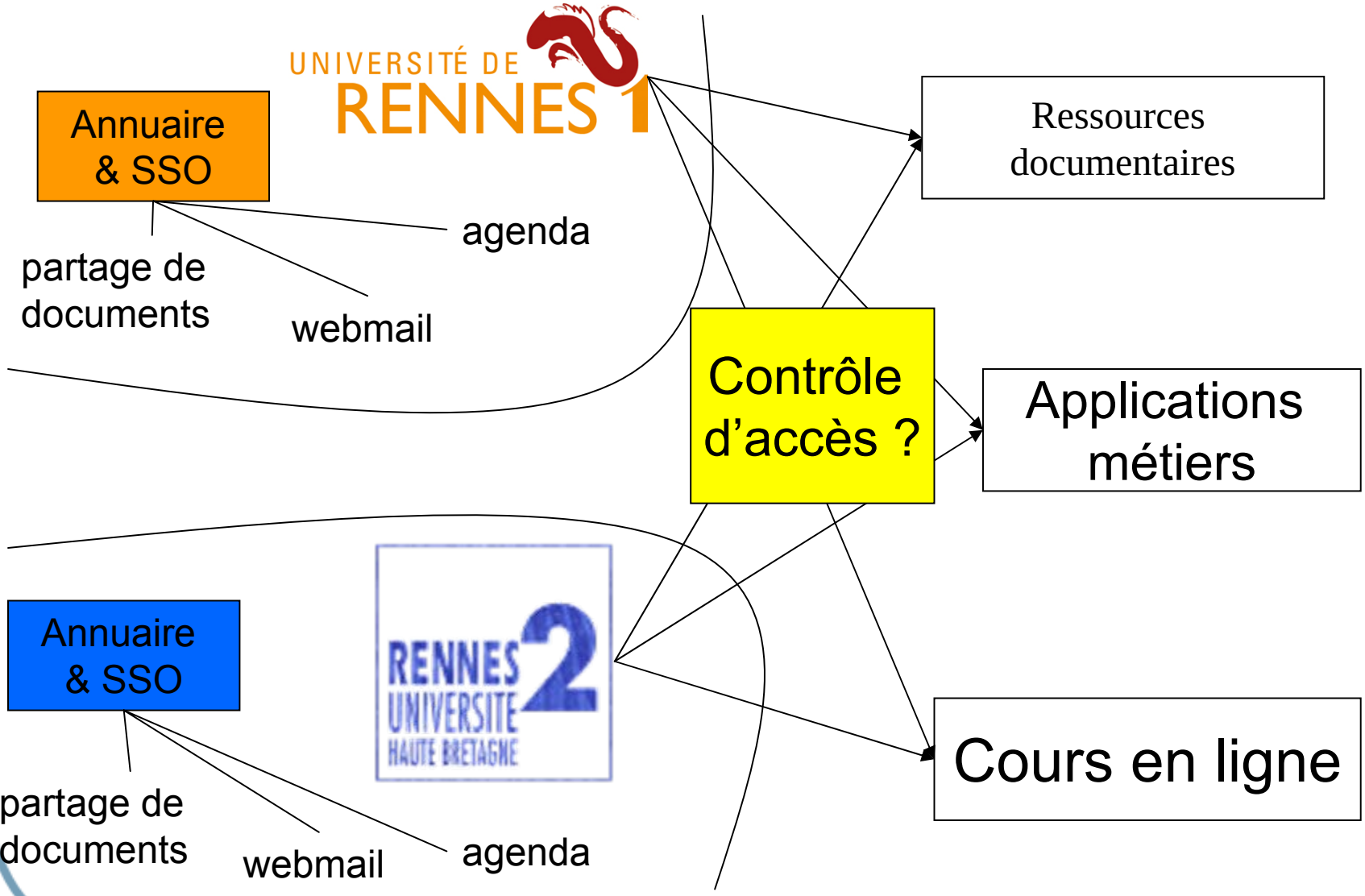
Simplification et sécurisation de l'accès à des services en ligne via une fédération d'identités

JSSI 2008, 22 mai 2008

Florent Guilleux, Mehdi Hached, Comité Réseau des Universités

Les universités partagent de plus en plus de ressources en ligne



L'accès à ces ressources doit être simple, sécurisée et se faire depuis n'importe où

- simple
  - sans installation ou configuration sur le poste client
  - sans nouveau mot de passe à retenir
- sécurisée
  - confidentialité, authentification et intégrité des données échangées
  - contrôle de la diffusion des données par leurs propriétaires
- depuis n'importe où : depuis la maison ou le cybercafé comme depuis le campus

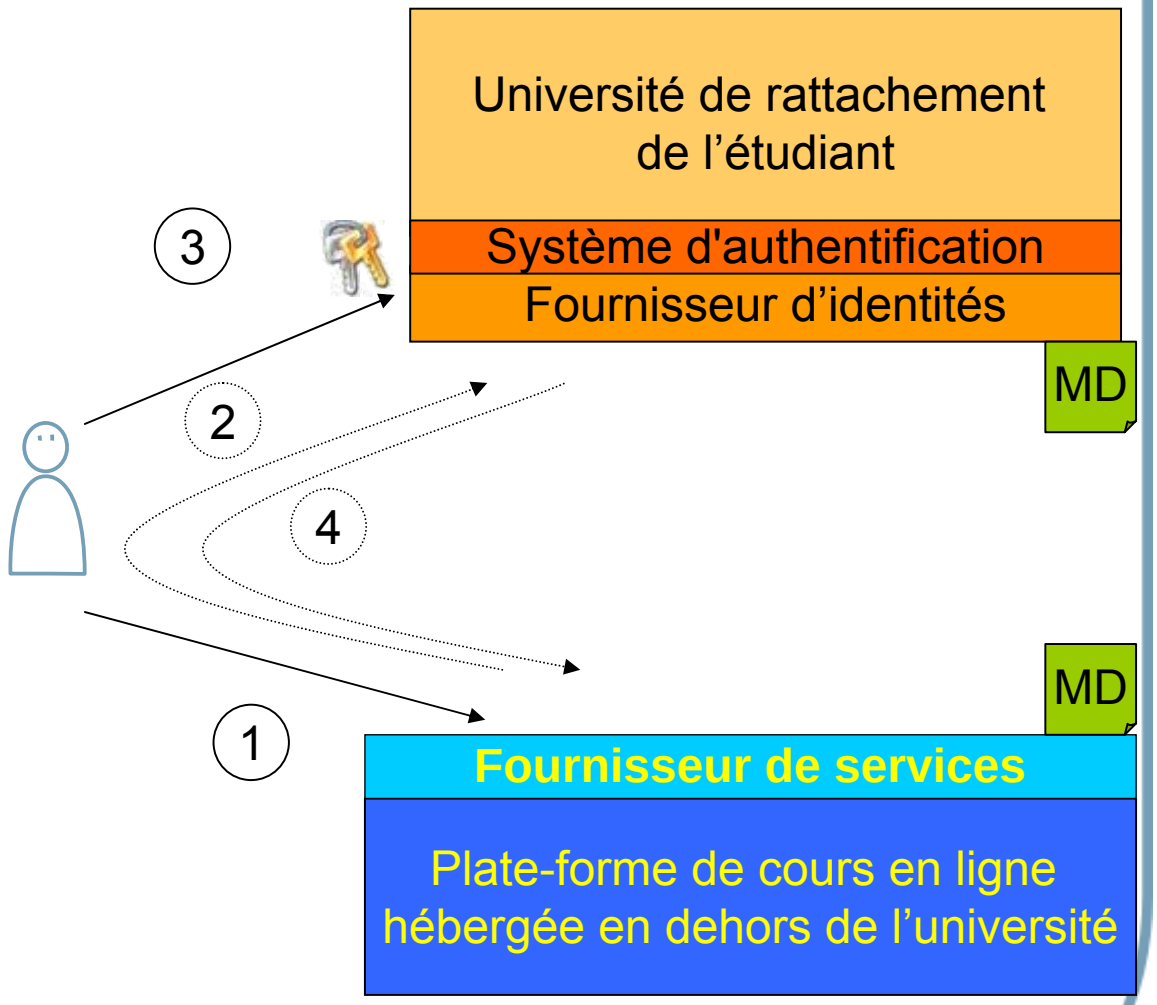
La fédération d'identités est une bonne solution pour le contrôle d'accès aux ressources en ligne

- pour l'utilisateur final
  - un simple navigateur suffit
  - pas de nouveau mot de passe
- pour le gestionnaire d'une application
  - plus besoin de gérer un système d'authentification
  - possibilités de contrôle d'accès riches avec des attributs utilisateurs fiables
- pour l'université gérant des comptes utilisateurs
  - réutilisation des briques déjà existantes dans le SI (SSO, annuaire)
  - maîtrise de la diffusion des identités (identité = ensemble d'attributs)

Principe de fonctionnement d’un accès via la fédération

Le fournisseur d'identités authentifie l'utilisateur, puis envoie une preuve d'authentification au fournisseur de services

- Tentative d'accès à la ressource
- Redirection vers le système d'authentification de l'établissement de rattachement
- Authentification
- Redirection vers la ressource avec une **preuve d'authentification**

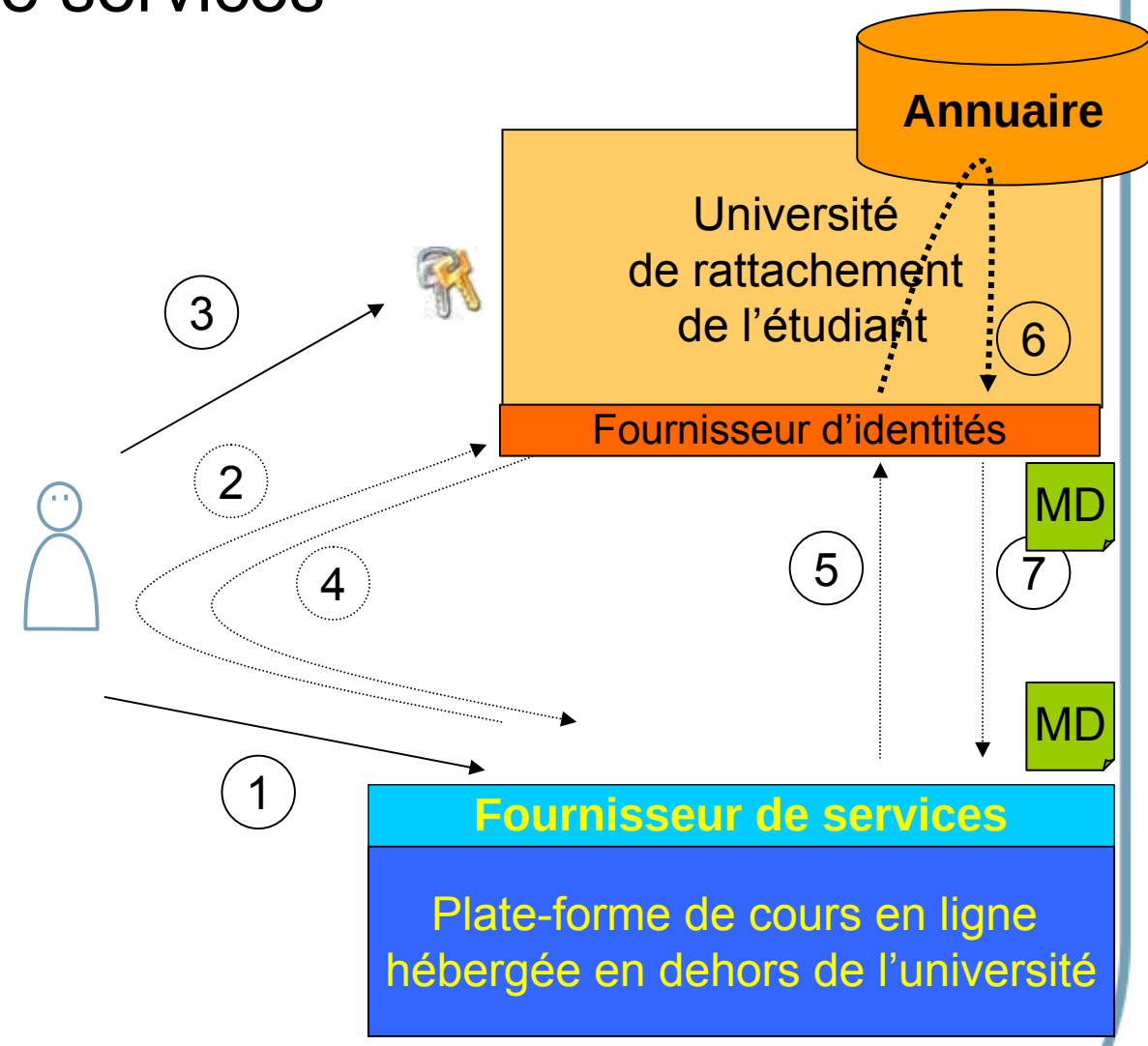


Des attributs d'un utilisateur peuvent être propagés vers le fournisseur de services

(5) Demande d'attribut sur l'utilisateur

(6) Extraction des attributs

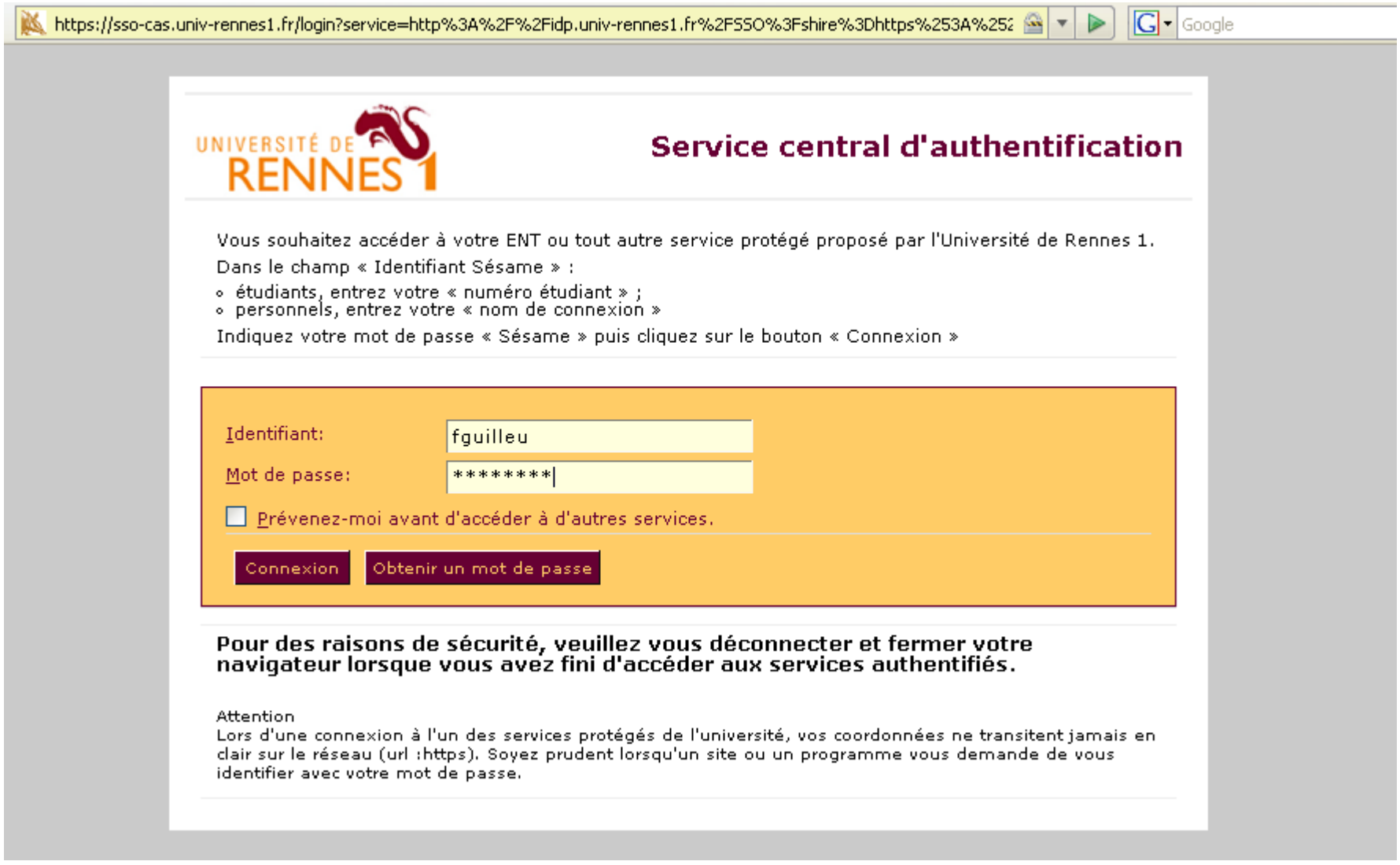
(7) Propagation vers la ressource



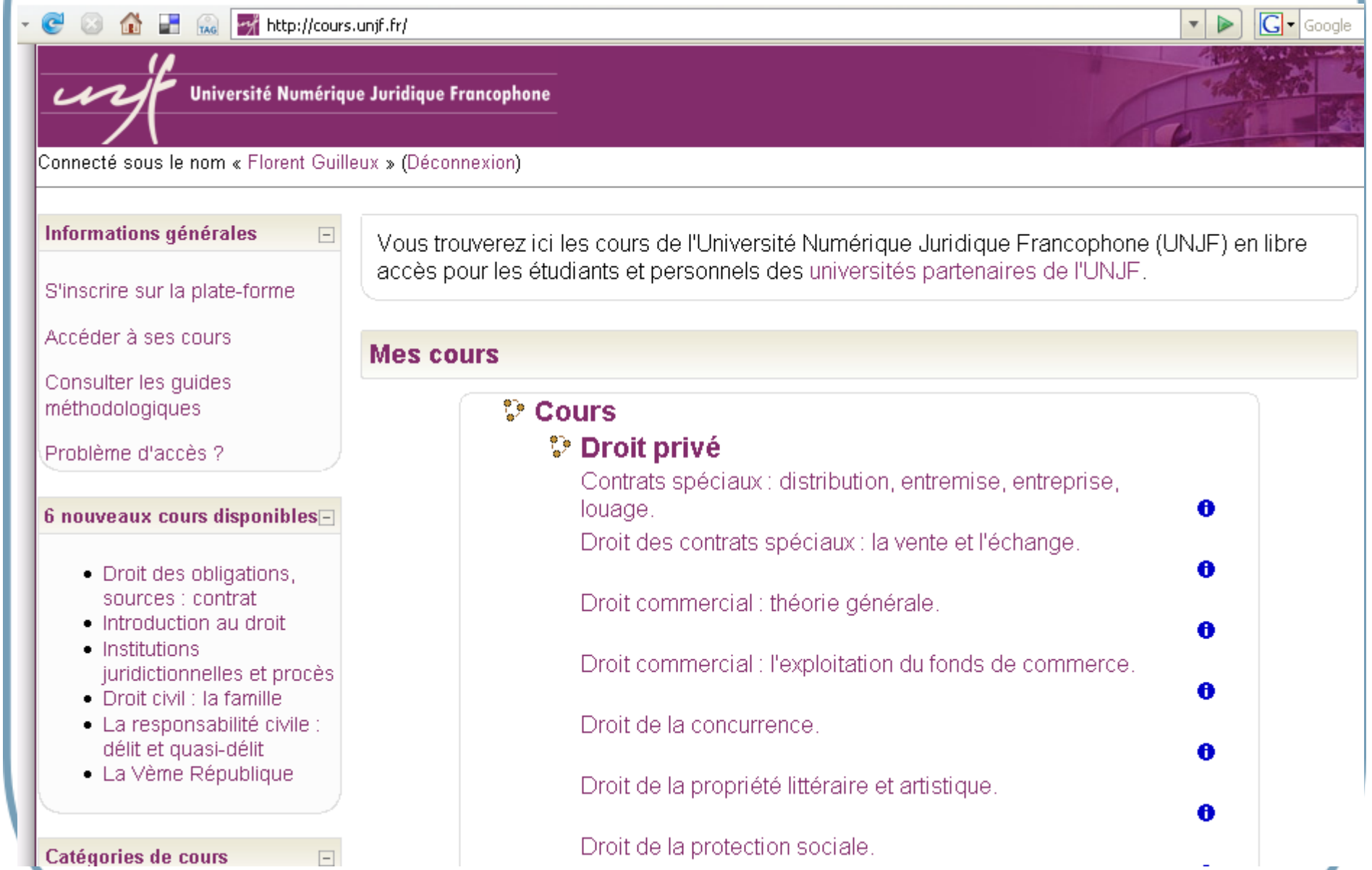
Exemple de l'accès à l'Université Numérique Juridique Francophone (démo)

Sélection de son université (démo)

Authentification sur le portail de son université (démo)



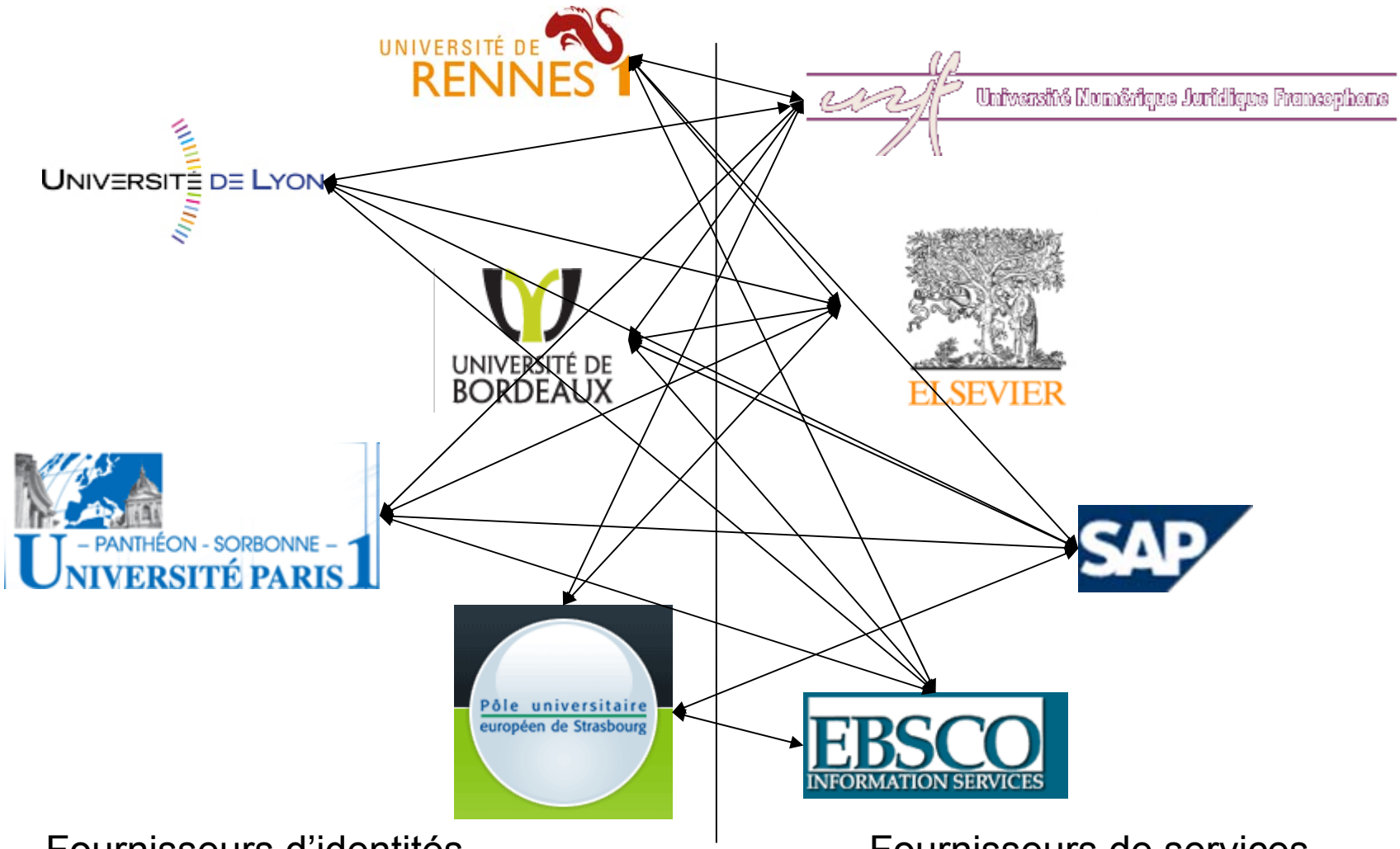
Retour authentifié sur l'UNJF (démo)



Les relations de confiance sont centrales

- Le fournisseur de services fait confiance aux fournisseurs d'identités
  - sur la disponibilité et la sécurité de leur système d'authentification
  - sur la qualité des attributs utilisateurs transmis
- Le fournisseur d'identités fait confiance aux fournisseur de services
  - sur la sécurisation et l'utilisation des attributs utilisateur obtenus

L'établissement de relations de confiance bilatérales ne passe pas à l'échelle



Fournisseurs d'identités

Fournisseurs de services

La fédération offre un cadre de confiance minimale (« cercle de confiance »)

- chaque fournisseur d'identités et de services s'inscrit en s'engageant à respecter un ensemble de règles
  - plus besoin de relations bilatérales de confiance

- la fédération définit également
  - un cadre technique d'interopérabilité
  - un ensemble d'attributs normalisés (nommage et sémantique)
  - éventuellement une représentation juridique et administrative

La fédération d’identités de l’enseignement supérieur

Le CRU opère le service de fédération pour l'enseignement supérieur

- a défini le cadre organisationnel et technique de la fédération
- publie les méta données
- représente la fédération : relations avec d'autres fédération et prospection de fournisseurs de services potentiels
- assure le support et la formation aux organismes
- effectue la veille technologique dans le domaine

Les fournisseurs d'identités sont les universités et grandes écoles françaises

- en mai 2008 40 universités inscrites et 700 000 étudiants connectés
  - inscription sur la base du volontariat

- engagements sur
  - la sécurisation et la disponibilité de leur système d'authentification et de leur annuaire
  - le provisionning de leur annuaire
  - le respect de la législation de la protection des données à caractère personnel
  - l'utilisation d'un produit de fédération compatible Shibboleth

Les fournisseurs de services

- universités, autres organismes publics, entreprises privées (françaises ou étrangères)

- en mai 2008, 37 fournisseurs de services
  - inscription sur la base du volontariat

- types de services
  - cours en ligne
  - ressources documentaires
  - nomadisme Wi-Fi inter campus
  - applications métiers (ex. : SAP)
  - téléchargement de logiciels
  - …

Cette fédération est un cadre technique de confiance

- aspects non couverts des relations entre fournisseurs : administratifs, financiers, fonctionnels…

- la fédération n'est pas signataire d'un contrat qui peut lier un fournisseur de services et des fournisseurs d'identités

- **chaque fournisseur reste libre d'établir une relation avec les fournisseurs de son choix**

Cadre technique de la fédération et gestion technique de confiance

SAML et Shibboleth sont la norme et la solution utilisées dans la fédération d'identités de l'enseignement supérieur

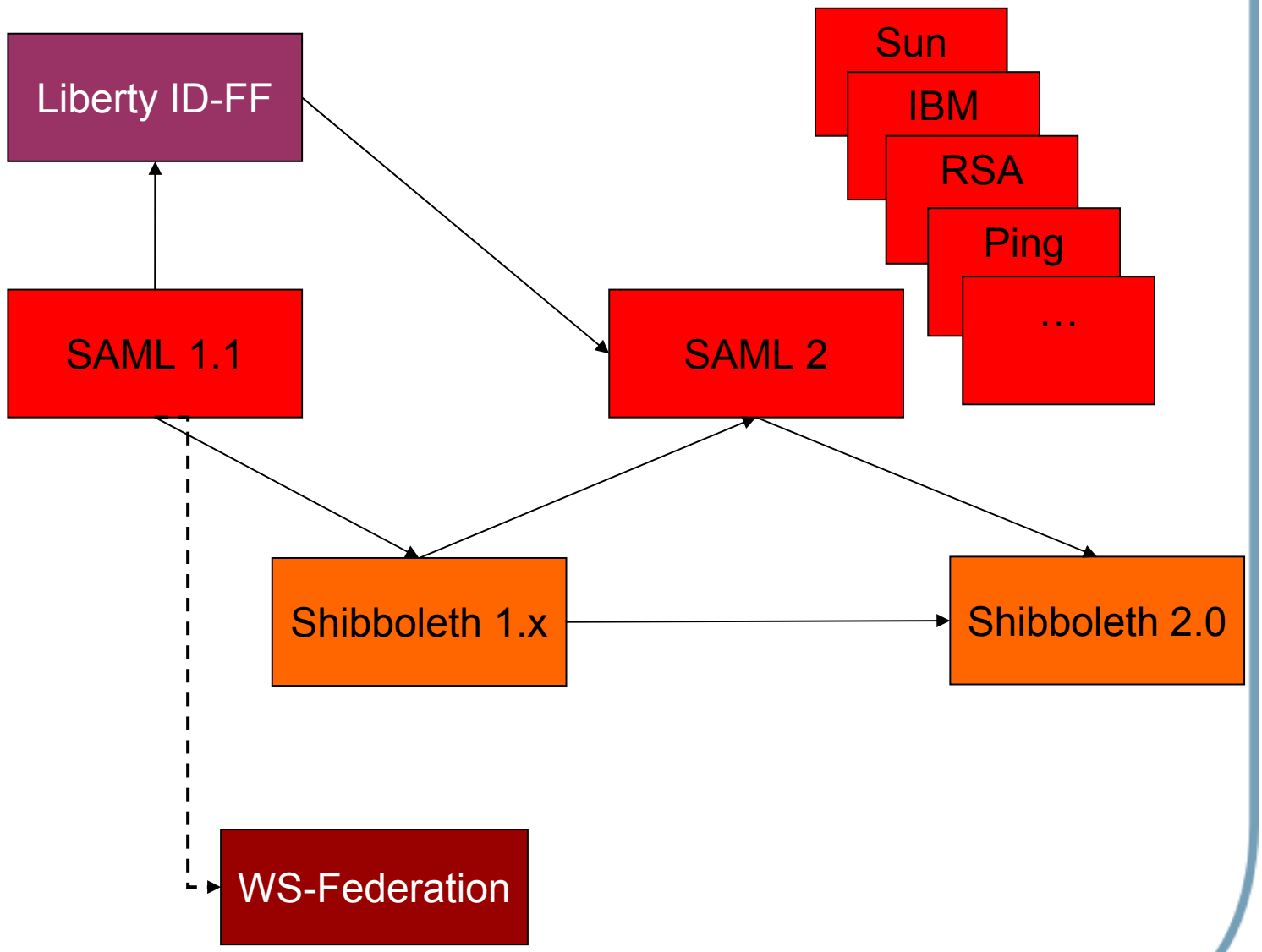
- SAML (Security assertion markup language) protocole standard OASIS pour l'échange d'assertions sécurisées entre applications

- Shibboleth : logiciel ***open source*** implémentant SAML
  - plus un profil Shibboleth spécifique dans la version 1.3

- aujourd'hui utilisation de Shibboleth 1.3, passage à Shibboleth 2.0 (compatible SAML 2)

SAML, Liberty Alliance et Shibboleth

- HTTP[S]
- SOAP
- X.509
- XML
- XML-sec
- XML-sig



Les méta données : socle de confiance de la fédération

- fichier XML listant notamment tous les membres de la fédération et leurs URL d'accès techniques
- généré, mis à jour et signé électroniquement par l’opérateur de la fédération
- publié sur un serveur centralisé

Des échanges SAML sécurisés entre entités

- utilisation de SSL/TLS, X.509, XML-Signature, XML-Encryption
- tous les échanges entre entités sont :
  - chiffrés (SSL/TLS et optionnellement au niveau SAML) : pas d'interception par un tiers
  - signés : pas de modification par un tiers
- authentification des entités communicantes via des certificats X.509

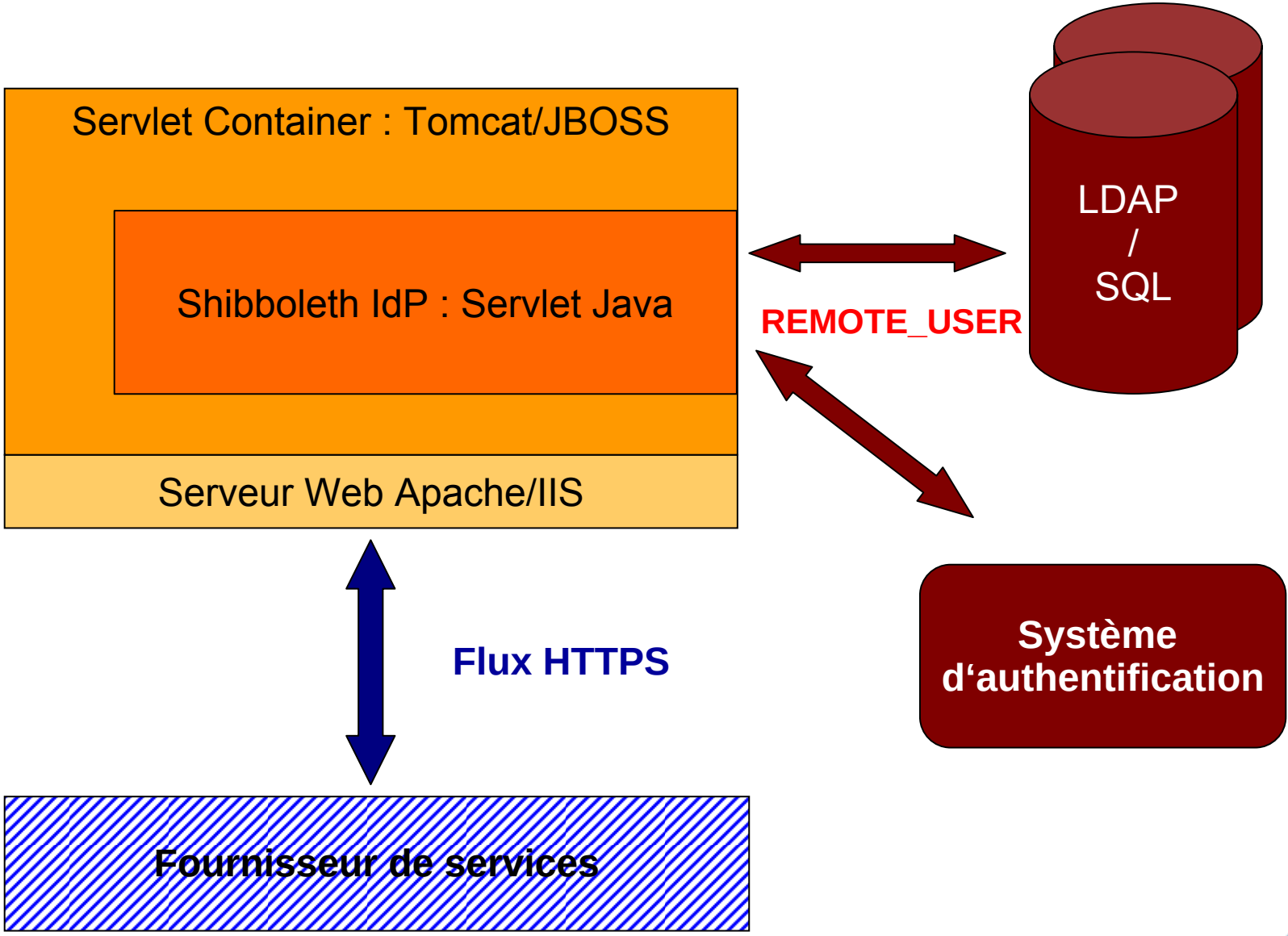
Les certificats X.509 des entités sont reconnus de deux façons

- **soit sans PKI** : publication directe des certificats des entités dans les méta données
  - les méta données jouent le rôle de socle de confiance pour les certificats
  - méthode désormais privilégiée car il faut connaître le certificat d'entité pour chiffrer les assertions qu'on lui envoie

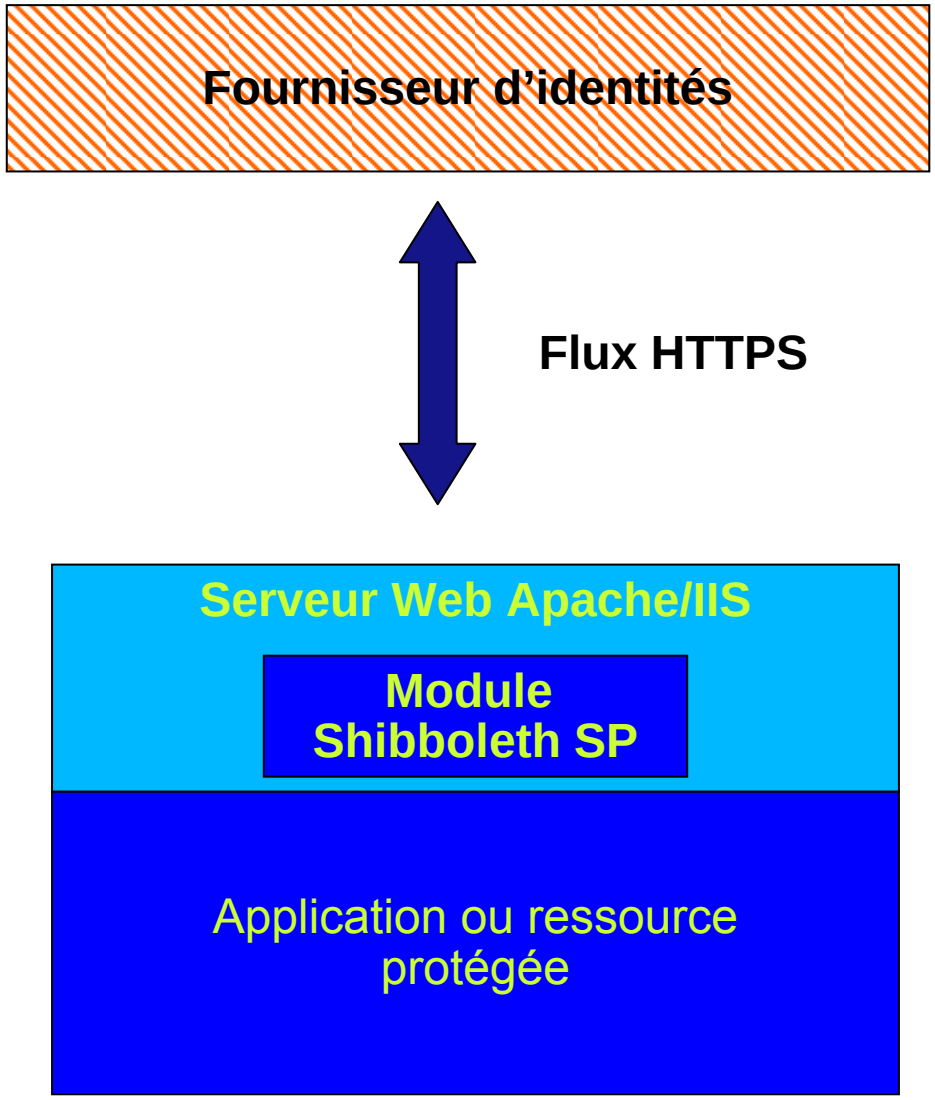
- **soit via une ou des PKI** : reconnaissance d'une ou plusieurs autorités de certification via la publication de leurs certificats dans les méta données

Intégration de Shibboleth dans les systèmes d'information des fournisseur d'identités ou de services

Intégrer Shibboleth dans le SI du fournisseur d'identités



Intégrer Shibboleth chez un fournisseur de services



Différents scénarios d'identification sont possibles

1. accès anonyme mais authentifié
   - aucun référentiel utilisateur dans l'application

2. pseudonymat : accès anonyme mais on peut reconnaître un même utilisateur d'un session à l'autre (attribut *persistentNameID*)
   - personnalisation
   - historique des recherches
   - services avancés

3. accès nominatif
   - problématique de la protection des données à caractère personnel
   - difficulté d'avoir un identifiant utilisateur unique à l'échelle de la fédération

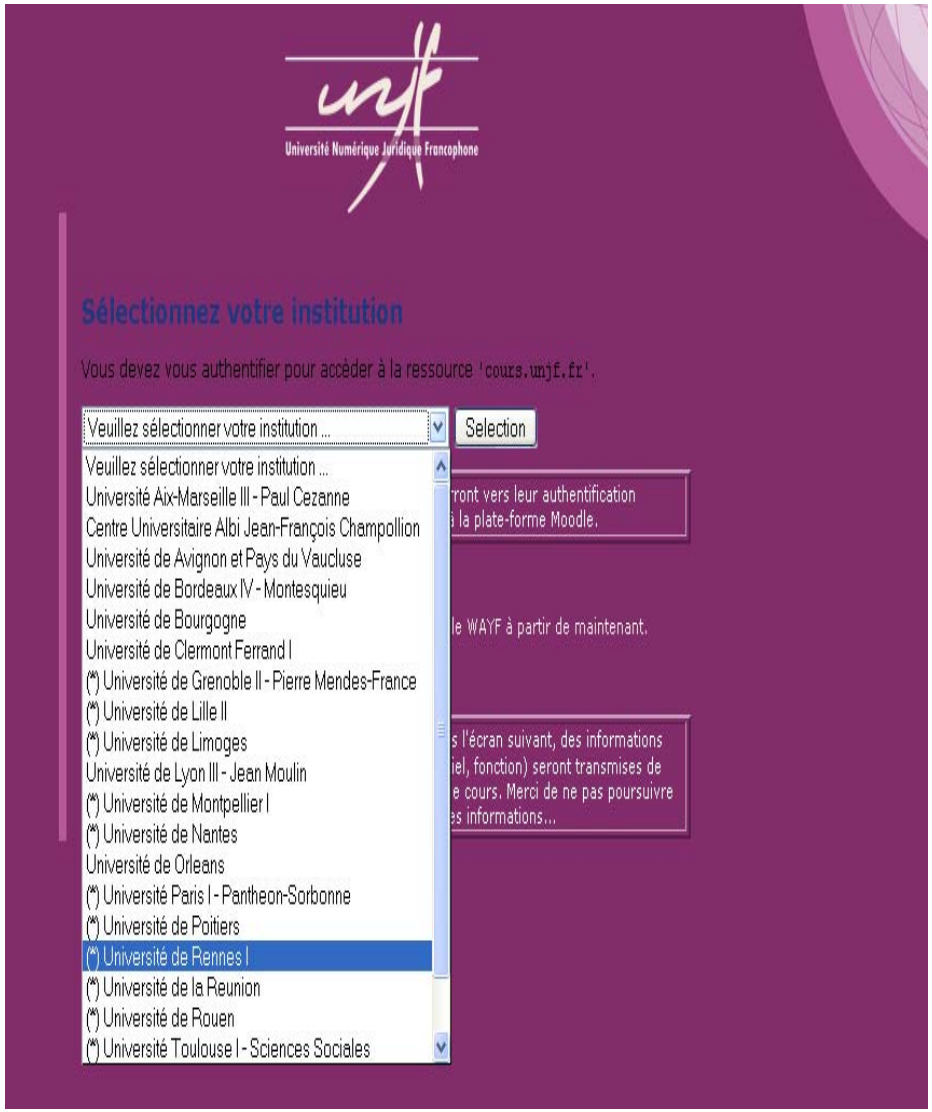
Différents scénarios de contrôle d'accès sont possibles

1. sur la base d'attributs utilisateur : accès restreint à des populations, par exemple
   - seulement aux enseignants universitaires
   - seulement aux doctorants bretons
   - seulement aux étudiants en droit de mastère
   - etc.

1. sur la base de l'appartenance à un groupe
   - la définition du groupe peut être dans l'application ou dans un référentiel tiers

Les limites et difficultés

Le service de découverte est un passage obligé mais peu ergonomique



- en général il est répété pour chaque service
- pour atténuer le problème
  - un service de découverte unique centralisé
  - accès direct sans service de découverte depuis le portail d'établissement

D'autres limites et difficultés

- la poule et l'œuf
  - pour avoir des fournisseurs d'identités, il faut des fournisseurs de services
  - et inversement
- la nécessité d'adapter les applications pour les rendre compatible avec la fédération
- difficulté de la normalisation du nommage et de la sémantique des attributs à l'échelle d'une fédération

Conclusion

Les raisons du succès de cette fédération

- 50 % des universités couvertes en 18 mois, progression constante du nombre de services proposés
- de réels besoins de partage de ressources en ligne
- culture de coopération entre université et relative homogénéité de leur SI
- pour de grandes populations d'étudiants, pas vraiment d'alternatives viables
  - accès simple pour l'utilisateur
  - contrôle d'accès sur la base d'attributs

Les évolutions de la fédération enseignement supérieur

- élargissement aux instituts de recherche français (“fédération RENATER”)
- augmentation du nombre de services accessibles
- avec Shibboleth 2.0, interfaçage avec d’autres produits SAML 2
- connexion avec d’autres fédérations académiques ?

Quelques pointeurs

- site web : **http://federation.cru.fr**
- prendre contact : **federation-admin@cru.fr**
- liste des membres de la fédération : **http://federation.cru.fr/cru/liste_fournisseurs**
- logiciel Shibboleth : **http://shibboleth.internet2.edu**

C’est fini ☺

Questions ?