La gestion des identités au CNRS
Le projet Janus

Claude Gross

CNRS/UREC

Janus : les origines

- Fin 2007 : Annonce de l'ouverture d'un service ouvert à toutes les unités CNRS
  - Besoin d'une solution d'authentification sure et couvrant l'ensemble des personnels.
  - Depuis 2001, utilisation des certificats CNRS
    - Constat de la difficulté à couvrir l'ensemble des unités.
    - Problème d'interopérabilité avec les partenaires.

- Démarrage du projet Janus
  - Offrir une solution de gestion d'accès aux applications CNRS, s'appuyant sur le SI existant et compatible avec lui.

Janus : les objectifs

- Objectifs initiaux
  - Disposer d'un service d'authentification centralisé pour les besoins internes au CNRS
  - Disposer d'un outil de gestion des autorisations
  - Interopérabilité avec nos partenaires

    ➜Technologie Shibboleth
- Besoins
  - Un fournisseur d'identités
  - Un référentiel (annuaire des personnels) Authentification
  - Outil de gestion des autorisations

Janus : le contexte

- Projet Contraint en délai
  - 1er client à T+4 mois
- Intégrable dans le SI
  - Identifiant @mail utilisé dans les applications impactant le plus d'utilisateurs.
  - Laisser la possibilité de s'authentifier par user/password ou par certificats CNRS
- Utilisant les briques existantes du SI.
  - Démarrage avec un annuaire incomplet mais déjà en place puis construction d'un nouveau référentiel.
  - Intégration dans une architecture réseau sécurisée déjà en place (pare-feux, DMZ, répartiteur de Charge)

Référentiel

- Besoin de disposer d'un annuaire
  - Adressant l'ensemble des personnels des unités
  - Contenant les bons choix d'attributs
  - Avoir un service hautement disponible

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

Référentiel - Spécifications

- Choix de l'identifiant
  - Pour l'utilisateur = mail « annuaire central »
- Annuaire de fonctions ou de personnes ?
  - Source principale de données = « annuaire central » : annuaire de fonctions
    - Présence et unicité du mail non garanties
  - Référentiel : choix d'un annuaire de fonctions
    - 1 personne avec N fonctions a N entrées dans le Référentiel.
    - Garantie de l'unicité du mail
    - Compte sans mail invalidé

Référentiel - Spécifications

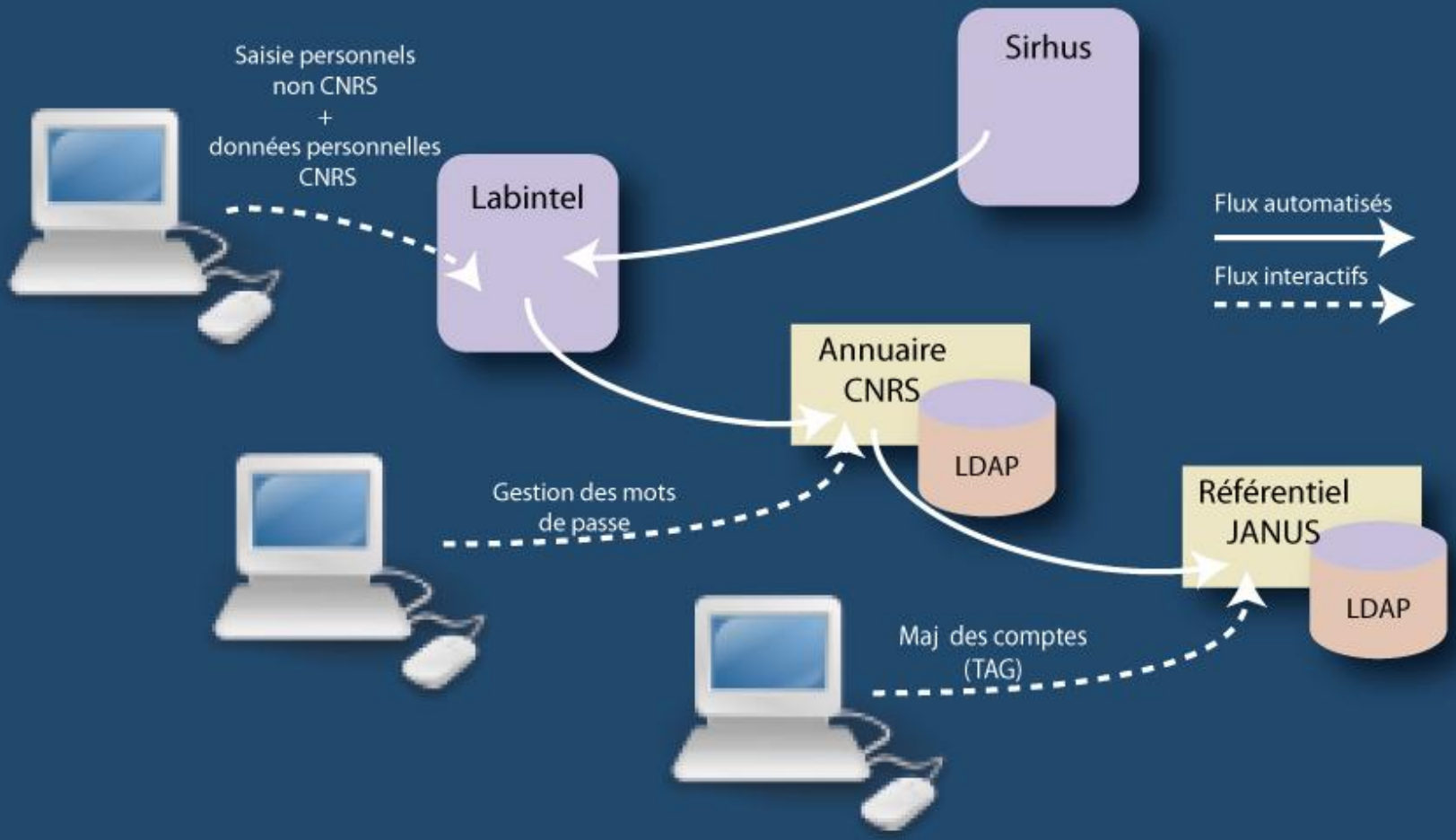
- Règles d'utilisation :
  - pas d'ajout d'entrées manuelles
  - pas de comptes génériques

- Information pour les gestionnaires et directeurs d'unités sur les nouveaux usages des données entrées et leur sensibilité

Référentiel - Contenu

- 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
  - Ex : ACMO, CSSI…
  - Un des buts de la suite de Janus traitant de la gestion des accréditations.

Référentiel - Alimentation



Architecture IdP

- Authentification
  - 2 modes :
    - Par certificat personnel CNRS

      { validation du certificat
      + existence email dans référentiel

    - Par identifiant/mot de passe

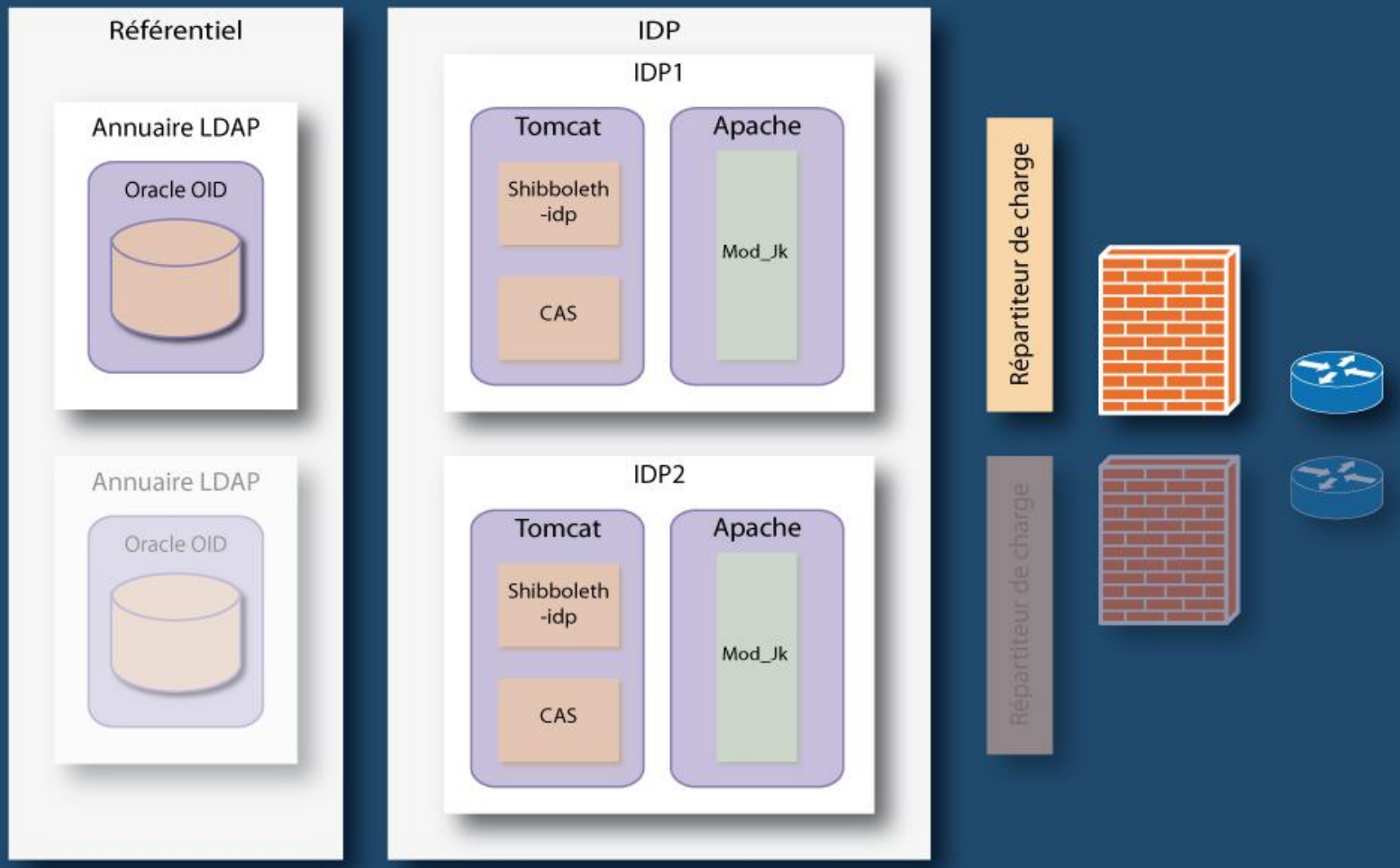
      Identifiant = email

- Service d'authentification CAS

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



Bilan

- Le fournisseur d'identités CNRS est opérationnel depuis avril 2008
- Le nouveau référentiel est opérationnel depuis janvier 2009
- Intégration dans fédération Education/Recherche en juillet 2009

Suites du projet : problèmes actuels

- Sécurisation du service
  - Nécessité d'un site de secours
- Déconnexion
  - Problème du SLO : Single logout
- SSO et compte unique
  - Accompagnement des utilisateurs

Suites du projet : évolutions

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

Suites du projet : évolutions

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

→ Nécessité de niveaux de confiance

Conclusions

- Les problèmes
  - Référentiel de fonctions ➜ référentiel de personnes
  - Technologie complexe
  - Qualité du référentiel
  - Criticité du service
  - Les utilisateurs
  - Quels niveaux de sécurité pour l'authentification?

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?