Une solution d'authentification unifiée dans un réseau hétérogène

Arnaud ANTONELLI
Samson BISARO
Christian MAILLARD

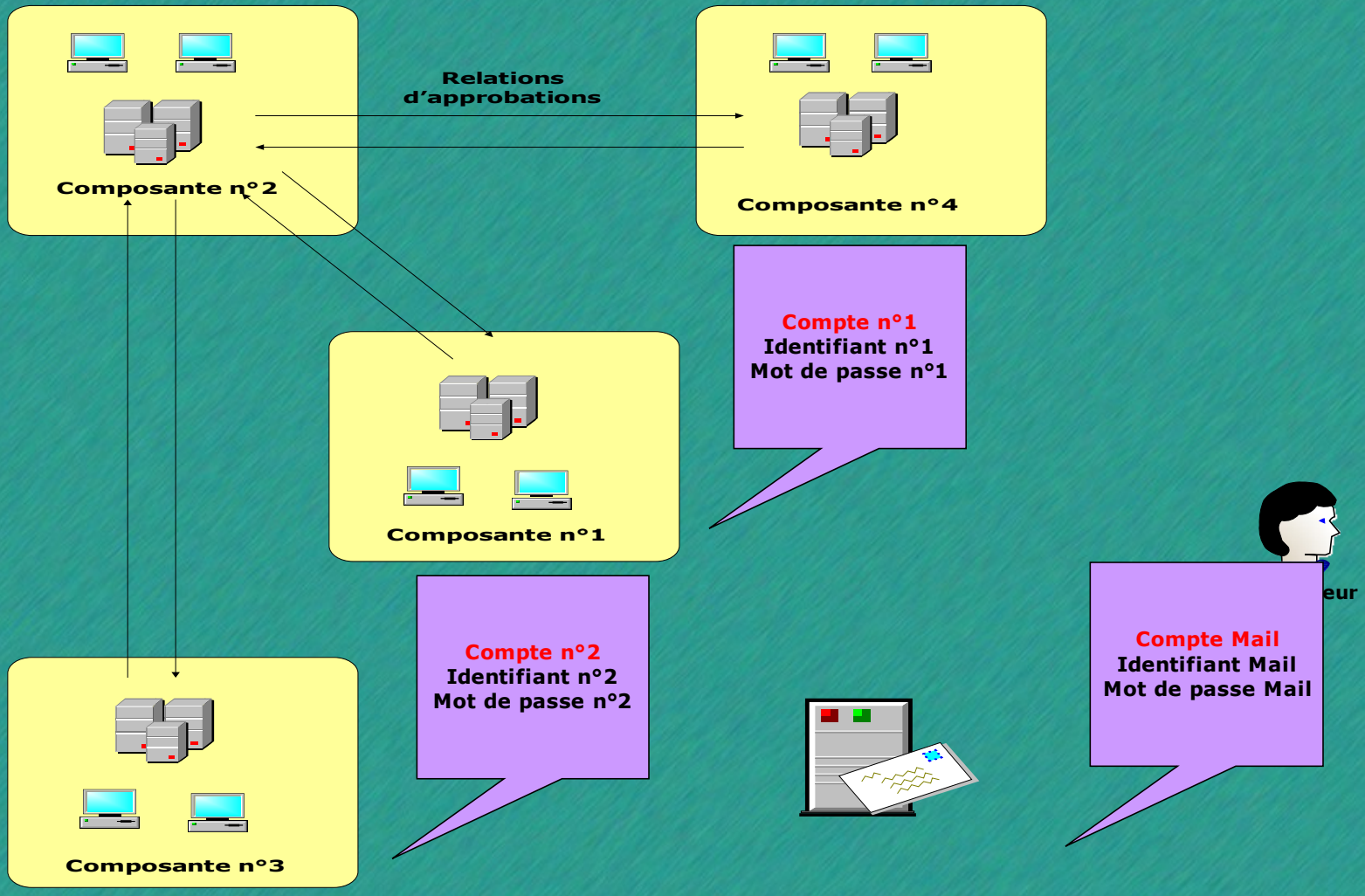
Sommaire

- État des lieux en 1999
- Objectifs
- Composants du projet
- État des lieux en 2005
- Évolutions
- Démonstration
- Questions

Sommaire

- État des lieux en 1999
- Objectifs
- Composants du projet
- État des lieux en 2005
- Évolutions
- Démonstration
- Questions

État des lieux en 1999



Sommaire

- État des lieux en 1999
- Objectifs
- Composants du projet
- État des lieux en 2005
- Évolutions
- Démonstration
- Questions

Objectifs 1/3

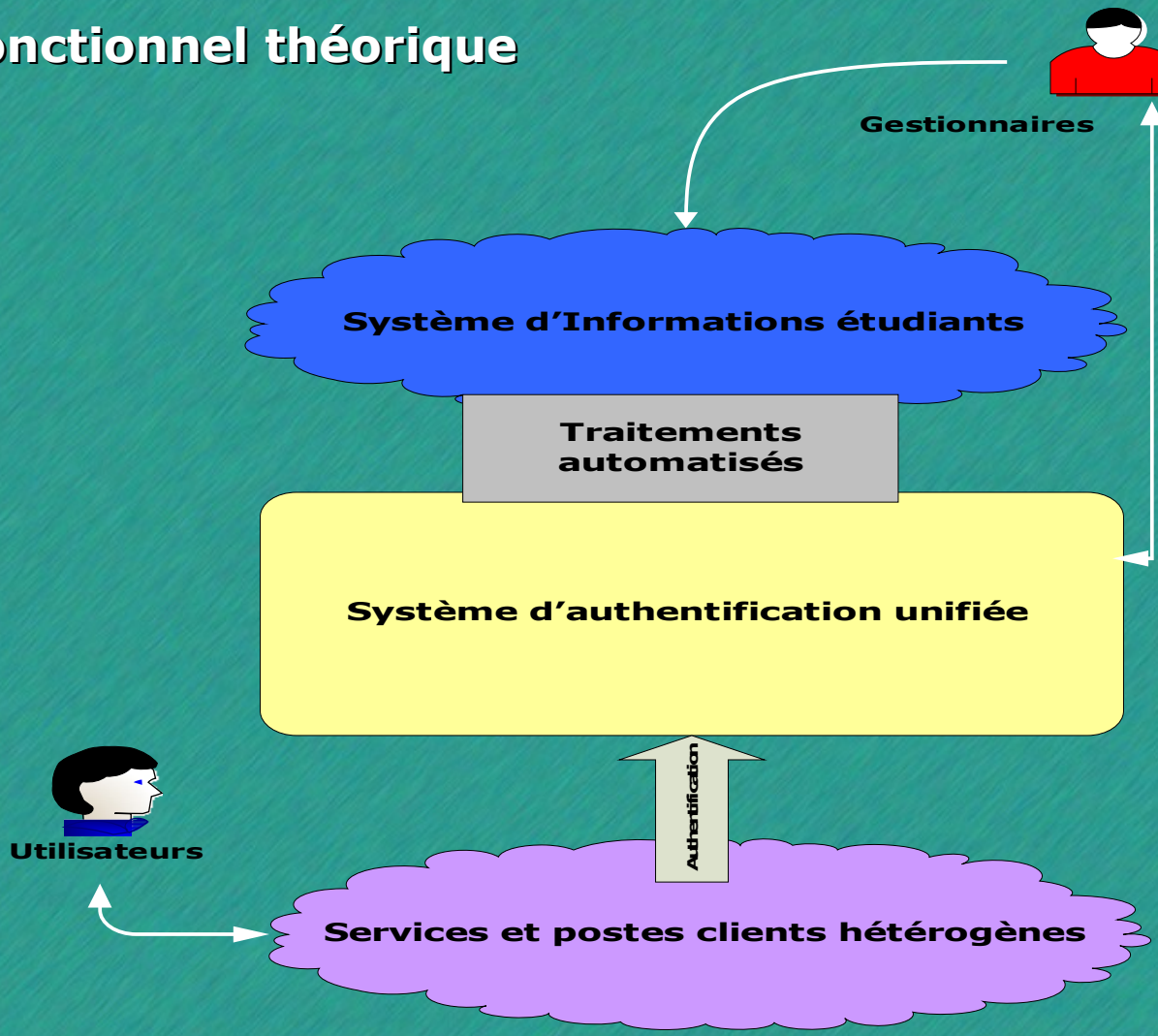
- **Unifier les identifiants des étudiants**
  - 1 seul login / mot de passe
  - 1 seule adresse électronique
- **Simplifier l'administration système**
  - Fiabilisation des bases d'authentification
  - Suppression des relations d'approbation
  - Authentification de toutes les connexions
  - Automatisation de la gestion des comptes

Objectifs 2/3

- **Conserver le mode de fonctionnement**
  - Pas d'ajout de logiciels spécifiques à la solution sur le poste client
  - Conservation des fonctionnalités existantes (GPO, PAM + OpenLDAP, …)
  - Autonomie des Administrateurs des composantes

Objectifs 3/3

Schéma fonctionnel théorique



Sommaire

- État des lieux en 1999
- Objectifs
- Composants du projet
- État des lieux en 2005
- Évolutions
- Démonstration
- Questions

Composants du projet

- La base d'informations
- Le serveur LDAP
- L'annuaire Active Directory
- La synchronisation des mots de passe
- Les outils d'administration

La base d'informations « LOGIN » 1/2

- **Les objectifs**
  - Générer le login et l'email de l'étudiant
  - Sélectionner les informations utiles à la gestion des comptes de l'étudiant
  - Disposer d'une base évolutive
  - Faciliter le traitement des cas particuliers
  - Mettre à disposition des outils d'accès aux informations de la base

La base d'informations « LOGIN » 2/2

- **La mise en œuvre**
  - Mise en place d'un serveur MySQL
  - Développement d'une bibliothèque en PHP de modules d'accès à la base
  - Extraction journalière d'APOGEE
  - Mise à disposition d'une interface web d'outils d'accès à la base

Le serveur LDAP « ETUMAIL » 1/2

- **Les objectifs**
  - Fournir un service d'annuaire
  - Fournir une base d'authentification
    - Système (Unix/Linux)
    - Serveur de courrier
    - WebMail (ETUMAIL)
    - Tout autre service WEB
  - Fournir des outils d'accès à l'annuaire

Le serveur LDAP « ETUMAIL » 2/2

- **La mise en œuvre**
  - Mise en place d'un serveur OpenLDAP
  - Définition d'un arbre LDAP par UFR puis par diplômes
  - Gestion des différents accès via des ACLS sur les attributs
  - Création et mise à jour automatiques des utilisateurs et des UFR/Diplômes
    - Interrogation journalière de la base «LOGIN»
    - Création journalière des nouvelles boîtes aux lettres
  - Mise à disposition d'une interface web d'outils d'accès à l'annuaire

Active Directory « AD-UHP » 1/3

- **Les objectifs**
  - Etudier les mécanismes d'authentification supportés par le système WINDOWS
  - Conserver les fonctionnalités utilisées par les administrateurs (GPO, contrôle d'accès, …)
  - Fiabiliser les bases d'authentification
  - Supprimer les relations d'approbation
  - Mettre à disposition des outils d'administration de l'annuaire

Active Directory « AD-UHP » 2/3

- **La mise en œuvre**
  - Déploiement d'un mono domaine
    - Supprime les relations d'approbation
    - Fiabilise les bases d'authentification
  - Etablissement de règles
    - Nommage des objets
    - Services autorisés ou interdits
    - GPO communes …

Active Directory « AD-UHP » 3/3

- **La mise en œuvre (suite)**
  - Création d'OU de composantes
    - Délégation de contrôle
    - Gestion des ordinateurs et des GPO
    - Indépendance des administrateurs
  - Création et mise à jour automatiques des utilisateurs et des groupes
    - Interrogation journalière de la base «LOGIN»
    - Stockage dans une OU spécifique indépendante des OU de composantes.
    - Utilisation par les administrateurs des groupes créés
  - Mise à disposition d'une interface web d'outils d'accès à l'annuaire

Synchronisation des mots de passe 1/2

- **Les objectifs**
  - Ne pas stocker le mot de passe en clair
  - Unifier les mots de passe
    - Modification instantanée des mots de passe
    - Assurer la concordance des mots de passe

Synchronisation des mots de passe 2/2

- **La mise en œuvre**
  - Développement de scripts de positionnement de mot de passe
    - Le mot de passe WINDOWS
      - Codage UNICODE
      - Utilisation obligatoire de certificat
    - Le mot de passe LDAP
      - Codage CRYPT, SHA, MD5
  - Passage obligatoire par interface web
  - Désactivation par GPO du changement de mot de passe depuis les postes clients WINDOWS
  - Modification uniquement si les serveurs sont opérationnels

Les outils d'administration « ETUHP » 1/2

- **Les objectifs**
  - Activation et gestion de ses comptes par l'étudiant
  - Mise à disposition des outils de gestion aux personnels
  - Sécurisation des opérations sur les serveurs

Les outils d'administration « ETUHP » 2/2

- **La mise en œuvre**
  - Développement d'une interface web
    - Point d'accès unique aux outils
    - Limitation des connexions directes sur les serveurs
    - Sécurisation des opérations sur les serveurs
    - Adaptation de l'interface en fonction d'un profil
      - Etudiant, gestionnaire, administrateur, …
    - Mise à disposition de personnels non informaticiens
      - Secrétaires, personnels de bibliothèques, …

Sommaire

- État des lieux en 1999
- Objectifs
- Composants du projet
- État des lieux en 2005
- Évolutions
- Démonstration
- Questions

État des lieux en 2005 1/3

Quelques chiffres

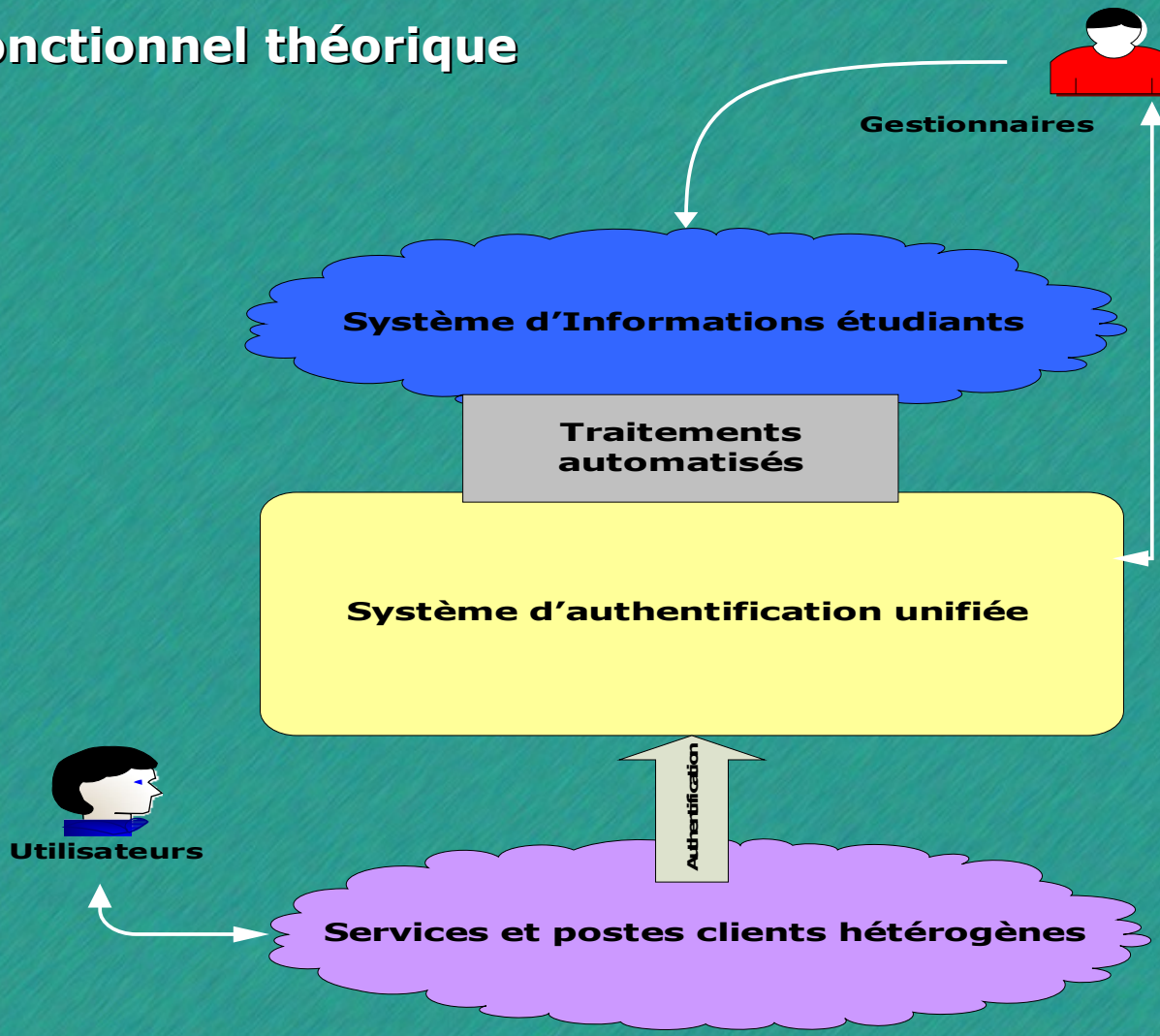
Serveurs d'exploitation	3
Serveurs Active Directory	23
Postes client Windows	770

Étudiants inscrits en 2005/2006	14609
Comptes validés	5955
Entrées dans la base LOGIN	28710

Gestionnaires ETUHP	68

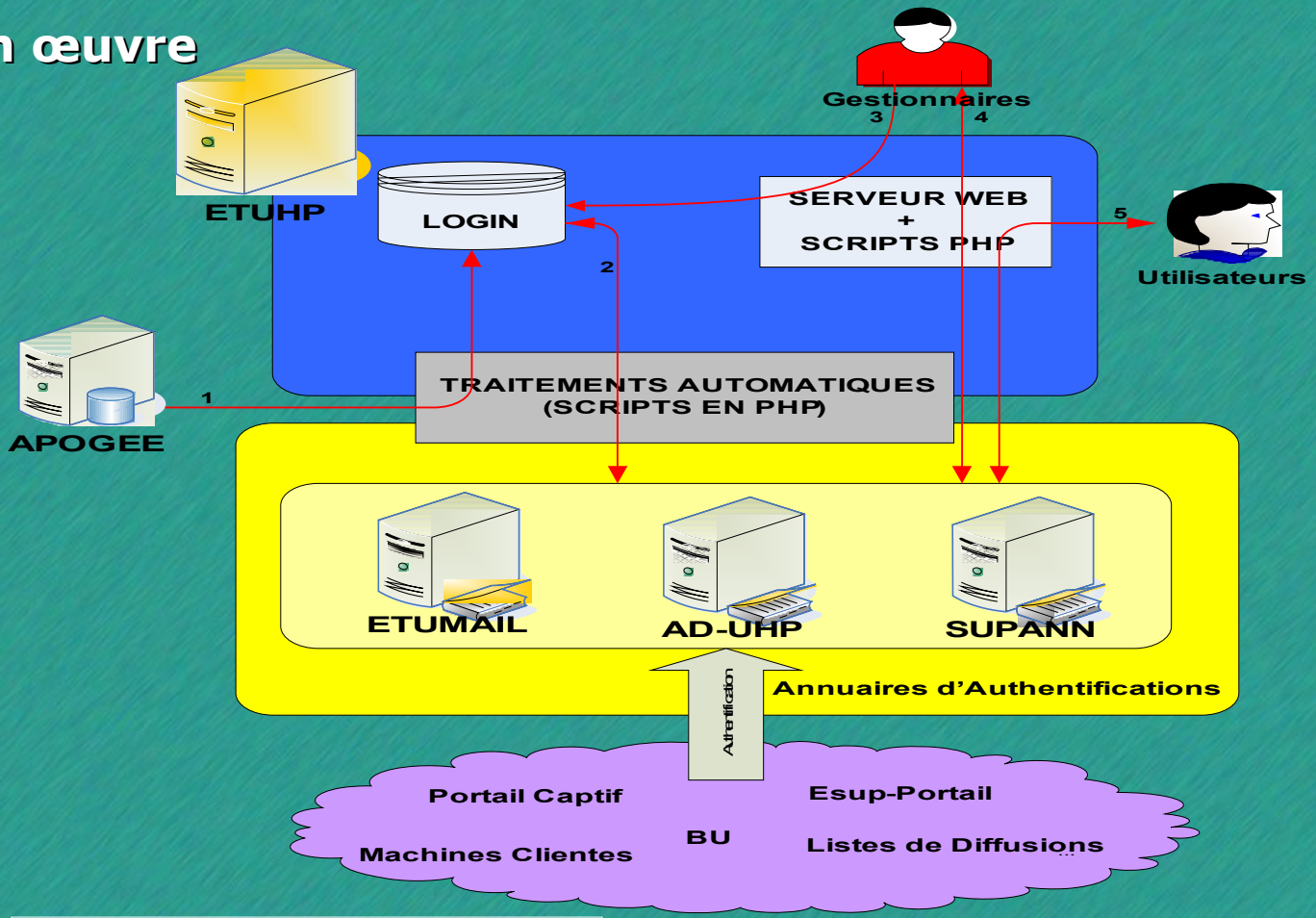
État des lieux en 2005 2/3

Schéma fonctionnel théorique



État des lieux en 2005 3/3

Mise en œuvre



LEGENDE
1 Peuplement journalier de la base LOGIN
2 Synchronisation et mises à jour des Annuaires
3 Ajouts et mises à jour manuelles
4 Consultation et gestion des comptes utilisateurs
5 Récupération et gestion de ses identifiants personnels

Sommaire

- État des lieux en 1999
- Objectifs
- Composants du projet
- État des lieux en 2005
- Évolutions
- Démonstration
- Questions

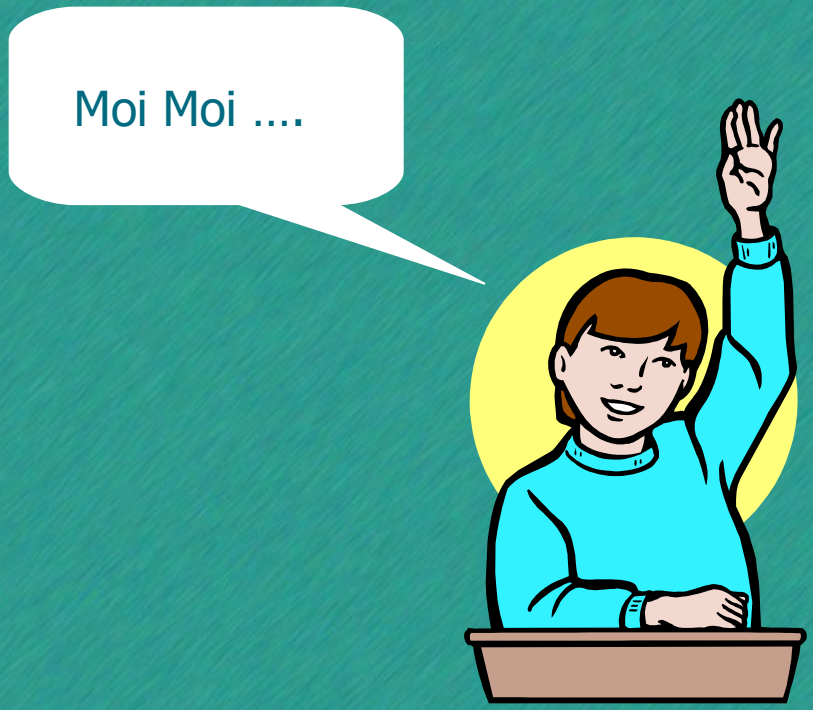
Évolutions

- *Cassification* de l'interface
- Authentification des clients UNIX
  - Validation des services de réplication OpenLDAP
- Fusion des annuaires ETUMAIL et SUPANN
- Traitement des inscriptions multiples
- Extension sur les sites délocalisés
- ...

Sommaire

- État des lieux en 1999
- Objectifs
- Composants du projet
- État des lieux en 2005
- Évolutions
- Démonstration
- Questions

Questions



FIN