

JOSY

« Authentification centralisée pour
les applications web »

Paris - 4 février 2010

- Présentations de quelques technologies
 - OpenId
 - CAS
 - Shibboleth

- Retour d'expériences

- Contexte : applications web

- Identification
 - associer un identifiant à une ressource
 - personne : login, certificat, URL
 - service : URL

 - choix de l'identifiant non trivial

■ Authentification

- vérification de l'identité d'une ressource
 - simple : ce que je connais → mot de passe
 - ce que j'ai : clé privée, calculatrice, carte à puce, information biométrique
 - simple ou forte
- 2 facteurs : ce que je possède + ce que je sais

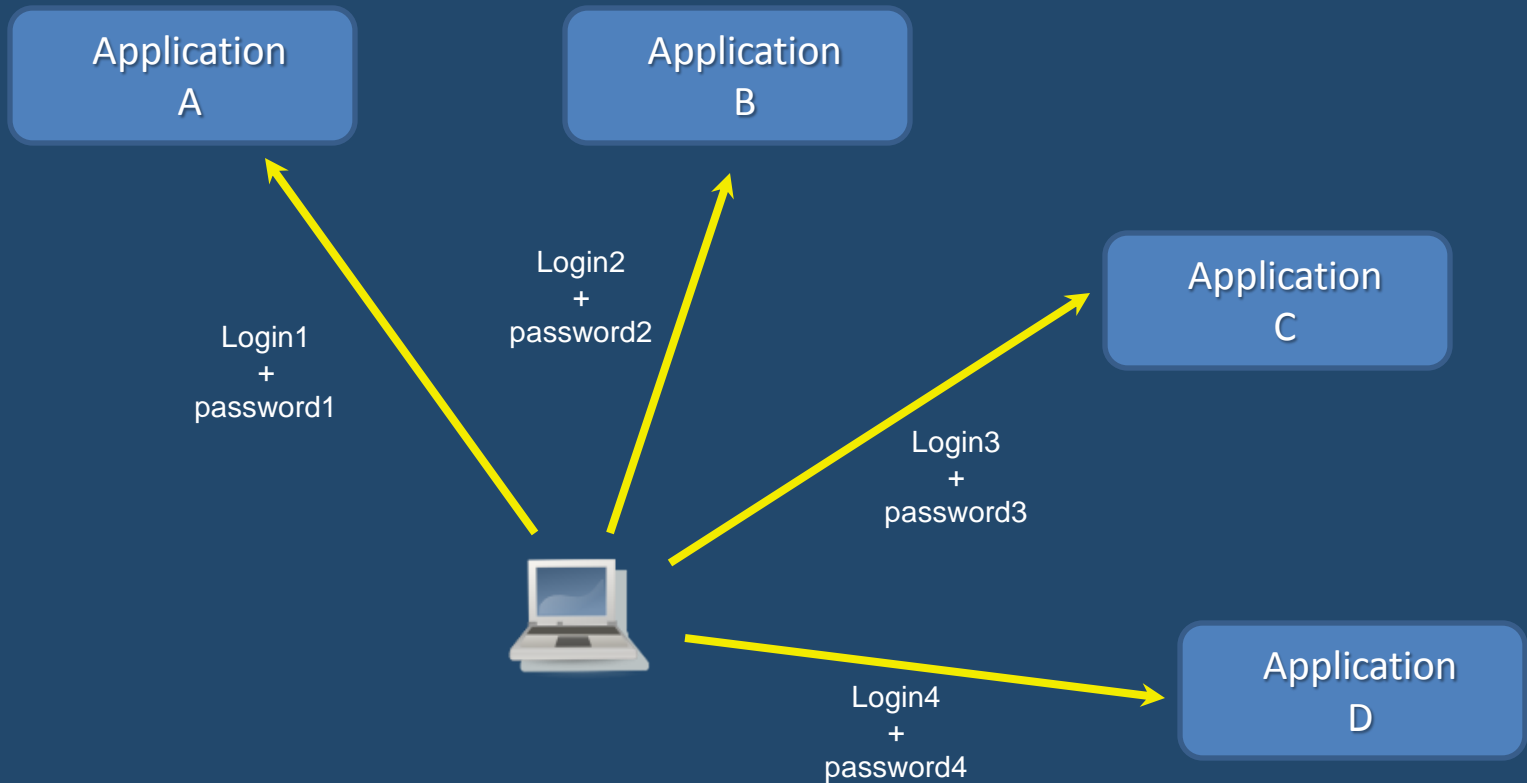
■ Autorisation

- Vérification des droits d'une ressource authentifiée

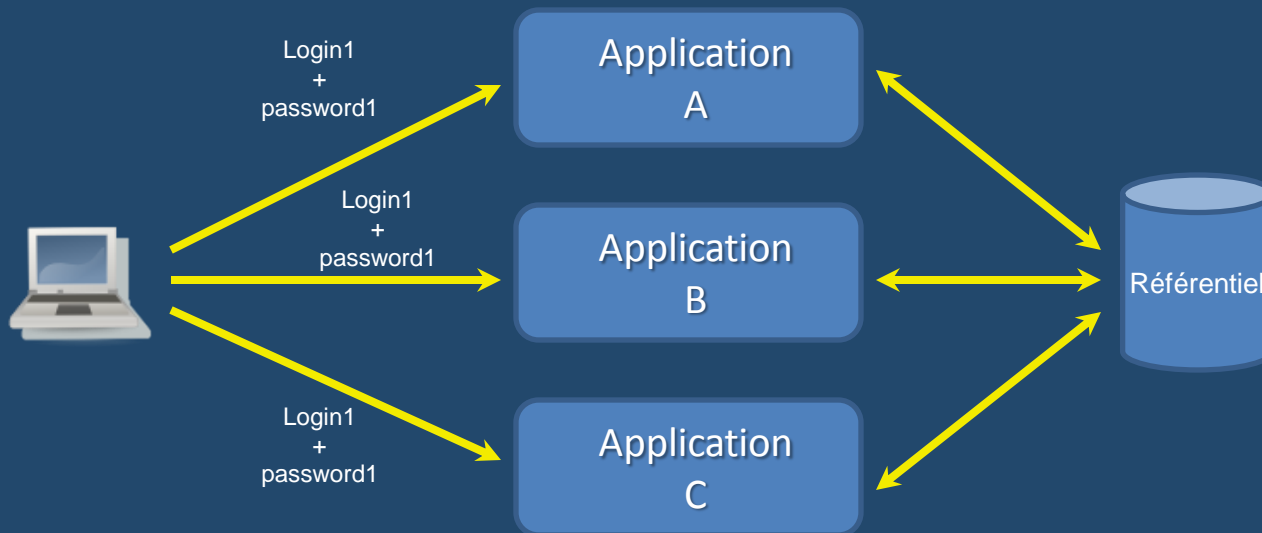
Les droits peuvent être fonction

- de l'authentification
 - d'informations associées à la ressource authentifiée →
profils
-
- séparer authentification et autorisation

- Une application = 1 compte



- Centralisation des informations de comptes
Ex : annuaire ldap, ...
 - Les utilisateurs n'ont qu'un seul compte
 - authentification sur chaque application

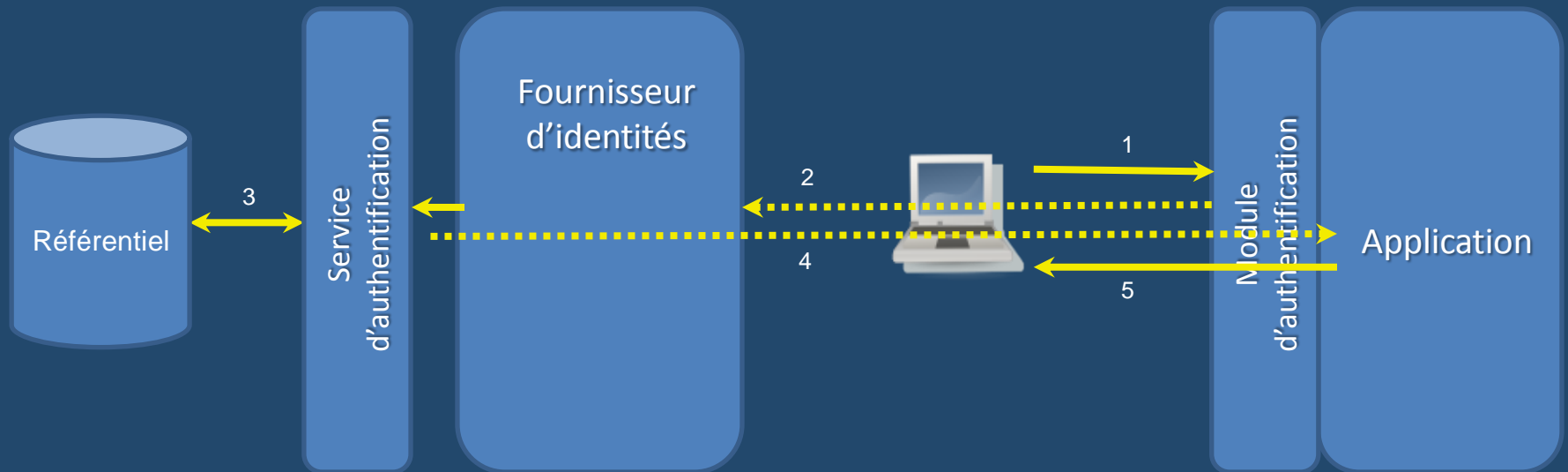


→ Référentiel

- Service d'authentification centralisé
 - CAS, Shibboleth, OpenId, ...
 - Délégation de l'authentification par les applications auprès d'un fournisseur d'identités
 - Nécessité de cercles de confiance
 - En général, fonctionnalité de **Single Sign On**, mais pas forcément

- Service de gestion de l'authentification et des autorisations
 - Mêmes technos + propagation d'attributs
 - Référentiels enrichis (informations de profils, rôles, fonctions, ...)
 - Nécessité d'outils de gestion des référentiels (gestion de groupes, ...)
 - Centralisation des données \neq centralisation de la gestion

■ Architecture générale



- Nécessité de référentiels contenant
 - les identifiants
 - éventuellement
 - des informations d'authentification (mot de passe, ...)
 - des informations de profils

- Technos :
 - bases de données (mysql, postgres, oracle, ...)
 - annuaires (LDAP, ...)

- Issus du système d'information de l'organisme (quand il y en a un)
- Nécessité de schémas communs inter-organismes (ex. SuppAnn)

→ un projet en soi

	Intra- organisme	Inter- organismes	Individuel
OpenId	?	x	x
CAS	x		
Shibboleth	x	x	

- Les +
 - Pour les utilisateurs
 - Confort par le biais de l'unicité de leur compte et de la fonction SSO.
 - Pour les administrateurs
 - Possibilité de déléguer complètement la gestion de l'authentification et des droits au fournisseur d'identités
 - Pour l'organisme
 - Amélioration de la sécurité des accès aux applications
 - Amélioration de la qualité des données du système d'information.
- Les -
 - Difficulté de mettre en place un référentiel de qualité
 - Ressources très critiques

- Actuellement, séparation entre
 - authentification postes de travail
 - authentification web

➔ vers une authentification unifiée