un IDM pour fusions, réorganisations, confinements... sans douleur ou presque

Thierry Aguéda, Laurence Comparat, Jacqueline Duclos

Un IDM pour fusions, réorganisations, confinements... sans douleur ou presque

Thierry Agueda

Laurence Comparat

Jacqueline Duclos
Université Grenoble Alpes
Direction générale déléguée – Systèmes d'information
Direction de l'appui numérique à l'administration
Equipe développement et référentiel
CS 40700 - 38058 Grenoble cedex 9
https://www.univ-grenoble-alpes.fr/

Résumé

L'Université Grenoble Alpes (UGA) utilise un gestionnaire d'identité (IDM) développé en interne depuis 2010 : Biper (129.000 personnes ayant 143.000 comptes dans 4 établissements[1], 31.000 groupes, 6.300 ressources pilotées).

Multiétablissements, Biper est alimenté par plus de 40 bases de gestion qui pilotent les informations, complétées par des correspondants. Il génère des annuaires, ou directement des accès dans des applications.

Pour la création de l'UGA (2016), l'IDM a permis de générer le nouveau SI en « dupliquant » ceux des 3 établissements préexistants, de maintenir les anciens accès et de les fermer progressivement. La fusion a été transparente pour les utilisateurs ! Toute évolution de l'organisation de l'établissement doit être paramétrée dans Biper pour permettre la continuité des droits (réorganisation 2020).

L'UGA pilote finement les accès numériques, et l'IDM fournit des outils de gestion en proximité : listes de diffusion, intranets, espace de partage… Les services informatiques peuvent accompagner les fonctionnels pour définir des règles d'accès. Pour des accès particuliers, il faut en identifier les responsables (pas toujours facile) et faire des revues de droits.

Les accès étant automatisés au maximum, nous avions tous les outils pour que la bascule en distanciel en mars 2020 se fasse quasi instantanément ! En quelques jours, outils de tchat (avec délégation de droits) et de visio furent ouverts aux personnels UGA.

Gérer l'IDM implique de maintenir paramétrage et scripts, de comprendre l'organisation de l'établissement et son SI. Nous profitons d'un outil souple, adapté à nos besoins et spécificités, moyennant des développements internes et réactifs.

Un IDM au centre du SI permet de faire face à tout... à condition de s'en occuper.

Mots-clefs

IDM, déploiement de services, fusion, habilitations, accès, délégation

1 Les personnes pouvant avoir leur compte utilisé dans différents établissements, il est normal que le nombre de comptes soit supérieur à celui des personnes, chaque compte étant détecté séparément car géré par des SI établissements différents.

1 Introduction

L'Université Grenoble Alpes (UGA) utilise un gestionnaire d'identité (IDentity Management - IDM) développé en interne depuis 2010 : Biper. Alimenté par les systèmes d'informations (SI) des établissements qui l'utilisent et complété par une saisie déléguée au sein des composantes et services, il permet de déployer des comptes à travers des annuaires ou directement dans des applications. Dans un deuxième temps, il a permis une évolution vers la gestion des autorisations d'accès pour les différents outils du SI. Nous verrons en quoi cet IDM nous a aidés dans les fusions et réorganisations successives de nos établissements. (Figure 1)

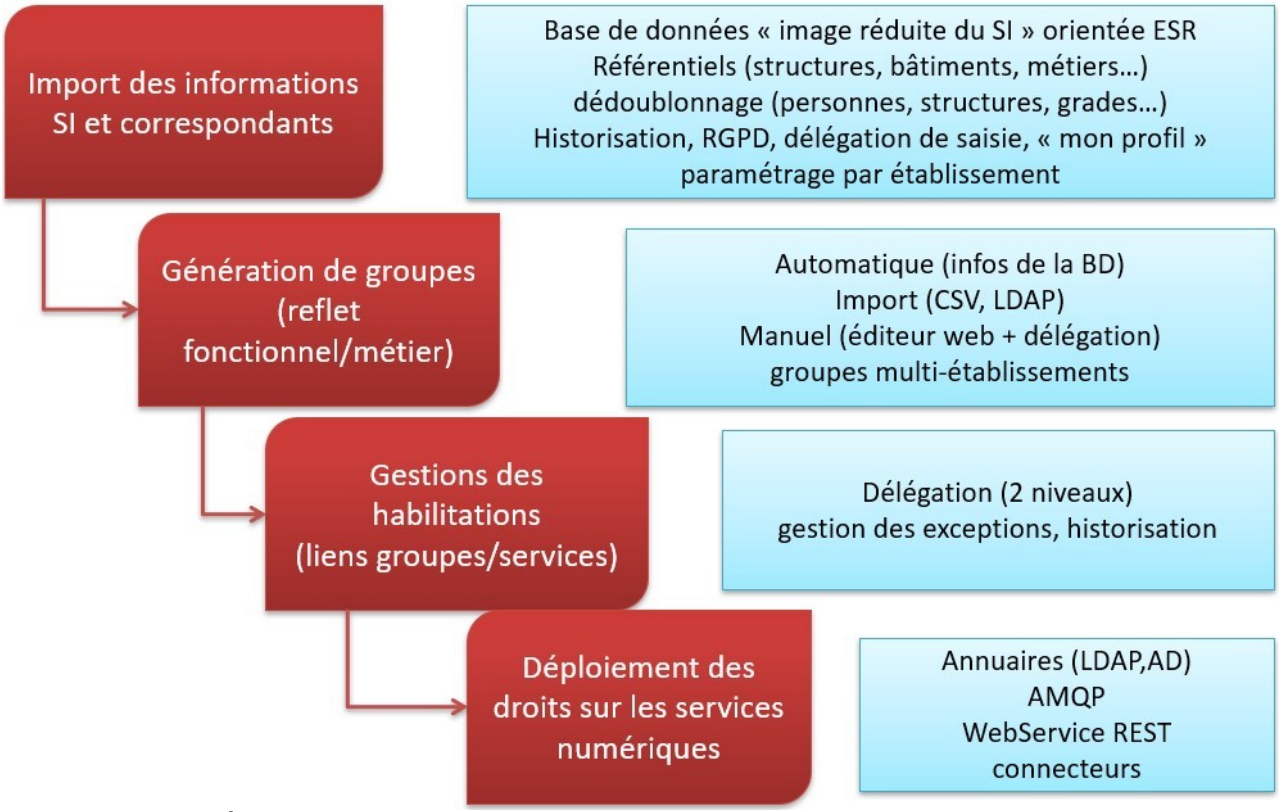

Figure 1 – Étapes du SI de gestion au déploiement des droits sur les services numériques

Nota : Dans cet article nous utiliserons de façon indifférenciée les termes « ressources » et « services » pour faire référence aux données et/ou aux outils numériques dont l'IDM gère les accès.

2 Une mise en œuvre sur le long terme

À l'origine, Biper ne se voulait pas un gestionnaire d'identité (terme alors peu utilisé). Son ADN est lié aux annuaires et aux fonctions occupées par des personnes au sein et autour de nos établissements, typiquement pour alimenter des pages blanches et des annuaires de contacts. Avec le temps sont venus s'ajouter les services numériques, les droits d'accès, les consentements qui ouvrent droit à des ressources (accès intranet étudiant, marché voyages, utilisation d'applications...), l'audit des accès...

Au centre se situe donc la personne, elle évolue dans un environnement physique (bâtiments, site), organisationnel (structures, écoles, services, directions...). Elle y joue un ou plusieurs rôles (personnel, étudiant, extérieur...). Ces différents éléments vont permettre de lui déployer des services (Figure 2).

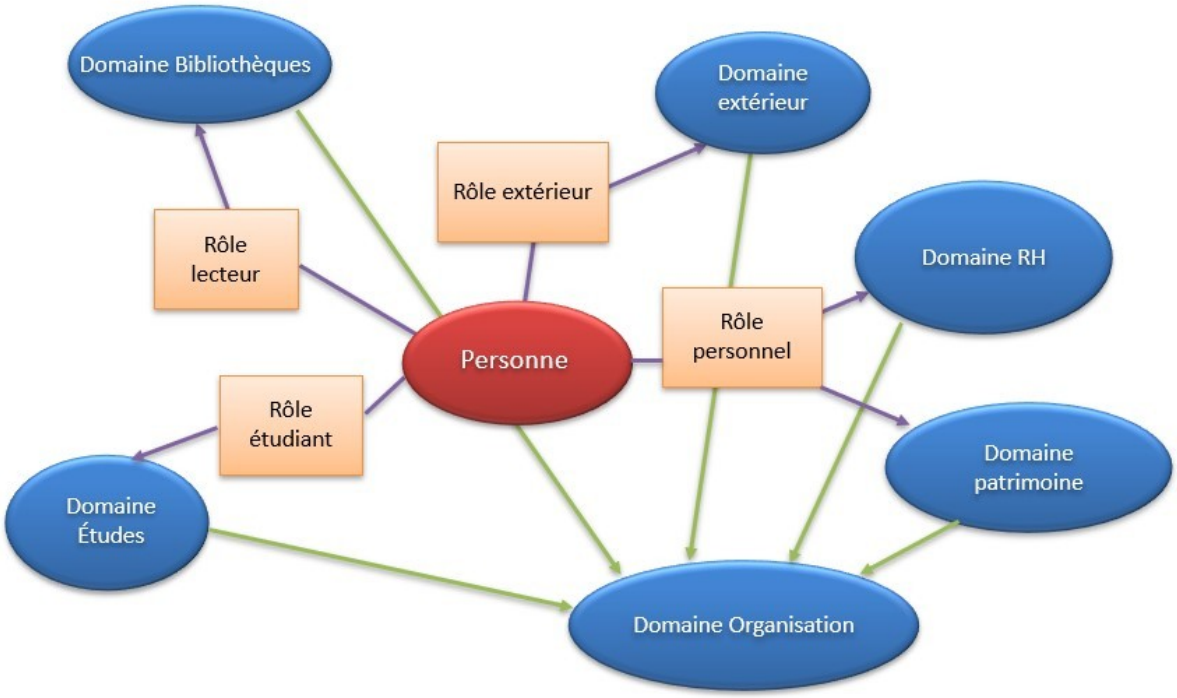

Figure 2 – La personne au centre de l'IDM, avec ses différents attributs

Biper est aussi un référentiel, ou la synthèse opérationnelle de plusieurs référentiels issus d'applications métier. Il est fortement lié au SI et a la particularité d'être non seulement alimenté par de nombreuses sources dont les données sont dédoublonnées et fusionnées, mais aussi par des correspondants fonctionnels, des informaticiens de proximité, des architectes SI qui complètent les informations en provenance des sources via des éditeurs web. Conçu pour fonctionner en mode multiétablissement, il offre une bonne vision des usagers des 4 établissements du site Grenoble-Savoie, avec comme credo :

– la personne est unique, ses rôles peuvent être multiples ;

– 1 personne = 1 compte informatique identique dans les différents établissements ;

– le SI pilote les informations, les correspondants les complètent ;

– la gestion facile de la masse (cas général et exceptions) ;

– les responsabilités sont déléguées au plus juste.

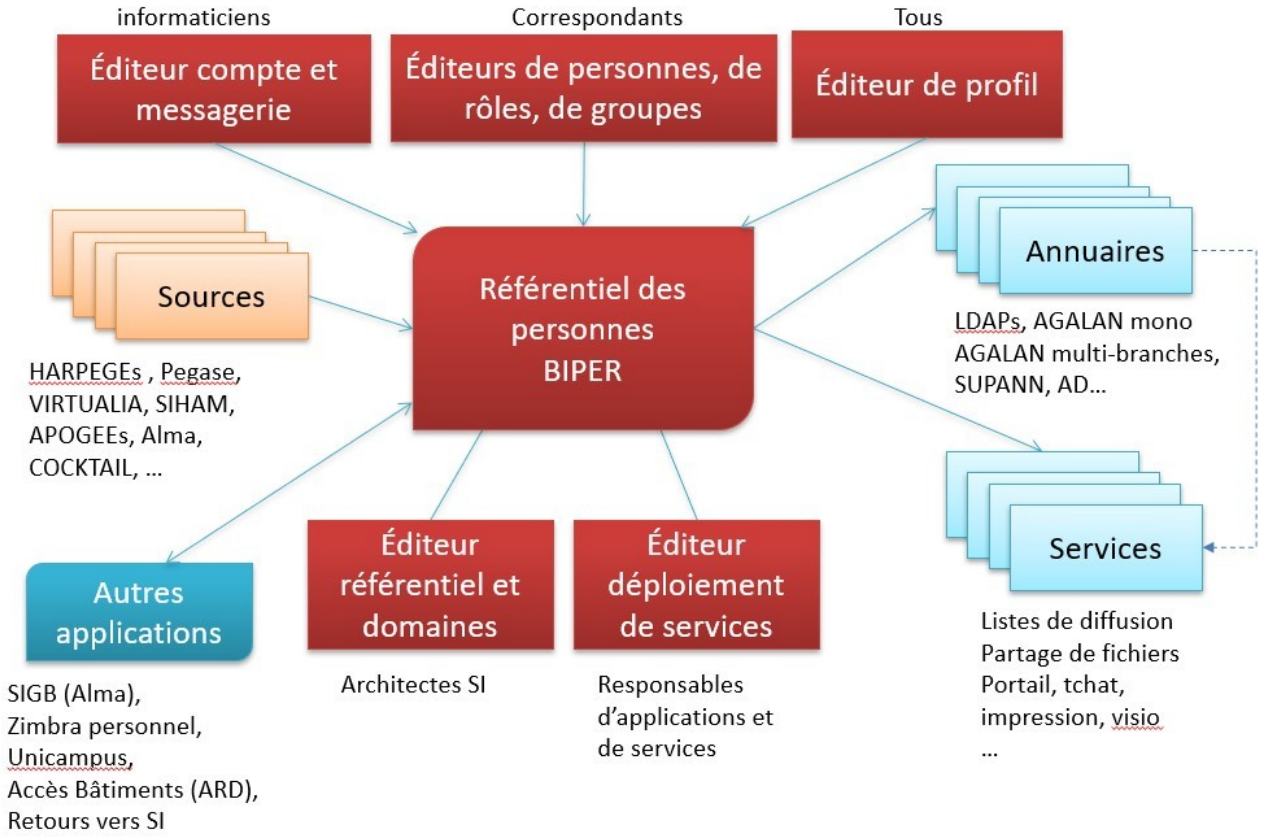

Figure 3 – Les différents outils de Biper (en rouge) et les intervenants

Cette centralisation des informations a facilité l'échange de populations entre établissements, et surtout posé une base unique (donc de référence) pour des informations issues de plusieurs SI, par exemple de plusieurs outils de gestion de scolarité ou de RH. (Figure 3)

Il faut garder en tête que l'IDM doit à tout moment permettre de répondre aux questions (Figure 4) :

– qui accède à tel service et avec quels droits ?

– à quels services accède telle personne ?

– et pourquoi / comment ces droits-ont ils été donnés ?

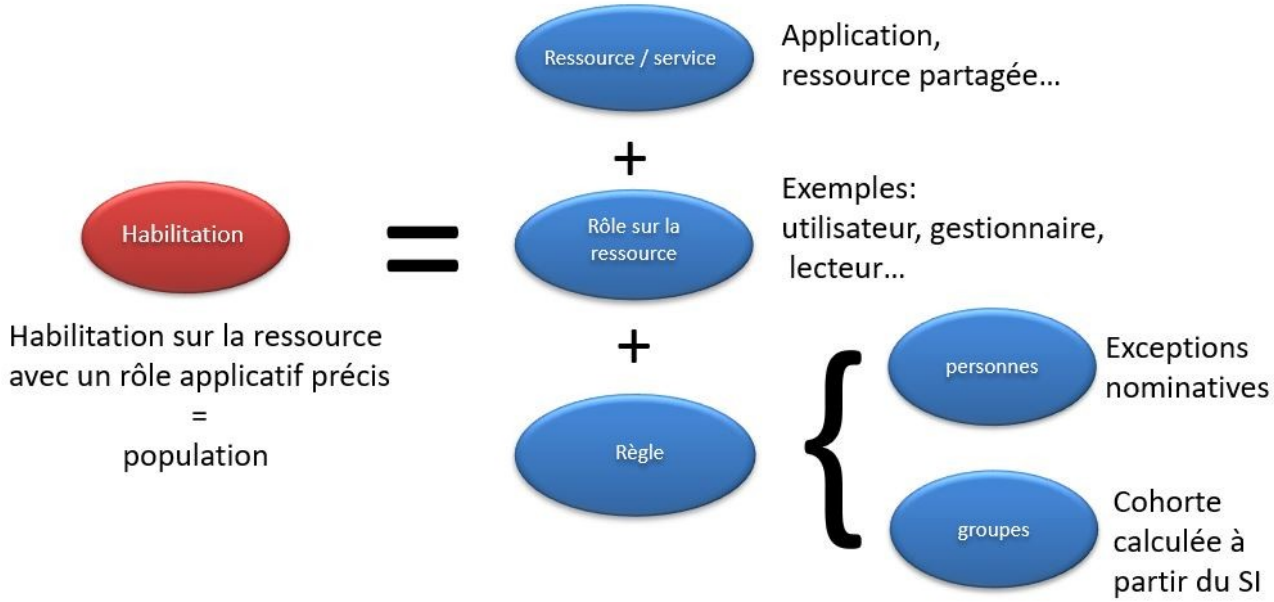

Figure 4 – La notion d'habilitation

Début 2022, l'IDM gère 129.000 personnes ayant 143.000 comptes dans 4 établissements, 31.000 groupes, 6.300 ressources pilotées, 750 structures, 1.5 million de droits d'accès (personnes/ressources).

3 La fusion : faire fonctionner 5 SI en parallèle

L'UGA, créée le 1er janvier 2016, est issue de la fusion de 3 universités : Joseph-Fourier (U1), Pierre-Mendès-France (U2) et Stendhal (U3). Il y avait donc auparavant 4 SI, ceux des 3 universités qui fusionnaient plus celui du PRES/ComUE.

Pour mettre en place le 5ème (celui de l'UGA), s'appuyer sur l'IDM a été crucial ! Il a été généré de manière anticipée en « dupliquant » les informations des 3 établissements U1, U2 et U3 au sein de Biper. Biper a ensuite pu maintenir les accès basés sur les 3 premiers ce qui a permis à la fois une migration service par service sans coupure d'accès et une fermeture progressive des 3 SI au fur et à mesure de la bascule sur le nouveau SI UGA fusionné (Figures 5 et 6). Il a donc rendu la fusion relativement transparente du point de vue des utilisateurs.

Ainsi, lors de l'installation d'un nouvel arrivant après la fusion, il avait non seulement accès aux services numériques du SI de l'UGA, mais aussi, en fonction de sa composante, aux services numériques de l'ancien établissement encore utilisés.

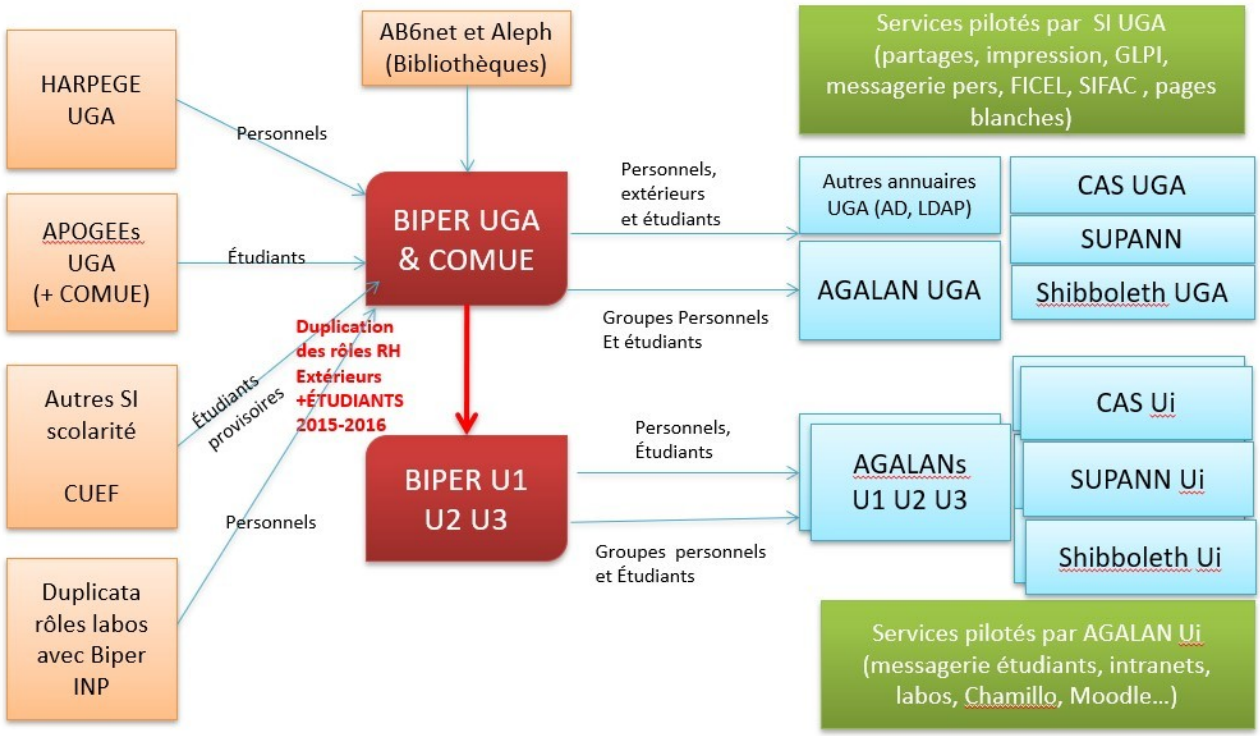

Figure 5 – *Schéma du SI en phase transitoire :*
les anciens SI sont maintenus via des mécanismes internes à Biper

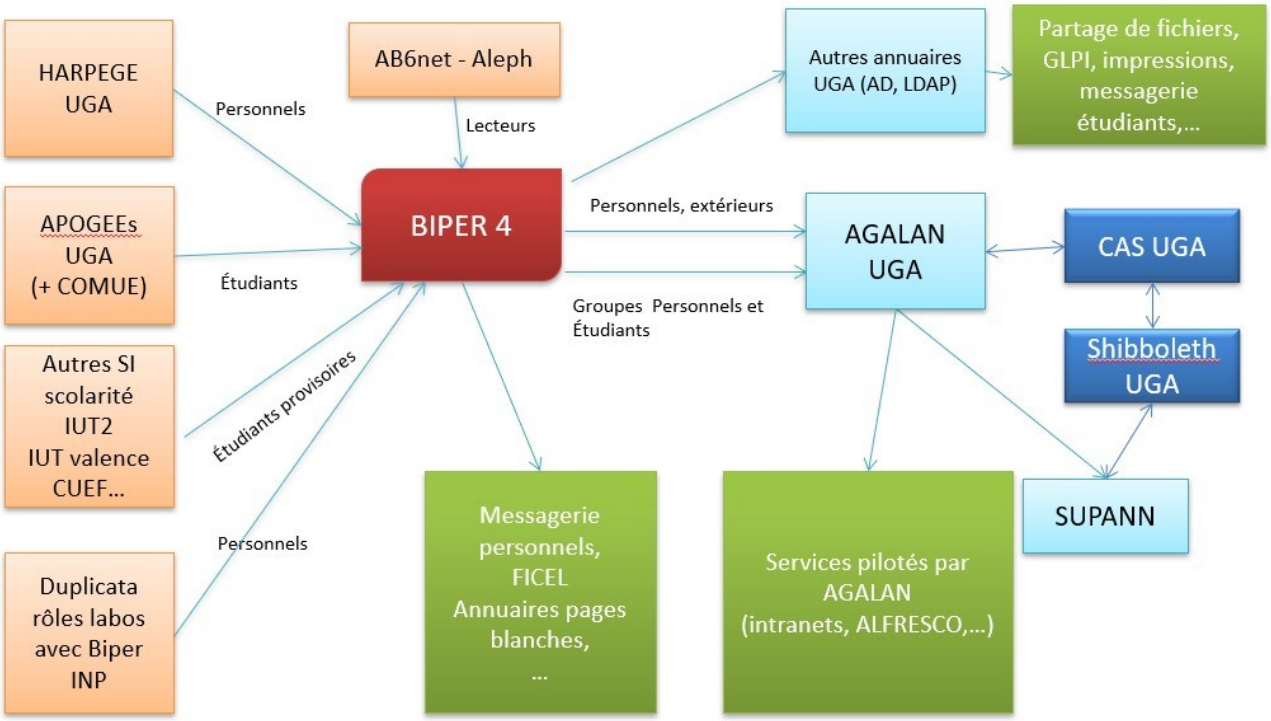

Figure 6 – *Schéma du SI en sortie de phase transitoire :*
bascule en mode fusionné, fin des anciens SI

La création du nouvel établissement a également été l'occasion de faire piloter plus finement les accès numériques des personnels et des étudiants par le SI, en fournissant aux services et composantes de l'UGA, via l'IDM , des outils pour gérer ces accès en proximité : listes de diffusion, accès intranets, espace de partage de services, boîtes courriel génériques en accès partagé, accès à des applications...

L'objectif est d'automatiser au maximum tout ce qui permet de piloter les droits numériques, en fonction du statut des personnes, de leur affectation, de leurs habilitations... Ceci au sein de l'établissement mais aussi avec ses partenaires, par exemple en répliquant automatiquement les informations des personnes affectées au sein des laboratoires cohabilités entre les différentes tutelles universitaires. (Figure 7)

Application	utilisateur	gestionnaire	enseignant	responsable	admin	referent	lecteur
ksupUGA-lect-siteINTRANETPERS-trombinoscope	8474	deployer	deployer	deployer	deployer	deployer	deployer
marches voyages	0	deployer	deployer	deployer	deployer	deployer	deployer
medatice	10689	deployer	deployer	deployer	deployer	deployer	deployer
nasa	9	deployer	deployer	deployer	3	deployer	1
numetuga	292	6	deployer	deployer	deployer	13	deployer
ordre_de_mission	16530	deployer	deployer	deployer	deployer	deployer	deployer
papercut	3458	deployer	deployer	deployer	deployer	deployer	deployer
ParapheurElectronique	17	deployer	deployer	deployer	deployer	deployer	deployer
partage-AD	deployer	293	deployer	deployer	deployer	deployer	deployer
portailEtudiant	deployer	deployer	deployer	deployer	deployer	deployer	deployer
Application	**utilisateur**	**gestionnaire**	**enseignant**	**responsable**	**admin**	**referent**	**lecteur**
portailEtudiant	deployer	deployer	deployer	deployer	10	deployer	deployer
PStage	593	293	307	deployer	deployer	25	deployer
recrutement des vacataires d'enseignement	443	deployer	deployer	deployer	deployer	deployer	deployer
recrutement-vacataire-enseignement	386	116	deployer	deployer	deployer	deployer	deployer
RefIMAG	994	0	deployer	deployer	deployer	deployer	deployer
ressourcesNumeriquesPourESPE	2628	deployer	deployer	deployer	deployer	deployer	deployer
ressourcesNumeriquesSHS	29385	deployer	deployer	deployer	deployer	deployer	deployer
ressourcesNumeriquesSTMGAEL	50814	deployer	deployer	deployer	deployer	deployer	deployer
rvn	350	6	deployer	deployer	deployer	deployer	deployer
SIFAC	604	deployer	deployer	deployer	deployer	deployer	deployer

Figure 7 – Vue synthétique des applications dont les droits sont pilotés par Biper et des rôles applicatifs déployés (liste non exhaustive)

4 Les réorganisations : les plus transparentes possibles

L'IDM est donc le passage obligé pour les comptes informatiques des personnes et leurs droits dans le SI. Toute évolution de l'organisation de l'établissement doit par conséquent être gérée dans l'IDM pour permettre la continuité des droits, ou mettre en place un tuilage si nécessaire.

Ainsi lors de la mise en place de l'établissement public expérimental UGA le 1/1/20, l'UGA a intégré la ComUE du site grenoblois, et a connu une importante réorganisation interne. De nombreuses personnes ont changé d'affectation, de lieu de travail... Les outils proposés par l'IDM ont permis d'assurer les tuilages, de progressivement ouvrir les nouveaux droits et fermer les anciens... de façon transparente pour nos collègues.

5 La qualité des données sources peut virer au cauchemar… ou pas !

La qualité des données de l'IDM, et donc des droits numériques calculés automatiquement, dépend fortement de la qualité des données présentes dans les sources qui l'alimentent : logiciels de gestion de scolarité, RH… Toute erreur dans une base source est répercutée dans l'IDM. C'est le fameux « garbage in, garbage out »[2] ! En temps normal, ces erreurs sont marginales et vite corrigées. Mais on rentre en phase de risque en cas de changement d'outil de gestion pour peu que les données soient mal reprises !

Suivant la façon dont les choses se passent avec la nouvelle base de gestion, le changement sera transparent pour l'IDM (cas de Pegase), ou virera au cauchemar (cas de Siham)...

En utilisant Biper comme référentiel central pour les informations permettant la gestion des accès, on en fait un élément tampon qui amortit les évolutions du SI en amont des annuaires. Si une source importante (comme le SI RH par exemple) n'est plus assez fiable, il convient de prendre des mesures pour garantir la continuité des accès existants et déployer ceux pour les nouveaux arrivants : alimentation partielle par le SI RH sur les données fiables, complément par une saisie directe dans l'IDM, prolongation exceptionnelle des accès…

6 Le confinement : ouvrir simplement de nouveaux services (et déléguer tout de suite la gestion des accès)

Après ces différentes étapes, nous avions tous les outils de pilotage du SI pour que la bascule brutale en distanciel lors du confinement de mars 2020 se fasse quasi instantanément ! Ainsi, en quelques jours, l'outil de tchat a été ouvert à l'ensemble des personnels UGA, avec possibilité de gérer en proximité les accès aux différents canaux de discussion, par service et/ou projet. Même chose pour les outils de visio.

7 Conséquences, limites, impacts sur l'organisation

7.1 On ne voit que ce qu'on pilote

Il est très facile de générer des LDAP, AD... avec un IDM. Mais l'IDM ne sait rien du mode d'utilisation des données par les applications branchées sur ces annuaires.

La cartographie des applications utilisant les annuaires en aval de l'IDM est vitale pour déterminer ce que l'IDM doit continuer à générer lors d'évolutions.

7.2 On peut aller finement dans la description du pilotage des accès des ressources

Par exemple, l'UGA a choisi de gérer tous les répertoires partagés de son AD avec Biper (avec 3 rôles applicatifs par répertoire, lecteur/auteur/gestionnaire). Ces rôles sont attribués selon l'appartenance à une composante, service, équipe, ou individuellement. Les gestionnaires d'un répertoire déterminent via Biper les lecteurs et auteurs. Ces droits sont répercutés immédiatement dans l'AD via un courtier de messages (AMQP – rabbitMQ).

2 Garbage in, garbage out : déchet en entrée, déchet en sortie.

7.3 Il faut déléguer la gestion des accès et faire des revues des droits

Autant les services informatiques peuvent accompagner les fonctionnels pour définir des règles d'accès aux services numériques, autant pour gérer des cas particuliers, nominatifs, on s'aperçoit qu'ils ne sont pas bien placés pour paramétrer qui a accès à quoi. Il faut identifier dans son organisation quelles sont les personnes à même d'être responsables des accès (ou des informations qui seront transformées en accès). Ce qui n'est pas toujours facile.

Sans compter que l'expérience montre que si la délégation aux services et composantes de proximité fonctionne très bien pour ouvrir des droits, leur suppression n'est pas aussi rigoureuse, ce qui peut poser des problèmes de sécurité du SI !

Si le cycle de vie d'un compte (en fonction de ses rôles) assure de couper les accès aux personnes parties, il n'en va pas de même pour la gestion des accès à des applications lors du changement d'affectation en interne.

Un mécanisme de confirmation des habilitations est nécessaire pour relancer les gestionnaires.

7.4 Ça ne marche pas tout seul

L'IDM s'insère dans une organisation globale, il demande un paramétrage important. Plus on le lie à l'organisation de l'établissement, plus il faut l'adapter lors des réorganisations (et souvent les anticiper). Plus on veut automatiser des cas particuliers, plus on a de paramétrage ou de scripts à maintenir. L'équipe qui gère l'IDM doit donc parfaitement comprendre l'organisation de l'établissement et son SI.

Biper est un outil maison, développé spécifiquement pour nos établissements afin de gérer notre complexité et nos spécificités. Il répond donc très finement aux besoins, mais implique d'avoir des compétences en développement en interne pour faire face aux évolutions des besoins.

Quand tout est en place, on gagne un temps considérable.

7.5 La mise en œuvre demande du temps

Vouloir tout brancher sur l'IDM dès le départ semble illusoire. Ajouter de nouveaux services pilotés par l'IDM est plus facile que changer la gestion des accès à un service existant. Il faut donc y aller progressivement. Un point clé est le pilotage (à 100% de préférence) d'annuaires par l'IDM.

8 Conclusion

Avec un IDM au centre du SI (Figure 8), vous êtes parés pour faire face à tout, même l'improbable !

... à condition de vous en occuper.

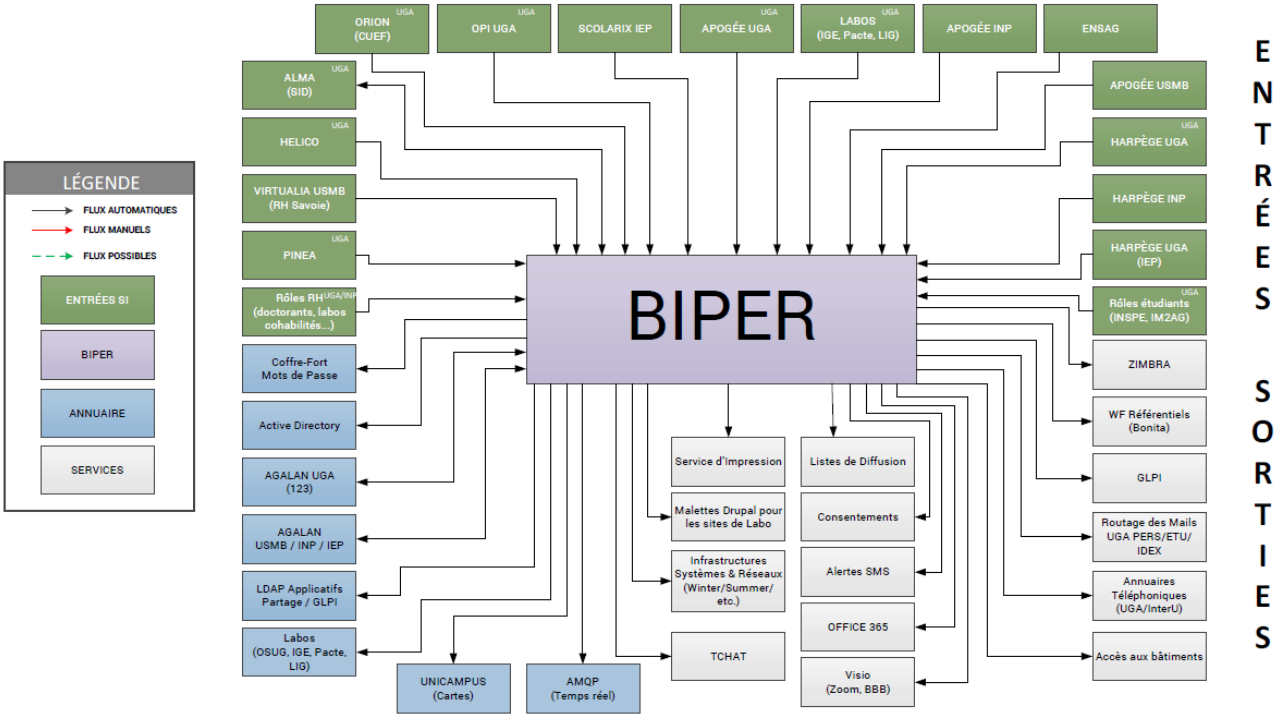

Figure 8 – L'IDM au centre du SI