# Sésame 2 : vers une gestion d'identités moderne

**Pascal Aubry, Henri Jacob & Saâd Aït Omar**
Université de Rennes 1 – Direction du Système d'Information

## Résumé

*L'université de Rennes 1 a mis en œuvre à la fin des années 1990 le système « Sésame » : une gestion d'identité mutualisée (entre l'université et deux écoles) qui ne cache plus le poids de son âge. Plusieurs générations du système se sont succédé pour s'adapter à l'évolution de l'université et de ses usages.*

*Les limites du système Sésame sont apparues au fil des années : les nouvelles exigences des services, de nouveaux enjeux de sécurité, l'impératif de limiter les tâches d'administration incombant à la DSI, l'apparition des services en* cloud *et de nouveaux supports de type* smartphone*, ainsi que la plus grande maturité des utilisateurs d'internet ont aujourd'hui rendu le système Sésame obsolète.*

*La modernisation de la gestion des identités est aujourd'hui un enjeu majeur pour notre établissement ; consciente de cette fragilité, la DSI de l'université a lancé en 2012 la refonte complète du système « Sésame ». Cette présentation décrit les lacunes de l'actuel système Sésame sur les plans fonctionnel et technique ; on montrera ensuite comment le système Sésame 2 comblera ces lacunes grâce notamment à :*

- *la prise en compte des fournisseurs d'identité externes à l'établissement ;*
- *la délégation « au plus près » des procédures d'administration ;*
- *l'utilisation d'une authentification forte ;*
- *une plus grande maîtrise des processus métier et des technologies.*

## Mots-clefs

*Gestion d'identités, authentification forte, Grouper, Active directory, OpenLDAP, OpenIDM*

## Êtes-vous concerné(e) par cet article ?

Pour savoir si vous êtes concerné(e) par cet article, il vous suffit de répondre à ces simples questions :

- la création de tout ou partie des comptes de vos utilisateurs est-elle effectuée par votre service informatique ?
- lorsqu'un utilisateur a besoin d'accéder à une application, lui est-il également automatiquement attribué un répertoire d'accueil et une adresse électronique ?
- l'accès aux applications sensibles est-il protégé par une authentification de type SSO ?
- lorsqu'un utilisateur change de statut ou quitte l'établissement, une intervention manuelle est-elle nécessaire pour supprimer tous les droits associés à son identifiant ?
- le même mot de passe est-il utilisé pour se connecter au réseau et pour la messagerie ?

Si vous avez répondu oui à au moins une de ces questions, alors vous serez peut-être intéressé(e) par cet article.

## 1 Les limites du système Sésame actuel

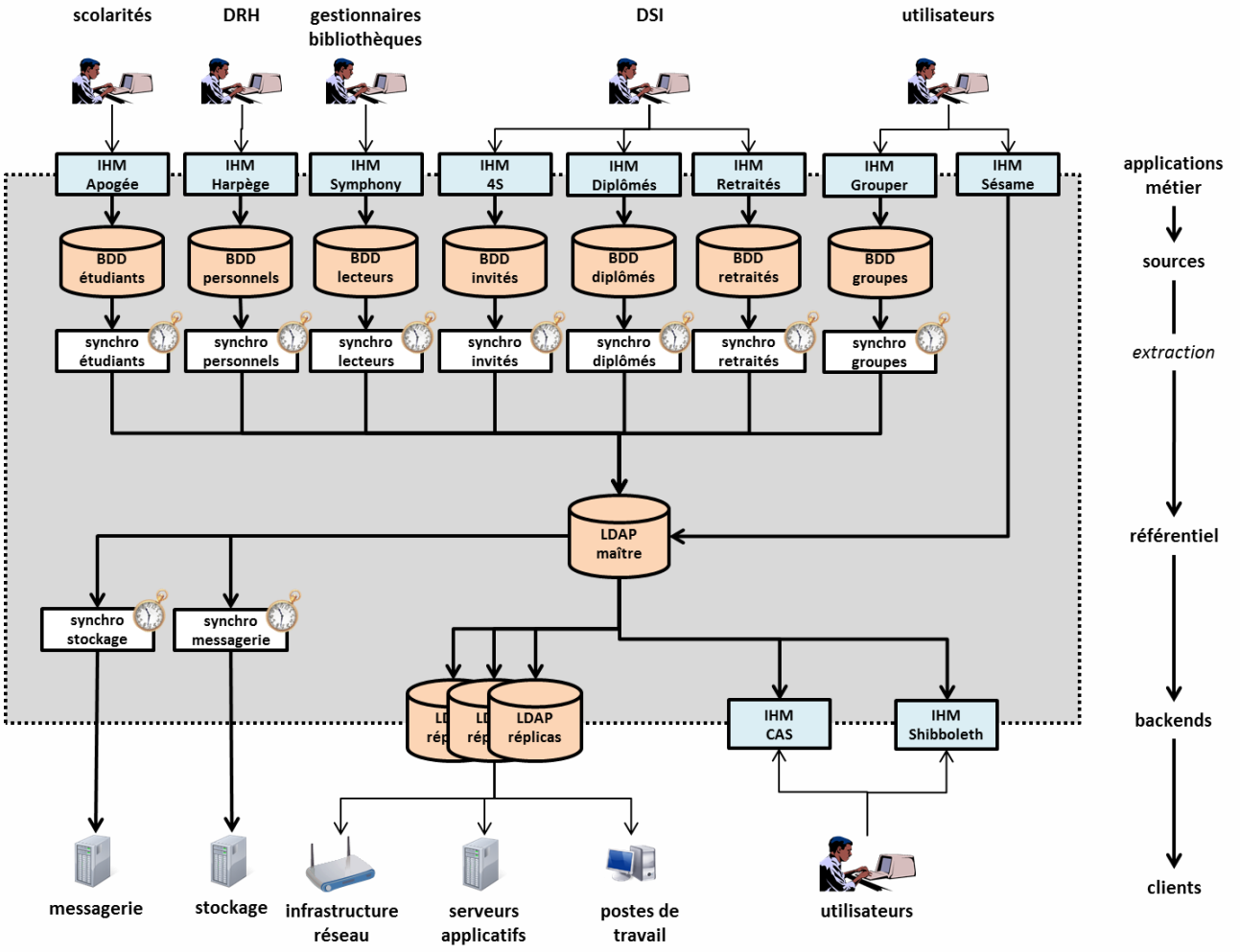
La gestion des identités et des autorisations peut être définie comme l'ensemble des processus qui permettent :

- d'allouer un identifiant à chaque utilisateur des services du Système d'Information ;
- d'offrir un service d'authentification permettant de sécuriser l'emploi de cet identificateur ;
- d'y associer des droits et privilèges dans les différents services du Système d'Information ;
- de supprimer les droits et privilèges des utilisateurs lorsque leur statut est modifié dans le Système d'Information (*deprovisioning*).

Le système de gestion d'identités de l'université de Rennes 1, baptisé Sésame, a été développé à la fin des années 1990. L'étude objective du système conduit inévitablement à un constat sans appel :

- fonctionnellement, Sésame remplit mal les besoins, et a un coût de gestion pour la DSI sans aucun rapport avec ses moyens ;
- sur le plan de la sécurité, de nombreuses lacunes entrent en conflit avec des mesures de PSSI élémentaires et empêchent leur mise en application ;
- sur le plan technique enfin, les coûts d'évolution sont trop élevés pour ne pas envisager une refonte radicale de l'existant.

## 1.1 Un système fonctionnellement dépassé




### 1.1.1 De nouvelles populations

Jadis réservé aux étudiants et personnels, le Système d'Information des établissements s'est ouvert vers de nombreuses autres populations : anciens étudiants (diplômés), retraités, utilisateurs des bibliothèques, … Les Systèmes d'Information des universités, celui de Rennes 1 en particulier, n'ont souvent suivi cette évolution qu'en adoptant des régimes d'exception pour les nouvelles populations.

Si la coopération avec des intervenants extérieurs, du monde académique, est parfois facilitée par l'utilisation de la Fédération d'Identités, cet outil est malgré tout limité aux populations d'établissements membres de la fédération et aux applications web. A l'international la mise en œuvre effective de la fédération de fédération *eduGAIN* est un autre frein. Ces contraintes sont contournées en enregistrant des utilisateurs extérieurs dans notre SI, mais aussi par l'utilisation « sauvage » des outils du *cloud* par les utilisateurs.

### 1.1.2 De nouveaux usages

De nouveaux usages sont apparus chez les utilisateurs, dont la maturité informatique a considérablement augmenté ces dernières années. La notion d'identité informatique a également considérablement évolué, notamment sous la forte poussée des réseaux sociaux. La possession d'un compte informatique et d'une adresse électronique institutionnelle, longtemps considérée comme une justification tangible de l'identité, ne fait plus référence : l'ouverture des Systèmes d'Information vers les prestataires d'identités extérieurs peut apporter un gain fonctionnel pour les utilisateurs sans pour autant dégrader la sécurité des systèmes.

### 1.1.3 Une décentralisation nécessaire

Le système Sésame actuel est essentiellement centralisé : si les bases institutionnelles (*Harpège*, *Apogée*, *Symphony*) sont effectivement gérées par les fonctionnels (personnels administratifs), toutes les procédures « à la marge » ajoutées pour traiter les exceptions (comptes étudiants banalisés pour les formations ponctuelles, comptes fonctionnels des composantes, comptes spécifiques à la recherche, …) sont traitées par les personnels de la DSI. L'impératif de limiter les charges de fonctionnement de la DSI ne peut se concevoir sans une délégation des tâches d'administration des identités, par des utilisateurs formés et responsables (responsables administratifs, responsables des formations, …).

## 1.2 Une tradition orale dans la transmission des processus métier

Il ne s'agit pas là d'un problème d'outils, les processus métier de gestion des utilisateurs manquent cruellement de formalisation : certaines règles (comme par exemple : « tout personnel présent plus de trois jours dans l'établissement doit être enregistré dans Harpège ») relèvent uniquement de la « tradition orale » : beaucoup de personnes connaissent et appliquent des règles dont on ne trouve nulle trace ni dans les relevés de décisions des instances de l'université ni dans les documentations de la DSI.

Compte tenu du *turn-over* observé dans les établissements, la formalisation des processus métier est une condition *sine qua non* d'une bonne gestion des utilisateurs. Si selon Amadou Hampate Bâ « *quand un vieillard meurt c'est une bibliothèque qui brûle* », nous avons personnellement observé que sans formalisation des processus et des règles métier, « *quand un ingénieur de la DSI part en retraite, il arrive qu'on ne sache plus pourquoi telle ou telle pratique est opposée aux utilisateurs comme une règle de sécurité*».

## 1.3 Un système à la sécurité approximative

### 1.3.1 De multiples services

Les services offerts aux utilisateurs se cantonnaient à une palette simple, essentiellement constituée de ressources : stockage, messagerie électronique, connexion aux postes de travail. Aujourd'hui, les ressources sont multiples et variées, notamment à travers les Environnements Numériques de Travail, et l'attribution d'accès aux services souvent directement reliée à l'attribution d'un compte dans le Système d'Information. Ce manque de souplesse dans l'allocation des privilèges a des conséquences non négligeables sur la sécurité des systèmes.

### 1.3.2 Une authentification pratique mais faible

Justifié par le confort d'utilisation des systèmes de *Single Sign-On* (*SSO*), l'utilisation d'un compte unique – et donc d'un mot de passe unique – a constitué un progrès indéniable en matière d'ergonomie du Système d'Information ; en revanche, son bilan dans le domaine de la sécurité est plus mitigé. Certes, il a permis de réduire de manière drastique les *post-it* « pense-bête » sur les écrans de nos utilisateurs. Grace à son architecture centralisée, il permet à moindre frais une mise en œuvre universelle de certaines mesures de sécurité (bloquer un compte, forcer le changement d'un mot de passe, ...). Cependant, les conséquences d'une compromission sont maintenant beaucoup plus graves. Cette « Authentification Unique et Unifiée » a en outre atteint ses limites pour l'authentification auprès de certains services sensibles.

### 1.3.3 Un *deprovisioning* déficient

Si l'allocation des privilèges est fidèle aux besoins (par nécessité), la suppression de ces mêmes privilèges lors des changements de statut des utilisateurs est souvent délaissée : ce manque de *deprovisioning* peut avoir des conséquences graves sur la sécurité.

### 1.3.4 Une imputabilité limitée

Une obligation faite aux établissements en tant que fournisseur d'accès internet est de pouvoir imputer toute action sur le réseau à une personne physique, par exemple en cas de réquisition judiciaire. L'utilisation à outrance des comptes banalisés pour contourner les insuffisances du système entraine une vraie difficulté à imputer les actions, par manque de traçabilité sur ces comptes.

## 1.4 Un système techniquement peu maîtrisé

De trop nombreuses technologies différentes mises en œuvre lors des évolutions successives des synchronisations depuis les bases métier rendent les évolutions et la maintenance du système très difficile et coûteuse. On notera en particulier la faible isolation entre les règles métier et le processus de transformation des données, qui induit une forte adhérence entre les différentes briques logicielles du système.

Le manque de maîtrise de la solution en place, par manque de temps et par perte de compétences, est un point de faiblesse important dans le Système d'Information. Cette faiblesse ne peut être diminuée que par une uniformisation des outils de synchronisation des bases de données et l'adoption de *frameworks* de plus haut niveau.

## 1.5 Une architecture obsolète

### 1.5.1 Une séparation insuffisante de la notion d'authentification et de celle d'autorisation

Le système Sésame actuel gère les identités : les autorisations d'accès aux ressources de l'établissement sont gérées soit au niveau des ressources elles-mêmes (par un mécanisme propre ou par appui sur les profils LDAP), soit au niveau de Grouper (par l'appartenance ou non à des groupes).

Dans les deux cas, l'allocation des droits d'accès aux services n'est pas décidée par la personne qui gère le compte au niveau du gestionnaire d'identités, ce qui rend la délégation non généralisable (trop coûteuse car elle doit être faite au niveau de chaque service).

### 1.5.2 Des lacunes fonctionnelles

Sur le plan fonctionnel, le système Sésame manque cruellement de délégation : la DSI effectue des tâches qui seraient normalement du ressort des fonctionnels de l'établissement. De même, le système de recouvrement du mot de passe en cas de perte de celui-ci par l'intéressé, ne peut en pratique se faire en totale autonomie. Ce défaut important conduit à de nombreux tickets d'assistance.

Il s'agit là de l'héritage d'un passé dans lequel les comptes informatiques étaient gérés par les informaticiens, et qui sera corrigé dans le système Sésame 2.

### 1.5.3 Un énorme manque de réactivité

On reproche également au système actuel la durée de propagation des modifications dans les bases institutionnelles : il faut parfois plusieurs heures pour que les utilisateurs aient accès à leurs ressources après leur enregistrement. Cela est dû au mécanisme de synchronisations mis en place, dont la fréquence est limitée par leur durée.

# 2 Objectifs du système Sésame 2

## 2.1 Prise en charge des « identités externes »

Parmi les améliorations attendues par le nouveau système de gestion des identités, on notera en particulier la souplesse fonctionnelle, grâce à la prise en compte des fournisseurs d'identités externes à l'université.

Des comptes pourront être créés par les utilisateurs eux-mêmes, en lien avec une identité externe au Système d'Information de l'établissement, fournie par un prestataire externe (un numéro de téléphone, une adresse électronique, un identifiant *Facebook*, *Twitter*, *LinkedIn*, *OpenID*, …). Cette ouverture vers des systèmes d'authentification externes devra permettre entre autre d'ouvrir nos outils à des coopérations avec des personnes externes. Elle n'est possible qu'en séparant fortement authentification et autorisation. Par défaut, ces comptes externes n'auront aucun privilège, ni accès à

aucun service ; l'accès aux services et aux ressources de l'établissement ne sera accordé qu'ensuite par les acteurs fonctionnels de l'établissement, suivant des modalités à définir.

Une formalisation des processus métier devrait conduire, malgré le fait que l'on s'appuie sur des fournisseurs d'identités externes, à une meilleure imputabilité des actions des utilisateurs sur le réseau. On distingue pour cela deux niveaux de vérification des identités externes :

- la vérification de l'identité, qui assure simplement l'existence de l'identifiant ; pour une adresse électronique par exemple, la vérification est classiquement effectuée en envoyant à l'adresse un jeton connu du système seul, et la réception du jeton en retour assure l'existence de la boite à lettres correspondante ;
- la vérification de la personne, qui assure l'existence de l'identifiant et l'appartenance de cet identifiant à une personne physique (par le contrôle d'une pièce d'identité en face-à-face, l'envoi d'un secret par voie postale à l'adresse du destinataire, ou tout autre mécanisme estimé assurer de l'identité réelle de la personne).

## 2.2 Délégation « au plus près » des procédures d'administration

Cette prise en compte des identités externes, ainsi que l'association entre identités externes et comptes du Système d'Information, ne peuvent se concevoir sans une remise à plat complète des processus métiers de l'établissement, en coopération avec les acteurs fonctionnels (scolarités et responsables des formations pour les étudiants, responsables administratifs pour les personnels).

La rigidité du système Sésame avait conduit les acteurs fonctionnels à contourner les règles métier pour permettre les usages attendus, de manière très régulière. La prise en charge des fournisseurs d'identités externes permettra d'atteindre un triple objectif :

- l'amélioration des processus métiers au niveau de l'enregistrement des utilisateurs ;
- la délégation des tâches administratives aux acteurs fonctionnels, au plus près des utilisateurs finaux ;
- la diminution de la charge de la DSI sur des tâches qui ne relèvent pas de son cœur de métier.

## 2.3 Authentification forte

L'accès à de nombreux services est sensible : l'usurpation d'identité peut avoir des conséquences non négligeables sur les plans financier (mauvaise utilisation des applications budgétaires par exemple) et juridique (recours des étudiants pouvant conduire à des réparations financières à la charge de l'université).

Dans ce cadre, la brique SSO CAS, utilisée depuis dix ans à l'université, est devenue un point faible de notre SSI. Son évolution vers une authentification unique à plusieurs niveaux d'assurance est devenue indispensable[1].

En particulier, l'authentification forte (certificat, OTP, double facteur, …) nous permettra une mise en conformité avec les exigences réglementaires en vigueur.

## 2.4 Maîtrise des processus métier

La maîtrise des processus métier, en particulier le *deprovisioning* qui permet de lier l'utilisation des ressources au statut des utilisateurs, est une condition *sine qua non* de la sécurité du système.

Sur le plan des outils, l'utilisation systématique (dès que possible) de Grouper pour la gestion des autorisations permet d'assurer un *deprovisioning* automatique, car les groupes Grouper sont reconstruits de manière régulière, reflétant automatiquement les changements de statut des utilisateurs dans les bases institutionnelles. Une fonction de recherche dans Grouper permettra d'assurer ce *deprovisioning*.

L'adoption d'outils adéquats n'est pas suffisante : la sensibilisation des acteurs fonctionnels de l'université à la sécurité et le contrôle continu de la qualité des données du Système d'Information font partie intégrale du projet.

[1] Délibération de la CNIL n° 2006-104 du 27 avril 2006 sur les ENT.

## 2.5 Maîtrise technologique

La sécurité du système ne peut enfin s'entendre sans une bonne maîtrise technologique de l'ensemble du système. L'actuel annuaire LDAP, pivot du système « Sésame », ne sera plus qu'un des multiples annuaires (authentification, autorisations, téléphonie, messagerie, ...), tous dérivés d'un référentiel global alimenté par les bases métiers.

La simplicité de la maintenance du système, son évolutivité et sa pérennité devront être garanties par l'utilisation uniforme de standards et de technologies ouvertes.

## 2.6 Évolutivité et ouverture

L'évolutivité du système est le critère fondamental dans le choix des outils et technologies qui seront adoptées pour la réalisation : ce projet est en effet mené dans le contexte de la fusion des universités Rennaises, et les systèmes de gestion d'identités des deux universités devront à terme être fusionnés. Le système Sésame 2 devra donc être assez ouvert pour accueillir des identités d'un autre établissement ou produire les informations sous un format permettant son intégration dans un autre système déjà existant.

Notons que la nature multi-établissements n'est pas une contrainte supplémentaire du projet : le système Sésame héberge déjà les identités de trois établissements (l'université de Rennes 1, l'École Nationale Supérieure de Chimie de Rennes et l'Institut d'Études Politiques de Rennes).

# 3 Description du système Sésame 2

## 3.1 Exemples de scenarii d'utilisation

### 3.1.1 Allocation d'un accès wifi externe à un participant d'un congrès

Il s'agit ici, pour l'organisateur d'un congrès, d'autoriser une liste de personnes extérieures à l'université (les participants du congrès) à accéder pendant une période donnée (le temps du congrès) au wifi de l'établissement.

Dans le système Sésame, il n'était pas possible d'allouer un identifiant n'ayant comme seul service accessible l'accès wifi (sauf en passant par une technologie de portail captif dont la conservation n'est pas un objectif de la DSI).

Dans le système Sésame 2 :

1. l'organisateur du congrès demande à la DSI l'autorisation d'allouer des comptes pour l'accès wifi.
2. la DSI, après vérification de la qualité d'organisateur du demandeur, lui délègue la création des comptes en lui indiquant la procédure à suivre (un lien vers une interface web).
3. en accédant à l'interface web de Sésame 2, l'organisateur peut créer des comptes correspondant aux adresses électroniques des participants et leur allouer l'accès au réseau wifi pour la durée du congrès :
    a. les adresses électroniques, issues de la base de données de l'organisation, sont vérifiées par un secret envoyé aux participants ;
    b. l'identité des participants est considérée comme vérifiée par le paiement préalable des droits d'inscription au congrès.

### 3.1.2 Création d'un boite à lettres de fonction pour le secrétariat d'une composante de l'université

On souhaite ici créer un compte informatique qui servira à relever le courrier électronique d'une boite de fonction ; on ne souhaite pas pour autant, comme c'est le cas dans le système Sésame actuel, que le compte permette la connexion au réseau (encore moins posséder un répertoire d'accueil).

Dans le système Sésame 2, le responsable administratif de la composante, autorisé par son statut, crée un compte informatique rattaché à sa composante, et n'ayant pour seul service accessible la messagerie électronique.

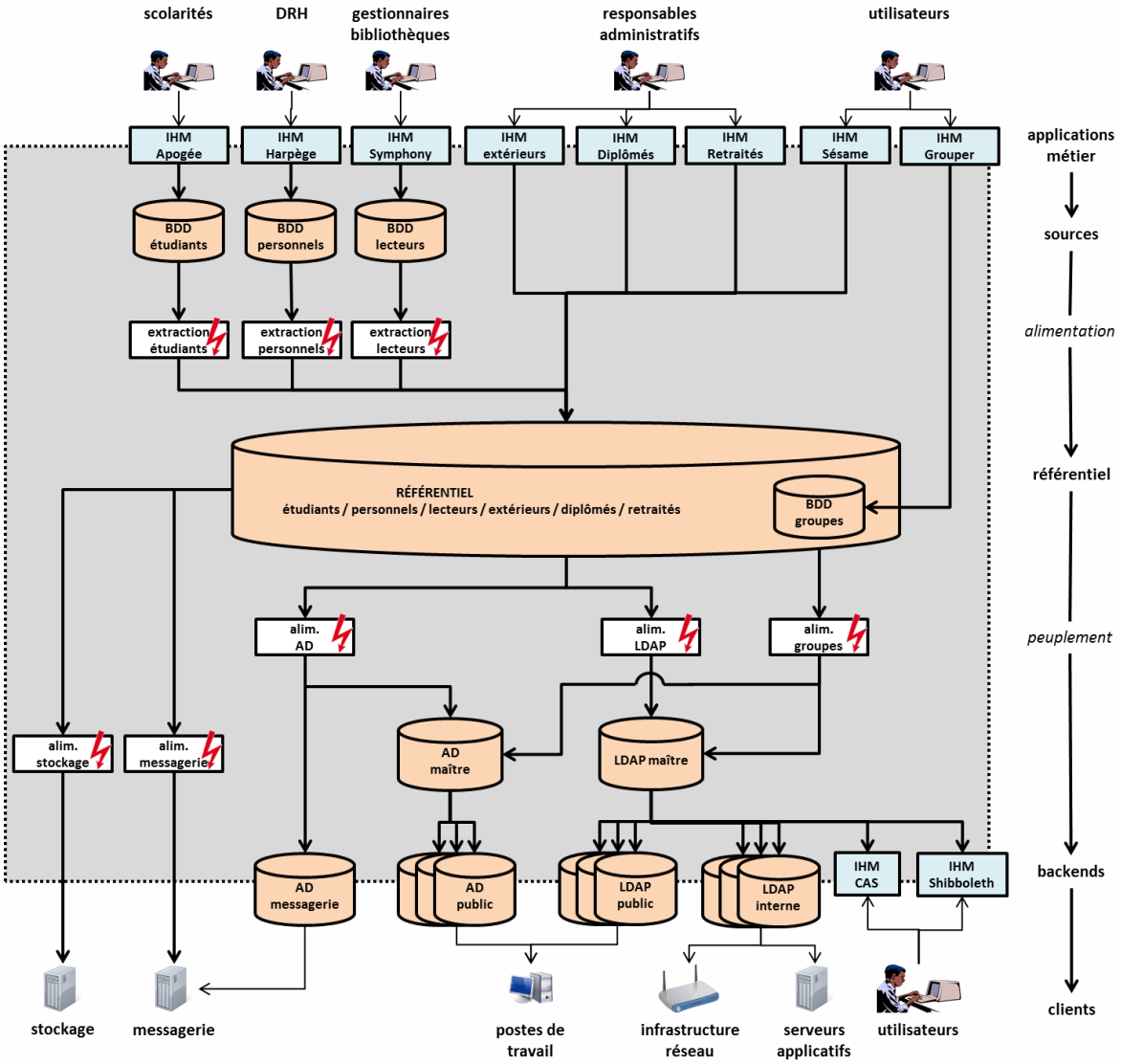
### 3.1.3 Gestion d'un site web à distance par un prestataire

On souhaite ici disposer d'un compte informatique permettant la mise à jour à distance de fichiers sur un site web par un prestataire extérieur à l'université. Dans le système Sésame 2, on allouera donc à ce compte :

- un espace de stockage pour l'application à maintenir à distance ;
- l'accès au service de mise à jour de l'espace de stockage grâce à une connexion FTP sécurisée ;
- une adresse électronique sans boite à lettres correspondante (l'adresse sera redirigée vers une autre adresse électronique).

Notons que dans ce cas ce sera un personnel de la DSI qui créera ce compte, pour le compte de son propre service.

## 3.2 Architecture fonctionnelle




Notons que dans cette nouvelle architecture, la DSI aura complètement délégué la gestion des utilisateurs.

## 3.3 Choix techniques

Deux pistes ont été explorées pour la mise en œuvre :

- l'utilisation (ou l'assemblage) de briques existantes : l'ETL *Talend* pour les opérations de *provisionning*, *ActiveMQ* pour le séquencement des opérations, *Grouper* pour les autorisations et un développement interne (*Java*) pour l'interface utilisateur ;
- l'utilisation d'un *framework* spécialisé pour l'orchestration globale de toutes les opérations de gestion des identités et *Grouper* pour la gestion des autorisations.

Excellent dans les opérations de *provisionning*, *TOS* (*Talend Open Studio*) s'est finalement révélé limité dans l'orchestration des opérations de transformation et propagation des données dans le système. L'adoption de la version payante de *Talend* (*TIS*, *Talend Integration Suite*) eut peut-être ouvert d'autres possibilités, mais des contraintes budgétaires ne l'ont pas permis. Dans tous les cas, le caractère généraliste de *Talend* aurait sans doute montré d'autres limites et nécessité des développements supplémentaires (audit, workflow, gestion des mots de passe, …).

Les regards se sont alors tournés vers des *frameworks* de développement dédiés à la gestion d'identités, avec une préférence pour les solutions libres (contraintes budgétaires et maîtrise technologique). Les trois solutions évaluées (*Apache Syncope*, *midPoint* et *openIDM*) sont relativement récentes mais sont utilisables en production. Les solutions *Apache Syncope* et *midPoint* ont été jugées plus appropriées à un environnement d'entreprise assez simple. La préférence a été donnée à *openIDM*, un *framework Java* modulaire et spécialisé dans la gestion d'identités.

## 3.4 Le processus de migration

Les dernières inconnues de ce projet concernent essentiellement le processus de migration du système actuel Sésame vers le futur système Sésame 2.

La difficulté d'élaboration d'un scenario de migration tient essentiellement à l'obligation de continuité des services opérés par la DSI. De ce fait, il apparaît comme une évidence impossible de migrer l'ensemble du système en une fois ; il faudra donc gérer, sur une période transitoire dont il est souhaitable qu'elle soit la plus courte possible, la coexistence de deux systèmes.

La date de recette prévue du projet est fin 2014.

*Remerciements à Serge Aumont pour avoir poussé les auteurs à sortir le nez du guidon et faire profiter la communauté de leurs doutes :-) et à Claude Gross pour sa patience…*