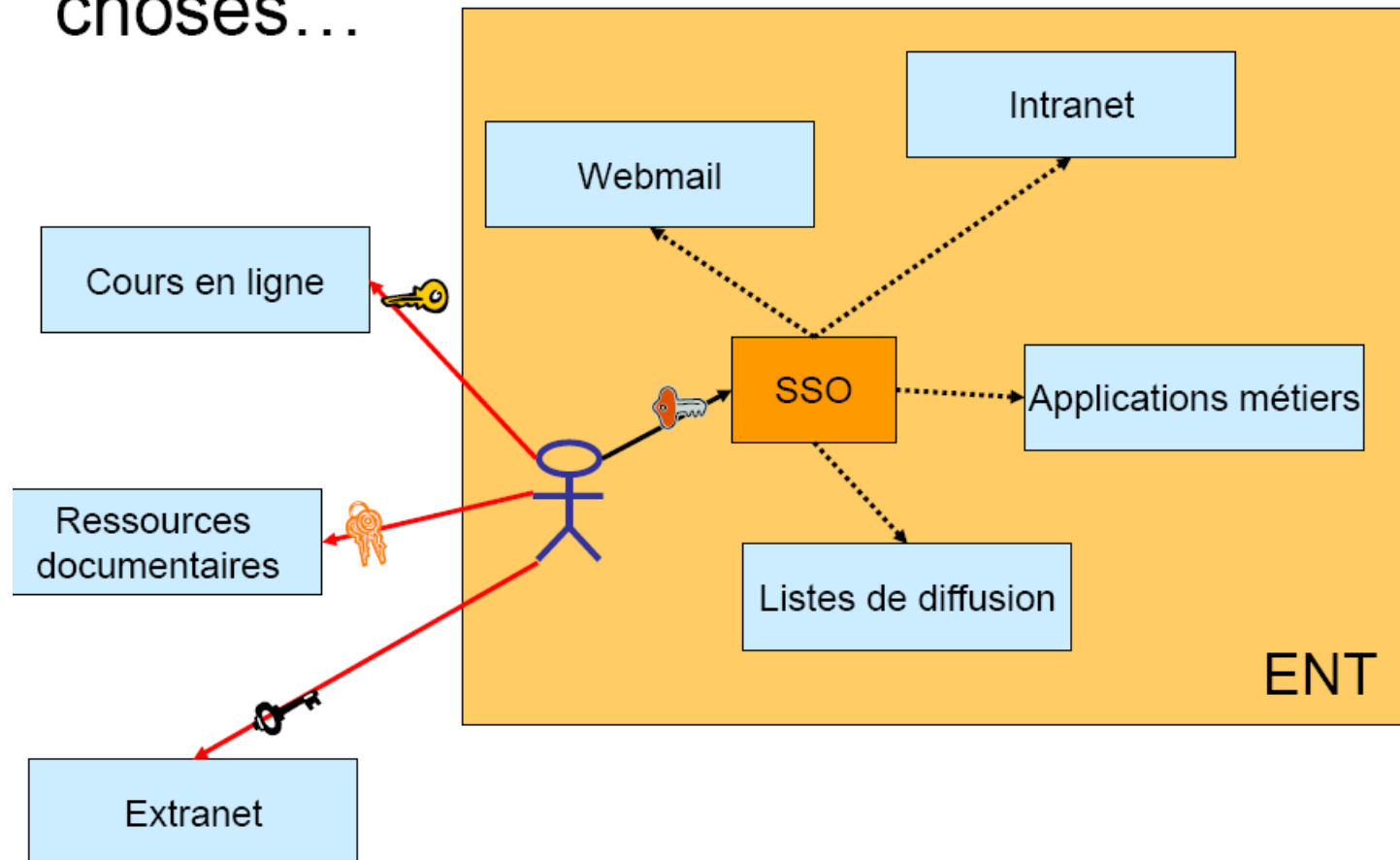
# 1 - Présentation de Shibboleth

Beaucoup de ressources web,  
autant de mots de passe



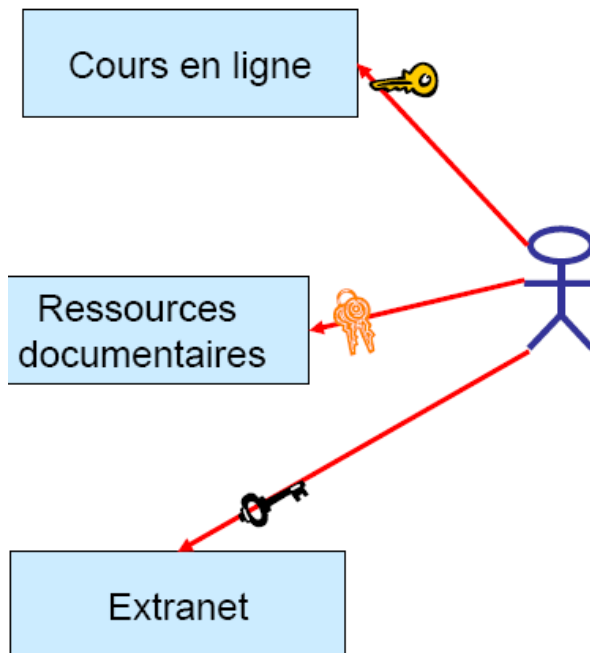
# 1 - Présentation de Shibboleth

La démarche ENT a amélioré les choses...



# 1 - Présentation de Shibboleth

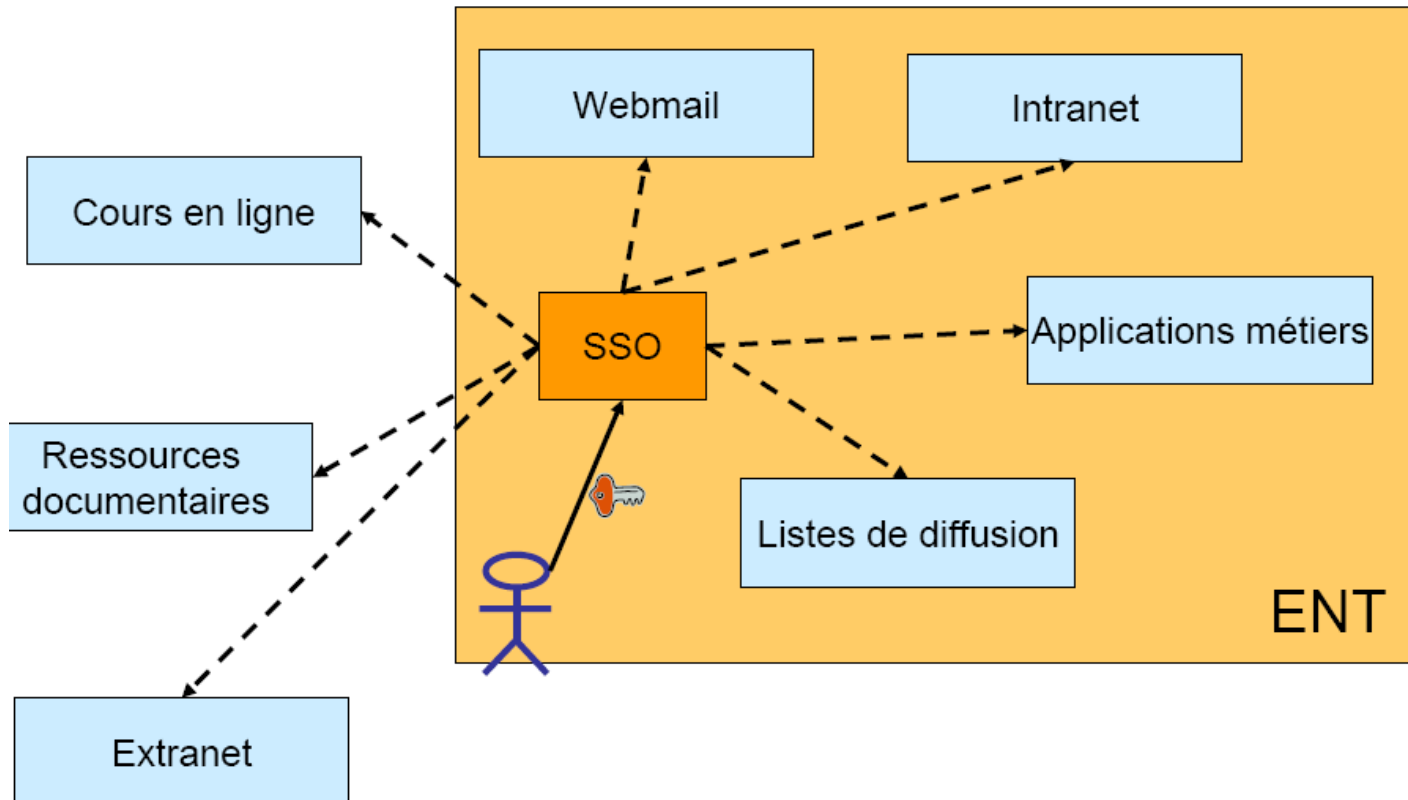
Comment authentifier des utilisateurs quand on ne les gère pas ?



- Le compte invité
  - Un seul mot de passe pour tout le monde
- L'identification du poste
  - L'enfer des plages d'adresse IP
- L'enregistrement local
  - Un effort démesuré
- Le méta-annuaire
  - Un seul ne suffira pas

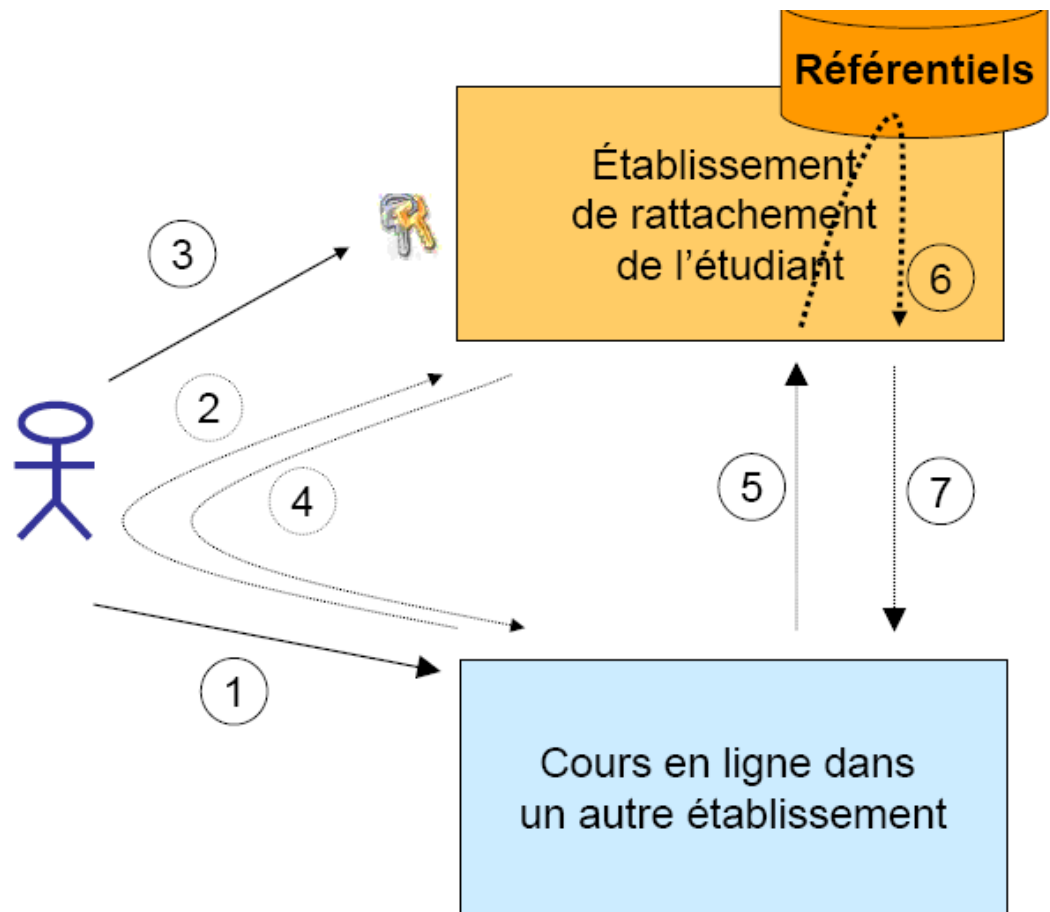
# 1 - Présentation de Shibboleth

La fédération d'identités doit permettre de rendre ces accès simples et sûrs



# 1 - Présentation de Shibboleth

1. Tentative d'accès à la ressource
2. Redirection vers le SSO de l'établissement de rattachement
3. Authentification sur le SSO
4. Redirection vers la ressource avec une **preuve d'authentification**
5. Demande d'attribut sur l'utilisateur
6. Extraction des attributs
7. Propagation vers la ressource



# 1 - Présentation de Shibboleth

## Fonctionnement du WAYF

Veillez sélectionner votre établissement ...

- Cellule technique du CRU
- INSA de Lyon
- INT test
- IUFM de Bretagne 1.3
- UCBL nov 2006
- UPMC
- Université de Artois
- Université de Bordeaux

**Service central d'authentification**

Vous souhaitez accéder à un service qui nécessite une authentification.

Entrez votre nom d'utilisateur et votre mot de passe puis cliquez sur le bouton **Connexion** ci-dessous pour continuer.

Utilisateur :

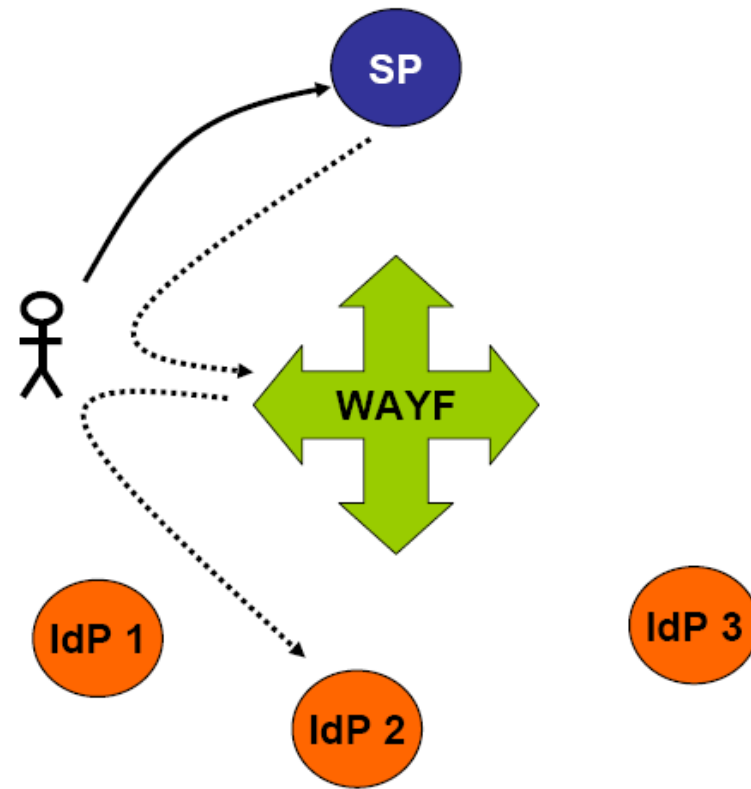
Mot de passe :

Je n'ai pas encore de compte à l'Université Paris 1.

*Pour des raisons de sécurité, fermez votre navigateur web après avoir accédé aux services protégés !*

Méfiez-vous de tous les programmes et pages web qui vous demandent de vous authentifier. Les pages web de l'Université de Paris 1 vous demandent votre nom d'utilisateur et votre mot de passe sur des URL de la forme <https://www.univ-paris1.fr/>. De plus, votre navigateur doit indiquer que vous accédez une page sécurisée.

[Université de Paris 1](#)



# 1 - Présentation de Shibboleth

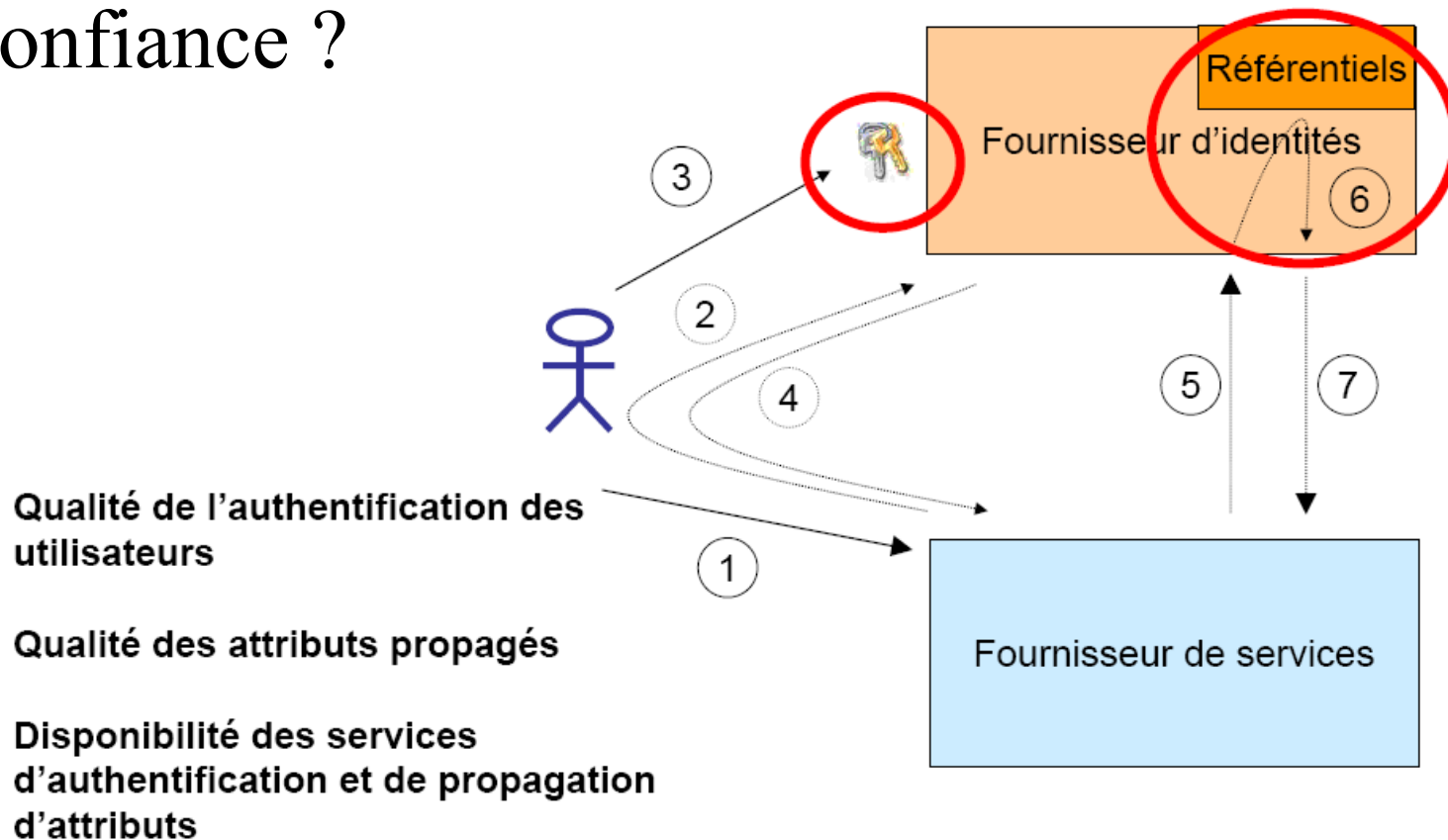
## Apports de la fédération d'identités

- Pour l'utilisateur
  - Il n'utilise que le mot de passe de son SSO
  - Adapté aux utilisateurs nomades
- Pour l'établissement de rattachement
  - Niveau de sécurité constant (SSO)
  - Meilleure maîtrise des données personnelles
- Pour les gestionnaires de ressources
  - Plus besoin de gérer des comptes utilisateurs
  - Accès à des données utilisateurs fiables



## 2 - Présentation de la fédération du CRU

Confiance ?

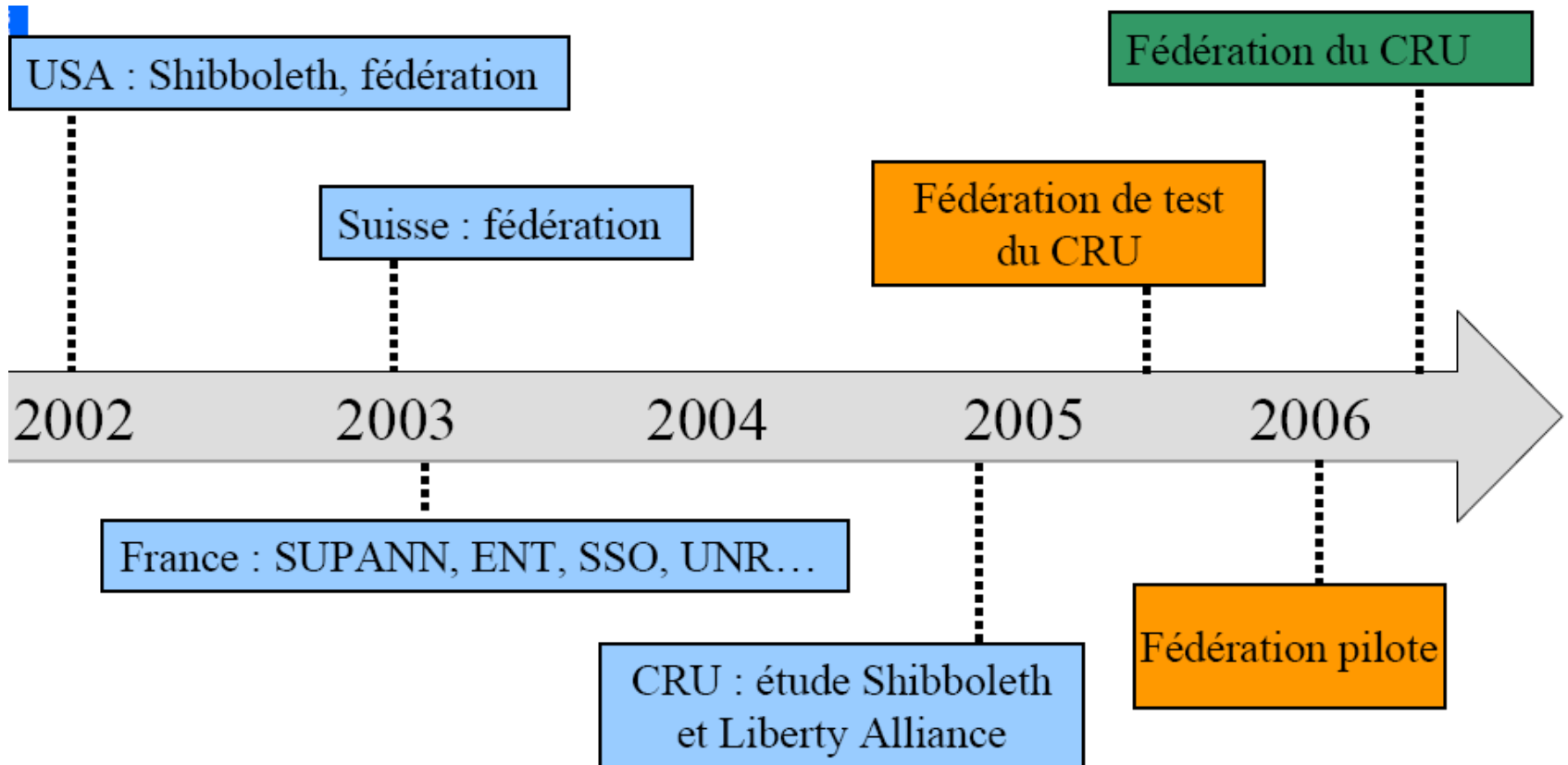


## 2 - Présentation de la fédération du CRU

~ Une fédération permet de mutualiser un niveau de confiance

- Fédération = ensemble de fournisseurs d'identités et de fournisseurs de services
- Pour intégrer la fédération, chacun s'engage à respecter un niveau minimal de pratiques
- On évite ainsi la multiplication d'accords bilatéraux

## 2 - Présentation de la fédération du CRU



## 2 - Présentation de la fédération du CRU

### Les membres de la fédération du CRU

- Fournisseur d'identités
  - établissements d'enseignement supérieur
- Fournisseurs de services
  - établissements d'enseignement supérieur
  - autre organismes publics
  - entreprises
- Le CRU

# 2 - Présentation de la fédération du CRU

## Conditions d'inscription Fournisseur d'identité

- . Prendre connaissance de la politique de la fédération du CRU  
<http://federation.cru.fr/cru/references/index.html>
  - . Installer et tester Shibboleth au sein de la fédération de test
  - . Adhérer à la fédération en signant la convention d'inscription
- Nommer un contact organisationnel et un contact technique
  - Utiliser un produit compatible Shibboleth
  - Sécuriser son environnement logiciel (SSO, ENT, annuaire)
  - Respecter le nommage des attributs définis au sein de la fédération
  - Formaliser les processus de gestion de l'annuaire
  - Journaliser les connexions des utilisateurs au SSO
  - Respecter la législation sur la protection des données à caractère personnelle

## 2 - Présentation de la fédération du CRU

Conditions d'inscription

Fournisseur de service

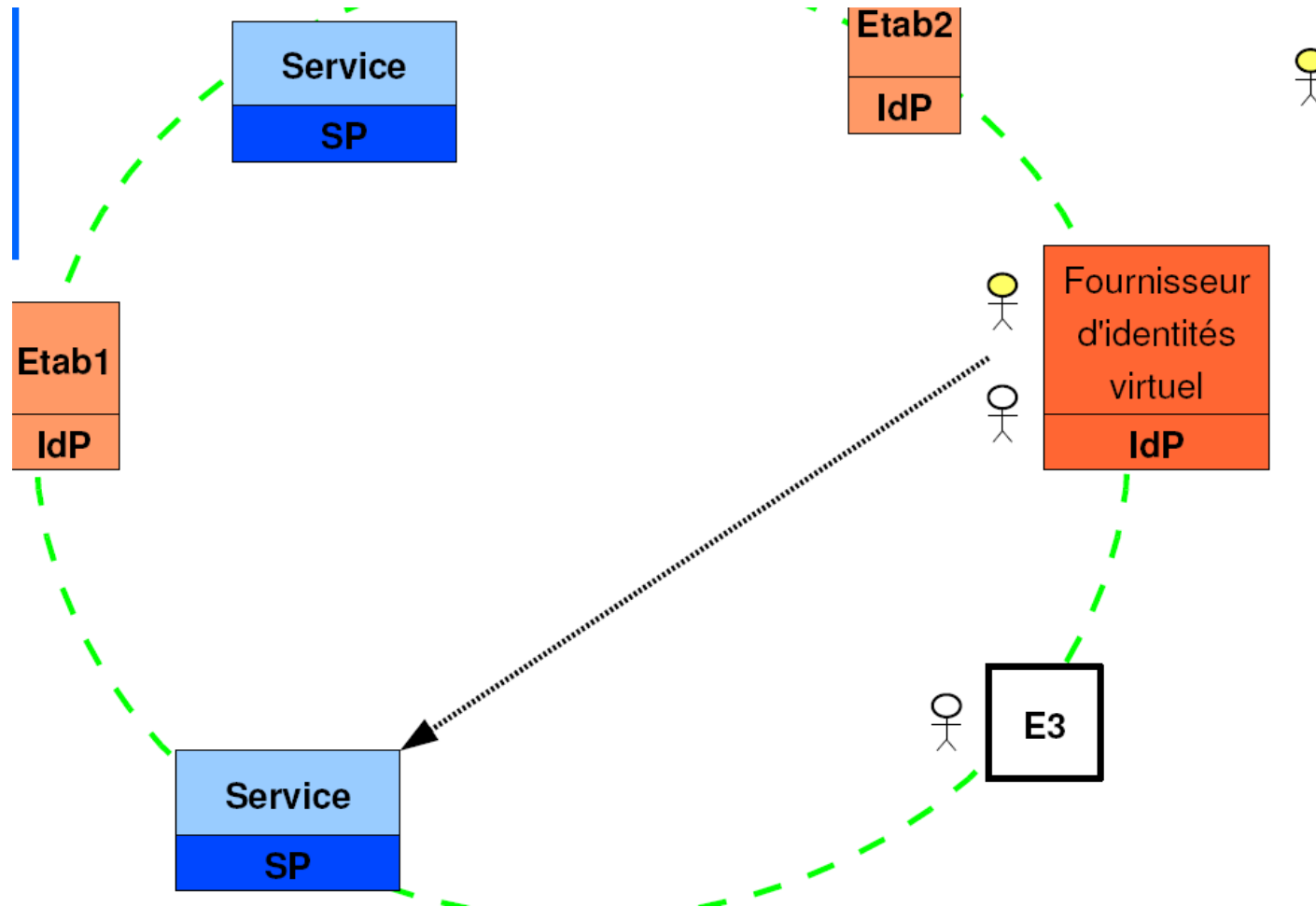
- Respecter le nommage des attributs définis au sein de la fédération
- Formaliser les processus de gestion de l'annuaire
- Journaliser les connexions des utilisateurs au SSO
- Respecter la législation sur la protection des données à caractère personnelle

## 2 - Présentation de la fédération du CRU

### Fédération du CRU et UNR

- La fédération du CRU a une échelle nationale
- Mais le niveau de sécurité de la fédération du CRU est générique et est défini pour correspondre aux besoins des établissements
- Et chaque fournisseur est libre de coopérer avec les fournisseurs de son choix
- On peut donc utiliser la fédération du CRU pour des besoins uniquement régionaux ou locaux

# 3 – Le fournisseur d'identité virtuel





# 3 – Le fournisseur d'identité virtuel

## Les 2 fonctions du fournisseur d'identités virtuel

### I. **Authentification** :


**Création et gestion d'identités** viables pour la fédération :

- Aux personnes ne faisant pas partie d'un des établissements de l'enseignement supérieur;
- Aux personnes dont les établissements n'ont pas encore installé les briques Shibboleth ;

### II. **Autorisation** :


**Création et gestion de groupes** d'utilisateurs selon leurs activités communes.

# 3 – Le fournisseur d'identité virtuel



## Fournisseur d'identités virtuel

---



Bonjour john1 Smith1

Déconnexion

[Mon Profil](#)

[Mes Groupes](#)

[Créer un groupe](#)

---

Chercher un groupe

---

→ Le gestionnaire d'identité sera votre outil de création d'une identité au sein de la fédération d'identité et de gestion de vos futurs groupes.

→ Le GIC vous permettra en effet de créer ou de vous abonner à des groupes vous permettant alors d'accéder à des ressources des établissements de l'enseignement supérieur.

→ Ici vous pourrez également modifier vos données personnelles.

→ Si vous souhaitez rechercher des groupes, vous créer un compte ou accéder à votre compte déjà existant, référez vous au menu en haut à gauche ou pour de plus amples informations, au menu navigation à gauche.

---

© CRU, Copyright 2006.

## 3 – Le fournisseur d'identité virtuel

<http://federation.cru.fr/FIV/index.html>

Date d'ouverture du service : **Mars 2007**

# 4 – Evolutions techniques de la Fédé. CRU

## Donner le contrôle de la diffusion d'attributs aux utilisateurs

**SWITCH***aai*  
[About AAI](#) : [About ID Card](#) : [FAQ](#) : [Help](#) : [Privacy](#)

This is the Digital ID Card to be sent to 'https://aai-rr.switch.ch':

Digital ID Card	
Surname	<b>Lenggenhager</b>
Given name	<b>Thomas</b>
Unique ID	<b>124758@switch.ch</b>
Home organization	<b>switch.ch</b>
Home organization type	<b>others</b>
Affiliation	<b>staff</b>
E-mail	<b>lenggenhager@switch.ch</b>

Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.

Please send your comments to this page to [aai@switch.ch](mailto:aai@switch.ch)

## 4 – Evolutions techniques de la Fédé. CRU

### Faciliter la gestion de la diffusion des attributs pour un IdP

- Pour un IdP, gestion fastidieuse de la diffusion des attributs pour beaucoup de SP (fichier arp.site.xml)
- Le CRU proposera une génération automatique d'un arp.site.xml en fonction des besoins des fournisseurs de service

## 4 – Evolutions techniques de la Fédé. CRU

# Il est possible d'éviter le WAYF

- Depuis un ENT, le passage par le WAYF pour accéder à une ressource extérieure est une gêne pour l'utilisateur
- Il est possible d'éviter le WAYF en utilisant des URL spéciales d'accès aux ressources

## 4 – Evolutions techniques de la Fédé. CRU

### Utiliser des certificats sans « pop-up »

- Les fournisseurs d'identités et de services utilisent des certificats serveur X.509
- Les certificats « maison » ou de l'IGC du CRU peuvent provoquer l'apparition de messages d'avertissement lors de l'utilisation de Shibboleth
- Le CRU met à disposition des certificats sans cet inconvénient, voir

[www.cru.fr/wiki/scs](http://www.cru.fr/wiki/scs)

## 4 – Evolutions techniques de la Fédé. CRU

Interopérabilité de Shibboleth avec  
SAML, Liberty Alliance et WS-  
Federation



## 4 – Evolutions techniques de la Fédé. CRU

### Deux technologies pour l'accès Wi-Fi nomade inter établissements

- *eduroam* : projet européen (volet français opéré par le CRU et RENATER)
  - protocoles 802.1X et RADIUS
- Shibboleth peut aussi être utilisé pour l'accès nomade inter établissement
  - portail captif « *shibbolisé* »

## 4 – Evolutions techniques de la Fédé. CRU

<i>eduroam</i>	Shibboleth
authentification	authentification + attributs
accès web + autres services : messagerie, SSH, web, VPN...	accès web seulement
échelle nationale, européenne voire internationale	échelle régionale ou nationale
niveau de sécurité élevé	niveau de sécurité moyen
configuration d'un client 802.1X	aucune configuration à effectuer sur le poste client