Comité Réseau des Universités

Shibboleth et la fédération du CRU

Olivier Salaün, Comité Réseau des Universités

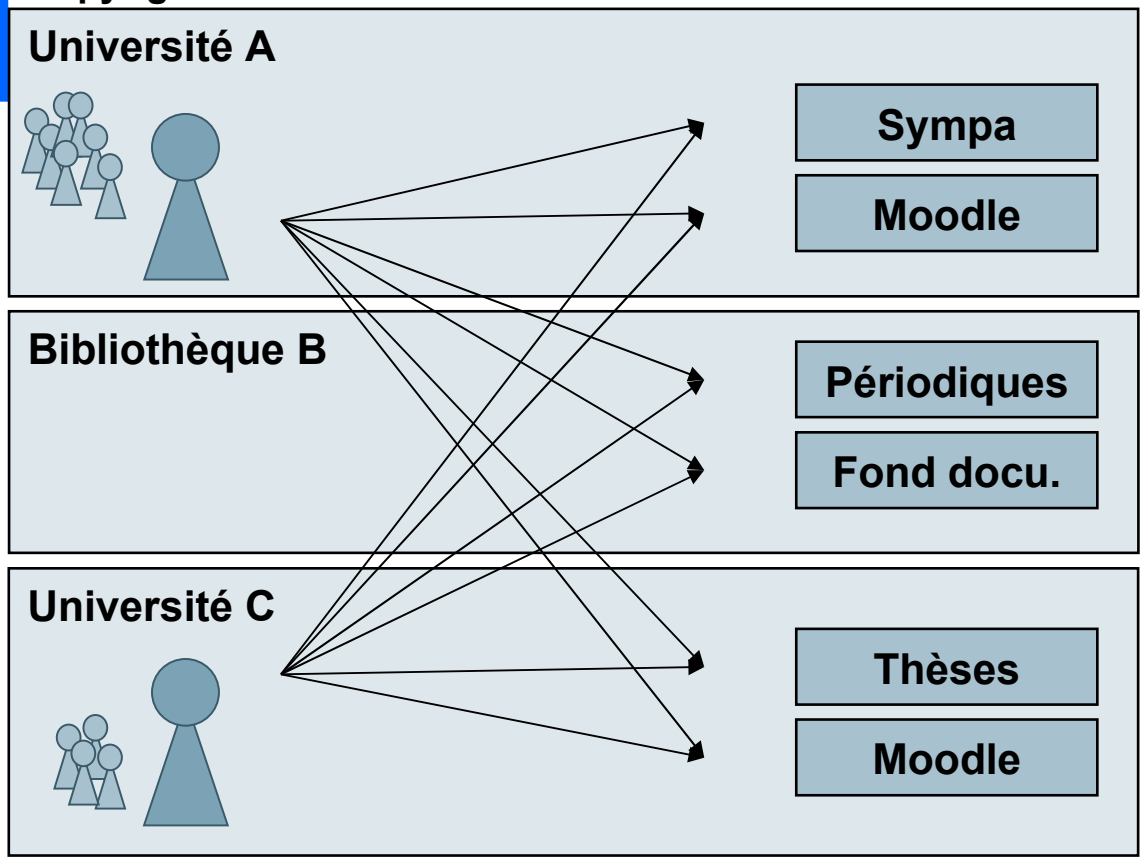
CRU

2. La technologie Shibboleth

4. La fédération pilote du CRU

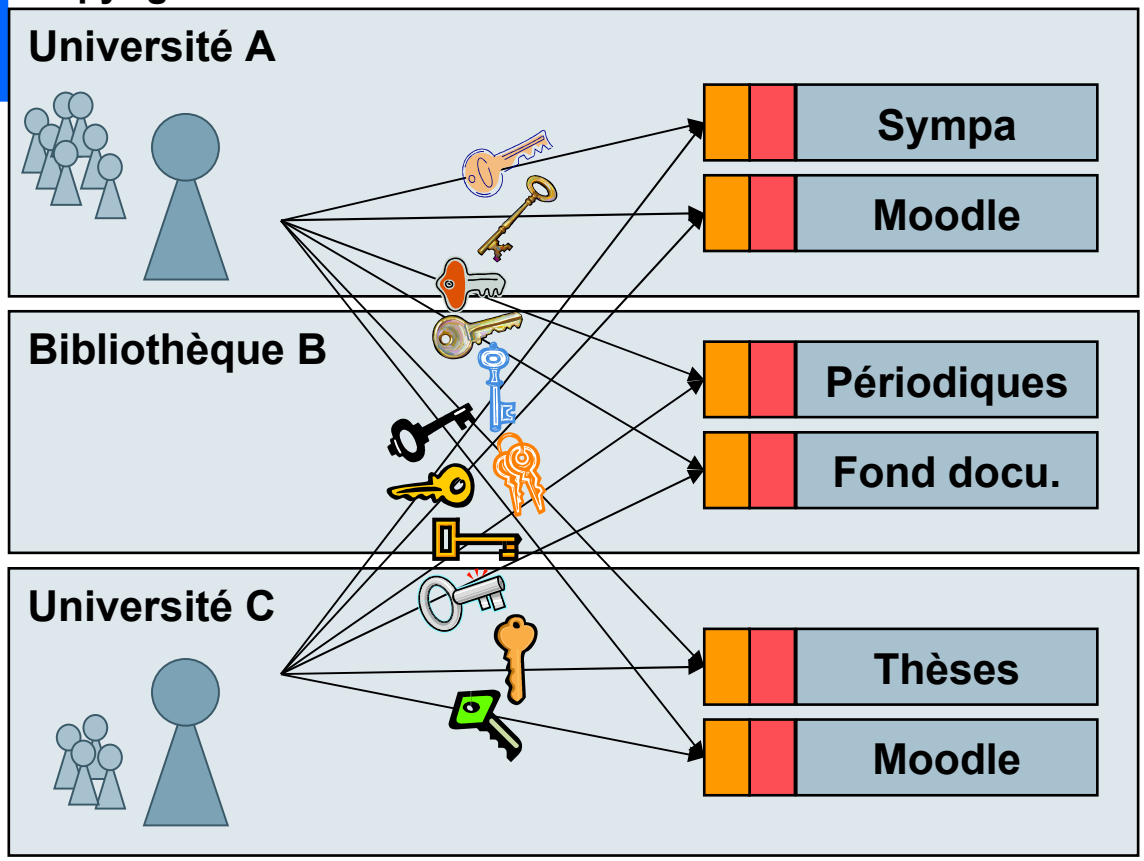
6. Comment utiliser le service

Comment contrôler l'accès à des ressources numériques ?



CRU

Avant le Single Sign-on

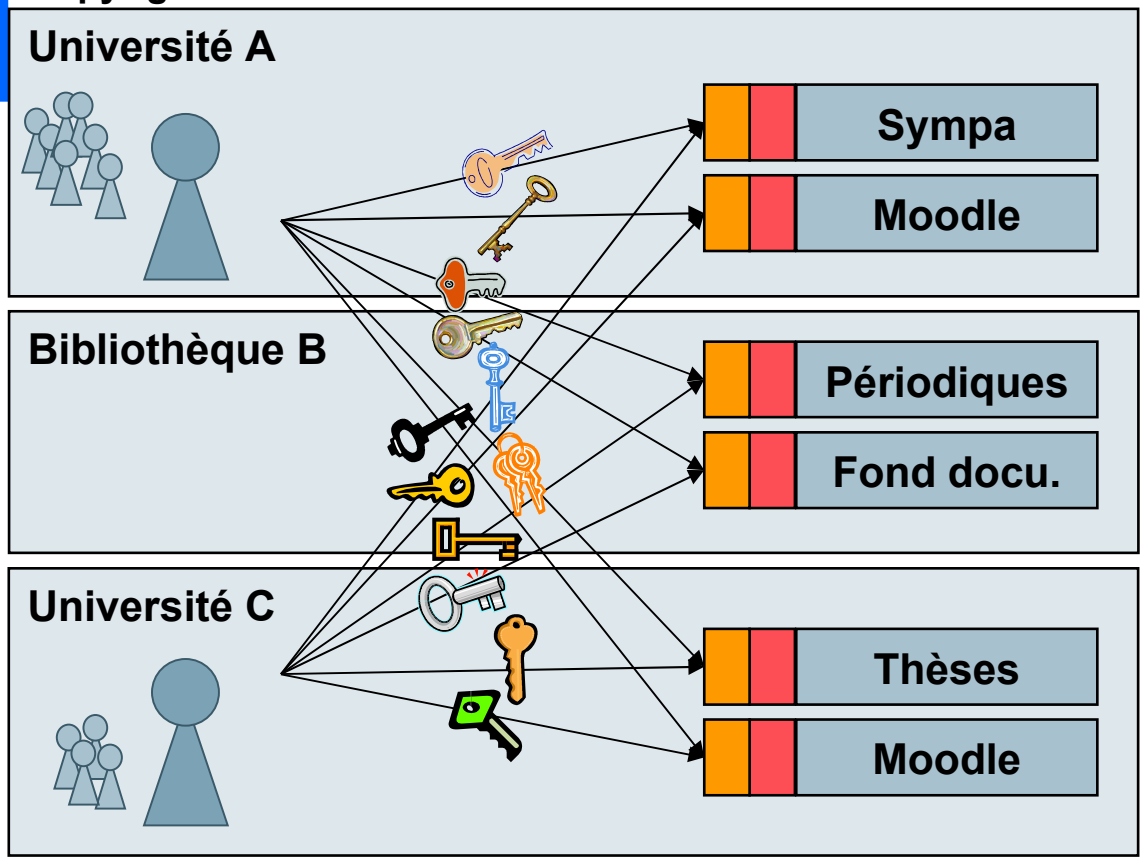


- Contrôle d'accès par adresses IP souvent utilisé
- Problèmes de gestion des utilisateurs au niveau de la ressource
- Multiplication des procédures de login
- Multiplication des comptes donc des mots de passe

Gestion utilisateurs / Authentification

Contrôle d'accès

Le Single Sign-On



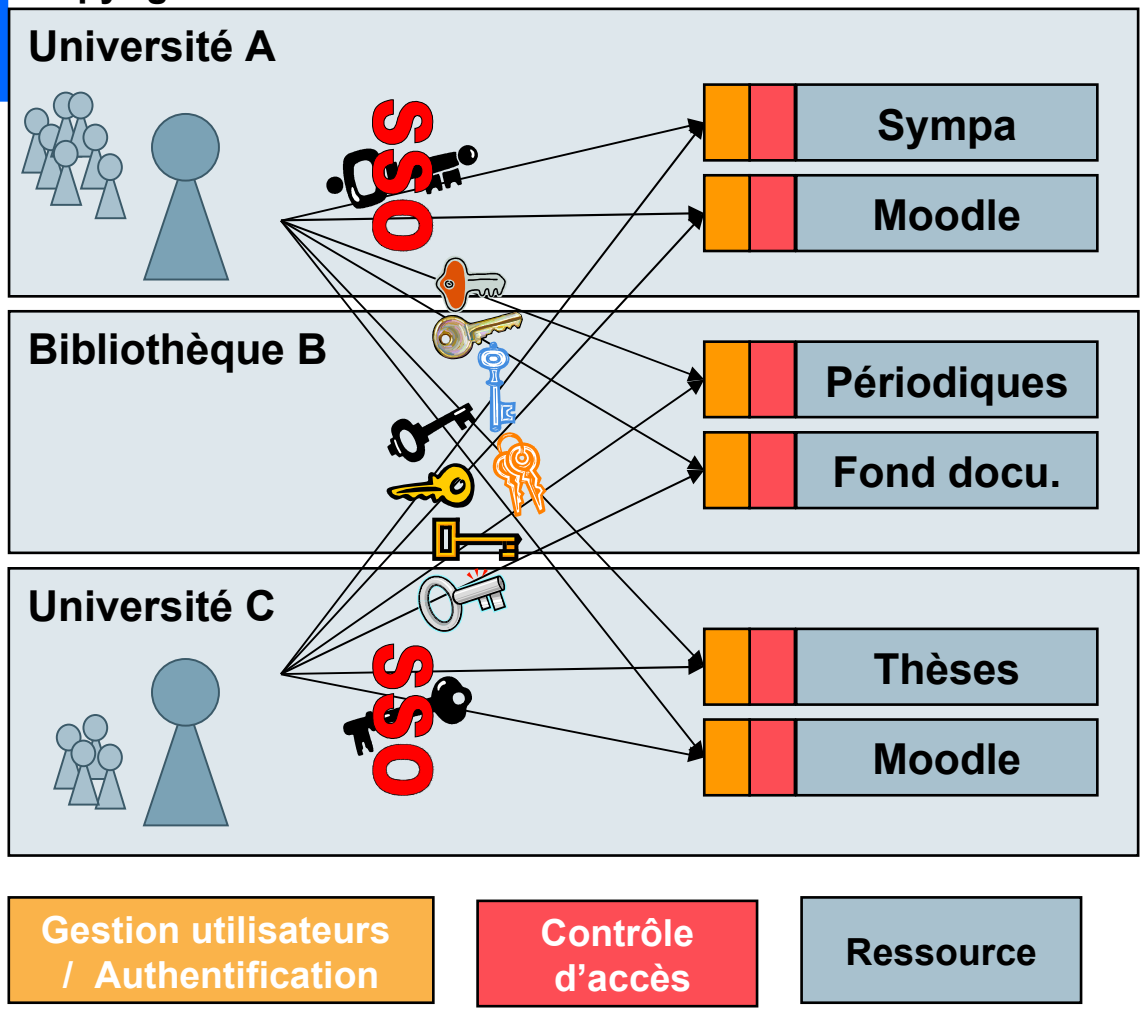
- Contrôle d'accès par adresses IP souvent utilisé
- Problèmes de gestion des utilisateurs au niveau de la ressource
- Multiplication des procédures de login
- Multiplication des comptes donc des mots de passe

Gestion utilisateurs / Authentification

Contrôle d'accès

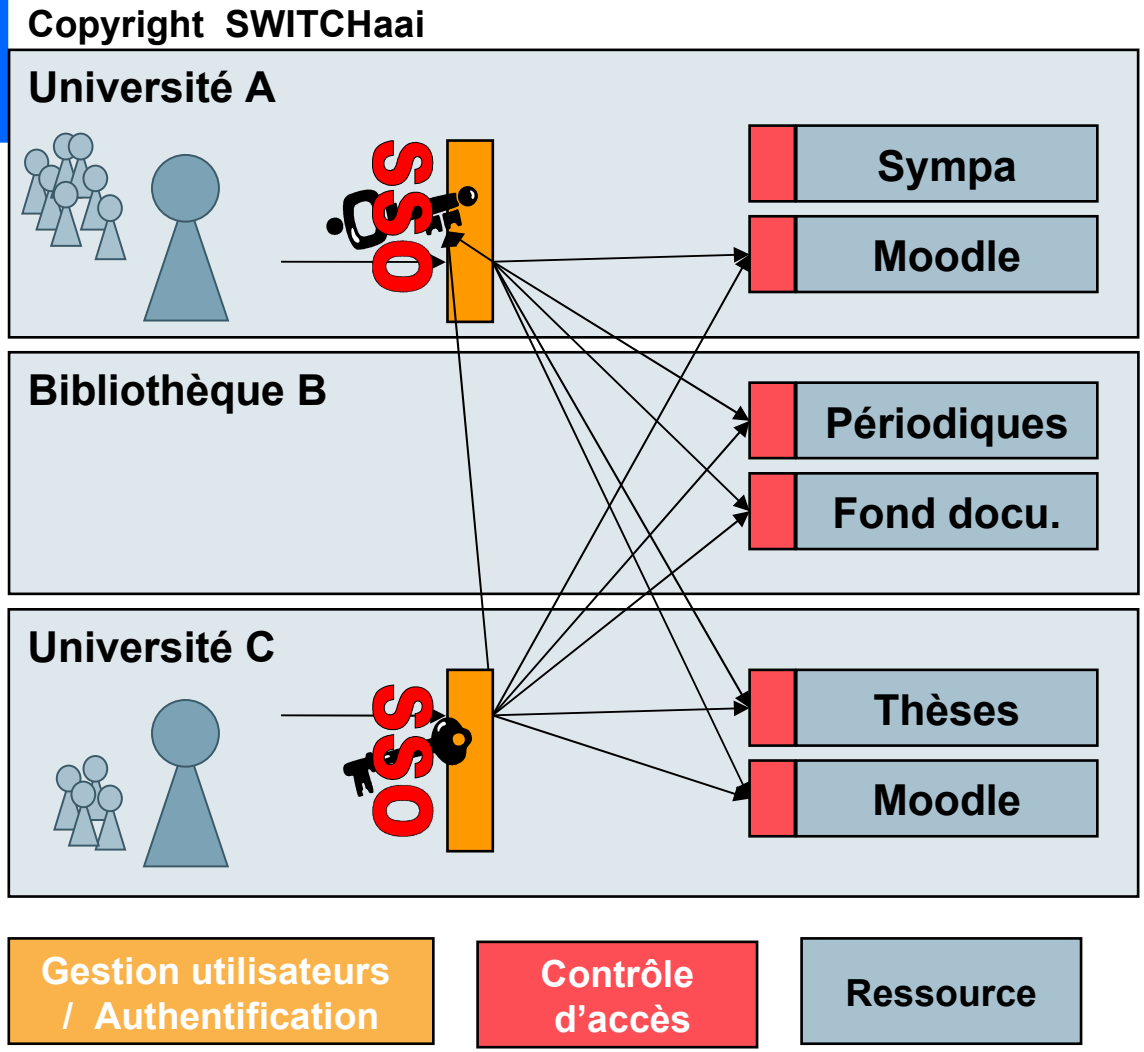
CRU

Le Single Sign-On



- Améliore la situation localement

La fédération d'identités



- Aucune tâche de gestion des utilisateurs au niveau de la ressource
- L'utilisateur s'authentifie une seule fois, dans son établissement
- Les ressources ont une plus grande audience

CRU

Shibboleth.

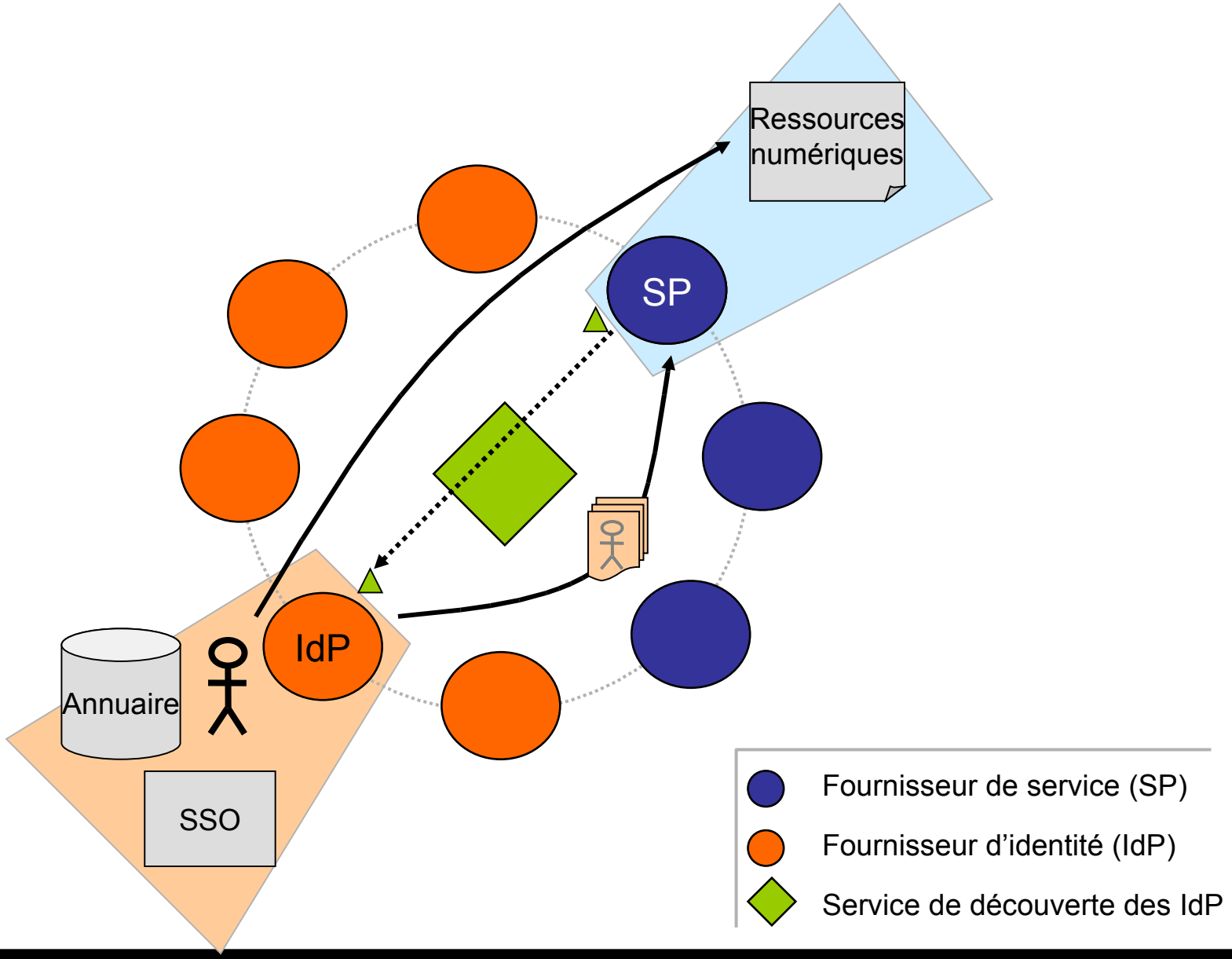
- Logiciel « open source »
- Issu du monde universitaire
  - USA, Internet 2
- Basé sur la norme SAML
- Utilisé dans d'autres pays
  - en production en Suisse, USA, Angleterre, Finlande, Australie
  - en cours de déploiement en Belgique, Allemagne

http://shibboleth.internet2.edu

Architecture de Shibboleth

- Le fournisseur d'identités
  - Propage l'identité des utilisateurs au-delà de leur organisme
  - Connecté au Système d'Information
    - Service de Single Sign-On (CAS)
    - Annuaire LDAP
- Le fournisseur de services
  - Consomme des identités numériques
    - Issues de plusieurs origines
  - Intégré à la ressource web, l'application

Structure d'une fédération



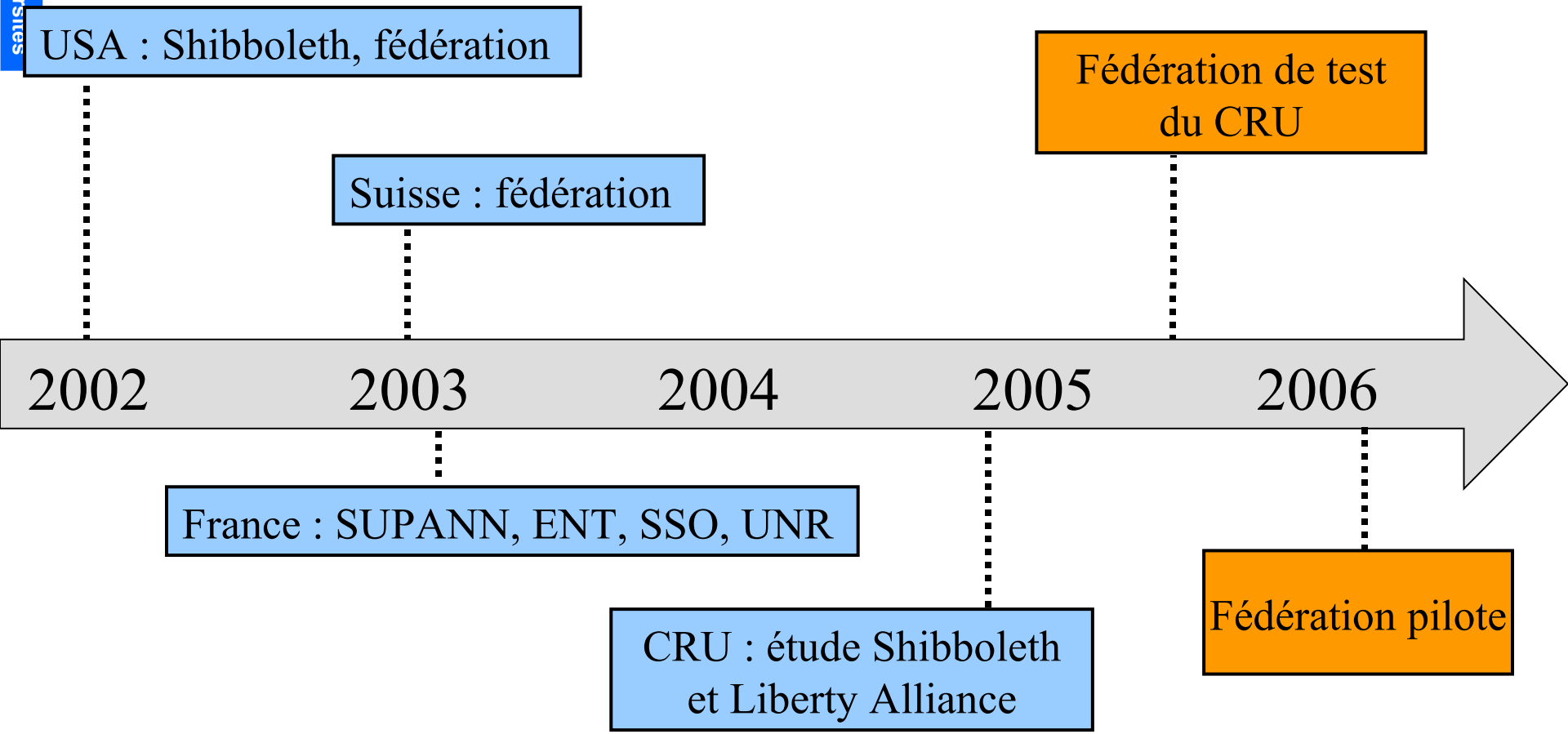
Les identités transmises…

- On peut transmettre le profil de l'utilisateur sans aucune donnée nominative
  - *étudiant de l'université X*
- Si besoin, un identifiant opaque mais persistant peut être fourni (besoin de personnalisation)
- Avec un partenaire de confiance, des attributs nominatifs peuvent être transmis
  - *Paul Ricard, pricard@univ-xx, resp. doc. Élec.*

Comité Réseau des Universités

CRU

La fédération du CRU



http://federation.cru.fr

CRU

Rôles du CRU dans la fédération

- Assistance et conseil
- Distribution des méta données
- Formaliser les relations de confiance
- Nommage et la sémantique communs des attributs

CRU

Les membres de la fédération

- Les fournisseurs d'identités
  - 3 établissements intégrés
  - 16 établissement en phase de tests

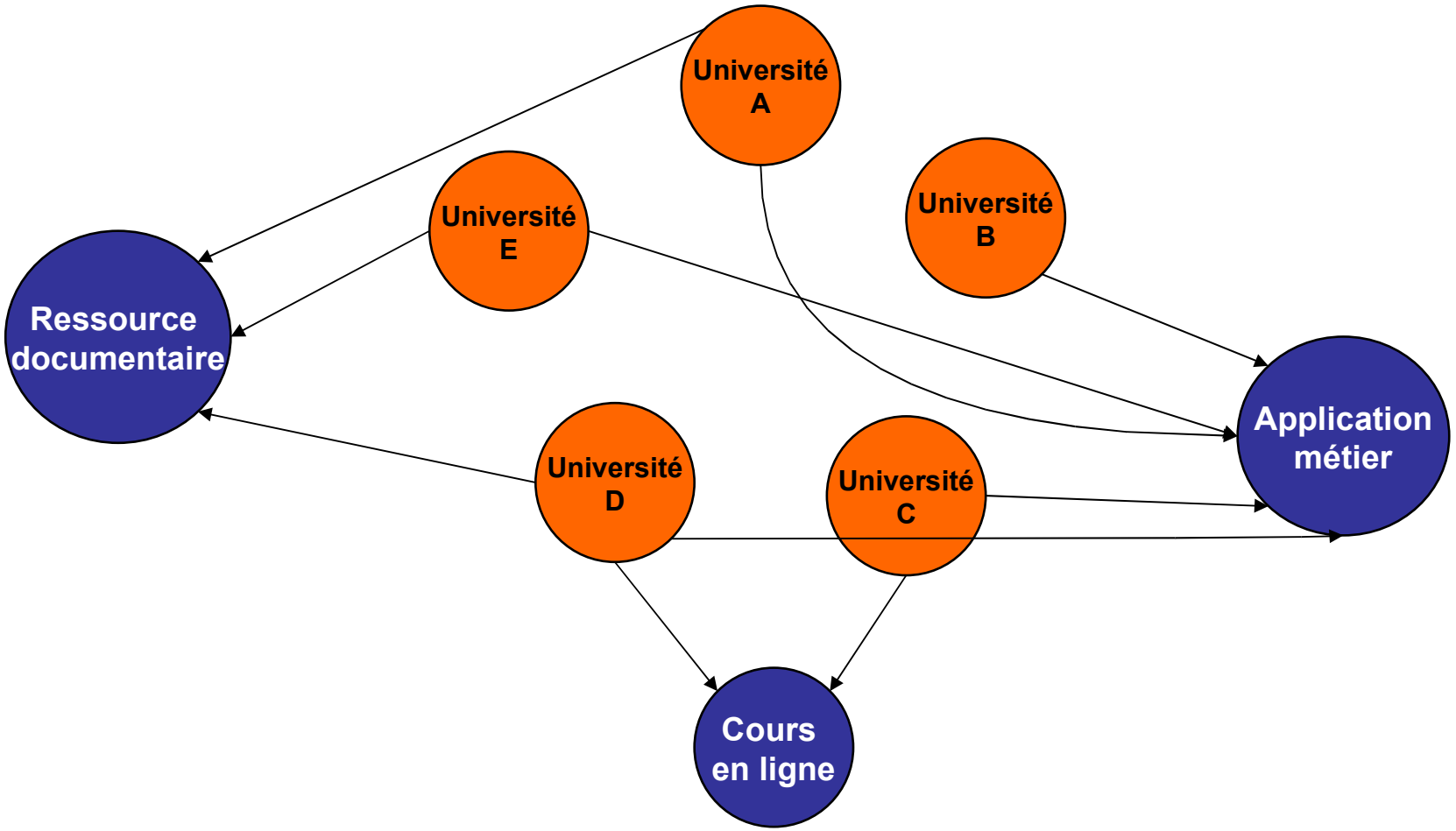
- Les fournisseurs de services
  - 2 entités (ABES et Science Direct)
  - Software Spectrum à venir
  - D'autres services au niveau des UNR

Les projets en cours

- Couperin/ABES/DES
  - accès aux périodiques électroniques
- MIPE3
  - accès à des ressources documentaires et logicielles pour les étudiants
- Ville de Bordeaux / région Bretagne
  - accès wifi pour les étudiants
- URN Bretagne
  - ressources pédagogiques + espace stockage
- UNIT
  - Moissonnage OAI
- Ecoles des mines
  - fédérer l'authentification pour l'accès à des ressources web.

CRU

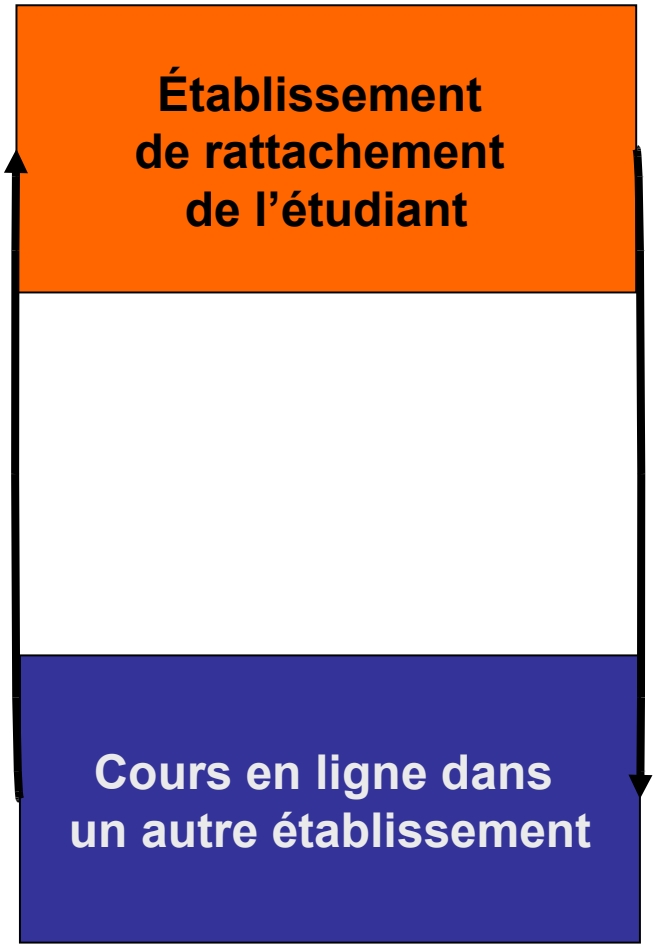
Échanges au sein de la fédération



Une confiance réciproque

Qualité et disponibilité de l'authentification

Qualité et disponibilité des attributs



Utilisation des attributs propagés

CRU

La politique de la fédération

- Régit le fonctionnement de la fédération
  - Organisation
  - Fonctionnement
  - Pré requis techniques
  - **Engagements de chacun des membres**

- **Ne régit pas d'aspects financiers, fonctionnels, contractuels**

- *http://federation.cru.fr/pilote/references/*

Principaux engagements des fournisseurs d'identités

- Utiliser un produit compatible Shibboleth
- Sécuriser son environnement logiciel (SSO, ENT, annuaire)
- Respecter le nommage des attributs définis au sein de la fédération
- Journaliser les connexions des utilisateurs
- Respecter la législation sur la protection des données à caractère personnelle

Etapes pour intégrer la fédération pilote

1. Prérequis : SSO + LDAP conforme SupAnn
2. Installer brique Shibboleth
3. Lire la politique de la fédération pilote
4. Faire signer la convention par le chef d'établissement
5. Validation par le CRU puis inscription effective

http://federation.cru.fr/pilote/integration-IdP.html

CRU

en bref…

- Shibboleth, technologie pivot
- Dans la continuité des ENT
- Ouvre des perspectives de collaboration
- Intérêt croissant des Universités
- Pas seulement en France
- Pas seulement pour la documentation électronique

http://federation.cru.fr