RAPPORT

LE PROJET D'ANNUAIRE D'ENTREPRISE

Pilotage par la valeur

SEPTEMBRE 2005

CIGREF

" PROMOUVOIR L'USAGE DES SYSTEMES D'INFORMATION
COMME FACTEUR DE CREATION DE VALEUR POUR L'ENTREPRISE. "

LE CIGREF

Le CIGREF, Club informatique des grandes entreprises françaises, existe depuis 1970. Sa finalité est la promotion de l'usage des systèmes d'information comme facteur de création de valeurs pour l'entreprise. Il constitue un lieu privilégié de rencontre et d'échange d'informations entre les responsables des grandes entreprises françaises ou européennes utilisatrices d'importants systèmes d'information. Ce partage d'expériences vise à faire émerger les meilleures pratiques. Chaque année, le CIGREF réalise des études sur des sujets d'intérêt commun.

Publications du CIGREF en 2004-2005

Charte Cigref-Syntec informatique
« Ingénierie et intégration de systèmes »
« Conseil en organisation et systèmes d'information »
« Progiciels »

CIGREF Syntec Informatique Charter

La fonction achats informatiques et télécoms

Intelligence juridique et systèmes d'information

Le marché de la mobilité en France et à l'international

Usages business des technologies sans fil

Dynamique des relations autour des systèmes d'information
dans les équipes de direction des grandes entreprises françaises

Relational Dynamics around Information Systems
within Management Teams of Major French Companies

La recherche au Cigref
« Cahier introductif »
« La recherche au Cigref - Cahier n° 1 »

Analyse Post Projet

Nomenclature RH 2005

L'Intelligence Economique appliquée
à la Direction des Systèmes d'Information

PARTICIPANTS

Ce livre blanc est issu des travaux d'un groupe de réflexion du CIGREF, dans le cadre de la thématique « Urbanisme, architectures et technologies » et a été rédigé avec la participation aux réunions de 2002 à 2005 des personnes et entreprises suivantes :

Francis Cauvé	Banque de France
Paul Chevalier	Groupama
David Delpeso	AG2R
Nadine Etienne	Générale des Eaux
Stéphane Gobin	Réunica
Eric Gosteau	Peugeot
Roland Gueye	Suez
Loïc Le Flem	CEA
Gérard Lièvremont	Caisse des dépôts
Victor Martins	Geodis
Patrick Méry	CNAV
Christophe Moreau	Maaf
Alain Plaignaud	Renault
Jean-Marie Pilot	CNAV
Hervé Robache	GSIT
Cho Sphabmixay	Crédit Lyonnais
Fanny Ternisien	SNCF
Paul Vincent	EDF
Jacqueline Pasquereau	EDF / AFNOR
Frédéric Maillard	AFNOR

L'étude a été pilotée par Frédéric Lau, chargé de mission.
L'animation de la réflexion a bénéficié de l'aide de Philippe Dajean, responsable de l'activité IAM & Annuaire de SoluCom.

SOMMAIRE

AVANT-PROPOS

Le comité de pilotage du CIGREF « Urbanisme, architecture et technologies » a souhaité que le CIGREF se penche sur une des problématiques des projets d'annuaires : leur valorisation.

Ce thème de l'annuaire, depuis plusieurs années, a été au CIGREF le sujet de débats, de retours d'expérience et de présentations de fournisseurs, aussi bien d'un point de vue technologique, architecture que sécurité.

Des discussions entre membres du CIGREF ont notamment eu lieu lors des réunions tenues sur le sujet de septembre 2002 à juin 2003.

Ces discussions n'avaient pas initialement l'objectif de mener à la publication d'un rapport. Compte tenu de la forte activité du marché des annuaires au cours des deux dernières années, il nous a néanmoins semblé utile de partager nos retours d'expérience.

Nous avons également profité pour élargir quelque peu notre propos aux évolutions récentes de la gestion des identités, qui est en train de devenir l'un des débouchés les plus marquants des démarches annuaires menées par nos membres.

Ce document ne développera aucunement les aspects techniques des annuaires. Il s'intéressera en revanche à la participation des acteurs, aux bénéfices attendus et aux méthodes mises en place, sous un angle d'information, voire de formation pour le lecteur, sans souci d'exhaustivité mais de bonne compréhension.

Les membres du CIGREF trouveront sur notre extranet l'intégralité des informations qui nous ont permis de bâtir ce document.

INTRODUCTION AUX ANNUAIRES D'ENTREPRISE

Un contexte globalement favorable mais complexe

De nos jours, il est une lapalissade disant que « les grands comptes sont en constante évolution sur des marchés de plus en plus concurrentiels ». Effectivement, ce ne sont que fusions, acquisitions, réorganisations, cessions et autres évolutions stratégiques, auxquelles sont soumises les grandes entreprises, les obligeant dès lors à optimiser de manière récurrente leur fonctionnement.

La recherche de l'amélioration permanente et de la performance mêle changement des organisations et mobilité croissante des ressources. L'entreprise mue, l'entreprise mute, l'entreprise s'ébroue et se réorganise, faisant disparaître les scories du passé et émerger les nouveaux besoins, répartissant ses ressources en fonction des nécessités.

Ces nouveaux besoins, tant fonctionnels qu'applicatifs, se concrétisent notamment par le déploiement à grande échelle de portails ou d'intranets fédérés et par de nouvelles applications orientées e-business aussi bien pour les clients que pour les fournisseurs.

Les deux enjeux majeurs deviennent alors de prendre en compte, de plus en plus rapidement, les nouvelles organisations afin de profiter au plus vite des synergies et de faciliter, voire d'accélérer, la mise en œuvre d'applications transverses à toute l'entreprise.

La complexité des organisations, la multiplication des référentiels, les contraintes technologiques et opérationnelles rendent ces changements difficiles. C'est pour cela que les annuaires sont progressivement devenus des maillons essentiels d'un système d'information de plus en plus complexe.

Mettre en place un annuaire n'est cependant pas chose aisée car c'est un projet particulier qui souffre d'une erreur de *casting* initiale : pour la majorité des collaborateurs de l'entreprise hors DSI, un annuaire ne sert qu'à avoir des informations pour contacter des gens.

Or un projet d'annuaire est comme un iceberg, la petite partie émergée, visible et appréciée concernant la gestion des utilisateurs est celle qui sert d'accroche dans sa compréhension.

La partie immergée plongeant dans le système d'information de l'entreprise prend, elle, en compte des enjeux autrement plus complexes concernant la sécurité du système d'information, les

référentiels de données de l'entreprise et la transversalité des applications. C'est elle qui est essentielle à l'entreprise… et c'est celle qui est la moins comprise.

Une majorité des membres du groupe de réflexion estime que cette problématique existe depuis environ cinq ans. Plus exactement il y a environ cinq ans qu'elle a commencé à évoluer du besoin « pages blanches » aux besoins applicatifs et sécurité.

Promouvoir un projet d'annuaire n'est donc pas inné ! L'objet de ce document est d'essayer de donner des éléments d'information, des conseils ou recommandations permettant de communiquer, expliquer, vendre un projet d'annuaire dans sa globalité.

Les deux faces de l'annuaire : infrastructure et service

Cadre général d'analyse

Avant tout chose, il nous faut rappeler ce que recouvre le terme « annuaire d'entreprise » pour prendre conscience de la réelle difficulté de mise en œuvre d'un projet le concernant. Nous allons donc mettre en évidence ses caractéristiques et en particulier ce qui le rapproche d'un projet d'infrastructure et ce qui l'en éloigne.

Cette mise en évidence passe notamment par une bonne compréhension de la distinction entre le **référentiel d'entreprise** des identités, sur les aspects contenant et contenu, et les **services d'annuaire** en tant que tels :

- Le premier thème relève de la mise en œuvre d'un service d'infrastructure permettant l'échange de données entre un référentiel central et le S.I ;
- le second thème est fonctionnel et correspond à des services de consultation de données (pour les utilisateurs) ou de gestion des données (pour les administrateurs).

Il est impératif de bien distinguer les deux notions pour expliquer aux décideurs ce qu'est un annuaire. Le schéma ci-dessous positionne globalement ces deux volets :

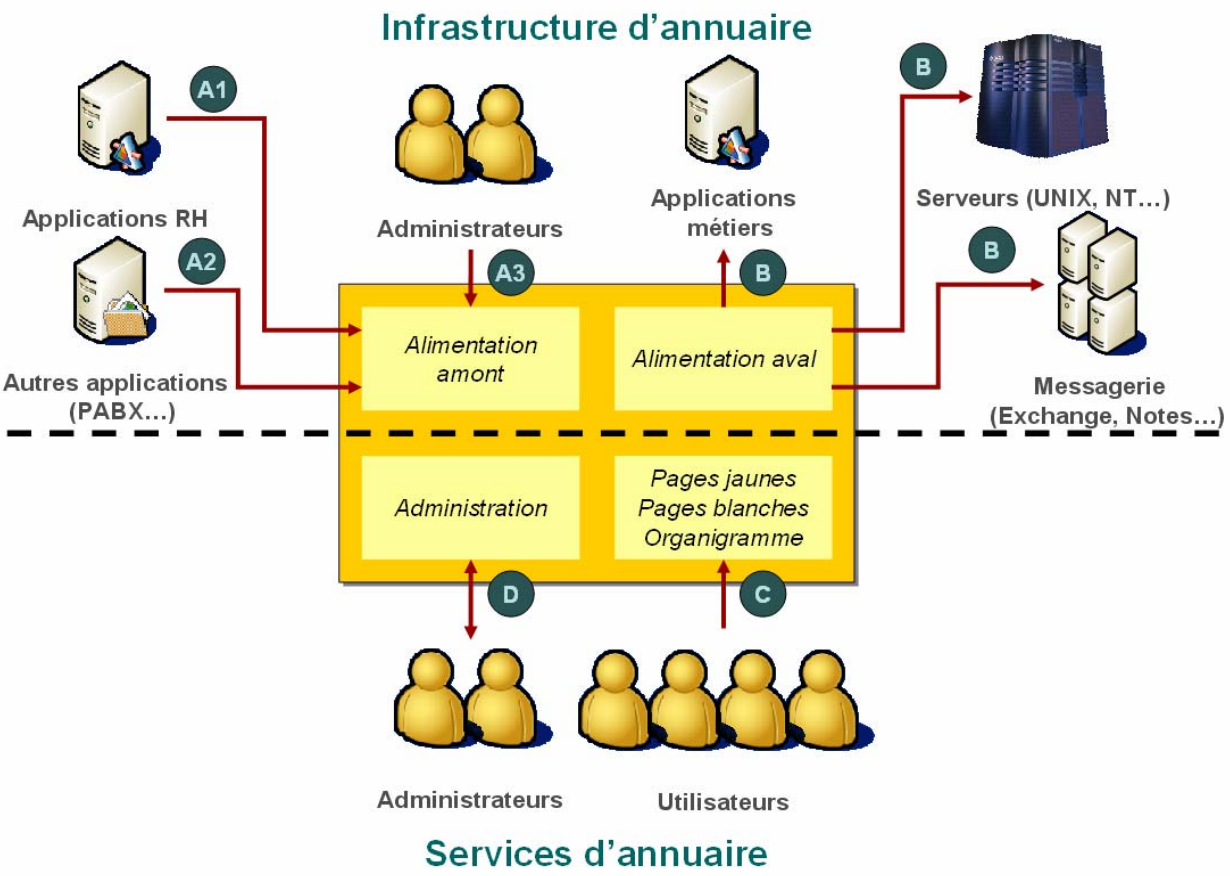

Figure 1
Positionnement des deux notions d'infrastructure
et de service d'annuaire

A – Alimentation amont

Trois canaux d'alimentation amont sont possibles :

- **A1** – Applications des ressources humaines : pour les utilisateurs internes, les applications des ressources humaines constituent les sources de l'annuaire. Ces sources peuvent être, entre autres, les fichiers du personnel.
- **A2** – Autres applications : les applications des ressources humaines n'ont pas nécessairement toutes les informations nécessaires pour alimenter l'annuaire. Par exemple, le numéro de téléphone d'une personne sera alimenté par le PABX. Ainsi, d'autres applications que celles des ressources humaines contribuent à l'alimentation amont.
- **A3** – Saisie manuelle : pour certaines catégories d'utilisateurs, il est possible qu'aucune application ne puisse être la source créatrice dans l'annuaire. Dans ce cas, les administrateurs doivent pouvoir saisir les informations nécessaires directement dans l'annuaire.

B – Alimentation aval.

Pour certaines applications et services du système d'information, l'annuaire est le point central d'alimentation des

comptes d'accès (identifiants, mots de passe et autres attributs). Cette alimentation concerne toutes les actions de gestion courante sur ces comptes.

C – Fonctions à destination des utilisateurs.

Les utilisateurs accèdent à l'annuaire pour obtenir des informations de type « Pages Blanches », « Pages Jaunes » ou « Organigramme ».

D – Fonctions à destination des administrateurs.

Les administrateurs disposent de vues spécifiques sur l'annuaire pour exécuter leurs tâches de gestion (création, modification, suppression, suspension, etc.) et lorsqu'ils sont en charge de la gestion des identités pour s'assurer que les bons droits d'accès sont attribués à la bonne personne pendant le bon laps de temps.

Les infrastructures d'annuaire

L'annuaire est une base de données spécialisée, permettant d'une part de stocker des informations typées et ordonnées sous une vue hiérarchique adaptée à l'entreprise, et d'autre part de lire ou de rechercher des informations selon des critères préétablis.

Nous considérons l'annuaire comme un service d'infrastructure : service transverse de stockage et de références, de consultation et de gestion de données…, sur lequel s'appuieront différentes applications (pages blanches, pages jaunes, gestion des droits…).

L'annuaire est composé des briques fonctionnelles suivantes :

Des données de référence

Il s'agit du cœur de l'annuaire, conteneur d'informations, qui s'appuie généralement sur une technologie conforme à la norme LDAP (reconnue par tous les fournisseurs de solutions). Il peut stocker tout type d'information sur les personnes, les organisations, les sites, les applications, les ressources techniques...

Ces informations peuvent être locales ou bien distribuées via des mécanismes de pointeurs vers des annuaires externes bâtis sur des principes communs. Il s'agit du principe de renvoi de références. Lorsque l'annuaire est sollicité, il renvoie au demandeur l'adresse d'un autre serveur d'annuaire pouvant répondre à la requête.

Des règles de nommage et un « schéma »

Le protocole LDAP s'appuie sur différents concepts issus d'une approche objet. Les informations stockées au sein d'un

annuaire sont référencées à l'aide de classes d'objets, chaque classe d'objet contenant une liste d'attributs auxquels sont associés un type et une syntaxe.

L'ensemble des classes d'objets, des attributs, de leurs syntaxes, des règles de comparaison constitue le schéma de l'annuaire. Par ailleurs, les objets (occurrences des classes) sont organisés de manière hiérarchique dans un arbre nommé DIT (*Directory Information Tree*).

Des règles de synchronisation avec d'autres annuaires

Cette synchronisation s'établit à l'aide d'applications spécifiques ou d'outils du marché de type *méta-annuaire*. Un méta-annuaire est composé des éléments suivants :

- une méta-vue, nom donné à l'annuaire de référence qui recueille l'ensemble des données synchronisées,
- un moteur de jointure qui réalise l'assemblage entre les données des différents référentiels (annuaires, bases) connectés avec la méta-vue. Il stocke l'ensemble des règles de synchronisation que les connecteurs utiliseront pour interagir avec les sources de données,
- des connecteurs, qui traduisent les flux de données en langage directement compréhensible pour la source de donnée distante et le moteur de jointure (interface côté méta-annuaire). Un connecteur est le plus souvent spécifique à un type de source de données. Si le connecteur n'existe pas pour une source, les éditeurs de solution proposent un connecteur universel qu'il est possible de programmer et de paramétrer pour connecter la source.

Des règles de gestion

Afin de gérer les données de référence de l'annuaire, il convient de définir des règles de gestion spécifiant d'une part, les acteurs responsables des différents périmètres de données (pour l'ensemble des données stockées), et d'autre part, les processus et les moyens de mises à jour de ces données (« *workflow* », interface d'administration, interface d'administration d'une source externe...).

Des interfaces d'accès

Enfin, l'annuaire est doté d'interfaces d'accès. Plusieurs types d'interfaces sont définis : une interface d'administration technique de la plate-forme annuaire, une interface de consultation des données ou encore une interface de mise à jour de ces données.

Les services d'annuaire

L'infrastructure d'annuaire, une fois bâtie, est un support pour différents bouquets d'applications ou de services :

- Des services de types pages blanches / pages jaunes (coordonnées et fonction des personnes).
- Des services d'organigramme (liens hiérarchiques entre les personnes, entre les organisations d'une entreprise).
- Des services de sécurité (habilitations, *Public Key Infrastructure* (PKI), *Single Sign-On* (SSO)...).

Nous reviendrons sur chacun de ces services, qui constituent la partie visible, dans la section « valeur de l'annuaire »

Quand parle-t-on d'annuaire d'entreprise…

Un annuaire d'entreprise est avant tout un référentiel décrivant un ensemble de ressources humaines d'une entreprise, accessible aussi bien aux utilisateurs qu'aux applications de cette entreprise. Son positionnement, unique ou sous forme de multiples instances spécialisées mais synchronisées, est transversal au sein du système d'information.

L'annuaire d'entreprise se distingue en effet par son caractère voulu d'universalité en opposition à des annuaires spécifiques (parfois appelés annuaires techniques) qui peuvent exister de part et d'autre, notamment au sein des diverses applications d'entreprise.

Dans cet ordre d'idées, la démarche de mise en œuvre d'un annuaire d'entreprise est parfois initiée par le constat des difficultés engendrées par la multiplication de ces annuaires spécifiques.

Comment vendre un projet d'annuaire

L'Ante projet, rampe de lancement

Le lancement du projet et sa réussite nécessitent de mettre en place un environnement adapté.

Cette étape est indispensable en raison de la nature du projet qui concerne les individus et la sécurité de leurs accès, de son caractère transversal, du nombre et de la diversité des acteurs à impliquer, de ses impacts techniques et organisationnels. Elle va donc avoir une influence déterminante sur le succès ou les difficultés à venir du projet.

Apprendre

Travailler sur l'environnement du projet consiste en l'élaboration d'un modèle économique basé, entre autres, sur l'étude des référentiels existants, du coût à ne pas faire le projet annuaire et des études d'impact sur l'organisation de l'entreprise. L'objectif *in fine* est, par une succession d'entretiens, de faire adopter très tôt une vision transverse aux différentes directions

opérationnelles et d'identifier les facteurs favorisants et déclenchants du projet.

C'est la phase d'apprentissage.

Expliquer

Communiquer implique de trouver un message fédérateur simple, qui peut être basé sur un service nouveau, mais surtout qui utilise un « langage » adapté à chaque entité concernée : orienté gains de productivité pour les financiers, exhaustivité des ressources pour les services généraux, rapidité d'accès à l'information pour les utilisateurs, support aux applications pour les directions fonctionnelles, renforcement de la sécurité pour la direction générale, etc.

Il faut donc faire attention à ce que cette communication ne soit pas ciblée majoritairement sur les directions générales. Il faut en effet faire aussi du « lobbying » auprès des correspondants locaux pour qu'ils vendent en interne dans les directions métiers les bénéfices de l'annuaire d'entreprise. Cette démarche doit permettre d'associer les initiatives locales à la démarche d'annuaire d'entreprise.

Elle doit également permettre de lever certaines réticences envers un projet qui peut être perçu comme un moyen de surveillance, *« big brother is watching you»*. Tout au contraire il faut mettre en avant l'aide procurée pour faciliter le travail de chacun.

Ce message fédérateur doit permettre de comprendre les enjeux et bénéfices du projet.

C'est la phase d'explication.

Persuader

Le problème de l'identification et de l'implication d'une maîtrise d'ouvrage sur un sujet transverse tel que l'annuaire (et non métier) reste entier.

L'ante projet doit donc permettre d'identifier ce que l'on peut appeler un « vecteur sponsor » fiable. Plusieurs cas peuvent alors se présenter :

- Une maîtrise d'ouvrage métier, le plus souvent la direction des ressources humaines (DRH) ou les services généraux, peut prendre le leadership car elle est la première intéressée par l'annuaire. Cette approche peut présenter quelques difficultés : la maîtrise d'ouvrage en question, une fois ses besoins couverts, ne positionne pas les souhaits d'évolution des autres métiers comme des priorités voire des sujets à traiter, ou encore elle n'assure pas le même pilotage sur ces évolutions.
- La direction générale pourrait également être la maîtrise d'ouvrage. Cependant, si elle permet le plus souvent de déclencher, supporter ou pousser l'annuaire, elle n'a

généralement pas pour rôle d'en assurer la maîtrise d'ouvrage.

- La direction des systèmes d'information se substitue aux maîtrises d'ouvrage métiers et assure celle de l'annuaire. Le travers de cette approche est l'éventuel décalage avec les besoins de l'entreprise, une vision trop technicienne ou encore une dérive en raison de l'absence d'une ligne directrice pilotée par des enjeux métiers. Par ailleurs, il est très complexe pour la DSI de jouer ce rôle et d'être tenue pour responsable de la qualité de l'annuaire alors qu'elle n'est pas propriétaire des données qui y sont stockées.
- Un pilotage de l'annuaire par les 3 ou 4 maîtrises d'ouvrage utilisatrices de l'annuaire peut sembler une approche pertinente et nécessite la mise en place d'un comité annuaire. Il reste à savoir si une telle organisation est envisageable dans votre entreprise.

Cette phase doit s'appuyer notamment sur un argumentaire fort sur l'analyse de la valeur ajoutée du projet annuaire. L'important est de rendre ce projet incontournable.

C'est la phase de persuasion.

Un projet ou programme au service des métiers

L'annuaire se positionne comme un véritable service d'infrastructure, au même titre que les infrastructures réseaux ou serveurs par exemple, pour tous les usages, aux bénéfices de toutes les divisions et branches de métiers de l'entreprise.

Certaines entreprises estiment que l'annuaire étant au service des projets, il doit s'adapter en permanence pour offrir les services souhaités. Dès lors elles ne parlent plus de projet mais de programme d'annuaire au sein d'une entreprise, c'est-à-dire d'une structure établie sur du long terme, transverse et disponible, bénéficiant d'une construction progressive et récurrente et au service des projets.

Comme le projet/programme d'annuaire ne doit pas « tirer » les projets mais au contraire être à leur service, il doit donc aussi être indépendant des technologies : on ne met pas en place la technologie LDAP mais bien un service de support aux applications ou aux utilisateurs qui offre des fonctionnalités d'annuaire.

La gouvernance des systèmes d'information doit donc être impliquée pour prendre en compte les problèmes d'infra-structures pérennes et évolutives de l'entreprise et veiller à ce que l'annuaire reste au service des différents projets. Le chef de projet annuaire se doit aussi d'être « proactifs » c'est-à-dire s'assurer d'avoir des acteurs, un périmètre d'action, des données à intégrer et des services à offrir pour les vendre aux autres projets.

Intéresser les autres projets aux services de l'annuaire permet de motiver les entités ou maîtrises d'ouvrage métier qui maîtrisent les données à participer financièrement au projet et à en devenir partenaire. La dimension fonctionnelle forte, due à la nature des données que l'annuaire va héberger, doit être mise en avant afin de motiver leur implication dans la mise en œuvre et son fonctionnement, cette implication jouant un rôle essentiel sur le niveau de fiabilité des données.

La valeur des différents arguments de vente

Nous verrons dans le chapitre 4 que la démonstration de la valeur générée par l'annuaire est au centre de la stratégie de communication et qu'elle doit être ajustée :

- en fonction de la population cible,
- en fonction des services proposés : les fonctions annuaire pages blanches, annuaire des sociétés, annuaire de sécurité, etc.

Dans certains contextes on pourra également insister sur la notion de référentiel d'entreprise fiable, incluant les populations internes et externes accédant au Système d'Information. Il faut néanmoins rester prudent car l'aspect « service d'infra-structure » (il s'agit bien de construire un socle fiable sur lequel s'appuiera chaque service d'annuaire) n'est pas toujours très vendeur et cela peut induire de la confusion, limiter le poids des arguments et *in fine* compliquer la prise de décision pour déclencher le projet.

Outre ces éléments liés à la valeur de l'annuaire, nous recommandons de mettre en œuvre une véritable démarche de vente en interne, selon trois axes principaux :

Faites la promotion des fonctionnalités d'annuaire en allant à la rencontre de vos alliés internes

Fait remarquable, l'annuaire est une des seules applications du S.I. qui intéresse l'ensemble des acteurs de l'entreprise :

- Les Directions Générales apparaissent en tête de liste. La plupart sont sensibles aux services facilitant la communication dans l'entreprise, développant le sentiment d'appartenance ou encore augmentant la productivité des employés. Mais surtout, elles sont bien souvent les premières utilisatrices de ces services qui leur permettent de retrouver instantanément n'importe quel collaborateur !
- Les employés sont également intéressés pour identifier avec précision leurs collègues.
- Enfin, les projets attribuent des rôles et des activités à des personnes et bénéficient à travers l'annuaire d'un support qui économise les mises à jour.

Mettez en avant les vertus d'un service géré au niveau Groupe

D'un côté, la mise à jour d'une information sur une personne devient immédiatement disponible par l'ensemble des services s'appuyant sur l'annuaire d'entreprise.

De l'autre, il suffit de quelques minutes pour créer un annuaire indépendant dans une entité. Lorsque plusieurs annuaires comportent des informations contradictoires, il est dès lors impossible d'identifier la bonne valeur.

Illustrez cette contradiction fondamentale, et demandez aux décideurs de se positionner par rapport à elle. L'annuaire d'entreprise a toutes les chances d'être mis en œuvre dès que l'entreprise disposera d'une gouvernance mature, ou que le niveau Groupe disposera d'une vraie légitimité par rapport aux entités opérationnelles et aux filiales.

Trouvez des « *quick-wins* » de l'annuaire adaptés au contexte de votre entreprise

De façon générale, le palier « pages blanches / pages jaunes » est facile à déployer avec les solutions du marché, il ne faut donc pas hésiter à l'utiliser comme catalyseur de la démarche. Pour les entreprises déjà dotées de ce palier, la mise en place d'organigrammes en ligne peut être un autre objectif attractif.

En dehors de ces *quick wins* génériques, il faut être capable d'exploiter les circonstances ; pour notre part nous en avons vu trois lors de nos discussions :

- Un incident qui crée souvent l'opportunité d'un contact avec de nouvelles sources d'information. Ce fut le cas lors des tempêtes de décembre 1999 qui ont nécessité des collaborations imprévues au sein d'EDF. Cela a permis d'utiliser de nouvelles sources d'information et de déployer en moins de 15 jours l'annuaire dans la totalité des régions sinistrées.
- Un rapprochement entre plusieurs groupes : de Pinault Printemps Redoute à Air France KLM en passant par Total Fina Elf ou Crédit Agricole Crédit Lyonnais, ces rapprochements n'ont pas manqué au cours des dernières années et ont presque toujours conduit à la mise en place d'infrastructures fédératrices, où les annuaires d'entreprise ont tenu toute leur place. Alors guettez le prochain rapprochement qui concernera votre compagnie…
- La mise en place d'une politique de sécurité. L'effet 11 septembre mais aussi les nouvelles normes IFRS, la recommandation Bâle II dans les banques ou le Sarbanes Oxley Act pour les sociétés implantées aux Etats-Unis ont été autant de facteurs qui ont favorisé la généralisation des

politiques de sécurité dans les grands groupes. Ces politiques de sécurité sont dorénavant achevées au niveau de leur définition et donnent lieu à un nombre de plus en plus important de démarche d'annuaires de sécurité. Le *quick win* que nous recommandons concrètement est de montrer la pertinence d'un tel annuaire en le mettant en place rapidement pour toutes les applications web de l'entreprise.

Comme on le voit, ces *quick wins* sont très divers. Puisse chacun y trouver une source d'inspiration pour inventer les siens.

LES POINTS CLES DU PROJET D'ANNUAIRE

Définir le périmètre le plus adapté au contexte de l'entreprise

Quelle représentation de l'entreprise à travers l'annuaire ?

Quelles personnes ?

L'annuaire d'entreprise concerne généralement les seuls collaborateurs (salariés et détachés) de l'entreprise.

Il est possible d'étendre le périmètre à d'autres catégories de personnes : clients, fournisseurs, prestataires… Il convient toutefois de prendre en compte attentivement toutes les dispositions, notamment vis-à-vis des contraintes réglementaires et législatives à ce sujet.

Inversement, il est également possible de restreindre le périmètre de l'annuaire en décidant d'exclure de la portée de l'annuaire certaines catégories de personnes, voire certaines branches de l'entreprise. Nous verrons qu'une solution alternative est de restreindre la visibilité de l'annuaire pour ces catégories et ces branches.

Quelles organisations ?

Les données incluses au sein d'un annuaire d'entreprise permettent, si on le désire, de refléter l'organisation de l'entreprise.

La structure arborescente d'un annuaire permet en effet de décrire facilement l'ensemble des éléments d'organisation : filiales, départements, divisions, services ou autre…Chaque élément d'organisation est alors mis en œuvre sous la forme d'une Unité Organisationnelle[1]. Chaque OU peut contenir des personnes, mais également d'autres OU, ce qui permet par un jeu de poupées russes de retranscrire les différentes structures de l'entreprise.

Une autre possibilité consiste à ne pas gérer l'organisation au sein d'un annuaire global mais à mettre en œuvre plusieurs annuaires dédiés à telle ou telle partie de l'organisation de l'entreprise. Des processus externes de consolidation peuvent dans ce cas être parallèlement mis en œuvre.

Enfin le choix peut être fait de ne jamais laisser transparaître l'organisation de l'entreprise au sein de l'annuaire. Tous les utilisateurs sont alors indistinctement rassemblés dans une seule OU de l'annuaire.

[1] En anglais « OU » pour *Organizational Unit*).

Quelles données ?

En fonction des usages que l'on désire mettre en œuvre au sein de l'annuaire, les données associées à chaque personne peuvent être plus ou moins détaillées.

Les informations minimales sont souvent liées à

- L'identification : nom, prénom, identifiant au sein de l'entreprise, parfois une photo
- La localisation et les modes de contact : adresse, téléphone, adresse électronique

D'autres informations peuvent inclure le positionnement hiérarchique, les contacts du secrétariat, la fonction au sein de l'entreprise. D'autres champs plus spécifiques peuvent associer un utilisateur par exemple aux certificats d'authentification électroniques qui lui ont été délivrés.

Enfin, la gestion des groupes d'utilisateurs permet de regrouper certains utilisateurs selon certains critères, soit au sein d'une même OU (équipe) ou de manière transversale au sein de l'entreprise (groupe de travail, structures sociales…)

Quels périmètres d'accès ?

Comme nous l'avons déjà dit, le périmètre d'accès concerne les personnels de l'entreprise, mais aussi des personnels externes (prestataires, fournisseurs, partenaires, clients et autres).

Dans ces conditions, l'accès aux données d'annuaire peut être anonyme ou nécessiter une authentification.

L'accès anonyme permet d'accéder par défaut à l'ensemble des objets décrits dans l'annuaire et à la plupart des attributs liés aux utilisateurs ou aux groupes. L'administrateur de l'annuaire peut néanmoins restreindre ces accès anonymes de façon à protéger l'accès à certains objets ou attributs de l'annuaire.

L'accès authentifié rend la gestion plus fine mais aussi plus délicate. Le travail d'administration de l'annuaire en est alors considérablement alourdi. Ainsi l'utilisateur authentifié pourra accéder à certains objets ou attributs supplémentaires. Il pourra également modifier certaines valeurs des attributs. Généralement, les annuaires permettent à chaque utilisateur de pouvoir modifier à leur guise certaines des informations les concernant.

Le contenu de l'annuaire est quant à lui conditionné par les services à mettre en œuvre. Les informations sont centrées autour de l'individu. Il convient d'être attentif à ce que l'annuaire ne devienne pas un fourre-tout ; il contient les données partagées et utiles à l'ensemble des acteurs de l'entreprise…

Comment choisir les sources de données ?

Dans toute entreprise il est des directions opérationnelles ou fonctionnelles qui détiennent la maîtrise d'un certain nombre de données. Or un projet d'annuaire a besoin de données fiables, il ne peut donc pas démarrer s'il n'y a pas accord sur la liste minimale des données auxquelles il peut s'attendre de la part des entités partenaires.

Il est important de faire comprendre à toutes les entités partenaires qu'il faut déterminer le périmètre de données utilisables par l'annuaire afin de lui permettre d'offrir les services promis. Elles doivent notamment être conscientes qu'elles devront assumer et assurer une liste minimale d'informations ainsi que des mises à jour régulières. La qualité de ses données conditionne les services à rendre et donc la crédibilité du projet annuaire.

Cette base minimum de données doit être plus utile qu'exhaustive. C'est-à-dire qu'elle ne doit prendre en compte que ce qui est réalisable dans l'immédiat : des choix devront être pris mais toujours en privilégiant la convergence. Il est plus facile de faire évoluer une petite structure au gré des opportunités, que de gérer une structure surdimensionnée qui intègre déjà tout dès le départ.

L'entreprise possède généralement un certain nombre de référentiels de données pouvant servir de source à l'annuaire. La principale difficulté est de trouver pour chaque information, la bonne source, celle qui possède l'information pertinente disponible.

Plusieurs stratégies peuvent alors être mises en œuvre :

Le pragmatisme peut conduire à réduire au maximum les sources et à ne favoriser que celles qui possèdent un quota maximum d'informations fiables.

S'il n'est pas possible de faire des choix dans les sources, deux options s'imposent : soit s'interfacer, soit les remplacer. Dans les deux cas, ce sont des actions périlleuses : l'interfaçage garantit d'avoir des informations mais pas leur pertinence, les remplacer pose des problèmes d'organisation. Dans les deux cas, il faudra donc passer des accords afin de mettre en place et garantir la mise à jour des données, que ce soit sur l'outil initial ou final.

La gestion du personnel

Garantissant l'appartenance des personnes à l'entreprise, le fichier des ressources humaines dispose du référentiel le plus étendu.

Si dans la théorie il peut contenir beaucoup d'informations importantes, la pratique révèle souvent que beaucoup d'entre elles ne sont pas rigoureuses : localisation géographique, libellé précis de la fonction, gestion des compétences…

Néanmoins, les informations liées à la rémunération et la qualification du poste sont en général très fiables. De plus il contient une information importante : l'identifiant unique de l'employé qui permet d'éviter les problèmes d'homonymie. Malheureusement, ce dernier n'est pas toujours mis à profit.

Enfin, le référentiel des ressources humaines se cantonne à l'entreprise. Il ne tient absolument pas compte des autres utilisateurs, personnes, ou populations comme les prestataires, les contacts…

L'annuaire de l'autocommutateur

C'est le référentiel le plus à jour. Les numéros de téléphone se doivent d'être justes, mais l'orthographe des noms de personne est souvent fonction de chaque administrateur ou des caractéristiques techniques des autocommutateurs.

Les annuaires sur papier

Ils correspondent aux usages, mais ne sont pas structurés en bases de données. Ce sont des sources de contrôle ou de saisie manuelle. Ils doivent pouvoir être reconstruits à partir de l'annuaire d'entreprise. L'annuaire papier est aussi un outil de promotion pour responsabiliser les personnes sur le processus de mise à jour de l'annuaire.

L'annuaire de la messagerie

Souvent fiable en termes d'informations sur les nouveaux arrivés, malheureusement beaucoup moins sur ceux qui sont partis.

Néanmoins, la plupart des personnes en entreprise disposent maintenant d'une adresse électronique. Cette adresse est souvent intégrée dans un annuaire « messagerie » qui est mis à jour par l'administrateur de messagerie. C'est de lui que dépend in fine la qualité des informations.

Comment tenir à jour un référentiel utilisable par tous ?

Tout d'abord il faut partir du principe qu'un annuaire doit être au service des autres projets qui partagent les mêmes référentiels. Il ne peut systématiquement s'imposer aux autres projets.

Il doit donc être vu comme un programme, au service des projets, un programme fédérateur. Il faut donc que chaque projet de système d'information soit perçu comme une opportunité de qualifier les flux de données pour un meilleur

usage, pour impliquer les acteurs des référentiels sur l'importance de la qualité des données en dehors de leur périmètre. L'architecture doit permettre la mise à jour unique de chaque information.

Elle doit néanmoins autoriser les circuits d'exception pour accélérer les mises à jour provisoires et pour garantir le fonctionnement de certains services.

Sécuriser les échanges

L'annuaire fédère la gestion des droits d'accès et apporte une vision claire du « qui fait quoi ».

Il devient dès lors la clé de toute mise en relation et il devient nécessaire de garantir une très haute disponibilité de sa consultation. L'étude des réplications, des plans de reprise d'activité, de la reconstruction des données suite à un incident sont des éléments essentiels.

L'identification des personnes devant être exacte, il est nécessaire d'impliquer chaque utilisateur pour les mises à jour des données, la hiérarchie validant et assurant la responsabilité des échanges. Ainsi chaque personne dispose des ressources nécessaires à son activité professionnelle.

Il est à noter qu'aujourd'hui il devient possible d'automatiser les tâches de gestion de l'annuaire par un circuit de *workflow*. Ce dernier permet de réduire le risque lié à une administration externe de l'annuaire.

Il existe aussi des solutions simples pour améliorer la sécurité des mises à jour : par exemple en verrouillant ou en différant les mises à jour le week-end.

Néanmoins il reste une lacune : la gestion des rôles pour effectuer des modifications globales des droits. Chaque éditeur propose différentes options et laisse souvent se développer chez son client des incohérences pour créer artificiellement des prestations. Il manque à ce jour une normalisation du concept de rôle. Pire encore, le concept de rôle est souvent détourné alors que les rôles d'une personne recouvrent l'ensemble des actions nécessaires à l'exercice d'une activité.

Maîtriser les étapes structurantes du projet d'annuaire

Bouclage du financement

Du projet

Les investissements sur le projet lui-même restent usuels.

Par contre, comme l'annuaire souhaite utiliser les sources d'information existantes (RH, autocommutateur…), il lui faut impliquer les acteurs d'autres systèmes d'information, créer les passerelles, définir des processus et souvent améliorer la qualité des données des sources. Les investissements en connecteurs sont très variables.

Des investissements d'exploitation

Bien évidemment, il est nécessaire de faire un suivi informatique de l'exploitation, d'assurer la montée en charge, améliorer les qualités de la collecte, élargir la couverture géographique.

Et il est indispensable de posséder la capacité d'être proactif pour satisfaire les attentes des projets qui sont susceptibles d'utiliser les services de l'annuaire : les services d'exploitation doivent donc disposer d'une marge de souplesse effective.

Construction du modèle de données

Outre la problématique d'unicité des collaborateurs (identifiant unique dans tous les référentiels ou correspondance entre les identifiants des référentiels), il est nécessaire de déterminer :

- le **périmètre de données** mises en « commun » dans le référentiel (et leur positionnement vis-à-vis de l'annuaire d'entreprise),
- l'organisation des données dans le référentiel.

Il convient d'être vigilant pour que le référentiel mis en œuvre ne devienne pas le « fourre-tout » des informations sur les utilisateurs. Il ne doit supporter que des données de référence d'une part attendues par les applications (ayant un sens « commun » et unique pour toutes les applications), et d'autre part pour lesquelles une gestion unifiée est pertinente.

Pour les identifier, il suffit d'appliquer une règle simple :

« Le référentiel ne contient que les données partagées et utiles à un ensemble d'applications ou de services ».

A contrario, les données spécifiques et fluctuantes nécessaires à une ou un nombre limité de ces applications sont exclues (notamment certaines données qui relèvent plus du fonctionnel

que de la sécurité) ; elles restent et resteront locales à un référentiel propre à l'application en question (par exemple, la notion de *privilège* dans certains progiciels).

A cette condition, le référentiel sera stable, indépendant d'influences particulières, gérable (complexité « raisonnable » du modèle de données), simplificateur pour la gestion des utilisateurs et il permettra une lecture compréhensible par tous des habilitations.

Cette approche présente donc les avantages suivants :

- ceux qui ont besoin de données spécifiques en assument la responsabilité ;
- elle limite les impacts organisationnels (outils et processus) et la conduite de changement associée en laissant à chacun la gestion des informations dont il est propriétaire et la poursuite de ses propres objectifs tout en maintenant leur propre outil de gestion ;
- il n'y a pas de risque de dégradation (complexité) de la qualité de l'annuaire à travers la prise en compte de toutes les demandes. Un contrôle des évolutions est exercé ;
- elle limite les risques d'échec lors de la construction de la solution en contrôlant son périmètre.

Il faut dissocier « le plus possible » la gestion des personnes de la gestion des accès et droits sur les ressources (type RBAC)

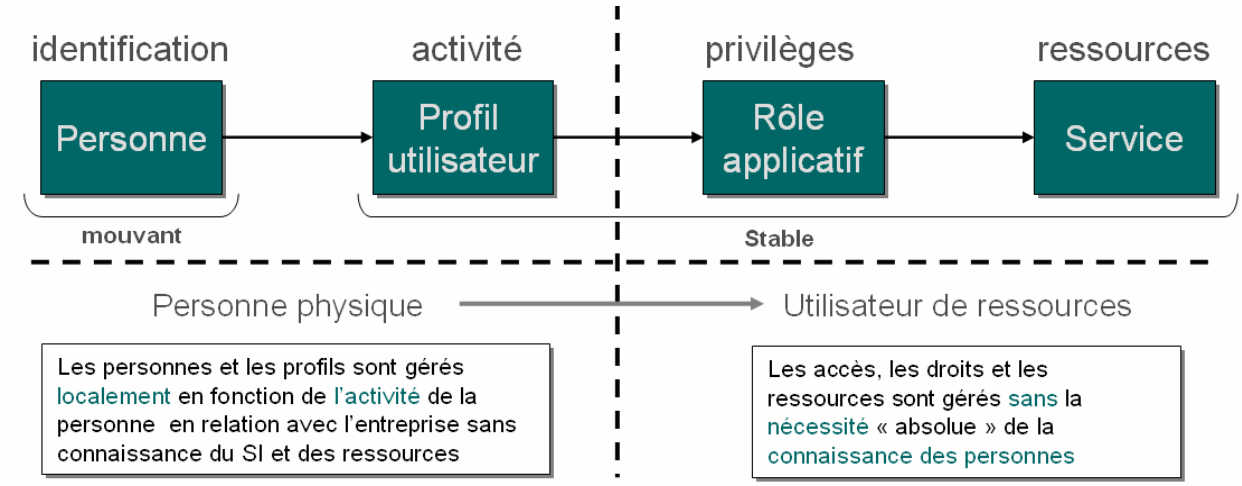

Figure 2
Illustration de la manière d'organiser les données dans le référentiel

Les bénéfices retirés de la mise en œuvre d'un tel modèle sont multiples :

- meilleure gestion des personnes : réalisée par des acteurs proches des événements - vision locale (les responsables SI n'ont généralement pas la capacité à qualifier les utilisateurs) ;

- simplification des processus de gestion des utilisateurs et de leurs accès :
  - gestion par bloc,
  - mouvements des personnes transparents pour la gestion des utilisateurs et de leurs accès,
  - partie SI moins sujette aux changements ;
- cohérence et homogénéité dans la gestion des utilisateurs et de leurs accès (application de règles d'entreprise) ;
- contrôle et audit facilités.

Néanmoins, l'application de ce modèle à l'échelle de l'entreprise suppose de parvenir à un consensus sur certains points :

- capacité à définir ces profils utilisateurs ;
- signification commune des profils utilisateurs pour le management et les utilisateurs au vu de la sécurité des accès ;
- attribution d'un nombre limité de profils utilisateurs à chacun tout en gardant un nombre limité de profils utilisateurs au total ;
- stabilité des profils utilisateurs.

De même, trois approches sont envisageables pour les droits d'accès :

- approche minimale : l'environnement mis en œuvre prend en charge la gestion des personnes et la définition des profils utilisateurs. Les applications sont chargées d'associer ces profils à des droits d'accès ;
- approche médiane : l'environnement mis en œuvre prend en charge en plus l'association profils/droits d'accès de premier niveau. Localement, les responsables fonctionnels gèrent les droits d'accès fins aux ressources et aux transactions des applications ;
- approche maximaliste : les applications délèguent entièrement la gestion des droits à l'environnement mis en œuvre.

Une approche maximaliste présente les risques suivants :

- multiplication des profils utilisateurs, des droits d'accès et des rôles applicatifs :
  - charge de gestion accrue,
  - perte de sens et d'efficacité de l'environnement partagé ;
- difficulté d'évolution : l'environnement doit évoluer à chaque fois qu'une application évolue ;
- difficulté technique : limitation de la granularité par les connecteurs du marché de solution de *provisioning*.

Il convient alors de trouver un **compromis** pour tirer pleinement bénéfice d'un environnement partagé de gestion des utilisateurs et de leurs accès.

En général, le référentiel porte les informations nominatives sur les utilisateurs et des données de rôles métiers.

La mise en place des rôles métiers est réalisée **le plus tôt possible** en travaillant avec chaque direction mais uniquement si le chemin à parcourir est réaliste pour une entreprise donnée. Elle peut notamment être faite **métier par métier**.

Elle s'accompagne de plus d'une certaine **souplesse** pour autoriser une gestion individuelle par exception de certains accès sur certaines ressources (notamment pour des raisons de sécurité afin de gérer de manière individuelle des accès sur des ressources très sensibles).

Les règles d'accès ou rôles applicatifs dont la logique est souvent spécifique à chaque application notamment dans le monde des progiciels restent en partie dans le périmètre de celles-ci. Seules, des premières règles d'accès macroscopiques en nombre « limité » peuvent être dans le référentiel. Pour les applications développées en spécifique, l'ensemble des règles peut être stocké dans le référentiel.

Intégration dans le SI

Pour y parvenir, il est nécessaire de :

- **mieux anticiper les impacts sur les applications** et prendre en compte leurs spécificités (gestion du multi-domaine…) à travers la mise en œuvre de moyens :
  - questionnaire vers les responsables des applications :

    modes d'accès à l'application, plates-formes supports, domaine, caractères spéciaux dans les URL, longueur des URL, utilisation de frames, iframes, layer…, schéma d'authentification, mode de gestion des sessions, mode de déconnexion, gestion des sessions, tests de surveillance de l'application, ressources à protéger…,
  - mise en place des environnements de qualification et qualification des applications,
  - définition et mise en place d'une organisation, de processus d'intégration des applications et de mise en production des applications ;
- avoir la capacité de gérer les versions de composants de la solution ;
- préparer la **migration des utilisateurs,** notamment la récupération de leurs mots de passe usuels lors de l'intégration des services applicatifs. Ce sujet est toujours très compliqué car les mots de passe en question sont

généralement stockés dans les référentiels existants de façon chiffrée et non réversible ;

- prendre en compte la **qualité de service** (performances, haute disponibilité) :
  - accessibilité : des services de SSO, contrôle d'accès qui deviennent un point de passage obligé lors des accès aux services,
  - performances : des systèmes qui peuvent avoir des impacts sur le niveau de performances des accès aux services applicatifs lors de l'authentification et le contrôle d'accès,
- adapter l'exploitation et la supervision : les outils mis en œuvre nécessitent d'adapter les solutions pour continuer à exploiter les services applicatifs et surveiller leur fonctionnement.

Adopter une approche orientée service

De la souplesse de la conception jusqu'à la recette

Il est généralement nécessaire de faire des compromis dans une démarche annuaire d'entreprise d'un grand groupe. Ils peuvent influencer la solution cible ainsi que la démarche de mise en œuvre de cette cible. Ils trouvent leur raison dans :

- des impacts organisationnels trop profonds pour les administrateurs et les utilisateurs,
- une complexité trop importante et des impacts technologiques trop forts sur les services existants ou sur les hommes en charge de la gestion du SI.

Les arbitrages à réaliser qui peuvent survenir dès la conception de la solution ou lors de la recette portent alors sur les thèmes suivants :

- les environnements à couvrir,
- le niveau de sécurité,
- le niveau fonctionnel,
- le confort utilisateur,
- le périmètre d'utilisateurs pris en compte.

Par exemple, les arbitrages peuvent porter sur les aspects suivants :

- niveau fonctionnel des services selon les environnements couverts ;
- niveau « acceptable » par certains utilisateurs de **complexité du mot de passe**, d'exigences sur les **paramètres de sessions** (*timeout* avant réauthentification)

ou encore de durée de suspension après échec d'authentification ;

- réactivité du *helpdesk* à travers des mots de passe réversibles pour certaines populations (ex. : VIP) ;
- **alertes de sécurité** « acceptables » par certains utilisateurs lors de leur connexion en raison du chiffrement du mot de passe transmis sur le réseau ;
- mot de passe proposé aux utilisateurs lors de la réinitialisation par le *helpdesk* ;
- procédures de *log off* du SSO adaptées aux modes de déconnexion propres aux utilisateurs ou aux services applicatifs.

Une gestion méthodique du changement

Il convient de garantir avant la livraison de la solution :

- l'appropriation des concepts et du modèle de sécurité par les RSSI ;
- la compréhension et l'adhésion sur :
  - les procédures d'administration des utilisateurs,
  - les modes d'accès pour les utilisateurs.

Pour y parvenir, il est notamment nécessaire :

- d'associer les métiers aux phases de conception du système ;
- de proposer aux métiers des services d'accompagnement et support pour l'utilisation des services ;
- d'être très attentif à la définition des IHM pour les utilisateurs en terme d'ergonomie, texte et cinématique ; cette définition doit être basée sur un prototype et se faire selon un processus itératif associant les utilisateurs finaux ;
- de proposer une communication et une formation adaptée à chaque type d'acteurs (administrateurs techniques et fonctionnels, utilisateurs, exploitants, architectes du SI, métiers, utilisateurs…) et distillée au moment approprié. Par exemple, la communication auprès des utilisateurs finaux peut se faire au sein des supports de communication interne à chaque métier, par mail, sur l'Intranet ou encore lors des premières utilisations des services d'authentification.

Un alignement de l'organisation

La fiabilisation de la gestion des utilisateurs, de leurs profils et de leurs accès est un impératif.

Des freins aux changements au niveau des administrateurs centraux et locaux en charge de la gestion des utilisateurs et de

leurs accès pour chaque application peuvent apparaître : nouveaux acteurs, redéfinition des rôles, difficulté à faire travailler ensemble des acteurs qui ne le font pas habituellement, changement des habitudes de travail…

Pour y parvenir, il sera nécessaire d'être attentif aux thèmes suivants :

- formaliser les objectifs de qualité (sans viser le « zéro défaut ») ;
- analyser la cinématique globale des processus ;
- identifier, qualifier et optimiser les référentiels de données « maître » ; impliquer et responsabiliser les propriétaires de ces données dans la construction du référentiel :
  - définir les niveaux de préséance entre les référentiels et les règles précises de dépendances (i.e. qui alimente qui ?),
  - fournir tous les outils d'aide facilitant la participation des propriétaires,
  - mettre en place des contrats d'objectifs avec les propriétaires,
  - mener les travaux de fiabilisation des données « maître » en collaboration avec les propriétaires,
  - mettre en place un identifiant fiable entre les référentiels de données « maître »,
  - définir des interfaces standard d'échanges de données,
  - adapter l'organisation et les processus de gestion en s'appuyant sur les **structures existantes**,
  - prendre en compte les **organisations multi-domaines** et la typologie des populations

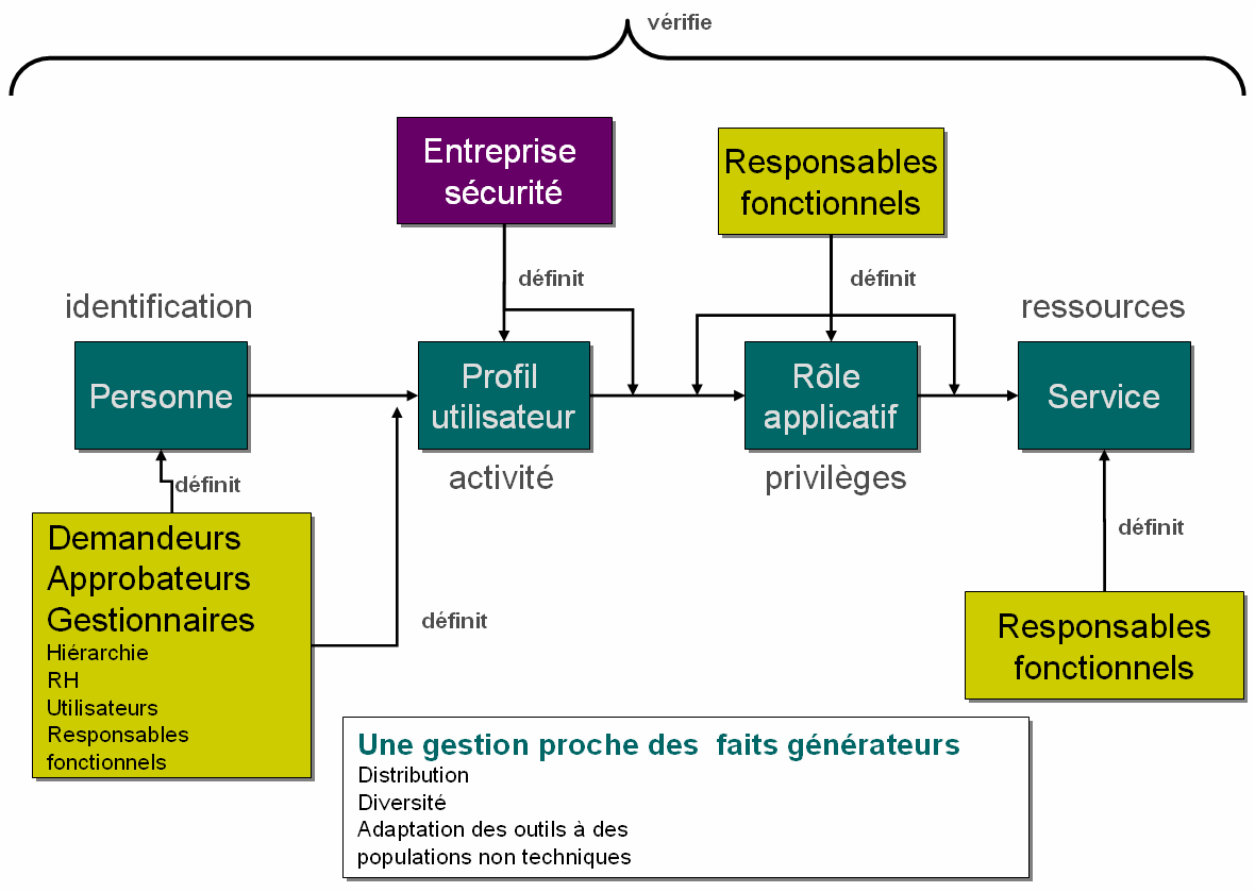

Figure 3
Organisation possible pour la gestion des données du référentiel

L'objectif est de parvenir à une organisation où l'on sait sans ambiguïté :

- **Qui exploite** : l'exploitant de l'annuaire est responsable des outils et de l'intégrité des informations, mais en aucun cas de la qualité des données.
- **Qui administre** : l'administrateur fonctionnel gère les données de l'annuaire, l'administrateur technique gère le tableau de bord de l'annuaire (qualité, performance) et assure sa diffusion.

Des aspects juridiques à traiter

Les conditions légales d'existence et de diffusion de l'annuaire

L'annuaire d'entreprise concerne, entre autres, les informations nominatives. Chacun sait qu'en France, il faut faire une déclaration à la CNIL. Elle ne pose pas de difficulté car c'est une demande courante. Toutefois des aspects juridiques sont multiples et dépendent des pays.

Il convient de rédiger et d'afficher la charte de l'annuaire qui précise les droits et devoirs de chacun et mentionne les actes juridiques autorisant l'existence de l'annuaire.

Pour les sociétés internationales, l'usage de bases de données contenant des informations nominatives sur les personnes et le transfert d'informations de ces bases de données vers des pays hors de l'Union Européenne fait l'objet de la directive européenne 95/46/EC (disponible sur le site Web *http://europa.eu.int).*

Les sociétés doivent notamment observer les principes suivants :

- les personnes recensées dans ces bases de données doivent en être informées et être informées du type d'informations stockées ;
- le traitement des informations doit respecter les lois en vigueur dans le pays où l'information est traitée ;
- les informations peuvent être utilisées pourvu que l'entreprise y ait un intérêt légitime et que ce traitement n'empiète pas sur les droits fondamentaux de la personne, notamment ses droits à la vie privée.

La directive définit le besoin de déclarer auprès des autorités nationales de protection des données (CNIL en France) les informations suivantes relatives à ces bases de données :

- le type de données traitées ;
- le but et l'objectif de ce traitement ;
- une description générale des données personnelles échangées ;
- le type de données qu'il est envisagé de transmettre hors du pays d'accueil de la base de données ; et le cas échéant, les raisons pour lesquelles ces données seront transmises vers un ou des pays n'offrant pas le niveau de protection adéquat ;
- les garanties relatives à la communication des données à des tierces parties ;
- la durée de vie des informations…

Le droit à l'image

L'annuaire supporte les photographies d'identité qui peuvent, par exemple servir de contrôle pour aider le personnel de gardiennage. Toutefois, chacun est maître de son image. Il est donc nécessaire d'impliquer chaque agent pour obtenir une photographie d'identité pour l'informer des possibilités d'intervention sur le choix de sa photographie. Le droit à l'image nécessite donc une action de communication très large et très claire.

Une preuve d'appartenance

L'annuaire définit les liens d'une personne avec une entreprise :

- pour être identifié par les collaborateurs,
- pour les accès aux services d'information,
- pour les ressources matérielles de son activité,
- par des relations hiérarchiques.

Il constitue une preuve d'appartenance au même titre qu'un bulletin de paie. Ainsi la jurisprudence considère qu'une personne figurant dans l'annuaire bénéficie des mêmes droits que les autres collaborateurs à défaut de preuve contraire. Il suffit de recevoir des courriels rattachés à une adresse de l'entreprise pour justifier de l'existence d'une rémunération. L'entreprise peut donc se voir condamner à considérer qu'une personne est son employé si elle ne peut fournir de preuve contraire. Ainsi il faut clairement identifier les personnes qui exercent un rôle dans l'entreprise et qui ne sont pas rémunérées par elle. Comme il n'est pas aisé dans les grandes entreprises de retrouver le contrat, EDF a choisi de mettre dans l'annuaire et l'adresse du courrier un A pour les personnes ayant un contrat de travail, un E pour des personnes extérieures qui ne peuvent prétendre à une rémunération directe.

Le respect de l'identité

Toute personne peut exiger voir afficher son nom d'usage à la place de son nom administratif. Cette modification ne peut être effectuée sous la responsabilité de l'exploitation de l'annuaire. Il faut étudier un processus qui s'appuie soit sur les Ressources Humaines, soit sur la hiérarchie locale.

La qualité des données

Les données de l'annuaire sont extraites d'autres systèmes d'information et sont publiées.

La principale difficulté est de publier les informations fournies par d'anciennes applications de qualité douteuse. Ces informations n'étaient pas visibles. L'annuaire révèle des carences dont les responsables sont ailleurs.

Le risque de déléguer l'administration

L'administrateur des informations de l'annuaire dispose de pouvoirs considérables. L'externalisation est un risque. Les personnes qui interviennent doivent être clairement identifiées et être assermentées. Pour limiter ce risque, les entreprises mettent en œuvre des procédures automatiques d'affectation de ressources (*e-provisioning*). Il suffit que les droits soient approuvés par la hiérarchie pour être mis en œuvre.

VALEUR DE L'ANNUAIRE POUR L'ENTREPRISE ET SES METIERS

La dynamique des projets d'annuaires s'organise autour de deux axes :

- une démarche orientée « annuaire de personnes » ou au contraire « annuaire d'utilisateurs du S.I »
- une démarche orientée « consolidation de référentiels » ou « mise en place de processus de gestion étendus »

Il en résulte fondamentalement quatre types de projets rappelés dans le tableau ci-dessous.

	Consolidation de référentiels existants	**Processus de gestion étendus**
Annuaire de personnes	Pages Blanches et Pages Jaunes	Organigrammes
Annuaire d'utilisateurs du S.I	Annuaire de Services	e-Provisioning / Gestion de profils utilisateurs

Tableau 1
Les 4 types de projet d'annuaire

Ces projets peuvent être vus comme autant de paliers d'une démarche globale d'annuaire d'entreprise dont nous allons maintenant examiner les principaux bénéfices.

Pour plus de lisibilité, nous avons réalisé une analyse sur deux ou trois pages pour chacun de ces cas d'usage des annuaires d'entreprise.

Nous espérons que cela constituera pour notre lecteur un bon argumentaire de départ pour la vente en interne de ce type de projets.

Volet 1 : « Pages Blanches » / « Pages Jaunes »

Description

Ce premier palier correspond à la mise en œuvre de la solution envisagée (méta-annuaire et annuaire) en s'appuyant sur l'utilisation telle quelle des référentiels de données disponibles au sein des entités opérationnelles. Ces référentiels identifiés comme contenant les données « maître » pour l'annuaire de personnes et l'annuaire de sociétés sont dans la plupart des cas les suivants :

- R.H.
- Paie.
- PABX.
- Messagerie

Analyse de la valeur

Ce palier présente pour le Groupe les bénéfices suivants :

La création d'une « carte d'identité collaborateur » facilitant la communication dans le Groupe et développant le sentiment d'appartenance au Groupe

Cette carte d'identité permet d'identifier et de désigner les collaborateurs du Groupe, de les localiser et facilite la communication entre collaborateurs.

L'annuaire génère alors les bénéfices suivants :

- Des gains de temps et du confort pour les utilisateurs.
  - Les informations sur les personnes sont disponibles dans un référentiel unique qui facilite et accélère les recherches. Aujourd'hui, il est souvent nécessaire pour obtenir des informations de les chercher dans plusieurs référentiels ou dans des annuaires « papier » qui ne sont pas toujours à jour.
  - La fiabilité de l'annuaire évite les fréquentes frustrations que vivent aujourd'hui les utilisateurs lorsqu'ils n'arrivent pas à trouver la « bonne » personne.
- Le développement des échanges entre les personnels du Groupe à travers une meilleure compréhension et connaissance du Groupe.

Une carte d'identité des entités du Groupe

Elle permet de connaître les localisations géographiques des sociétés pour les déplacements des collaborateurs, les moyens

d'accès ainsi que les moyens pour communiquer avec ces sites géographiques.

Elle permet à chacun de mieux comprendre l'organisation du Groupe et le métier des différentes sociétés.

Ces informations sont en particulier pertinentes en cas d'arrivée ou de mutation de collaborateurs pour facilement expliciter le contexte (travail des RH).

Des gains financiers à travers la diminution des annuaires papier

Le nombre d'exemplaires papiers des annuaires à diffuser se trouve fortement réduit. De même, les charges de travail fournies par différentes entités (RH, communication, marketing…) pour construire et gérer un ou plusieurs de ces annuaires papier diminuent.

Un service d'infrastructure, composant fondateur et accélérateur pour les applications

L'annuaire de personnes devient un service d'infrastructure généraliste et universel à travers la mise à disposition de services communs à un ensemble d'applications ou d'utilisateurs.

Cette mise à niveau facilite la prise en compte et le déploiement de nouvelles applications, favorise le développement de nouveaux usages et rend plus aisées les futures évolutions du Système d'Information.

Les bénéfices de l'annuaire sont les suivants :

- Des réductions des délais de déploiement des applications et une meilleure maîtrise de ces délais.
- La garantie d'un niveau de service constant pour les applications et les utilisateurs à travers une vision globale du fonctionnement de ce service d'infrastructure.
- Une rationalisation de l'architecture des applications ce qui facilite leur maintenance.
- Des économies sur le développement des applications par la mise à disposition de services communs.
- Une souplesse et une flexibilité pour faciliter les futures évolutions du Système d'Information tant sous l'angle technique que fonctionnel.

Volet 2 : « Organigrammes »

Description

Il s'agit d'un enrichissement du premier palier. L'organigramme permet à tous les employés :

- de trouver des informations à jour, complètes et cohérentes sur les entités du Groupe (adresse de site, téléphone, plan d'accès, visibilité sur l'organisation, ses membres…) ;
- surtout, de disposer d'une vision des relations hiérarchiques, opérationnelles et fonctionnelles entre les individus et les entités du Groupe.

Ce palier se conçoit sans connecter de nouveaux référentiels, mais en mettant en œuvre de nouveaux processus de gestion : l'organigramme doit en effet refléter au plus juste l'organisation de l'entreprise, c'est-à-dire qu'il doit être piloté dans une double logique de « juste à temps » et de « traçabilité » dont les principales caractéristiques sont les suivantes :

- Les informations accessibles ont fait l'objet d'une approbation formelle à travers un processus de publication qui garantit leur exactitude le jour où elles deviennent accessibles ;
- Une gestion déléguée doit permettre des mises à jour d'informations sur les entités par des populations relais (assistantes notamment) dans des délais très brefs ;
- Une gestion de pré-publication (avec des dates de début de validité) doit permettre la préparation puis la prise en compte de changements dans les rattachements d'une personne à des entités ;
- Des fonctions de sauvegarde doivent permettre de restaurer un organigramme devenu inaccessible et des fonctions d'archivage de conserver une trace des organigrammes précédents.

Analyse de la valeur

Ce palier présente les bénéfices suivants.

Facilite la relation de l'employé avec son entreprise

Il est perçu par chacun comme essentiel de pouvoir fournir aux collaborateurs du Groupe des moyens de se repérer à chaque instant dans un environnement changeant, et de leur donner accès à des informations fiables et actualisées sur l'entreprise dans laquelle ils évoluent.

A ce titre les organigrammes procurent les gains suivants :

- Des gains de temps sur des processus transverses (ressources humaines, comptabilité…) à travers une

identification plus rapide et efficace des personnes concernées et d'une compréhension immédiate de l'organisation en place.

- Cela facilite et accélère l'intégration des nouveaux collaborateurs.
- Cela permet aux nouvelles organisations qui se mettent en place d'être plus vite opérationnelles et efficaces car plus vite assimilées par les collaborateurs.

- Des gains de temps sur des processus métiers à travers une identification plus rapide de toute personne de l'entreprise qui peut aider à trouver une solution à un problème (expert), et de savoir où cette personne, quelle qu'elle soit, se situe dans l'organisation.

Dynamise le fonctionnement en réseau

L'entreprise est amenée à fonctionner de plus en plus en mode « réseau », et les employés doivent dès lors être considérés comme étant les membres d'une ou plusieurs communautés locales à une entité ou transverses.

- Les communautés « métier / fonctions » (R.H., Communication, Finance, Juridique, etc.)
- Les communautés « projets ».
- Les communautés « géographiques » ou thématiques.

Pour être efficaces, les membres des communautés qui ne se connaissent pas nécessairement tous ont besoin d'outils leur permettant de mieux communiquer. Ce palier y contribue par la connaissance qu'il permet d'avoir de la fonction, de la position dans l'organisation et des langues préférées (communication adaptée).

Intègre plus rapidement des nouvelles sociétés ou des modifications organisationnelles dans le Groupe.

La présence de l'annuaire permet de rapidement intégrer les modifications de structure du Groupe et de rapidement les diffuser auprès de tous au sein du Groupe.

L'annuaire permet de trouver des personnes par rôle ou fonction, dans la structure, par société, par application ou par communauté, cependant, les personnels externes, membres de différents réseaux, ne sont pas recensés.

Volet 3 : « Annuaire de services »

Description

L'annuaire permet d'identifier une personne pour l'accès aux applications (Intranets, portails de communautés…). Il permet également le stockage des profils utilisateurs au bénéfice de ces mêmes applications. Ces identités et profils sont utilisés pour contrôler les accès sur des ressources ou la personnalisation de l'interface et des fonctions.

Ce palier correspond à la construction de la solution et au raccordement des applications des entités opérationnelles en s'appuyant sur l'utilisation telle quelle des référentiels de données disponibles dans ces entités.

Ces référentiels identifiés comme contenant les données « maîtresses » pour l'annuaire de personnes sont dans la plupart des cas les suivants :

- Bases de comptes (NT, Messagerie…).
- Base applicative.

Analyse de la valeur

Ce palier d'annuaire d'utilisateurs de ressources S.I (systèmes, applications) présente les bénéfices suivants.

Une amélioration du niveau de sécurité des accès aux ressources de l'entreprise, notamment pour les nouvelles applications.

L'annuaire constitue un référentiel unique et commun qui permet d'identifier de manière unique une personne et de lui donner des droits d'accès aux applications locales ou transverses du Groupe. Ainsi les membres d'une même communauté ont des accès identiques et contrôlés sur les applications.

De nombreux domaines applicatifs illustrent ce besoin :

- Employee Self-Service (ESS) pour consulter et maintenir à jour la fiche personnelle des employés, procéder à des évaluations en ligne, etc.
- Portails employés, partenaires ou clients pour un accès personnalisé à un certain nombre de services, d'informations et de connaissances en fonction des caractéristiques du profil des personnes y accédant.
- Application d'inscription en ligne à des formations

De ce fait, il fournit une meilleure cohérence (réduction des risques d'erreurs) et un meilleur contrôle dans l'attribution des

ressources (vision d'ensemble des utilisateurs et de leurs droits).

La réduction des coûts de la DSI liée aux gains sur les charges de validation et de saisie des informations associées aux utilisateurs et à leurs droits d'accès.

Ceci est notamment permis par :

- Une efficacité et une simplicité dans la gestion des utilisateurs pour les administrateurs à travers l'utilisation d'une interface unique.
- La mise en place de synchronisation bidirectionnelle entre l'annuaire et les référentiels existants

Ces temps peuvent être valorisés en coûts d'administration comme suit :

Gains = coûts actuels - coûts après la mise en œuvre de l'annuaire :

Coûts actuels :

- Nombre de référentiels
- Temps de vérification du contenu par référentiel
- Coût moyen de chaque vérification
- Nombre de personnes dans chaque référentiel
- Pourcentage de modifications par référentiel
- Nombre de référentiels
- Temps moyen des changements
- Coût moyen des changements
- Bilan coût actuel : Nombre de référentiels x (coût de vérification + nombre de changements x coût moyen de changement)

Coûts après mise en œuvre de l'annuaire :

- Temps de vérification du contenu de l'annuaire
- Coût moyen de cette vérification
- Temps résiduel de gestion par référentiel synchronisé
- Coûts de cette gestion
- Bilan coût cible : Coût vérification de l'annuaire + nombre de référentiels synchronisés x coûts résiduels de gestion.

Le tableau suivant met en évidence sur un cas concret un gain de 14 hommes/an sur la gestion des référentiels au sein d'une entreprise de plus de 10 000 personnes.

	Nombre	Type de référentiel	Temps de gestion annuel d'un utilisateur (en heures)
Existant	10	Services existants	0,16
	2	Nouveaux services	0,80
Avec annuaire de services	2	Nouveaux services	0,03
	2	Référentiels supprimés (dont 3 délégations)	0
	8	Référentiels synchronisés	0,03
	2	Référentiels non synchronisés	0,16
	1	Annuaires de service	0,40
Nombre moyen d'utilisateur dans chaque référentiel :			**10 000**
Gain annuel récurrent en heures / an :			**14**

Tableau 2
Calcul du gain obtenu sur la gestion des référentiels au sein d'une entreprise de plus de 10 000 personnes

On notera que le Giga Group estime un gain financier de 70 000$ US annuels par tranche de 1 000 utilisateurs.

Il y a également des gains sur les temps de support et de *helpdesk* pour la réinitialisation des mots de passe des utilisateurs et la gestion des droits d'accès (limitation des risques d'erreurs) pour les applications utilisant l'annuaire. Le Giga Group estime sur ce poste un gain financier de 75000$ US par an par tranche de 1000 utilisateurs.

Enfin, l'expérience montre une diminution des délais et des coûts de développement, d'évolution et de déploiement des nouvelles applications grâce à la mise à disposition de ce référentiel fiable.

L'exemple ci-dessous montre l'impact sur une DSI dont le budget de développement annuel serait de 300 000 j.h.

Gain total sur applications informatiques de 7 000 k€ HT, décomposés comme suit :

- gains réalisés en développements, maintenance et exploitation : 10% des j.h informatiques,
- périmètre des applications concernées par l'annuaire : 1/3 du système d'information.

L’annuaire de sécurité construit dans ce palier 3 induit donc des gains très significatifs dans le budget d’investissement et de fonctionnement d’une DSI. Cependant, les limitations sur la fiabilité des informations qu’il contient notamment en termes de profils utilisateurs conduisent beaucoup d’entreprises à mettre en œuvre le palier 4 décrit ci-dessous pour pérenniser ces gains.

Volet 4 : « e-Provisioning / gestion des profils utilisateurs »

Description

Ce volet consiste à :

- Mettre en place des outils de « *provisioning* » associés à la gestion des personnes (automatisation, contrôle).
- Mettre en cohérence l'ensemble des processus de gestion des personnes au niveau de chaque entité.
- Conduire le changement auprès des acteurs.

Un système de *« provisioning »* permet:

- L'allocation automatique des ressources informatiques (messagerie, applications…) ou physiques (bureau, PC, mobile…) nécessaires à un collaborateur, en gérant ses profils métiers, donc ses droits d'accès.
- Le lancement automatique du circuit d'approbation d'une demande pour l'allocation de ces ressources.

Il inclut les composants suivants :

- La prise en compte des notions de **profils métiers** pour la gestion des habilitations (des droits attribués à une personne en fonction de son métier…)
- La prise en compte de « workflow » dans les processus métiers pour la gestion des habilitations
- La synchronisation systématique des mots de passe et la gestion des politiques de mots de passe.
- L'audit et le reporting sur les accès

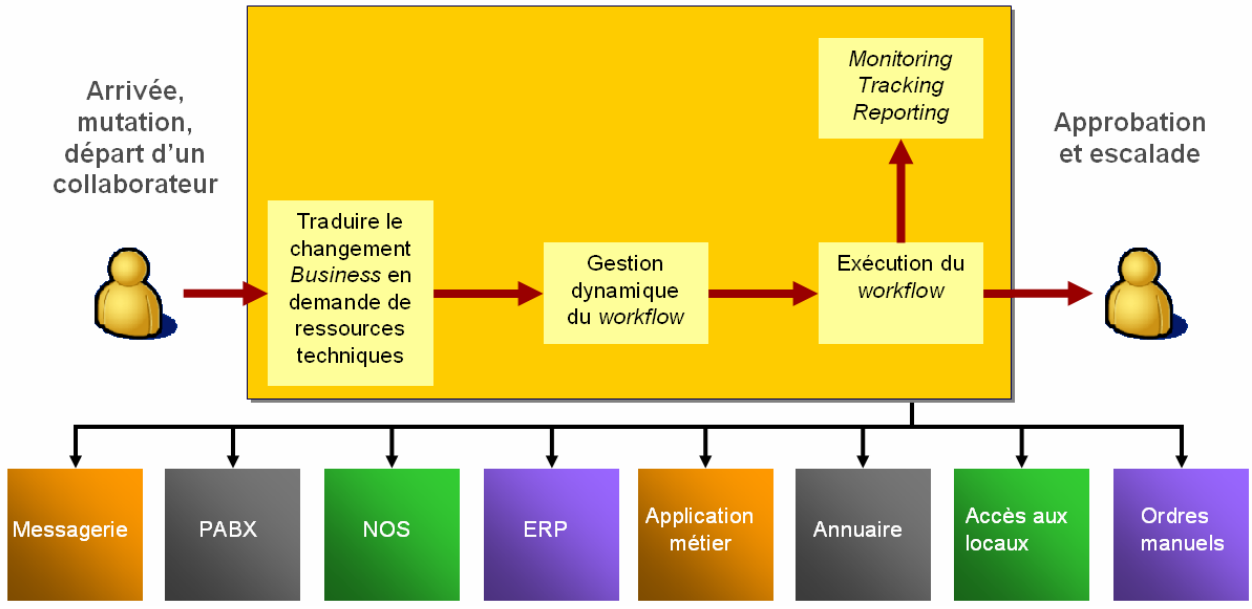

Figure 4
Illustration du principe de fonctionnement

Analyse de la valeur

Ce volet présente les bénéfices suivants.

Une pérennisation des gains de l'annuaire de services au niveau Groupe comme au niveau local grâce à une meilleure fiabilité des données consolidées.

Lorsque tous les processus nécessaires ont été mis en place, les gains sont alors nombreux :

- Un excellent niveau de sécurité des accès aux ressources de l'entreprise.
- La personnalisation dans les applications.
- Une meilleure efficacité, fluidité et simplicité à travers l'automatisation, le contrôle des tâches d'administration et la limitation du nombre d'intervenants.
- La réduction des temps de recherche, de validation, de saisie des informations associées aux utilisateurs et à leurs droits d'accès.
- Localement, la suppression des coûts d'exploitation et de maintenance des référentiels utilisateurs supprimés.
- Des gains sur les temps de support et de *help-desk* pour la réinitialisation des mots de passe des utilisateurs et la gestion des droits d'accès.
- La diminution des coûts de développement, d'évolution et de déploiement des applications.

Une conformité aux exigences de plus en plus élevées de traçabilité

Ce palier permet notamment de répondre aux questions suivantes :

- Qui utilise quelles applications ?
- A quelles ressources mes collaborateurs ont-ils accès ? Pourquoi celui-ci a-t-il accès à la « base des contacts » ?
- Quelles modifications ont été faites pour Mr X. ? Qui a approuvé ces modifications ?
- Qui accède à quoi, est-ce en phase avec leurs impératifs business ?

La cohérence et la rapidité dans l'attribution des ressources.

Cela se traduit par :

- La réduction des délais. Aujourd'hui, de trop nombreuses opérations impliquant différents intervenants sont encore

nécessaires pour retranscrire l'arrivée ou le départ d'un collaborateur dans le S.I : introduction de données dans le S.I RH, création d'un compte de messagerie, gestion des accès et des habilitations aux applications, …

- La prise en compte de la dimension métier à travers la définition par profils et par rôles.
- Une utilisation des ressources du S.I validée par le management (*workflow*, notifications et escalades) qui retrouve ainsi son pouvoir de décision et un meilleur contrôle dans l'attribution des ressources :
  - En prenant en compte les évolutions des collaborateurs (sites, poste, projets).
  - En protégeant l'activité lors du départ des collaborateurs

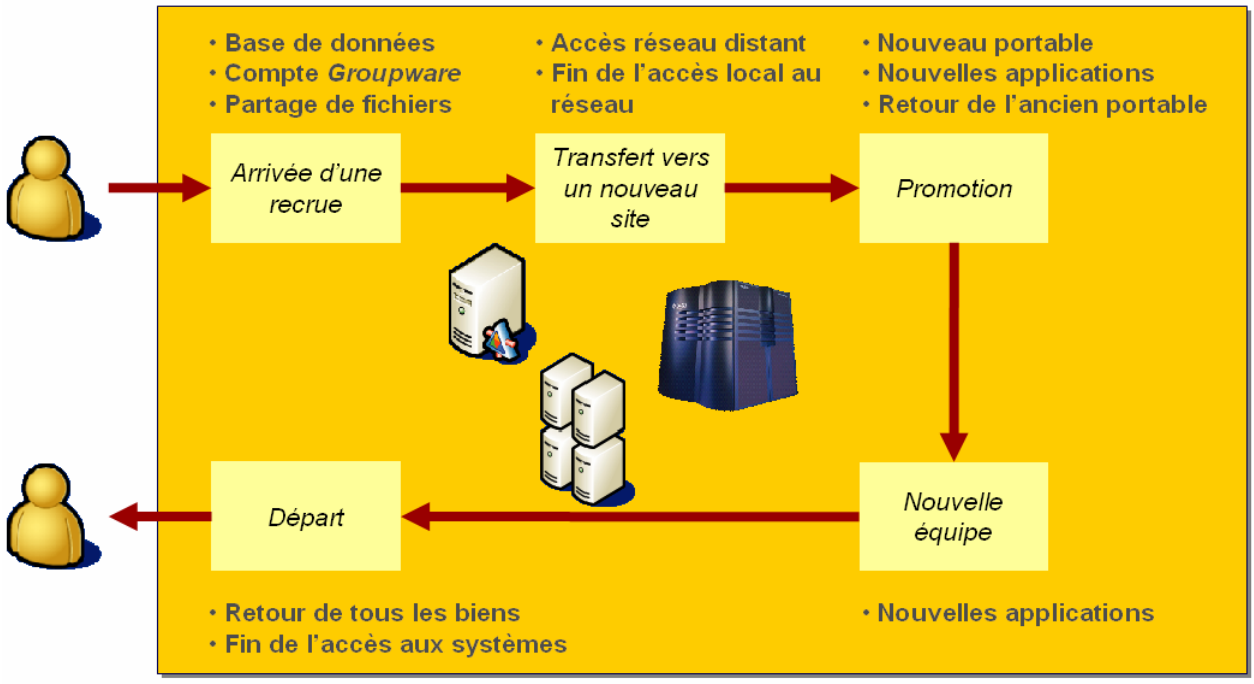

Figure 5
Illustration du principe

A l'arrivée, les bénéfices sont très variables mais il faut noter que l'un des membres du CIGREF qui a mis en place tous les modules de *provisioning* est passé d'une charge moyenne de 5 j.h. à 10 minutes par utilisateur…

PERSPECTIVES

Les grands groupes français et internationaux semblent durablement entrés dans une phase de mutation profonde où trois forces majeures vont s'exercer :

Une orientation du système d'information vers le client

- généralisation au sein des entreprises d'applications accessibles par des portails intranet ou extranet
- création d'un S.I. étendu : nouvelles applications orientées e-business ou e-commerce pour de nouveaux acteurs (partenaires, clients et fournisseurs)

Une grande flexibilité et une meilleure réactivité

- des changements de périmètre : fusions-acquisitions, partenariats, cessions…
- des reconfigurations : réorganisations, externalisations totales ou sélectives, délocalisations…

Des contraintes réglementaires de plus en plus fortes

- conformité du S.I en termes d'audit des opérations, de traçabilité, d'archivage et de transparence comptable ;
- engagements sur la disponibilité du système pour les personnes autorisées.

Dans ce contexte, nous pensons qu'il faut dorénavant retenir un objectif essentiel : faire évoluer les projets d'annuaire vers un système complet de gestion des identités capable de « donner les bons droits d'accès aux bonnes personnes au bon moment ».

Les avantages d'une telle approche sont nombreux et ne peuvent être tous cités ici. Pour notre part, nous en retiendrons trois :

- La prise de conscience par le management de l'entreprise des enjeux d'une gestion des identités
- L'augmentation importante du niveau de sécurité global, mais un niveau cohérent avec la sensibilité des applications et la nature des accédants, qui ne s'oppose pas à la rapidité du business
- Les gains en coût et en délais (pour accélérer la prise en compte des organisations, faciliter et accélérer le déploiement et la mise en œuvre d'applications…)

Les obstacles à surmonter ne doivent cependant pas être sous-estimés :

Les organisations ne sont pas vertueuses par nature

- Tendance naturelle dans un grand groupe à multiplier les référentiels pour servir des besoins spécifiques
- Difficultés fréquentes à faire coopérer des acteurs n'ayant pas de liens hiérarchiques directs : Métiers, DRH, DSI, Services Généraux, Paie, etc.

Des failles de sécurité ressurgissent à tout moment

- Gestion non cohérente de données sur les utilisateurs et leurs droits d'accès (stratégies non homogènes)
- Données redondantes et souvent fausses ou obsolètes

L'improductivité vit à l'insu du management

- Processus hétérogènes et désynchronisés (par mail, téléphone, fax…)
- Tâches répétitives à faible valeur ajoutée
- Multiplication de « *login /password* » pour l'utilisateur

Compte tenu de la puissance des trois forces évoquées plus haut, il nous semble qu'il faut pourtant conserver l'ambition de lancer un projet de transformation bénéficiant à toutes les divisions et branches métiers de l'entreprise.

De fait, nous constatons avec plaisir que les nombreuses démarches annuaires et gestion des identités lancées par nos membres se concentrent maintenant sur trois dimensions qui sont autant de gages de succès :

- **Le marché** : une démarche de communication, de valorisation et de vente des services d'annuaire auprès des entités clientes
- **L'offre** : une stratégie d'investissement dans des infrastructures adaptées sur des périmètres successifs de plus en plus larges
- **L'organisation en support** : refonte des processus de gestion du cycle de vie des données et alignement des missions des acteurs concernés

La route est encore longue, elle ne sera sans doute jamais finie puisque la gestion des identités est consubstantielle de la pérennité de l'activité économique de nos membres, mais le chemin est passionnant et finalement aucun des participants n'a regretté les efforts entrepris dans ce domaine car **la dynamique importe plus que la cible.** D'où ce rapport qui aura peut-être contribué à convaincre les sceptiques et donné des raisons de continuer à ceux qui ont mis en place les premiers paliers…