CAPITOUL – 18/10/2007

Problématique de l'authentification unique et de la fédération d’identités

Concepts

- Identité : ensemble des éléments qui définissent une entité (personne, programme, machine…)
- Identifiant : information permettant d'associer une entité à son identité
- Authentification : mécanisme destiné à vérifier une identité
- Autorisation : permission d'accéder à des ressources une fois authentifié

Pourquoi ?

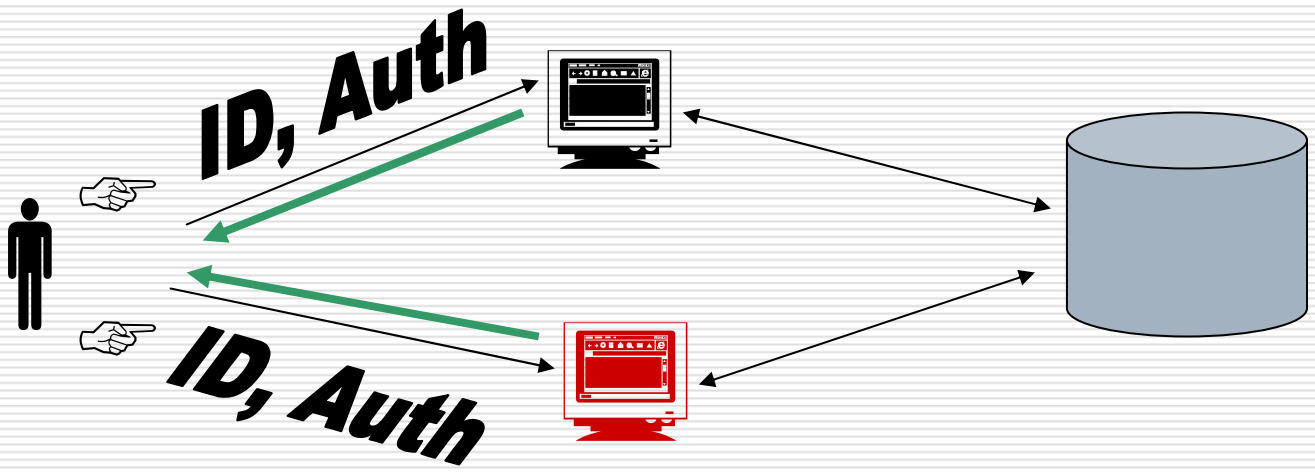
- Obtenir des autorisations d'accès à de nombreux types de ressources
  - Type système
    - Ouverture de session locale (connexion au poste de travail) ou distante (Telnet, FTP, ssh…)
    - Accès à des données (système de fichiers local ou distant, messagerie…)
  - Type applicatif
    - Web
    - Enregistrements dans une base de données
- Des technologies très variées
- Qu'il va falloir gérer

Comment

- **Organisme unique** : la liste des utilisateurs est connue et peut être recensée
  - **Identifiant et authentifiant uniques** : l'utilisateur s'authentifie sur tous les systèmes et applicatifs avec les mêmes "valeurs"
  - **Single signed on** : l'utilisateur s'authentifie **une seule fois** sur tous les systèmes et applicatifs avec les mêmes "valeurs"
- **Fédération d'identités** : "partage" de listes d'utilisateurs entre entités
- Les identifiants et authentifiants peuvent être :
  - un couple login/mot de passe,
  - un certificat,
  - une carte à puce…

Identifiant et authentifiant uniques

- Systèmes d'authentification reposant sur l'utilisation d'annuaire(s) unifié(s)
  - Un seul annuaire
  - Un ensemble d'annuaires synchronisés
  - Ex : NIS, NIS+, LDAP

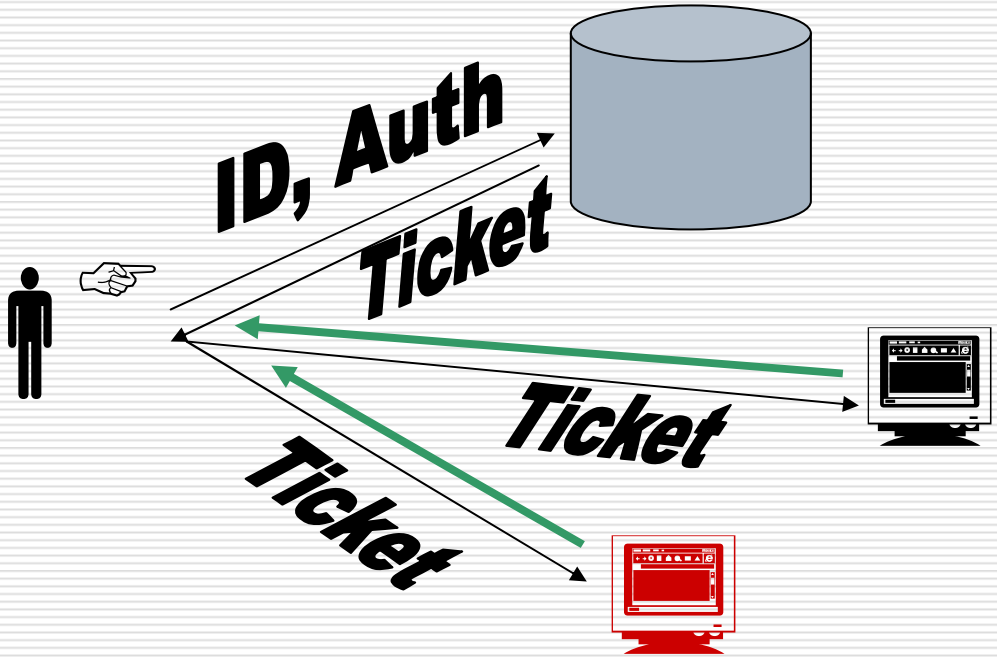


Technologies d'annuaire

	NIS	NIS+	NTDS	LDAP
Plate-forme	Unix		Windows	Multiple
Approche	Ouverte		Fermée	Ouverte
Mise en œuvre	Simple	Complexe	Simple	Complexe
Extensibilité	Lourde Lourde		?	Native
Sécurité	Non	Oui		

Single signed on (SSO)

- Système d'authentification, avec un annuaire centralisé, délivrant des tickets
- Ex: Kerberos, Active Directory, CAS



Single Signed On (SSO)

- Active Directory
  - DNS
  - LDAP
  - SSO par Kerberos
- « Kerberisation »
- « Cassification »

Fédération d'identités

- Objectifs
  - Éviter de dupliquer les informations
  - Fournir un mécanisme de SSO entre entités
  - Favoriser le respect de la vie privée
- Concepts
  - Délégation de l'authentification
  - Propagation des attributs utilisateur
  - Fournisseur d'identité
  - Fournisseur de service
- Principalement réservée aux applications web

Fédération d'identités

- Cercle de confiance
  - Identités et attributs valides
  - Utilisation des attributs aux fins prévues
  - Disponibilité du service
- Mise en œuvre
  - Approche centralisée
    - ⇨ Un seul annuaire
  - Approche fédérative
    - ⇨ Plusieurs comptes liés
  - Approche coopérative
    - ⇨ Comptes répartis

Prérequis organisationnels

- Référentiel unique et valide
  - Identifier les sources de données, les informations requises par les annuaires
  - Décrire les circuits de circulation de l'information, de mise à jour
  - Définir le cycle de vie des comptes
- Décider des annuaires à mettre en place et des informations nécessaires

Prérequis techniques

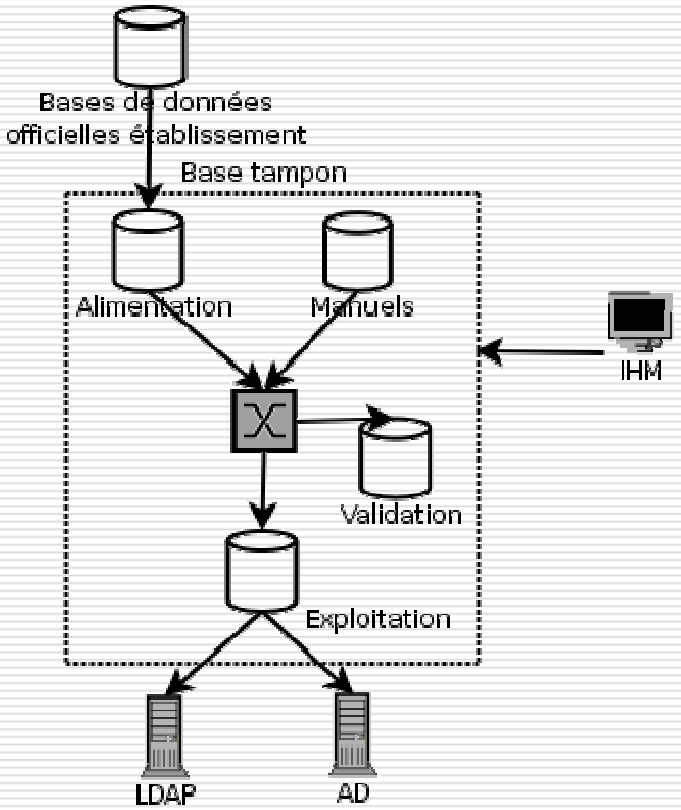
- Authentifiants uniques
  - "LDAPiser" les applications
  - Déjà vrai pour les nouvelles applications web
  - Plus difficile pour les anciennes applis
- Single signed on
  - "Cassification" ou "kerberization" des applications
  - Opération relativement complexe

État des lieux – INSA [1]

- 2003 : Mise en place d'un annuaire LDAP pour l'authentification système
- 2007 : Référentiel unique dont découlent un annuaire LDAP et un annuaire Active Directory
  - Connexion aux systèmes Unix / Windows
  - Gestion du courrier électronique
  - Accès aux sites webs internes avec authentification
  - VPN / Réseaux invités (filaires et sans fil)
    - ⇨ Ressources documentaires électroniques
  - Accès réseau inter-établissements
  - Annuaires d'entreprise papier et web

État des lieux – INSA [2]

- Principe de génération des annuaires



État des lieux – LAAS [1]

- 19?? : Mise en place d'un annuaire NIS pour l'authentification système sur SUN et le mail
- 1999 : Mise en place d'un domaine NT4 puis Active Directory synchronisé avec NIS/NIS+
- 2002 : Mise en place d'un annuaire LDAP synchronisé aux autres
- 2007 : Création d'un compte unique dans tous les annuaires
  - Authentifiant unique pour tous les systèmes
  - Pas d'annuaire unique même si on tend vers LDAP
  - Pas de single signed on

État des lieux – LAAS [2]

- Authentifiants
  - Login + mot de passe
  - Certificats CNRS
- Authentification des applications web
  - Utilisations de modules apache :
    - Mod_auth_ldap (LDAP seul)
    - modXLDAPAuth (LDAP + certificats)
  - Modifications d'applications
    - Ex: Sympa
- Manque un référentiel unique

Risques et palliatifs

- Vol d'identité
  - Imprudence de l'utilisateur
    - Mot de passe trop « simple »
    - Communication des identifiants
    - Stockage des identifiants (navigateur, à l'extérieur…)
  - Services peu/mal sécurisés
    - Le maillon le plus faible…
- Éduquer/sensibiliser les utilisateurs
- Sécuriser les systèmes
  - Chiffrement des communications
  - Authentification forte
  - Réactivité en cas de « vol » des identifiants