

Utilisation de la fédération d'identités pour les universités françaises

Olivier Salaün

Comité Réseau des Universités

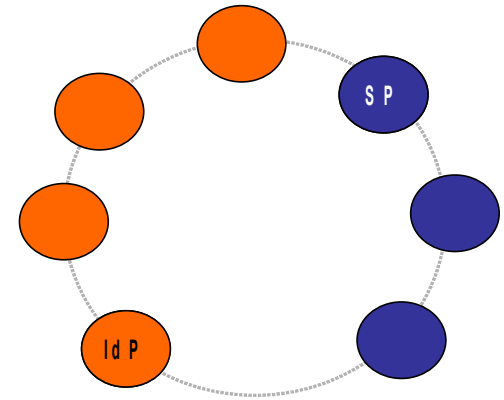
<http://federation.cru.fr>

Le Comité Réseau des Universités

- Structure nationale pour l'enseignement supérieur
 - Dépend du ministère de l'enseignement supérieur
- Nos activités
 - Définition d'un schéma d'annuaire commun (Supann)
 - Infrastructure réseau répartie (eduroam)
 - Développement d'un serveur de listes (Sympa)
 - Gestion d'une forge (sourceSup)
 - Infrastructure de fédération d'identités

La fédération du CRU

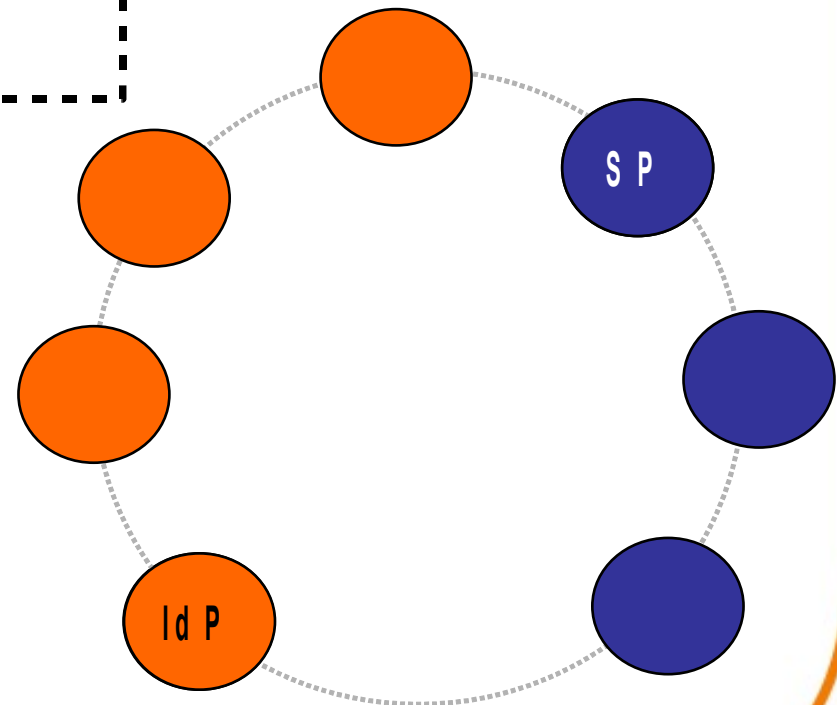
- Service opérationnel depuis 2006
- Topologie de ce cercle de confiance
 - N fournisseurs d'identités
 - M fournisseurs de services
- Objectif
 - Permettre le partage de ressources web entre universités
 - Contexte de rapprochement des universités
 - Besoin de mécanismes d'authentification distribués



La fédération du CRU

Les fournisseurs d'identités

- Les établissements d'enseignement supérieur
- Aujourd'hui :
 - 35 universités
 - 600.000 étudiants (=45%)



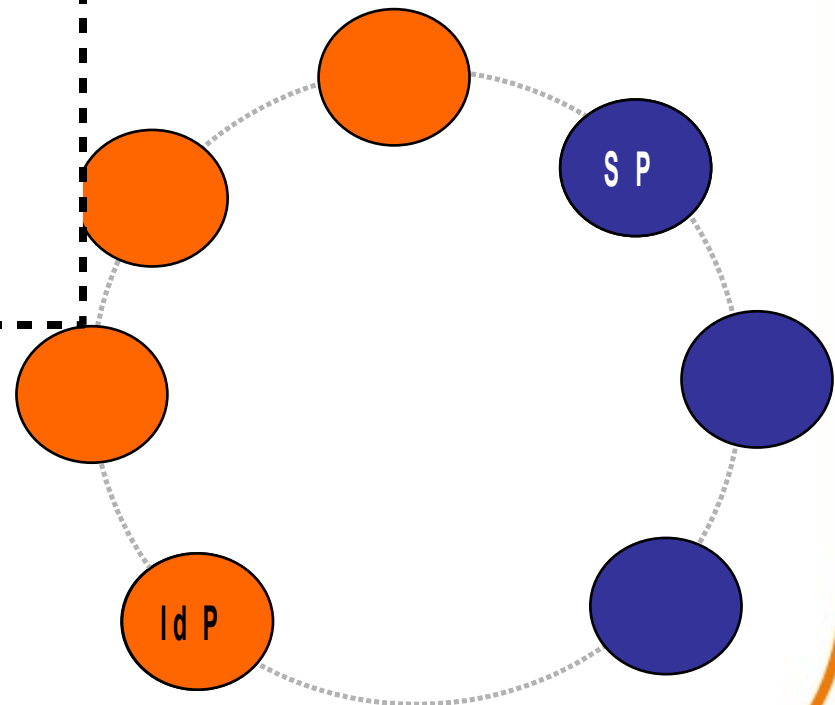
La fédération du CRU

Les fournisseurs de services

- Universités ou organisme public ou entreprise privée
- Aujourd'hui : 25 services

Type de services

Wi-Fi, ressources documentaires, enseignement à distance, distribution de logiciels, application métier



Le cercle de confiance...

- regroupe un ensemble de fournisseurs de services et de fournisseurs d'identités
- garantit l'interopérabilité
- définit un niveau de sécurité minimum et des bonnes pratiques
- évite la multiplication d'accords bilatéraux
- est un lieu d'échanges et de coordination

Gestion de la confiance

- Le cercle de confiance définit un niveau de confiance minimal entre ses membres
 - Formalisé par des documents administratifs : politique, convention, lettre d'inscription
- La politique définit
 - Les responsabilités des SPs, des IdPs, du CRU
 - Un ensemble de bonnes pratiques
- Confiance technique
 - Certificats x.509
 - Méta données distribuées

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-x, étudiant en 2ème année...

Technologie



Shibboleth.

- Shibboleth
 - logiciel open-source (consortium Internet2)
 - Utilise SAML
- Adopté par d'autres communautés universitaires
 - USA, Grande-Bretagne, Australie, Allemagne, Suède, Finlande, Danemark, Suisse...
- 3 briques logicielles
 - IdP, SP, WAYF (devient le Discovery Service)
- Dernière version implémente SAML 2.0

Rôle du CRU dans la fédération

- Gestion des méta données et des conventions
- Opère
 - une fédération de test
 - un fournisseur d'identités par défaut
- Accompagnement (formations)
- Définition des attributs échangés

Impressions

- Bonne adoption par les universités
 - Aucune obligation (incitation ministère)
 - Technologie pivot pour de nombreux besoins
- Intérêt important des éditeurs de contenus
 - Remplace les contrôles d'accès par @IP
 - Si besoin, on peut identifier l'utilisateur
 - Possibilité d'accès à des attributs utilisateurs
- Shibboleth, une bonne solution logicielle
 - Open source
 - Très configurable
 - Facile à intégrer dans un Système d'Information

Évolutions du projet

- Facteurs de croissance
 - Infrastructure appelle les services
 - Nouveaux services motivent les universités
- Passage à SAML 2.0
- Définition de nouveaux attributs utilisateurs + nomenclature + sémantique
- Échanges avec l'enseignement secondaire
- Interconnexion des fédérations européennes : eduGain

- Le CRU : <http://www.cru.fr>
- Fédération du CRU : <http://federation.cru.fr>
- Shibboleth : <http://shibboleth.internet2.edu>