JOSY

« Authentification centralisée pour les applications web »

Paris - 4 février 2010

Sommaire de la journée

- Présentations de quelques technologies
  - OpenId
  - CAS
  - Shibboleth

- Retour d'expériences

➔ Contexte : applications web

Rappels

- Identification
  - associer un identifiant à une ressource
    - personne : login, certificat, URL
    - service : URL
  - choix de l'identifiant non trivial

Rappels

- Authentification
  - vérification de l'identité d'une ressource
    - simple : ce que je connais ➔ mot de passe
    - ce que j'ai : clé privée, calculette, carte à puce, information biométrique
    - simple ou forte

    ➔ 2 facteurs : ce que je possède + ce que je sais

Rappels

- Autorisation

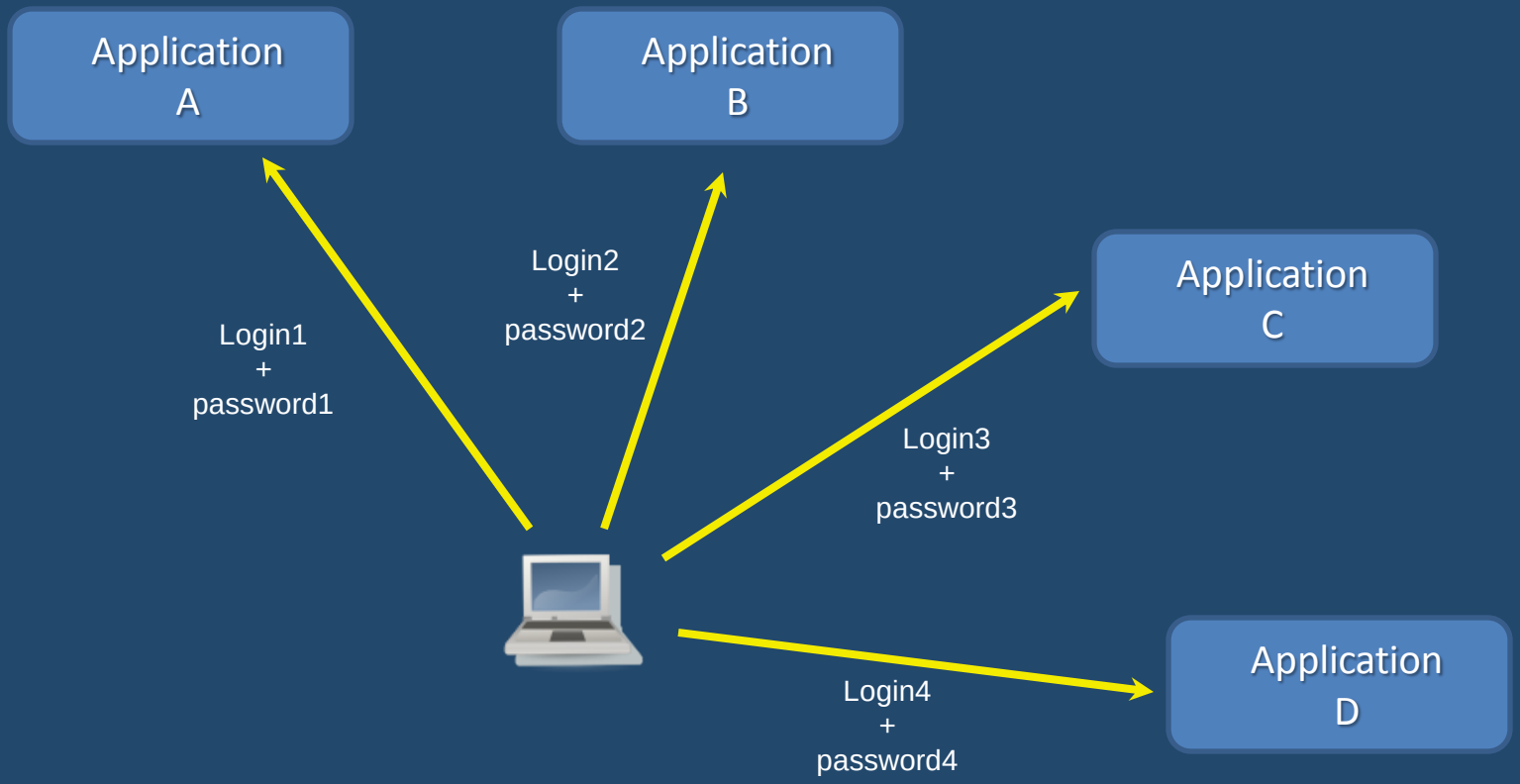
  - Vérification des droits d'une ressource authentifiée

    Les droits peuvent être fonction
    - de l'authentification
    - d'informations associées à la ressource authentifiée ➜ profils

  - séparer authentification et autorisation

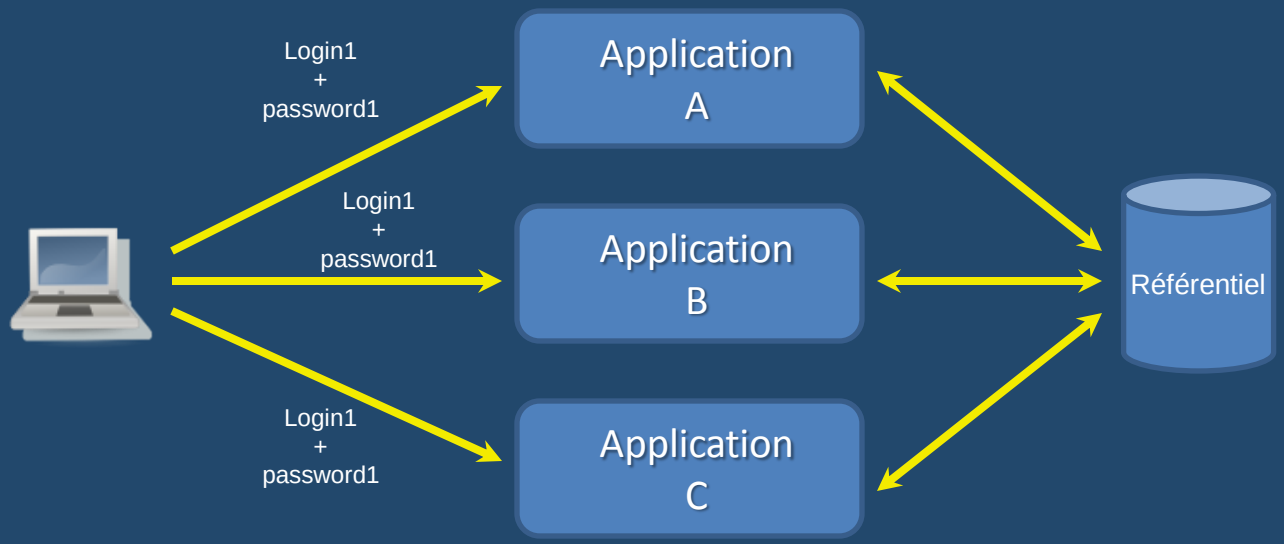
A l'origine

- Une application = 1 compte



L'étape 1

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



→ Référentiel

L'étape 2

- 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

L'étape 3

- Service de gestion de l'authentification et des autorisations
  - Mêmes technos + propagation d'attributs

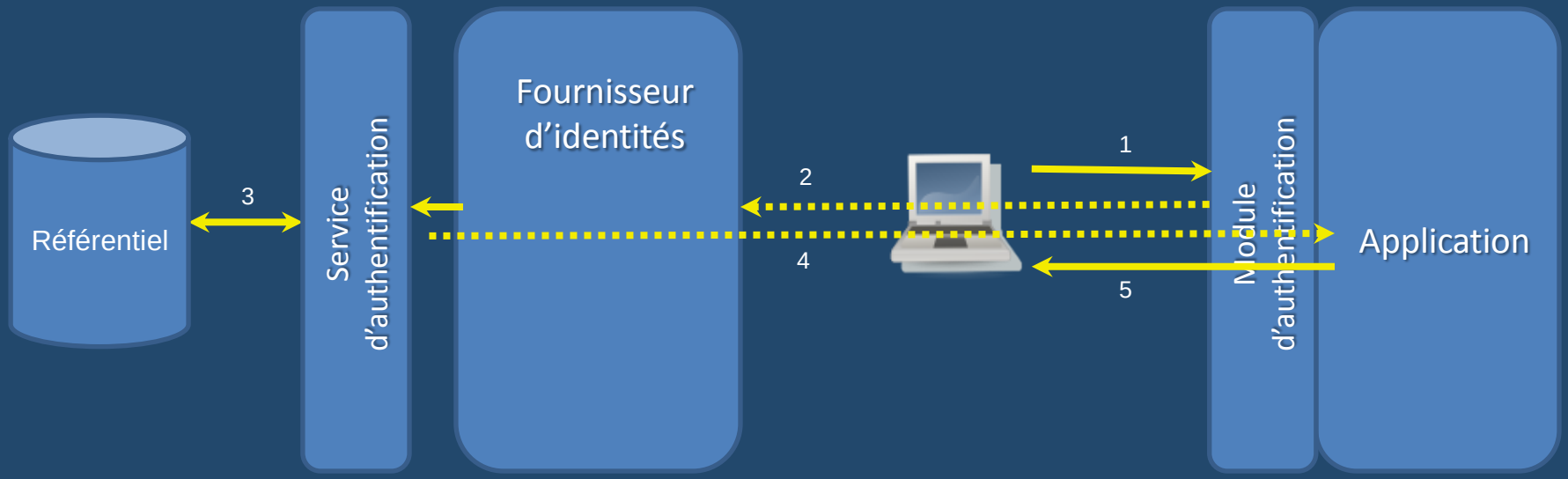
    ➜ Référentiels enrichis (informations de profils, rôles, fonctions, ...)

    ➜ Nécessité d'outils de gestion des référentiels (gestion de groupes, ...)

  - Centralisation des données ≠ centralisation de la gestion

Architecture

- Architecture générale



Référentiels

- 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, ...)

Référentiels

- 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

Les technologies

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

Conclusions

- 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

L’avenir

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

➡ vers une authentification unifiée