BIPER V4 : un référentiel des personnes pour le déploiement des services en ligne

Thierry AGUEDA
Direction des Systèmes d'Information (DSI)
Equipe Accompagnement, Architecture, Applications
Bâtiment Langues et Nouvelles Technologies - Bureau 36
Université Pierre-Mendès-France (Grenoble 2)

Résumé

L'université Pierre-Mendès-France a développé, il y a plusieurs années, un référentiel des personnes et de leurs rôles dans l'établissement. Les premières versions géraient des informations liées à la localisation des personnels via un réseau de correspondants locaux situés au plus près de l'information. Une nouvelle version a vu le jour en intégrant un spectre plus large des personnes (étudiants, invités…), une couverture mufti-établissements et des périmètres métiers plus larges (patrimoine, gestion des études, bibliothèque…). Les données alimentant BIPER sont issues de plusieurs logiciels métier (AMUE, Cocktail, développements locaux...).

Déployé dans quatre des établissements grenoblois, ce référentiel commun permet de fédérer des informations issues de différentes applications métier et de les compléter par des informations de terrain plus fiables en mettant en œuvre des mécanismes de délégation avancés. Cette délégation permet également aux personnes de proximité de donner des accès à des services informatiques en liaison avec l'organisation locale du fonctionnement (messagerie, VPN, intranet, portail, domaine et partage samba...).

Nous décrivons également les concepts de base du référentiel, modélisés en notions de base de données relationnelle, son architecture avec un système de poids associé à chaque source d'information, son implémentation dans le SI, son mode d'alimentation par les applications métier et la gestion des conflits qui peuvent apparaître. Nous montrons comment centraliser la gestion des accès à des services en s'appuyant sur le référentiel et en mettant en œuvre l'organisation humaine nécessaire pour en déléguer la gestion à des fonctionnels responsables du contenu ou des accès à ces services tout en favorisant la sécurité et la réactivité.

Mots clefs

services, référentiel, personnes, déploiement, groupes, annuaires, rôles, domaines d'activités, applications métier

1 Présentation et contexte

1.1 En quelques mots

BIPER (Base Interuniversitaire des Personnes Et de leurs Rôles) est un référentiel de personnes conçu par l'université Pierre-Mendès-France (UPMF). Il regroupe des informations sur toutes les personnes en rapport avec les établissements : étudiants, personnels, lecteurs autorisés, invités, extérieurs...

Développé depuis 2004, il a évolué de simple annuaire de localisation et de compétences vers une brique centrale du système d'information de l'UPMF, puis de 5 autres établissements.

En lien avec les applications métier, complété par un réseau de correspondants, il permet de déployer aisément des services pour les utilisateurs. Grâce à ses possibilités de délégation, les services informatiques sont allégés de tâches répétitives de création de compte et d'ouverture de droits.

Pensé dès l'origine pour fonctionner dans un environnement multi-établissements, il mutualise une partie des informations, ce qui facilite le travail sur la cohérence des référentiels métiers, évite des doubles saisies et permet d'améliorer la qualité des données, y compris dans les applications métier.

1.2 Intégré dans le système d'information global

BIPER est alimenté par des données issues d'applications métier. Le paramétrage de BIPER permet, pour chaque donnée de définir des priorités entre les informations en provenance de ces applications de gestion. Ces liens automatisés assurent la cohérence de BIPER avec les briques du Système d'Information, évite des doubles saisies, simplifie les processus de gestion de l'arrivée des personnes dans les établissements, de la mobilité des personnels entre services, de la durée de vie des comptes informatiques...

1.3 Au plus près de l'information

Les données issues des applications métier sont en général des informations administratives de gestion, par exemple le rattachement administratif d'un agent à un service ou une composante. Si elles correspondent souvent à des informations collant à la réalité, elles demandent à être complétées par des personnes sur le terrain.

Ces compléments peuvent être de plusieurs ordres :

- des informations absentes des applications métier, qu'elles soient des données difficilement à jour dans une application de gestion de ressources humaines (numéros de téléphone, de fax, bureau) ou pas assez fines dans ces applications (appartenance à une équipe, un département) ;

- des informations contradictoires avec ce qui est saisi dans les applications de gestion. Par exemple une personne affectée officiellement à une structure, mais qui en réalité travaille partiellement dans une autre.

Dès le départ, BIPER a été pensé pour déléguer la saisie auprès de correspondants au plus près de l'information. La saisie d'informations est réalisée en général au niveau de secrétariats de composante, de service ou de laboratoire. Le système de gestion des droits permet de cloisonner cette saisie : un correspondant peut uniquement ajouter ou modifier des données de la (ou des) structure(s) qu'il gère.

Cette saisie décentralisée permet de compléter les données issues d'applications métier, mais pas de les supprimer ou de les modifier.

2 Concepts

2.1 Centré sur l'individu

BIPER est construit autour des personnes et de leurs relations avec leur environnement dans les établissements. La personne, élément central du référentiel, s'entend comme personne physique, un individu. Les informations qui s'y rattachent sont les noms et prénoms usuels et de naissance, la date de naissance.

L'individu évolue dans des domaines (études, patrimoine, organisation...) dans lesquels il joue un ou plusieurs rôles (voir Figure 1)

2.2 Données de référence : les domaines

Afin de fédérer des données issues de différentes sources (en particulier les applications métier), BIPER contient des données de référence qui peuvent soit être mises à jour par ces applications métier, soit en être indépendantes et dans ce cas, un mécanisme de traduction (mapping) permet de faire le lien.

Les données de référence peuvent être regroupées en grands domaines correspondants aux activités des établissements. Les principaux domaines sont :

- domaine patrimoine : décrit les bâtiments et les sites où ils se trouvent

- domaine organisation : décrit pour chaque établissement les structures qui le composent (services, composantes, département, équipe de recherche,...). Les structures peuvent être gérées par plusieurs établissements.
- domaine Ressources Humaines (RH) : décrit les types de contrat, les grades, les corps, ...
- domaine études :décrit les diplômes, les cursus, …

Les domaines sont bien sûr liés entre eux : un bâtiment est géré principalement par un établissement, une structure peut appartenir à plusieurs établissements, ...

2.3 Les rôles

Les rôles permettent de lier les personnes aux domaines. Par exemple, le rôle étudiant lie une personne au domaine études en précisant le cursus suivi. Une personne peut avoir plusieurs rôles de type différent et dans des établissements différents.

Le dénominateur commun de tous les rôles est qu'ils se déroulent dans un établissement sur une période donnée.

Les rôles implémentés dans BIPER 4.1 sont :

- rôle personnel (ou RH pour ressources humaines) : pour les personnes travaillant dans un établissement, ou hébergées dans un établissement. Il peut s'agir de personnels enseignants, administratifs, de chercheurs d'organisme, de doctorants hébergés, d'enseignants d'autres université, de vacataires, de stagiaires... En résumé de personnes-ressources.
- Rôle extérieur : pour les personnes ne faisant pas partie de l'établissement, n'ayant pas un bureau, pour lesquelles l'établissement va offrir des services informatiques (accès wifi par exemple).
- Rôle étudiant : pour les personnes suivant des études dans un établissement.
- Rôle Lecteur de S(I)CD : pour les personnes présentes dans le système d'information documentaire, auxquelles on offre des services (consultation de base documentaire, wifi,...) et qui ne sont pas forcément personnel ou étudiant.
- Rôle membre de conseil ou de commission : personnes participant à des instances dans un établissement. Il peut s'agir de personnalités invitées auxquelles on va offrir un accès à l'intranet d'un conseil.

Tous ces rôles sont cumulables pour un même individu, dans un ou plusieurs établissements.

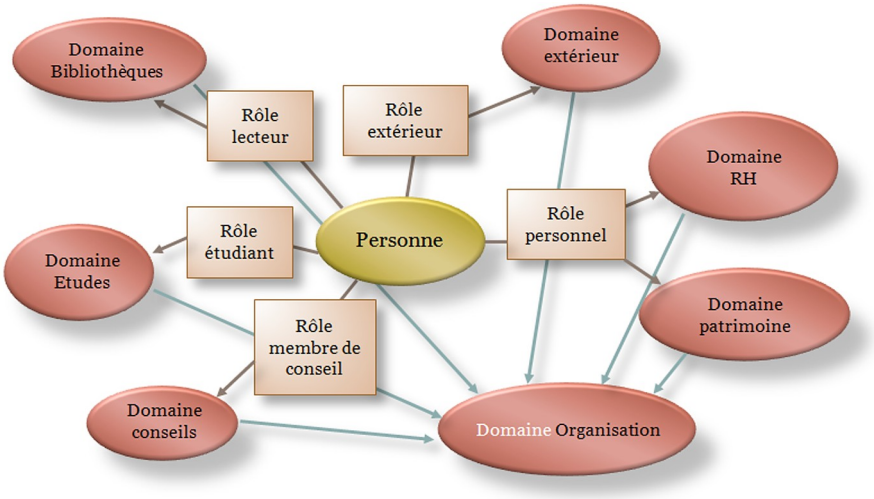

Figure 1: Les domaines et les rôles

Le rôle RH (ou personnel) est le plus complexe et le plus utile qualitativement. Il concerne les personnes travaillant dans un établissement. Il est borné dans le temps (pour les titulaires et les contrats à durée déterminée, il n'y a pas de date de fin de contrat).

Il est lié au domaine RH (BAP, discipline enseignée, discipline de recherche, grade, emploi, fonctions exercées…selon des nomenclatures nationales). Il s'effectue dans un ou plusieurs lieux de travail (bâtiment, bureau, structure, téléphone, courrier électronique,...).

2.4 Les groupes

Les groupes sont des ensembles d'individus. Les groupes peuvent appartenir à un établissement. On dispose de 2 types de groupe dans BIPER :

- les groupes gérés manuellement : via un éditeur web, on peut créer des groupes et les peupler d'individus,
- les groupes automatiques : il est possible de créer des groupes à partir de requêtes sur les données de BIPER. Ces groupes sont mis à jour par programme (cron). On définit pour cela deux requêtes :
    - la première pour définir les groupes à créer (exemple la liste des composantes) ;
    - le seconde pour définir les personnes de chacun des groupes correspondant à la première requête (les personnes d'une composante).

Dans la philosophie de BIPER, les groupes correspondent à des entités réelles (groupe de travail, commission, catégories de personnels, personnes travaillant dans une structure...) plutôt qu'à des ensembles utilisateurs d'application (voir plus loin le chapitre sur les services).

2.5 Cycle de vie: durée de vie des informations

Une personne peut avoir différents états selon ses rôles : présent, suspendu, (parti), prolongé.

Lorsque l'état d'une personne est présent ou prolongé, ses accès informatiques sont opérationnels. Dès que cet état devient suspendu, elle n'a plus accès à ses services en ligne.

L'état de la personne est calculé à partir des dates de fin ou de validité de tous ses rôles :

Date de validité d'un rôle = date de fin + délai.

Le délai est paramétrable selon l'établissement et le type de rôle. Il permet de gérer les retards de saisie dans les sources de données.

Il est surtout intéressant pour les personnels en mutation interne, car il permet un recouvrement des périodes de présence dans l'ancienne et la nouvelle structure. L'agent accède ainsi naturellement aux services de ses deux structures, facilitant les biseaux.

La Figure 2 décrit, selon un chronogramme, les différents états. Une personne est présente tant qu'un de ses rôles est actif. Elle est prolongée lorsque tous ses rôles sont dans ce délai de grâce, et suspendues lorsqu'aucun de ses rôles n'est plus valide ou prolongé.

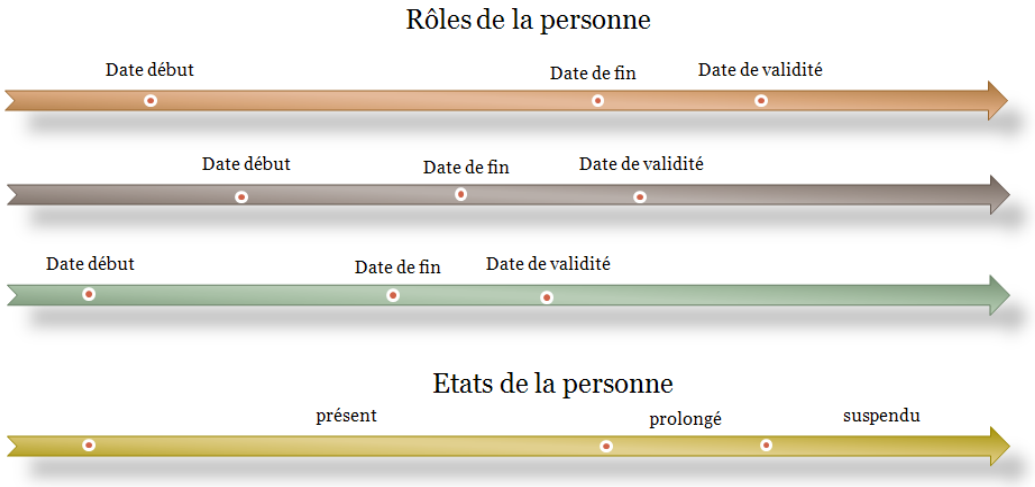

Figure 2: États et rôles

2.6 Les sources de données

Les sources de données alimentent BIPER en information. Ce sont des applications nationales ou locales qui peuvent piloter :

- les domaines,
- les personnes,
- les rôles.

Il est souhaitable d'avoir une seule source de données par domaine (et par établissement), mais il est possible, moyennant certaines précautions, d'en avoir plusieurs. Typiquement, les personnes sont pilotées aussi bien par les applications métier de RH que de scolarité ou de bibliothèque ; les rôles RH sont pilotés par l'application de RH, les rôles étudiant par celle de scolarité, etc.

2.7 Les correspondants BIPER

Dès la première version de BIPER en 2003, on s'est rendu compte que les applications métier contenaient des informations administratives collant au besoin du domaine géré. Bien qu'utiles à d'autres domaines, elle se sont souvent révélées incomplètes pour certains usages. Par exemple, une Direction des Ressources Humaines connaît rarement le téléphone ou le bureau exact des agents. Si elle est performante quant au rattachement administratif des agents, elle ne saisit pas nécessairement dans son application-métier des informations assez précises pour déployer certains services. Par exemple, l'affectation d'un agent peut être saisie dans une composante alors que la personne travaille plus précisément dans un département ou dans un laboratoire.

Les personnels d'organisme de recherche sont souvent mal connus des DRH qui ne les saisi pas systématiquement dès leur arrivée dans un laboratoire car elle ne gère pas leur carrière. Les correspondants du laboratoire sont en charge de mettre à jour BIPER pour cette population.

Toutes ces informations de terrain ne sont connues que des personnes directement au contact des agents. C'est pourquoi BIPER permet à un réseau de correspondants de mettre à jour le référentiel via une interface web. Les correspondants sont des personnes occupant des postes stratégiques (secrétariats, responsable de petites structures...) au plus près du terrain.

BIPER permet de paramétrer la priorité, information par information, entre les informations saisies par un correspondant et celles issues de sources de données. Typiquement, on paramètre le référentiel pour qu'un correspondant ne puisse pas modifier une information issue de l'outil de DRH, mais qu'il puisse ajouter de l'information. Les applications métier priment donc sur les correspondants. Ces derniers remontant les anomalies constatées pour correction dans l'application métier.

BIPER est doté d'une gestion des droits liée à la zone d'intervention : un correspondant a des droits dans telle ou telle structure. Il peut ajouter des personnes, ajouter des rôles ou des lieux de travail dans sa structure, mais il ne peut en aucun cas modifier des information ou en ajouter dans les autres structures.

3 Architecture

3.1 Vue globale

BIPER est construit autour d'un noyau (Figure 3) qui permet la manipulation des différents concepts (domaines, rôles). Le noyau assure la cohérence de l'information, gère les droits des utilisateurs, assure l'interface avec les sources de données externes, historise les modifications et stocke les données dans une base relationnelle.

Le noyau est accessible via différentes API : classes PHP, SOAP et REST.

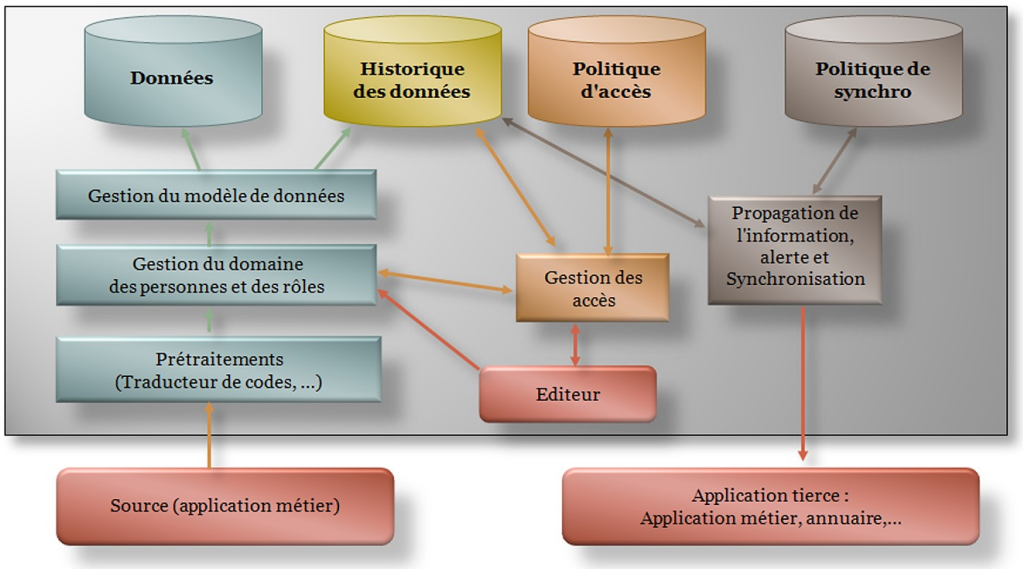

Figure 3: Fonctionnement logique

Des éditeurs permettent par une interface web d'interagir avec le référentiel :

- éditeur de personnes : réservé aux correspondants, il permet de mettre à jour les informations sur les personnes (études suivies, lieu de travail, participation à des conseils...) et offre un tableau de bord pointant des anomalies
- éditeur pour architecte : réservé aux administrateurs de BIPER, il offre une interface pour gérer le référentiel (nomenclatures, paramétrages...) et offre des outils avancés pour résoudre des conflits (doublons, anomalies,...)
- éditeur de groupes : déployé auprès de fonctionnels, il permet de créer des groupes de personnes, soit manuellement, soit à travers des requêtes sur les données du référentiel
- éditeur de services : réservé aux gestionnaires de service, il facilite le déploiement de services informatiques (messagerie, accès à des intranets, à des partages samba, listes de diffusion...).

Ces éditeurs s'appuient sur les API PHP du noyau.

3.2 Technologies utilisés

BIPER 4 est développé en PHP 5.3. La base de données utilisée est mySQL, à travers une couche d'abstraction. Les différentes interfaces graphiques ont été développées avec le framework MVC (Modèle-Vue-Contrôleur) cakePHP 1.3.

L'authentification des utilisateurs se fait via des serveurs CAS externes à BIPER (un par établissement).

Les recommandations ou normes suivantes sont respectées XHTML 1.0, CSS 2, SOAP 2.0, REST, CAS 2.

4 Intégration dans le Système d'Informations

4.1 Alimentation par des sources

Le référentiel de BIPER peut être alimenté par différentes sources. Ces sources peuvent gérer les même données et un mécanisme d'alerte avertit les gestionnaires des incohérences entre les sources de données. Par exemple un nom orthographié de façon différente dans deux HARPEGE.

Les éditeurs sont considérés comme des sources de données par le noyau. Il obéissent aux mêmes règles de contrôle de données et de droit d'accès que les sources externes.

Pour chaque élément du référentiel (c'est à dire pour chaque champ de chaque table, il est possible de paramétrer BIPER afin de déterminer si une source peut modifier la donnée. Chaque source dispose d'un poids pour chacun de ces éléments. Une source n'est autorisée à modifier une donnée que si cette donnée n'a pas été modifiée par une source disposant d'un poids plus fort.

Il est ainsi possible de définir par exemple que l'outil de gestion des Ressources Humaine est prioritaire sur les données de type RH (rôle RH, contrat de travail, structure de rattachement administratif...) par rapport à l'éditeur utilisé par les correspondants. Ou que les données issues d'APOGEE sont prioritaires par rapport à un fichier d'étudiants issu d'un tableur.

Si deux sources ont le même poids sur une donnée, elles peuvent toutes deux la modifier. Un mécanisme de détection est en place pour signaler aux gestionnaires du Système d'Information les sources incohérentes qui modifient à tour de rôle une même information.

Objet / Sous-objet	**HARPEGE 1**	**HARPEGE 2**	**APOGEE 1**	**Éditeur des correspondants**	**Commentaire**
Personne /Nom usuel	9	9	8	5	On donne un légère priorité aux outils de DRH car il y a plus de contrôle que pour ceux de scolarité. En revanche les correspondants qui peuvent jouter des personnes voient leur saisie écrasé par les applications métier si BIPER parvient à faire le lien entre la personne saisie à la main par un correspondant et celle issue d'une de ces sources de données.
Personne /Nom patronymique	9	9	8	5	
Personne/Prénom (de naissance)	9	9	8	5	
Personne/Prénom usuel	.	.	.	5	Les applications de gestion ne connaissent pas le prénom usuel. En revanche le correspondant oui.
Rôle RH / début de contrat	9	9	.	5	Priorité à l'application-métier

Tableau 1: Exemple de poids sur les sources de données

4.2 Types d'intégration

Les données du référentiel sont accessibles en écriture via des programmes d'importation de fichiers (format de type CSV) et via les API PHP, SOAP et REST. Tous ces accès passent par le noyau de BIPER qui effectue les contrôles de droit et de cohérence des données.

L'utilisation d'outils « extracto-chargeurs » (Extract Transform Load ou ETL) est possible pour générer les données à intégrer dans BIPER, mais le chargement doit être effectué par le noyau pour deux raisons principales :

- maintenance facilitée : un seul code pour assurer la qualité des données, leur cohérence, la gestion des droits,
- efficacité : le chargement de données en masse est optimisé.

En lecture, il est également possible d'interroger directement la base de données.

En écriture, cette voie est fortement déconseillée car elle court-circuite le noyau.

4.3 Quelques application liées à BIPER

En alimentation :

- applications métier : HARPEGE (3 instances à ce jour), APOGEE, VIRTUALIA*, SCOLARIX*
- Gestion de compte : récupération des login et adresses de messagerie générées par un annuaire AGALAN (LDAP).

En utilisation :

- annuaire interne : intégré au CMS KSUP, OpenStreetMap et GoogleMaps,
- annuaire académique (pages blanches),
- Helpdesk : renseignement automatique des bureaux, téléphone, bâtiment pour faciliter les interventions,
- SIFAC : adresses et téléphone des utilisateurs (via SOAP),
- annuaires LDAP (AGALAN et SUPANN) : groupes et individus,
- application de signature électronique des chartes,
- services en ligne (voir plus loin).

* implémentation en cours

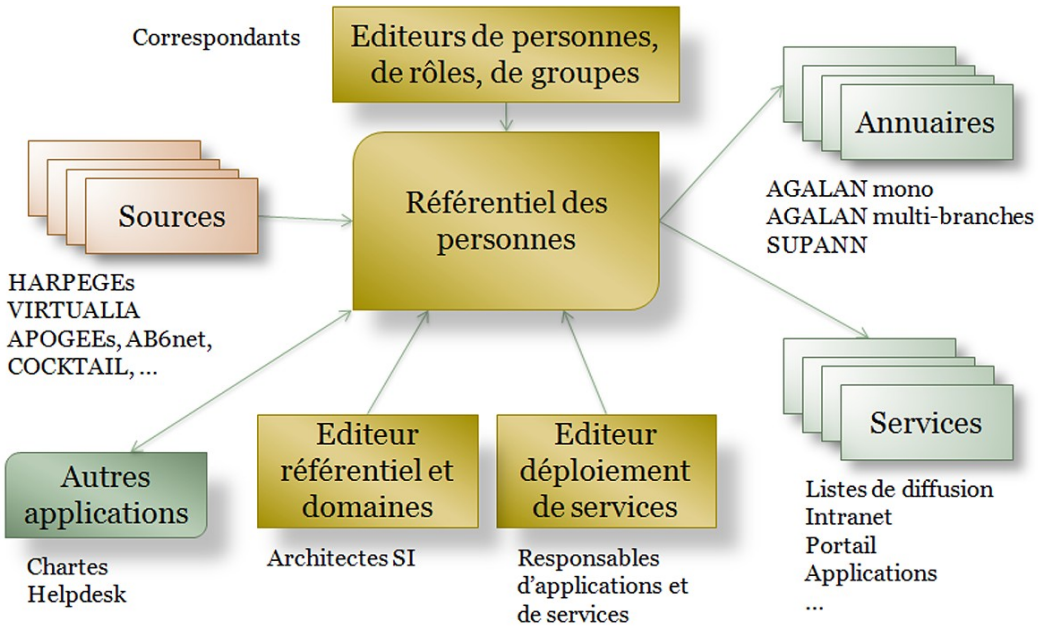

Figure 4: BIPER dans le Système d'Informations

La Figure 4 résume la place de BIPER dans le Système d'Information des établissements, en particulier les flux de données.

5 Services autour de BIPER

5.1 Déployer des services pour des individus et des groupes

BIPER permet de déployer des services informatiques de façon manuelle ou automatique.

Le déploiement manuel consiste à indiquer via une interface web quelles personnes ou quels groupes de personnes doivent avoir accès à un service.

Le déploiement automatique consiste à définir des groupes de personnes dynamiquement via des requêtes sur les données du référentiel. Par exemple, toutes les personnes qui ont un rôle RH valide sur un site accèdent à l'intranet du site. L'écriture de ces requêtes est réservée aux personnes connaissant bien l'organisation du référentiel.

Il est possible d'arriver au même résultat en utilisant des groupes dynamiques, dons les membres sont calculés en fonction de données du référentiel.

Ces deux mécanismes permettent un déploiement automatique des services dès que les données arrivent dans le référentiel. Ainsi la simple intervention d'un correspondant qui indique dans BIPER la présence d'un chercheur d'un organisme dans son laboratoire ouvre à ce dernier le droit d'utiliser les machines du laboratoire, donne accès au partage smb de son labo, l'ajoute dans la liste de diffusion du labo...

Le déploiement manuel est plutôt réservé aux personnes extérieures et aux exceptions, lorsqu'une catégorie de personne n'a pas le droit d'utiliser une application, mais telle ou telle personne le peuvent.

5.2 Délégation

On considère deux types de personne pouvant donner accès à des services :

- les gestionnaires de service : ils peuvent ajouter des personnes, des groupes aux utilisateurs d'un service, via une interface spécifique (vue centrée sur les services : qui accès à un service ?) ;
- les correspondants avec droit : ils peuvent donner accès à des services aux personnes de leur structure en cochant simplement des cases dans une interface web (vue centrée sur les individus : à quel service un individu a-t-il accès ?).

On a ainsi en place une délégation qui allège le gestionnaire de service.Quelques services déployés

Les services peuvent être déployés selon plusieurs techniques :

- via un annuaire LDAP par ajout de l'utilisateur dans un groupe ou par ajout d'un attribut dans l'entrée utilisateur. Un connecteur de service lié à l'annuaire offre alors les accès au service
- via un programme externe (connecteur) appelé à la volée par l'éditeur de service, ou par un cron. Ce programme se charge de configurer le service

Les accès de l'utilisateur dépendent de la finesse de la description d'un service dans BIPER et de l'intelligence du connecteur. On peut ainsi avoir des services très basiques pour lesquels BIPER offre uniquement le point d'entrée à l'utilisateur (exemple : accès Wifi). Pour d'autres services, il permet d'aller jusqu'aux droits de l'utilisateur dans le service (rubriques d'un intranet)

Parmi les services déployés, citons :

- des accès réseau : Wifi, VPN, EduRoam,
- de l'authentification :SSO (CAS, Shibboleth), accès à des domaines (SMB),
- des accès à des outils collaboratifs : fichiers (smb), intranet (xtek), Gestion Électronique de Documents (Alfresco), plateforme pédagogique (Dokeos),
- messagerie : boîte aux lettres, gestion de listes de diffusion,
- des accès à des données : ressources documentaires de S(I)CD,
- le pilotage d'annuaire LDAP : AGALAN et SUPANN.

6 Conclusion et perspectives

La mise en œuvre de BIPER a facilité le déploiement de services informatisés. Grâce au réseau de correspondants, les utilisateurs bénéficient rapidement d'un environnement de travail numérique opérationnel, sans intervention systématique d'un informaticien.

Nous avons paramétré BIPER pour que la création de compte informatique, la réservation de l'adresse électronique et le déploiement des services de bases se fassent dans la demi-journée suivant la saisie dans le progiciel de RH (ou dans BIPER). Les services sont donc disponibles dans la quasi totalité des cas dès l'installation de la personne dans son établissement.

De plus, la centralisation dans un référentiel de personnes d'informations issues de sources différentes a facilité la mise en cohérence des applications métier, au sein d'un établissement, et entre établissements.

L'aspect inter-établissement de BIPER offre un login unique aux personnes fréquentant plusieurs universités.

Le nécessaire suivi de l'évolution des applications métier, sources de BIPER, nous mène à poursuivre les développements d'urbanisation vers les nouvelles applications utilisées par nos établissements, en particulier SIHAM pour la gestion des Ressources Humaines.

De même, l'entrée dans BIPER d'un établissement utilisant la suite Cocktail nous amène à coupler le référentiel avec GRHUM.

Fort des apports de BIPER dans l'aide à la cohérence des données, nous allons étudier les moyens d'une rétro-action vers les applications métier, qu'elle soit automatique ou manuelle sous forme d'alerte. En particulier en détectant dans une source la modification de données communes à d'autres sources, même lorsque ces données ne sont pas exactement au même format, comme par exemple c'est le cas pour les adresses postales. Si cet aspect ne faisait pas partie des préoccupations initiales de BIPER, ce sera la cerise sur la gâteau...