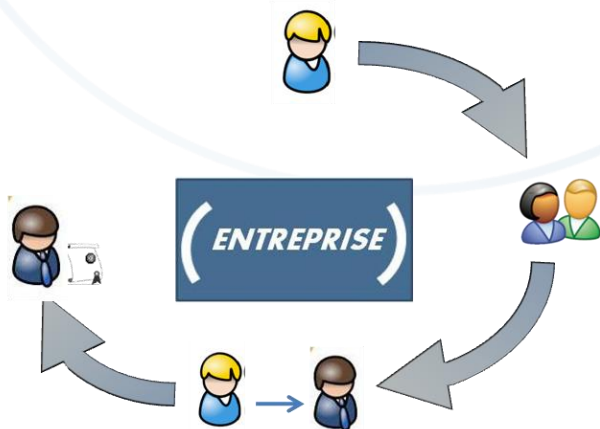




# La gestion des identités et des accès

Guillaume Garbey (Consultant sécurité)

Contributeurs: Gilles Morieux, Ismaël Cisse, Victor Joatton



*Lyon, le 25 février 2009*

# AGENDA

---

---

- ✔ Introduction à la gestion des identités et des accès
  - ✔ Enjeux et objectifs
  - ✔ Les fondamentaux de la gestion des identités
  - ✔ Solutions de gestion des identités et des accès
  - ✔ Approche projet "type"
  - ✔ Retours terrains
  - ✔ Questions / réponses
-

# INTRODUCTION À L'IAM

*Une définition de la gestion des identités et des accès*

*Quoi?*

*Historique*

*Contexte*

## UNE DÉFINITION...

---

### ✔ Pourquoi "une" définition?

- Parce que la définition n'a pas toujours été la même; l'idée de gestion des identités et des accès a évolué et a mûri...

### ✔ "La gestion des identités et des accès consiste à gérer le cycle de vie des personnes dans le système d'information"

### ✔ Oui MAIS:

### ✔ "c'est le faire de manière automatisée pour partie et déléguée à un niveau fonctionnel / métier pour le reste"

---

# LA GESTION DES IDENTITÉS ET DES ACCÈS QUOI?

---

## ✓ **La gestion des identités et des droits**

- Constitue un maillon clé dans la chaîne de sécurité des organisations
- Renforce le niveau de sécurité général en garantissant la cohérence d'attribution des droits d'accès aux ressources hétérogènes du SI
- Permet de répondre aux exigences réglementaires de plus en plus fréquentes relatives à la traçabilité.

## ✓ **Consiste à gérer le cycle de vie des personnes**

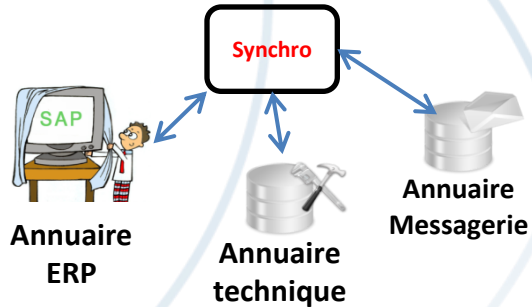
- La gestion doit pouvoir être réalisée d'un point de vue fonctionnel par des non-informaticiens

## ✓ **Solution transverse (globale)**

- Sur la base d'une infrastructure centralisée
  - Avec une gestion fonctionnelle distribuée
-

# HISTORIQUE

Besoin de synchronisation



Cycle de vie des identités ET des accès  
Automatiser et déporter sur  
Des fonctions métier la gestion  
Du cycle de vie

Première  
génération  
le  
désordre...



2 ième  
génération

Annuaire  
LDAP  
spécialisés

3 ième  
génération

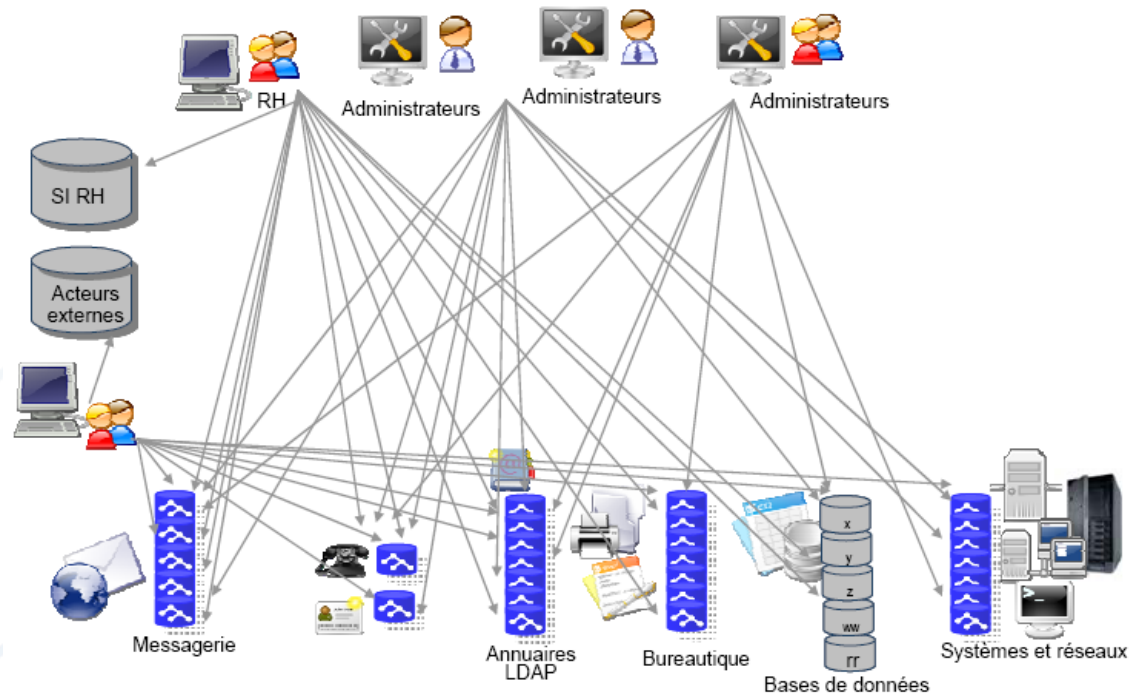
Approche  
service



# CONTEXTE

## ✔ Problématique des référentiels utilisateurs multiples

- Multiplication des applications hétérogènes
- référentiels utilisateurs multiples et incompatibles (SGBD, annuaires systèmes, fichiers plats)



# CONTEXTE

---

## ✔ **Conséquences pour l'utilisateur**

- L'utilisateur doit mémoriser de nombreux couples identifiant/mot de passe
- Risque de l'effet « Post-It sur écran »
- Mauvaise image de l'outil informatique

## ✔ **Conséquences sur l'administration**

- L'administrateur doit gérer de nombreux référentiels utilisateurs au travers de plusieurs consoles et développer de multiples compétences spécifiques
- Traitements manuels et répétés

## ✔ **Conséquences sur l'intégrité des données**

- Gestion de batchs de synchronisation à intervalles réguliers
- ETL ou développements spécifiques

## ✔ **Conséquences sur la sécurité**

- Niveau de sécurité incertain
  - Niveau de sécurité global = niveau de sécurité de l'application la moins sécurisée
-

# ENJEUX ET OBJECTIFS

*Synthèse des besoins métier*

*Vision globale – champ d'application*

*Couverture & exigences fonctionnelles*

*Objectifs opérationnels*

*Les gains*

# SYNTHÈSE DES BESOINS MÉTIERS

---

- ✔ **Réduire les coûts** en mettant en place une solution automatisant un grand nombre de tâches habituellement effectuées manuellement.
  - ✔ **Limiter le risque sécuritaire** en contrôlant les accès utilisateurs ainsi que leurs autorisations sur les différents composants du SI en impliquant le cœur du métier.
  - ✔ **Alignement sur les normes réglementaires** : la mise en place de procédures de validation électroniques des demandes et de détection des divergences permet d'atteindre un alignement avec les normes telles que SOX et de répondre aux besoins d'audit.
  - ✔ **Améliorer la traçabilité des accès** en fournissant des rapports et une vision temps réel de l'ensemble prérogatives des collaborateurs du groupe à partir d'une plate forme unique.
  - ✔ **Conserver l'historique des actions de demande d'habilitations** et de droits afin d'être capable de produire des rapports sur les processus et droits des personnes
-

# VISION GLOBALE – CHAMP D'APPLICATION

---

- ✔ Gestion des **Identités** et des **Accès** (GID)
  - ✔ GID couvre la gestion de l'affectation des droits aux utilisateurs selon leurs métiers..
  - ✔ GID réconcilie les différents annuaires et référentiels existants. Il assure le provisionnement et la synchronisation bidirectionnelle des annuaires et référentiels.
  - ✔ GID ne remet pas en cause les référentiels et annuaires existants qui restent les références pour les applications (dans la plupart des cas).
  - ✔ Les référentiels existants peuvent conserver leur administration fonctionnelle et technique des habilitations et des ressources : Postes Fonctionnels, Fonctions Applicatives, Ressources techniques, ACL
-

# COUVERTURE FONCTIONNELLE

---

- ✔ **Gestion du référentiel central** des utilisateurs (alimentation référentiels sources)
  - ✔ Gestion du référentiel central des ressources concernées par la gestion des droits d'accès
  - ✔ **Gestion des habilitations** (gestion des profils, rôles, utilisateurs, workflow)
  - ✔ **Provisionnement** : synchronisation des référentiels cibles de sécurité
  - ✔ **Auto administration, gestion par les utilisateurs des mots de passe et des données privées**
  - ✔ **Audit et reporting**
  - ✔ **Contrôle d'accès** : authentification et autorisation
-

## EXIGENCES FONCTIONNELLES (RETOUR TERRAIN)

---

- ✔ **Affecter des Profils techniques aux utilisateurs automatiquement** en fonction de leurs caractéristiques (positive profile).
  - ✔ **Gérer les comptes utilisateurs** ainsi que leurs autorisations sur les systèmes cibles
  - ✔ Permettre de **visualiser** en « temps réel » **les droits des utilisateurs** attribués via la gestion d'identité.
  - ✔ Permettre via un composant de **Workflow** de valider les demandes.
  - ✔ Permettre de détecter les divergences entre les prérogatives théoriques des utilisateurs et la réalité.
  - ✔ Proposer la gestion des accès sous forme de **catalogue de service**
  - ✔ Alimenter périodiquement en données temps réel un système décisionnel gérant l'historique des demandes d'habilitation afin que celui-ci puisse être interrogé pour éditer des rapports et répondre à toute interrogation.
-

# LES OBJECTIFS OPÉRATIONNELS

---

- ✔ **Faciliter l'audit de la gestion des utilisateurs et des droits d'accès** aux applications et aux outils techniques
  - ✔ **Unifier la gestion des demandes d'habilitations** dans le cadre de processus automatisés, sécurisé et optimisé (gain potentiel ETP).
  - ✔ **Identifier rapidement l'ensemble des droits d'accès** d'un utilisateur.
  - ✔ **Fédérer** l'information relative aux utilisateurs et leur accès aux applications dans un annuaire d'administration.
  - ✔ **Compléter l'architecture existante** d'annuaires d'exploitation et de référentiels avec un niveau d'administration globalisé prenant en compte le multi-référentiel : **ex métiers nationaux , portails et annuaire d'entreprise**
  - ✔ **Automatiser la propagation des modifications administratives vers les annuaires d'exploitation et les référentiels** (« provisioning »)
  - ✔ **Mettre en place l'outillage d'administration centralisée de la sécurité**
-

## LES GAINS 1/2

---



**!!! Ne pas oublier le ROI des projets de gestion des identités et des accès !!!**

---

## LES GAINS 2/2



### DIRECTION

- **Conformité** aux réglementations sur l'auditabilité et la traçabilité.
- Des référentiels d'entreprise **exhaustifs et à jour.**



### RSSI

- **Cohérence et contrôle** dans l'attribution des droits sur les ressources.
- **Vision globale** de l'application des règles de l'entreprise.



### ADMINISTRATEURS TECHNIQUES

- **Efficacité, fluidité et simplicité** dans la gestion des utilisateurs.
- **Automatisation** de la gestion des comptes.



### COLLABORATEURS

- **Réactivité** dans la prise en main de leurs comptes et services applicatifs.
- **Ergonomie et autonomie** dans la mise à jour de leurs informations personnelles.



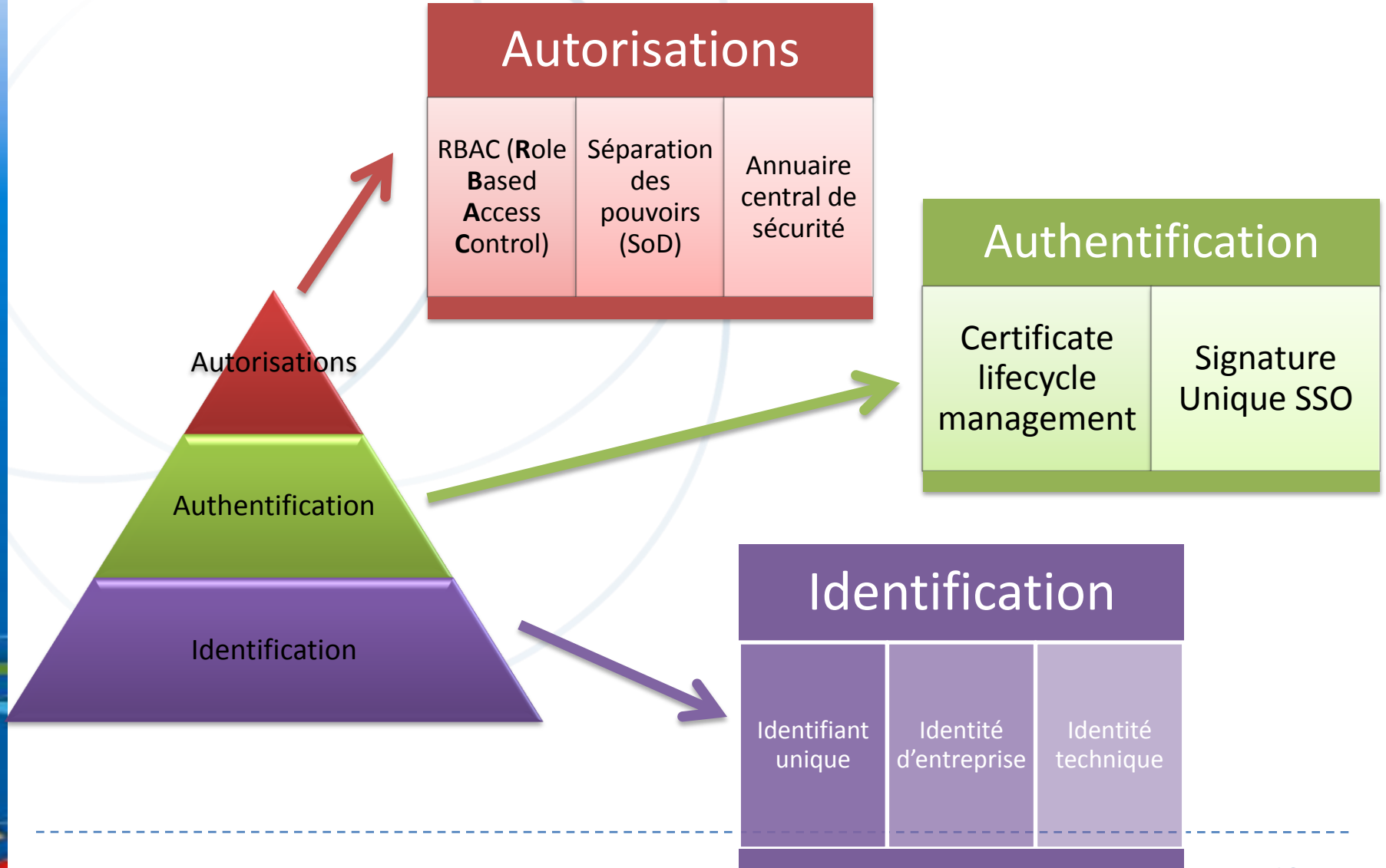
# LES FONDAMENTAUX DE LA GESTION DES IDENTITÉS ET DES ACCÈS

*La pyramide IAM*

*Les composants*

*Modèle RBAC*

# LA PYRAMIDE IAM



# IDENTIFICATION

## Identification

Identifiant  
unique

Identité  
d'entreprise

Identité  
technique

- **Caractériser une personne dans le SI:**
  - **Identifier de manière unique** (fait généralement parti des exigences réglementaires comme SOX, PCI-DSS)
  - **Modéliser les attributs** d'un utilisateur selon:
    - **Identité entreprise** (généralement il s'agit de données dont le référentiel autoritaire est la base RH pour les internes)
    - **Identité technique** (attributs utilisés à des fins techniques telles que les attributs AD, ou des attributs pour automatiser les traitements)
    - **Identité personnelle** (attributs pour lesquels l'utilisateur a la propriété des données – généralement laissée en self-servie; ex: tel portable perso, description perso de métier, ...)

# AUTHENTIFICATION

## Authentification

Certificate  
lifecycle  
management

Signature  
Unique SSO

- **Gestion des mécanismes de vérification de l'identité d'une personne:**
  - **Authentification forte** par certificats (gestion du cycle de vie des certificats dans le respect des exigences des normes visées, ex PRIS V2)
  - **SSO**; Signature unique. Chantier de sécurité qui simplifie la vie des utilisateurs dans le SI...