

AUTORISATIONS

Autorisations

RBAC (Role Based Access Control)	Séparation des pouvoirs (SoD)	Annuaire central de sécurité
----------------------------------	-------------------------------	------------------------------

- **Gestion des autorisations / habilitations dans le SI:**
 - S'appuyer sur la modélisation fonctionnelle et métier du système d'habilitation comme RBAC (Role Based Access Control)
 - Règles de non cumul des pouvoir ; SoD matrices
 - Modélisation d'un annuaire central de sécurité qui permette de gérer les profils, les rôles, les règles d'association et d'attribution, et leur cycle de vie.
 - Permet d'avoir un point centralisé pour l'attribution de l'ensemble des droits dans le SI

LES COMPOSANTS

Services d'annuaire



- Référentiels permettant le stockage et l'administration des comptes, informations d'identité, et crédits (mots de passe, certificats)

Service de gestion du cycle de vie



- Processus et technologies utilisés pour créer, supprimer et gérer les modifications relatives aux comptes et profils, ainsi que pour vérifier la conformité aux stratégies de sécurité ainsi que la conformation aux normes et règles

Service de gestion des accès



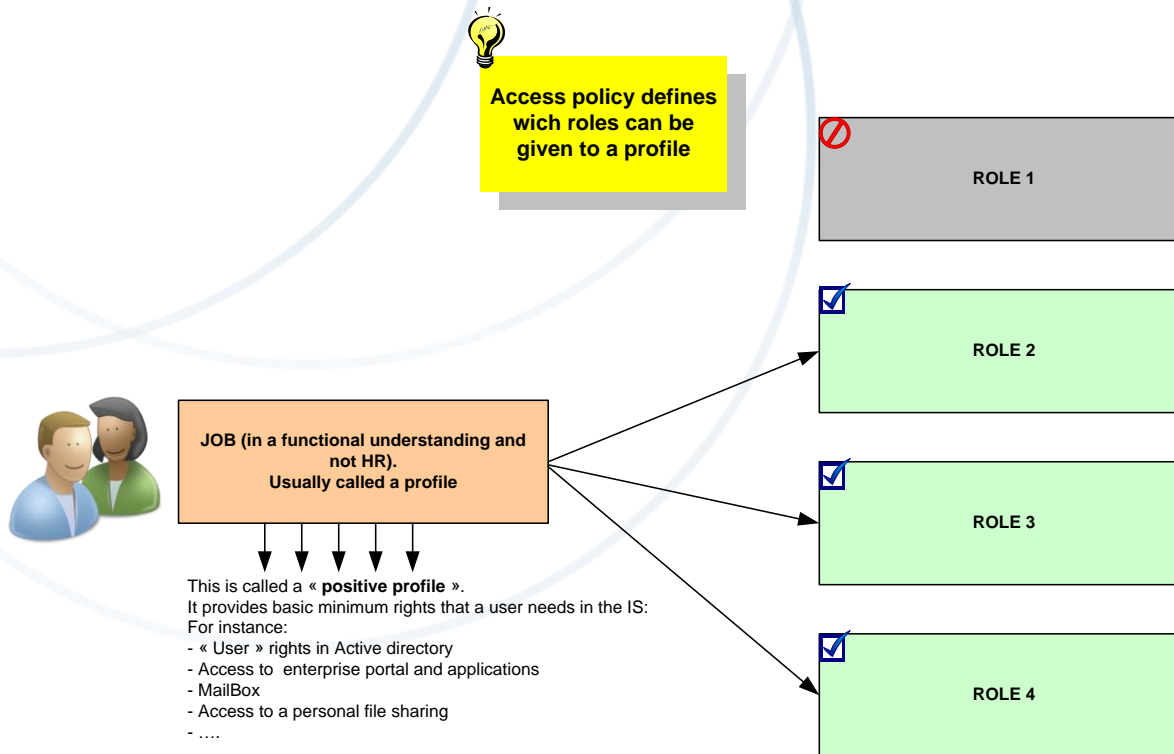
- Le processus d'authentification des crédits et de contrôle d'accès aux ressources basé sur la confiance et l'identité.
- La gestion des habilitations basé sur des modèles tels que RBAC.

MODÈLE RBAC

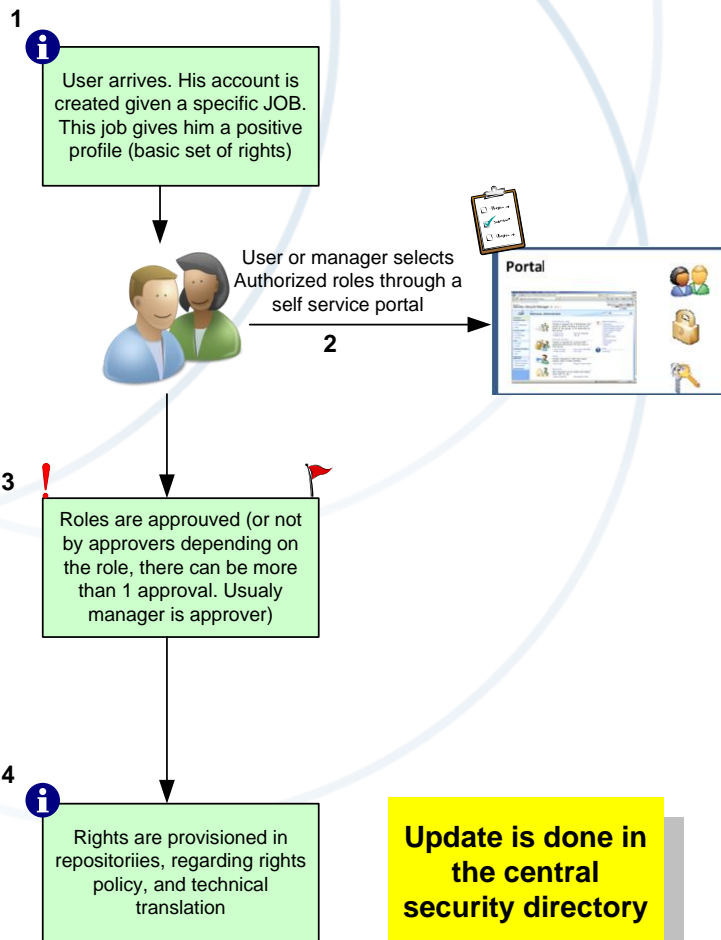
- **Role Based Access Control:**
 - Le modèle RBAC modélise des fonctions métiers plutôt que des accès à des ressources informatiques
 - Un rôle correspond à une fonction au sein d'une organisation
 - **Principe de base:** 2 utilisateurs qui ont le même rôle ont les mêmes droits sur le système
 - Les associations entre les rôles et les ressources physiques sont modélisées séparément par les concepteurs d'application et maitrise d'ouvrage métier
-

DÉCLINAISON... RBAC AVEC CONTRAINTES

- Ajoute au modèle RBAC de base les contraintes de non cumul et de séparation des pouvoirs



GESTION DES HABILITATIONS AU TRAVERS D'UN CATALOGUE DE SERVICE



Meilleur niveau de sécurité

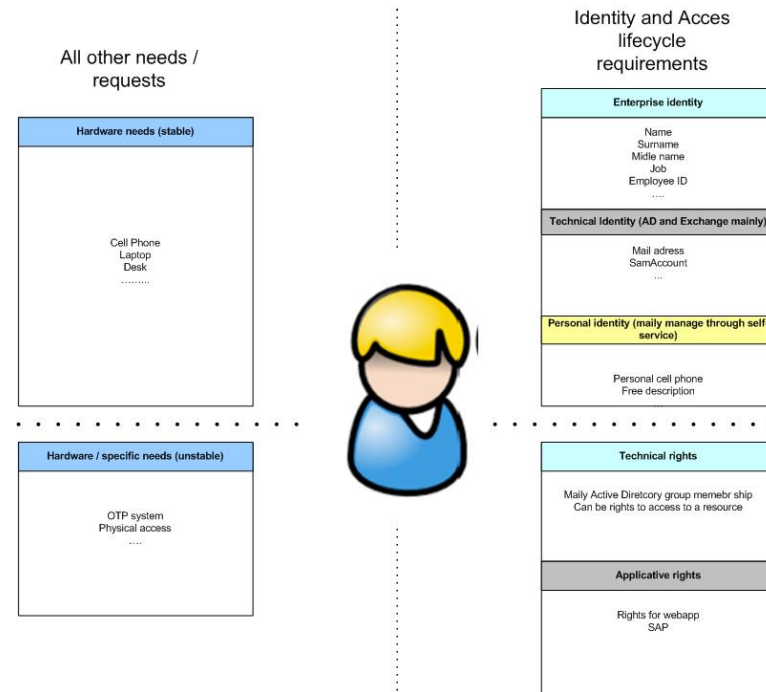
Gestion de l'historique

Déléguer la gestion des droits à un niveau « poste fonctionnel »

Conformité SOX

LA NOTION DE CATALOGUE DE SERVICE

- **Le catalogue de service est le point d'entrée de tout besoin pour un utilisateur dans le SI; il peut traiter:**
 - Les besoins liés à l'identité
 - Les besoins liés aux droits
 - Les besoins matériel (tel, token,)
- **Le catalogue de service s'appuie sur:**
 - Une interface (web la plupart du temps)
 - Un moteur de Workflow
 - Un Gestionnaire de tickets
 - **et la solution de gestion des identités (elle inclut généralement les composants sus-cités)**



SOLUTIONS DE GESTION DES IDENTITÉS

Synoptique général

Etat du marché Gartner

Architectures fonctionnelles

SYNOPTIQUE GÉNÉRAL



Utilisateur



Responsable
Hiérarchique



Administrateur
Opérationnel



R.S.S.I.

FRONTAL UTILISATEUR

Pages Blanches / Pages
Jaunes

Gestion du cycle de vie
des identités

Audit et étude des traces

Self Reset de mot de
passe

Modèle de rôles
(rôle métiers, rôles applicatifs,
profils applicatifs)

Réconciliation /
Conformité

WORKFLOWS



- Arrivée
- Départ
- Mutation
- Prolongation de contrat
- Modification de droits
- Création / Modification / Suppression de Rôles
- Règles de sécurité / confidentialité

ANNUAIRE GLOBAL



Structures



Personnes



Comptes



Règles



Rôles

MOTEUR DE PROVISIONNING

Utilisateur



CONNECTEURS



AD /
Exchange



Ldap PIG



Ldap
SIRIS



EDS vis
Exchange



TSS



Oracle



Ldap
Unix

REFERENTIELS OPERATIONNELS

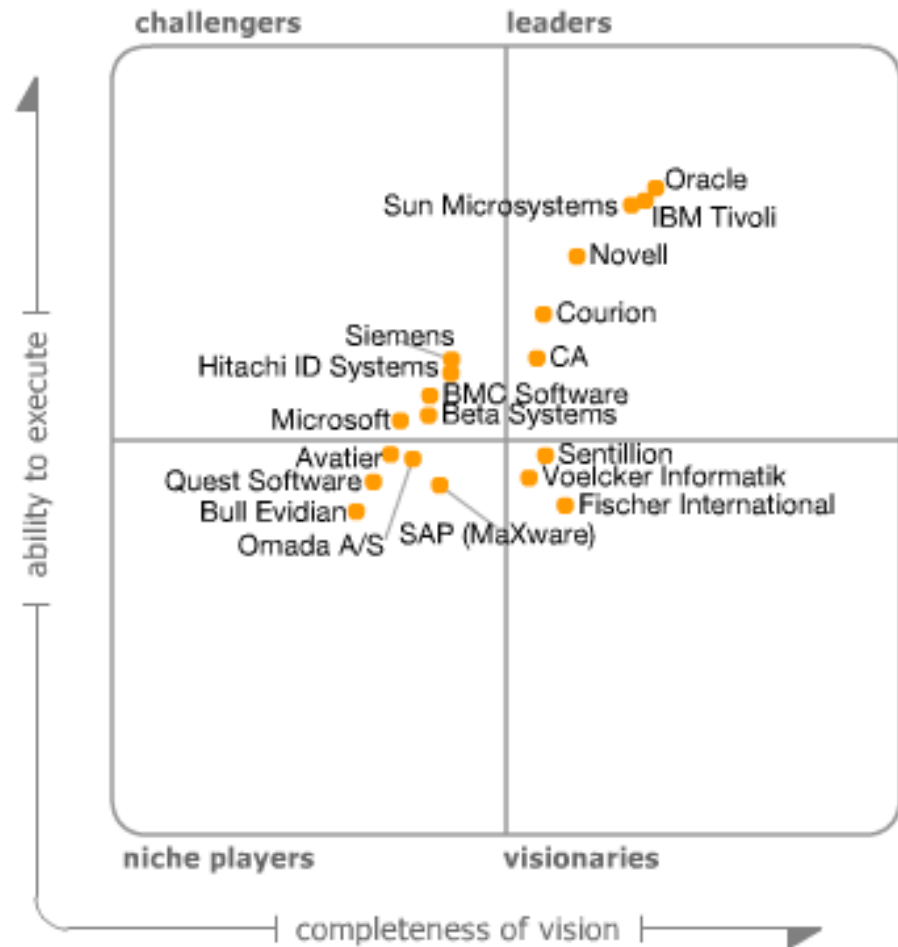


Echanges



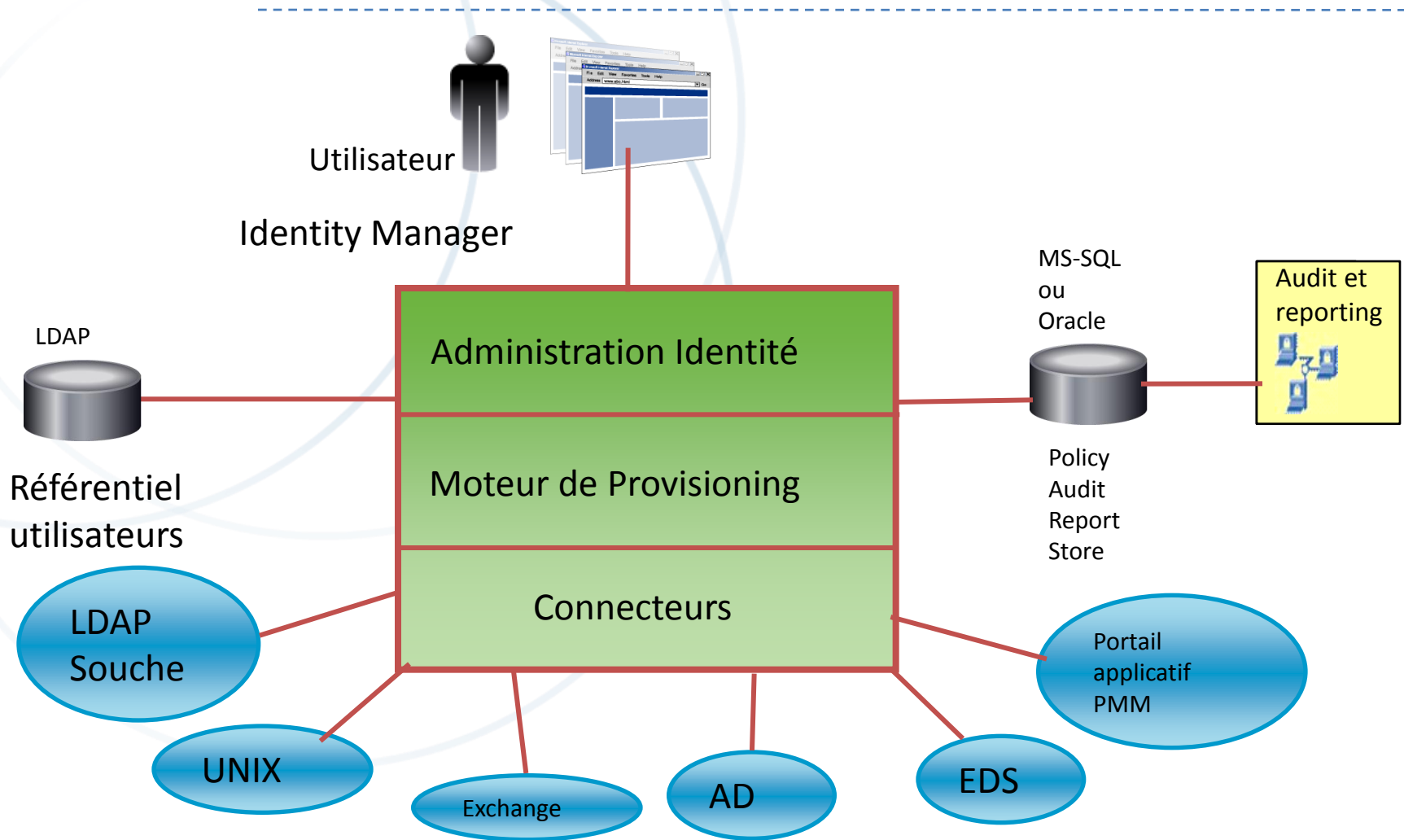
ÉTAT DU MARCHÉ - GARTNER

- “User provisioning”

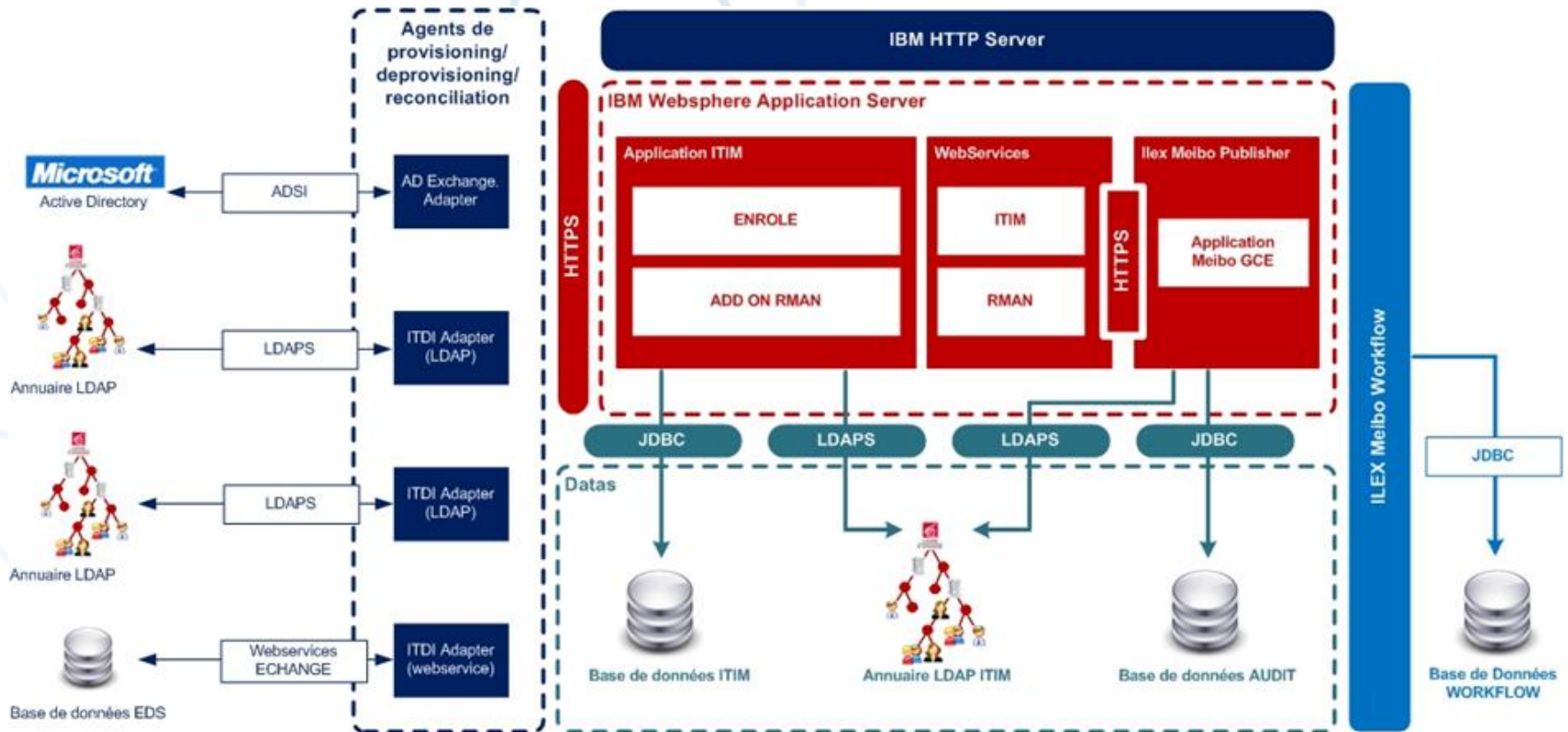


As of August 2008

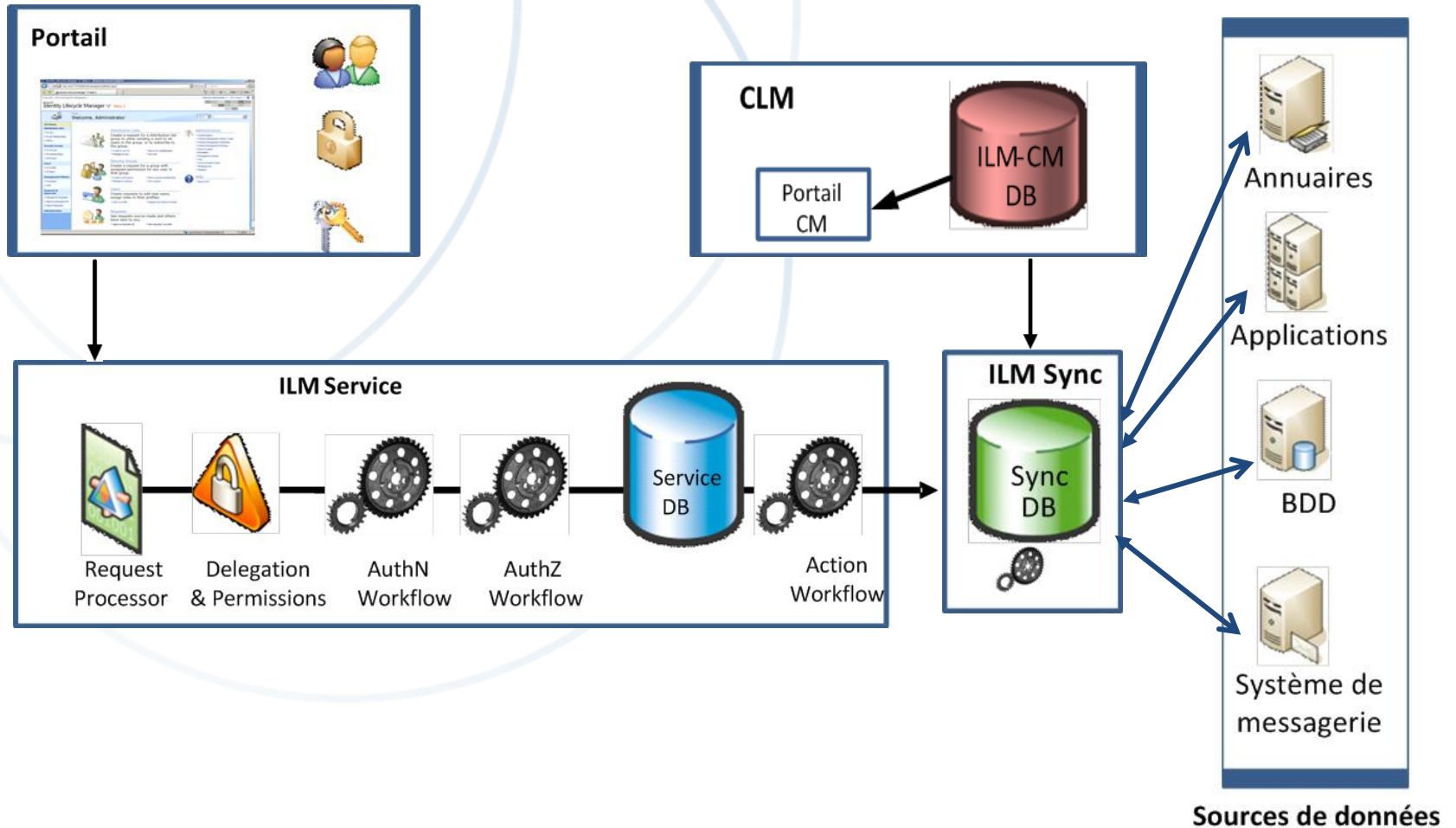
CA : ARCHITECTURE FONCTIONNELLE TYPE



IBM : ARCHITECTURE FONCTIONNELLE TYPE



MICROSOFT: ARCHITECTURE FONCTIONNELLE TYPE





APPROCHE PROJET

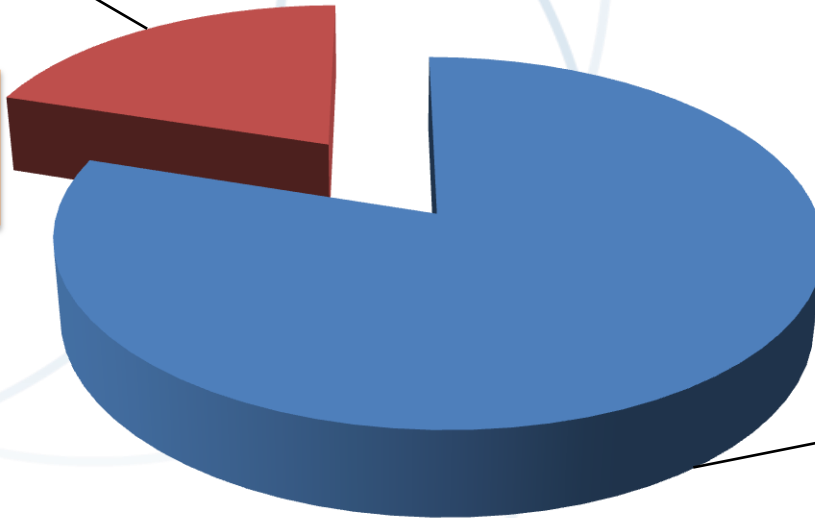
Les 3 chantiers IAM

Démarche projet type

LES CHANTIERS IAM

Chantier technique
20%

Définition et mise en place du socle technique



Définition et mise en place des grandes fonctions de l'IAM (Cellule RH, Contrôle, Validation...)

Approfondissement et généralisation de **RBAC**

Chantier Organisationnel & Fonctionnel
80%

Accompagnement au changement Admin et utilisateurs

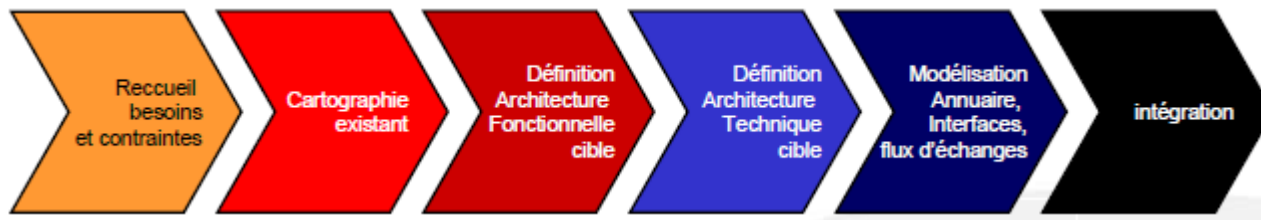
Spécifications de Workflows



Organisationnel et fonctionnel sont 2 chantiers distincts mais fortement liés

DÉMARCHE PROJET TYPE

- **Mise en oeuvre d'un annuaire LDAP au sein d'un SI préexistant**
 - Démarche d'urbanisation très structurante
 - Projet d'entreprise global : fonctionnel, technique et organisationnel
- **Nécessité de méthodologie d'urbanisation**
 - Recueil des contraintes et des besoins
 - Cartographie de l'existant
 - Analyse des besoins et conception de l'architecture fonctionnelle cible
 - Analyse des contraintes et conception de l'architecture technique cible
 - Choix des solutions d'annuaire, d'intégration, etc.



RETOURS TERRAIN

Caractéristiques des projets IAM

Démarche IAM

Maturité ressentie des entreprises françaises

Mise en musique d'un projet IAM

CARACTÉRISTIQUES D'UN PROJET IAM

- Un mot “**TRANSVERSE**”
 - **Implique:**
 - La DSI (fourniture du service d'accès au système)
 - Les gestionnaires applicatifs (Gestion des droits et attribution)
 - Les RH (Garants de l'identité, organigramme...)
 - Les Gestionnaires de contrat (Pour les externes)
 - La com' interne (Annuaire pages blanche, trombinoscope, ...)
 - Les moyens généraux (téléphonie, badges...)
 - ...
-

- 2 mots “**PRAGMATISME**” , et
“**SPONSORING**”
 - “**Pragmatisme**”: ne pas vouloir tout faire en même temps;
technique des “petits pas”
 - “**Sponsoring**”: projets structurants et couteux, sponsoring DSI /
DG / RH nécessaire

MATURITÉ RESENTIE DES ENTREPRISES FRANÇAISES

- **Différent selon les secteurs:**
 - Le bancaire semble plus en avance du fait des contraintes réglementaires fortes, et de la simplicité "relative" de ses métiers et son parc applicatif. Le réglementaire a été le premier levier pour lancer de tels projets
 - La santé et le pharmaceutique ont une bonne maturité sur l'industrialisation de leurs processus de gestion des identités.
 - Secteur public: diversité de paysage...

MISE EN MUSIQUE D'UN PROJET D'IAM

- L'équation à résoudre est la suivante:
 - $0,2 * \text{Expertise technologique} + 0,8 \text{ Conseil}$
(compréhension des processus de l'entreprise) =
Projet IAM réussi

QUESTIONS / REPONSES

**Merci de votre
attention**

Des questions?

