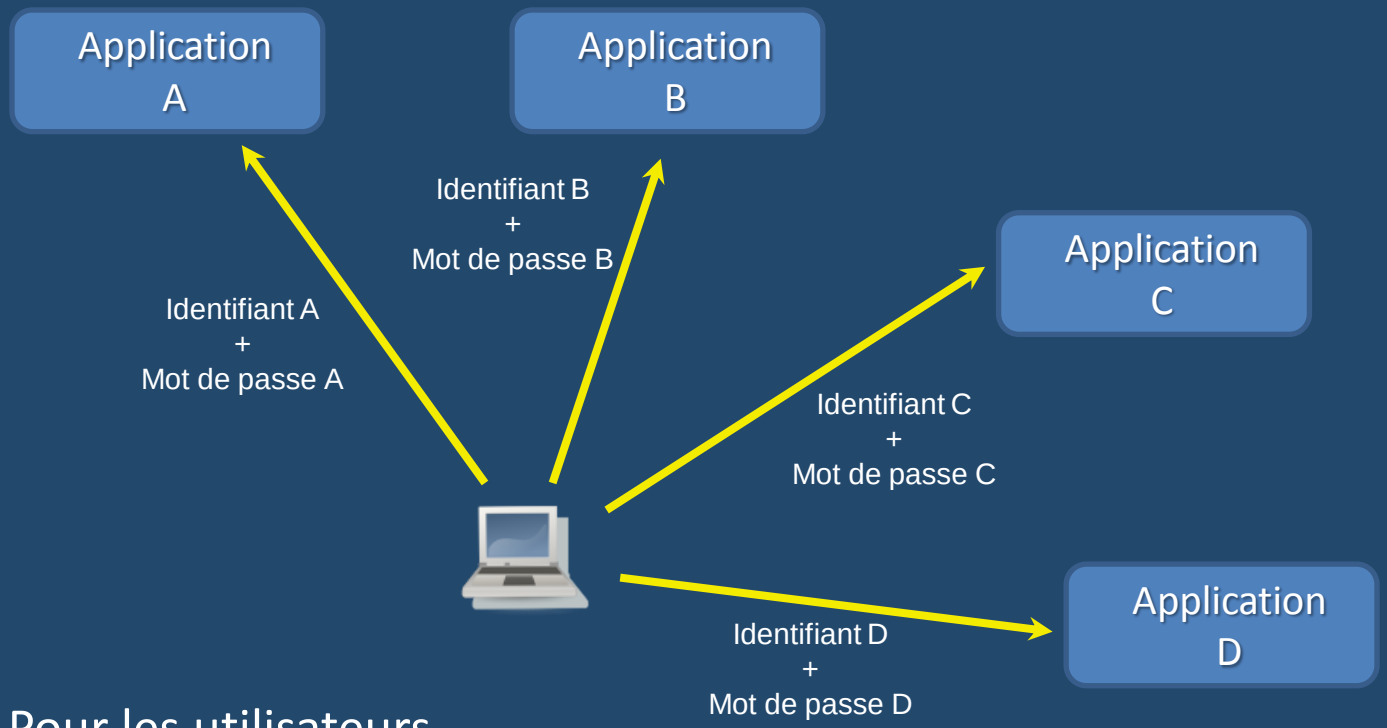
Janus
La gestion des identités au CNRS

Claude Gross
CNRS/UREC

Septièmes Journées Informatiques IN2P3-IRFU

Aux origines

- Une application = 1 compte



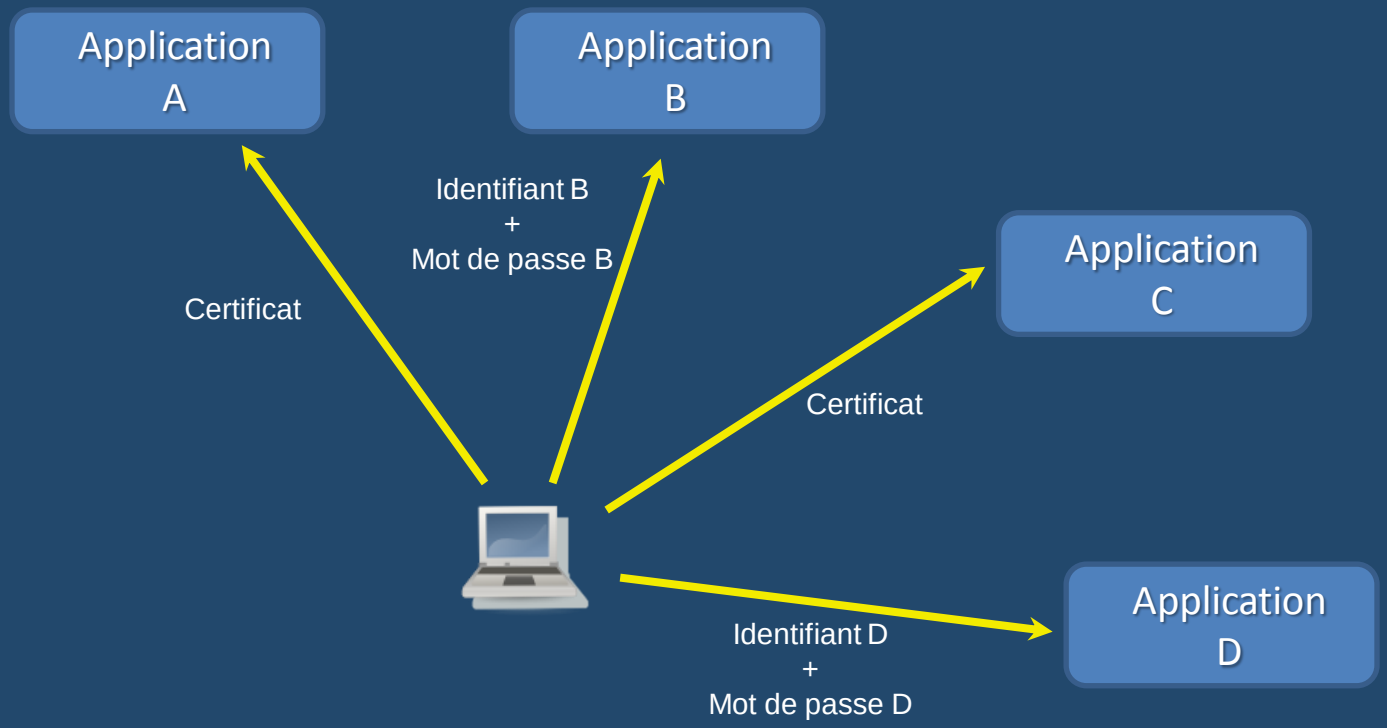
Pour les utilisateurs

➜ Multiplication des comptes

Pour les administrateurs

➜ Gestion des comptes dans chaque applications

- Utilisation des certificats X509



➜ Toutes les applications n'utilisent pas de certificats

➜ Tous les utilisateurs n'ont pas de certificats

Janus : les objectifs

- Fin 2007 : Démarrage du projet Janus
- Les objectifs
  - Une solution d'authentification couvrant l'ensemble des personnels
  - S'appuyant sur le SI existant et compatible avec lui
  - Interopérable avec nos partenaires
  - Permettant la gestion des autorisations

Choix technologiques

- Interopérabilité
  - ➜ Technologie Shibboleth
  - ➜ Fournisseur d'identités CNRS
  - ➜ Référentiel

Référentiel

- Nécessité de disposer d'un annuaire
  - Adressant l'ensemble des personnels des unités
  - Contenant les bons choix d'attributs

- Un projet à part entière
  - Spécification des besoins (instances, populations…)
  - Construction du schéma d'annuaire et alimentation – reprise des données
  - Alimentation, organisation

Référentiel : Identification

- Choix de l'identifiant
  - Choix de l'adresse mail
  - Source : Labintel
    - Information pour les gestionnaires et directeurs d'unités sur les nouveaux usages des données entrées et leur sensibilité

  ➜ Choix pragmatique

Référentiel : Authentification

- Authentification
  - 2 modes :
    - Par certificat personnel CNRS

      { validation du certificat
      + existence email dans référentiel

    - Par identifiant/mot de passe

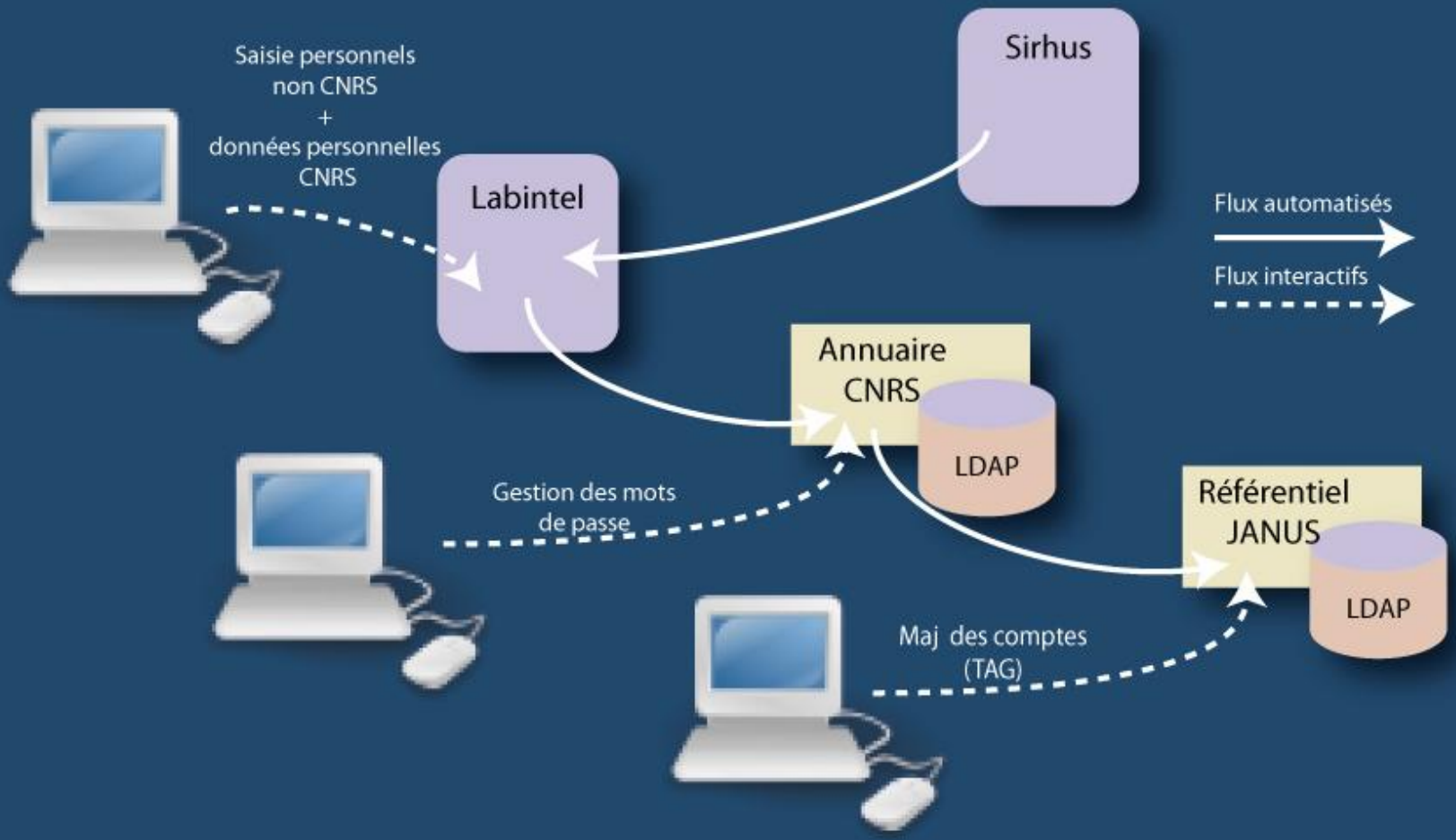
      Identifiant = adresse mail

➜ Service d'authentification CAS

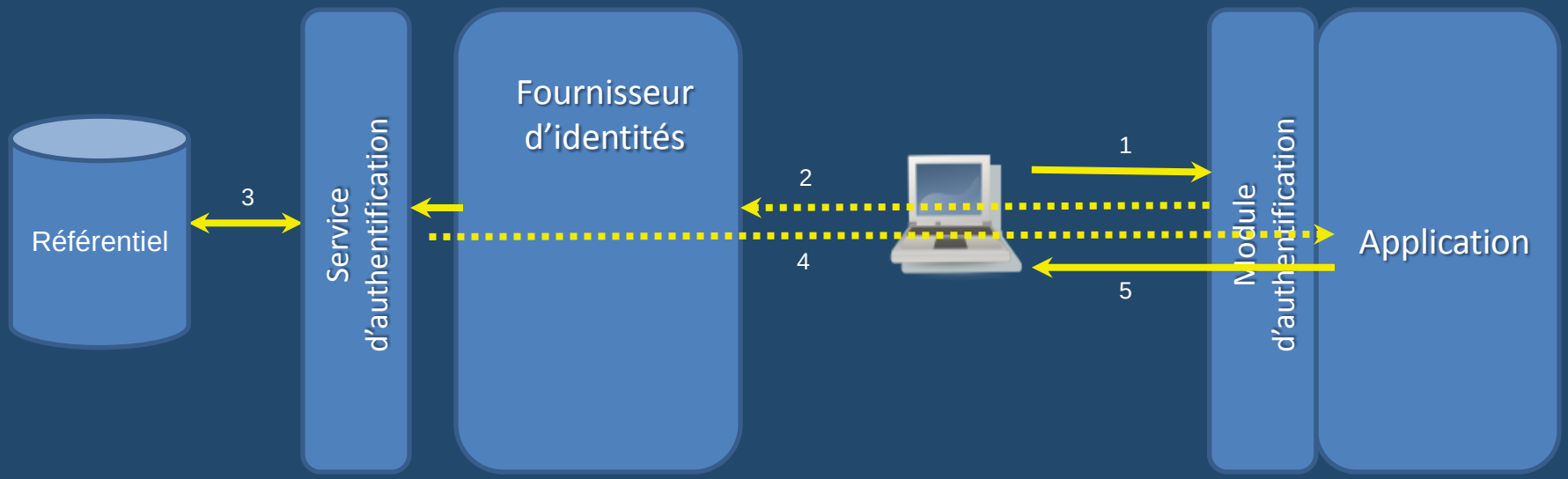
Référentiel - Contenu

- Démarrage avec un annuaire existant puis mis en place d'un nouvel annuaire
- Reprise des informations disponibles dans l'annuaire central (Labintel)
- Ajout d'attributs spécifiques : Tags (définition de rôles) , User SAP, …
- Pour la suite : définir des rôles intéressants à valoriser et les intégrer dans le référentiel (ou dans un autre annuaire)
  - Ex : ACMO, CSSI…
  - Un des buts de la suite de Janus traitant de la gestion des accréditations.

Référentiel - Alimentation



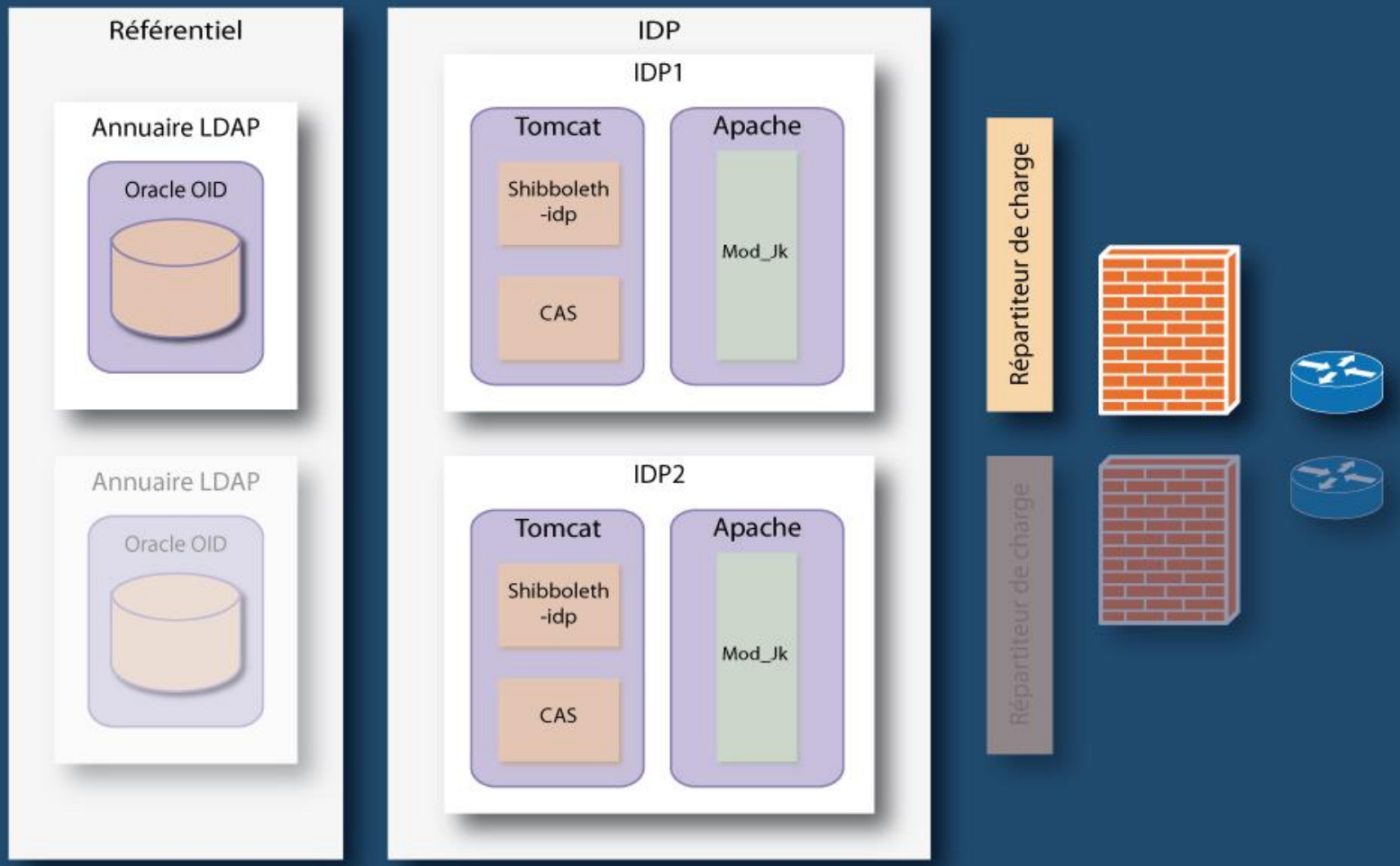
Architecture générale



Architecture IdP - Composants

- IdP : 2 serveurs avec :
  - serveur httpd apache
    - module mod_jk
  - tomcat
    - shibboleth IdP 1.3.3 + extension Hashib
    - CAS
- Référentiel : 2 serveurs LDAP (Oracle OID)
- 2 répartiteurs de charge (BIGIP 3400 – F5)
- 2 pare-feux (CISCO ASA 5540)
- 2 routeurs (CISCO 3845)

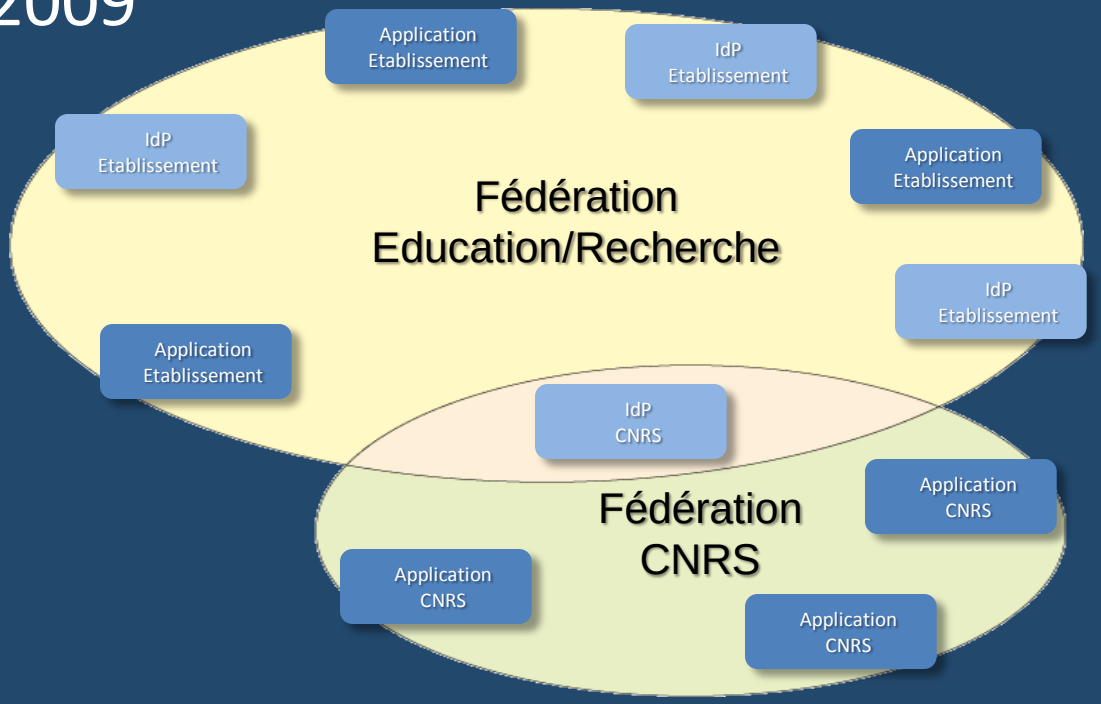
Architecture IdP - Composants



➜ Traitement de la répartition de charge

Bilan

- Le fournisseur d'identités CNRS est opérationnel depuis avril 2008
  - 23 applications nationales et régionales
- Intégration dans fédération Education/Recherche en juillet 2009



Suites du projet : problèmes actuels

- Côté service
  - Qualité du référentiel
  - Criticité du service
    - ➜ Sécurisation du service
    - ➜ Nécessité d'un site de secours

- Côté utilisateurs
  - SSO et compte unique
    - ➜ Accompagnement des utilisateurs
  - Problème de la déconnexion
    - ➜ Problème du SLO : Single logout

Suites du projet : évolutions

- Gestion des habilitations
  - Spécifications d'un ensembles de rôles, fonctions et droits associés
  - Choix des outils de gestion
    - Gestion distribuée
    - Possibilité de délégation

- Référentiel de fonctions ➜ référentiel de personnes

Suites du projet : évolutions

- Niveaux d'authentification
  - Actuellement 2 modes d'authentification
    - Certificat personnel
    - Identifiant/mot de passe
    - Mais : # applications avec # besoins de sécurité

➔ Nécessité de niveaux de confiance

Conclusions

- Les problèmes
  - Technologie complexe
  - Qualité du référentiel
  - Criticité du service
  - Sensibilisation des utilisateurs

Conclusions

- Apports du projet
  - Pour les utilisateurs
    - compte unique et SSO
    - Accès aux ressources de la fédération
  - Pour les administrateurs d'applications
    - délégation de la gestion de l'authentification
    - possibilités de gestion des droits d'accès
  - Amélioration de la sécurité des accès aux applications
  - Amélioration de la qualité des données du SI
  - Disponibilité d'un référentiel des personnels

Questions?