Gestion des identités et des accès pour le système d'information du CNRS

Guillaume Harry

le cnam

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Centre d'enseignement de PARIS

MEMOIRE

présenté en vue d'obtenir

le DIPLOME D'INGENIEUR CNAM

SPECIALITE : Informatique

OPTION : Systèmes d'information

par

Guillaume HARRY

Gestion des identités et des accès pour le système d'information du CNRS

Soutenu le 19 juin 2013

JURY

PRESIDENT : Mme Isabelle WATTIAU Professeur

MEMBRES :	**M. Jacky AKOKA**	**Professeur**
	M. Yves LALOUM	**Professeur**
	M. Olivier PORTE	**Ingénieur de recherche**
	M. Jacques BERLIOZ	**Ingénieur de recherche**

Remerciements

Je remercie et exprime ma gratitude la plus profonde à mon responsable, **Monsieur Olivier PORTE**, pour son soutien, son écoute, ses précieux conseils et l'expérience dont il a su me faire profiter.

J'adresse également un remerciement spécial à **Monsieur Marc DEXET** pour son aide tout au long de ce projet. Je n'oublierai pas toutes nos discussions nocturnes tardives.

Je remercie **Monsieur Jacques BERLIOZ** pour sa participation.

Mes remerciements s'adressent également au service de la formation permanente qui m'a offert les moyens de suivre le cursus de formation au CNAM.

Je tiens à remercier **Monsieur Jacky AKOKA** qui a m'a accompagné dans cette étude et supervisé mon travail.

Je remercie les membres du jury, **Madame Isabelle WATTIAU** et **Monsieur Yves LALOUM**, pour le temps passé sur ce mémoire.

Je remercie également **Madame Edwige BONBARON**. Son suivi régulier et son journal de bord m'ont permis de prendre du recul sur le travail réalisé.

Ce projet n'aurait pas été possible sans le soutien permanent de ma famille. Je dédie ce mémoire à ma compagne et à mes deux enfants.

Liste des abréviations

- AC : **A**utorité de **C**ertification
- ACL : **A**ccess **C**ontrol **L**ist (anglais)
  Liste de contrôle des accès (français)
- AD : Microsoft **A**ctive **D**irectory
- AE : **A**utorité d'**E**nregistrement
- API : **A**pplication **P**rogramming **I**nterface (anglais)
  Interface de programmation (français)
- ARESU : **A**rchitecture **R**éseau **E**xpertise et **S**upport aux **U**nités
- BPM : **B**usiness **P**rocess **M**anagement (anglais)
  Gestion de processus métier (français)
- BRR : **B**usiness **R**eadiness **R**ating (anglais)
  Taux d'adéquation au métier (français)
- CIL : **C**orrespondant **I**nformatique et **L**ibertés
- CMMI : **C**apability **M**aturity **M**odel **I**ntegration
- CNIL : **C**ommission **N**ationale **I**nformatique et **L**ibertés
- CNRS : **C**entre **N**ational de la **R**echerche **S**cientifique
- CORE : **CO**mmunauté pour la **RE**cherche (français)
  COmmunity for **Re**search (anglais)
- CRBAC : **C**onstrained **R**ole **B**ased **A**ccess **C**ontrol (anglais)
  Contrôle d'accès base sur les rôles avec contraintes (français)
- CRBF : **C**omité de **R**églementation **B**ancaire et **F**inancière
- CRU : **C**ompte **R**éseau **U**niversel
- DAC : **D**iscretionary **A**ccess **C**ontrol (anglais)
  Contrôle d'accès discrétionnaires (français)
- DGDR : **D**irection **G**énérale **D**éléguée aux **R**essources
- DGDS : **D**irection **G**énérale **D**éléguée à la **S**cience
- DMAS : **D**irectory **M**anagement & **A**dministration **S**ystem (anglais)

Système de gestion et d'administration d'annuaire (français)

- DR : **D**élégation **R**égionale
- DSI : **D**irection des **S**ystèmes d'**I**nformation
- DU : **D**irecteur d'**U**nité
- EAI : **E**nterprise **A**pplication **I**ntegration (anglais)
  Intégration d'applications d'entreprise (français)
- EPST : **E**tablissement **P**ublic à **C**aractère **S**cientifique et **T**echnique
- ESB : **E**nterprise **S**ervice **B**us (anglais)
  Bus de service d'entreprise (français)
- FLOSS : **F**ree/**L**ibre and **O**pen **S**ource **S**oftware (anglais)
  Logiciel libre et Open Source (français)
- GIP : **G**roupement d'**I**ntérêt **P**ublic
- HRBAC : **H**ierarchical **R**ole **B**ased **A**ccess **C**ontrol (anglais)
  Contrôle d'accès base sur les hiérarchies de rôles (français)
- IAM : **I**dentity & **A**ccess **M**anagement (anglais)
  Gestion des Identités et des Accès (français)
- IBAC : **I**dentity **B**ased **A**ccess **C**ontrol (anglais)
  Contrôle des accès basé sur l'identité (français)
- IdP : **Id**entity **P**rovider (anglais)
  Fournisseur d'identité (français)
- IEEE : **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
- IGC : **I**nfrastructure de **G**estion des **C**lés (français)
  Public **K**ey **I**nfrastructure (PKI) (anglais)
- INRIA : **I**nstitut **N**ational de **R**echerche en **I**nformatique et **A**utomatique
- ITA : **I**ngénieur, **T**echnicien ou **A**dministratif
- IUP : **I**dentifiant **U**nique **P**ersonnel
- JPA : **J**ava **P**ersistance **A**PI (anglais)
  Interface de persistance Java (français)

- MAC : **M**andatory **A**ccess **C**ontrol (anglais)
  Contrôle d'accès obligatoire (français)
- MCO : **M**aintien en **C**ondition **O**pérationnel
- MVC : **M**odèle **V**ue **C**ontrôleur (français)
  Model **V**iew **C**ontroler (anglais)
- NIST : **N**ational **I**nstitute of **S**tandards and **T**echnology
- ORM : **O**bject-**R**elational **M**apping (anglais)
  Correspondance objet-relationnel (français)
- PIE : **P**ôle **I**ngénierie et **E**xploitation
- PKI : **P**ublic **K**ey **I**nfrastructure (anglais)
  Infrastructure de **G**estion des **C**lés (IGC) (français)
- PSSI : **P**olitique de **S**écurité des **S**ystèmes d'**I**nformation
- RBAC : **R**ole **B**ased **A**ccess **C**ontrol (anglais)
  Contrôle d'accès base sur les rôles (français)
- Renater : **Ré**seau **Na**tional de télécommunications pour la **T**echnologie l'**E**nseignement et la **R**echerche
- RP : **R**elying **P**arty (anglais)
  Consommateur (français)
- RSI : **R**esponsable des **S**ystèmes d'**I**nformation en délégation régionale
- RSSI : **R**esponsable de la **S**écurité des **S**ystèmes d'**I**nformation
- SGBDR **S**ystème de **G**estion de **B**ases de **D**onnées **R**elationnelles
- SIRHUS **S**ystème d'**I**nformation des **R**essources **H**umaines des **U**nités et des **S**ervices
- SMSI **S**ystème de **M**anagement de la **S**écurité de l'**I**nformation
- SOAP **S**imple **O**bject **A**ccess **P**rotocol (anglais)
  Protocole d'accès pour des objets simples (français)
- SoD : **S**egregation **o**f **D**uty (anglais)
  Séparation des responsabilités (français)
- SOX : **S**arbanes-**Ox**ley

- SP : **S**ervice **P**rovider (anglais)
  Fournisseur de service (français)
- SSO : **S**ingle **S**ign-**O**n (anglais)
  Authentification unique (français)
- TCO : **T**otal **C**ost of **O**wnership (anglais)
  Coût total de possession (français)
- TWE : **T**rust**w**orthy **E**lements (anglais)
  Eléments de confiance (français)
- UMI : **U**nités **M**ixtes **I**nternationales
- UMR : **U**nité **M**ixte de **R**echerche
- UPR : **U**nité **P**ropre de **R**echerche
- WAYF : **W**here **A**re **Y**ou **F**rom (en)
- XUL : **X**ML **U**ser Interface **L**anguage (anglais)
  Langage XML d'interface utilisateur (français)

Glossaire

Table des matières

Introduction

Contexte des organisations virtuelles

La notion d'équipe virtuelle ou d'entreprise virtuelle est née dans les années 1990 pour décrire les nouvelles formes de management et d'échanges numériques inter-équipes ou inter-entreprises. L'organisation virtuelle est définie comme « une alliance temporaire d'organisations (institutions, industries, entreprises, …) indépendantes, connectées, géographiquement disséminées, incluant un haut niveau de confiance qui collaborent et partagent leurs ressources et compétences dans le but de répondre aux demandes des clients » [1]. Ce nouveau schéma d'organisation a pour objectif de mener à bien un projet et prend fin quand la phase de production commence. Ainsi, l'équipe formée de l'ensemble des personnes impliquées dans les différentes phases, incluant les membres des maitrises d'ouvrage, des maitrises d'œuvre et des fournisseurs, peut être définie comme une organisation virtuelle.

Comme pour tout projet, le succès réside sur une relation de confiance autour du partage des connaissances et des compétences. La communication est donc un facteur clé de réussite de ce type particulier d'organisation où les distances et la dématérialisation sont une difficulté. En effet, toutes les personnes participantes doivent avoir accès aux informations et outils mis en commun au moment opportun.

La flexibilité est une autre caractéristique des organisations virtuelles. En effet, leur nature dynamique est due à la participation ponctuelle des membres. Les participants rejoignent et quittent le projet en fonction des compétences requises dans les différentes phases. La complexité se situe pour les coordinateurs dans la fourniture rapide d'un accès aux moyens mis en commun et dans la révocation de ces autorisations aussitôt après leur départ. Les responsables doivent également s'assurer que le savoir-faire acquis ainsi que les réalisations soient préservés et partagés même après la fin de la collaboration.

Les technologies de l'information et de la communication mis en œuvre ont alors pour objectif de mettre en relation les membres de l'équipe virtuelle et les systèmes d'informations des organisations physiques d'origine impliquées dans le partenariat. La difficulté réside alors dans les différences au niveau des infrastructures et des politiques de sécurités implémentées par chacun des partenaires. Chacun d'entre eux doit s'interconnecter avec les autres et permettre le partage des

[1] M.R. Nami, A. Malekpour. Virtual Organizations : Trends and Models. Dans IFIP International Federation for Information Processing, Volume 288; *Intelligent Information Processing IV*; Zhongzhi Shi, E. Mercier-Laurent, D. Leake, p 190–199, 2008

ressources tout en préservant la sécurité de sa propre organisation [2]. Tous doivent offrir un moyen de communication assurant l'intégrité et la confidentialité des données. De même, ils doivent disposer d'un moyen de vérifier l'identité des personnes et des systèmes qui prennent part dans la collaboration.

Enjeux pour le CNRS

Les organismes de recherche tels que le Centre National de la Recherche Scientifique (CNRS) sont particulièrement confrontés aux problématiques des organisations virtuelles. En effet, cet établissement de recherche scientifique pluridisciplinaire a établi des collaborations avec plus de six cents partenaires. Le nombre d'unités du CNRS ayant conclu un accord représentait 90% du nombre total d'unités du CNRS en 2010 [3].

Par exemple, les unités mixtes de recherche (UMR) sont des entités administratives, créées généralement pour quatre ans, issues d'une association d'un ou plusieurs laboratoires de recherche avec le CNRS. Les interconnexions entre les systèmes d'information de gestion (personnels, budget, comptabilité, etc.) des différentes tutelles sont faibles. Dans ce contexte, la tâche d'administration des comptes applicatifs et des accès est double. En effet, chacun des utilisateurs possède au moins un compte pour l'utilisation des outils informatiques utilisés dans le cadre de leur recherche, mais également un ou plusieurs comptes auprès de leur établissement qui les emploie ainsi que des éventuels organismes qui financent leur unité.
Pour diminuer le nombre de comptes que les personnes ont à utiliser et ainsi en faciliter la gestion, le groupement d'intérêt public (GIP) du réseau national de télécommunications pour la technologie l'enseignement et la recherche (Renater) a déployé une solution permettant aux applications de réutiliser les moyens d'identification définis par les organismes de rattachement des utilisateurs. Grâce aux mécanismes de la fédération d'identité les utilisateurs doivent s'authentifier auprès de leur employeur. La fédération d'identité permet ainsi de mettre à disposition une plus grande diversité de ressources stratégiques.

En 2008, le CNRS a intégré la fédération d'identités « Éducation-Recherche » gérée par Renater, grâce au projet de gestion des identités et accès Janus. La première phase fut la mise en place d'un service de fournisseur d'identité auquel les applications peuvent déléguer la fonction d'authentification et d'un référentiel d'utilisateurs dédié contenant toutes les informations d'identification et d'authentification.

---

[2] J. Magiera, A. Pawlak. Security Frameworks for virtual organizations. Dans *Organizations: Systems and Practices*. Springer, pages 133-148, 2005

[3] A. Sigogneau, S. Landel. *2010, une année avec le CNRS, données chiffrées et indicateurs*. 33 pages, 2011

La mise en œuvre de ces nouveaux outils a permis, dans un premier temps, d'offrir au CNRS un mécanisme d'accès à l'application des dossiers annuels, puis dans un second temps, de fournir une méthode uniforme de connexion aux systèmes d'information de la Direction des systèmes d'Information (DSI).

Thème du mémoire

Le pôle « Architecture Réseaux, Expertise et Support aux Unités » (ARESU) de la DSI déploie un portail collaboratif pour le CNRS et ses partenaires. Il a pour objectif entre autres de sécuriser et faciliter le partage d'information, d'aider à la gestion des projets et des appels à projets et d'offrir un support aux communautés scientifiques, techniques et administratives. Cette plate-forme d'échange doit donc répondre aux besoins de confiance et de flexibilité, des différents membres d'un projet scientifique ou de gestion répartis dans des structures géographiquement éloignées. Pour cela, la DSI doit mettre en place un système de gestion du cycle de vie des comptes de tous les utilisateurs.

Les enjeux de sécurité et réactivité incitent à démarrer la seconde phase du projet Janus. Cette étape consiste à apporter des outils de gestion des identités numériques, de gestion des accès, de gestion des habilitations, des rôles et des profils pour les systèmes d'information de la DSI du CNRS, le tout intégrant des fonctionnalités d'audit et de traçabilité.

Le présent mémoire a pour objectif de détailler chacune des étapes du projet de gestion des identités et des accès pour les systèmes d'information du CNRS. Afin de comprendre les difficultés que rencontre le CNRS dans la gestion des identités et des accès, la première partie décrit sa structure et son fonctionnement spécifique issus de ses soixante-dix années d'activités et des changements stratégiques opérés ces dernières années. Ensuite, pour mieux comprendre les termes manipulés par les outils, chacun de ces aspects sera défini dans un premier temps avec les bonnes pratiques et modèles qui leur sont associés. Puis les besoins des projets sont recensés afin de déterminer les priorités à étudier dans le choix des outils. Enfin, un ou plusieurs développements de démonstrateur seront réalisés pour démontrer la capacité d'adaptation des solutions envisagées.

I Contexte

I.1 Centre National de la Recherche Scientifique

I.1.1 Historique

Denis Guthleben [4] relate qu'au début du XXème siècle la recherche scientifique était financée par la Caisse des Recherches Scientifiques qui fut créée en 1901. Conjointement, à partir de 1930, la Caisse Nationale des Sciences avait pour vocation d'attribuer des bourses aux jeunes chercheurs. En 1935, ces deux institutions furent réunies pour former la Caisse Nationale de la Recherche Scientifique. Par conséquent, elle avait pour rôle d'allouer des bourses et de participer au financement des laboratoires.

Parallèlement à ces organismes de financements, à partir de 1922, l'Office National des Recherches Scientifiques et Industrielles et des Inventions avait pour objectifs de coordonner et soutenir les recherches scientifiques de tout type.
En 1938, il est remplacé par le Centre National de la Recherche Scientifique Appliquée. Il avait alors pour mission dans un premier temps d'analyser l'organisation de la recherche appliquée, tant en France, en réalisant l'inventaire de l'ensemble des laboratoires français, qu'à l'étranger. Puis, dans un second temps, il lista les grands problèmes à résoudre et lança des appels à projets autour de ces thèmes. Un mois après l'entrée en guerre, en octobre 1939, le Centre National de la Recherche Scientifique Appliquée fut associé à la Caisse Nationale de la Recherche Scientifique pour devenir le Centre National de la Recherche Scientifique. Il avait pour vocation de réunir les chercheurs et éviter qu'ils ne soient mobilisés, comme ce fut le cas lors de la première guerre mondiale qui impliqua la mort de nombreux savants. Le CNRS eut alors pour fonction de rassembler et coordonner toutes les institutions de recherche pour les besoins militaires à sa création puis autour des thèmes de l'énergie et alimentaires pendant l'occupation. Réorganisé à la libération, l'établissement s'orienta vers la recherche fondamentale, la recherche appliquée étant confiée à des organismes spécialisés, tel que le Commissariat à l'Energie Atomique (CEA).
En 1958, date de l'arrivée du général De Gaulle au pouvoir, la recherche scientifique devint une priorité, et vécut un « âge d'or » pendant les années 1960.
En 1966, le CNRS évolua pour offrir des moyens financiers et humains à des laboratoires universitaires appelés unités associées, ancêtres des actuelles Unités Mixtes de Recherche (UMR).

---

[4] Denis Guthleben. *Histoire du CNRS de 1939 à nos jours.* Armand Colin, 480 pages, 2003

En 1982, la loi dite « Chevènement » décréta que le personnel du CNRS dépendait du régime de la fonction publique. Cette situation avait pour avantage d'offrir la stabilité nécessaire à la recherche et de s'affranchir de la dépendance des financements privés et des changements de politique propres aux successions de gouvernements.

L'année 2007 marqua un tournant pour l'organisation de la recherche scientifique française. Le gouvernement a élaboré un plan stratégique dans l'objectif de mettre les universités au cœur de la recherche. Cela s'est traduisit notamment pour elles par plus de responsabilités dans les Unités Mixtes de Recherche. Pour le CNRS, douze objectifs ont été fixés pour l'horizon 2020.

I.1.2 Extraits du plan stratégique « Horizon 2020 »

Le plan stratégique a pour objectif de renforcer la mission du CNRS au sein de la politique scientifique de la France dans les nouveaux environnements européens et mondiaux face à l'accession des universités à l'autonomie. Le CNRS reste le premier partenaire scientifique des établissements d'enseignement supérieur et de recherche en assurant un rôle d'agence de moyens. En matière de recherche, la stratégie scientifique de l'établissement doit fédérer les disciplines et les compétences. Le CNRS doit contribuer au développement économique en tant qu'acteur national et international de la production des connaissances et de l'innovation. Pour cela l'organisme doit mobiliser ses ressources et se réorganiser selon une logique de réseaux pour conduire des projets de qualité.

Le plan stratégique se décline en douze objectifs répartis selon trois volets : « la recherche : cœur de métier », « la société de la connaissance » et « une organisation mieux adaptée aux défis pour 2020 ». Le projet de gestion des identités et des accès doit s'inscrire dans la stratégie du CNRS en étant un soutien à la réalisation de ces objectifs.

I.1.2.1 La recherche : cœur de métier du CNRS

- ***Objectif 1 : faire avancer le front de la connaissance***

« Le programme de recherche du CNRS s'appuiera sur la force des disciplines sur leur capacité à s'associer, échanger et construire des concepts en commun. Le CNRS devra maintenir ce socle et favoriser son développement, associer ces compétences et garantir une plus grande réactivité en réponse à de nouveaux défis. »

- ***Objectif 2 : relever les grands défis de la planète***

« Les contributions du CNRS se déploieront préférentiellement sur le climat, la biodiversité, l'environnement et le développement durable, les risques naturels, la santé, les ressources naturelles, l'énergie, la sécurité et les nouvelles formes de vulnérabilité, les grandes mutations sociales. »

- ***Objectif 3 : faire dialoguer les concepts et les technologies de pointe***

« La découverte et la validation de grandes théories nécessitent de développer des technologies sophistiquées. Ces dernières peuvent être à leur tour source d'applications originales dans des domaines auxquels elles n'étaient pas destinées initialement. Le CNRS favorisera ce dialogue porteur de progrès pour la science et la technologie. »

- ***Objectif 4 : fédérer les disciplines et les compétences***

« Le CNRS suscitera des convergences autour de thèmes fédérateurs abordant des questions scientifiques fondamentales à fort impact culturel ou technologique. »

- ***Objectif 5 : promouvoir et mutualiser les équipements indispensables à la recherche***

« La mise en place d'équipements et d'infrastructures à dimension nationale et internationale est nécessaire aux progrès de la plupart des champs disciplinaires. Le CNRS poursuivra une politique ambitieuse d'investissement dans les très grandes infrastructures et les plates-formes mutualisées, pour créer et maintenir ces équipements au meilleur niveau international. »

I.1.2.2 Le CNRS et la société de la connaissance

- ***Objectif 6 : le CNRS, acteur de la croissance économique***

« Le CNRS doit devenir un des grands outils de la croissance économique. Le dialogue entre le CNRS et l'entreprise sera favorisé par une mobilité accrue des personnes. Le CNRS développera une gestion stratégique de son portefeuille de brevets et soutiendra en complément la création d'entreprises. »

- ***Objectif 7 : le CNRS, acteur de la formation et partenaire des universités***

« Le CNRS veut développer la perception de l'importance des sciences dans la pratique professionnelle. L'organisme se mobilisera pour accompagner les universités et les grandes écoles

dans la compétition mondiale de l'enseignement supérieur et de la recherche et pour répondre à la demande croissante de formation continue que nécessite une recherche industrielle de pointe. »

- ***Objectif 8 : le CNRS, acteur dans la société***

« Dans un contexte mondial nouveau marqué par l'expansion des connaissances et de la communication, par certaines tendances à une privatisation croissante des résultats de la recherche, par une demande sociale d'efficacité, d'ouverture sociale, de transparence politique et de responsabilité éthique, le CNRS sera à l'image des évolutions de la société. Il s'impliquera de façon significative en créant plus d'espaces de débat, d'échange et d'information scientifique. »

- ***Objectif 9 : le CNRS, acteur européen et international***

« La construction de l'Espace Européen de la Recherche (EER) dynamisera la communauté scientifique européenne. Avec ses partenaires universitaires, les actions du CNRS s'inscriront dans cette perspective. L'action internationale visera principalement à consolider l'excellence avec les grands pays industrialisés et à positionner le CNRS dans les grands pays émergents. »

I.1.2.3 Une organisation mieux adaptée aux défis pour 2020

- ***Objectif 10 : les femmes et les hommes – acteurs de l'avenir du CNRS***

« Le CNRS construira une stratégie sur le long terme misant sur une évolution des métiers et des compétences de tous les acteurs, qu'il faudra définir, planifier et accompagner dans le respect des carrières. Celle-ci sera organisée pour anticiper les évolutions, responsabiliser et motiver tous les acteurs. »

- ***Objectif 11 : une organisation en instituts et en réseaux***

« Pour une meilleure synergie des opérateurs de terrain, le CNRS se réorganisera selon une logique d'Instituts avec une double fonction d'agence et d'opérateur, et de réseaux pluridisciplinaires et délocalisés, capables de se mobiliser pour faire face aux grands enjeux scientifiques. Par une conduite de projet de qualité, des conditions d'efficacité comparables à celles de nos homologues étrangers les plus compétitifs seront visées à tous les niveaux. »

- ***Objectif 12 : une évaluation en cohérence avec les objectifs stratégiques***

« L'évaluation individuelle ou collective accompagnera l'investissement de tous sur les objectifs du plan stratégique en couvrant l'ensemble des réseaux, dans les régions, en France, en Europe et à l'international, auxquels le CNRS participera. »

I.1.3 Organisation

La nouvelle organisation du CNRS doit répondre à trois grands objectifs :

1. « Assurer l'interdisciplinarité, garante de grandes découvertes. Cette interdisciplinarité ne pourra se développer qu'en s'appuyant sur des disciplines fortes. »
2. « S'adapter au nouvel environnement de la recherche en France, les universités devenant autonomes et les organismes nationaux devant mieux se coordonner entre eux. »
3. « Organiser l'expression des compétences et des talents et optimiser l'usage des ressources, en particulier des fonds publics. »

I.1.3.1 Direction

La direction du CNRS a notamment, la responsabilité :

- de l'élaboration du plan stratégique de l'établissement et de la négociation, avec l'Etat, de son contrat pluriannuel d'objectifs.
- de la répartition du budget de l'établissement que l'Etat attribue globalement à l'établissement (moyens humains et financiers), la politique de gestion des ressources humaines, la modernisation et la simplification de l'appui apporté aux laboratoires, la coordination et la consolidation de la politique partenariale nationale et internationale de l'organisme, la communication et l'administration du Centre.

Elle décide des budgets et des moyens des Instituts, dans le cadre de contrats d'objectifs et de moyens pluriannuels. Chaque Institut dispose de deux enveloppes budgétaires, correspondant aux deux rôles d'opérateur et d'agence de moyens.

I.1.3.2 Direction Générale Déléguée à la Science (DGDS)

La Direction Générale Déléguée à la Science conduit, aux côtés du président, la politique scientifique de l'établissement. Ainsi, elle a en charge la coordination de l'action des dix Instituts du CNRS, veille à promouvoir l'interdisciplinarité et organise les partenariats avec les divers acteurs de la recherche, à l'échelle régionale, nationale, européenne ou internationale. Dans ce cadre, et en relation étroite avec la direction générale déléguée aux ressources, elle s'appuie sur les compétences des délégations régionales.

Pour remplir ses missions, la DGDS s'appuie sur :

- les dix instituts et les unités de recherche qui leur sont rattachées,
  - Institut des sciences biologiques (INSB) ;
  - Institut de chimie (INC) ;
  - Institut écologie et environnement (INEE) ;
  - Institut des sciences humaines et sociales (INSHS) ;
  - Institut des sciences de l'information et de leurs interactions (INS2I) ;
  - Institut des sciences de l'ingénierie et des systèmes (INSIS) ;
  - Institut national des sciences mathématiques et de leurs interactions (INSMI) ;
  - Institut de physique (INP) ;
  - Institut national de physique nucléaire et de physique des particules (IN2P3) ;
  - Institut national des sciences de l'Univers (INSU) ;
- Les trois directions chargées des relations partenariales avec les institutions publiques ou privées, françaises ou étrangères,
  - la direction d'appui à la structuration territoriale de la recherche (DASTR) ;
  - la direction Europe de la recherche et coopération internationale (DARCI) ;
  - la direction de l'innovation et des relations avec les entreprises (DIRE) ;
- la direction de l'information scientifique et technique (DIST),
- la mission pour l'interdisciplinarité.

I.1.3.3 Direction Générale Déléguée aux Ressources (DGDR)

La DGDR a pour mission de soutenir la stratégie et la réalisation des missions de la DGDS. A ce titre, elle propose et met en œuvre les politiques financières, patrimoniales et des ressources humaines de l'établissement. Sa fonction de support du CNRS lui permet d'assurer la cohérence d'ensemble du dispositif d'appui à la recherche et des procédures de gestion. Elle définit également la stratégie de l'établissement en matière de systèmes d'information et de télécommunication dans les domaines administratifs et scientifiques.

La DGDR regroupe :

- la direction des ressources humaines (DRH),
- la direction des comptes et de l'information financière (DCIF),
- la direction de la stratégie financière, de l'immobilier et de la modernisation de la gestion (DSFIM),
- la direction du système d'information (DSI),
- la direction des affaires juridiques (DAJ),

- la coordination nationale de prévention et sécurité (CNPS),
- les dix-neuf délégations régionales (DR),
- la mission pilotage et relations avec les délégations régionales et les instituts

Les DR représentent le CNRS en région auprès des partenaires académiques, institutionnels ou industriels et assurent une gestion administrative et financière de proximité des unités de recherche et des personnels ainsi qu'un soutien logistique.

I.1.4 Structures opérationnelles du CNRS

Le terme d'unité du CNRS fait référence à une structure opérationnelle pilotée (unité propre) ou co-pilotée (unité mixte) par le CNRS. Dans ce dernier cas, les moyens accordés par le CNRS s'ajoutent à ceux alloués par les autres établissements dont elles dépendent. Le CNRS peut également apporter des moyens financiers, matériels et humains à des unités relevant d'autres établissements de recherche.

Les unités de recherche sont des structures opérationnelles de recherche incluant les unités propres de recherche (UPR) et les unités mixte de recherche dont font partie notamment les unités mixtes internationales (UMI).

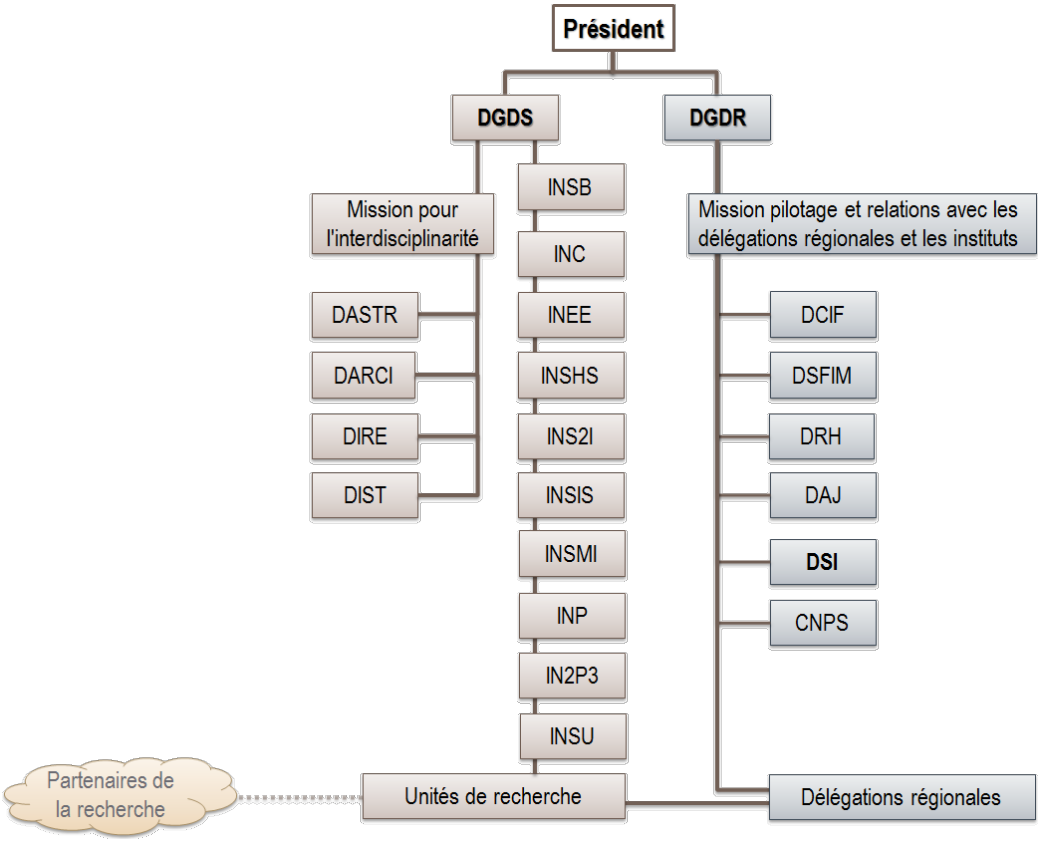


Figure 1 - Organigramme du CNRS

Les unités de service sont des structures organisationnelles qui ont pour vocation de mener des actions d'accompagnement de la recherche et d'apporter un soutien aux unités de recherche en mettant à disposition des moyens matériels. N'ayant pas pour objectif d'effectuer des activités de recherche, l'affectation de chercheurs à ces unités est limitée.

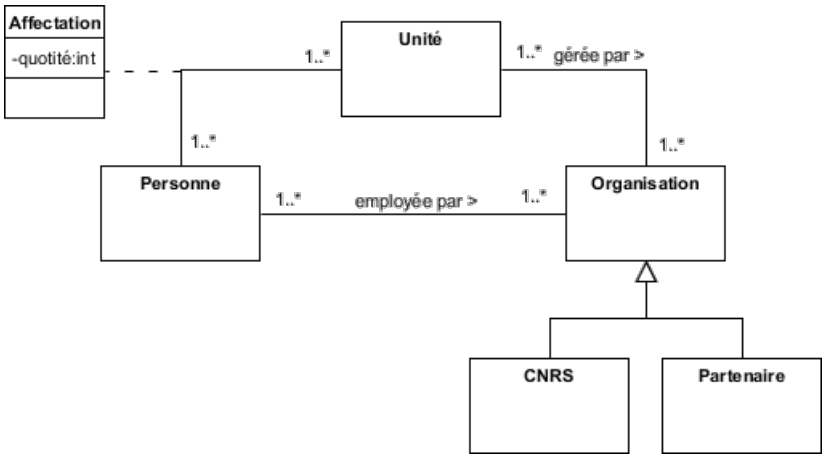


Figure 2 - Diagramme de classe des structures opérationnelles du CNRS

I.2 Direction des Systèmes d'Information

I.2.1 Présentation

La DSI définit et met en œuvre les systèmes d'information destinés au pilotage de la recherche scientifique et à la gestion des différentes activités de l'établissement ce qui inclut par exemple la gestion et la paie du personnel CNRS, la gestion budgétaire, financière et comptable de l'établissement ainsi que la gestion des opérations de partenariats de recherche. Ces systèmes sont élaborés pour les laboratoires, les délégations régionales et les directions administratives et scientifiques du CNRS.

À ce titre, la DSI est chargée de définir, mettre en place et gérer les moyens techniques nécessaires, et planifier leur évolution dans le cadre d'un schéma directeur. Elle contribue, par ses compétences et ses moyens, au développement des actions communes décidées entre l'établissement et ses partenaires.

La DSI s'est réorganisée autour de pôles de compétences.

Le pôle « Organisation, méthodes et urbanisation » identifie et gère les projets liés au pilotage du CNRS. Il définit également les référentiels de données utilisés par le système d'information.

Le pôle « Application » assure la maintenance des applications du système d'information.

Le pôle « Ingénierie et Exploitation » (PIE) met en œuvre et gère le cycle de vie opérationnel des applications du système d'information.

Le pôle « Architecture Réseaux, Expertises et Support aux Unités » (ARESU) a pour mission d'étudier les architectures réseaux et en assure l'évolution. Il travaille en liaison avec différents partenaires de la recherche en participant à l'animation de la communauté des informaticiens, en assurant un support aux outils de développement. Il assume également un rôle de veille technologique dans le domaine des réseaux, logiciels et middleware et de promotion des nouveaux usages et outils des systèmes d'information.

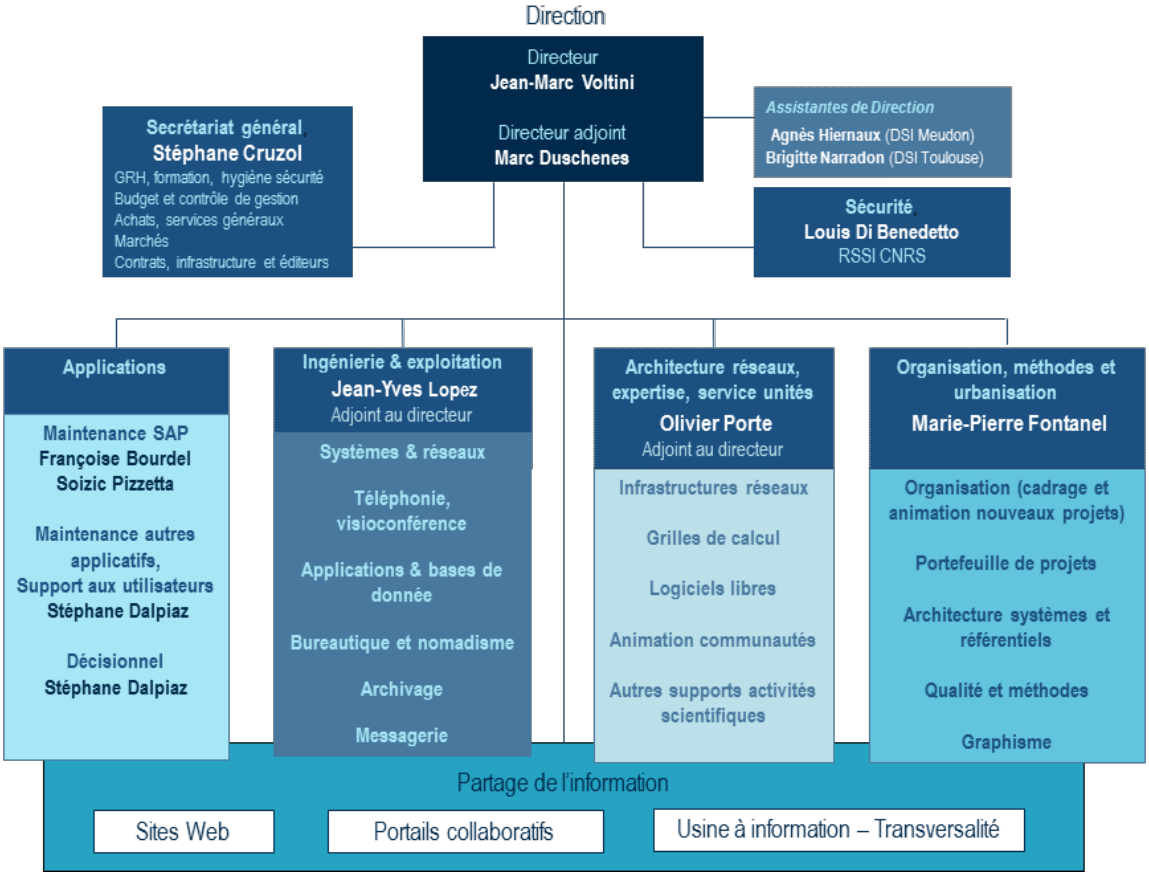


Figure 3 - Organigramme de la Direction des Systèmes d'Information
(source : http://www.dsi.cnrs.fr/la-DSI/organigramme.htm)

I.2.2 Extraits du schéma directeur

Le plan stratégique « Horizon 2020 » du CNRS établi en 2008 fut décliné en un schéma directeur pour la DSI pour une période de quatre ans. Ainsi depuis 2009, la DSI poursuit la refonte du système d'information en suivant quatre objectifs principaux : « capitaliser sur les socles existants », « poursuivre l'intégration des différents systèmes dans l'optique d'une gestion modernisée », « garantir la fiabilité des données de référence dans le système d'information global » et « industrialiser la gestion de la sécurité et des infrastructures ». De même, le système d'information se doit d'évoluer pour soutenir la stratégie de l'établissement en se focalisant sur l'ouverture des flux d'information avec les partenaires du CNRS et la simplification de la gestion des laboratoires.

Dans le cadre de l'optimisation du système d'information existant, la DSI a pour objectif de :

- Maximiser l'intégration des fonctionnalités au sein d'un même outil
- Faciliter la gestion des processus de bout en bout, sans rupture ou cloisonnement liés à l'organisation et à la ressaisie d'informations redondantes
- Capitaliser sur les compétences internes

En outre, dans le cadre de l'industrialisation de la gestion de la sécurité et des infrastructures, la DSI a initié une Politique de Sécurité des Systèmes d'Information (PSSI) qu'il reste à décliner, déployer et piloter afin de maintenir les risques à un niveau acceptable. Pour cela, la DSI doit identifier les éléments sensibles du système d'information et les sécuriser.

C'est pour répondre à l'ensemble de ces objectifs que les pôles ARESU et PIE ainsi que les responsables de la sécurité des systèmes d'information du CNRS et de la DSI souhaitent étudier la problématique de gestion des identités et des accès.

II Concepts et états de l'art

II.1 Gestion des identités

II.1.1 Définitions

II.1.1.1 Identité

Dans l'article « Trust Requirements in Identity Management » [5], l'identité est définie comme « un ensemble de caractéristiques propres par lesquelles une personne ou une organisation est connue ou reconnue. Ces éléments peuvent être définis, comme le nom, l'adresse, la nationalité, ou peuvent être innés comme les empruntes digitales. Pour l'identité d'une organisation, les caractéristiques sont acquises ».
Le standard international ISO/IEC 24760-1[6], basé sur la recommandation UIT-T Y.2720 rédigée par l'Union Internationale des Télécommunications, étend la définition d'identité à l'« information utilisée pour représenter une entité dans un système d'information et de communication ». Une entité représente une personne physique ou morale (organisation, entreprise, …), une ressource (un objet tel qu'un matériel informatique, un système d'information ou de communication) ou un groupe d'entités individuelles.

Une entité peut posséder plusieurs identités numériques. Chaque identité permet alors d'exposer des informations en fonction de l'environnement. Ainsi, un individu peut présenter, par exemple, des informations publiques le concernant dans le cadre de son activité professionnelle, ce qui représentera une identité, et d'autres informations personnelles le présentant dans son contexte familial, ce qui désignera une autre identité.

Une identité peut être utilisée dans plusieurs contextes. Conjointement, dans un même domaine, une entité peut être incarnée par plusieurs identités. De plus, plusieurs identités d'une même entité peuvent partager les mêmes caractéristiques, ce qui implique que les identités peuvent ne pas être uniques dans un même contexte.

---

[5] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, S. Pope. Trust Requirements in Identity Management. *Australasian Information Security Workshop 2005* volume 44, pages 99-108, 2005

[6] ISO/IEC 24760-1:2011(E). ISO/IEC, 20 pages, 2011

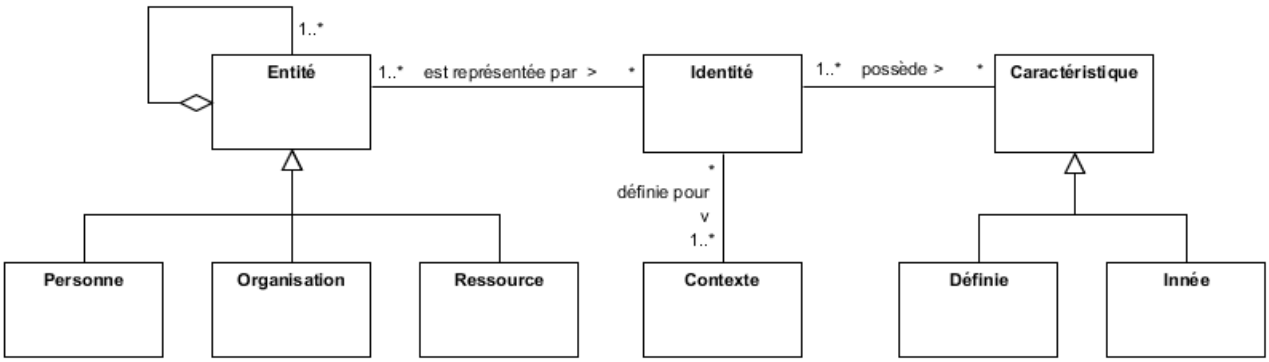


Figure 4 - Diagramme de classe du concept d'identité

Dans le présent document, le terme d'identité fera référence à une identité numérique limitée aux informations utilisées dans le contexte professionnel dont l'employeur doit gérer le cycle de vie.

II.1.1.2 Attributs et identifiants

L'attribut d'une identité décrit une caractéristique d'une entité dans un contexte déterminé [6]. Chaque attribut est défini par un type, une valeur et un contexte. Il peut éventuellement avoir un nom qui peut être utilisé pour le référencer. Un attribut certifié conforme par un organisme officiel et/ou digne de confiance est appelé « claim » (la traduction française étant « affirmation »).

L'identifiant est une information qui permet de distinguer sans ambiguïté une identité d'une autre pour un contexte donné. L'identifiant peut être un attribut. Dans ce cas, la valeur d'un identifiant ne peut pas être utilisée par plusieurs identités. De ce fait, il est généralement utilisé dans le processus d'identification qui est responsable de la reconnaissance de l'identité dans un contexte. De même qu'une entité peut posséder plusieurs identités pour présenter des informations en fonction des contextes, une identité peut être représentée par plusieurs identifiants.

L'identifiant de référence est un identifiant pour un contexte donné qui ne changera pas pendant la durée de vie de l'entité qu'elle représente. Il doit perdurer tant que l'entité doit être connue du domaine. Il peut même durer plus longtemps, en fonction de la politique d'archivage à laquelle est soumise l'organisation. L'identifiant de référence ne pourra être utilisé par une autre entité uniquement sous condition que l'entité propriétaire ne soit plus référencée dans le domaine et après une période déterminée par la politique de sécurité du domaine.

L'identifiant unique personnel (IUP) est un identifiant qui permet de désigner une entité. Sa valeur est donc la même pour les toutes les identités d'une même entité. Deux entités ne peuvent pas partager le même identifiant unique personnel.

Les justificatifs d'identité (en anglais : « identity credentials ») sont des informations qui peuvent être utilisées en tant qu'attestation de l'identité revendiquée par une entité. Il peut s'agir d'une chaîne de caractère connue uniquement de l'identité (mot de passe) ou d'une empreinte digitale par exemple.

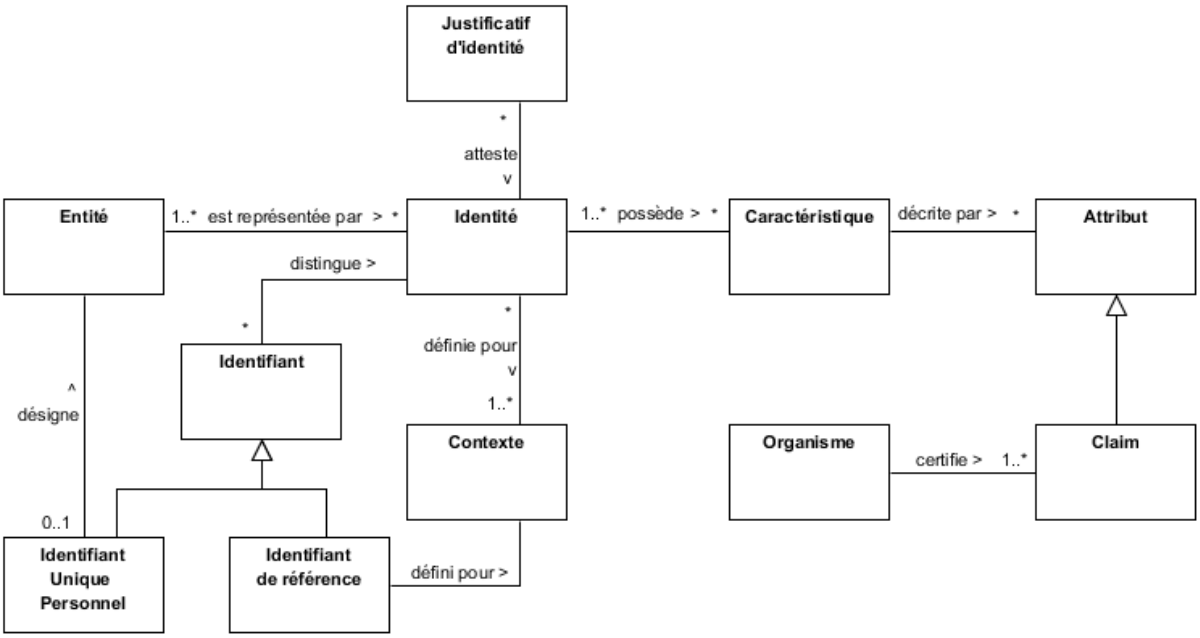


Figure 5 – Diagramme de classe des concepts d'attribut et d'identifiant

II.1.1.3 Fournisseurs de service et d'identité

Le fournisseur de service (SP : « Service provider » en anglais) est une ressource informatique qui est le support à la réalisation d'une activité d'une organisation (réelle ou virtuelle). Un fournisseur de service peut être un système d'information de gestion ou le système qui pilote une machine à commande numérique. Dans certains cas, l'accès au service est restreint et l'identité des utilisateurs doit être vérifiée avant de pouvoir lancer l'exécution d'une tâche.

Le fournisseur d'identité (IdP : « Identity provider » en anglais) est un fournisseur de service qui construit la représentation numérique des identités [7]. Il est notamment responsable de la gestion des attributs et le garant de l'alimentation de leurs valeurs.

Un fournisseur de service peut être mis en œuvre en corrélation avec le fournisseur d'identité afin de gérer les aspects liés à l'authentification (processus de vérification de l'exactitude d'un ou plusieurs attributs d'une identité) pour les autres fournisseurs de service de l'organisation. Dans ce cas, ce fournisseur de service est un support à la notion de confiance évoquée pour les organisations virtuelles et à la politique de sécurité de l'organisation.

[7] E. Bertino, K. Takahashi. *Identity Management: Concepts, technologies and systems*. Artech House, 194 pages, 2010

Le consommateur d'identité (RP : « Relying Party » en anglais) est un fournisseur de service dont l'utilisation nécessite l'authentification des identités présentées par un fournisseur d'identité. En fonction du domaine d'activité de l'organisation et du type de service rendu, un consommateur d'identité peut être soumis au respect d'une ou plusieurs lois (cf. les paragraphes « Cadre juridique » des chapitres « Gestion des identités » et « Gestion des accès »). Dans ce cas, l'organisation est contrainte à la mise en place d'outils de contrôles et de gestion des processus liés aux identités.

Un domaine d'identité correspond à l'ensemble composé d'un fournisseur d'identités et des consommateurs d'identités pour lesquels une identité est connue et utilisable. Le concept de « contexte » évoqué précédemment peut être un domaine d'identité.

II.1.1.4 Fédération d'identité

Une fédération d'identité est un accord entre plusieurs domaines d'identités qui spécifie comment les différentes parties prenantes peuvent échanger des informations relatives aux identités. L'accord définit les protocoles utilisés, les formats des données et les procédures de protection et d'audit. L'identité ainsi fédérée pourra être utilisée dans les différents domaines de la fédération.

II.1.1.5 Gestion des identités

Le CLUSIF [8] définit la gestion des identités comme la gestion du « cycle de vie des personnes (embauche, promotion, mutation, départ, etc.) au sein de la société et les impacts induits sur le système d'information ». Ces changements ont des conséquences sur les informations connues et gérées par le domaine d'identité de l'organisation.

En effet, avant de travailler au sein d'une équipe, une relation contractuelle est établie avec la personne, que ce soit directement pour ce qui concerne un employé, par l'intermédiaire d'un partenaire ou par l'intermédiaire d'une société de service pour un prestataire. Ce contrat définit la mission de l'individu qui inclut des informations telles que le résultat attendu, la date de début de mission et sa durée. En contre partie du travail fourni, l'organisation s'engage à rémunérer l'individu directement ou via son organisation d'appartenance, selon le type de relation établie. Le contrat permet également d'initier les démarches administratives telles que l'enregistrement auprès du service de comptabilité qui initiera le processus de paiement de la paie ou de la facture. Il est

[8] A. Balat, R. Bergeron, A. Butel, M. Cottreau, F. Depierre, G. Khouberman, L. Mourer, W. Poloczanski. *Gestion des identités*. CLUSIF, 63 pages, 2007

également le socle qui permet de mettre fin au processus de paiement. A partir de ces informations, une identité peut être construite puis enregistrée auprès du fournisseur d'identité.

Ensuite, lorsque la personne commence son contrat, l'identité qu'il doit présenter auprès des fournisseurs de service est activée, afin de lui permettre d'interagir avec les ressources utiles à sa mission.

A la fin de ladite mission, l'identité peut être suspendue, donc temporairement inutilisable, s'il est prévu de la réutiliser pour un prolongement de contrat par exemple. Une autre possibilité consiste à archiver l'identité. Cela implique que les informations lui étant liées ne sont plus exploitables pour l'authentifier auprès du domaine. Par contre, l'ensemble, ou une sous-partie, des informations archivées peut être réutilisé pour construire une nouvelle identité (processus de restauration).

Après un délai établi par l'organisation et par la loi, toutes les informations relatives à l'identité sont supprimées (cf. chapitre « Cadre réglementaire »).

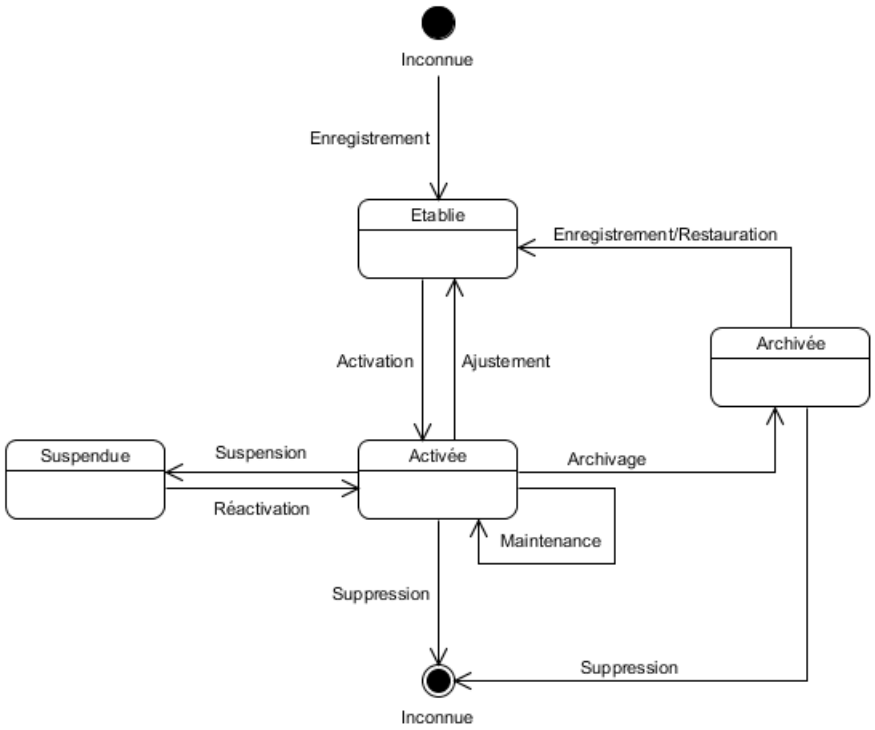


Figure 6 - Cycle de vie d'une identité

De plus, selon la norme ISO/IEC 24760 [6], la gestion des identités inclut la gouvernance, les politiques, les processus, les données, les technologies et les standards permettant notamment :

- d'authentifier les identités,
- d'établir la provenance des informations des identités,
- d'établir le lien entre les informations sur les identités et les entités,
- de maintenir à jour les informations sur les identités,
- d'assurer l'intégrité des informations sur les identités,

- de fournir les justificatifs d'identité et les services pour faciliter l'authentification d'une entité en tant qu'identité reconnue,
- d'ajuster les risques de sécurité liés au vol d'information par exemple.

II.1.1.6 Exemples dans le contexte CNRS

Une personne travaillant pour une unité du CNRS peut être connue sous plusieurs identités. Ce cas de figure se présente notamment lorsque la personne travaille pour plusieurs unités ou occupe différentes fonctions. En effet, dans le contexte de l'activité de recherche qu'un chercheur exerce au sein d'une unité, son établissement de tutelle, le CNRS, le connaît par exemple sous l'identité « Chercheur CNRS *Jean Perrin* de l'unité *uuu* ». Parallèlement, il peut être chargé de mission en tant que directeur dans une autre unité. Dans ce cas, l'établissement de tutelle de cette unité, le CNRS dans le cadre de cet exemple, lui fournit et gère l'identité « Directeur de l'unité *xxx J.B. Perrin* ». Conjointement à ces activités, en tant qu'employé, son employeur, dans ce cas le CNRS, produit l'identité « Employé CNRS *Jean-Baptiste Perrin* ». Ces identités ne sont valables que pour le contexte « *CNRS* ». Dans le cas où les unités seraient des UMR, ces identités ne seraient pas connues de l'établissement de tutelle qui fournirait alors au chercheur au moins une identité spécifique à ce contexte.

Les caractéristiques appartenant à chaque identité ne sont pas nécessairement communes et les attributs les présentant sont construits indépendamment. Par ailleurs, les identités ne sont pas obligatoirement liées. Ainsi, les identités « Chercheur » et « Directeur » peuvent être liées à l'identité « Employé » permettant à cette dernière d'avoir accès à certaines informations des autres identités. Inversement, les deux premières identités sont indépendantes et n'ont pas de visibilité sur les informations d'autres identités.

Tableau I - Exemple d'identités dans le contexte du CNRS

	Chercheur	Directeur d'unité	Employé
Nom	PERRIN	PERRIN	PERRIN
Prénom	Jean	J.B.	Jean-Baptiste
Date de naissance	30 septembre	30 septembre	30 septembre
Lieu de naissance	-	-	LYON
Diplômes	-	-	Agrégation de physique Doctorat ès sciences

	Chercheur	Directeur d'unité	Employé
			physiques
Quotité de travail	50%	50%	100%
Affectation	Unité *uuu*	Unité *xxx*	-
Employeur			
Discipline scientifique	Physique	Chimie	-
Identifiant	jean-baptiste.perrin@cnrs.fr	JBP	153545
Justificatif d'identité	Certificat numérique	« @zer1yuioP »	« azertyuiop »

Le CNRS met à disposition un service de compte-rendu de l'activité de recherche , un service de dépôt et consultation de documents scientifiques pour les chercheurs travaillant dans une unité dont le CNRS est une des tutelles, un service de gestion des congés, un service d'accès au dossier pour la retraite pour les employés du CNRS, un service de saisie des demandes de moyens pour l'unité et un service de gestion du budget de l'unité à destination des directeurs d'unité que le CNRS finance.

Tableau II - Exemple de services dans le contexte du CNRS

Service	Identité utilisatrice potentielle
Compte-rendu de l'activité de recherche (Crac)	Chercheur dans une unité CNRS
Dépôt et consultation de documents scientifiques (Doc)	Chercheur dans une unité CNRS
Gestion du budget de l'unité (Bdg)	Directeur d'unité CNRS
Saisie des demandes de moyens (Ddm)	Directeur d'unité CNRS
Dossier de retraite (Ret)	Employé CNRS
Gestion des congés (Cge)	Employé CNRS

II.1.2 Modèles

Dans un domaine d'identité, le partage des attributs utilisés par les mécanismes d'identification (association de l'identifiant et d'un justificatif d'identité ; l'identification est souvent réalisée conjointement à l'authentification) implique pour les fournisseurs de service de partager les risques en cas de corruption d'une identité. Les différents modèles de gestion des données permettent donc de déporter les risques et les charges d'administration à différents niveaux.

Différents modèles de gestion des identités peuvent cohabiter au sein de la même organisation. A. Jøsang, J. Fabre, B. Hay, J. Dalziel et S. Pope [5] proposent les trois modèles suivants de gestion des identités.

II.1.2.1 Identité isolée

Dans ce modèle, chaque fournisseur de service utilise son propre domaine d'identité, donc, son propre fournisseur d'identité. Un utilisateur doit utiliser un identifiant et un justificatif d'identité différents pour s'authentifier auprès de chacun des domaines.

Du point de vue de chacun des fournisseurs d'identité, la gestion des identités est plus simple. De plus, en cas de corruption d'identité dans un domaine d'identité, les autres fournisseurs de service ne sont pas impactés. Ce modèle a également l'avantage de permettre de définir un niveau de sécurité différent pour les justificatifs d'identités (longueur du mot de passe, nombre de justificatifs à présentés, etc.).

Cependant, cette approche peut devenir complexe du point de vue de l'utilisateur. En effet, ce dernier doit répéter les étapes d'authentification et d'identification auprès de chacun des domaines d'identité rattachés aux fournisseurs de services. De ce fait, il doit gérer et se souvenir d'autant d'identifiants et d'informations utiles à l'authentification que de services auxquels il doit accéder. Cela augmente donc le risque d'oubli ou de perte de ces informations, surtout pour les services auxquels il n'accède que rarement. De plus, cette situation peut être source de faible adhérence à la politique de sécurité de l'organisation qui sera jugée trop contraignante.

Le schéma ci-dessous représente l'accroissement du nombre de domaines d'identité et par conséquent du volume d'information nécessaire en fonction du nombre de fournisseurs de services.

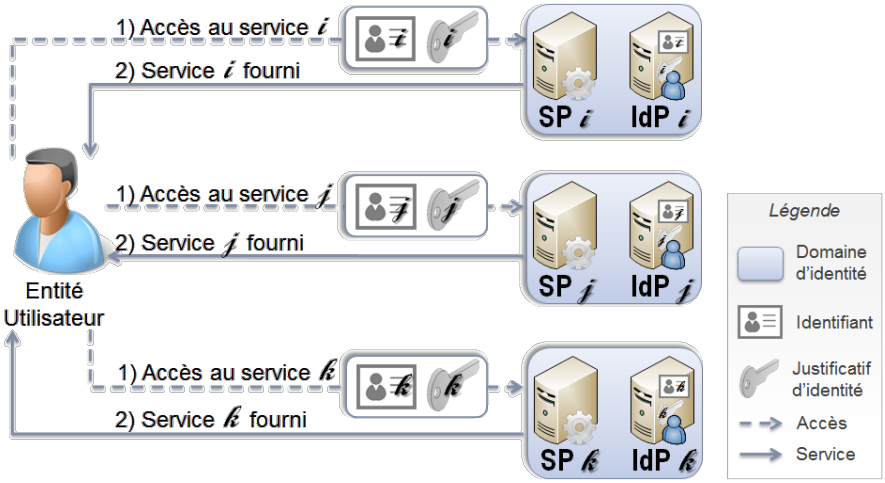


Figure 7 – Modèle de gestion d'identité : « identité isolée »

Dans le cadre de l'exemple décrit précédemment, l'utilisation du modèle d'identité isolée implique que chaque service que la personne doit utiliser correspond à un contexte unique. De ce fait, elle doit manipuler autant d'identités que de services. Ainsi, pour le service de gestion des congés, le chercheur présente l'identité « Employé CNRS - *Congés* » pour le domaine d'identité « CNRS - *Congés* », qui est un dérivé de l'identité « Employé CNRS » décrite précédemment. Ce contexte ayant son propre fournisseur d'identité, il doit gérer le cycle de vie de cette identité, ce qui inclut la mise à jour des informations, dont le justificatif d'identité et la génération d'un ou plusieurs identifiants. Pour utiliser les cinq autres services décrits précédemment, la personne doit présenter cinq autres identités distinctes potentiellement dissemblables. En effet, les fournisseurs d'identité peuvent utiliser des informations proches mais pourtant différentes. Les informations sont donc répliquées proportionnellement au nombre de services les utilisant. Cela augmente le risque d'erreur due à une rupture dans la chaîne d'approvisionnement. De plus, cette situation est aggravée par le cycle de mise à jour des informations et de renouvellement des justificatifs. Ces derniers sont gérés par des fournisseurs d'identités indépendants qui forcent ainsi l'utilisation de six justificatifs différents dans le cadre de l'exemple comme illustré dans le tableau suivant. En effet, les consommateurs d'identités peuvent demander des contraintes différentes sur les justificatifs d'identité. Par exemple, pour les mots de passe, la chaîne de caractère doit contenir un nombre minimum de caractères, de chiffres, de symboles ou non en fonction de la politique de sécurité du fournisseur de service.

Tableau III - Synthèse de l'exemple pour le modèle d'identité isolée

Fournisseur de service	**SP Crac**	**SP Doc**	**SP Bdg**	**SP Ddm**	**SP Ret**	**SP Cge**
Domaine	Crac	Doc	Bdg	Ddm	Ret	Cge

Fournisseur de service	SP Crac	SP Doc	SP Bdg	SP Ddm	SP Ret	SP Cge
d'identité						
Fournisseur d'identité	IdP Crac	IdP Doc	IdP Bdg	IdP Ddm	IdP Ret	IdP Cge
Nom	PERRIN	PERRIN	PERRIN	PERRIN	PERRIN	P
Prénom	Jean	Jean-Baptiste	J.B.		Jean-Baptiste	JB
Affectation	Unité *uuu*	Unité *uuu*	Unité *xxx*	Unité *xxx*	-	-
Identifiant fourni et utilisé	jean.perrin @*uuu*.cnrs.fr	jb.perrin @*uuu*.cnrs.fr	jean.perrin @*xxx*.cnrs.fr	j-b.perrin @xxx.cnrs.fr	153545	JPB
Justificatif d'identité fourni et utilisé	Certificat numérique *uuu*.cnrs.fr	« azertyuio »	« @zer1yui0 »	Certificat numérique *xxx*.cnrs.fr	« Je@nPerr1n »	« JPB »

II.1.2.2 Identité fédérée

Dans l'article « Trust Requirements in Identity Management » [5], la fédération d'identité est définie comme un ensemble d'accords, standards et technologies permettant à un groupe de fournisseurs de service de reconnaître les identifiants provenant d'autres fournisseurs de services appartenant à la fédération. La fédération donne aux utilisateurs l'illusion de n'utiliser qu'un seul et unique identifiant alors qu'il continue à en présenter un différent à chaque fournisseur de service.

Dans une architecture d'identité fédérée, chaque fournisseur de service utilise son propre fournisseur d'identité, mais est capable d'accepter les identités provenant d'autres fournisseurs. L'accès à un fournisseur de service peut alors se faire au travers d'une identité d'un fournisseur d'identité autre que le sien. Comme pour le modèle isolé, une personne est connue par une identité par service au minimum, mais cette personne n'a pas à toutes les utiliser. Une correspondance est établie entre les identifiants des identités appartenant au même utilisateur dans le domaine d'identité fédéré. Quand un utilisateur est authentifié auprès d'un premier fournisseur de service en utilisant un de ses identifiants et le justificatif qui lui est associé, tous les identifiants sont alors reconnus auprès de l'ensemble des fournisseurs d'identités de la fédération. Pour accéder à un autre fournisseur de service, l'utilisateur n'est alors pas soumis directement aux processus d'authentification et d'identification, car les informations sous-jacentes ont été transmises.

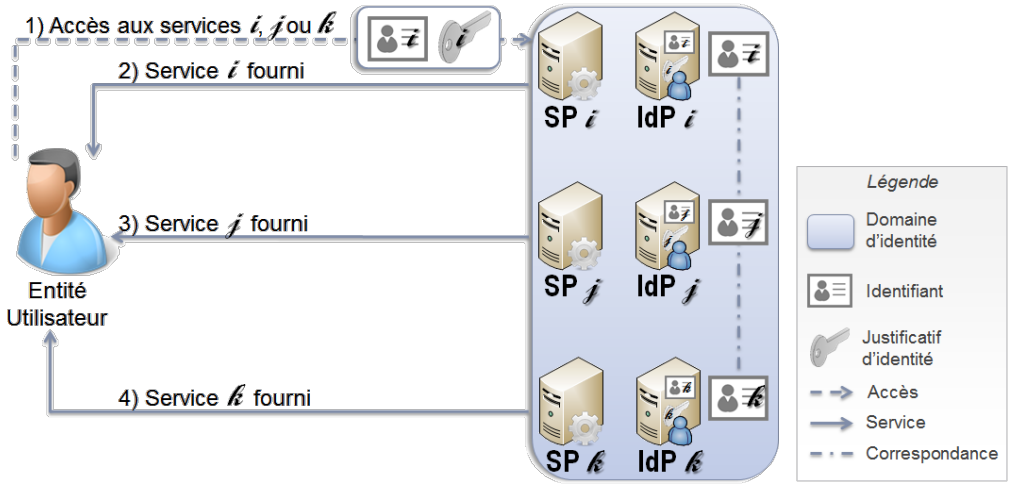


Figure 8 - Modèle de gestion d'identité : « identité fédérée »

Ce schéma illustre les avantages de la fédération pour l'utilisateur par rapport au modèle de gestion précédent, où chaque fournisseur de service utilisait indépendamment son propre domaine d'identité. En employant une identité fédérée, du point de vue de l'utilisateur, les informations nécessaires aux processus d'authentification et d'identification sont les mêmes quelques soient les fournisseurs de services sollicités. Il existe donc autant de domaines d'identité, de fournisseurs d'identité, d'identités que de services, mais l'utilisateur n'en n'a pas conscience.

Dans le cadre de l'exemple décrit précédemment, le modèle d'identité fédérée permet au chercheur d'utiliser un unique couple identifiant-justificatif d'identité quel que soit le service demandé au sein d'une même fédération. Ainsi, le CNRS peut déployer une fédération « Chercheur CNRS » pour l'ensemble des services liés aux activités de chercheur. Dans ce cas, la personne ne manipule qu'un seul couple identifiant-justificatif d'identité (« jean.perrin@*uuu*.cnrs.fr » - Certificat numérique « *uuu*.cnrs.fr »). L'identité correspondante (« Chercheur CNRS - *Crac* ») est alors certifiée par le fournisseur d'identité « Crac » et de ce fait automatiquement acceptée par les autres fournisseurs d'identité de la fédération. Ensuite, une équivalence est établie par le fournisseur d'identité impactés « Doc », permettant de présenter l'identité « Chercheur CNRS - *Doc* » au service « Doc ».

Une autre fédération « DU » peut être mise en place pour les services mis à disposition des directeurs d'unité. Dans ce cas, l'identifiant « j-b.perrin@*xxx*.cnrs.fr » assorti du certificat numérique « *xxx*.cnrs.fr » peut permettre d'utiliser le service de gestion du budget de l'unité sous l'identité « Directeur d'unité CNRS - *Bdg* » et le service de saisie des demandes de moyen sous l'identité « Directeur d'unité CNRS - *Ddm* ». De même, une fédération peut être mise en place pour simplifier l'utilisation des services mis à disposition pour la gestion des ressources humaines.

Par contre, aucune interaction n'est possible nativement entre les différentes fédérations. Seule une fédération de fédération peut permettre d'établir des correspondances entre les domaines d'identité.

Tableau IV - Synthèse de l'exemple pour le modèle d'identité fédérée

Fournisseur de service	**Crac**	**Doc**	**Bdg**	**Ddm**	**Ret**	**Cge**
Domaine d'identité	Chercheur		DU		RH	
Fournisseur d'identité	IdP Crac	IdP Doc	IdP Bdg	IdP Ddm	IdP Ret	IdP Cge
Nom	PERRIN	PERRIN	PERRIN	PERRIN	PERRIN	P
Prénom	Jean	Jean-Baptiste	J.B.		Jean-Baptiste	JB
Affectation	Unité *uuu*	Unité *uuu*	Unité *xxx*	Unité *xxx*	-	-
Identifiant fourni	jean.perrin @*uuu*.cnrs.fr	jb.perrin @*uuu*.cnrs.fr	jean.perrin @*xxx*.cnrs.fr	j-b.perrin @xxx.cnrs.fr	153545	JPB
Justificatif d'identité fourni	Certificat numérique *uuu*.cnrs.fr	« azertyuio »	« @zer1yui0 »	Certificat numérique *xxx*.cnrs.fr	« Je@nPerr1n »	« JPB »
Identifiant utilisé	jean.perrin@*uuu*.cnrs.fr		j-b.perrin@*xxx*.cnrs.fr		153545	
Justificatif d'identité utilisé	Certificat numérique *uuu*.cnrs.fr		Certificat numérique *xxx*.cnrs.fr		« Je@nPerr1n »	

II.1.2.3 Identité centralisée

Dans ce modèle, seuls un identifiant et un justificatif sont utilisés par les fournisseurs de service. A. Jøsang, J. Fabre, B. Hay, J. Dalziel et S. Pope [5] donnent trois exemples d'implémentation de ce type de gestion d'identité.

- ***Identité commune***

Dans ce modèle, une entité unique agit en tant que fournisseur d'identité pour l'ensemble des fournisseurs de service. Le mode de fonctionnement est à mi-chemin entre le modèle d'identité isolée et le modèle d'identité fédérée du point de vue de l'utilisateur. En effet, ce dernier doit répéter les processus d'authentification et d'identification avant de pouvoir utiliser un service. Cependant, le domaine d'identité rattaché à chacun des fournisseurs de service est le même. De ce fait, l'utilisateur utilise les mêmes informations d'identifiant et de justificatif quel que soit le fournisseur de service sollicité, ce qui simplifie l'accès aux différents services.

Avec ce type d'implémentation le fournisseur d'identité unique est un point central et sensible pour l'ensemble des fournisseurs de service. En effet, en cas de défaillance ou de modification au niveau du domaine d'identité, toutes les entités dépendantes sont impactées. De ce fait, ce modèle de gestion impose que chaque fournisseur de service lié au domaine d'identité unique soit déclaré explicitement. Dans le cas contraire, il est difficile d'évaluer les conséquences d'un changement ou d'une altération vis-à-vis des services mis à disposition de l'utilisateur par le biais de cette architecture.

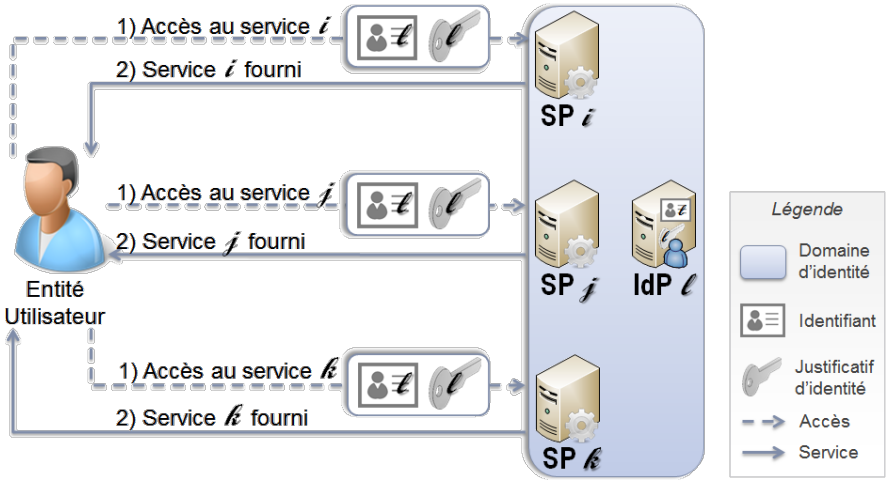


Figure 9 - Modèle de gestion d'identité : « identité commune »

Dans le cadre de l'exemple décrit précédemment, le modèle d'identité commune permet au chercheur d'utiliser un unique couple identifiant-justificatif d'identité quel que soit le service demandé, comme dans le modèle d'identité fédérée. De ce fait, une seule identité est présentée aux différents services du domaine « RH CNRS ». L'unique fournisseur d'identité doit donc construire une identité qui contient les informations nécessaires aux différents services. Un protocole d'accord doit donc être accepté par les différents fournisseurs concernant le contenu et la forme des informations. Ainsi l'identité « Employé CNRS » doit contenir l'identifiant « 153545 » connu par le service « Ret » ainsi que l'identifiant « JPB » connu par le service « Cge ». Par contre les deux services doivent être capables de reconnaître le justificatif d'identité « Je@nPerr1n ». De même, dans les exemples précédents, les valeurs de l'attribut « prénom » des identités « Employé CNRS - *Ret* » et « Employé CNRS - *Cge* » n'étaient pas équivalentes, alors que le modèle d'identité commune impose que cet attribut soit partagé.

Tableau V - Synthèse de l'exemple pour le modèle d'identité commune

Fournisseur de service	**Crac** **Doc**	**Bdg** **Ddm**	**Ret** **Cge**
Domaine d'identité	Chercheur	DU	RH
Fournisseur d'identité	IdP Chercheur	IdP DU	IdP RH
Nom	PERRIN	PERRIN	PERRIN
Prénom	Jean-Baptiste	J.B.	Jean-Baptiste
Affectation	Unité *uuu*	Unité *xxx*	-
Identifiant applicatif 1	jean.perrin@*uuu*.cnrs.fr	jean.perrin@*xxx*.cnrs.fr	153545
Identifiant applicatif 2	jb.perrin @*uuu*.cnrs.fr	j-b.perrin @*xxx*.cnrs.fr	JPB
Identifiant utilisé	jean.perrin@*uuu*.cnrs.fr	j-b.perrin@*xxx*.cnrs.fr	153545
Justificatif d'identité utilisé	Certificat numérique *uuu*.cnrs.fr	Certificat numérique *xxx*.cnrs.fr	« Je@nPerr1n »

- ***Méta-identité***

La mise en œuvre d'un domaine de méta-identité permet aux fournisseurs de service de partager des informations relatives aux identités. Par exemple, une correspondance peut être établie entre les identifiants des différents domaines d'identité et un méta-identifiant (identifiant du domaine de méta-identité) qui n'est pas connu de l'utilisateur. Cet identifiant particulier permettant de désigner de façon unique une entité quelques soient les identités dans les domaines concernés, la notion de méta-identifiant se rapproche de la notion d'identifiant unique personnel.

Les justificatifs peuvent être liés au méta-identifiant. Dans ce cas, les justificatifs sont les mêmes pour tous les domaines d'identités concernés. Du point de vue de l'utilisateur, cette architecture peut être perçue comme un mécanisme de synchronisation des justificatifs entre les différents domaines d'identité.

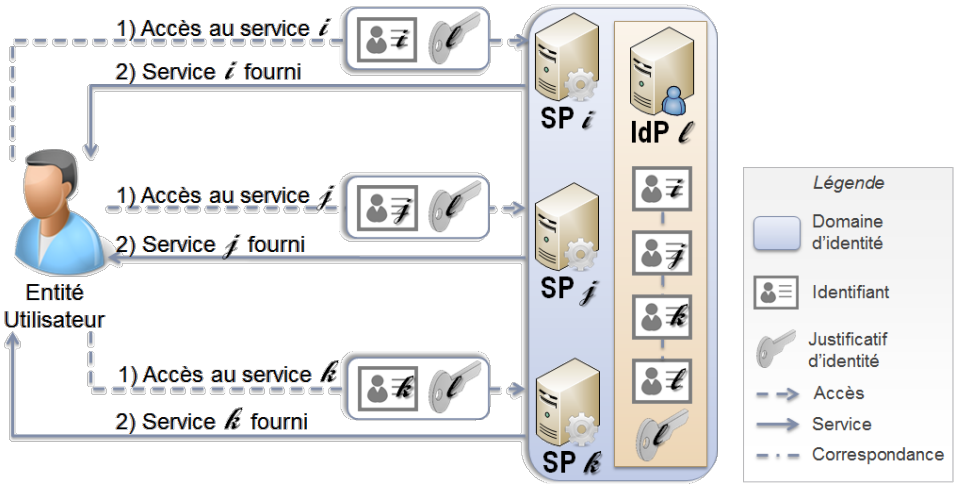


Figure 10 - Modèle de gestion d'identité : « méta-identité »

Cette approche est un moyen de faciliter l'intégration de différents domaines d'identité, comme lors de la fusion de plusieurs organisations. Ainsi, le modèle de méta-identité permet à des domaines d'identité isolés de mettre en commun des informations et éviter la réplication des informations. Dans le cadre de l'exemple d'identité isolée décrit précédemment, la mise en œuvre d'un domaine de méta-identité « Chercheur » permet d'unifier les informations fournies par les fournisseurs d'identité « Crac » et « Doc ». La gestion de ces informations est alors déléguée au fournisseur de méta-identité « Chercheur ». Par ailleurs, le fournisseur de service « Crac » doit être capable d'établir une correspondance entre l'identifiant fourni « jean.perrin@uuu.cnrs.fr » et le méta-identifiant « fsd15f7s51f2s74 » afin de pouvoir accepter le justificatif d'identité sous forme de certificat numérique. De même, le fournisseur de service « Doc » doit pouvoir faire le lien entre l'identifiant fourni « jb.perrin@uuu.cnrs.fr » et le méta-identifiant « fsd15f7s51f2s74 ». Pour le chercheur, le domaine de méta-identité permet de gérer moins de justificatifs d'identité. Cependant, contrairement aux modèles d'identité fédérée ou commune, la personne doit continuer à utiliser des identifiants différents. Pour le CNRS, cette architecture permet de restreindre le volume de données, mais la difficulté est de mettre en place un mécanisme qui permet de lier les informations gérées par le fournisseur d'identité « Crac » à celles du fournisseur d'identité « Doc ».

Tableau VI - Synthèse de l'exemple pour le modèle de méta-identité

Fournisseur de service	**Crac**	**Doc**	**Bdg**	**Ddm**	**Ret**	**Cge**
Domaine d'identité	Crac	Doc	Bdg	Ddm	Ret	Cge
Fournisseur d'identité	IdP Crac	IdP Doc	IdP Bdg	IdP Ddm	IdP Ret	IdP Cge

Fournisseur de service	**Crac**	**Doc**	**Bdg**	**Ddm**	**Ret**	**Cge**
Nom	PERRIN		PERRIN		PERRIN	PERRIN
Prénom	Jean-Baptiste		J.B.		Jean-Baptiste	JB
Affectation	Unité *uuu*		Unité *xxx*		CNRS	
Identifiant fourni	jean.perrin @*uuu*.cnrs.fr	jb.perrin @*uuu*.cnrs.fr	jean.perrin @*xxx*.cnrs.fr	j-b.perrin @xxx.cnrs.fr	153545	JPB
Domaine de méta-identité	Chercheur		DU		RH	
Méta-identifiant	fsd15f7s51f2s74		dg4d5h7d54s2		23s4fgsd564fds6	
Justificatif de méta-identité	Certificat numérique *uuu*.cnrs.fr		Certificat numérique *xxx*.cnrs.fr		« Je@nPerr1n »	

- ***Single Sign-On (SSO)***

L'approche Single Sign-On est similaire à une fédération d'identité, mais aucune correspondance d'identité n'est nécessaire, car il n'existe qu'un seul fournisseur d'identité. Dans cette architecture, un utilisateur n'a besoin de s'authentifier qu'une seule fois (en anglais « single sign-on ») auprès d'un fournisseur de service. Il est alors authentifié *de facto* auprès des autres fournisseurs de service.

Le modèle Single Sign-On peut être associé au modèle de fédération d'identité, permettant une authentification unique inter-domaine.

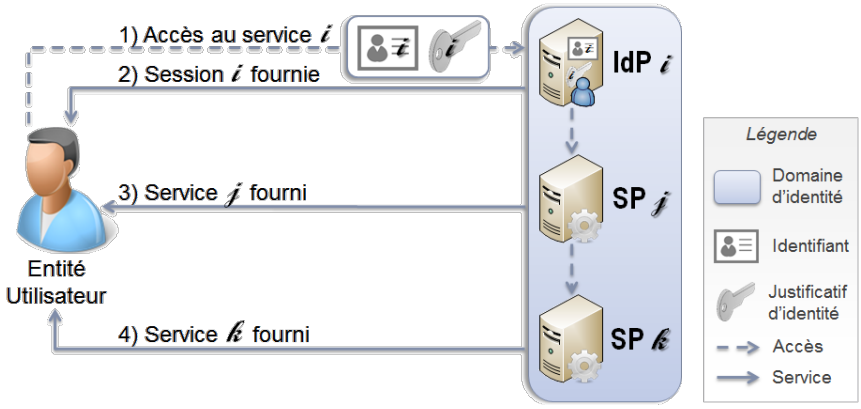


Figure 11 - Modèle de gestion d'identité : « Single Sign-On »

Dans le cadre de l'exemple décrit précédemment, ce modèle d'identité permet au chercheur d'utiliser un unique couple identifiant-justificatif d'identité quel que soit le service demandé au sein du domaine d'identité. Ainsi, comme dans le cas d'une fédération, le CNRS peut déployer un domaine de SSO « Chercheur CNRS » pour l'ensemble des services liés aux activités de chercheur. Dans ce cas, la personne ne manipule qu'un seul couple identifiant-justificatif d'identité (« jean.perrin@*uuu*.cnrs.fr » - Certificat numérique « *uuu*.cnrs.fr ») lors de la connexion au service « Crac ». L'identité correspondante (« Chercheur CNRS ») est alors automatiquement reconnue par le service « Doc », permettant au chercheur de l'utiliser sans phase d'authentification préalable.

Tableau VII - Synthèse de l'exemple pour le modèle de Single Sign-On

Fournisseur de service	**Crac**	**Doc**	**Bdg**	**Ddm**	**Ret**	**Cge**
Domaine d'identité	Chercheur		DU		RH	
Fournisseur d'identité	IdP Chercheur		IdP DU		IdP RH	
Nom	PERRIN		PERRIN		PERRIN	
Prénom	Jean-Baptiste		J.B.		Jean-Baptiste	
Affectation	Unité *uuu*		Unité *xxx*		-	
Identifiant fourni	jean.perrin@*uuu*.cnrs.fr		j-b.perrin@*xxx*.cnrs.fr		153545	
Justificatif d'identité fourni	Certificat numérique *uuu*.cnrs.fr		Certificat numérique *xxx*.cnrs.fr		« Je@nPerr1n »	

II.1.3 Cadre réglementaire

La loi française Informatique et Libertés n° 78-17 du 6 janvier 1978 modifiée par la loi du 6 août 2004 définit les principes à respecter lors de la collecte, du traitement et de la conservation des données personnelles. Cette loi est applicable dès qu'il existe un traitement automatisé ou un fichier manuel, c'est-à-dire un fichier informatique ou un fichier « papier » contenant des informations personnelles relatives à des personnes physiques.

La Commission Nationale Informatique et Libertés (CNIL) veille à la mise en œuvre des principes de la loi Informatique et Libertés dont ceux :

- de pertinence des données : « les données personnelles doivent être adéquates, pertinentes et non excessives au regard des objectifs poursuivis »,
- de durée limitée de conservation de données : « les informations ne peuvent pas être conservées de façon indéfinie dans les fichiers informatiques ; une durée de conservation doit être établie en fonction de la finalité de chaque fichier » (par exemple : le temps de la présence du salarié pour une application de gestion des carrières, cinq ans pour un fichier de paie, deux ans après le dernier contact avec le candidat à un emploi pour un fichier de recrutement),
- de sécurité et de confidentialité : « l'employeur, en tant que responsable du traitement, est astreint à une obligation de sécurité : il doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation à des tiers non autorisés ». L'article 34 précise que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».
- du principe de transparence : la loi garantit aux personnes l'accès à l'information relative aux traitements auxquels sont soumises des données les concernant et les assure de la possibilité d'un contrôle personnel. Le responsable de traitement des données personnelles doit avertir ces personnes dès la collecte des données et en cas de transmission de ces données à des tiers.

L'article 226-17 du code pénal réprime la non observation de ces principes de précaution par des dispositions particulièrement lourdes. En effet, « le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ». Par ailleurs, l'article 226-22 est également applicable, suite à la plainte d'une victime d'indiscrétion, même s'il s'agit d'une simple négligence. Il précise que « le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la

divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

Le Correspondant Informatique et Libertés (CIL) se positionne en intermédiaire entre le responsable des traitements des données concernées et la CNIL. Il doit avoir une connaissance approfondie de l'organisation responsable des traitements. De ce fait, il doit être un employé. Il est responsable de la création et de la mise à jour de la liste des traitements effectués, ainsi que de la publication de cette liste. Il veille également au respect des principes de la protection des données personnelles. Il a un rôle d'information pour les personnes au sujet de l'existence de leurs droits d'accès, de rectification et d'opposition.

II.2 Gestion des accès

II.2.1 Définitions

II.2.1.1 Ressources et gestion des accès

Afin de permettre de réaliser ses projets en toute sécurité, une organisation doit gérer les accès aux ressources dont elle dispose.

Comme évoqué précédemment lors de la définition du concept d'identité, une ressource désigne un fournisseur de service identifié par un libellé tel qu'un système d'information ou de communication. La gestion des accès permet de s'assurer de mettre à disposition de chacune des personnes impliquées dans les projets de l'organisation, à tout instant, tous les moyens nécessaires à la réalisation de la mission qui leur a été confiée, et que ces moyens soient à chaque instant limités au juste nécessaire [7].

Par la politique de gestion des accès, les accès aux ressources sont limités par des contraintes établies par l'organisation dont les définitions sont développées dans les paragraphes suivants :

- Mode d'authentification et contrôle d'accès ;
- Périmètre d'accès ;
- Rôles, profils et groupes autorisés.

II.2.1.2 Comptes utilisateurs

Un compte est un ensemble d'informations composé d'« un identifiant, un mot de passe (ou un justificatif d'identité d'une autre nature) et plusieurs attributs supplémentaires en fonction de l'environnement dans lequel il est créé » [8]. Un compte peut donc être la représentation informatique d'une identité. Il existe trois principaux types de comptes : le compte utilisateur, le compte d'administration et le compte de service.

Le compte utilisateur est associé à une entité utilisateur. Il est utilisé pour se connecter aux ressources d'un contexte auprès desquelles la personne est habilitée.

Le compte global est un compte utilisateur unique qu'une personne utilise pour tous les processus d'authentification et autorisation de l'ensemble des ressources de l'organisation.

Le compte d'administration permet à une entité d'accéder à une unique ressource et d'en assurer la gestion. Cependant, il n'est pas associé à une entité, ce qui implique qu'il ne doit pas être connu des référentiels d'identité. Son utilisation doit être limitée aux tâches techniques qui ne peuvent pas être réalisées au travers des rôles (cf. définition ci-après) d'administration. Il est souvent créé lors de l'installation d'une application avec des valeurs d'attributs prédéfinies. C'est pour cette raison qu'il

est préférable de désactiver tous les comptes de cette nature. En effet, les mots de passe étant affectés avec une valeur par défaut à l'installation, ils sont connus de tous et présentent donc une faille de sécurité importante [9].

Le compte de service fonctionnel ou technique est associé à une entité ressource. Il permet de s'authentifier (ou simplement s'identifier) auprès d'une autre ressource pour accéder à ses services. Les droits d'accès octroyés à ce compte sont limités. Aucune personne n'est autorisée à utiliser ce type de compte.

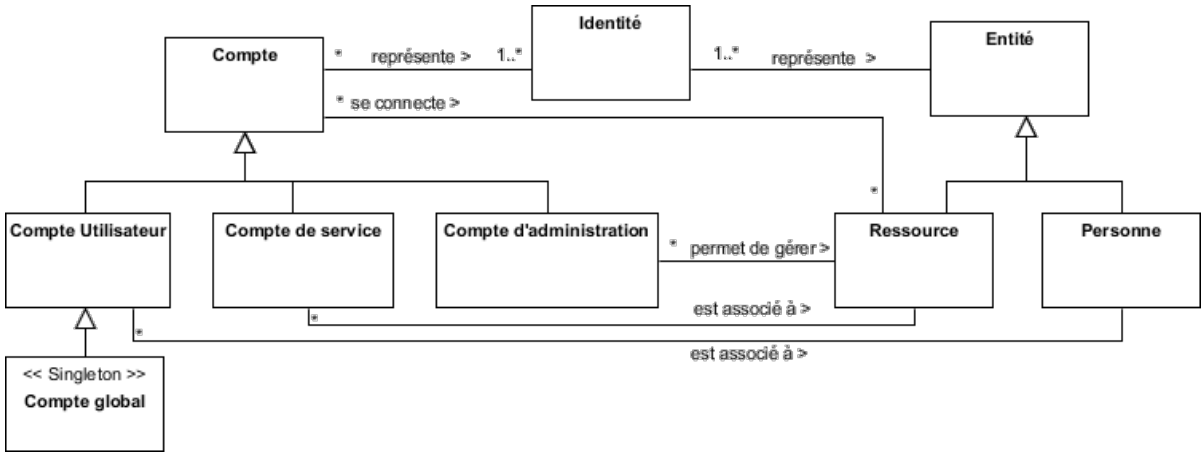


Figure 12 - Diagramme de classe des comptes

II.2.1.3 Habilitations et contrôle d'accès

Le CLUSIF [8] décrit une habilitation comme un droit d'effectuer une action sur une ressource. Elle est associée à un périmètre qui limite quand et comment cette ressource peut être utilisée par une entité. Les habilitations sont attribuées en fonction des besoins des métiers au sein de l'organisation.

F. Ferraiolo, D. R. Kuhn et R. Chandramouli [10] définissent un contrôle d'accès comme un processus pour vérifier les habilitations affectées à une entité.

Les contrôles d'accès sont un des moyens d'assurer la sécurité de l'information qui peut être définie par trois concepts complémentaires :

1. La confidentialité est l'assurance qu'une information ne peut être lue que par les entités qui en ont le droit ;

[9] G. Harry. *Failles de sécurité des applications Web*. CNRS, 38 pages, 2012

[10] D. F. Ferraiolo, D. R. Kuhn, R. Chandramouli. *Role-Based Access Control, Second Edition*. Artech House, 381 pages, 2007

2. L'intégrité est la protection de l'information contre des modifications par des entités qui n'en ont pas le droit ;
3. La disponibilité est la capacité à mettre l'information à disposition quand les entités en ont besoin.

   Les contrôles d'accès permettent d'assurer la confidentialité et l'intégrité de l'information. La disponibilité de l'information dépend de celle des mécanismes mis en œuvre pour assurer les contrôles d'accès. En effet, si le moyen de réaliser les contrôles d'accès est inutilisable, alors l'information ne peut être ni lue, ni modifiée, la rendant indisponible.

II.2.1.4 Rôle, profil, groupe et périmètre

Les termes de rôle, de profil et de groupe sont souvent confondus, alors que ce sont des concepts manipulés régulièrement dans la gestion des identités et des accès.

Un rôle est un ensemble d'habilitations nécessaires à un type d'utilisation d'une ressource. Un rôle applicatif est un rôle propre à une seule fonction et appartient à une seule application. Il est recommandé d'utiliser les rôles applicatifs comme unique moyen d'accorder des habilitations à un compte. De ce fait, les rôles permettent de maîtriser les permissions octroyées et de déceler les conflits entre les droits.

De même, un rôle ne doit pas être octroyé directement à un compte utilisateur. Il est préférable de les attribuer au travers des profils métiers qui regroupent l'ensemble des rôles nécessaires à la réalisation d'une mission. Un profil correspond donc généralement à une fonction exercée au sein d'une organisation.

Lorsque des entités doivent obtenir les mêmes habilitations spécifiques, mais que leurs profils ne correspondent pas, elles peuvent être regroupées en groupes statiques ou dynamiques. Par exemple, des personnes participant à un projet ont besoin de pouvoir partager des documents au sein d'un espace de travail collaboratif. Un groupe statique est constitué par une liste exhaustive des comptes utilisateurs devant obtenir une habilitation particulière. L'utilisation de ce type de groupe n'est pas recommandée lorsque la liste doit évoluer souvent. Dans ce cas, il est préférable d'opter pour un groupe dynamique qui est généré sur la base d'un critère tel que la présence ou la valeur d'un attribut dans les comptes utilisateurs. Dans le cadre de l'exemple sur les projets, tous comptes utilisateurs possédant l'attribut « Administrateur Système et Réseau » font partie du groupe du même nom qui leur donne le droit de déposer et de modifier des documents dans le répertoire « Architecture informatique » et leur permet également de lire tous les comptes-rendus d'avancement du projet. Par contre, une liste statique de comptes utilisateur établie quels sont ceux

qui ont la capacité de déposer et modifier ces comptes-rendus. Les groupes permettent donc de faciliter la gestion massive d'habilitations indépendamment des rôles.

Comme évoqué précédemment, une habilitation est soumise à un périmètre applicatif qui restreint les capacités d'utilisation d'une ressource.

Le périmètre temporel interdit les accès à une ressource en dehors des périodes autorisées. Il peut être assigné à un compte utilisateur, un rôle ou une ressource. Les restrictions sont exprimées en fonction de trois critères cumulables :

- La période, définie par une date de début et une date de fin, n'autorise l'utilisation de la ressource cible que si la tentative d'accès est opérée entre ces deux dates ;
- La plage horaire, définie par une heure de début et une heure de fin, n'autorise l'utilisation de la ressource cible que si la tentative d'accès est réalisée entre les heures spécifiées ;
- Le calendrier, défini par une liste de jours calendaires, une liste de semaines ou une liste de mois, n'autorise l'utilisation de la ressource cible que si la tentative d'accès est opérée un jour appartenant à une des listes citées.

  Le périmètre géographique limite les accès à une ressource en fonction du lieu à partir duquel un utilisateur tente de se connecter. Il peut être affecté à un compte ou un rôle. L'ensemble des habilitations liées au profil du compte utilisateur évolue alors en fonction du lieu de présence de la personne auquel il appartient, permettant ainsi par exemple d'empêcher la manipulation d'informations confidentielles à partir de points d'accès non fiables. Les restrictions sont de trois types :

- Le poste de travail physique, identifié par un numéro d'inventaire ou une adresse IP, à partir duquel l'organisation souhaite autoriser ou interdire certaines opérations ;
- Un lieu, un groupe de lieu ou une zone géographique dans laquelle le poste de travail doit se situer lors de la tentative de connexion pour obtenir le droit d'utiliser la ressource cible ;
- Une typologie d'accès pour permettre les accès à la ressource. Il peut s'agir d'un accès par le réseau de l'organisation, un réseau mis à disposition par un partenaire ou un réseau privé dédié.

  Le périmètre fonctionnel limite l'exécution de traitements applicatifs en fonction de la valeur ou de la nature des informations fournies en paramètre. Il peut être assigné à un rôle. Les données peuvent être relatives par exemple à un secteur géographique, à l'affectation au sein de l'organisation ou au type d'appareil utilisé pour se connecter.

II.2.1.5 Authentification et autorisation

Comme évoqué lors de la définition de la gestion d'identité, l'authentification est le processus qui permet de vérifier que l'identité revendiquée par une entité est légitime. Elle est basée sur un ou plusieurs mécanismes de reconnaissance :

- Quelque chose que l'entité connaît comme par exemple un mot de passe ou un numéro personnel d'identification (code PIN) ;
- Quelque chose que l'entité possède, telle qu'une carte ou une clé ;
- Une caractéristique physique telle qu'une empreinte digitale ou rétinienne.

L'authentification est plus sûre si plusieurs techniques sont utilisées conjointement [8]. En effet, un mot de passe peut être deviné, une clé peut être perdue et une reconnaissance faciale peut être faussée à cause des marges d'erreur. Aussi, l'utilisation d'une technique ne fournit pas un niveau de sécurité suffisant. Il faut en utiliser plusieurs pour diminuer les risques d'erreur ou de falsification. Le mode d'authentification peut être déterminé en fonction du rôle associé aux comptes utilisateurs ou de la ressource utilisée.

L'autorisation est le processus responsable d'établir les habilitations dont dispose une identité au travers d'un compte et du profil qui lui est associé ou des groupes auxquels il appartient. Ce processus détermine donc ce qu'une identité a le droit de faire pour chacune des ressources qui lui est mise à disposition. Des modèles d'autorisation d'accès sont exposés dans le paragraphe « Modèles des gestions d'accès ».

Ces deux concepts sont utilisés conjointement pour les contrôles d'accès, le processus d'autorisation étant dépendant du bon fonctionnement de l'authentification. En effet, si le moyen d'authentifier une identité n'est pas sûr, alors il n'est pas possible de garantir que les autorisations soient accordées à la bonne entité. Dans ce cas, le contrôle d'accès ne permet pas d'assurer la confidentialité et l'intégrité des informations qu'il doit protéger.

II.2.1.6 Exemples dans le contexte CNRS

Pour la gestion des unités, le CNRS met à disposition plusieurs ressources : un service de gestion du budget de l'unité nommé « Bdg » et un service de rapports décisionnels pour le pilotage de l'organisme nommé « Rpt ». Le service « Bdg » offre la possibilité de saisir des commandes et de produire des rapports analytiques détaillés ou synthétiques sur les dépenses et les subventions. Pour se connecter à ce service, il est nécessaire de disposer d'un compte. Ainsi, pour un directeur d'unité connu sous l'identité « Directeur de l'unité *xxx - J.B. Perrin* » un compte utilisateur « Bdg-JBP » est créé. Pour son assistante, le CNRS produit l'identité « Gestionnaire de l'unité *xxx - G. Mineur* » à laquelle est lié le compte utilisateur « Bdg-GM ». Par ailleurs, le CNRS dispose

d'une équipe de la production applicative responsable du maintien en condition opérationnelle (MCO) des ressources à laquelle appartient l'« Exploitant Joseph Licklider ». A ce titre, l'équipe dispose d'un compte d'administration « Bdg-ADMIN ». De plus, pour produire des rapports au niveau de l'établissement, la ressource « Rpt » doit accéder à la ressource « Bdg », ce qui est réalisable au travers du compte de service « Bdg-READ ».

Tableau VIII - Exemple de comptes utilisateurs

Compte **Information**	**Bdg-GM**	**Bdg-JBP**	**Bdg-READ**	**Bdg-ADMIN**
Identité représentée	Gestionnaire de l'unité *xxx* *G. Mineur*	Directeur de l'unité *xxx* *J.B. Perrin*	Ressource « Rpt »	*Non applicable*
Nom	G. Mineur	J.B. Perrin	Rapport	ADMIN
Unité	Unité *xxx*	Unité *xxx*	CNRS	Production applicative
Type de compte	Utilisateur	Utilisateur	Service	Administration
Personne manipulant le compte	Gabrielle MINEUR	Jean-Baptiste PERRIN	*Non applicable*	Joseph LICKLIDER
Ressource cible	Service « Bdg »	Service « Bdg »	Service « Bdg »	Service « Bdg »
Identifiant	GM	JBP	READ	ADMIN
Justificatif d'identité	« G@brie11e »	« @zer1yuioP »	« f&jdsu_oehyè »	« myEXP1@cnt »

Le service « Bdg » offre la possibilité de :

- lire (action « read ») ou saisir/modifier (action « write ») des commandes pour un périmètre fonctionnel limité à l'unité et à l'année,
- lire (action « read ») ou saisir/modifier (action « write ») les crédits alloués pour un périmètre fonctionnel limité à l'unité et à l'année,
- lire (action « read ») ou générer (action « execute ») des rapports sur le budget pour un périmètre fonctionnel limité à l'unité,
- lire (action « read ») les informations techniques des journaux évènementiels,
- Démarrer et arrêter (action « execute ») le service « Bdg ».

Les habilitations liées à ces fonctionnalités sont octroyées au travers de rôles valides uniquement pour la ressource « Bdg ». Le tableau suivant montre l'affectation des habilitations et leur périmètre sur les rôles « Intendance unité », « Responsable unité », « Lecture budget unité », « Rapport budget unité » et « MCO ».

Tableau IX - Exemple de rôles applicatifs

Profil Rôle	Intendance unité	Responsable unité	Lecture budget unité	Rapport budget unité	MCO
Périmètre	Unité	Unité	Unité	Unité	-
Commandes	read, write	-	read	-	-
Crédits	-	read,write	read	-	-
Rapport	-	-	read	execute	-
Informations techniques	-	-	-	-	read
Service	-	-	-	-	execute

Un compte utilisateur ayant le profil « Directeur d'unité », tel que « Bdg-JBP », doit obtenir les habilitations à saisir les crédits alloués à son unité, à lire tout type d'information liées à son unité durant son mandat et à en générer les rapports. Pour ce faire, ce profil se voit octroyer les rôles « Responsable unité », « Lecture budget unité » et « Rapport budget unité ». Conjointement, un compte utilisateur ayant le profil « Gestionnaire », tel que « Bdg-GM », doit obtenir l'habilitation à saisir des commandes et à visualiser des rapports sur le budget de l'unité d'affection et l'année en cours. A cet effet, ce profil dispose des rôles « Intendance unité » et « Lecture budget unité ». Un compte ayant le profil « Lecture », tel que le compte de service « Bdg-READ », doit disposer des

habilitations permettant de lire des informations budgétaires pour l'ensemble des unités dans l'application « Bdg ». Pour répondre à ce besoin, ce profil dispose du rôle « Lecture budget unité » sur l'ensemble des unités enregistrées. Un compte d'administration, utilisé notamment par l'« Exploitant Joseph Licklider », doit être habilité à démarrer et arrêter le service « Bdg », à accéder aux informations techniques liées aux évènements applicatifs et à pouvoir lancer la génération de rapports en cas de défaillance. Ainsi, le profil « Production applicative » possède les rôles « MCO » et « Rapport budget unité ».

Tableau X - Exemple de profils

Profil Rôle	Gestionnaire	Directeur d'unité	Lecture	Production applicative
Intendance unité	Périmètres unité, année	-	-	-
Responsable unité	-	Périmètres unité, année	-	-
Lecture budget unité	Périmètres unité, année	Périmètres unité, année	Sans limite	-
Rapport budget unité	-	Périmètres unité, année	-	Périmètres unité, année
MCO	-	-	-	Sans limite

II.2.2 Modèles

Comme évoqué précédemment, le contrôle des accès revêt plusieurs aspects pour assurer la sécurité des ressources et des informations. Il repose sur l'utilisation de différentes notions telles que les identités avec les modèles IBAC, les rôles avec le modèle RBAC ou les périmètres avec des modèles tels qu'ABAC ou OrBAC.

II.2.2.1 Identity based access control (IBAC)

F. Cuppens et N. Cuppens-Boulahia [11] présentent le modèle IBAC comme étant historiquement le premier type de contrôle d'accès. Bien qu'introduit par B. Lampson en 1971, il

[11] F. Cuppens, N. Cuppens-Boulahia. Les modèles de sécurité. Dans *Sécurité des systèmes d'information, (Traité IC2, série Réseaux et télécoms)*. Hermès, pages 13-48, 2006

est toujours utilisé par les systèmes d'exploitation sur les marchés des ordinateurs personnels, avec Microsoft Windows par exemple, et des serveurs avec les systèmes Unix et Linux. Ce modèle repose sur une matrice composée d'un ensemble fini d'entités, de ressources cibles et de règles. Il conduit à l'établissement d'une liste exhaustive d'autorisations d'accès (ACL : « Access control list » en anglais). Cela implique que tout accès non explicitement autorisé est interdit. Ainsi, les habilitations sont affectées directement aux comptes utilisateurs. Ainsi chaque droit est assigné nominativement.

Le tableau suivant est un exemple de matrice ACL pour les comptes utilisateurs et habilitations décrits dans l'exemple décrit précédemment. Ainsi le directeur de l'unité *xxx* nouvellement nommé ne pourra saisir les crédits que pour l'année en cours mais pourra consulter les crédits et rapports de l'ensemble des années.

Tableau XI - Exemple de matrice ACL du modèle IBAC

	Bdg-GM	**Bdg- JBP**	**Bdg-READ**	**Bdg-ADMIN**
Commandes unité *xxx* 2011	read, write	read	read	-
Commandes unité *xxx* 2012	read, write	read	read	-
Crédits unité *xxx* 2011	read	read	read	-
Crédits unité *xxx* 2012	read	read, write	read	-
Rapport unité *xxx* 2011	read	read	-	execute
Rapport unité *xxx* 2012	read	read,execute	-	execute
Informations techniques	-	-	-	read
Service	-	-	-	read

Une des implémentations du modèle IBAC est le contrôle d'accès discrétionnaire (DAC : « Discretionary Access Control » en anglais) qui repose sur la notion de propriétaire de la ressource. Ce dernier a le contrôle total sur la ressource qu'il a créée et dont il est responsable. Il détermine ainsi quelle entité a droit à quel type d'action sur sa ressource.

La complexité des ACLs augmente en fonction du nombre d'identités et du nombre de ressources puisqu'il faut lister exhaustivement les autorisations pour chacune des combinaisons. En effet, lors la mise à disposition d'une nouvelle ressource ou à l'arrivée d'un nouvel utilisateur, la liste des autorisations doit être mise à jour. Les modèles qui suivent permettent de faciliter la gestion des habilitations.

II.2.2.2 Mandatory Access Control (MAC)

Dans le cas où le propriétaire d'un système d'information ne doit pas être responsable de la gestion de la sécurité sous-jacente, les modèles de type MAC permettent de limiter les accès en fonction de la sensibilité des données. Dans cet objectif, les entités cibles sont hiérarchisées en différents niveaux de sécurité (MLS : « multi-level security » en anglais) appelés labels.

En 1973, D. Bell et L. LaPadula ont développé un modèle où un niveau minimum de sécurité est requis pour avoir le droit d'accéder à la ressource. Ce niveau définit le niveau d'habilitation de l'utilisateur. De même, un niveau de sécurité est affecté à la ressource. Ce niveau détermine le niveau de classification de la ressource. L'utilisateur n'a alors accès à la ressource que si son niveau d'habilitation est supérieur ou égal au niveau de classification de la ressource. De plus, pour une application, un niveau d'exécution, appelé niveau courant, est également défini. Le niveau courant d'une application est toujours inférieur ou égal au niveau d'habilitation de l'utilisateur responsable de l'exécution de l'application. La condition « no read up » implique qu'une application ne peut accéder en lecture à des informations que si le niveau courant de l'application est supérieur ou égal au niveau de classification de la ressource qui gère ces données. De même, la condition « no write down » suppose qu'une application ne peut transmettre des informations à une ressource que si son niveau courant est inférieur ou égal au niveau de classification de la ressource cible. Ce modèle de contrôle des accès est également appelé Rule Based Access Control (RuBAC), car les accès sont régis par des règles.

Dans le cadre des restrictions évoquées dans l'exemple de comptes utilisateurs décrit précédemment, les niveaux d'habilitation peuvent être définis sur cinq niveaux. Ainsi, les informations gérées par la ressource « Bdg » sont classifiées de niveau 3. Les comptes utilisateurs devant s'y connecter doivent donc disposer d'une habilitation de niveau supérieur ou égal à 3. Ainsi, le compte « Bdg-GM » dispose du niveau d'habilitation 4, « Bdg-JBP » du niveau d'habilitation 5. Le compte « Bdg-ADMIN » responsable de l'exécution du service a un niveau d'habilitation minimum, ce qui implique qu'il a le niveau d'habilitation 3. Le niveau courant de l'application « Bdg » doit donc être inférieur ou égal au niveau d'habilitation 3 du compte « Bdg-ADMIN ». Pour respecter la contrainte « no read up », le niveau courant de l'application « Bdg » doit également être supérieur au niveau de classification 3 des informations, ce qui implique que le niveau courant de l'application doit être fixé à 3. Par ailleurs, la contrainte « no write down » implique que la ressource « Rpt », qui doit être en mesure lire des données de la ressource « Bdg », doit avoir un niveau de classification supérieur ou égal au niveau courant 3 de l'application « Bdg ». De plus, étant établi que l'accès aux informations de la ressource « Rpt »

requiert le niveau d'habilitation le plus élevé, le niveau de classification de la ressource « Rpt » est imposé à 5 obligeant à définir le niveau courant de l'application « Rpt » à 5.

Tableau XII - Exemple d'implémentation du modèle MAC

Niveau	Compte « Bdg-GM »	Compte « Bdg-JBP »	Compte « Bdg-ADMIN »	Ressource « Bdg »	Ressource « Rpt »
Habilitation	4	5	3		
Classification				3	5
Courant				3	5

En 1986, D. Bell propose une version étendue de ce modèle où le niveau courant d'une application n'est plus déterminé par un unique niveau mais par un intervalle de niveaux, ce qui offre plus de flexibilité. Dans ce cas, une application peut accéder en lecture à toute information dont la classification est comprise entre la borne inférieure et la borne supérieure du niveau courant de l'application. Ce modèle est proche de celui utilisé actuellement par le système de gestion de bases de données Oracle via l'option Label Security pour segmenter les données.

II.2.2.3 Role Based Access Control (RBAC)

Contrairement au modèle IBAC où les habilitations sont octroyées directement à l'utilisateur, dans le modèle RBAC, élaboré par le National Institute of Standards and Technology (NIST) à partir de 1992 [9], les habilitations sont affectées à des rôles. La gestion des habilitations est alors simplifiée. En effet, par exemple, lors de l'enregistrement d'un nouvel utilisateur, il suffit de lui attribuer les rôles nécessaires à la réalisation de sa mission au lieu de lui octroyer l'ensemble des habilitations sous-jacentes. Ainsi, dans l'exemple des rôles applicatifs, lors de sa prise de fonction, un gestionnaire se voit attribuer le rôle « Intendance unité » au travers de son compte utilisateur. Il a alors accès en lecture, en saisie aux commandes de l'unité pour l'année en cours.

Par ailleurs, le NIST propose plusieurs déclinaisons du modèle RBAC [12]. Le modèle RBAC hiérarchique (HRBAC : « hierarchical role based access control » en anglais) prend en compte les liens de parenté entre rôles. Ainsi lorsqu'une habilitation est octroyée ou enlevée à un rôle parent, les rôles fils en héritent et acquièrent, ou respectivement perdent, cette habilitation. HRBAC supporte deux types de hiérarchie. La variante générale (« General Hierarchical RBAC » en anglais) accepte des héritages ascendants et descendants multiples. Par opposition, dans la

[12] D. F. Ferraiolo , R. Sandhu , S. Gavrila , D. R. Kuhn , R. Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security* v.4 n.3, pages 224-274, 2001

variante limitée (« Limited Hierarchical RBAC » en anglais) un rôle ne peut hériter que d'un seul parent. Dans le cadre de l'exemple des rôles applicatifs, le rôle « Lecture budget unité » est commun aux profils « Gestionnaire » et « Directeur d'unité ». Ce rôle est donc nécessaire lorsque les rôles « Intendance unité » et « Responsable unité » sont affectés. La modélisation de ces rôles peut alors être simplifiée en définissant « Lecture budget unité » comme rôle parent de « Intendance unité » et « Responsable unité ». Seuls ces deux derniers rôles sont alors octroyés, car ils héritent des habilitations du rôle parent « Lecture budget unité ».

La seconde déclinaison du modèle RBAC permet la gestion des conflits d'intérêts induits par des rôles incompatibles octroyés à un même utilisateur. En effet, le modèle RBAC avec contraintes (CRBAC : « constrained role based access control » en anglais) assure la séparation des responsabilités (SoD : « Segregation of Duty » en anglais) en empêchant le cumul d'habilitations contradictoires. Ainsi, dans les exemples de rôle décrits précédemment, un compte ne peut pas être associé en même temps aux rôles « Intendance unité » et « Responsable unité » qui représentent deux fonctions dans l'organisme qui ne peuvent être exercées par une seule personne au sein d'une unité. Par ailleurs, la mise en œuvre de la séparation statique des responsabilités (en anglais : « static separation of duty ») implique la définition de règles d'affectation de rôles. L'administrateur responsable des accès ne peut alors pas affecter des rôles incompatibles. Ainsi un utilisateur appartenant à un rôle ne peut pas se voir attribué un rôle rendu interdit par ces règles. La séparation dynamique des responsabilités (en anglais : « dynamic separation of duty ») permet de ne pas retirer un rôle en cas de non-respect des règles, mais simplement de le révoquer temporairement au moment où l'utilisateur demande à se connecter à la ressource.

La mise en place d'un système de contrôle d'accès basé sur le modèle RBAC au sein d'une organisation requiert la mise en œuvre d'une stratégie de définition des rôles (en anglais : « role engineering ») qui n'est pas une tâche aisée. Il existe deux principaux types d'approche « bottom-up » (du bas vers le haut) et « top-down » (du haut vers le bas) complétés par des approches hybrides.

Pour les organisations disposant déjà d'un système de gestion des droits d'accès la démarche bottom-up permet de construire des rôles en examinant les habilitations existantes. Des outils de rolemining permettent d'accélérer cette recherche [13]. Ils exploitent des algorithmes de datamining, chacun ayant un objectif différent, tel que minimiser le nombre de rôles découverts, établir les hiérarchies de rôles ou découvrir un nombre faible de rôles possédant le plus grand dénominateur commun d'habilitations. Cependant les droits inutilisés résiduels peuvent perturber

[13] M. Frank, J. M. Buhmann , D. Basin. On the definition of role mining. *Proceeding of the 15th ACM symposium on Access control models and technologies*, pages 35-44, 2010

cette analyse et mener à des définitions de rôles qui n'ont aucune correspondance avec des concepts métier.
A l'inverse, la démarche top-down étudie par itérations successives les fonctions métiers pour en déduire les habilitations et les rôles inhérents. La difficulté réside alors dans l'exhaustivité et la granularité des rôles. En effet, des rôles trop larges admettent trop de droits et des rôles trop restreints vont augmenter la difficulté d'administration.
L'approche hybride consiste à rechercher les rôles par l'approche bottom-up et les affiner ensuite par confrontation avec les informations collectées par l'approche top-down.

Le modèle RBAC est aujourd'hui un standard qui permet notamment la mise en conformité vis-à-vis de la loi Sarbanes-Oxley (cf. paragraphe « cadre réglementaire »). Il s'adresse plus particulièrement aux organisations dont la définition des métiers et des missions est figée et évolue peu. Dans le cas contraire, des exceptions seront nécessaires pour autoriser des accès spécifiques ou temporaires. Cette situation implique la mise en place d'une liste annexe de contrôle d'accès, comme dans le modèle IBAC. Il n'est alors plus possible de se baser sur les définitions des rôles et des profils pour déterminer qui possède quel type d'accès sur quelle ressource.

II.2.2.4 Attribute Based Access Control (ABAC)

Le modèle ABAC, défini par L. Wang, D. Wijesekera, S. Jajodia [14], propose de définir les droits d'accès en fonction des caractéristiques des identités. A l'instar du modèle IBAC, la politique des droits d'accès peut être matérialisée par une matrice, mais en ne se basant pas sur les identités. De ce fait, les droits d'accès à une ressource ou un service sont définis pour un ou plusieurs attributs que les identités sont susceptibles de posséder. Ce paradigme offre donc plus de flexibilité. De plus, en définissant un attribut se rapprochant de la notion de rôle, ABAC permet de simuler le comportement d'un modèle RBAC, mais le généralise en ne limitant pas les droits d'accès aux seuls utilisateurs présents dans l'organisation. Il permet notamment de déterminer des droits d'accès avec une granularité plus fine. De plus, en définissant un rôle comme un ensemble d'attributs, il est plus facile de gérer les conflits. Par ailleurs, la gestion des droits d'accès est facilitée, car elle ne nécessite pas d'informations supplémentaires. Cependant, la sécurité des accès repose alors sur les valeurs affectées aux attributs et donc sur la qualité et l'intégrité des informations liées aux identités.

---

[14] L. Wang, D. Wijesekera, S. Jajodia. A logic-based framework for attribute based access control. *Proceedings of the 2004 ACM workshop on Formal methods in security engineering*, pages 45-55, 2004

Dans le cadre des exemples décrits précédemment, le modèle ABAC implique que l'attribution de l'attribut « Directeur d'unité » à un compte utilisateur a pour effet de donner accès automatiquement aux lignes de crédits et rapports. L'attribut « Directeur d'unité » peut être perçu comme la matérialisation du profil « Responsable unité ».

II.2.2.5 Organization Based Access Control (OrBAC)

Avec le modèle OrBAC [11], l'organisation est perçue d'un point de vue abstrait comme un ensemble d'activités que les rôles ont la permission, interdiction ou obligation de réaliser au travers des vues. Tout comme dans RBAC, il est possible d'utiliser la notion d'héritage pour les rôles. Concrètement, les habilitations sont octroyées à des sujets pour des actions sur des objets au travers de matrices à trois dimensions.

Ce modèle semble permettre une gestion plus fine des droits d'accès, mais reste cependant peu implémentée.

II.2.2.6 Comparaison

Quelque soit le modèle implémenté au sein d'une organisation, l'objectif est de limiter la capacité d'action des entités utilisatrices des ressources au strict nécessaire pour réaliser leurs missions.

Dans le modèle IBAC, les contrôles d'accès reposent sur une liste exhaustive d'habilitations pour chaque compte autorisé.

Le modèle RBAC permet de diminuer la taille de liste des habilitations. Les contrôles d'accès sont réalisés sur les rôles attribués aux comptes. Les rôles applicatifs sont octroyés en fonction du profil métier.

Dans le modèle ABAC, les contrôles d'accès vérifient la présence et la valeur d'attributs applicatifs définis au niveau des comptes. Il est alors possible de simuler le comportement RBAC en calquant les attributs sur la définition des rôles.

Dans le modèle OrBAC les autorisations ou interdictions reposent sur des expressions contextuelles définies d'après la structure organisationnelle de l'établissement.

Le modèle MAC s'appuie sur le contrôle des flux. Des contraintes sont définies sur les données et les ressources. Le niveau d'habilitation d'un compte détermine alors s'il a le droit ou non d'accéder aux informations.

II.2.3 Cadre réglementaire

Bien que le CNRS ne soit pas concerné par les lois encadrant le comportement des entreprises privées, celles qui sont liées à la sécurité de l'information vont être exposées dans les paragraphes suivants afin de présenter les bénéfices et les contraintes liées à la gestion des accès. De plus, essayer de s'en rapprocher permet de diminuer les risques relatifs à la sécurité.

II.2.3.1 Loi américaine Sarbanes-Oxley

La loi Sarbanes-Oxley (SOx) fut votée par le congrès américain en juillet 2002 dans le but de redonner confiance aux investisseurs dans les marchés financiers suite aux scandales ENRON et WORLCOM. D. F. Ferraiolo, D. R. Kuhn et R. Chandramouli [9] précisent que la loi implique pour les entreprises cotées aux Etats-Unis et leurs filiales, y compris à l'étranger, ou qui empruntent sur le marché américain que les contrôles internes et les processus utilisés pour la production des rapports financiers soient certifiés auprès de la « Securities and Exchange Commission ». L'impact pour les systèmes d'information est un contrôle accru sur l'utilisation des logiciels dont l'organisation dépend pour ses données financières. Cela inclut également les outils de gestion des transactions, des données comptables, personnelles, d'inventaire et toute autre donnée qui peut être utilisée pour la production des rapports financiers. La surveillance doit assurer que tout changement soit opéré par une personne autorisée et selon un processus certifié.

Trois sections sont applicables aux systèmes d'information :

1. La section 302 implique que le comité exécutif certifie la complétude et l'exactitude des rapports financiers de l'organisation ;
2. La section 404 contraint l'organisation à maintenir « des procédures et des structures de contrôles internes adéquats pour la production de rapports financiers ». Les contrôles internes doivent être validés par des auditeurs externes pour assurer de leur authenticité, vérifier les renseignements sur site et avertir des insuffisances. Les responsables encourent des pénalités s'ils dissimulent l'absence ou l'insuffisance de contrôles ;
3. La section 409 requiert la présentation dans les plus brefs délais des rapports aux investisseurs et régulateurs de toute information concernant un changement dans les finances ou les opérations de l'organisation.

La section 404 de Sarbanes-Oxley est plus particulièrement liée à la gestion des identités et des accès. Dans ce paragraphe le terme « adéquat » concernant les contrôles internes n'est pas explicitement défini. Cependant, quelques bonnes pratiques sont citées dont les suivantes :

- Contrôles renforcés sur les identifiants et les permissions liées aux identifiants,

- Surveillance rigoureuse des attributions, mises à jour ou révocations de privilèges, incluant des capacités d'audit complet,
- Séparation des responsabilités pour l'accès ou la modification d'informations financières,
- Contrôle et audit des modifications présentant qui les a réalisées, quand et par quels moyens,
- Suivi et contrôle renforcé sur la mise à jour et les changements effectués sur les logiciels,
- Documentation sur la configuration et la maintenance des logiciels,
- Installation dès que possible des mises à jour de sécurité avec écriture dans les traces d'audit,
- Documentation complète sur les contrôles internes déficients qui réduisent les capacités de l'organisation à réaliser les objectifs cités précédemment.

La mise en œuvre de Sarbanes-Oxley peut être coûteuse, mais elle offre l'opportunité de mettre en place des processus internes sûrs. De plus, de part ces obligations, les organisations certifiées ISO-27001 (cf. paragraphe « Norme ISO-2700x ») respectent automatiquement Sarbanes-Oxley.

Les outils de gestion des identités et des accès des grands éditeurs sont compatibles avec la mise en conformité à Sarbanes-Oxley.

II.2.3.2 Accords internationaux Bâle II

Le comité Bâle sur le Contrôle Bancaire réunit les principales autorités de contrôle bancaire du monde. En 1988, il publia un premier accord, « Bâle I », sur la gestion des risques de crédit et la quantité de fonds propres minimaux pour les banques pour faire face à d'éventuelles pertes. En 1992, il fut décliné en différentes lois dans les pays du G10.

En 2004, le comité Bâle publia une seconde série d'accords, « Bâle II » qui prend en compte plus de catégories de risques et améliore le calcul et la gestion de ces risques [15]. Ils ont pour objectifs une meilleure transparence des entreprises, la protection des épargnants et un renforcement des contrôles. L'ensemble des obligations qui composent cette réforme est scindée selon trois piliers :

Pilier I : Disposer d'un montant de fonds propres pour couvrir les risques,

Pilier II : Les autorités disposent de pouvoirs renforcés pour imposer des exigences de fonds propres supérieurs à ceux envisagés par l'entreprise,

Pilier III : Obligation de publier des informations complètes sur la nature, le volume et les méthodes de gestion des risques ainsi que l'adéquation de leurs fonds propres.

---

[15] G. Chamoret, F. Chavoutier, M. Copitet, J-P Godard, P. Grassart, J. Mauferon, L. Mourer, T. Ramard, G. Remy. *La réforme BÂLE 2, une présentation générale*. CLUSIF, 28 pages, 2004

Pour être conforme au premier pilier, l'organisation doit disposer d'une analyse économique des risques pour en connaître et ensuite limiter les impacts sur son bilan. Les risques sont répartis en trois catégories : risques de crédit, risques de marchés et risques opérationnels. Ces derniers incluent les risques relatifs à la sécurité des biens et des personnes, les risques informatiques liés aux développements et à la maintenance des programmes, traitements et services de télécommunications.

Chaque étape du processus de gestion des risques doit être prise en compte : l'identification, l'analyse, le traitement ainsi que son financement. Par ailleurs, les paragraphes 670 à 676 précisent que l'estimation des risques doit reposer, entres autres, sur des bases d'incidents et de pertes couplées à des outils d'analyse de scénario. Les bases d'incidents permettent de disposer d'un historique des sinistres constatés et leur fréquence, ce qui permet d'assurer un suivi des évolutions des différents risques et des mesures correctrices mises en œuvre. Les outils d'analyse de scénario doivent aider à construire des modèles statistiques de prévision des risques à partir de l'historique de la base des pertes.

L'obligation de transparence du troisième pilier implique de rendre compte dans un rapport des procédures de gestion des risques mises en place, notamment du système de contrôle interne. Ce dernier doit assurer un suivi des risques opérationnels, dont celui de conflit d'intérêt. Pour cela, l'organisation doit implémenter un système d'approbations et d'autorisations pour veiller à la séparation des responsabilités. L'organisation doit également protéger les accès et l'utilisation des actifs et des informations détenus par la banque.

En 2010, une première version du troisième accord, « Bâle III », fut publiée. Il ajuste les exigences de fonds, mais ne prend pas en compte les origines de la crise des « subprime ». Son impact est faible sur les systèmes d'information conformes à Bâle II.

II.2.3.3 Loi de sécurité financière (LSF)

La loi française n° 2003-706 du 1 août 2003 de sécurité financière s'applique à toutes les sociétés anonymes ainsi qu'aux sociétés faisant appel à l'épargne publique. Elle ne s'applique donc pas aux grands groupes. A l'instar de la loi américaine Sarbanes-Oxley, la loi de sécurité financière repose principalement sur une responsabilité accrue des dirigeants, un renforcement du contrôle interne et une réduction des sources de conflits d'intérêt.

Le contrôle interne doit permettre l'amélioration de la communication en temps réel et la fiabilisation de la production d'informations, répondant ainsi au besoin de transparence. Pour cela, l'organisation doit être capable de retracer le processus de génération de l'information depuis l'origine des données jusqu'aux décisions qui s'en sont suivies.

L’organisation doit donc mettre en place des outils de documentation permettant de décrire les activités et les processus inhérents de génération de rapports et de gestion de contenu pour conserver, gérer et mettre à disposition les informations de l'entreprise.

II.2.3.4 CRBF 97-02

Inspiré des démarches internationales comme celles du Comité de Bâle, le Règlement 97-02 du Comité de Réglementation Bancaire et Financière (CRBF) décrit les obligations de contrôle interne pour les établissements de crédit. Il est fondé sur cinq thèmes principaux : le système de contrôle des opérations et des procédures internes, l'organisation comptable et du traitement de l'information, les systèmes de mesure des risques et des résultats, les systèmes de surveillance et de maîtrise des risques ainsi que le rôle des organes exécutifs et délibérants.

Il en résulte qu’une entreprise assujettie doit mettre en œuvre un système de contrôle des opérations, des systèmes de surveillance et de maîtrise des risques ainsi qu’un système de documentation et d’information. De plus, l’organisme doit mettre en place des procédures de suivi des actions correctrices vis-à-vis des obligations de conformité.

Par ailleurs, l’article 4*n* stipule que l’établissement doit développer un plan de continuité de l’activité permettant la réalisation des tâches et services indispensables en cas de scénario de crise, ainsi qu’un plan de retour planifié aux conditions normales quand le problème est résolu.

II.3 Gestion de projet

Un projet de gestion des identités et des accès repose sur l'ensemble des informations sur les personnes et comptes utilisateurs existants et à venir. Dans le cycle de vie du projet, la phase initiale de spécification doit donc prendre en compte les systèmes d'informations actuels ainsi que le besoin de pouvoir augmenter le périmètre avec l'ajout de nouvelles applications de l'organisme ou de certains partenaires.

II.3.1 Cycle de vie

L. Audibert [16] rappelle que tout logiciel ou système d'information suit un cycle de vie divisé en cinq étapes dont chacune englobe un ensemble d'activités.

La phase de spécification et d'analyse des besoins permet de définir l'ensemble des besoins auxquels devra répondre le futur système. Il en résulte généralement un document de spécifications issu des dialogues entre les équipes métiers et les équipes de développement.

La phase de conception permet de définir l'architecture générale du produit attendu en se basant sur les spécifications définies précédemment. A l'issue de cette phase un planning général est décidé et une ébauche de l'interface graphique peut être proposée.

La phase de codage est le moment où les équipes de développement produisent le code opérationnel.

La phase de test permet d'examiner et valider la qualité du produit en se basant sur plusieurs critères. Ainsi, les tests d'acception doivent vérifier que le produit répond aux attentes spécifiées lors de la phase de spécifications. Les tests d'intégration permettent de s'assurer que les différents éléments du système produit s'interfacent correctement avec les autres systèmes d'information de l'organisation. Les tests unitaires, qui doivent être rédigés pendant la phase de codage, reflètent le comportement de l'application. Ils permettent également de connaitre quelles portions de code opérationnel ont été testées et sont conformes aux spécifications.

La phase de maintenance a pour but de corriger ou faire évoluer le produit livré.

La mise en production peut être considérée comme une étape intermédiaire. Cette étape consiste à déployer le système dans l'environnement cible et à ouvrir l'accès aux utilisateurs.

Ce découpage de projet peut être géré selon plusieurs modèles dont l'utilisation dépend du type de projet et de la réactivité attendue. Les méthodes dites « classiques » imposent des modèles stricts où les étapes sont clairement définies avec une production importante de documentation, ce qui convient généralement à de gros projets. A l'opposé, les méthodes dites « Agiles » suivent des

---

[16] L. Audibert. *UML 2 de l'apprentissage à la pratique*. Ellipses, 298 pages, 2009

modèles itératifs orientés d'avantage sur le code opérationnel que sur la documentation, permettant ainsi des livraisons plus fréquentes.

II.3.2 Cycle en cascade

En 1970, W. W. Royce [17] a publié le modèle en cascade (en anglais : « Waterfall model »). Le projet, proche du mode de gestion des projets industriels, est alors un enchainement linéaire d'étapes avec un retour possible sur les précédentes. Chaque étape se termine à une date prédéterminée par la livraison de documents ou de modules logiciels. De plus, une nouvelle phase ne peut débuter que si la précédente est complétement achevée et validée, ce qui implique que les livrables attendus sont jugés satisfaisants.

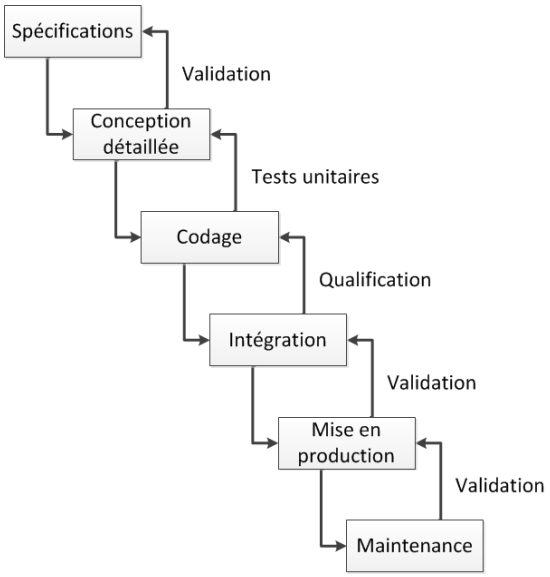


Figure 13 - Cycle de vie de projet en cascade

Ce type de cycle de vie, simple à comprendre et à implémenter, convient aux projets où la qualité a plus d'importance que les coûts ou les délais, et dont les besoins sont clairement définis et stables. Dans le cas contraire, la prise en compte de nouveaux besoins nécessite de dérouler toute la cascade depuis le début. De plus, le client n'est impliqué qu'au début du projet et il ne peut tester le produit qu'à la fin du processus.

Dans le cadre d'un projet de gestion des identités et des accès, les besoins peuvent évoluer. En effet, le déploiement de nouveaux services implique notamment la définition de nouveaux profils ainsi que de nouveaux rôles applicatifs qui doivent être pris en compte, même après la phase

[17] W. W. Royce. Managing the Development of Large Software Systems : concepts and techniques. *Proceedings of the 9th international conference on Software Engineering*, pages 1-9, 1970

de spécification. De ce fait, ce modèle de gestion de projet ne convient pas aux projets de gestion des identités et des accès.

II.3.3 Cycle en V

En 1983, J. McDermid et K. Ripken [18] ont développé un modèle de cycle de vie pour pallier au manque de réactivité inhérent au modèle précédent. Pour cela, chaque livrable doit être testé pour chacune des étapes. L'omniprésence des tests en parallèle des activités garantit la qualité du produit final. En fonction du jalon, la nature des tests diffère. Ainsi les spécifications sont validées par des tests fonctionnels, également appelés tests de recette, dont le déroulement suit des scénarii décrits dans les documents de spécification. Idéalement, ils sont automatisés, ou réalisés par des personnes indépendantes de l'équipe de développement. Ces tests n'étant exécutés qu'une seule fois à la fin du projet (sauf si le produit livré n'est pas jugé satisfaisant), il serait coûteux de les automatiser.

Les tests d'intégration ont pour but de valider que les développements réalisés s'interfacent correctement avec les systèmes d'information existants.

Les tests unitaires ont pour objectif de vérifier que des portions du code opérationnel se comportent comme le développeur l'a prévu. Pour le développement de ces tests, il est conseillé de suivre le modèle de développement mené par les tests (en anglais : « Test Driven Development ») [19]. Ce processus suit quatre étapes :

1. Ecrire un premier test,
2. Vérifier qu'il échoue (car le code qu'il teste n'existe pas) afin de vérifier que le test est valide,
3. Ecrire le code minimal suffisant pour que le test s'exécute correctement sans erreur,
4. Vérifier que le test n'échoue plus,
5. Améliorer et compléter le code tout en gardant les mêmes fonctionnalités.

---

[18] J. McDermid, K. Ripken. Life cycle support in the Ada environment. *ACM SIGAda Ada Letters*, v.III n.1, pages 57-62, 1983

[19] K. Beck. *Test Driven Development: By Example*. Pearson Education, 240 pages, 2002

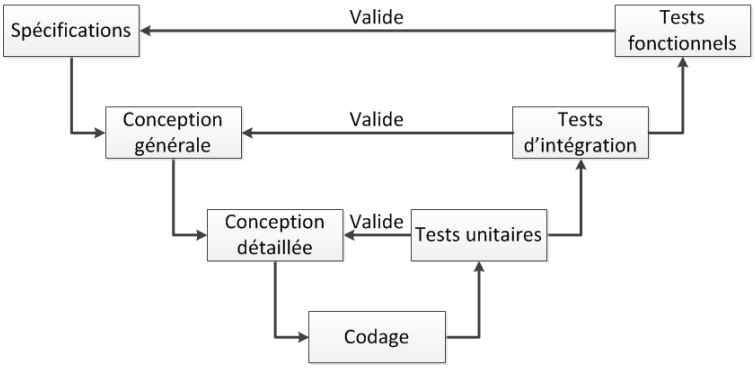


Figure 14 - Cycle de vie de projet en V

A l'instar du modèle en cascade, le modèle en V prend difficilement en charge de nouveaux besoins ou la modification des spécifications. En effet, l'effet tunnel induit par les modèles séquentiels montre qu'une erreur dans la formulation ou l'interprétation des spécifications ne peut être détectée qu'à la fin du cycle. En effet, la maîtrise d'ouvrage n'est impliquée qu'en début et fin de cycle, ce qui peut représenter plusieurs mois d'intervalle pour un gros projet.

Bien que plus nombreuses que dans un cycle en V, les possibilités de prise en compte de nouveaux besoins restent faibles. En effet, dans le cadre d'un projet de gestion des identités et des accès, après la phase de spécification, la mise à disposition d'un nouveau service, ne peut être prise en compte qu'au moment des tests d'intégration. De plus, ces changements impliqueraient la remise en cause du travail effectué jusqu'à la phase des tests unitaires. L'utilisation de ce type de cycle de vie pour un projet de gestion des identités et des accès implique que l'ajout d'une application, de laquelle découle de nouveaux rôles, impose un projet propre avec le déroulement complet du cycle de vie. De ce fait, ce modèle n'est pas recommandé dans le cas d'un projet de gestion des identités et des accès.

II.3.4 Cycle en spirale

En 1988, B. W. Boehm [20] a introduit les notions d'itération et de prototypage dans le cycle de vie d'un projet informatique pour pallier au manque de visibilité inhérent aux démarches séquentielles.

Une itération correspond à l'exécution du cycle de vie pour un sous-ensemble des spécifications qui se conclut par la livraison d'un produit opérationnel. La prise en compte de l'ensemble des spécifications nécessitant plusieurs itérations, l'équipe fonctionnelle du projet dispose régulièrement d'un outil qu'elle peut soumettre à l'ensemble des tests évoqués avec le cycle

[20] B. W. Boehm. A Spiral Model of Software Development and Enhancement. *ACM SIGSOFT Software Engineering Notes*, Volume 11 n.4, pages 14-24, 1986

en V. Cette démarche permet de réajuster régulièrement les spécifications, budgets et délais. Une itération peut prendre en compte des spécifications qui ont déjà fait l'objet d'une itération, ce qui offre une capacité de réaction face à l'évolution des besoins.

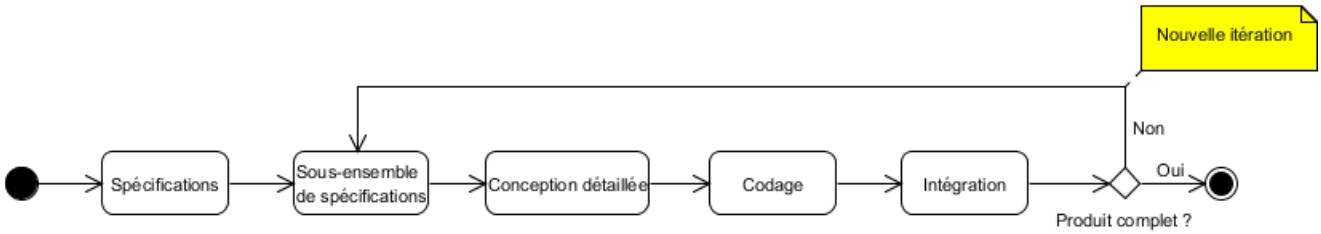


Figure 15 - Diagramme d'activité d'une démarche itérative

Un prototype est une réalisation partielle de l'étape de codage qui simule le comportement d'un sous-ensemble des fonctionnalités attendues. Les règles de codage ne sont alors pas nécessairement suivies. Le prototype n'a pas vocation à être déployé. En effet, le but est que les développeurs soumettent leur compréhension des spécifications. Ce dialogue permet de diminuer les risques en s'assurant à différents jalons du projet que les choix d'implémentation répondent aux besoins des clients du projet. En effet, le prototype est soumis à l'évaluation de l'équipe fonctionnelle du projet et peut subir des modifications jusqu'à ce qu'il soit validé. C'est seulement à partir de cette étape que les activités du projet peuvent continuer.

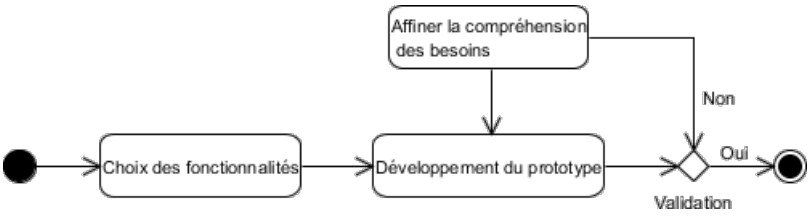


Figure 16 - Diagramme d'activité de réalisation d'un prototype

Le modèle en spirale, proposé par B. W. Boehm, divise le cycle de vie global d'un projet en minimum trois itérations (représentées graphiquement par des spirales) qui suivent chacune un cycle de vie complet composé de quatre phases :

1. Détermination des objectifs à partir de l'analyse des besoins ou du résultat des cycles précédents,
2. Analyse des risques avec une phase dédiée au prototypage,
3. Développements et tests. Dans la dernière spirale il est possible de suivre une démarche séquentielle telle que la cascade ou le V,
4. Validation du résultat puis planification.

La première itération de l'analyse des besoins et des risques permet de placer les fonctions critiques dans le premier cycle de prototypage et de développement. Ainsi, les objectifs et les

développements à prendre en compte dans les itérations suivantes auront un risque d'impact minimisé sur les itérations antérieures.

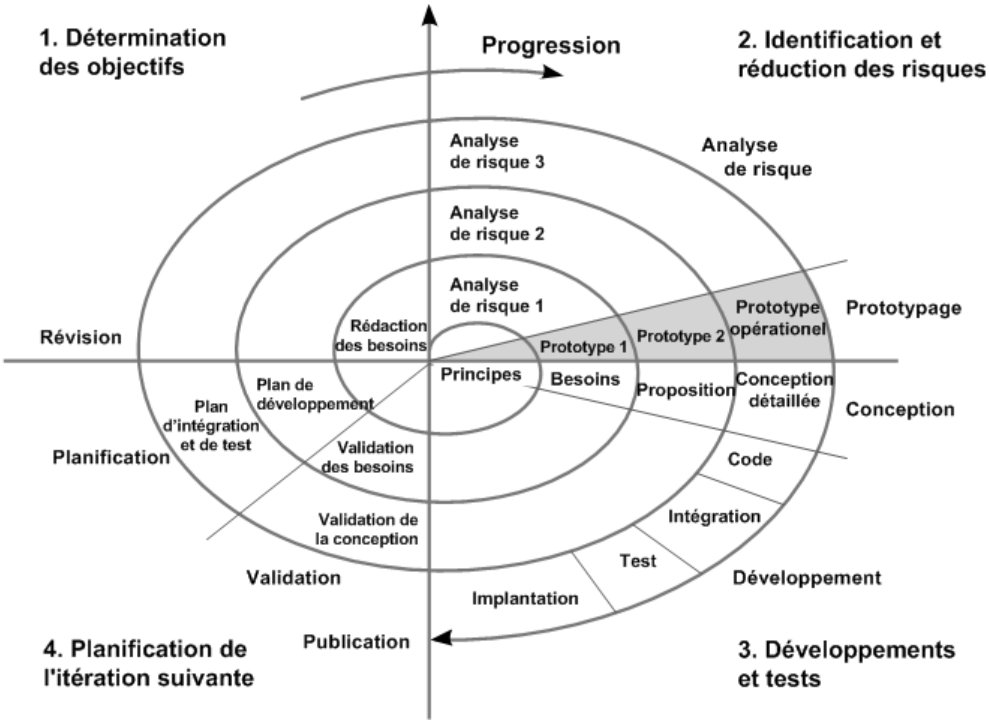


Figure 17 - Cycle de vie de projet en spirale

L'évaluation répétée des besoins, des risques et des développements propre à ce modèle permet de contrôler régulièrement si les délais et budgets seront respectés, contrairement aux démarches séquentielles où ils ne peuvent être vérifiés qu'à l'approche de la date de livraison. De plus, le client du projet est plus impliqué dans la vie du projet que dans les modèles linéaires, où son action est limitée à la phase de rédaction du cahier des charges et à la validation du produit final.

La démarche en spirale permet des interactions plus fréquentes entre les différentes équipes engagées dans un projet par rapport aux modèles linéaires. Cependant, après la phase de spécification, les besoins peuvent être ajustés, mais il n'est pas facile de prendre en compte d'importantes modifications ou ajouts. En effet, ce type de changement implique de reprendre complètement l'analyse de risque qui représente une part important du projet dans le cycle en spirale.

Dans le cadre d'un projet de gestion des identités et des accès, ce type de cycle de vie permet de prendre en compte de nouveaux besoins induits par le déploiement de nouveaux services. Cependant, les possibilités sont limitées. Les spécifications doivent intégrer la capacité de modification du périmètre des applications sans imposer la réalisation d'une nouvelle analyse de risque qui peut être longue et coûteuse. Cette possibilité particulière doit être testée au plus tôt lors de la réalisation d'un prototype. Le cycle de vie itératif semble donc envisageable pour des projets

de gestion des identités et des accès. Cependant le cycle de vie en spirale n'est pas le plus adapté à cause des impacts financiers et en délai des analyses de risque.

II.3.5 Méthodes Agiles

En 2001, dix-sept experts en développement logiciel se sont réunis pour présenter leurs méthodes (Adaptive Software Development, XP, Scrum, Crystal, Feature Driven Development, Dynamic System Development Method (DSDM) et « pragmatic programming ») [21]. Suite à l'analyse des avantages de chacune de ces méthodes, ils ont extrait quatre valeurs fondamentales et douze principes pour constituer le manifeste des méthodes de développement Agiles (cf. annexe 1 « The Manifesto for Agile Software Development »).

Afin d'obtenir un produit opérationnel répondant aux attentes des utilisateurs, les démarches Agiles reposent sur les quatre règles fondamentales suivantes.

- Les individus et leurs interactions plutôt que les processus et les outils,
- Des logiciels opérationnels plutôt qu'une documentation exhaustive,
- La collaboration avec les clients plutôt que la négociation contractuelle,
- L'adaptation au changement plutôt que le suivi d'un plan.

Pour mettre en pratique ces principes, les méthodes Agiles préconisent un cycle itératif et incrémental incluant notamment les phases de spécification, développement et validation. Par rapport à la démarche en spirale, en Agilité le cycle est complété par la notion d'incrément même si la notion est proche de celle d'itération, dans le cas de l'incrément, le découpage du projet en sous-ensemble ne se fait plus au niveau des spécifications, mais au niveau des composants. Un seul ensemble de composants est développé par incrément. Chaque incrément vient s'intégrer au premier incrément du projet appelé le noyau. La mise en œuvre de cette division des besoins et des composants, se fait au travers de « Sprints ». Le sprint correspond à une étape d'un mois maximum dont les objectifs sont définis dans le carnet du sprint, le « Sprint backlog ». Le sprint backlog spécifie les fonctionnalités qui doivent être développées ou corrigées lors du sprint. Les méthodes agiles ayant pour principe de privilégier la réalisation de code fonctionnel plutôt que la rédaction de documentation technique ou fonctionnelle, cette dernière peut faire l'objet d'un sprint dédié. Par ailleurs, la plus grande partie des fonctions de l'outil est définie en début de projet dans le carnet du produit, le « Product backlog ». Chaque cas d'utilisation est décrit dans une « User story » à laquelle sont affectées une priorité et une estimation du volume de travail nécessaire pour le développer, le tester et le valider.

---

[21] A. Cockburn. *Agile software development*. Addison-Wesley Longman Publishing Co., 278 pages, 2002

De plus, les méthodes Agiles prônent la collaboration entre les personnes impliquées dans et par le projet, ce qui requiert notamment l'intégration de la maîtrise d'ouvrage et des utilisateurs au cours du développement. Pour répondre à ces besoins, l'équipe projet inclut un propriétaire du produit (en anglais : « Product owner ») qui est un expert du métier. Il va jouer le rôle du client. Il doit être capable de définir les spécifications fonctionnelles, d'établir la priorité des fonctionnalités à développer ou corriger et valider les fonctionnalités développées.

Afin de favoriser le dialogue, les méthodes Agiles prévoient plusieurs types de réunions qui sont à programmer à différents moments du projet.
Avant chaque sprint, une réunion de planification, le « Sprint planning » ou « Iteration planning », permet de sélectionner dans le product backlog les fonctions à implémenter qui constitueront le sprint backlog en fonction des priorités du client.
Durant le sprint, la « mêlée » permet à l'équipe de se regrouper pendant quinze minutes maximum quotidiennement pour évoquer les problèmes rencontrés dans la journée, éventuellement y assigner des développeurs supplémentaires, mais sans chercher à les résoudre. L'identification des problèmes peut être facilitée par la mise en place d'une plate-forme d'intégration continue. Ce type d'outil permet de compiler, vérifier et tester automatiquement l'ensemble du code opérationnel dès qu'un nouvel élément est publié, ce qui implique de suivre le modèle « Test Driven Development » évoqué précédemment. Cette réunion permet également de vérifier que toutes les user stories du sprint backlog seront terminées à la date de fin prévue de l'itération.
A la fin du sprint, une réunion de rétrospective, la « Sprint review », permet de capitaliser sur les problèmes rencontrés, les solutions mises en œuvre, ainsi que les causes de perte d'efficacité et de qualité. C'est également l'occasion de présenter le résultat du sprint avec la démonstration des nouvelles fonctions ou des corrections.

La mise en œuvre de ces concepts permet d'offrir de la souplesse au projet et de donner de la visibilité au client sur les réalisations.

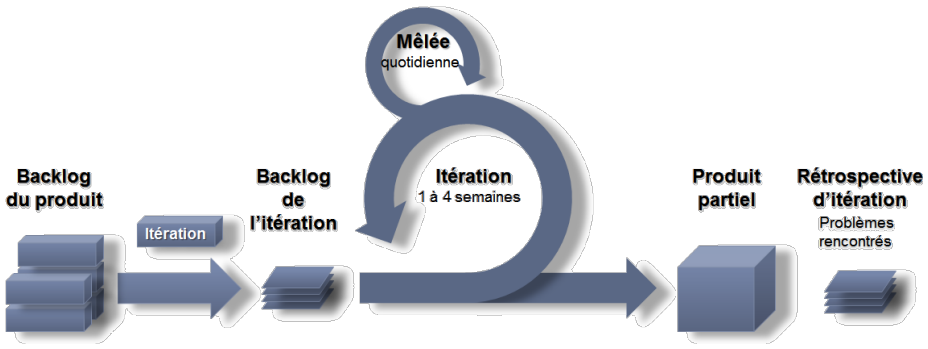


Figure 18 - Cycle de vie en « Agilité »

Cette méthode est applicable pour le développement initial d'un projet mais aussi lors de la maintenance applicative.

Dans le cadre d'un projet de gestion des identités et des accès, la livraison d'itérations simples et successives peut permettre d'assembler les informations sur les personnes et les comptes utilisateurs au fur et à mesure de la prise en compte de nouveaux systèmes d'information. La difficulté de synchronisation entre toutes les applications impactées est alors répartie sur plusieurs itérations. L'évolution des besoins étant la base de ce type de cycle de vie, il convient parfaitement aux projets de gestion des identités et des accès.

II.4 Bonnes pratiques

II.4.1 Normes

Bien qu'il ne soit pas nécessaire de suivre au sein d'une organisation les normes décrites ci-après, il est préférable de respecter le vocabulaire qui y est défini. De plus, il n'est pas forcément souhaitable d'atteindre le niveau d'exigence de la norme ISO-27002, notamment pour des raisons de coûts, mais tendre à s'en rapprocher permet de mettre en place un niveau de sécurité satisfaisant.

II.4.1.1 ISO-24760

La norme ISO-24760 citée précédemment est un ensemble de prescriptions concernant la gestion des identités divisé en trois parties.

La première partie (ISO-24760 A framework for identity management - Part 1 : Terminology and concepts [6], cf. annexe 2 « ISO-24760 ») est consacrée à la définition des concepts liés aux identités. Les notions décrites sont reprises et explicitées dans le présent document.

La seconde partie (ISO-24670 A framework for identity management - Part 2 : Reference architecture and requirements) ne sera publiée officiellement qu'en décembre 2013. Elle proposera une architecture pour la mise en œuvre de la gestion des identités.

La troisième partie (ISO-24760 A framework for identity management - Part 3 : Practice) qui est également en cours de rédaction détaillera la mise en pratique de l'architecture définie dans la seconde partie de la norme.

II.4.1.2 ISO-2700x

Les normes 2700x sont une famille de normes traitant de la sécurité de l'information où la gestion des identités et des accès y est évoquée.

- ***ISO/IEC 27000:2009 : Information security management systems - Overview and vocabulary***

Publiée en 2009, la norme ISO/CEI 27000 présente les concepts qui sont manipulés dans les autres normes ISO-2700x. Elle décrit notamment la notion de mesure de sécurité (en anglais : « control ») comme étant un « moyen de gestion du risque, comprenant les politiques, les procédures, les lignes directrices, les pratiques ou l'organisation, qui peuvent être de nature administrative, technique, managériale ou juridique ». Le système de management de la sécurité de l'information (SMSI) est présenté comme une « partie du système de management global, basée sur

une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information ». Le processus de qualité PDCA (en anglais : « Plan-Do-Check-Act/Adjust » ; en français : « Planifier-Déployer-Contrôler-Agir/Ajuster ») y est présenté brièvement.

- ***ISO/IEC 27001:2005 : Information security management systems - Requirements***

Publiée en 2005, la norme ISO/IEC 27001 définit les exigences pour mettre en œuvre, documenter, exploiter et faire évoluer un SMSI dont le modèle cyclique PDCA est le support. Cette démarche itérative est composée de quatre étapes. La phase de planification concerne la conception du SMSI. La phase de déploiement correspond à la réalisation de ce qui a été planifié. La phase de contrôle permet de vérifier qu'il n'existe pas d'écart entre ce qui a été planifié et ce qui a été implémenté. La phase d'action permet de corriger les écarts constatés lors de l'étape précédente.

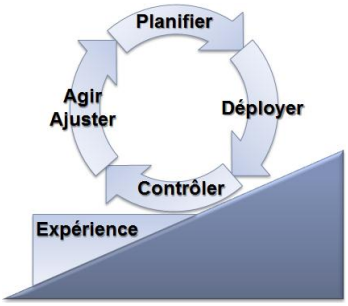


Figure 19 - Processus itératif PDCA de la norme ISO-27001

- ***ISO/IEC 27002:2005 : Code of practice for information security management***

Publiée en 2005, la norme ISO/IEC 27002 est un recueil de bonnes pratiques sur la sécurité de l'information. Elle propose un ensemble de mesures de sécurité organisationnelles et techniques, mais aucune solution technique. Le chapitre 11 expose notamment des mesures consacrées à la gestion des identités et des accès dans le but de maîtriser l'accès à l'information (cf. annexe 3 « ISO-27002 – chapitre 11 ») [22]. La politique de contrôle des accès inclut des exigences par exemple autour des « profils d'accès utilisateur normalisés pour les rôles courants au sein de l'organisme » ou de l'« annulation de droits d'accès ». Le sous-chapitre 11.2 décrit les mesures relatives à la gestion de l'accès utilisateur, dont l'enregistrement des utilisateurs, des privilèges et des mots de passe.

[22] *ISO/CEI 27002:2005(F)*. ISO/IEC, 130 pages, 2005

- ***ISO/IEC 27003:2010 : Information security management system - implementation guidance***

Publiée en 2010, la norme ISO/IEC 27003 contient un guide pratique de mise en œuvre du SMSI suivant le processus PDCA et respectant les exigences de la norme ISO-27002.

- ***ISO/IEC 27004:2009 : Information security management system - Measurement***

Publiée en 2009, la norme ISO/IEC 27004 fournit des métriques permettant d'évaluer le niveau d'efficacité du SMSI et par conséquent le niveau de sécurité de l'organisation.

- ***ISO/IEC 27005:2011 : Information security risk management***

Publiée en 2008 et révisée en 2011, la norme ISO/IEC 27005 contient un guide de gestion du risque. Elle repose sur les concepts en sécurité de l'information définis par la norme ISO/IEC 27001.

- ***ISO/IEC 27006:2011 : Requirements for bodies providing audit and certification of information security management systems***

Publiée en 2009 et révisée en 2011, la norme ISO/IEC 27006 est un recueil d'exigences à destination des organismes qui procèdent à l'audit et à la certification ISO 27001.

- ***ISO/IEC 27007:2011 : Guidelines for information security management systems auditing***

Publiée en 2011, la norme ISO/IEC 27007 est un recueil d'instructions pour l'audit et la certification ISO 27001 d'un SMSI.

- ***ISO/IEC 27008:2011 : Guidelines for auditors on information security controls***

Publiée en 2011, la norme ISO/IEC 27008 est un recueil d'instructions à destination des auditeurs accrédités pour vérifier la qualité d'implémentation des mesures de sécurité décrites dans la norme ISO 27002.

II.4.2 Démarche projet orientée gestion des identités et des accès

L'objectif d'un projet de gestion des identités et des accès est de gérer les utilisateurs et leurs habilitations afin d'arriver à déterminer qui a le droit d'accéder à quoi. La difficulté de ce type de projet évoquée lors des retours d'expérience réside dans la complexité des systèmes d'information existants qui ne permettent pas de construire un ensemble cohérent d'informations. En effet, les informations sont réparties dans de nombreux référentiels. De ce fait, il n'existe aucun

moyen d'établir aisément la relation entre identité et habilitations et d'identifier les profils métiers ou les rôles applicatifs. C'est pourquoi il est conseillé d'établir au préalable une cartographie qui prend en compte tous les systèmes d'information permettant de recueillir des informations sur les personnes, les comptes utilisateurs, les profils métiers, les rôles ainsi que les ressources auxquels ils accèdent.

La cartographie doit permettre de mettre en évidence des besoins. L'étape suivante consiste donc à fixer les priorités tant au niveau du système d'information global qu'au niveau fonctionnel. Les différents niveaux de priorité vont définir les objectifs que le système de gestion des identités et des accès devra atteindre. Chaque besoin doit être associé à un responsable ou une maîtrise d'ouvrage métier qui devient alors un des commanditaires, appelé sponsor, du projet. La gestion des identités ayant un impact sur les processus liés aux ressources humaines, au moins en tant que consommateur des informations, un responsable doit donc être impliqué au plus tôt dans le projet.

Une difficulté supplémentaire évoquée lors des retours d'expérience de projets de gestion des identités est une durée trop importante qui est responsable de la diminution de l'implication des équipes fonctionnelles. Comme évoqué pour les démarches séquentielles, le manque de visibilité sur l'avancement du projet peut démotiver les clients du projet. C'est pourquoi les cabinets de conseil et d'intégration préconisent de suivre une méthode itérative avec des livrables visibles à chaque étape.

La démarche préconisée est donc proche des modèles Agiles. Chaque itération, d'une durée n'excédant pas un mois, doit permettre de livrer un composant de la gestion des identités et des accès auquel sera associé un sponsor correspondant au product owner des méthodes Agiles.

Les différentes étapes s'inscrivent dans un schéma à long terme reposant sur trois phases.
La première phase consiste à bâtir une base solide pour les services de gestion des identités et des accès. Ce socle repose sur la connaissance des associations compte-identité. Pour cela il est nécessaire de nettoyer et mettre en cohérence les différents systèmes et de mettre en place un identifiant unique personnel.
La seconde phase est le déploiement des services de gestion des identités et des accès. Elle intègre la formalisation et l'automatisation des processus de gestion des habilitations. Elle a pour objectif d'offrir un moyen de gérer les accès et d'en réaliser un audit et de produire des rapports.
La dernière phase doit fournir une gestion fine des rôles. Elle débute par une réconciliation des rôles et des accès afin de déterminer qui accède à quelle application, à quel compte, selon quelle règle et avec quels privilèges. L'objectif est de fournir un moyen de gérer intuitivement cet ensemble d'information.

III Projet IAM

III.1 Présentation

Le projet Janus initié en 2006 par la DSI et l'Unité Réseau du CNRS (UREC) avait pour objectif de prendre en charge la gestion des identités et des accès. En 2008, pour les besoins du déploiement de la nouvelle application de saisie des dossiers annuels des agents du CNRS, le projet Janus a abouti à la mise en place d'un fournisseur d'identité, et d'un fournisseur de service pour l'application SIRHUS (cf. chapitre « Cartographie »). Le déploiement de ces outils a permis d'intégrer la fédération « Éducation-Recherche » qui est gérée actuellement par le groupement Renater. Suite à cette mise en production, le besoin de déployer un outil de gestion des habilitations a été identifié. Ayant participé à la création d'un annuaire dédié à Janus, j'ai mené une étude d'opportunité sur la mise en œuvre d'un outil dont la conclusion fut que le marché n'offrait pas d'outil répondant aux besoins de la DSI.

En 2011, le projet stratégique de portail collaboratif CORE (cf. chapitre « Cartographie ») a émis le besoin d'un outil de gestion des rôles pour faciliter la gestion du partage des informations communautaires. Le périmètre de Janus étant actuellement figé et limité à l'écosystème du fournisseur d'identité et des différents fournisseurs de service, j'ai identifié un projet connexe de gestion des identités et des accès pour répondre aux besoins de gestion des comptes non CNRS et de gestion des habilitations.

A ce titre, je suis missionné pour mener la nouvelle étude de faisabilité du projet de gestion des identités et des accès IAM (« Identity and Access Management » en anglais) pour le système d'information du CNRS. L'objectif est de recueillir l'ensemble des besoins, de définir une architecture pouvant y répondre et les étapes à suivre pour la construction d'un tel outil.

Dans le cadre du mémoire d'ingénieur, le périmètre de l'étude est réduit aux seuls besoins de la DSI et à l'examen des logiciels libres. Les offres commerciales seront évoquées à titre comparatif pour mesurer le risque lié aux solutions libres. Le choix de l'outil sera validé par la réalisation d'un démonstrateur qui aura pour objectif de vérifier la capacité à remplacer les outils existants et à prendre en charge un besoin fonctionnel.

III.2 Organisation

Dans la démarche Agile, l'équipe du projet est constituée principalement d'un propriétaire du produit, d'une équipe de développement, d'une équipe de test ainsi qu'un sponsor qui doit porter le projet au sein de l'organisation.

Les besoins du client sont donc remontés par son représentant, le « product owner » . Dans le cadre d'un projet de gestion des identités et des accès, le propriétaire du produit peut être le Responsable de la Sécurité des Systèmes d'Information (RSSI).

A terme l'équipe de développement affectée au développement d'une solution de gestion des identités et des accès sera réduite. L'étude doit donc montrer que l'outil sélectionné peut être installé, configuré et modifié pour répondre aux besoins avec seulement deux développeurs disponibles au maximum.

L'étude étant limitée aux besoins de la DSI du CNRS, le sponsor des itérations n'a pas vocation à en être extérieur. L'objectif de l'étude étant de trouver une solution pour maîtriser les flux des identités, le sponsor peut être la cellule « Urbanisation » qui pourra porter les réalisations au sein de la DSI du CNRS.

III.3Démarche

Ayant assisté à plusieurs retour d'expérience de projet de gestion des identités et des accès, il s'avère que l'effet tunnel induit par les cycles de vie séquentiels, mène dans la plupart des cas à l'abandon des projets. En effet, ce type de projet est souvent long car les besoins sont nombreux et complexes et nécessitent l'investissement de différents métiers fonctionnels au sein de l'organisation. De ce fait, j'ai fait le choix d'utiliser une démarche Agile pour la phase de réalisation du mémoire sans privilégier particulièrement une méthode. Seuls les concepts généraux seront appliqués. Cela permettra également de valider que ce type de processus correspond à la taille réduite de l'équipe qui sera responsable de la conception, de la mise en œuvre et de l'évolution du système de gestion des identités et des accès pour la DSI du CNRS.

Conformément à la démarche évoquée précédemment dans les bonnes pratiques de gestion de projet, la première étape de la présente étude est de réaliser la cartographie des référentiels et outils qui permettent actuellement de gérer les comptes et leurs accès. Suite à cet état des lieux, la première itération aura pour objectif de définir le product backlog et les objectifs des sprints suivants jusqu'à la livraison d'un démonstrateur basé sur un outil Free/Libre Open-Source (FLOSS)[*]. Ensuite, le contour du projet global pourra être ouvert aux offres commerciales et aux besoins des autres unités du CNRS dans des itérations ultérieures.

[*] Couvre à la fois les logiciels libres et les logiciels open source, les deux grands mouvements soutenus respectivement par la Free Software Foundation et l'Open Source Initiative.

IV Cartographie de l'existant

La cartographie a été réalisée en auditant les processus qui interviennent dans la gestion des identités et des accès. A cette fin, j'ai procédé à des entrevues avec les responsables d'applications et des utilisateurs quotidiens de ces outils.

IV.1 Référentiels des personnes

IV.1.1 Personnel CNRS

Les agents du CNRS sont gérés dans le Système d'Information des Ressources Humaines des Unités et des Services (SIRHUS) qui couvre la gestion des ressources humaines dans son ensemble. L'application, qui repose sur des outils SAP, permet de gérer la carrière administrative et professionnelle des agents CNRS, la paie ainsi que les supports budgétaires. Il est le référentiel du personnel payé par le CNRS permanent ou en contrat à durée déterminée ainsi que des nomenclatures RH pour le personnel CNRS.

L'outil d'intégration d'applications d'entreprise (EAI : « Enterprise Application Integration » en anglais) a été mis en place par la DSI du CNRS pour propager des données issues des différents éléments du système d'information de pilotage. Il met à disposition les informations sur les personnes et leur nomenclature quotidiennement par un flux d'extraction, appelé « demi-flux SIRHUS » vers un fichier XML appelé « Format pivot ». Par ailleurs, un flux entrant permet d'importer des informations utilisées dans la construction du dossier administratif du personnel CNRS, telles que des renseignements sur les structures incluant la nomination des directeurs d'unité.

Les processus métier retenus dans le cadre de la gestion des identités pour les agents CNRS correspondent aux cas d'utilisation représentés dans le diagramme suivant :

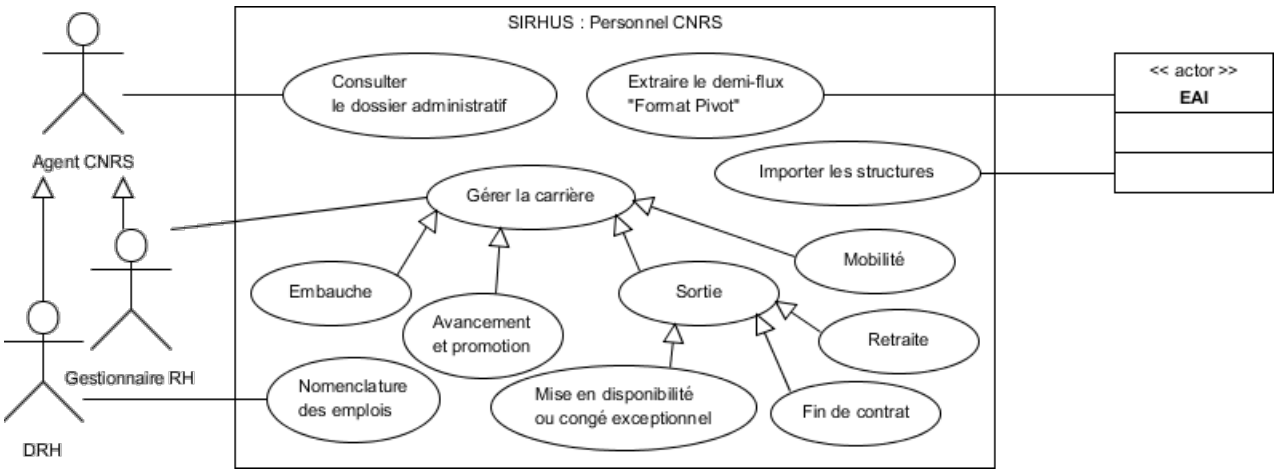


Figure 20 - Diagramme des cas d'utilisation de SIRHUS pour la gestion des identités

IV.1.2 Personnel CNRS et non-CNRS

L'application Labintel permet de gérer les informations relatives aux laboratoires avec lesquels le CNRS a signé un contrat d'association. Elle permet de décrire les structures CNRS et non CNRS, leurs activités, contrats, et les moyens tels que les ressources financières, équipements et productions ainsi que le personnel CNRS et non CNRS qu'elles emploient. Labintel ne permet pas de gérer les personnes, uniquement les affectations. De ce fait, une personne qui travaille pour plusieurs unités est connue sous plusieurs identités indépendantes, chacune correspondant à l'affectation de la personne dans l'unité. Pour le personnel CNRS, les données sont issues de l'application SIRHUS décrite ci-dessus. De ce fait, il est possible d'établir le lien entre identités en utilisant le numéro de matricule SIRHUS. Néanmoins, le numéro de matricule SIRHUS n'existe pas pour les personnels non CNRS, ce qui implique qu'il est difficile d'établir un lien entre les différentes affectations d'une personne.

Labintel est le référentiel des structures, du personnel non-CNRS, des directeurs d'unité, des nomenclatures des structures ainsi que des groupes de discipline. L'ensemble de ces informations sont propagées aux autres systèmes d'information dont SIRHUS au travers de l'EAI. Les informations relatives aux organismes partenaires sont issues de l'application « Référentiel des partenaires » qui offre une interface contrôlable directement depuis l'application Labintel.

Les processus métier retenus dans le cadre de la gestion des identités correspondent aux cas d'utilisation représentés dans le diagramme suivant :

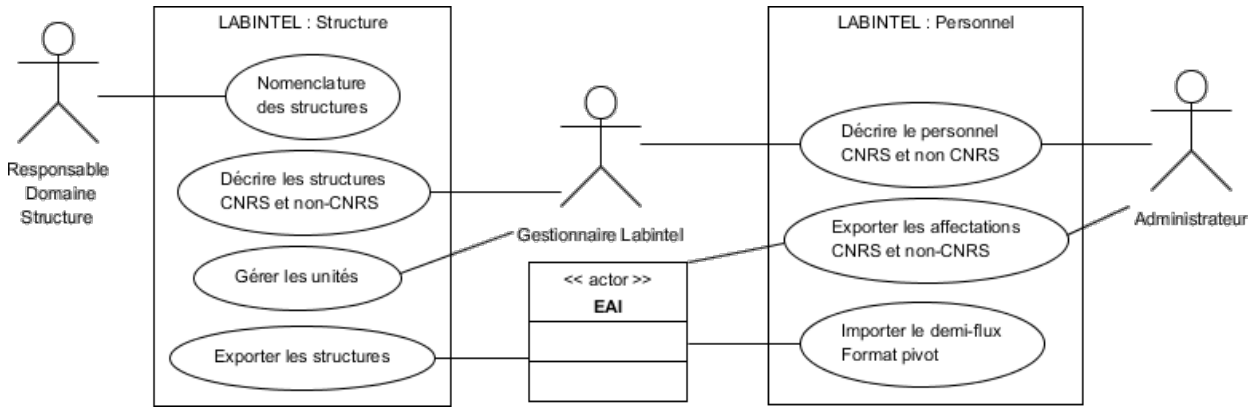


Figure 21 - Diagramme des cas d'utilisation de LABINTEL pour la gestion des identités

IV.1.3 Prestataires

Actuellement, il n'existe aucun registre des personnes sous contrat de prestation. La notion de contrat existe au niveau de l'application de comptabilité et de gestion financière, mais aucun lien n'existe avec les personnes qui travaillent au sein des unités du CNRS dans le cadre de cette collaboration.

IV.1.4 Cartographie des flux d'informations liés aux personnes

En important les informations du référentiel des personnels CNRS SIRHUS, Labintel peut être considéré comme une source fiable de renseignements sur l'ensemble des personnes travaillant au sein d'une structure dont le CNRS est une des tutelles. Cependant, l'absence de relation directe entre ces applications rendent difficile la construction d'une vision globale des identités liées à une personne. En effet, en réalisant l'import des données, l'EAI transforme les informations sur les personnes en données sur les affectations. Ce sont ensuite ces dernières qui sont utilisées par les autres systèmes d'informations.

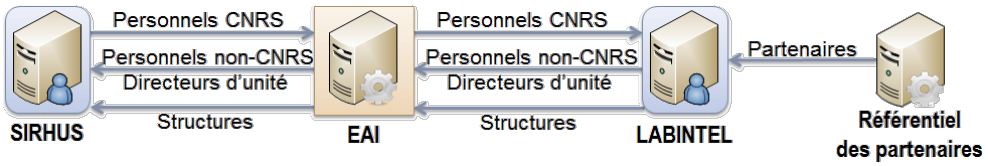


Figure 22 - Schéma des flux d'informations liés aux personnes

IV.2 Gestion des identités et des accès

IV.2.1 Directory Management & Administration System (DMAS)

La DSI du CNRS a mis en place en 2004 dans le cadre de l'urbanisation de son système d'information un système de propagation des informations sur les personnes travaillant dans des unités pour lesquelles le CNRS est une des tutelles à destination d'un annuaire d'entreprise (cf. le paragraphe « Annuaire Central »). La fréquence de mise à jour, souhaitée aussi courte que possible, ne permettait pas d'utiliser l'EAI mis en place par la DSI du CNRS. En effet, en cours de développement et initialement destiné à réaliser des traitements de masse, il n'offrait pas la capacité de transmettre des données en flux tendu.

DMAS étant un outil automatisé servant d'intermédiaire, il ne permet d'agir sur le cycle de vie des identités. Il est uniquement un support à la transmission des informations. Les cas d'utilisation pour les acteurs humains sont donc limités à son administration.

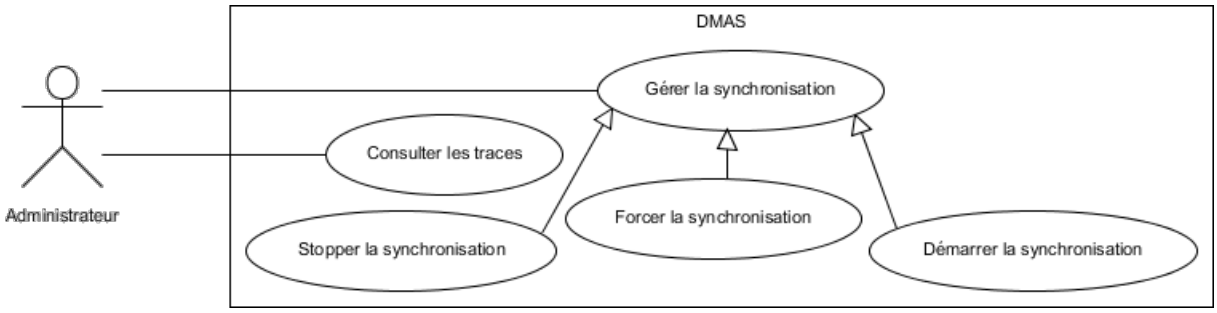


Figure 23 - Cas d'utilisation de l'outil « Directory Management & Administration System »

L'outil DMAS est constitué d'un logiciel agent et d'un broker JMS. A l'origine, les agents étaient uniquement destinés à alimenter des annuaires. Cependant, ils ont été développés dans le but d'être génériques. Il est possible de développer des règles de transformation des messages pour alimenter différents types de ressources et de lire tout type de source de données. Ainsi, un agent est déployé pour suivre les mises à jour d'informations dans une application source. Il interprète ensuite l'information et exécute une action correspondante dans une ressource. Le broker JMS peut alors être une ressource cible où les informations sont envoyées en tant que message pour être diffusées. Ensuite, un autre agent, abonné à la file de messages, lit l'information et la répercute dans une application cible.

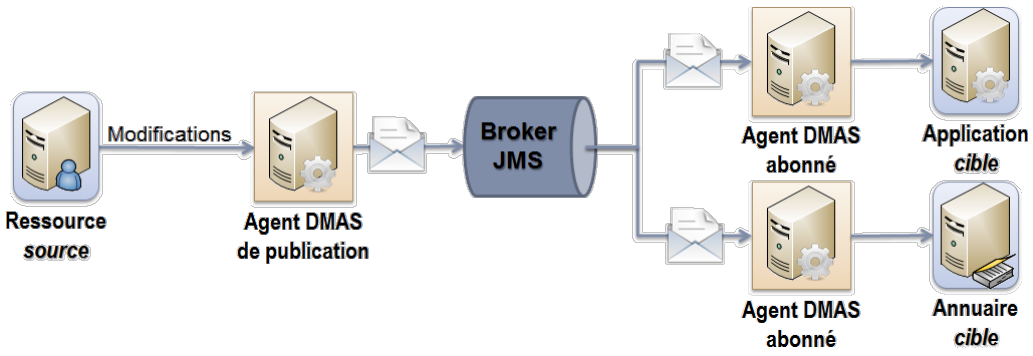


Figure 24 - Schéma des flux d'informations dans DMAS

IV.2.2 Annuaire « Central »

Dans le cadre de l'urbanisation, la DSI a mis en œuvre un annuaire pour permettre l'authentification des utilisateurs du système d'information. Les comptes utilisateurs sont alimentés automatiquement par l'outil DMAS avec pour unique source le référentiel métier Labintel. Il n'a donc pas vocation à être manipulé par des utilisateurs. Seules les applications autorisées ont la capacité à l'interroger pour obtenir des informations sur les comptes utilisateur ou en demander l'authentification.

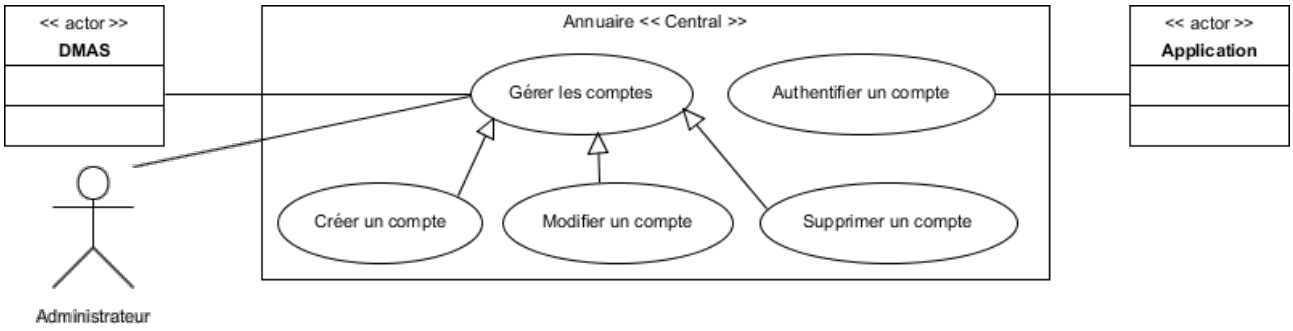


Figure 25 - Cas d'utilisation de l'annuaire « Central »

L'annuaire est décomposé en deux parties principales. La partie transverse contient les comptes liés aux personnes, alors que la partie des groupes fonctionnels contient des comptes liés aux applications et aux habilitations, dont Labintel. Les comptes utilisateurs sont stockées sous la racine « ou=people, dc=cnrs, dc=fr » qui est composée de trois branches. La branche CNRS « ou=cnrs, ou=people, dc=cnrs, dc=fr » contient les titulaires CNRS. La branche EXTER « ou=exter, ou=people, dc=cnrs, dc=fr » contient les titulaires non CNRS. La branche TEMP « ou=temp, ou=people, dc=cnrs, dc=fr » contient les non titulaires CNRS, ce qui inclue les contractuels, les doctorants et les stagiaires.

Cette organisation se rapproche du modèle RBAC. Chaque branche correspond alors à un rôle.

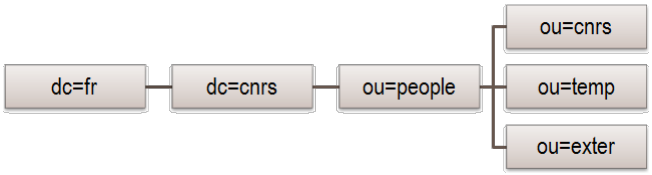


Figure 26 - Structure de l'annuaire « Central » pour les comptes utilisateurs

Une entrée dans l'annuaire correspond à une fiche agent Labintel, donc une affectation, dans une structure. L'annuaire compte environ 130 000 entrées. Seules les informations métier utiles aux applications du système d'information sont extraites par l'outil. Ainsi, les seules informations personnelles sont le nom et le prénom de l'utilisateur. Les autres informations sont issues de la fiche agent et décrivent donc l'emploi et la structure d'accueil. L'alimentation est réalisée sans l'intermédiaire du broker JMS.

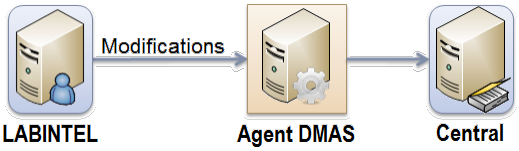


Figure 27 - Schéma des flux d'informations vers l'annuaire « Central »

Ces informations sont chargées automatiquement dans l'annuaire central si et seulement si la personne est décrite comme présente en unité et n'est pas du type personnel privé (personne employée sur les fonds propres de l'unité ou de l'institut, donc non gérée par le CNRS). Une entrée est automatiquement supprimée si elle ne remplit plus une des conditions précédentes ou si l'enregistrement est supprimé de Labintel.

Le processus de propagation des informations de Labintel est entièrement automatisé. Les phases manuelles concernent la saisie des fiches agent.

1. L'application Labintel notifie une modification de fiche agent.
2. L'agent DMAS « Central » détecte la mise à jour. Il la répercute dans l'annuaire « Central ».
3. L'agent DMAS « Central » vérifie que l'opération s'est correctement déroulée
4. Si le compte est correctement créé ou mis à jour dans l'annuaire « Central », l'agent DMAS « Central » envoie un message sur le broker JMS.

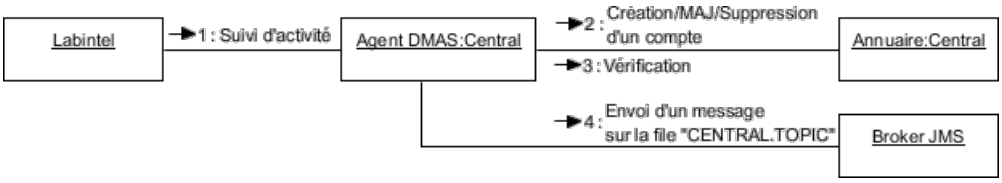


Figure 28 - Diagramme de collaboration de l'alimentation de l'annuaire « Central »

Lors de la fusion ou de l'éclatement de structures, les affectations des personnes dans l'unité d'origine sont clôturées dans Labintel et les personnes se voient attribuées une nouvelle affectation dans la nouvelle unité. Cela implique la suppression des comptes sous-jacents dans l'annuaire et la création de nouveaux comptes dans la nouvelle unité. Les informations relatives aux anciens profils ne sont pas reportées dans les profils nouvellement créés.

IV.2.3 Annuaire « Référentiel »

L'annuaire référentiel a été déployé pour servir de socle aux fournisseurs d'identité du CNRS « Janus » pour les agents affectés dans les unités CNRS et « Janus-ext » dédié aux personnes extérieures. La version de recette intègre des comptes utilisateurs non-nominatifs utilisés pour les formations. La version de production intègre des comptes utilisateurs externes aux organismes de recherche partenaires, tels que les contractuels ou les membres d'autres ministères.

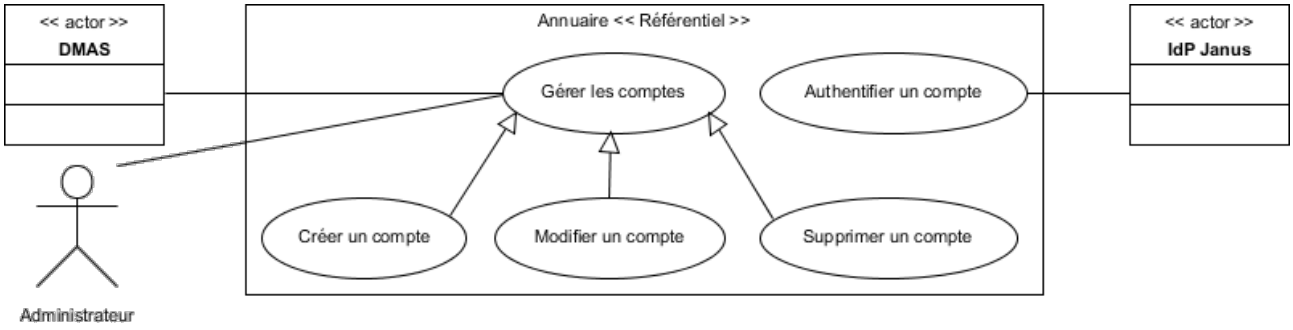


Figure 29 - Cas d'utilisation de l'annuaire « Référentiel »

L'annuaire « Référentiel » peut être considéré comme une extension de l'annuaire « Central » avec un formalisme différent. En effet, la source d'information pour l'alimentation automatisée du périmètre du fournisseur d'identité « Janus » est l'annuaire « Central ». L'alimentation des comptes pour le fournisseur d'identité « Janus-ext »se fait par le biais de fichiers plats.

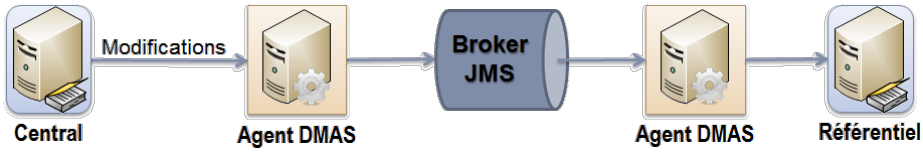


Figure 30 - Schéma des flux d'informations vers l'annuaire « Référentiel »

La branche « ou=people, dc=cnrs, dc=fr » utilisée par le fournisseur d'identité Janus reprend les informations extraites de Labintel pour les personnels travaillant dans les unités du CNRS. Les conditions de synchronisation avec Labintel sont identiques à celles de l'annuaire « Central ». Bien que les données issues de Labintel soient strictement communes, le formalisme des attributs diffère. En effet, le format se rapproche de la norme SupAnn 2009 développée par les universités françaises et pilotée par le groupement Renater. Les autres types de compte utilisateur sont placés dans la branche des extérieurs « ou=foreigner, dc=cnrs, dc=fr ». Dans cette arborescence, la feuille « ou=contractors » permet de gérer les comptes utilisateurs des prestataires. Elle est utilisée par le fournisseur d'identité « Janus-Ext ». La feuille « ou=others » accueille tous les autres comptes utilisateurs. La feuille « ou=formation » disponible uniquement en recette ne peut recevoir que des comptes temporaires utilisés uniquement lors de formation sur des outils mis en œuvre par la DSI du CNRS.

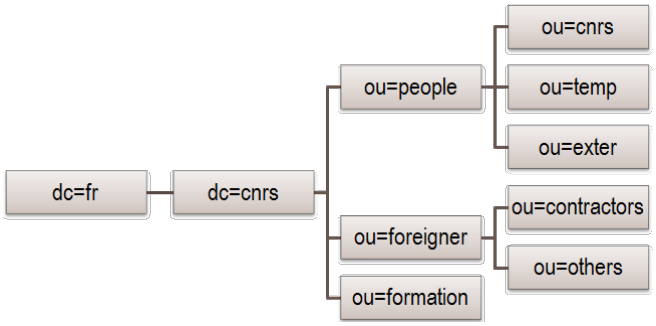


Figure 31 - Structure de l'annuaire « Référentiel »

A l'instar de l'annuaire « Central » l'annuaire « Référentiel », l'alimentation de la branche « people » est entièrement automatisée par l'outil DMAS.

5. L'agent DMAS « Référentiel » écoute la file de message JMS en provenance de l'annuaire « Central » et prend en compte les mises à jour.
6. L'agent DMAS « Référentiel » alimente l'annuaire « Référentiel ».
7. L'agent DMAS « Référentiel » vérifie que l'opération s'est correctement déroulée.
8. Si le compte est correctement créé ou mis à jour dans l'annuaire « Référentiel », l'agent DMAS « Référentiel » envoie un message sur le broker JMS.

Les comptes des branches « foreigner » et « formation » sont gérés manuellement par l'équipe responsable de l'exploitation technique des applications du système d'information du CNRS. Dans ce cas, l'agent DMAS ne prend pas en compte ces comptes. Les mises à jour de ces comptes ne sont donc pas propagées automatiquement.

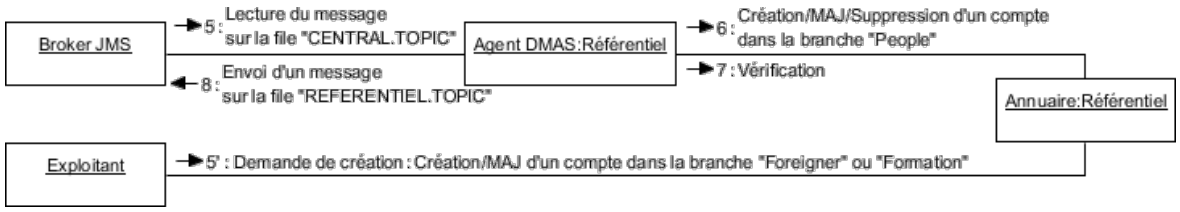


Figure 32 - Diagramme de collaboration de l'alimentation de l'annuaire « Référentiel »

Des attributs spécifiques permettent de gérer les droits d'accès macroscopiques à certaines applications dont les fournisseurs de service sont dans le domaine du fournisseur d'identité « Janus » ou « Janus-ext ». Dans ce cas, ces attributs particuliers permettent une gestion des accès de type ABAC. Les habilitations fines sont alors octroyées au sein des applications.

IV.2.4 Annuaire « SAP »

Pour les applications basées sur SAP, dont SIRHUS, la fonctionnalité d'authentification est assurée par le fournisseur d'identité Janus. L'administration des droits d'accès aux fonctionnalités des outils SAP, est réalisée dans une base de comptes propre à SAP. Celle-ci est alimentée toutes les quinze minutes par un outil spécifique SAP depuis un annuaire LDAP lui-même synchronisé avec l'annuaire « Référentiel » par l'outil DMAS.

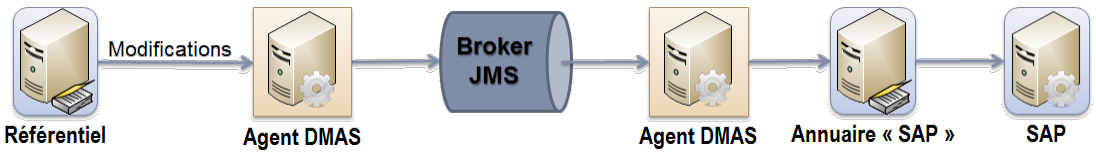


Figure 33 - Schéma des flux d'informations vers l'annuaire « SAP »

L'administration des comptes pour les outils SAP ne peut être réalisée que dans l'annuaire SAP, car la base de comptes est entièrement vidée et chargée périodiquement.

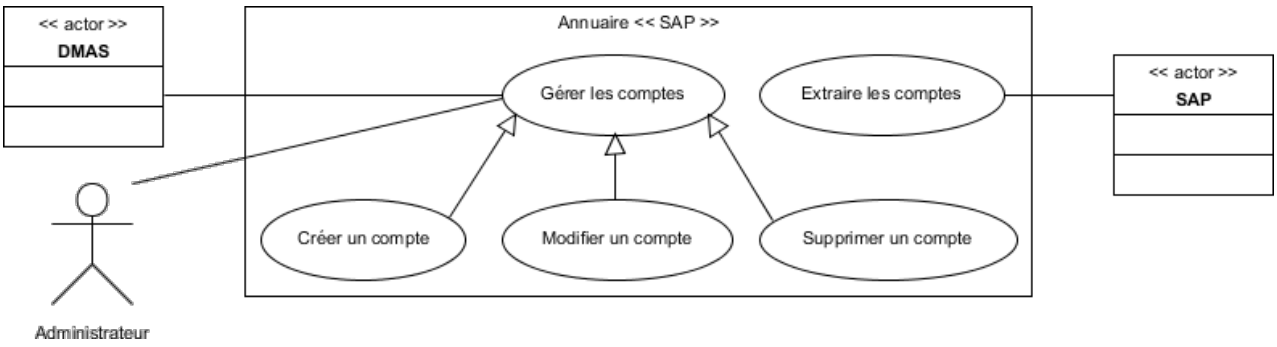


Figure 34 - Cas d'utilisation de l'annuaire « SAP »

L'approvisionnement dans l'annuaire « SAP » est réalisé automatiquement pour les comptes de l'annuaire « Référentiel » déclarés comme titulaire du CNRS, directeur d'unité ou affecté dans le rôle « Utilisateur SAP ».

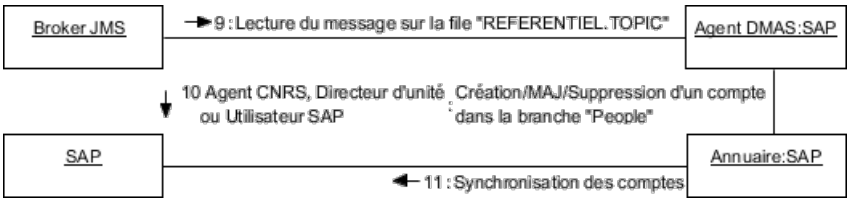


Figure 35 - Diagramme de collaboration de l'alimentation de l'annuaire « SAP »

La structure de l'arborescence comporte une seule branche correspondant aux racines transverses des annuaires « Central » et « Référentiel ».

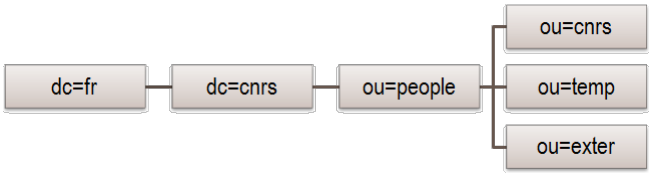


Figure 36 - Structure de l'annuaire « SAP »

IV.2.5 Annuaires de messagerie « CORE-ADM » et « CORE-Labo »

Chaque délégation régionale ainsi que la DSI met en œuvre des annuaires Microsoft Active Directory « CORE-ADM » pour les unités administratives qui sont sous la responsabilité des délégations régionales. Chacun de ces annuaires fait partie d'une forêt d'annuaires qui permet une réplication en local des autres annuaires, mais reste géré indépendamment. Ainsi chaque délégation régionale est responsable de la gestion du cycle de vie de ses comptes utilisateurs.

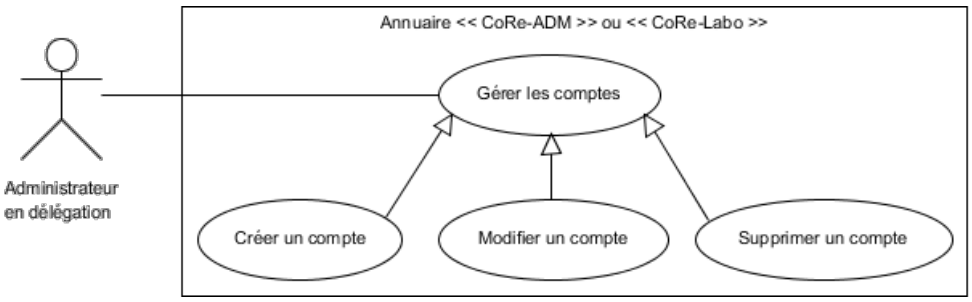


Figure 37 - Cas d'utilisation des annuaires « CORE » impliqués dans la gestion des identités

Actuellement, les annuaires sont alimentés par des processus propres à chaque délégation, mais il est prévu à terme qu'ils soient synchronisés avec Labintel ou l'annuaire « Référentiel ».

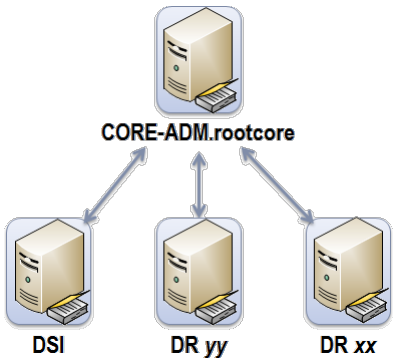


Figure 38 - Schéma des flux de la forêt d'annuaires « CORE-ADM »

Par ailleurs, la DSI a mis en place une offre de service dont une plate-forme d'hébergement de messagerie « CORE-Labo » à destination des unités de recherche dont le CNRS est une des tutelles. L'annuaire sous-jacent est alimenté avec les données issues de Labintel à l'exception des comptes gérés par « CORE-ADM ». A cet effet, l'EAI, abonné au fil de message véhiculé par le broker JMS de l'outil DMAS, met à jour l'annuaire Active Directory « CORE-Labo » grâce au flux spécifique « Flow-AD-Core ».

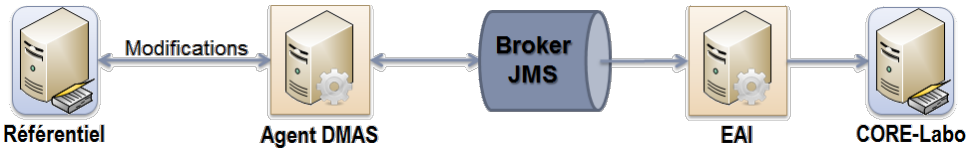


Figure 39 - Schéma du flux d'alimentation de l'annuaire « CORE-Labo »

A l'instar des annuaires « CORE-ADM », la gestion des annuaires « CORE-Labo » est assurée dans les délégations régionales par les RSI.

L'ensemble des annuaires « CORE » possède la même structure permettant de gérer les comptes de messagerie, les comptes utilisateurs et leurs habilitations dans les outils Microsoft SharePoint (cf. paragraphe « Recueil des besoins »).

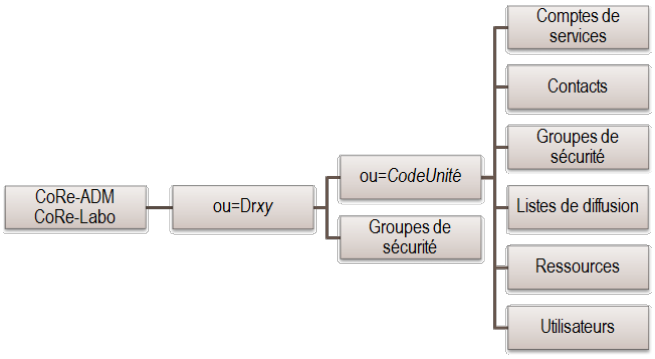


Figure 40 - Structure des annuaires « CORE-ADM » et « CORE-LABO »

IV.2.6 IHM

L'outil « IHM » est une application Web à destination des administrateurs pour leur permettre de consulter les informations sur les comptes utilisateurs dans les annuaires « Central », « Référentiel » et « SAP ». Il permet également de déléguer la gestion de l'affectation des attributs utilisés dans les contrôles d'accès aux applications au travers du portail Janus aux administrateurs des délégations régionales.

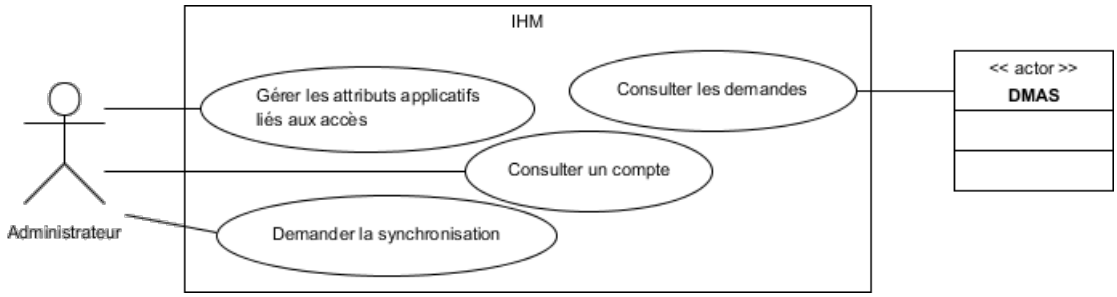


Figure 41 - Cas d'utilisation de l'IHM

L'application Web « IHM » dispose d'une base de données où sont enregistrées les demandes de modifications. Ces informations sont traitées par l'outil DMAS qui les propage ensuite à l'annuaire cible.

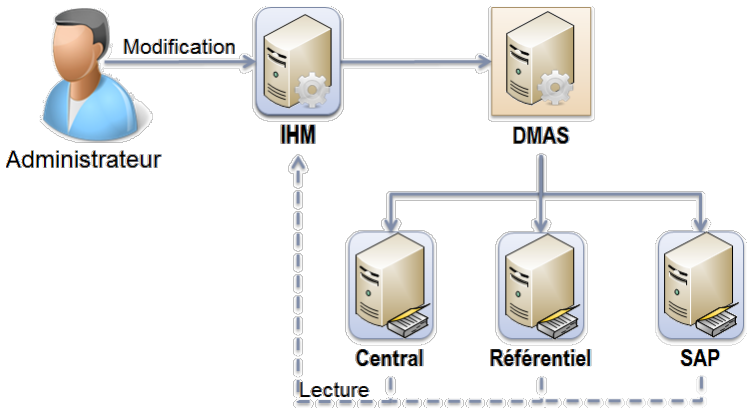


Figure 42 - Schéma des flux IHM

IV.2.7 Gestion des mots de passe

L'outil Sésame permet de rechercher un compte utilisateur et d'en changer le mot de passe dans les annuaires « Central », « Référentiel » et « CORE-LABO ». Pour pouvoir changer son mot de passe, un utilisateur recherche son compte dans l'outil. Ensuite, il peut demander le changement de mot de passe pour ce compte. Un courriel est automatiquement envoyé. Il contient un ticket électronique sous forme de lien hypertexte. Ce lien mène à un formulaire pour saisir le nouveau mot de passe en respectant des conditions fixées dans la PSSI du CNRS. A la soumission du mot de passe, le ticket devient invalide et ne peut être réutilisé.

Conjointement, il est également possible de demander à un administrateur d'effectuer la demande de changement de mot de passe. Ce dernier peut également visualiser les demandes en cours et d'annuler une demande en cas de problème.

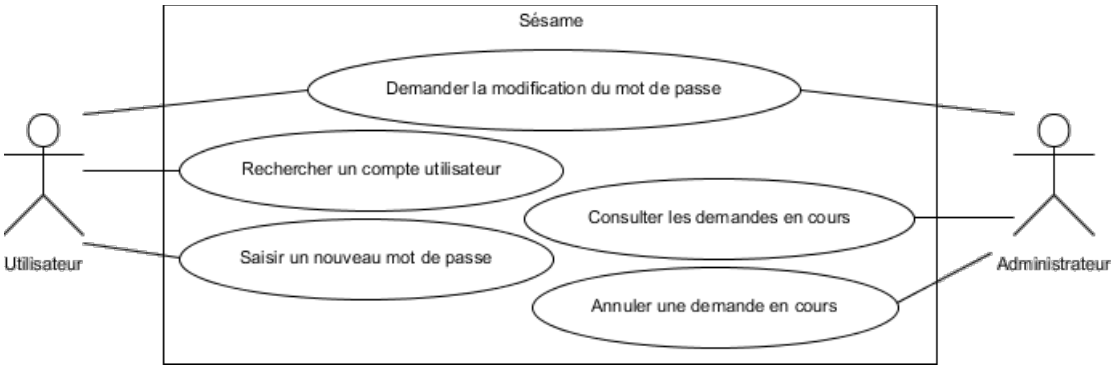


Figure 43 - Cas d'utilisation de Sésame

L'ordre de modification est envoyé directement et en parallèle aux différents annuaires sans l'intermédiaire de l'outil DMAS. Ensuite, l'action n'est pas réversible et il n'est pas possible de lire le mot de passe en clair à partir des annuaires.

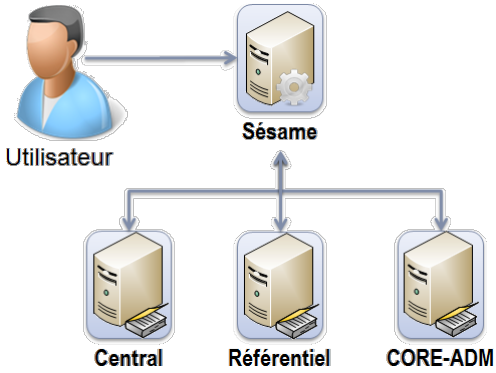


Figure 44 - Schéma du flux de changement de mot de passe

Actuellement, la politique de sécurité pour la durée de vie des mots de passe n'est pas mise en œuvre car les outils ne permettent de communiquer à l'utilisateur la fin de validité de son mot de passe.

IV.2.8 Infrastructure de Gestion des Clés (IGC)

Afin de faciliter l'authentification des comptes utilisateurs, le CNRS propose une alternative aux nombreux mots de passe imposés par les applications de son système d'information. Les certificats électroniques sont les cartes d'identité numériques des comptes utilisateurs liés à une entité. Pour une personne, le certificat contient entre autres le nom de l'autorité qui a créé le certificat, le nom et le prénom de la personne, son entreprise, son adresse électronique, son service (l'unité dans le cas du CNRS), les dates de validité du certificat ainsi qu'une signature électronique.
De même que des cartes d'identité sont émises par des autorités compétentes, les préfectures, les certificats électroniques sont émis par des autorités de certification (AC).
Pour chaque unité, une personne est nommée en tant qu'autorité d'enregistrement (AE). Elle a autorité pour valider les demandes de certificat du personnel et des ressources de cette unité. Cette personne est par défaut le directeur. Ce dernier peut déléguer cette fonction à une personne de confiance de son unité qui agira en son nom pour ces procédures.

Le CNRS a déployé une Infrastructure de Gestion de Clés pour administrer les différentes autorités de certification qui délivrent les certificats pour les serveurs et les personnels qui travaillent dans une unité du CNRS ou dans un projet de grille de calcul. Ainsi l'autorité de certification « CNRS2-Standard » s'adresse à toutes les personnes travaillant dans une unité pour laquelle le CNRS est une des tutelles pour des utilisations standard. Les personnes qui sont autorité d'enregistrement de l'IGC CNRS utilisent des certificats délivrés par l'autorité de certification « CNRS2-Plus ». L'IGC du CNRS intègre des autorités de certification pour les serveurs, dont « CNRS2-Projets/SIG2 » pour les applications de la DSI du CNRS.

Les principales fonctions d'une IGC pour la gestion des certificats sont l'enregistrement de demande et la vérification des critères d'attribution, la création des certificats, la diffusion des certificats, la gestion des listes de révocation, l'archivage des certificats et la délégation de pouvoir à d'autres entités.

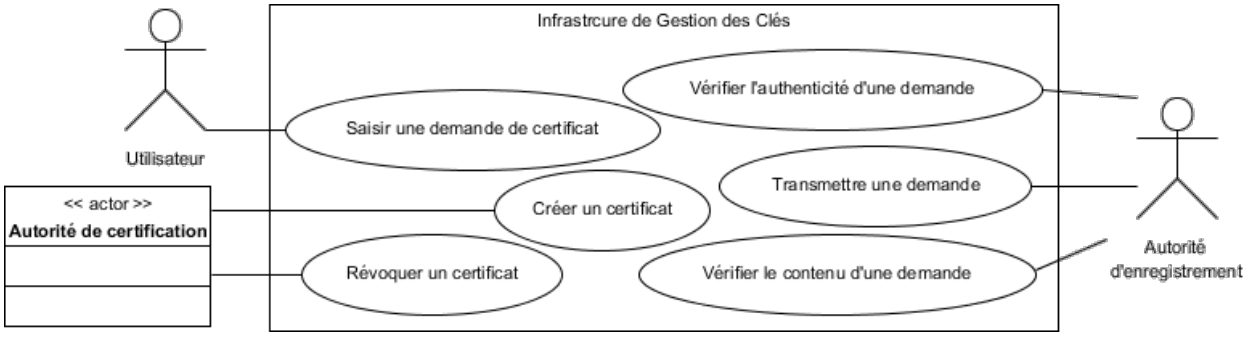


Figure 45 - Cas d'utilisation de l'infrastructure de gestion des clés

Le processus de création de certificat pour un utilisateur est le suivant :

1. L'utilisateur saisit un formulaire électronique en ligne qui demande toutes les données qui vont figurer dans le certificat.
2. Un message électronique est envoyé à l'utilisateur pour confirmation et vérification de l'adresse de courrier électronique.
3. L'autorité d'enregistrement est avertie par messagerie électronique qu'une demande de certificat est arrivée.
4. L'autorité d'enregistrement vérifie dans Labintel les informations contenues dans la demande.
5. L'autorité d'enregistrement contacte le demandeur pour vérifier s'il est à l'origine de cette demande. Si la demande est validée, elle est transmise à l'autorité de certification.
6. L'autorité de certification crée le certificat puis le dépose sur un serveur Web et dans l'annuaire LDAP des certificats CNRS, puis envoie un message électronique à l'utilisateur.
7. L'utilisateur récupère son certificat sur le serveur Web.

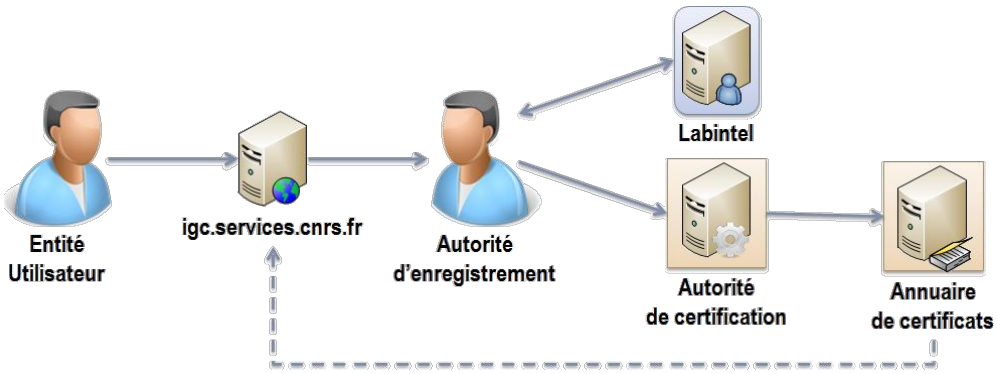


Figure 46 - Schéma des flux de création de certificat

IV.2.9 Janus et la fédération d'identité

Le projet Janus débuté en 2008 avait pour premier objectif de déployer en 2009 un fournisseur d'identité pour le CNRS ainsi qu'un fournisseur de service pour l'application SIRHUS. Depuis 2011, Janus assure la délégation de l'authentification pour toutes les nouvelles applications mises en place par la DSI du CNRS. Plusieurs instituts ont également mis en œuvre des fournisseurs de service autour du fournisseur d'identité Janus.

Le fournisseur d'identité Janus est enregistré auprès de la fédération « Éducation-Recherche » qui est l'infrastructure nationale de fédération d'identités couvrant le périmètre des établissements de l'enseignement supérieur et de la recherche. La fédération constitue un cercle de confiance réalisé par l'inscription et la validation de ses participants auprès de l'opérateur de la fédération, Renater, mais aussi par leur engagement à respecter un cadre technique. Le GIP spécifie des recommandations liées à la sécurité, à la gestion d'identités et fixe les normes et les protocoles utilisés. Les accès via le mécanisme de fédération d'identités sont basés sur la transmission, par les fournisseurs d'identités, d'un ensemble d'attributs utilisateurs nécessaires à chaque ressource. Ces informations sont issues de référentiels d'établissements respectant les recommandations SupAnn, l'annuaire « Référentiel » pour le CNRS avec Janus. Les valeurs des attributs sont échangées entre les fournisseurs via le protocole d'assertions sécurisées SAML2. Ce dernier est le protocole standard de la fédération « Éducation-Recherche » adopté par la plupart des fédérations d'identités académiques dans le monde. Par ailleurs Il existe un projet de mise en relation des fédérations d'identités académiques nommé eduGAIN. La participation à eduGAIN se fait par inscription volontaire de l'établissement voulant y opérer son fournisseur d'identités ou y proposer une ou plusieurs de ses ressources. Le fournisseur d'identité doit alors respecter la norme EduPerson.

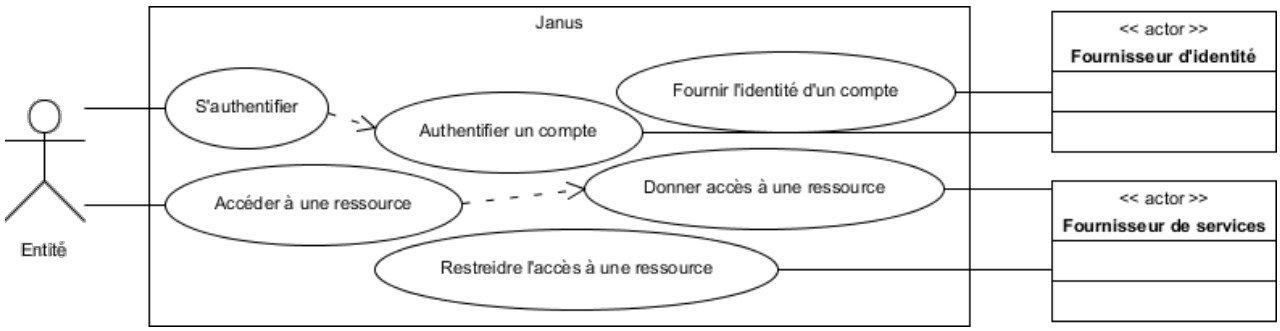


Figure 47 - Cas d'utilisation de Janus

Le fournisseur d'identité s'appuie sur la technologie Shibboleth en version 2.3. Cet outil est largement répandu dans la construction de fédérations d'identité dans les communautés de l'enseignement supérieur et de la recherche européennes et nord américaines. La phase d'authentification est déléguée à l'outil CAS (Central Authentication Service) qui est un système de SSO développé par l'université américaine de Yale.

Le fournisseur de service repose sur l'outil Shibboleth SP pour les applications mises en œuvre par la DSI du CNRS. Cependant, le format d'échange d'informations entre les fournisseurs d'identité et de services étant prescrit dans le cadre de la fédération « Éducation-Recherche », il est possible d'utiliser tout type de fournisseur de service qui respecte le standard SAML2, tel que SimpleSAMLphp.

Le processus d'accès à une ressource du CNRS au travers de Janus est le suivant :

1. L'utilisateur tente d'accéder à une ressource. Dans le cas des applications protégées par Janus, le rôle de fournisseur de service est assuré par un reverse proxy.

1'. (*Optionnel*) Si l'accès à la ressource est ouvert à d'autres fournisseurs d'identité que Janus, l'utilisateur doit préciser son établissement auprès du service WAYF (Where Are You From).

2. Le module Shibboleth SP installé sur le serveur reverse-proxy redirige le navigateur vers son fournisseur d'identité. Celui-ci vérifie si l'utilisateur est déjà authentifié. Dans ce cas, le navigateur est redirigé vers le fournisseur d'identité, ce qui évite les deux étapes suivantes. Sinon, le navigateur est redirigé vers le système d'authentification CAS.

3. Le serveur CAS envoie une demande d'authentification d'abord par certificat électronique. A défaut, l'utilisateur s'authentifie par un formulaire d'authentification avec son identifiant qui correspond à son adresse électronique et son mot de passe. Dans le cas du certificat, le serveur CAS teste la validité du certificat.

4. Si l'authentification se fait par identifiant et mot de passe, le serveur CAS vérifie dans un premier temps dans l'annuaire l'existence d'une entrée correspondant à cette adresse électronique. Puis une seconde requête dans l'annuaire tente d'authentifier cette entrée avec le

mot de passe fourni.

5. Après authentification sur le serveur CAS, celui-ci redirige le navigateur vers le fournisseur d'identité en fournissant un ticket TGT (« Ticket Granting Ticket » en anglais).
6. Le fournisseur d'identité se connecte au serveur CAS pour vérifier la validité du ticket et récupérer l'identifiant de l'utilisateur, son adresse électronique.
7. Le fournisseur d'identité fait ensuite une requête dans l'annuaire pour obtenir les attributs de l'entrée correspondante, dont ceux utilisés comme filtre d'accès.
8. Le fournisseur d'identité redirige le navigateur vers le reverse-proxy en fournissant un flux SAML2. Cette assertion contient un identifiant opaque ainsi que les attributs récupérés précédemment. Le fournisseur de service est configuré pour vérifier la présence d'un attribut dont l'une des valeurs doit vérifier une expression régulière. Si cette vérification est satisfaite, le module reverse-proxy envoie les informations vers la ressource en tant qu'en-têtes http.
9. L'utilisateur est authentifié auprès de la ressource et le navigateur reçoit la page demandée.

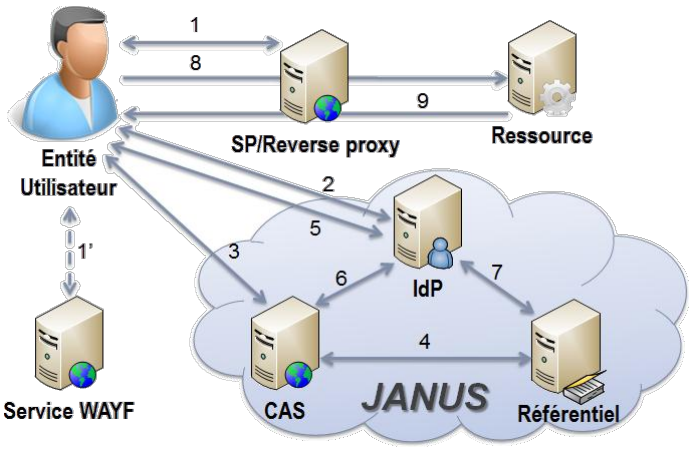


Figure 48 - Schéma des flux de connexion par Janus

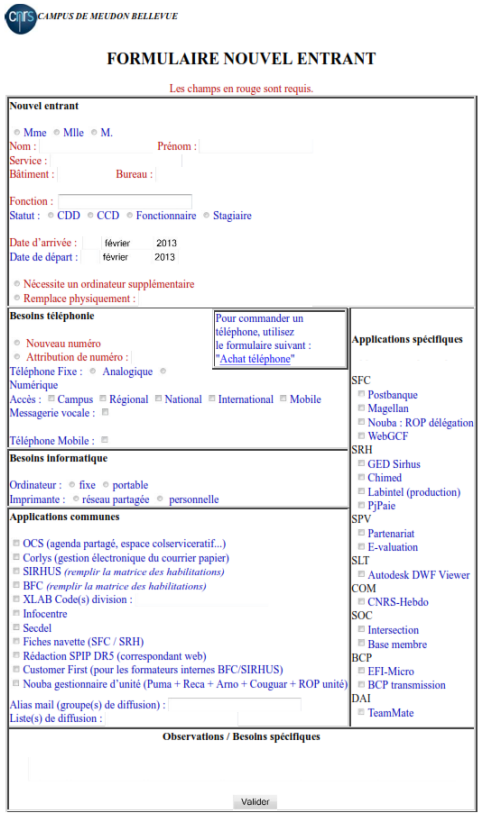
IV.2.10 Ressources locales dans les unités

Pour gérer les accès aux ressources d'une unité, chacune d'entre elle déploie ses propres annuaires ou référentiels et développe ses propres outils. Ces ressources difficiles à recenser car dispersées ne sont pas prises en compte dans la présente étude.

Parallèlement, avant le déploiement des annuaires « CORE-ADM », les délégations régionales avaient mis en œuvre des annuaires locaux pour gérer les comptes utilisateurs et les comptes de messagerie des services administratifs du CNRS. Notamment, la délégation régionale d'Aquitaine DR15, est abonnée au fil de messages « CENTRAL.TOPIC » du broker JMS de l'outil DMAS pour alimenter un annuaire local qui sert pour la messagerie. Depuis le déploiement des

annuaires « CORE-ADM », le contenu de ces annuaires locaux est intégré à la forêt d'annuaires. De ce fait, ces annuaires régionaux ne sont pas pris en compte dans le périmètre de la présente étude.

Pour gérer ces différents référentiels régionaux, chaque délégation régionale a mis en place des processus et des outils indépendants de gestion des demandes de création de compte et d'accès aux applications déployées par la délégation régionale ou par la DSI du CNRS. Ainsi la délégation régionale d'Ile de France Ouest & Nord DR05, a développé un formulaire spécifique qui permet au gestionnaire de l'unité ou à son administrateur systèmes et réseaux de demander la création d'un compte et les accès nécessaires pour un nouvel entrant. La demande est générée sous forme de fichier Microsoft Excel qu'un administrateur traite manuellement en utilisant différents outils, dont l'IHM cité précédemment.


CAMPUS DE MEUDON BELLEVUE

FORMULAIRE NOUVEL ENTRANT

Les champs en rouge sont requis.

Nouvel entrant

Mme Mlle M.
Nom : Prénom :
Service :
Bâtiment : Bureau :
Fonction :
Statut : CDD CCD Fonctionnaire Stagiaire
Date d'arrivée : février 2013
Date de départ : février 2013
Nécessite un ordinateur supplémentaire
Remplace physiquement :

Besoins téléphonie
Nouveau numéro
Attribution de numéro :
Téléphone Fixe : Analogique Numérique
Accès : Campus Régional National International Mobile
Messagerie vocale :
Téléphone Mobile :
Pour commander un téléphone, utilisez le formulaire suivant : "Achat téléphone"

Besoins informatique
Ordinateur : fixe portable
Imprimante : réseau partagée personnelle

Applications communes
OCS (agenda partagé, espace colserviceratif...)
Corlys (gestion électronique du courrier papier)
SIRHUS *(remplir la matrice des habilitations)*
BFC *(remplir la matrice des habilitations)*
XLAB Code(s) division :
Infocentre
Secdel
Fiches navette (SFC / SRH)
Rédaction SPIP DR5 (correspondant web)
Customer First (pour les formateurs internes BFC/SIRHUS)
Nouba gestionnaire d'unité (Puma + Reca + Arno + Couguar + ROP unité)
Alias mail (groupe(s) de diffusion) :
Liste(s) de diffusion :

Applications spécifiques
SFC
Postbanque
Magellan
Nouba : ROP délégation
WebGCF
SRH
GED Sirhus
Chimed
Labintel (production)
PjPaie
SPV
Partenariat
E-valuation
SLT
Autodesk DWF Viewer
COM
CNRS-Hebdo
SOC
Intersection
Base membre
BCP
EFI-Micro
BCP transmission
DAI
TeamMate

Observations / Besoins spécifiques

Valider

Figure 49 - Exemple de formulaire de gestion des comptes et des accès développé dans une délégation régionale

Bien que ces applications spécifiques ne rentrent pas dans le périmètre de la présente étude, les besoins auxquels ils ont répondu doivent être pris en compte dans le cadre d'un projet global CNRS de gestion des identités et des accès.

IV.2.11 Cartographie générale des flux d'identité

La DSI du CNRS dispose donc d'un système centralisé pour les flux d'identités au travers notamment de l'outil DMAS. Pourtant, les possibilités d'interaction et de contrôle du cycle de vie des identités sont limitées.

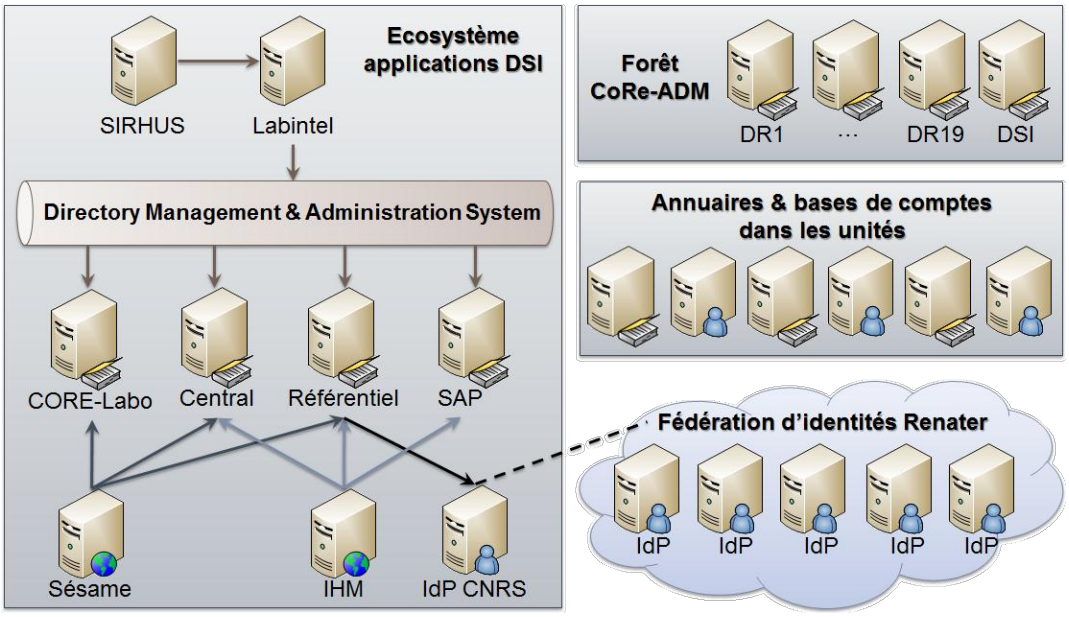


Figure 50 - Schéma des flux d'informations liés aux identités

Dans le système d'information du CNRS, la gestion des accès est assurée par ABAC. En effet, le positionnement d'attributs dans les annuaires « Central » et « Référentiel » permettent à Janus ou aux applications clientes de restreindre l'accès aux seuls comptes détenteurs. Les attributs utilisés pour limiter les accès à une application sont « CnrsRole » et « RefRole » respectivement pour les annuaires « Central » et « Référentiel ». Ce type d'attribut peut être perçu comme le support à la notion de rôle applicatif.

IV.3 Cycle de vie des identités

IV.3.1 Définition du périmètre

Les personnes travaillant pour les unités du CNRS, propres ou mixtes, sont répartis dans deux catégories d'emploi : les chercheurs et les ingénieurs, techniciens, administratifs (ITA). Cette distinction pourra être prise en compte au niveau des rôles, mais ne fait pas l'objet d'une gestion différenciée des personnes.

La difficulté de gestion d'une personne est liée aux types de contrat. Un personnel permanent n'a pas le même parcours qu'un employé en contrat à durée déterminée. De plus, une personne peut être affectée à une ou plusieurs unités suivant une quotité de temps de travail préétablie.

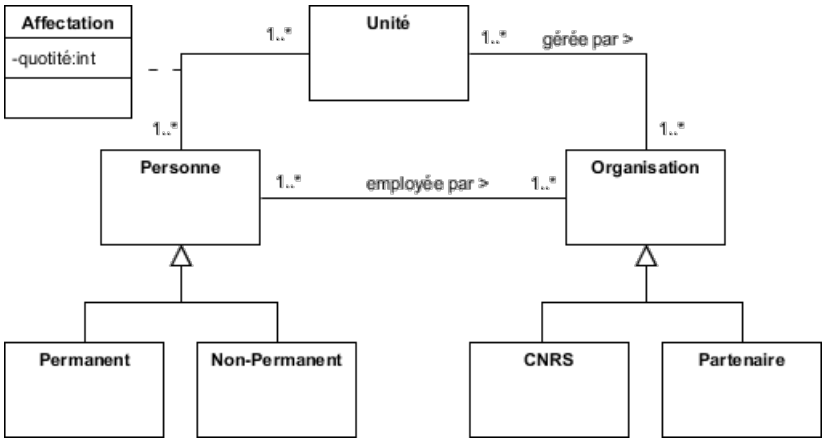


Figure 51 - Diagramme de classe des Personnes

Pour le périmètre de la gestion des identités, les cas d'utilisation concernant le cycle de vie des personnes au sein du CNRS devant être pris en compte sont les suivants :

- Recrutement d'un nouveau personnel CNRS ou non CNRS
- Gestion du contrat CNRS, dont la prolongation du contrat pour les contrats à durée déterminée
- Modifications d'informations sur l'identité de la personne
- Départ de la personne, dont le changement d'établissement, la mise en disponibilité ou le départ à la retraite
- Changement de structure de l'unité, suite à éclatement de l'unité en plusieurs unités ou la fusion de plusieurs unités
- Mobilité au sein du CNRS

Un cas particulier du cycle de vie devant être étudié concerne la nomination d'un directeur d'unité (DU). En effet, les entrevues ont permis de mettre en évidence que ce type de personnel

joue un rôle particulier dans le cycle de vie des comptes utilisateurs du système d'information du CNRS.

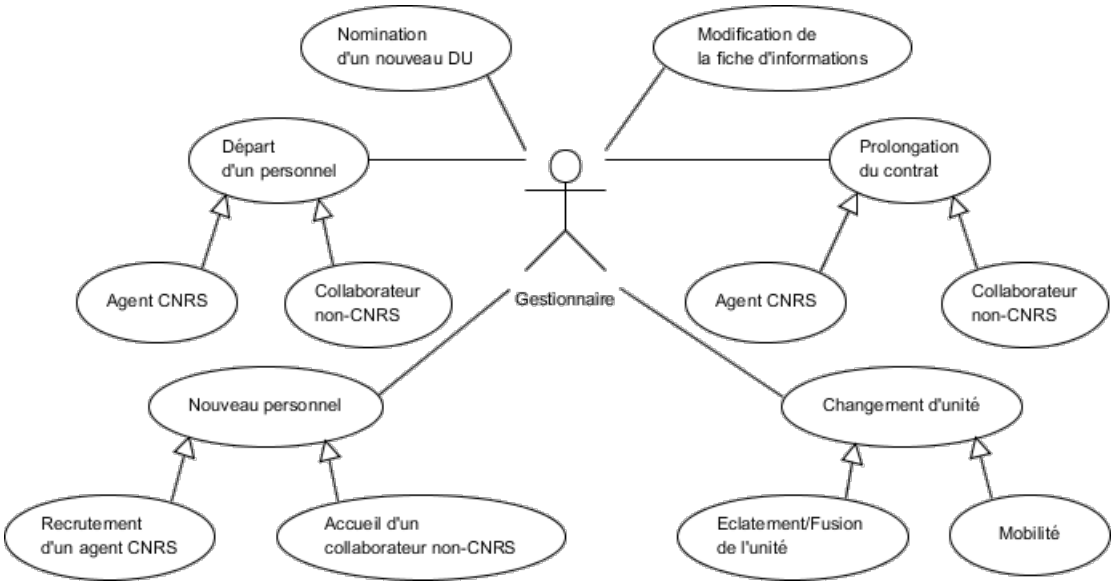


Figure 52 - Cas d'utilisation du cycle de vie d'une personne

Les cas d'utilisation de gestion des identités ont pu être détaillés suite aux entrevues avec une gestionnaire au service des ressources humaines, un des responsables techniques de SIRHUS à la DSI et le responsable technique de Labintel pour les personnes à la DSI.

IV.3.2 Nouveau personnel

IV.3.2.1 Recrutement d'un agent CNRS

Dans le cas d'un recrutement CNRS, la source d'information est le dossier SIRHUS. Celui-ci n'est exposé aux autres applications qu'à condition que son affectation soit effective. C'est à partir de ce moment que le dossier est importé dans Labintel, puis qu'un compte est créé dans les différents annuaires

- ***Permanent : recrutement sur concours***

1. Le service des concours envoie la notification de réussite au concours au candidat.
2. Le candidat accepte la nomination du concours et l'envoie au service des concours.
3. Le service des concours envoie les informations sur la personne et l'affectation au service des ressources humaines.
4. A la réception, le gestionnaire des ressources humaines crée une fiche « agent ». Un numéro de matricule est affecté à la fiche et la tranche de décompte de paie est positionnée par défaut à

« non significatif » (valeur « 99 » dans l'application). De ce fait, cet état implique que la fiche n'est pas propagée dans le système d'information.

5. A la date de prise de fonction, un procès verbal d'installation est envoyé à l'agent.
6. Après signature, l'agent renvoie le procès verbal d'installation au service des ressources humaines de sa délégation d'affectation.
7. La mesure administrative de recrutement au CNRS est enregistrée dans SIRHUS. La tranche de décompte est positionnée à « mensuel » (valeur « F0 » dans l'application).
8. La fiche est visible dans le demi-flux d'extraction SIRHUS « Format Pivot Personnel » pour pouvoir être consommée par les autres applications du système d'information quand la situation est effective.

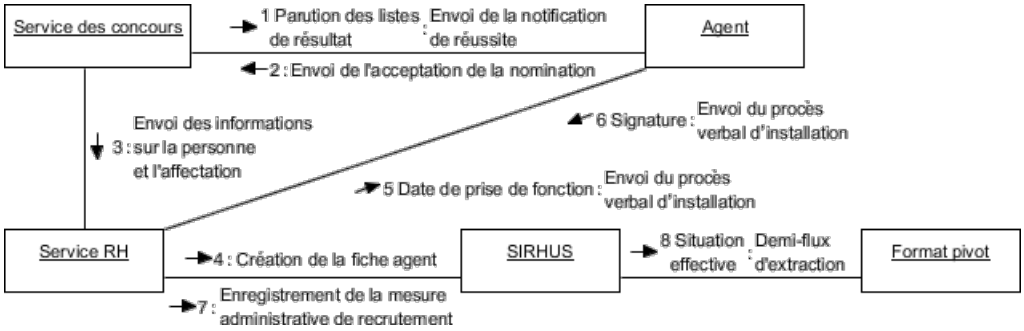


Figure 53 - Diagramme de collaboration d'un recrutement CNRS sur concours

Bien que la fiche agent ait pu être créée et complétée plusieurs mois à l'avance, elle n'est visible dans le système d'information que plusieurs jours après la prise de fonction de l'agent. En effet, l'affectation n'est positionnée comme effective dans SIRHUS, qu'à partir du retour du procès verbal d'installation signé par l'agent dans son unité. C'est seulement à partir de ce moment que la personne apparaît dans l'extraction EAI « Format pivot », ce qui déclenche le processus de création de compte utilisateur décrit dans le paragraphe suivant.

- ***Non permanent : recrutement sur contrat à durée déterminée***

1. Le directeur d'unité initie la procédure de recrutement par l'envoi de la demande au service des ressources humaines de la délégation régionale dont dépend l'unité
2. A la réception de la demande, le gestionnaire des ressources humaines l'étudie. Elle peut être refusée à cause de justificatifs administratifs insuffisants par exemple. Si elle est jugée conforme, une fiche « agent » est créée dans SIRHUS. Un numéro de matricule est affecté à la fiche et la tranche de décompte de paie est positionnée par défaut à « non significatif » (valeur

« 99 » dans l'application). De ce fait, cet état implique que la fiche n'est pas propagée dans le système d'information.

3. Une demande d'autorisation est envoyée au service financier pour paiement. L'étude de cette demande peut nécessiter un jour à une semaine. Pendant ce temps, la fiche est positionnée au statut « attente »
4. Si la demande est validée, une notification de décision est envoyée à la délégation régionale pour signature, ce qui peut prendre jusqu'à trois jours.
5. Cette décision est envoyée à l'agent pour signature.
6. Après signature, l'agent renvoie le procès verbal d'installation au service des ressources humaines de sa délégation d'affectation.
7. La mesure administrative de recrutement au CNRS est enregistrée dans SIRHUS. La tranche de décompte est positionnée à « mensuel » (valeur « F0 » dans l'application).
8. La fiche est visible dans le demi-flux d'extraction SIRHUS « Format Pivot Personnel » pour pouvoir être consommée par les autres applications du système d'information quand la situation est effective.

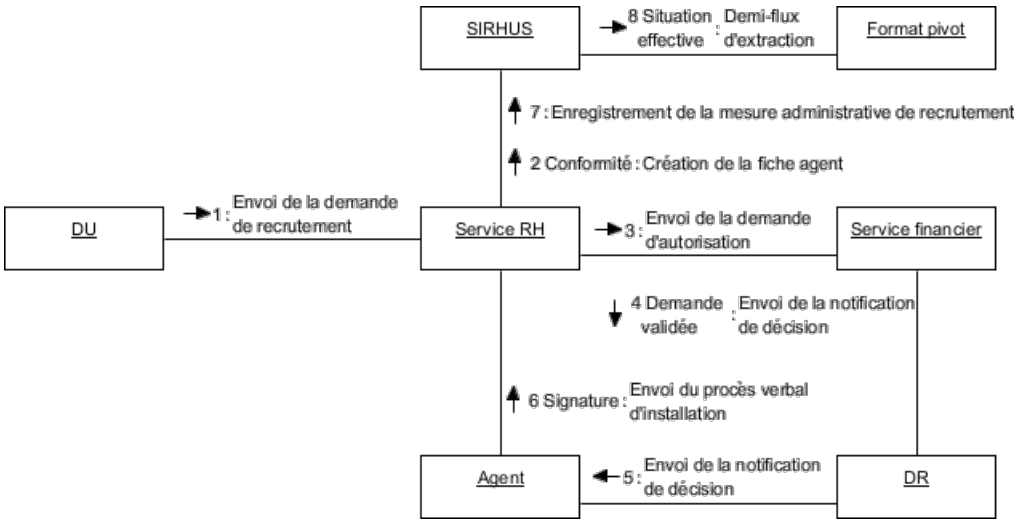


Figure 54 – Diagramme de collaboration d'un recrutement CNRS sur CDD

Finalement, il peut s'écouler trois semaines entre la demande de recrutement rédigée par le directeur d'unité et la prise en compte par l'ensemble du système d'information de la fiche de la personne recrutée. Ensuite, c'est à partir du flux « Format pivot » que le processus de création de compte utilisateur, décrit ultérieurement, est déclenché.

En outre, les personnels non destinés à percevoir une quelconque rémunération de la part du CNRS ne seront jamais exposés dans le format pivot personnel : c'est le cas par exemple des accueils en délégation et accueil en chaire non rémunérés par le CNRS.

- ***Création du compte utilisateur***

1. Lorsque le dossier SIRHUS est rendu visible au travers du demi-flux SIRHUS il est importé dans Labintel. Le processus d'import crée alors une fiche agent.
2. L'agent DMAS « Central » qui suit les activités de Labintel prend en compte l'information de création.
3. L'agent DMAS crée un nouveau compte dans l'annuaire « Central » dans la branche « CNRS » ou « TEMP », respectivement pour un permanent CNRS ou non permanent CNRS.
4. L'agent DMAS « Central » vérifie que l'opération s'est correctement déroulée
5. Si le compte est correctement créé, l'agent DMAS « Central » propage les informations sur la nouvelle affectation en tant que message pour le broker JMS.
6. L'agent DMAS « Référentiel » écoute la file de message JMS en provenance de l'annuaire « Central » et prend en compte les informations sur le nouveau compte.
7. L'agent DMAS « Référentiel » crée un nouveau compte dans l'annuaire « Référentiel » dans la branche « CNRS » ou « TEMP ».L'agent attribue un identifiant « SAP username » pour les comptes de la branche « CNRS ».
8. L'agent DMAS « Référentiel » vérifie que l'opération s'est correctement déroulée.
9. Si le compte est correctement créé dans l'annuaire « Référentiel », un message est envoyé sur le broker.
10. L'agent DMAS « SAP » écoute la file de message JMS en provenance de l'annuaire « Référentiel » et prend en compte les informations sur le nouveau compte.
11. L'agent DMAS « SAP » crée un nouveau compte dans l'annuaire « SAP » dans la branche « CNRS » ou « TEMP ».
12. La base de comptes SAP est synchronisée avec l'annuaire « SAP » toutes les 15 minutes.

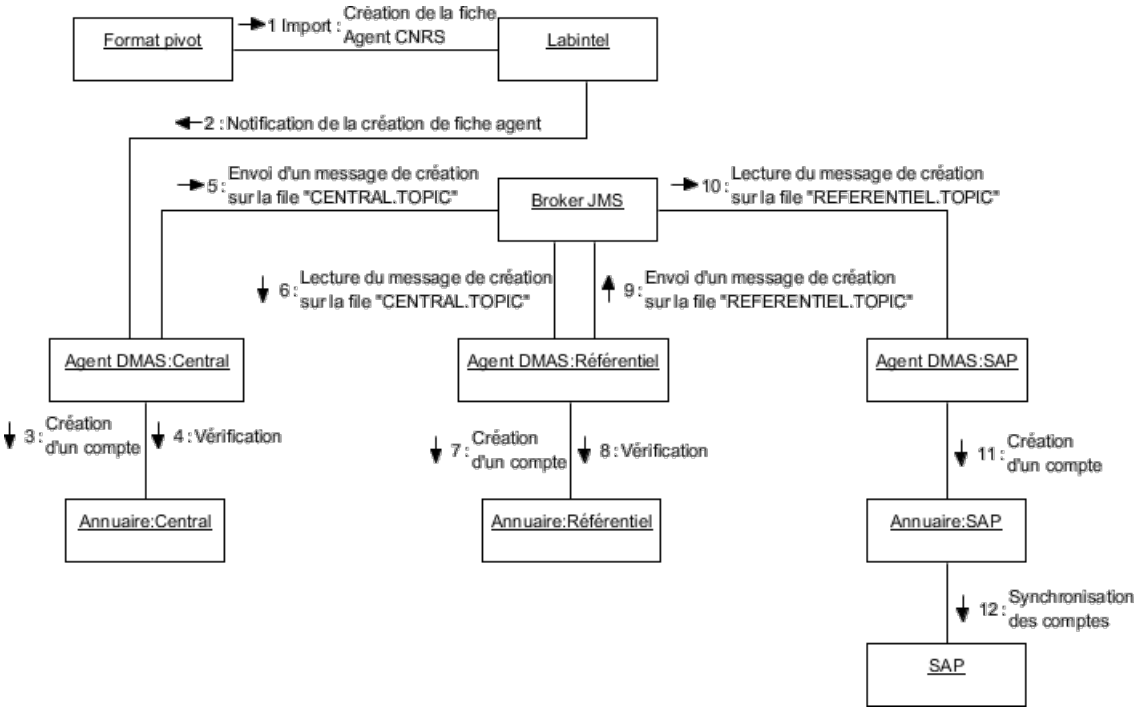


Figure 55 - Diagramme de collaboration de création de compte CNRS dans les annuaires

Le processus actuel répond parfaitement aux besoins de sécurité. En effet, il est préférable de s'assurer qu'un compte correspond à une personne physique présente en unité. Cependant, pour des raisons d'efficacité, le processus doit être amélioré pour permettre à une personne de travailler dès son arrivée dans l'unité. Sachant que dès que la personne est visible dans l'extraction « Format pivot », tout le processus est automatisé et quasi immédiat, le gain de temps ne peut être envisagé que pour faire apparaître l'affectation plus tôt dans les flux EAI. Dans ce cas, la fiche agent doit pouvoir être extraite alors que la prise de fonction n'est pas encore validée. Il faudrait alors modifier le processus d'extraction pour pouvoir prendre en compte toutes les fiches agent, même non entérinées. Ensuite, en dehors des processus automatisés, il serait nécessaire de créer une procédure nécessitant une intervention manuelle. Ainsi, une personne autorisée pourrait demander la création d'un compte utilisateur temporaire sur la fiche de l'agent non validée. La période d'activation du compte devrait alors être limitée pour permettre d'attendre la validation. Après la date d'échéance, le compte devrait être automatiquement suspendu.

IV.3.2.2 Enregistrement d'un collaborateur non CNRS

Le CNRS n'ayant pas d'accès aux systèmes de gestion du personnel des partenaires, les informations sur les personnes sont saisies manuellement par les gestionnaires des unités dans Labintel. De ce fait, la qualité des données n'est donc pas vérifiée et il est impossible de suivre l'activité d'une personne non-CNRS dans le système d'information du CNRS. De plus, une personne affectée dans plusieurs unités est saisie dans Labintel par différents gestionnaires et

aucune liaison n'est possible au travers de l'outil. Cette situation est à l'origine de la création d'un compte utilisateur par affectation.

Le processus d'enregistrement d'un agent non CNRS débute par la saisie d'une fiche agent à laquelle est attribué un séjour. Ensuite les outils DMAS créent les comptes dans les différents annuaires.

1. Le gestionnaire de l'unité crée une nouvelle fiche agent dans Labintel.
2. Le gestionnaire de l'unité crée un séjour dans Labintel pour la fiche agent.
3. L'agent DMAS « Central » qui suit les activités de Labintel prend en compte l'information de création.
4. L'agent DMAS crée un nouveau compte dans l'annuaire « Central » dans la branche « EXTER ».
5. L'agent DMAS « Central » vérifie que l'opération s'est correctement déroulée
6. Si le compte est correctement créé, l'agent DMAS « Central » propage les informations sur la nouvelle affectation en tant que message pour le broker JMS.
7. L'agent DMAS « Référentiel » écoute la file de message JMS en provenance de l'annuaire « Central » et prend en compte les informations sur le nouveau compte.
8. L'agent DMAS « Référentiel » crée un nouveau compte dans l'annuaire « Référentiel » dans la branche « EXTER ».
9. L'agent DMAS « Référentiel » vérifie que l'opération s'est correctement déroulée
10. Si le compte est correctement créé dans l'annuaire « Référentiel », un message est envoyé sur le broker.
11. L'agent DMAS « SAP » écoute la file de message JMS en provenance de l'annuaire « Référentiel ». Si l'agent est déclaré comme directeur d'unité ou affecté dans le rôle « Utilisateur SAP », l'agent DMAS « SAP » prend en compte les informations sur le nouveau compte.
12. L'agent DMAS « SAP » crée un nouveau compte dans l'annuaire « SAP » dans la branche « EXTER ».
13. La base de comptes SAP est synchronisée avec l'annuaire « SAP » toutes les 15 minutes.

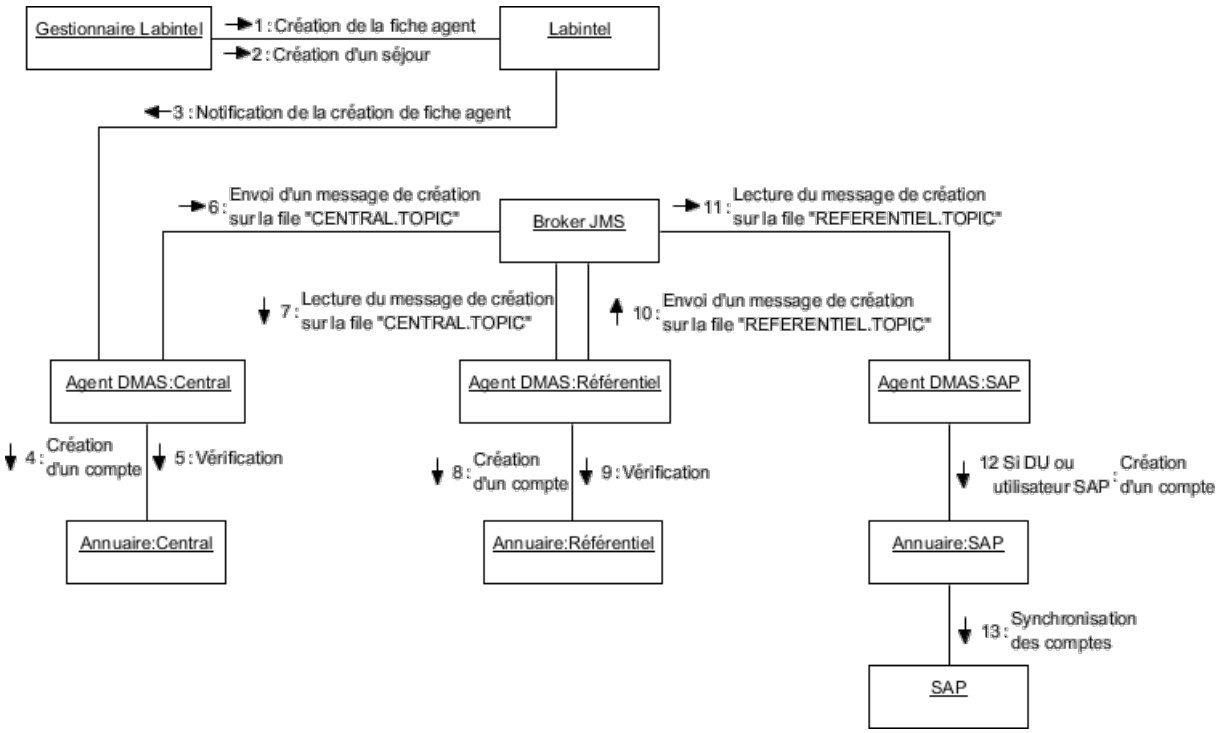


Figure 56 - Diagramme de collaboration de création de compte non CNRS dans les annuaires

IV.3.2.3 Enregistrement d'un personnel « privé »

Les unités ont la possibilité de faire intervenir des personnes sur leurs fonds propres (appelées personnel privé), que ce soit en contrat à durée indéterminée ou au travers d'une prestation de service. Dans ce cas, le CNRS n'a pas de visibilité sur ces contrats. C'est pour cette raison qu'actuellement, ces affectations ne sont pas prises en compte pour les outils DMAS. Il n'y a donc aucun processus automatique de génération de compte attenant à ces affectations. Pour des raisons de sécurité, il serait toutefois opportun que les comptes qui sont créés par d'autres moyens soient gérés pour les outils de gestion des identités et des accès du système d'information du CNRS.

IV.3.2.4 Personne extérieure

- ***Identité issue de la fédération***

Les comptes issus de la fédération d'identité Renater ne sont pas gérés par le CNRS, ce qui est l'avantage du modèle d'identité fédérée. Chaque application du système d'information fait le choix d'accepter les identités d'autres fournisseurs d'identité au travers du service WAYF proposé par Janus.

- ***Personne hors fédération***

Les comptes des personnes extérieures à la fédération Renater peuvent être créés par deux canaux distincts. Pour les personnes intervenant dans les unités du CNRS, un compte peut être alimenté dans l'annuaire « Référentiel » dans la branche « Foreigner ». Dans ce cas, ils peuvent être authentifiés et identifiés au travers du fournisseur d'identité « Janus-Ext ». Pour les autres personnes qui souhaitent utiliser des services proposés au niveau de la fédération d'identité, ils ont la possibilité de créer un Compte Réseau Universel (CRU) géré par Renater.

IV.3.2.5 Cas particuliers

Des personnes peuvent être payées par le CNRS sans appartenir à une de ses structures. C'est le cas notamment des inventeurs qui perçoivent une rémunération mais ne sont pas employés. Dans ce cas, pour la gestion de leur dossier administratif, ils sont affectés à une unité fictive, dont le code d'unité est « EXT_*codeDR*00 », qui représente les personnels hors structure CNRS.

La création de la fiche agent dans cette unité déclenche le processus de création d'un nouveau personnel dans SIRHUS. De ce fait, la personne dispose implicitement d'un compte dans les annuaires correspondant à cette affectation, même si elle est virtuelle, tant que la situation est effective. Ce comportement peut être considéré comme une faille de sécurité en offrant un moyen d'accès au système d'information non légitime puisque la personne ne travaille pas au sein du CNRS. Une règle de gestion doit donc être développée pour corriger cet effet de bord et gérer ces cas particuliers.

IV.3.3 Départ d'un personnel

IV.3.3.1 Sortie d'un agent CNRS

- ***Départ à la retraite***

La personne souhaitant partir à la retraite doit déposer une demande d'admission à la retraite six mois avant la date de cession d'activité envisagée. Le service du personnel remet à l'agent de pension civil qu'il doit compléter et retourner. A la réception, le service du personnel saisit la décision de radiation. A la date déterminée, la mesure de radiation est effective. Le dossier de la personne n'apparaît plus dans le flux « Format pivot ». L'affectation prend fin au niveau de Labintel, ce qui déclenche la suppression du compte sous-jacent dans les différents annuaires.

- ***Détachement***

Dans le cadre d'un détachement auprès d'un autre organisme, la personne reste affectée à l'unité du CNRS pendant un an. Après ce délai, elle est affectée à l'unité pour les personnels hors structure CNRS « EXT_*codeDR*00 » ce qui permet de gérer son dossier administratif. En effet, l'agent perçoit sa rémunération de l'organisme d'accueil mais continue à bénéficier de ses droits à l'avancement et à la retraite au CNRS.

A la fin du détachement, la personne réintègre son unité, si le détachement est inférieur à un an. Si le détachement est supérieur à un an, elle sera affectée à une nouvelle unité.

- ***Mise en disponibilité ou congé longue durée***

La disponibilité permet aux agents CNRS d'exercer leurs fonctions hors du CNRS. Elle peut être demandée pour réaliser des études ou recherches présentant un intérêt général, pour convenances personnelles, pour créer une entreprise ou pour motifs familiaux. La durée est variable selon le type de disponibilité. Pendant cette période, le CNRS cesse de rémunérer l'agent qui ne bénéficie plus de ses droits à avancement et à la retraite.

Dans ce cadre, la personne reste affectée à l'unité du CNRS pendant six mois. Après ce délai, elle est affectée à l'unité pour les personnels hors structure CNRS « EXT_*codeDR*00 ».

A la fin la mise en disponibilité, la personne réintègre son unité, si le détachement est inférieur à six mois. Dans le cas contraire, elle sera affectée à une nouvelle unité.

- ***Fin de contrat à durée déterminée***

Pour les contrats à durée déterminée, une date de sortie est enregistrée lors de la saisie de la mesure de recrutement. A la date déterminée, l'affectation prend fin au niveau de Labintel, ce qui déclenche la suppression du compte sous-jacent dans les différents annuaires.

- ***Changement d'affectation***

Lorsqu'un agent CNRS effectue une mobilité interne au CNRS, à la date de changement d'affectation, son ancienne affectation prend fin. Sa nouvelle affectation est effective dans le système d'information uniquement lorsque sa nouvelle délégation de gestion prend son dossier. Si l'agent ne change pas de délégation, alors le changement est immédiat. Dans le cas contraire, il peut y avoir un délai avant que son dossier ne soit repris dans SIRHUS et donc soit présent dans Labintel. Dans le cas d'un contrat à durée déterminée, il s'agit simplement d'un nouveau contrat.

- ***Suppression du compte utilisateur***

Lorsqu'une affectation prend fin, l'information suit le même flux que pour la création d'un compte utilisateur.

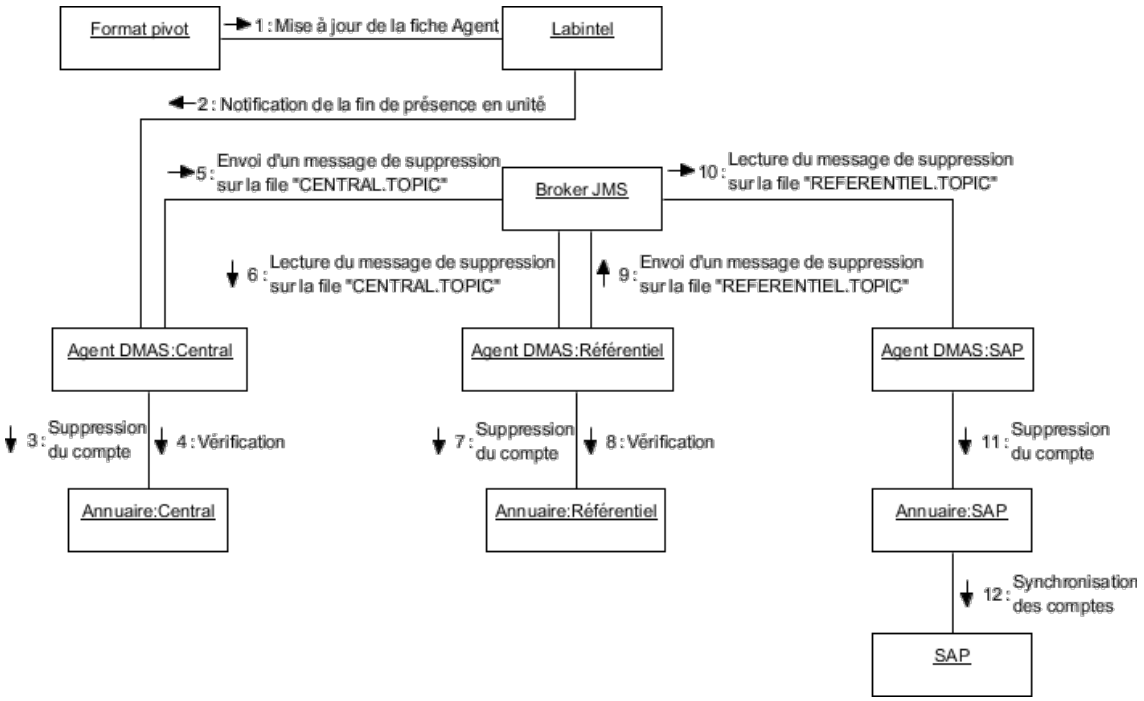


Figure 57 - Diagramme de collaboration de suppression de compte dans les annuaires

IV.3.3.2 Sortie d'un collaborateur non CNRS

Le séjour saisi dans Labintel comportant la date de fin, à cette date, l'affectation prend fin au niveau de Labintel, ce qui déclenche la notification à l'agent DMAS « Central » et engendre la suppression du compte sous-jacent dans les différents annuaires.

IV.3.3.3 Personne extérieure

Les comptes créés manuellement dans l'annuaire « Référentiel » dans la branche « Foreigner » n'ont actuellement de période de validité. De ce fait, la désactivation de ce type de compte est manuelle et dépend de la personne qui est à l'origine de la création. Actuellement, il n'existe aucun moyen pour vérifier quels sont les comptes légitimes et ceux qui devraient être désactivés.

IV.3.4 Prolongation d'un contrat (renouvellement)

IV.3.4.1 Non permanent CNRS

- ***Avenant au contrat***

Dans le cas où la mission de la personne est inchangée, le directeur de l'unité peut faire la demande d'un avenant au contrat afin de le prolonger. Après validation, le service des ressources humaines le saisit dans SIRHUS. Cet avenant ne peut être enregistré que lorsque le contrat actuel est terminé. De ce fait, entre le contrat actuel et sa prolongation, il existe une période de latence où il est considéré comme clos. A la date de fin du contrat initial, le processus de fin de contrat est déclenché, ce qui engendre la suppression des comptes dans les différents annuaires. Puis lorsque l'avenant est enregistré, la fiche est à nouveau exposée au demi-flux d'extraction SIRHUS « Format Pivot Personnel » pour pouvoir être consommée par les autres applications du système d'information. Cette étape peut être soumise à la signature d'un procès verbal d'installation qui peut être obligatoire dans certaines délégations régionales.

La période de renouvellement du contrat perturbe le fonctionnement des unités, car la personne peut être présente, mais n'a plus accès au système d'information du CNRS. De ce fait, les processus métier doivent évoluer pour permettre la continuité de service. Pour cela, il serait possible de se baser sur notion de « décision administrative » qui permet de savoir si le contrat est en cours d'instruction ou signé

- ***Nouveau contrat***

Dans le cas où la personne change de mission, le contrat à durée déterminée initial prend fin et un nouveau contrat est établi avec le CNRS, ce qui déclenche le processus de recrutement décrit précédemment.

IV.3.4.2 Non permanent non CNRS

Pour les personnes en contrat à durée déterminée mais issues d'autres organismes, les affectations sont liées à la notion de séjour. En cas de renouvellement du contrat, le gestionnaire de l'unité doit alors saisir dans Labintel un nouveau séjour dans la fiche de l'agent non-CNRS. Au niveau de Labintel, cela permet de conserver la même valeur de « NUM_PER ». La personne peut donc continuer à utiliser le même compte. Cependant, les gestionnaires confondent souvent les notions d'affectation et de séjour et créent une nouvelle fiche agent lors du renouvellement du contrat. Cela implique une nouvelle valeur de « NUM_PER » et la création d'un nouveau compte. La mauvaise compréhension de l'outil entraîne un problème de qualité des données.

IV.3.5 Nomination d'un directeur d'unité

Initialement, un mandat de directeur d'unité fait l'objet d'une proposition. Celle-ci est saisie dans Labintel plusieurs mois à l'avance par l'institut dont dépend l'unité. A ce moment, une fiche agent doit être créée pour préparer l'affectation. Au moment du début du mandat, la plupart du temps le 1er janvier, la proposition est validée, rendant la nomination effective. La fiche agent est alors mise à jour. Par conséquent, les annuaires « Central » et « Référentiel » sont mis à jour. Les attributs « CnrsRole » et « RefRole » sont positionnés respectivement à « DU – *code unité* » et « du=*code unité* ». Cette information est ensuite répercutée dans l'annuaire « SAP » dans l'attribut « cnrsrole ». De plus, le poste dans la fiche agent SIRHUS est automatiquement mise à jour. Parallèlement, la description de l'unité est mise à jour dans le référentiel des structures de Labintel.

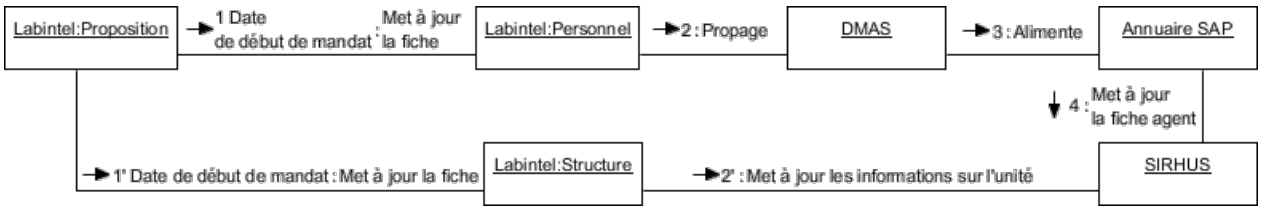


Figure 58 - Diagramme de collaboration dans la nomination d'un directeur d'unité

Lors de la nomination d'un directeur, une fiche agent a donc été préalablement créée dans Labintel. Elle peut n'être activée qu'au moment de la prise de fonction de la personne en tant que directeur de l'unité.

IV.4 Conclusion

La phase de cartographie a permis de mettre en évidence que la gestion du cycle de vie des identités n'est pas exhaustivement pris en compte par les outils existants.

En effet, il n'est actuellement pas possible de positionner une identité, au travers du compte utilisateur la représentant, à l'état « suspendue », car la fin d'un contrat dans Labintel implique la suppression automatique du compte dans les annuaires. Parallèlement, des comptes sont créés automatiquement alors que leur existence n'est pas légitime. Les règles de gestion implémentées dans les agents DMAS doivent donc évoluer.

De plus, seul l'outil IHM offre une interface graphique pour agir dans sur les identités. Cependant, son périmètre d'action est limité à l'attribution ou à la révocation de certains attributs utilisés lors de l'identification d'un compte. De même, Sésame, le seul outil offert aux utilisateurs du système d'information, permet uniquement de modifier le mot de passe de son compte utilisateur. Des initiatives individuelles au sein des délégation régionales ont permis de mettre en place des formulaires de demandes de création de compte ou de demande d'accès à certaines applications du système d'information mis en place par la DSI du CNRS ou par la délégation régionale de tutelle.

Les outils actuellement mis en œuvre ne permettent pas d'intervenir dans le cycle de vie des identités. Tous les processus étant automatisés, les comptes utilisateurs sont étroitement liés aux affectations décrites dans Labintel. De ce fait, le cycle de vie des comptes et des accès dépend des mesures administratives. Finalement, le concept d'identité n'existe pas dans le système d'information du CNRS puisqu'à partir d'un compte il est difficile d'identifier la personne à qui il appartient et quel est son rôle au sein de l'établissement.

Afin que les comptes puissent avoir un cycle de vie indépendant des situations administratives, il sera nécessaire de définir une gouvernance des identités et des accès propre. Les référentiels et outils cités dans la cartographie de l'existant pourront être un support à la réalisation de cette gouvernance.
Ainsi, par exemple, un compte pourra être mis à disposition de l'utilisateur dès sa prise de fonction et un compte ne sera pas nécessairement supprimé dès la fin d'un contrat.

V Réalisation

V.1 Itération 0 – Définition du « Product backlog »

V.1.1 Sprint backlog

La présente étude a pour but de démontrer la faisabilité de mise en œuvre d'une application ou d'un ensemble cohérent d'outils de gestion des identités et des accès reposant sur une offre FLOSS.

L'objectif de cette première itération est de définir le périmètre des fonctionnalités de l'application. Les lacunes identifiées lors de l'étape précédente de cartographie seront une base de travail pour le recueil des besoins en gestion des identités et des accès. Ainsi répertoriés, ils seront ensuite étudiés afin de sélectionner ceux qui correspondent aux objectifs de la présente étude. Enfin la priorisation des tâches permettra de définir les itérations nécessaires au développement de l'application de démonstration.

V.1.2 Recueil des besoins

Le projet de gestion des identités et des accès IAM doit respecter les objectifs fixés par le schéma directeur de la DSI tout en accompagnant sa mise en œuvre.

A la suite de l'étape de cartographie des outils, flux et cycles de vie des identités, il apparaît que plusieurs aspects de la gestion des identités et des accès ne sont pris en charge par les outils actuellement déployés. Cet état de fait pose plusieurs problèmes qui sont remontés pendant la phase d'entretien avec les différentes équipes. Pour débuter, cette itération porte sur un nombre limité de projets ainsi que sur des échanges avec les équipes responsable de la sécurité des systèmes d'information du CNRS, de l'urbanisation du système d'information déployé par la DSI du CNRS et des responsables régionaux des systèmes d'information du CNRS.

V.1.2.1 Sécurité des Systèmes d'Information du CNRS

La PSSI rédigée par le RSSI du CNRS précise au chapitre 3.4 « Contrôle d'accès » :

- « L'accès au système d'information exige une identification et une authentification préalable. L'utilisation de comptes partagés ou anonymes doit être évitée. Des mécanismes permettant de limiter les services, les données, les privilèges auxquels à accès l'utilisateur en fonction de son rôle dans l'organisation doivent être mis en œuvre dans la mesure du possible. »
- « Les accès doivent être journalisés. »

- « L'attribution et la modification des accès et privilèges d'un service doivent être validées par le propriétaire du service. Pour les services sensibles, un inventaire régulièrement mis à jour en sera dressé. Il importe de bien différencier les différents rôles et de n'attribuer que les privilèges nécessaires. »

Le RSSI souhaite le déploiement d'un ou plusieurs outils qui seraient un support à ces directives en prenant en compte les cas d'utilisation suivants.

Les outils actuellement déployés au sein du CNRS ne permettent pas de garantir l'exhaustivité des droits d'accès attribués. Le RSSI du CNRS souhaite donc disposer de moyens pour réaliser un audit sur les comptes et droits d'accès dans les applications mises en œuvre au sein du CNRS.

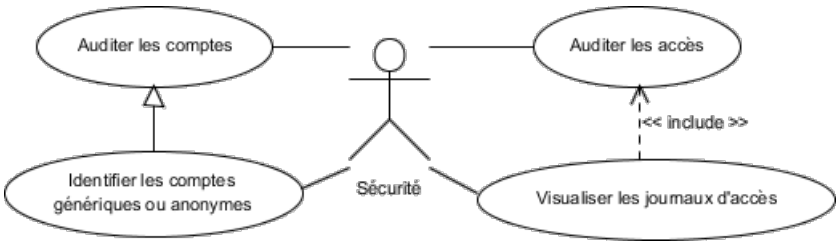


Figure 59 - Cas d'utilisation relatifs aux besoins en audit

Actuellement, les droits d'accès sont attribués au niveau de chaque application. Pour faciliter l'audit et la gestion des accès, le RSSI souhaite une gestion centralisée des profils. Ces derniers seraient alors déclinés en rôles applicatifs au sein des applications.

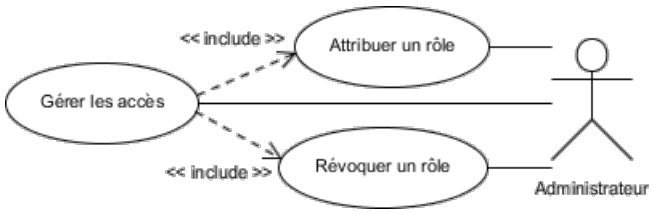


Figure 60 - Cas d'utilisation relatifs aux besoins de gestion des accès

V.1.2.2 Exploitation des systèmes d'information de la DSI du CNRS

Actuellement, pour des raisons de réactivité, l'équipe responsable de l'exploitation des applications déployées par la DSI du CNRS est amenée à modifier directement les valeurs des attributs des entrées dans les annuaires. De ce fait, des erreurs de saisies, telles que des caractères spéciaux dans les valeurs d'« uid », ont entraîné des comportements inhabituels de ces annuaires qui n'ont pu être corrigées qu'en modifiant directement les valeurs dans les systèmes de stockage sous-jacents. Cette situation est due au fait qu'il n'existe aucun outil répondant au besoin de saisie. Par ailleurs, il n'existe actuellement aucun moyen de retracer la demande ni l'opération de

modification. Par conséquent, il est nécessaire de disposer d'un outil permettant de modifier des informations dans les différents annuaires, d'en contrôler la validité et d'en conserver une trace. Il serait également avantageux de disposer d'un moyen d'annuler ces modifications.

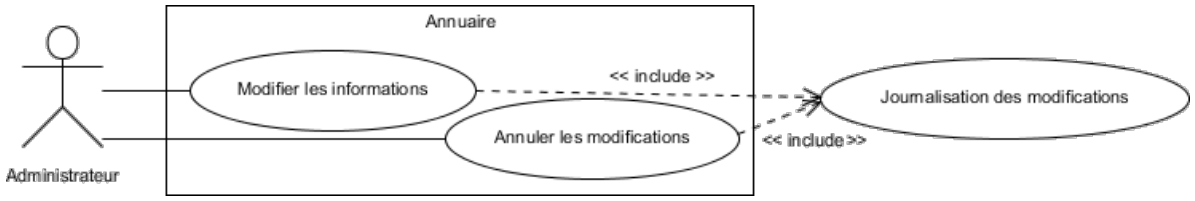


Figure 61 - Cas d'utilisation relatifs aux besoins de modifications

V.1.2.3 Cycle de vie des comptes utilisateurs

Comme l'a révélé l'audit réalisé lors de la cartographie des processus liés à la gestion des identités, il existe un délai non négligeable entre le moment où une personne commence à travailler dans une unité et le moment où un compte lui est attribué. Les flux liés aux personnes ne permettent actuellement pas d'extraire les informations nécessaires à la création des comptes. En effet, les informations nécessaires à la création des comptes ne sont disponibles dans le système d'information qu'au moment où la prise de fonction est effective du point de vue du service des ressources humaines. Les flux liés aux personnes ne permettent actuellement pas d'anticiper la création d'un compte pour que la personne puisse travailler dès son arrivée. Les responsables régionaux des systèmes d'information ont besoin de pouvoir créer un compte à partir d'une fiche agent existante dans SIRHUS mais dont le procès verbal d'installation n'est pas enregistré. Pour des raisons de traçabilité, il sera nécessaire que la personne qui prendra la responsabilité de valider ce type de compte soit identifiée et que l'opération soit journalisée.

De même, actuellement quand un contrat arrive à son terme, le compte est supprimé dans les différents annuaires. Pourtant, les responsables régionaux des systèmes d'information ont mis en évidence deux cas pouvant nécessiter que le compte soit encore opérationnel après cette date. Ainsi, dans le cas où le contrat est renouvelé, il est nécessaire que le compte soit maintenu pour éviter que les personnes perdent tous ses droits d'accès, ce qui arrive actuellement à cause de la suppression. Même si le contrat n'est pas renouvelé, il peut être nécessaire qu'une personne ait besoin que son compte reste actif. La situation se présente fréquemment pour les doctorants. En effet, bien que leur mission relative au sujet de thèse soit terminée, ils peuvent avoir besoin d'accéder à certaines applications pendant la phase suivante de rédaction. Actuellement, le compte étant simplement supprimé, ils doivent donc emprunter le compte d'une personne du laboratoire, ce qui entraîne une usurpation d'identité du point de vue sécurité des systèmes d'information du CNRS.

De plus, pour les séjours de très courte durée de collaborateurs, il est indispensable de pouvoir créer des comptes temporaires, donc à durée de vie courte et limitée. Actuellement, ce type de compte est

saisi manuellement dans les annuaires, mais il n'existe pas de moyen automatique de désactiver le compte à la fin de la mission. De ce fait, il existe de nombreux comptes qui ne devraient plus exister, ce qui représente une faille importante de sécurité.

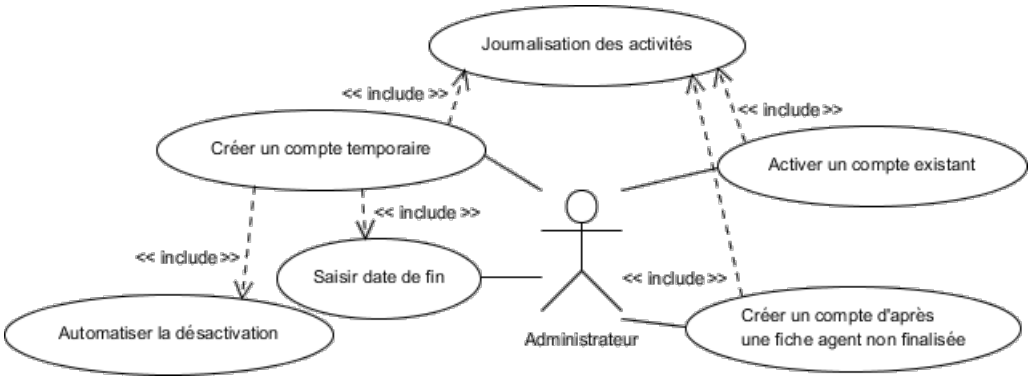


Figure 62 - Cas d'utilisation relatifs aux besoins de création et activation de comptes

V.1.2.4 CORE

Parmi les projets potentiels du périmètre de l'étude, CORE a été identifié comme projet prioritaire pour la DSI du CNRS. Etant ouvert à une large population, les besoins inhérents doivent être pris en compte au plus tôt dans le projet IAM. En effet, CORE permet au CNRS de mettre à disposition des espaces collaboratifs sous Microsoft SharePoint 2010 pour faciliter le partage d'informations et de documentation au sein des unités ainsi que la navigation vers les applications du système d'information du CNRS. Celui-ci propose également de fournir des espaces collaboratifs pour des réseaux professionnels et des projets regroupant divers acteurs de la recherche relevant ou non du CNRS. Cette offre de service permet à ces communautés de partager et modifier entre autres des fichiers, des documents électroniques, des agendas ainsi que des plans de gestion de projet. Elles ont également la possibilité d'utiliser des blogs, forums, wiki et des bibliothèques de différents types de médias. L'objectif pour le CNRS est d'éviter que ces organisations aient besoin d'utiliser les offres publiques de type Google Apps, Microsoft Office 365, dropbox ou encore iCloud. Potentiellement, tous les comptes connus dans la fédération Education-Recherche peuvent avoir besoin d'accéder à un espace collaboratif en fonction des sites mis en place. Les personnes extérieures à la fédération peuvent utiliser les Comptes Réseau Universels gérés par le GIP Renater. Des rôles peuvent être affectés aux comptes présentés par le fournisseur d'identité Janus. En effet, SharePoint bénéficie d'une liaison avec l'annuaire « Référentiel » pour obtenir des informations issues des attributs tels que « refrole » qui concerne les rôles. Le nombre de rôles est actuellement limité, car il n'existe pas de moyen pour les positionner aisément. La souplesse d'évolution de CORE est donc dépendante de la mise en place d'un outil permettant de gérer les rôles.

La connexion à l'annuaire « Référentiel » permet également d'effectuer des recherches de personnes dans l'outil pour les ajouter dans des groupes, des communautés ou des projets. SharePoint étant capable d'extraire des informations directement dans l'annuaire au travers de son connecteur, il existe donc actuellement un contournement permettant de synchroniser CORE avec les données de Labintel. Cependant, ce mode de fonctionnement implique que SharePoint réplique régulièrement ces données en interne. Il serait profitable de fournir un moyen de synchronisation.

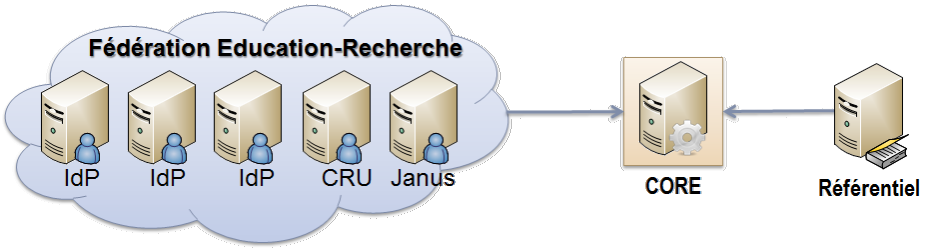


Figure 63 - Schéma des flux d'informations relatifs aux identités pour CORE

Le support de premier niveau est assuré par défaut par les propriétaires de site, ce qui inclut la gestion des accès. A cette fin, ils peuvent gérer les comptes autorisés, leurs niveaux d'autorisation et les délégations de droit éventuels. Techniquement, les droits d'accès sont référencés au sein de l'outil SharePoint.

Les responsables régionaux des systèmes d'informations ont la responsabilité du support de second niveau. Ils ont en charge la gestion des demandes de site, l'assistance de proximité aux utilisateurs et l'administration technique qui inclut notamment l'activation de fonctionnalités ainsi que le choix de la charte graphique. Les comptes autorisés à réaliser ces opérations sont identifiés par les rôles administrateur et valideur respectivement représentés dans l'attribut multivalué « refrole » par les valeurs « {core}admin=*DRxx* » et « {core}valid=*DRxx* » présentés par le fournisseur d'identité Janus.

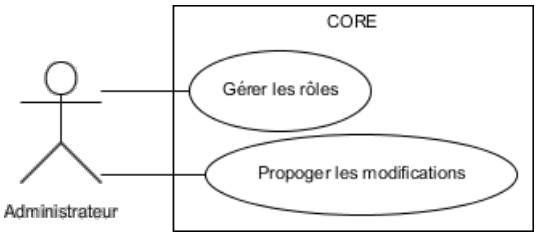


Figure 64 - Cas d'utilisation relatifs aux besoins de CORE

V.1.2.5 Simbad

Le portail Simbad permet aux agents CNRS d'accéder aux outils de réservation en ligne de leurs déplacements professionnels, ce qui inclue les transports et hébergement. Le système propose une authentification unique pour toutes les applications accessibles à partir du portail. Son

fonctionnement reposant essentiellement sur la notion de rôles des différents acteurs impliqués dans le processus de réservation des missions, il a été identifié comme faisant partie du périmètre de l'étude pour offrir un large panorama des besoins en matière de gestion des rôles applicatifs et des profils métiers.

En effet, outre les processus métiers « pré-réservation en ligne d'un transport ou d'un hébergement », « validation d'un transport ou d'un hébergement pré-réservé », le portail doit intégrer un gestionnaire de profil voyageur et permettre la gestion des rôles. Le profil voyageur intègre des informations propres aux déplacements professionnels, tels que le centre de coût pour la facturation, les préférences de transport et aucune information sur les habilitations. Ce type d'information n'a donc pas vocation à être traité par un outil de gestion des identités et des accès. Par contre, les rôles identifiés pour Simbad permettent de donner accès à des fonctionnalités de l'application. Ainsi, l'administrateur détient les droits complets sur Simbad, la gestion des profils et des habilitations, et la gestion du paramétrage. Le référent mission a le rôle d'administrateur régional pour la délégation dont il dépend. Le valideur valide les voyages pré-réservés. Un chargé de voyages pré-réserve des voyages pour des agents de n'importe quelle unité ou pour des invités. Il est généralement un gestionnaire d'unité, mais il peut aussi être un personnel d'unité qui invite des personnes extérieures. Le gestionnaire de profil peut attribuer au sein de son unité les rôles « chargé de voyages » et « valideur » et modifier ses attributions. Par défaut, chaque directeur d'unité est gestionnaire de profils de son unité. Il peut déléguer ce rôle à une ou plusieurs personnes de son unité. Cette liste met en évidence des besoins relatifs à la gestion des rôles. Les cas d'utilisation retenus dans le cadre de la gestion des identités et des accès sont illustrés dans le diagramme suivant.

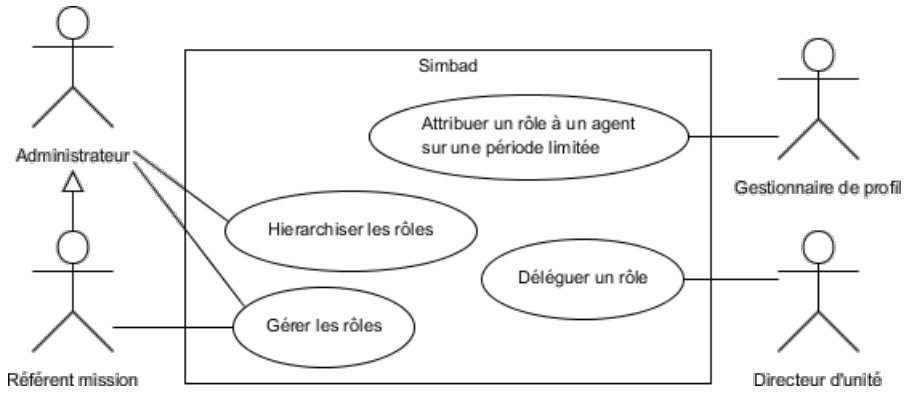


Figure 65 - Cas d'utilisation relatifs aux besoins en gestion des rôles

V.1.2.6 Gestion de l'identifiant

Historiquement, l'adresse de courrier électronique renseignée dans les attributs du compte fut définie comme l'identifiant de référence. Comme évoqué précédemment, cela implique que la

valeur de cet attribut ne peut être attribuée à plusieurs comptes et qu'il ne doit pas changer tout au long de la vie du compte. Cependant, il est fréquent que l'adresse électronique saisie dans Labintel soit utilisée par plusieurs comptes. Notamment, dans le cas d'un secrétariat de laboratoire composé de plusieurs personnes peut utiliser une adresse de courrier électronique commune à des fins de communication vers les personnels de l'unité. Des campagnes d'information régulières permettent de faire modifier ces valeurs afin que Labintel soit mis à jour. De plus, il est courant que suite à un changement de situation familiale, des personnes changent de nom. Dans ce cas, cette information peut être répercutée au niveau de l'adresse de courrier électronique pour prendre en compte le nouveau nom de famille. De même, lors du renouvellement de mandat d'une unité, cette dernière peut changer de nom, ce qui peut avoir pour conséquence un changement du nom de domaine des ressources exposées sur Internet, ce qui inclut le nom de domaine des adresses électroniques. Finalement, l'identifiant de référence choisi n'est ni pérenne dans le temps ni obligatoirement unique.

Par ailleurs, les applications déployées par la DSI du CNRS reposent également sur cet identifiant de référence. Ainsi, lors de la création d'un compte dans une de ces applications, la valeur de l'identifiant technique est initialisée avec la valeur de l'adresse de courrier électronique. Cette situation semble d'autant plus justifiée pour les applications utilisant Janus, car l'identifiant renvoyé par ce dernier est l'adresse électronique. Cependant, bien, qu'il existe un flux d'initialisation d'un compte qui va chercher des informations dans les annuaires lors de la création, il n'existe pas obligatoirement de flux de suivi des mises à jour. Ainsi, ces applications n'ont pas connaissance des modifications d'adresse de courrier électronique. Cela implique qu'une personne venant de changer d'adresse peut correctement s'authentifier auprès de Janus, car l'outil DMAS a correctement mis à jour l'annuaire « Référentiel », mais qu'elle ne soit pas reconnu au niveau de l'application. De ce fait, un changement d'adresse de courrier électronique implique actuellement une perte de tous les droits d'accès et habilitations dans les applications qui ne sont pas abonnées au flux de message du broker JMS de l'outil DMAS, ce qui représente plus de 90% du parc applicatif de la DSI du CNRS.

Ce disfonctionnement remonté régulièrement par les responsables régionaux des systèmes d'information et par l'assistance utilisateur fait apparaître un besoin de propagation des modifications des attributs vers toutes les bases de comptes des applications qui reposent sur des informations issues de Labintel.

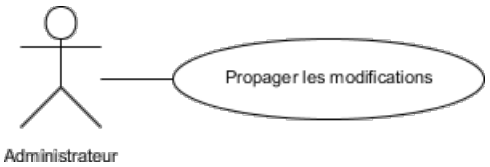


Figure 66 - Cas d'utilisation de propagation d'information

V.1.2.7 Cartographie fonctionnelle

La phase de recueil des besoins a permis de mettre en évidence des besoins récurrents qui ne peuvent pas être pris en charge facilement par les outils existants. L'ensemble des projets du système d'information du CNRS n'ayant pas été étudié, la liste des besoins n'est pas exhaustive. Cependant, cela a permis d'entrevoir les priorités et ainsi d'établir le périmètre de la présente étude de faisabilité.

Les cas d'utilisation sont répertoriés par catégorie d'utilisateur d'un système d'information de gestion des identités et des accès, puis par type de finalité.

- ***Agent travaillant pour une unité du CNRS***

  Gérer les rôles
    - Déléguer un rôle

- ***Administrateur***

1. Gérer les accès
    - Attribuer un rôle
    - Révoquer un rôle
2. Gérer les comptes
    - Créer un compte d'après une fiche agent non finalisée
    - Créer un compte temporaire
        - Définir une date de fin
        - Automatiser la désactivation
    - Réactiver un compte existant
    - Modifier les informations
    - Propager les modifications
    - Annuler les modifications
3. Gérer les rôles
    - Définir une hiérarchie de rôles
    - Déléguer un rôle

- Attribuer un rôle à un agent sur une période limitée

- ***Auditeur***

1. Identifier les comptes génériques
2. Identifier les comptes anonymes
3. Visualiser les journaux d'accès
4. Visualiser les modifications d'information
5. Visualiser les activités

V.1.3 Product backlog

V.1.3.1 Périmètre du démonstrateur

La phase de recueil a permis d'identifier des besoins essentiels à une gouvernance des identités et des accès. Cependant, comme il ne s'agit que d'une étude de faisabilité et non pas de la réalisation complète d'un outil, le cahier des charges ne peux pas prendre pas en compte tous les besoins répertoriés. Ainsi, bien que la création anticipée d'un compte pour l'arrivée d'un agent soit un besoin critique et ancien, il ne sera pas traité dans le cadre de cette étude. La solution dépend de la mise en place de nouveaux flux d'extraction depuis SIRHUS.
De plus, le produit qui sera développé doit pouvoir reprendre les fonctionnalités des outils existants détaillées dans l'étape de cartographie de la gestion des identités et des accès qui sont indispensables au fonctionnement du système d'information du CNRS.

En outre, conformément aux préconisations Agiles décrites précédemment, chaque itération fera l'objet d'une rétrospective pour évoquer les éventuels problèmes rencontrés et les solutions mises en œuvre.

V.1.3.2 Itération 1 – Définition de l'architecture cible

1. Définition des critères d'évaluation
2. Etude des offres commerciales
3. Etude des offres FLOSS
4. Comparatif
5. Choix

V.1.3.3 Itération 2 – Construction du socle technique

1. Description de l'architecture de l'outil sélectionné
2. Installation de l'outil sélectionné

V.1.3.4 Itération 3 – Construction du référentiel des identités

1. Définition du modèle des identités
2. Initialisation des données par lecture de la base de données Labintel

V.1.3.5 Itération 4 – Gestion des rôles

1. Définition du rôle « directeur d'unité » et des rôles applicatifs CORE et Simbad
2. Processus d'attribution du rôle « directeur d'unité »
3. Processus d'attribution des rôles applicatifs

V.1.3.6 Itération 5 – Approvisionnement des ressources cibles

1. Définition du modèle d'approvisionnement
2. Alimentation des tables de compte d'une base de données Oracle
3. Alimentation d'un annuaire LDAP
4. Propagation de modifications effectuées dans Labintel

V.1.3.7 Itération 6 – Désactivation de comptes

1. Fin de présence en unité dans Labintel

V.1.3.8 Itération 7 – Délégation d'habilitation

1. Développement d'un processus de délégation de gestion d'un rôle

V.1.3.9 Itération 8 – Gestion des comptes temporaires

1. Gestion des contrats à durée déterminée issus de Labintel
2. Gestion des comptes hors Labintel

V.1.3.10 Planning prévisionnel

Chaque itération correspond à un travail compris entre cinq et quinze jours homme en fonction du travail de configuration et de développement à réaliser. Par conséquent, la charge totale est évaluée entre deux et quatre mois.

ID	Nom de tâche	Début	Terminer	Durée
1	Définition de l'architecture	03/09/2012	14/09/2012	2s
2	Construction du socle technique	17/09/2012	21/09/2012	1s
3	Construction du référentiel des identités	24/09/2012	05/10/2012	2s
4	Gestion des rôles	08/10/2012	12/10/2012	1s
5	Approvisionnement des ressources cibles	15/10/2012	26/10/2012	2s
6	Suppression de comptes	29/10/2012	09/11/2012	2s
7	Délégation d'habilitation	12/11/2012	23/11/2012	2s
8	Gestion des comptes temporaires	26/11/2012	07/12/2012	2s

Figure 67 - Diagramme de Gantt prévisionnel des itérations

V.2 Itération 1 – Définition de l'architecture

V.2.1 Sprint backlog

L'objectif de cette itération est de définir une architecture pour la solution de gestion des identités et des accès en étudiant les solutions commerciales et FLOSS du marché. La première étape consistera à déterminer les critères d'évaluation qui permettront ensuite de sélectionner un outil répondant au mieux au product backlog. Le développement d'une solution interne sera évoqué pour proposer une éventuelle évolution des outils actuellement déployés.

Afin de respecter la démarche Agile, l'objectif de l'itération doit être exprimé en terme de « User story » qui se présente sous la forme « En tant que …, je veux … », ce qui correspond pour le sprint présent à : « En tant qu'architecte technique, je veux définir le socle technique de la solution à développer ». Les versions étudiées sont celles disponibles au mois de septembre 2012.

V.2.2 Etude comparative de l'offre commerciale

V.2.2.1 Evaluation

La société américaine Gartner propose régulièrement une évaluation des offres commerciales dans différents domaines. La gestion des identités et des accès a fait l'objet d'une étude au mois de décembre 2011 [23]. Le quadrant suivant se concentre sur la facilité de déploiement, de maintenance et l'offre commerciale autour des produits.

[23] P. Carpenter, E. Perkins. *Magic Quadrant for User Administration/Provisionning*. Gartner Inc., 42 pages, 2011

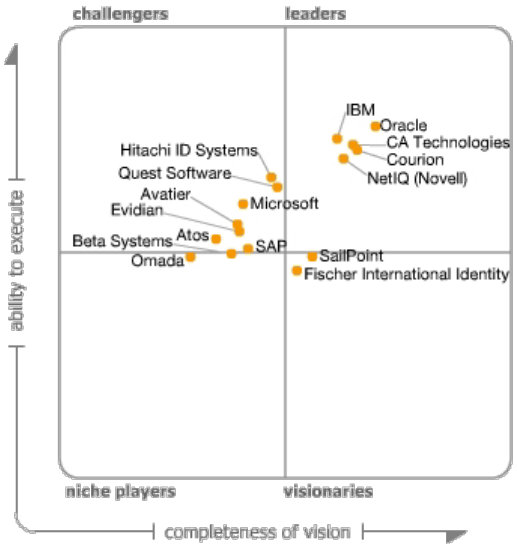


Figure 68 - Comparatif Gartner 2011 « Magic Quadrant for User Administration/Provisioning »
(source : www.gartner.com)

Le schéma directeur de la DSI recommande de capitaliser les investissements déjà réalisés sur les outils actuellement déployés. De ce fait, seules les solutions des éditeurs avec lesquels la DSI du CNRS a signé un contrat seront évoquées dans un premier temps. Ainsi, seules seront décrites les solutions Microsoft, Oracle et SAP. En outre, elles feront l'objet d'un descriptif rapide, car le sujet du présent document concerne uniquement les offres FLOSS. Les solutions commerciales sont évoquées à titre purement indicatif. De ce fait, les solutions telles que Evidian IAM Suite, CA Identity Manager, Tools4Ever User Management Resource Administrator, SailPoint IdentityIQ, Novell Identity Manager, NetIq Identity Manager ne seront examinées que si une solution FLOSS ou une solution d'un éditeur déjà présent à la DSI n'est pas jugée adéquate.

- ***Oracle IdM 11gR2***

La DSI du CNRS utilise la technologie d'annuaires LDAP Oracle Internet Directory qui sont un des composants de l'offre Oracle Identity Management. La DSI du CNRS pourrait donc profiter de l'expérience acquise dans l'administration et l'optimisation de ces outils. De plus, en 2009, l'institut national de physique nucléaire et de physique des particules a réalisé une étude comparative des outils de gestion des identités et des accès qui avait conclu que l'offre Oracle répondait le mieux à ses besoins. Le projet n'avait pas pu aboutir pour des raisons budgétaires et organisationnelles.

- ***Microsoft Forefront Identity Manager 2010***

La technologie FIM est déployée au sein de la DSI du CNRS au travers de la plateforme collaborative CORE. En effet, l'outil SharePoint intègre nativement plusieurs composants de FIM

pour la gestion des profils utilisateur et des groupes. L'offre Microsoft pourrait donc être plus largement déployée pour répondre aux besoins de synchronisation de CORE puis d'autres applications.

- ***SAP Identity Management***

Les applications SIRHUS et BFC reposant sur les outils SAP, le choix de SAP Identity Management correspondrait aux démarches évoquées dans le plan stratégique du CNRS et au schéma directeur de sa DSI. Cependant, SAP n'est utilisé que pour gérer le personnel CNRS, ce qui représente seulement 30% de la population des comptes gérés actuellement dans l'annuaire « Référentiel ». Donc, finalement, cet outil ne permettrait pas de gérer convenablement l'ensemble des identités référencées. De plus, le marché de tierce maintenance actuellement en vigueur sur les outils SAP ne permet pas de prendre en charge un projet de gestion des identités, quelle que soit sa taille.

V.2.2.2 Conclusion

Parallèlement à la construction d'un démonstrateur basé sur une FLOSS, la réalisation d'un démonstrateur avec la solution Oracle peut être envisagée, mais elle ne sera pas prise en compte dans le présent document.

V.2.3 Etude comparative de l'offre Open Source

V.2.3.1 Critères d'évaluation

La sélection de la solution FLOSS pour le projet IAM se fera à l'aide d'un graphique semblable à celui du Gartner où les critères d'évaluation technique seront opposés à l'évaluation du risque lié à l'Open Source. Les critères de maturité utilisés par Gartner sont difficilement transposables aux offres libres. Par contre, la taille et la vivacité de la communauté d'utilisateurs et de contributeurs sur un projet Open Source donnent une bonne indication quant à sa pérennité, chose que l'on peut plus difficilement mesurer avec une solution éditeur. Par ailleurs, la viabilité d'une solution est fortement liée à sa solidité technique, que ce soit pour un logiciel libre ou propriétaire. Or cette solidité ne peut être évaluée que lorsqu'on a accès aux sources. En effet, cela permet de suivre les évolutions et ainsi déterminer si la communauté reste active et vérifier si le socle technique est stable depuis suffisamment longtemps. Le contexte FLOSS sera donc estimé à partir de la taille de la communauté, le volume de la documentation, le nombre d'installations en production ainsi que la prévision d'une prochaine version. Pour ces critères environnementaux, le

site web www.ohloh.net permet de comparer des projets FLOSS selon le nombre de validation, le nombre de participants, le nombre de lignes de code ainsi que la durée d'existence.

Pour l'évaluation technique, j'ai conçu une méthode où les critères peuvent recevoir des notes allant de 0 à 5, la note de 0 indiquant que la fonctionnalité n'est pas du tout prise en compte et la note de 5 indiquant que la fonctionnalité est parfaitement prise en charge par la solution. La grille des critères techniques est construite à partir du cahier des charges de gouvernance des accès mis à disposition gratuitement par la société guidescomparatifs.com et des besoins techniques recueillis lors de la définition du product backlog.

Le site www.ohloh.net qui référence les projets FLOSS a permis de retenir les projets ForgeRock OpenIdm, OpenIam Identity Manager, Evolveum MidPoint, Apache Syncope, Kuali Identity Management. De plus, suite à une conférence lors du salon de l'Open Source 2012 à Paris, la rencontre avec Clément OUDOT de Linagora a ouvert l'étude à l'offre LinId. Par ailleurs, l'étude prend également en compte le projet Open Registry de Jasig qui a conçu le système d'authentification CAS utilisé dans Janus.

V.2.3.2 Evaluation

- ***ForgeRock OpenIdm***

La société ForgeRock fut fondée le 1er février 2010 par d'anciens employés de Sun suite à son rachat par Oracle. Elle a repris le développement de trois outils de Sun. OpenDJ est une solution d'annuaire LDAP créée à partir de Sun Directory Server. OpenAM est une solution d'authentification créée à partir de Sun Access Manager.

OpenIDM est la solution de gestion des identités créée à l'origine à partir de Sun Identity Manager. En 2011, l'outil a été complètement repensé et le code a été réinitialisé. La version 2.0 a été livrée fin 2011 et a été corrigée depuis, avec la livraison en mars 2012 de la version 2.0.3. Les connecteurs aux ressources font l'objet d'un projet à part entière OpenICF qui est également issu de la reprise d'un outil de Sun.

Les versions 2.0.*x* n'intègrent pas d'interface graphique. La partie réservée aux administrateurs est prévue pour la version 2.1 planifiée pour le second trimestre 2013, mais la partie réservée aux utilisateurs n'est toujours pas planifiée.

Tableau XIII - Synthèse de l'évaluation de ForgeRock OpenIdm sur la gestion des identités

	Référentiel intégré	Connecteurs	Transformation	Provisioning	Moyenne
Notes	2,0	5,4	2,9	5,5	**3,9**

Tableau XIV - Synthèse de l'évaluation de ForgeRock OpenIdm sur la gestion des accès

	Gestion des rôles	Gestion des habilitations	Gestion des mots de passe	Contrôle et traçabilité	Moyenne
Notes	3,0	1,7	9,6	6,9	**5,3**

Tableau XV - Synthèse de l'évaluation de ForgeRock OpenIdm sur l'environnement

	Développeurs	Lignes de code	Validations	Mois d'existence	Versions prévues	Installations
Valeurs	21	157 769	1 487	31	4	-

- ***OpenIAM Identity Manager***

La société OpenIAM fut fondée en 2008. Son offre repose sur deux produits, Access Manager pour l'authentification et Identity Manager pour la gestion des identités. Pour chacun, deux versions sont disponibles. La version communautaire gratuite dispose des fonctionnalités principales, alors que la version Entrerpise payante offre des fonctionnalités supplémentaires. La version communautaire 2.2 d'Identity Manager a été mise à disposition en juillet 2012 et la prochaine version 2.3 est prévue pour novembre 2012. La version payante suit un cycle différent, car elle intègre des livraisons de correctifs. La version 2.2.3 a été produite fin août 2012. L'étude ne prend en compte que la version communautaire.

La solution repose sur une architecture orientée services tant pour la propagation des informations que pour leur gestion au travers des différents modules fonctionnels.

Tableau XVI - Synthèse de l'évaluation d'OpenIAM Identity Manager sur la gestion des identités

	Référentiel intégré	Connecteurs	Transformation	Provisioning	Moyenne
Notes	8,0	6,6	7,1	8,1	**7,5**

Tableau XVII - Synthèse de l'évaluation d'OpenIAM Identity Manager sur la gestion des accès

	Gestion des rôles	Gestion des habilitations	Gestion des mots de passe	Contrôle et traçabilité	Moyenne
Notes	5,0	7,1	10,0	8,1	**7,6**

Tableau XVIII - Synthèse de l'évaluation d'OpenIAM Identity Manager sur l'environnement

	Développeurs	Lignes de code	Validations	Mois d'existence	Versions prévues	Installations
Valeurs	9	284 881	584	43	4	25

- ***Evolveum MidPoint***

Lors de la réinitialisation de l'outil OpenIdm de ForgeRock mi-juillet 2011, le code de la version 1.0 fut repris par la société Evolveum qui a continué depuis à le faire évoluer pour aboutir à une version stable 2.0 en juin 2012. Une mise à jour est planifiée pour novembre 2012. La jeunesse de l'organisation est donc compensée par les développements antérieurs du code.

L'architecture repose sur plusieurs technologies issues des développements réalisés par ForgeRock. Ainsi, la transmission d'informations, gérée par l'ordonnanceur libre Quartz, se fait au travers des connecteurs OpenICF.

Tableau XIX - Synthèse de l'évaluation d'Evolveum MidPoint sur la gestion des identités

	Référentiel intégré	Connecteurs	Transformation	Provisioning	Moyenne
Note	4.0	6,6	2,9	7,3	**5,2**

Tableau XX - Synthèse de l'évaluation d'Evolveum MidPoint sur la gestion des accès

	Gestion des rôles	Gestion des habilitations	Gestion des mots de passe	Contrôle et traçabilité	Moyenne
Notes	5,2	2,9	8,9	7,3	**6,1**

Tableau XXI - Synthèse de l'évaluation d'Evolveum MidPoint sur l'environnement

	Développeurs	Lignes de code	Validations	Mois d'existence	Versions prévues	Installations
Valeurs	11	333 189	4 253	31	3	-

- ***Apache Syncope***

La fondation Apache, à l'origine de nombreux outils devenus des standards tels que Apache HTTP Server et le containeur de servlet Tomcat, a initié en 2011 le projet Syncope en mode incubateur. Les versions 1.0.*x*, dont la dernière version 1.0.3 date d'octobre 2012, sont toujours en mode incubateur. La version 1.1 planifiée pour la fin 2012 doit permettre de faire rentrer le projet dans un mode de fonctionnement plus stable.

L'architecture repose naturellement sur des outils standards du monde du libre, dont plusieurs gérés par la fondation. La lecture et l'écriture d'informations dans les systèmes source et respectivement cibles se font avec les connecteurs du projet Apache ConnId.

Tableau XXII - Synthèse de l'évaluation d'Apache Syncope sur la gestion des identités

	Référentiel intégré	Connecteurs	Transformation	Provisioning	Moyenne
Note	3,0	5,4	1,8	6,1	4,1

Tableau XXIII - Synthèse de l'évaluation d'Apache Syncope sur la gestion des accès

	Gestion des rôles	Gestion des habilitations	Gestion des mots de passe	Contrôle et traçabilité	Moyenne
Notes	4,7	4,6	8,9	8,8	**6,7**

Tableau XXIV - Synthèse de l'évaluation d'Apache Syncope sur l'environnement

	Développeurs	Lignes de code	Validations	Mois d'existence	Versions prévues	Installations
Valeurs	15	204 087	1898	18	9	-

La version 1.1 devra prendre en compte des nouveautés fonctionnelles susceptibles de modifier significativement les notes attribuées grâce à l'intégration, par exemple, de la gestion des flux d'escalade.

- ***Kuali Identity Management***

Kuali est une communauté d'universités américaines fondée en 2004 pour répondre au besoin de développer une solution de gestion financière pour ses établissements. Depuis 2006, l'offre s'est étendue aux outils de pilotage de la recherche et de gestion des ressources humaines. Les différents logiciels reposent sur une architecture commune appelée « Kuali Rice ». Celle-ci intègre différents modules dont Kuali Service Bus (KSB), qui est un service de bus de messages, et Kuali Identity

Management (KIM), qui est un service de gestion des identités et des accès. La synchronisation et l'approvisionnement sont assurés par des APIs («Application Programming Interface » en anglais, « interface de programmation » en français) que les applications sources et cibles exploitent pour respectivement envoyer et recevoir les informations. Les messages sont transmis par KSB. Tous les processus métier sont gérés par l'outil Kuali Enterprise Workflow (KEW).

Les versions 2.*x* de la plate-forme Kuali Rice sont orientées vers le développement rapide d'application permettant de bénéficier des avantages de l'intégration des différents composants. La version 2.1 a été mise à disposition en mai 2012 avec quelques correctifs depuis, et la version 2.2 est planifiée pour la fin de l'année 2012.

Le projet CIPHER (Community Identity Framework for Education and Research) de gestion des identités pour la communauté éducation-recherche a identifié les outils Kuali Identity Management et Kuali Rules Management System comme socles d'une solution complète de gestion des identités dont les outils Shibboleth et CAS permettent de gérer l'authentification.

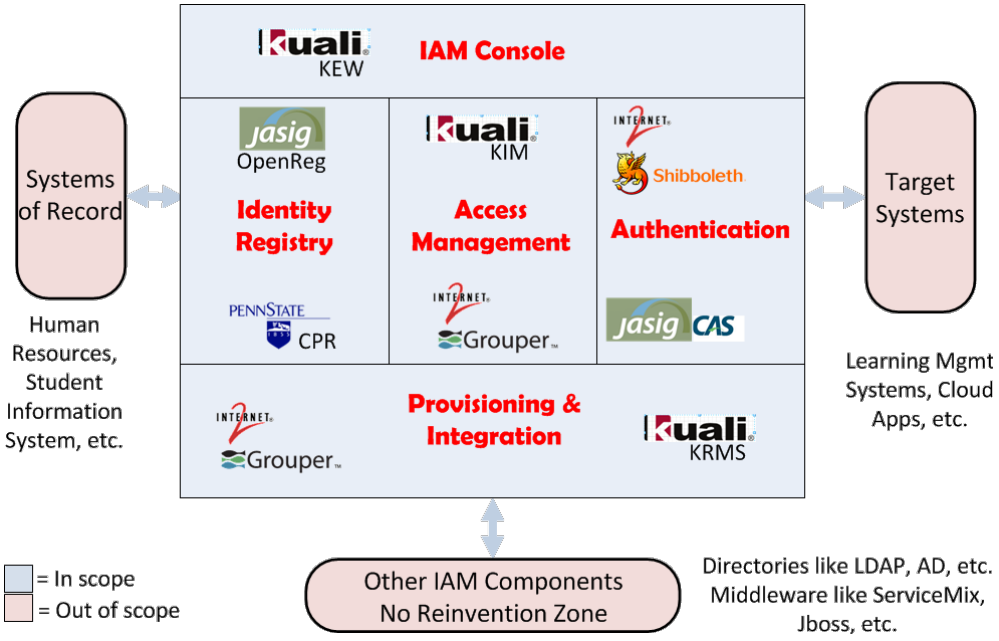


Figure 69 - Architecture de la solution proposée par le projet CIPHER

(Source : http://ciferproject.org)

Dans l'architecture du projet CIPHER présentée dans ce schéma, les aspects liés à l'authentification sont assurés par des produits n'appartenant pas à l'offre de Kuali, ce qui tend à montrer que Kuali répond pleinement aux besoins liés à la gestion des accès. En effet, KIM n'est pas capable d'administrer les différents aspects liés à la gestion des mots de passe.

Tableau XXV - Synthèse de l'évaluation de Kuali Identity Management sur la gestion des identités

	Référentiel intégré	Connecteurs	Transformation	Provisioning	Moyenne
Note	7,0	7,7	2,9	8,1	**6,4**

Tableau XXVI - Synthèse de l'évaluation de Kuali Identity Management sur la gestion des accès

	Gestion des rôles	Gestion des habilitations	Gestion des mots de passe	Contrôle et traçabilité	Moyenne
Notes	5,3	5,9	1,9	7,3	**5,1**

Tableau XXVII - Synthèse de l'évaluation de Kuali Identity Management sur l'environnement

	Développeurs	Lignes de code	Validations	Mois d'existence	Versions prévues	Installations
Valeurs	42	877 299	4 523	49	2	31

- ***Jasig OpenRegistry***

La communauté Jasig qui est à l'origine de l'outil CAS employé par la DSI du CNRS pour l'authentification dans Janus a repris début 2009 le projet OpenRegistry qui fut initié par l'université de Reuters en 2008. Depuis, il est en mode « incubation ». La version 0.9 a été mise en ligne en juin 2012 alors qu'elle était planifiée pour juillet 2011 et qu'une version 1.0 était prévue pour fin 2011.

Par ailleurs, OpenRegistry n'étant pas pris en compte par le site web www.ohloh.net, le code source a été soumis à la plate-forme d'intégration continue de la DSI du CNRS. Le métrique de volume de code source développé montre que le projet n'est pas au niveau des projets étudiés dans les paragraphes précédents.

Ces différents indicateurs montrent qu'en 2012 OpenRegistry ne peut pas être considéré comme un candidat solide à la mise en œuvre d'un outil de gestion des identités et des accès.

- ***LinId***

La société de service Linagora fut créée en 2000 et inventa le concept de Société de Services en Logiciels Libres (SS2L) qui est maintenant une marque déposée. Depuis 2009, Linagora a pour objectif de devenir un éditeur Open Source. Dans cette optique elle développe des produits Open Source, dont la solution de gestion et de fédération d'identité LinId. Cette offre repose sur quatre

outils « LINID Directory Manager », « LINID Directory Server » qui est un clone d'OpenLDAP, « LINID Provisioning Manager » et « LINID Access & Federation Manager » qui est l'équivalent des outils Shibboleth déployés dans le cadre de Janus. Les deux premières applications sont plus orientées vers l'administration d'annuaire que vers une véritable solution de gestion des identités. En effet, il n'existe pas de possibilité de conserver une trace de tous les changements, pour pouvoir annuler une action par exemple. De ce fait, l'ensemble d'outils de l'offre LinId n'a pas été retenu dans le périmètre de l'étude comparative.

V.2.3.3 Conclusion

Les réponses aux grilles d'évaluation ont permis d'évaluer les solutions FLOSS en fonction de leur adéquation aux besoins de la DSI du CNRS. L'étude de l'environnement lié aux outils a permis d'établir un profil sur les investissements à venir et réalisés par les organisations. La représentation graphique de ces résultats est volontairement proche de celle du Gartner afin de pouvoir comparer les offres libres et payantes.

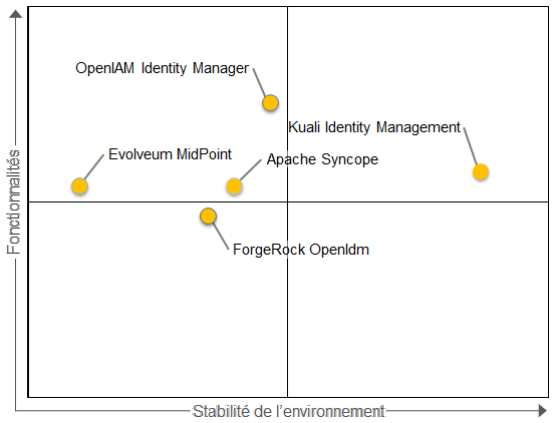


Figure 70 - Comparatif des offres libres de gestion des identités

Le graphique montre que l'offre d'OpenIAM répond le mieux aux besoins fonctionnels, mais que celle de Kuali présente moins de risques liés à l'environnement Open Source et qu'elle est tout de même en mesure de répondre à une majorité de besoins.

Par ailleurs Kuali est l'organisation qui dispose de la plus grande expérience pour l'environnement spécifique de la recherche scientifique. De plus, l'architecture Rice démontre une stabilité du produit depuis plusieurs années. Bien que, comme évoqué dans les paragraphes précédents, il manque des fonctionnalités autour de l'authentification, elles peuvent être remplacées par des outils complémentaires. Notamment, pour la gestion des mots de passe il est possible de continuer à utiliser l'outil Sésame qui est développé et utilisé par la DSI du CNRS.

La conclusion de cette étude comparative est que Kuali semble présenter moins de risques qu'OpenIAM. Bien que toutes les fonctionnalités ne soient pas couvertes, des solutions sont

envisageables pour les prendre en charge. Le développement consistera donc à installer, configurer et développer un démonstrateur sur la base des outils proposés par Kuali.

V.2.4 Développement interne

Les modèles de données développés pour chacune des architectures présentées précédemment reposent sur des systèmes de gestion de bases de données relationnelles (SGBDR) et montrent de grandes divergences. Il ne semble donc pas exister de modèle optimal. Un développement interne peut donc être étudié sur un modèle de type NoSQL. En effet, l'objectif d'un outil d'IAM étant d'établir un lien entre une identité, des rôles et des groupes, les graphes peuvent être une solution simple et efficace. Cependant, la taille des développements des offres libres montrent un important investissement. Aussi, la volonté de réaliser un développement interne doit prendre en compte la dimension coût de développement. Une autre possibilité de développement peut être la reprise du code d'un outil existant pour l'adapter aux besoins spécifiques de la DSI du CNRS.

V.2.5 Conclusion

L'étude comparative des offres FLOSS a abouti au choix de l'outil Kuali Identity Management. Parallèlement, une étude des offres commerciales peut être menée ce qui peut permettre d'affiner les besoins pour des itérations ultérieures en fonction des fonctionnalités proposées.

V.3 Itération 2 – Construction du socle technique

V.3.1 Sprint backlog

L'objectif de l'itération est de procéder à l'installation du produit Kuali Identity Management. Pour cela, la première phase consiste à appréhender l'architecture du produit afin de comprendre comment interagissent les différents composants et quelles sont les possibilités de déploiement pour répondre aux besoins d'une mise en production avec la population connue des différents annuaires LDAP et Active Directory.

La « User story » du présent sprint peut être exprimée par la phrase suivante : « En tant qu'architecte technique, je veux installer le socle technique Kuali Identity Management 2.1.1 ».

V.3.2 Environnement d'installation

Afin de tester l'installation des différents outils, la solution la plus souple consiste à utiliser des machines virtuelles qui peuvent être démarrées, arrêtées, détruites et recréées à volonté sans intervention d'un administrateur système.

Les serveurs appartenant à la DSI sont habituellement déployés avec le système d'exploitation RedHat. Cependant, dans le but d'être indépendant du volume de licences consommées dans le cadre du contrat, j'ai souhaité utilisé un système d'exploitation qui ne nécessite pas de licence commerciale. Par ailleurs, pour des besoins ultérieurs, il faudra tester la capacité de l'outil à s'interfacer avec le fournisseur d'identité Janus. Pour éviter de modifier les architectures actuellement en place, il est préférable de simuler Janus. Pour cela, il faudra réaliser l'installation d'un fournisseur d'identité et d'un fournisseur de service Shibboleth dans une machine virtuelle. J'ai donc utilisé un des systèmes d'exploitation compatibles avec Shibboleth et ne nécessitant aucun achat de licence, OpenSuse. Ayant subi quelques problèmes de ce dernier lors de l'installation dans une machine virtuelle, j'ai souhaité capitaliser les solutions en utilisant également OpenSuse pour l'installation des machines virtuelles de test des offres open source.

V.3.3 Architecture

L'outil KIM fournit des services de gestion des identités et des accès aux applications clientes proposées par Kuali. Il permet ainsi nativement de gérer les comptes dans ces outils ainsi que leurs habilitations avec une interface centralisée.

KIM est un des modules de l'infrastructure Kuali Rice sur laquelle reposent toutes les applications Kuali. De ce fait, utiliser KIM implique d'installer et d'utiliser l'ensemble des modules Rice.

Les informations échangées entre les applications Kuali, plus précisément entre les différents composants sont transmises par travers d'un bus de service, « Kuali Service Bus » (KSB). Par ailleurs, KIM est construit comme les autres applications proposées par Kuali. L'application de gestion des identités bénéficie donc des moteurs de l'offre Kuali Rice, qui inclue Kuali Enterprise Workflow (KEW). Nativement, ce dernier intègre les processus liés aux mouvements de personnes au sein d'une université. Tous les concepts manipulés au sein de l'offre Kuali, dont les modules de gestion des ressources humaines, des contrats ou de comptabilité, sont développés sur la plate-forme de standardisation « Kuali Nervous System » (KNS). Ainsi, les processus définis dans KEW reposent sur les modèles de KNS. En s'appuyant sur ces standards, il existe plusieurs moyens d'intégrer des applications extérieures à l'écosystème Kuali. Il est notamment possible d'utiliser des APIs pour que des applications développées en Java puissent interagir avec les différents modules de l'offre Kuali Rice. Il est ainsi possible d'adapter une application non compatible avec KIM en application conforme aux standards. Une solution moins intrusive consiste à faire appel à des web services respectant le standard SOAP (« Simple Object Access Protocol »). Par ailleurs, depuis la version 2 de cette dernière, il est possible d'utiliser la plate-forme de développement rapide d'application Web Kuali Rapid Application Development (KRAD) qui repose sur les standards KNS. De ce fait, une telle application est capable de dialoguer avec l'infrastructure de Kuali Rice sans développement spécifique.

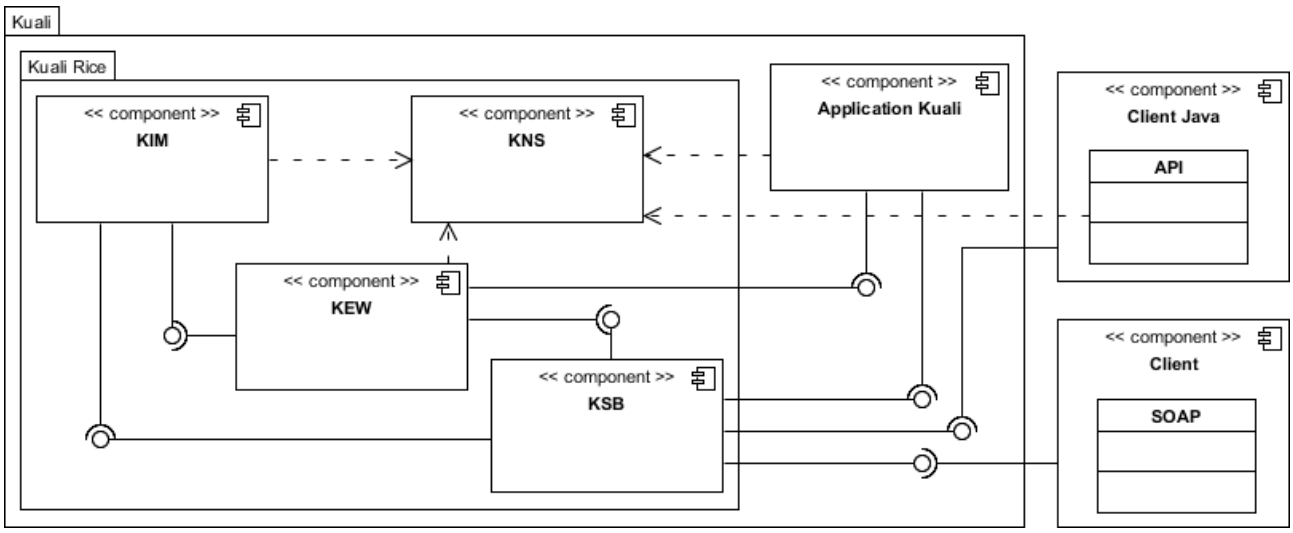


Figure 71 - Diagramme de composants de Kuali Rice

L'ensemble des modules Rice partage une base de données unique pour stocker leurs données. Les SGBDR supportés sont Oracle et MySQL. Pour limiter la consommation mémoire de la machine virtuelle qui héberge l'infrastructure Rice, j'ai fait le choix d'utiliser le moteur MySQL. Parallèlement, chaque application cliente dispose de sa propre base de données. Cette itération ne concernant que la phase d'installation des composants Rice, l'installation d'une ressource extérieure fera l'objet d'une itération ultérieure.

Tous les composants Rice reposent sur des standards tels que Struts MVC pour la partie présentation. La persistance des objets métier dans la base de données (ORM : « Object Relational Mapping » en anglais) est opérée initialement par l'outil Apache ObJectRelationalBridge (OJB). Mais au fur et à mesure des montées de version des modules, cette plate-forme est abandonnée au profit du standard Java Persistance API (JPA) implémenté par l'ORM Hibernate.

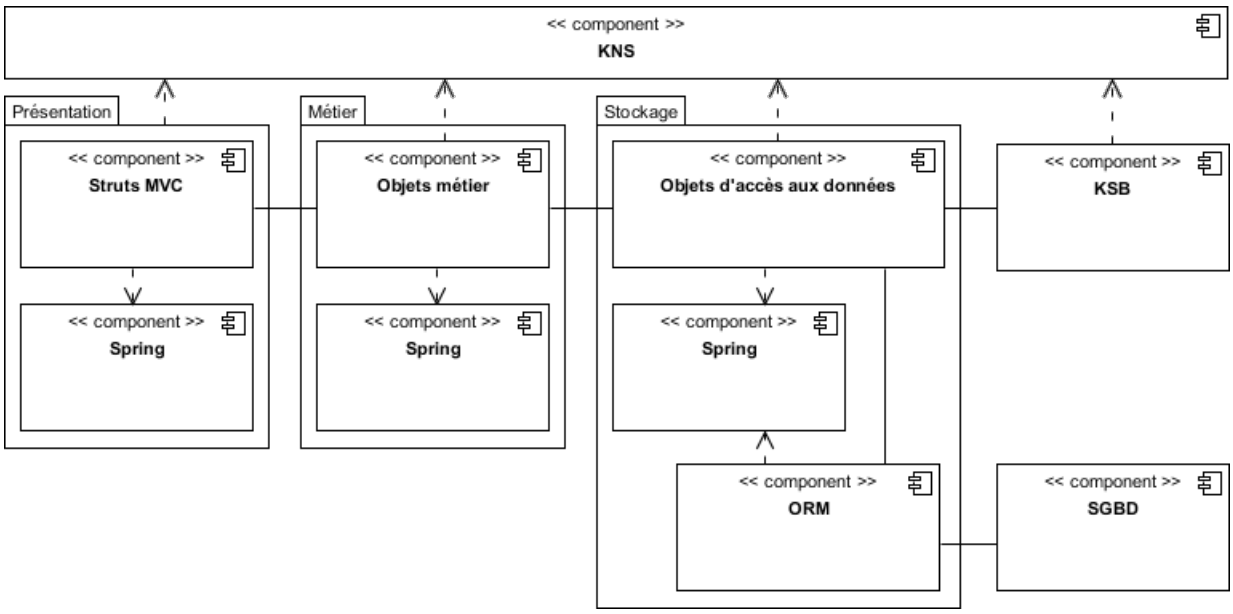


Figure 72 - Diagramme de composants de Kuali Identity Management

L'ensemble des modules Rice sont livrés au sein d'une archive Java unique au format WAR. Pour les environnements de développement, ce fichier est inclus dans une distribution complète intégrant les fichiers de configuration de la base de données.

L'installation des différents composants repose alors sur l'utilisation de l'outil d'automatisation Apache Maven.

V.3.4 Rétrospective de l'itération

En respectant la documentation d'installation de la version téléchargée 2.1.1, plusieurs problèmes ont été rencontrés lors de la construction de la base de données puis lors de l'utilisation de l'application.

V.3.4.1 Construction de la base de données

Lors de la première tentative d'installation en spécifiant le nom d'hôte, le chargement des données a généré l'erreur de refus d'accès suivante :

```
[ERROR] Failed to execute goal org.kuali.maven.plugins:sql-maven-plugin:1.0.10:execute
(validate) on project rice-impex-server-demo: Access denied for user
'RICESERVERDEMO'@'localhost' to database '/riceserverdemo' -> [Help 1]
```

Figure 73 - Message d'erreur lors de la configuration de la base de données de Kuali Rice

Pourtant, les étapes précédentes de Maven indiquaient que les connexions à la base de données se déroulaient sans problème. Des recherches sur Internet n'ont pas permis de trouver une solution. Le site de Kuali indique en effet que pour obtenir de l'assistance il faut faire appel à un des prestataires partenaires de la fondation.

Suite à cela, j'ai décidé d'utiliser le mode de connexion local, bien que cela exclut de pouvoir tester l'architecture telle que préconisée par Kuali pour un environnement de production. Bien que le chargement des données se soit correctement déroulé, les mêmes erreurs se produisent au moment de l'exécution du serveur Tomcat.

```
java.sql.SQLException: Cannot get connection for URL
jdbc:mysql://localhost:3306/riceserverdemo : Access denied for user
'riceserverdemo'@'localhost' (using password: YES)
```

Figure 74 - Message d'erreur de connexion lors de l'installation de Kuali Rice

Ces erreurs montrent que la version 2.1.1 de Kuali n'a pas été correctement testée sur l'environnement MySQL. La situation a permis également de s'apercevoir qu'il n'existe pas de communauté active qui puisse être contactée facilement.

Pour contourner les problèmes rencontrés avec le SGBDR MySQL, la documentation ne laisse que la possibilité d'utiliser le SGBDR Oracle. L'installation et la configuration ont pu être réalisées avec l'outil d'automatisation Maven et se sont terminées avec la mention « Build success ».

V.3.4.2 Utilisation

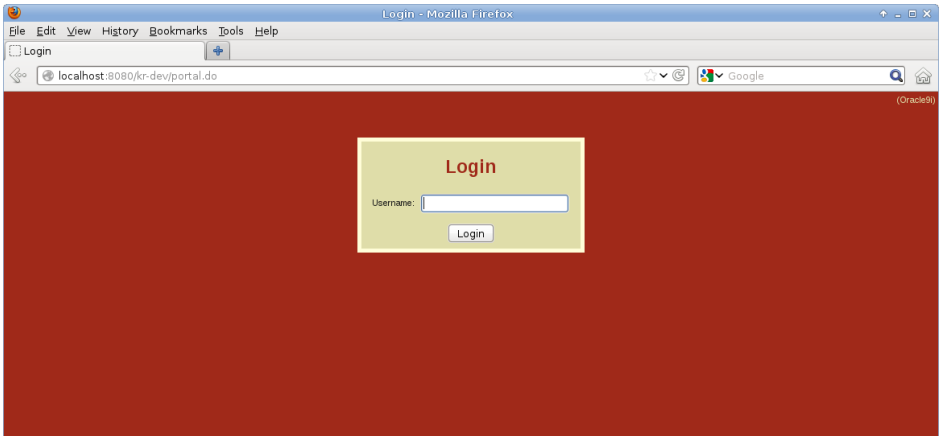


Figure 75 – Capture d'écran de la page d'accueil de Kuali Rice

La documentation n'indique pas d'identifiant à utiliser pour se connecter la première fois à l'outil. Cependant, la saisie de l'identifiant « admin » permet de rentrer dans l'application, alors que les tentatives avec les valeurs « root » ou « quickstart » apparaissant dans certaines images de la documentation ont été infructueuses. La documentation semble incomplète, mais il n'existe pas de moyen de contact pour en demander la correction.

Par ailleurs, lors de l'utilisation de l'interface d'administration, plusieurs erreurs apparaissent.

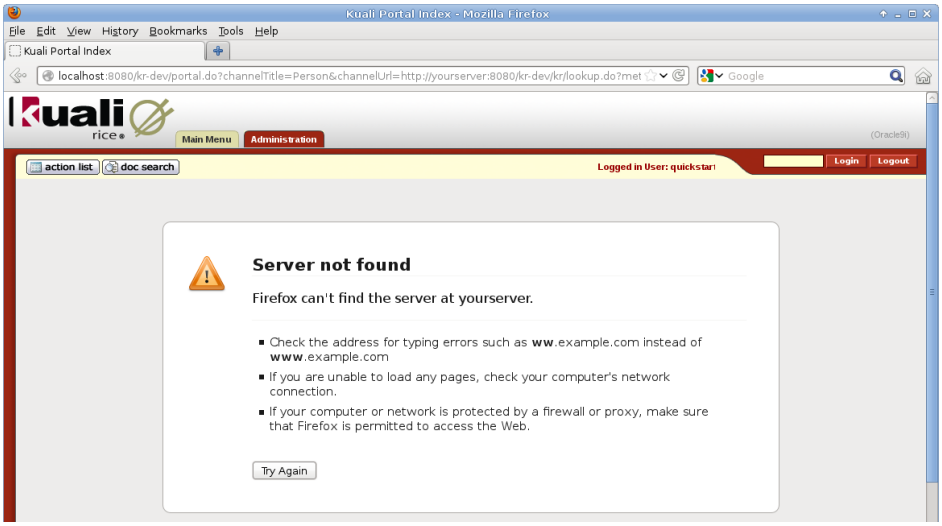


Figure 76 - Capture d'écran d'une erreur lors de l'utilisation de Kuali Rice

Cependant, ce problème ne génère par de message d'erreur dans les journaux du serveur Tomcat, mais simplement un message d'information.

```
INFO  org.kuali.rice.kns.web.struts.action.KualiRequestProcessor - Finished processing
request: '/kr-dev/portal.do' w/ query string: 'selectedTab=administration'

INFO  org.kuali.rice.kns.web.struts.action.KualiRequestProcessor - Started processing
request: '/kr-dev/portal.do' w/ query string:
'channelTitle=Person&channelUrl=http://yourserver:8080/kr-
dev/kr/lookup.do?methodToCall=start&businessObjectClassName=org.kuali.rice.kim.api.iden
tity.Person&docFormKey=88888888&returnLocation=http://yourserver:8080/kr-
dev/portal.do&hideReturnLink=true'
```

Figure 77 – Extrait des messages d'informations du serveur Tomcat de Kuali Rice

Ces erreurs montrent un problème avec l'adresse « yourserver », ce qui semble démontrer un problème de configuration alors que l'étape précédente a été réalisée sans remontée de problème.

V.3.4.3 Conclusion

Finalement, l'application Kuali Rice ne peut pas être installée avec le moteur MySQL. Avec le SGBDR Oracle la configuration s'est correctement déroulée, mais l'application ne peut pas être utilisée. Cependant, la difficulté réside dans le manque de moyen pour trouver des solutions ou demander de l'aide. Le seul moyen de joindre une personne membre de la communauté et soit d'en devenir un membre participant actif, soit de faire appel à une société commerciale. Aucune des deux solutions n'étant envisageable pendant la phase d'étude de faisabilité, il s'avère que le choix de Kuali en tant que solution Open Source de gestion des identités et des accès n'était pas approprié.

Par ailleurs, cette itération montre que les critères de notation et de sélection de l'environnement du projet n'étaient pas adéquats. C'est pourquoi la phase de sélection doit être

corrigée pour permettre de choisir un outil mieux testé avec une communauté plus active et réactive. Ensuite, l'itération « Construction du socle technique » pourra être réalisée avec la nouvelle architecture.

V.4 Reprise de l'itération 1 – Nouvelle définition de l'architecture

V.4.1 Sprint backlog

L'objectif de cette itération est de faire le choix d'une nouvelle architecture, l'itération précédente ayant invalidé l'infrastructure Kuali Rice. La « User story » du présent sprint peut donc être exprimée par la phrase « En tant qu'architecte technique, je veux évaluer les solutions techniques FLOSS et sélectionner celle qui correspond le mieux aux besoins de la DSI du CNRS ».

La première tâche consistera à définir une méthode d'évaluation des solutions Open Source différente de celle utilisée précédemment. Une étude devra permettre de trouver si un modèle existe au sein de la communauté FLOSS et si possible supporté ou sponsorisé par une organisation reconnue.

La seconde tâche consistera à appliquer la méthode sur l'ensemble des outils évoqués lors de précédente étude comparative. Les projets ForgeRock OpenIdm, OpenIam Identity Manager, Evolveum MidPoint, Apache Syncope. Kuali Identity Management sera à nouveau évaluer pour.

V.4.2 Modèles d'évaluation de la maturité

Les risques remontés lors de l'itération « Définition de l'architecture » montrent que la grille d'évaluation technique n'est pas suffisante. L'évaluation de la solution technique doit être complétée par celle du projet dans sa globalité. Pour les organismes développant des logiciels, des services ou délégant leur intégration, un modèle d'évaluation est proposé par le Software Engineering Institue, le « Capability Maturity Model Integration » (CMMI). Il permet de mesurer la maturité des processus de l'organisation liés aux développements de logiciels ou de services ou à la gestion des relations contractuelles. Chacun de ces aspects est traité dans un document spécifique, bien que la plupart des processus étudiés soient communs [24]. Ainsi CMMI pour l'acquisition est destiné à la gestion des relations avec les sous-traitants qui ont la responsabilité de concevoir et fournir des logiciels ou des services. CMMI pour le développement se focalise plus particulièrement sur les processus de développement. Enfin, CMMI pour les services est orienté vers les processus de gestion et de fourniture de services, incluant les détails de gestion de la disponibilité, des interruptions, du point de vue technique et organisationnel.

Quel que soit le document utilisé, un modèle CMMI propose deux approches pour l'évaluation de la maturité des processus et de leur évolution. La plus utilisée est la représentation

[24] M. Phillips, S. Shrum. *Which CMMI Model Is for You?*. Software Engineering Institute, Carnegie Mellon University, 4 pages, 2011

étagée [25]. Dans ce cas, l'organisation est catégorisée en fonction de niveaux de maturité. Chaque niveau de maturité est caractérisé par des secteurs clés, eux-mêmes définis par un ensemble de pratiques.

Dans le niveau par défaut, appelé « initial », des processus liés aux projets de logiciels peuvent exister au sein de l'organisation, mais leur exécution n'est pas vérifiée systématiquement car non obligatoire. Ce niveau ne fait l'objet d'aucun secteur clé. De ce fait, les estimations des coûts financiers et en temps des projets sont variables. La gestion des projets ne repose pas sur des indicateurs clés établis par l'établissement. Elle est uniquement basée sur les délais et ne prend pas en compte d'éventuelles successions de problèmes. De plus, les projets ne font l'objet d'aucune capitalisation des difficultés ou erreurs rencontrées. Cette situation n'implique pas que les produits ou services fournis ne sont pas de qualité, mais que tous les engagements ne sont pas obligatoirement respectés et qu'il n'existe pas de moyen de reproduire les sources de succès dans les projets.

Atteindre le second niveau, appelé « discipliné » ou « reproductible », implique qu'un minimum de discipline existe dans les projets bien que des variations subsistent. Ainsi, l'utilisation de processus définis au niveau de l'organisation est contrôlée, les réalisations sont comparées aux exigences initiales et des actions correctrices sont mises en place. De plus, les rôles et responsabilités de chacun des acteurs impliqués sont clairement établis. Ces exigences ont notamment pour conséquence d'améliorer la fiabilité des estimations. Ce niveau est caractérisé par les six secteurs clés « Gestion de configuration logiciel », « Assurance qualité logiciel », « Gestion sous-traitance au forfait », « Suivi de projet », « Planification » et « Gestion des exigences ».

Le niveau suivant, appelé « ajusté » ou « défini », met l'accent sur l'amélioration et à la prévention. Cela implique la mise en place de processus de capitalisation systématiques à la fin des projets, ce qui entraîne le perfectionnement des processus existants et la réutilisation du savoir-faire, des réalisations telles le code applicatif ou la documentation. Cette cohérence entre les projets conduit à une meilleure gestion des risques. Ce niveau est caractérisé par les sept secteurs « Revues par les pairs », « Coordinations intergroupes », « Ingénierie produit logiciel », « Gestion intégrée de projet », « Formation », « Définition du processus » et « Amélioration du processus ».

Au quatrième niveau, appelé « quantifié » ou « contrôlé », l'organisation exploite des modèles de performances et de prévision basés sur des indicateurs quantitatifs et est capable de mesurer les impacts liés aux évolutions de processus. Chaque projet doit alors respecter des objectifs qui sont régulièrement évalués. L'examen systématique des données issues des projets permet d'éviter une

---

[25] Equipe produit CMMI. *CMMI pour le développement, version 1.3*. Software Engineering Institute, Carnegie Mellon University, 570 pages, 2010

régression de la maturité obtenue. Ce niveau est caractérisé par les deux secteurs clés « Gestion de la qualité logiciel » et « Gestion quantitative du processus ».

Le dernier niveau « optimisé » correspond à une optimisation permanente des processus. Il repose sur la mise en œuvre de processus d'innovation et d'analyse des causes et solutions des problèmes rencontrés par les projets. L'organisation a alors appris à gérer les changements et à assurer un suivi des performances individuelles et collectives. Le cinquième niveau est caractérisé par les trois secteurs clés « Gestion des évolutions du processus », « Gestion des évolutions de la technologie » et « Prévention des défauts ».

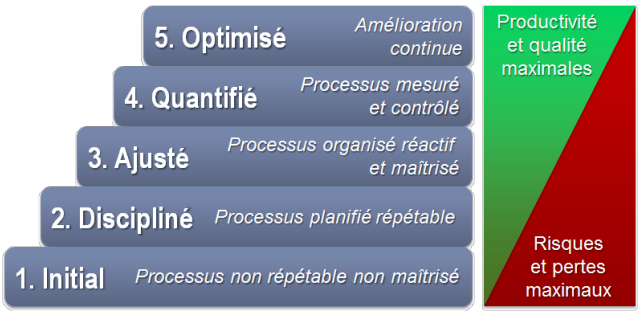


Figure 78 - Echelle de maturité à cinq niveaux de CMMI

Comme le démontrent H. Glazer, J. Dalton, D. Anderson, M. Konrad et S. Shrum, les modèles CMMI peuvent être utilisés pour des organismes dont la gestion de projet suit des méthodes Agiles [26]. Aussi, la maturité, la pérennité et l'engagement de qualités des projets de logiciels FLOSS qui reposent sur des développements itératifs pourraient être évalués à l'aide de modèles tels que CMMI pour le développement et les services. Cependant, la difficulté de tels projets réside dans l'organisation des développements qui peuvent être réalisés en dehors de tout processus explicite. C'est pourquoi, il est plus difficile d'appliquer CMMI aux processus de développement. De ce fait, les méthodes de gestion de projet et de production du code propres aux logiciels FLOSS doivent être prises en compte par un modèle de maturité spécifique. K.-J. Stol et M. Ali Babar [27] ont retenu vingt approches pour l'évaluation des logiciels libres parmi lesquelles cinq utilisent des critères relatifs aux coûts totaux de possession (TCO : « Total Cost of Ownership » en anglais) ainsi qu'à la maturité du projet.

[26] H. Glazer, J. Dalton, D. Anderson, M. Konrad, S. Shrum. *CMMI or Agile: Why Not Embrace Both!*. Software Engineering Institute, Carnegie Mellon University, 45 pages, 2008

[27] K.-J. Stol, M. Ali Babar. A Comparison Framework for Open Source Software Evaluation Methods. Dans *Open Source Software: New Horizons*, pages 389-394, 2010

V.4.3 Modèles d'évaluation de la maturité pour les logiciels FLOSS

La structure spécifique des organisations développant des logiciels FLOSS ne permet pas de s'appuyer sur CMMI pour évaluer la maturité des offres FLOSS. Les modèles Open Source Maturity Model de Cap Gemini, ou de Navica, QSOS d'Atos, OpenBRR et QualiPSo présentés dans les paragraphes suivants prennent en compte les spécificités des logiciels FLOSS.

Open Source Maturity Model (OSMM) de la société Cap Gemini a été développé en 2003. Ce modèle repose sur douze critères, notés de un à cinq, répartis en quatre catégories [28]. L'évaluation du produit se base sur l'âge du produit, le type de licence, le degré de hiérarchie au sein des développeurs, les points forts de l'outil et la communauté de développeurs. L'intégration de la solution est jugée sur sa modularité et sa capacité à s'interfacer avec d'autres produits. Ensuite, la facilité d'utilisation est estimée à partir des standards utilisés et des offres de support. Enfin, la facilité d'adoption de la solution est examinée d'après la facilité de déploiement, la communauté des utilisateurs ainsi que la pénétration du marché. Cette méthode d'évaluation étant soumise à une licence payante, elle ne sera pas étudiée plus amplement.

En 2004, B. Golden [29] dirigeant de la société Navica a publié un OSMM concurrent. L'évaluation d'une solution libre repose sur les six éléments clés suivants : la solution logicielle, l'offre de support, la documentation, l'offre de formation, la capacité d'intégration du produit et l'offre de services. La note de chacun de ces sujets est construite en quatre étapes. La première phase consiste à déterminer les besoins. Puis, il faut déterminer les ressources disponibles sur le produit, en contactant les développeurs, les organismes partenaires, etc. Ensuite, il faut évaluer la maturité de l'élément étudié. Chacun des chapitres dispose de ses propres critères de maturité. Ainsi, le modèle propose de considérer par exemple la pérennité, la qualité de la solution logicielle, les différents types de support, la présence de tutoriaux ou encore les différents moyens de formation disponibles. La dernière étape est d'attribuer une note sur une échelle de un à dix. Les différentes catégories clés ont des pondérations par défaut qu'il est possible d'ajuster en fonction des besoins et de la marge de risque acceptable. Suite à ces différentes étapes, une note est calculée pour chaque élément clé permettant d'estimer la maturité de tout l'environnement de la solution libre étudiée. Ce modèle reposant uniquement sur la publication réalisée par une seule personne et la société Navica n'existant plus, il a été abandonné. De ce fait, il ne peut pas être utilisé pour la présente étude.

---

[28] F.-W. Duijnhouwer, C. Duijnhouwer. *Open Source. Maturity Model*, Capgemini Expert Letter, 2003

[29] B. Golden. *Succeeding with Open Source*. Addison-Wesley Professional, 272 pages, 2004

En 2004, la société Atos a développé la méthode de qualification et de sélection de logiciels Open Source (QSOS) [30]. Elle repose sur un processus itératif composé de quatre étapes.

La première phase « Définir » a pour objectif de définir la typologie de la solution logicielle au niveau de la licence et de la communauté. La seconde phase « Evaluer » est la constitution des fiches d'identité des outils ainsi que des fiches d'évaluation. La notation est réalisée sur des critères répartis selon les axes de couverture fonctionnelle, de risque utilisateur et éventuellement du risque du point de vue du prestataire de service si l'étude est réalisée par une société de services. Le processus étant itératif, le niveau de granularité des critères d'évaluation peut être affiné en trois itérations. Ainsi l'évaluation est faite au niveau des cinq catégories principales pour la première, au niveau des sous-catégories pour la seconde et au niveau des critères le plus fins pour la dernière.

La troisième phase du processus « Qualifier » permet d'ajuster les critères au contexte. Ainsi, pour la couverture fonctionnelle l'objectif est d'affecter un niveau d'exigence à chaque fonctionnalité (requise, optionnelle ou non requise) et pour les risques utilisateurs de définir le degré de pertinence des critères. La quatrième phase « Sélectionner » permet de faire le choix d'un outil en se basant sur les critères définis précédemment.

Atos Origin fournit un outil qui permet d'assister l'utilisateur dans l'exécution des différentes étapes et de générer des graphiques facilitant la comparaison des solutions Open Source. Par ailleurs, la méthode étant sous licence GNU Free Documentation, les documents générés avec QSOS et ses outils sont également soumis à ce type de licence.

---

[30] R. Semeteys, O. Pilot, L. Baudrillard, G. Le Bouder. *Méthode de Qualification et de Sélection de logiciels Open Source (QSOS) version 1.6*. Atos Origin, 36 pages, 2006

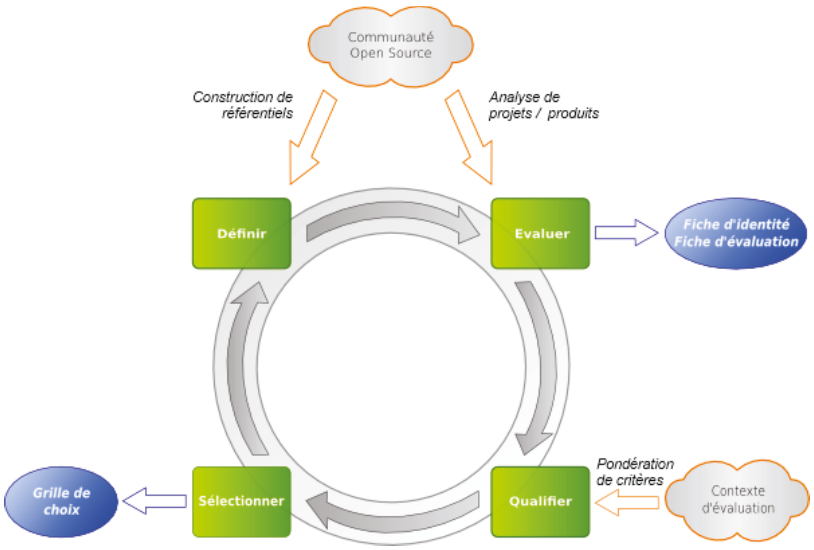


Figure 79 - Processus itératif de qualification et de sélection de logiciels Open Source (QSOS)
(source : http://www.qsos.org)

En 2005, l'université de Carnegie Mellon Silicon Valley, les sociétés SpikeSource, O'Reilly et Intel ont débuté la rédaction de la méthode Business Readiness Rating for Open Source (OpenBRR)[31]. A l'instar de QSOS, OpenBRR est une méthode en quatre étapes facile à mettre en œuvre. La première phase « Evaluation rapide » permet de filtrer les solutions candidates en fonction de critères de licence et de viabilité fournis par la méthode. La seconde phase « Evaluation de l'utilisation cible » a pour objectif de lister et pondérer l'ensemble des critères à évaluer. Pour cela, la méthode fournit douze catégories qu'il faut classer par ordre d'importance. Ensuite il faut affecter un poids aux sept premières, les suivantes n'étant pas utilisées. Ensuite pour chaque catégorie, il faut procéder comme précédemment, donc classer les critères par ordre d'importance vis-à-vis des besoins métiers et leur affecter un poids. La troisième phase « Collecte des données et traitement » vise à réunir les informations sur les outils pour chaque critère sélectionné à l'étape précédente puis à calculer une note en appliquant la pondération. La dernière phase « Traduction des données » requiert d'utiliser les notes obtenues par chaque critère pour calculer une note globale pour chacune des catégories sélectionnées à la seconde étape. Ce score permet d'établir le taux d'adéquation au métier (BRR : « Business readiness rating » en anglais). Cependant, la méthode est encore à l'état de « Request For Comment » et aucune publication plus récente que la première version n'est disponible. De ce fait, les critères de maturité tels qu'évoqués par cette même méthode tendent à avertir d'un risque fort quant à sa viabilité. De ce fait, il est préférable de ne pas l'utiliser.

[31] A. Wasserman, M. Pal, C. Chan. *Business Readiness Rating for Open Source, BRR Whitepaper 2005 Request For Comments 1*. OpenBRR.org, 22 pages, 2005

Le consortium « Quality Platform for Open Source Software » (QualiPSo) fut fondé en 2006 par la Commission Européenne au travers de son sixième programme cadre des technologies de l'information (FP6 IST) « Information Society Technologies: thematic priority under the specific program "Integrating and strengthening the European research area" (2002-2006) » auxquels se sont joints des entreprises telles qu'Atos Origin et des organismes gouvernementaux européens, brésilien et chinois, dont la gendarmerie nationale française et l'Institut National de Recherche en Informatique et Automatique (INRIA). QualiPSo, qui compte actuellement dix-huit participants, a pour objectifs de développer des méthodologies, des processus et des outils pour les projets Open Source et ainsi se rapprocher des exigences de qualité des solutions propriétaires pour donner confiance dans ces solutions aux clients potentiels. Dans ce cadre, QualiPSo a conçu une certification de qualité et de maturité OpenSource Maturity Model (OMM) dérivée de CMMI et adaptée aux organisations virtuelles qui ne dépendent pas d'infrastructures et/ou d'outillages formels. OMM ne se focalise donc pas sur les processus de l'organisation mais sur douze éléments qui peuvent donner confiance (en anglais : (TWE : « Trustworthy elements » en anglais) dont certains sont extraits ou inspirés de CMMI [32] :

1. Documentation du produit (PDOC) correspondant au paragraphe SP 3.2 « Développer la documentation de soutien au produit » du domaine de processus « Solution technique » du niveau 3 de maturité CMMI [25],
2. Popularité du produit (REP),
3. Standards établis et répandus (STD) correspondant au domaine de processus CMMI « Assurance qualité processus et produit » du niveau 2 de maturité CMMI [25],
4. Feuille de route du produit (RDMP : « roadmap » en anglais) évoqué dans CMMI aux paragraphes SP 2.1 « Établir les exigences produit et composants de produit » du domaine de processus « Développement des exigences » et SP 1.1 « Établir une stratégie d'intégration » du domaine de processus « Intégration de produit » du niveau 3 de maturité CMMI [25],
5. Plan de tests de la qualité (QTP) correspondant au paragraphe SP 1.3 « Établir les procédures et les critères de vérification » du domaine de processus « Vérification » du niveau 3 de maturité CMMI [25],
6. Relations entre les parties prenantes (STK : « stakeholder » en anglais) correspondant aux paragraphes SP 2.6 « Prévoir l'implication des parties prenantes » du domaine de processus « Planification de projet » du niveau 2 de maturité CMMI [25] et SP 2.1 « Gérer l'implication

[32] M. Wittmann, R. Nambakam, G. Ruffati, S. Oltolina, E. Petrinja, F. Ortega, V. Malheiros, D. Tosi. *Working Document 6.3.1 - CMM-like model for OSS*. Qualipso, 140 pages, 2009

des parties prenantes » du domaine de processus « Gestion de projet intégrée » du niveau 3 de maturité CMMI [25],

7. Licences (LCS),
8. Environnement technique (ENV) correspondant aux paragraphes SP 2.4 « Prévoir les ressources du projet » du domaine de processus « Planification de projet » du niveau 2 de maturité CMMI [25] et SP 2.1« Gérer l'implication des parties prenantes » du domaine de processus « Gestion de projet intégrée » du niveau 3 de maturité CMMI [25],
9. Nombre de validations et de bugs rapportés (DFCT),
10. Maintenabilité et stabilité (MST) correspondant aux paragraphes SP 1.2 « Transformer les besoins des parties prenantes en exigences client » du domaine de processus « Développement des exigences » et SP 2.1 « Concevoir le produit ou le composant de produit » du domaine de processus « Solution technique » du niveau 3 de maturité CMMI [25],
11. Contribution de sociétés de logiciels commerciaux dans le développement de logiciels libres (CONT),
12. Résultats d'évaluation du produit par une société tierce (RASM).

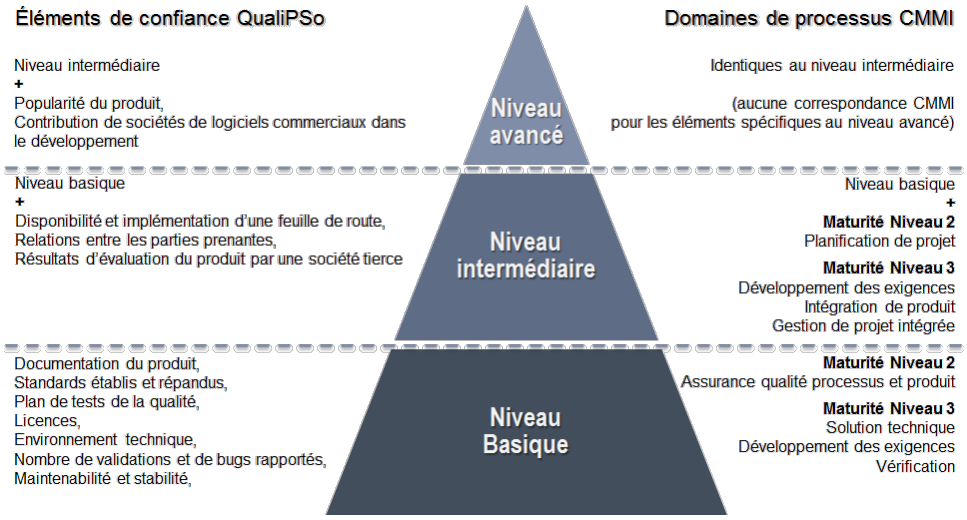


Figure 80 - Echelle de maturité à trois niveaux de QualiPSo

Comme le montrent ces éléments d'évaluation, le modèle de maturité de QualiPSo est destiné aux organisations qui produisent des outils Open Source ou qui les auditent dans un objectif d'amélioration des activités connexes au développement. Si l'organisation qui gère le projet libre applique ce modèle, alors le résultat peut être utilisé pour évaluer le produit et son environnement. Dans le cas contraire, il n'est pas opportun d'envisager ce moyen pour sélectionner des produits.

Comme aucune solution candidate pour le projet IAM n'a été examinée via le modèle de maturité de QualiPSo, il ne peut donc pas être utilisé pour les comparer. Aussi, parmi les cinq modèles d'évaluation seul QSOS est finalement utilisable.

V.4.4 Evaluation par la méthode QSOS

V.4.4.1 Définir la grille d'évaluation

L'étape « Définir » a pour objectif de construire les référentiels typologiques utilisés dans les étapes suivantes. Pour chaque type de licence, il faut évaluer si le code modifié peut être rendu propriétaire ou s'il doit rester libre, s'il doit être placé obligatoirement sous la même licence et s'il est possible d'appliquer des restrictions supplémentaires. Ces référentiels fournis par Atos semblent complets et ne nécessitent donc pas de mise à jour.

V.4.4.2 Evaluer le projet

L'étape d'évaluation débute par la constitution de la fiche d'identité du projet qui contient plusieurs critères quantifiables mais qui ne font pas partie de la notation. Ensuite, la fiche d'évaluation permet de noter plusieurs critères sur la couverture fonctionnelle qui sont repris de la grille d'évaluation rédigée lors de la première étape ainsi que des critères liés à l'utilisation du logiciel Open Source pour l'organisme qui le déploie.

La méthode propose également un ensemble d'outils pour faciliter la saisie des informations. Ainsi les critères de couverture peuvent être enregistrés dans une carte heuristique (en anglais « mindmap ») avec l'outil freeMind. Un fichier modèle est disponible incluant les critères liés à l'adoption d'un logiciel Open Source (cf. annexe 4 « Carte heuristique QSOS de maturité »). Comme évoqué précédemment, il est possible de procéder par itération pour construire le modèle. Chaque itération permet alors de renseigner un niveau de profondeur supplémentaire. Ensuite, via un fichier XSLT fourni, la carte heuristique saisie est transformée en fichier XML au format XUL. Développé par la fondation Mozilla, XUL (XML User interface Language) permet de réaliser des interfaces graphiques Web riches au même titre qu'Adobe Air/Flex avec le langage XML. L'application ainsi générée permet de saisir la fiche d'évaluation de chacun des logiciels étudiés.

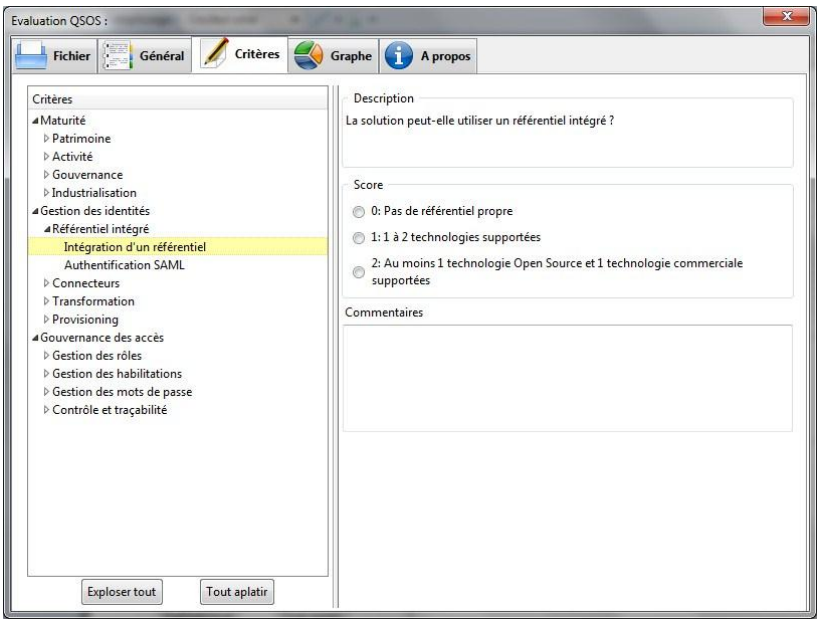


Figure 81 – Application XUL générée par les outils QSOS

V.4.4.3 Qualifier le contexte

L'étape de qualification a pour objectif d'adapter les critères au contexte de l'organisation. Pour cela, il est possible de positionner des filtres aux différents critères notés dans l'étape précédente. Ces filtres sont exprimés sous forme de pondération.

Ainsi sur la fiche d'identité des projets, il est possible de ne pas prendre en compte certains critères en positionnant un poids nul. Cette première étape optionnelle de filtrage permet d'éliminer des projets ne correspondant pas aux attentes de l'utilisateur.

L'étape suivante de couverture fonctionnelle permet d'affecter un niveau d'exigence aux critères. Chaque fonctionnalité doit être définie comme requise, optionnelle ou non requise. Ces exigences sont traduites en valeur numérique de pondération respectivement de « +3 », « +1 » et « 0 ».

Ensuite, il est possible d'attribuer un degré de pertinence aux risques liés à l'utilisation d'un outil Open Source, incluant l'environnement, l'activité, la gouvernance ou le niveau d'industrialisation. Chacun des risques utilisateur doit être défini comme non pertinent, pertinent ou critique. La pertinence est associée à une valeur numérique de pondération respectivement de « 0 », « 1 » et « 3 ». Les valeurs peuvent être positives ou négatives en fonction de l'impact positif ou négatif du respect du critère sur la capacité du logiciel à répondre aux besoins.

Un filtre supplémentaire peut être employé par un prestataire de services pour évaluer les logiciels et les prestations à intégrer dans son offre et déterminer les niveaux d'engagement associés.

L'outil Open Source Selection Software (O3S) offre une interface graphique pour saisir ces informations, puis comparer les fiches d'évaluation réalisées dans l'étape précédente.

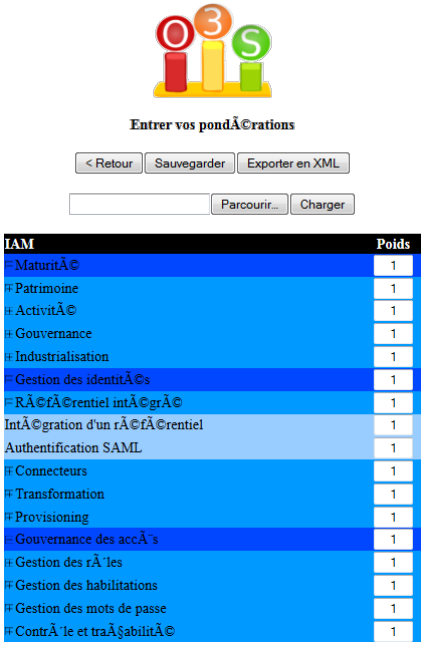


Figure 82 – Capture d'écran de saisie de qualification du contexte dans l'outil O3S

V.4.4.4 Sélectionner

La sélection d'un logiciel peut être réalisée selon deux modes distincts.

La méthode stricte consiste à éliminer un projet dès qu'une fonctionnalité requise n'est pas disponible. De même, un projet est exclu quand un critère de risque utilisateur n'est pas satisfait, ce qui implique une note inférieure à « 1 » pour un critère pertinent ou à « 2 » pour un critère critique. Cette méthode peut éventuellement mener à un résultat nul dans le cas où tous les candidats ont été rejetés. Ensuite, les notes finales de chaque critère sont calculées à partir des notes affectées à l'étape d'évaluation en appliquant les filtres et coefficients déterminés à l'étape de qualification. Ces valeurs permettent alors de comparer les logiciels.

La méthode souple ne permet pas d'éliminer des logiciels mais simplement de mesurer l'écart constaté par rapport aux filtres définis précédemment. Comme avec la méthode stricte, le calcul des notes permet d'obtenir un comparatif objectif des projets.

Comme précédemment, l'outil O3S offre une interface graphique pour réaliser cette démarche. La comparaison peut alors être réalisée à partir d'un tableau comparatif, d'un graphique radar ou de type quadrant.

Dans le cadre du projet IAM, la méthode souple a été choisie pour effectuer la sélection. Après application des pondérations pour les critères requis, l'outil O3S permet de générer le quadrant suivant.

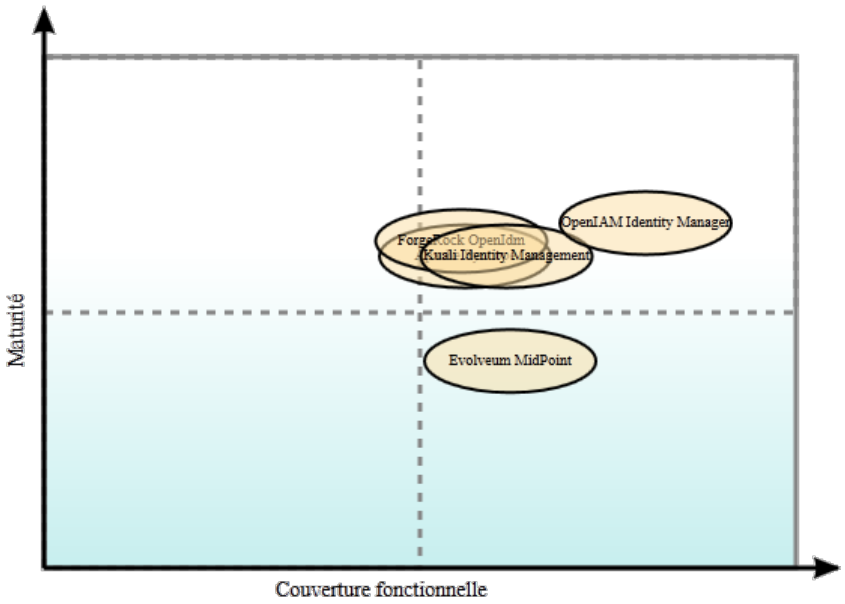


Figure 83 - Quadrant généré par l'outil O3S

Le graphique montre que la solution de Kuali répondait bien aux besoins. Cependant, la méthode QSOS donne un net avantage à OpenIAM Identity Manager.

V.4.5 Rétrospective de l'itération

La méthode QSOS semble plus fiable que la méthode utilisée précédemment. En effet, la maturité de Kuali est montrée comme étant plus faible que trois autres offres, ce qui tend à prouver que KIM ne devait pas être choisi.

V.5 Reprise de l'itération 2 – Construction du nouveau socle technique

V.5.1 Sprint backlog

Suite au choix d'un nouvel outil, cette itération reprend les objectifs du sprint de construction technique qui s'est conclu par des problèmes d'installation de l'outil Kuali Identity Management. L'objectif de l'itération est donc de procéder à l'installation du produit OpenIAM Identity Management. Pour cela, la première phase consiste à appréhender l'architecture du produit afin de comprendre comment interagissent les différents composants et quelles sont les possibilités de déploiement pour prendre en charge la population connue des annuaires LDAP et Active Directory.

La « User story » du présent sprint peut être exprimée par : « En tant qu'architecte technique, je veux installer le socle technique OpenIAM Identity Manager 2.2.2».

V.5.2 Environnement d'installation

Une nouvelle machine virtuelle est préparée afin que les réalisations à venir ne soient pas impactées par les reliquats résiduels de l'installation précédente. Elle est construite à partir de la sauvegarde réalisée entre l'installation du système d'exploitation et l'installation des logiciels.

V.5.3 Architecture

OpenIAM Identity Manager est une solution trois tiers J2E exécutée par le containeur de servlets Tomcat livré en version 6.0.35. Elle est composée d'outils interagissant ensemble au travers de composants appartenant à trois couches de services.

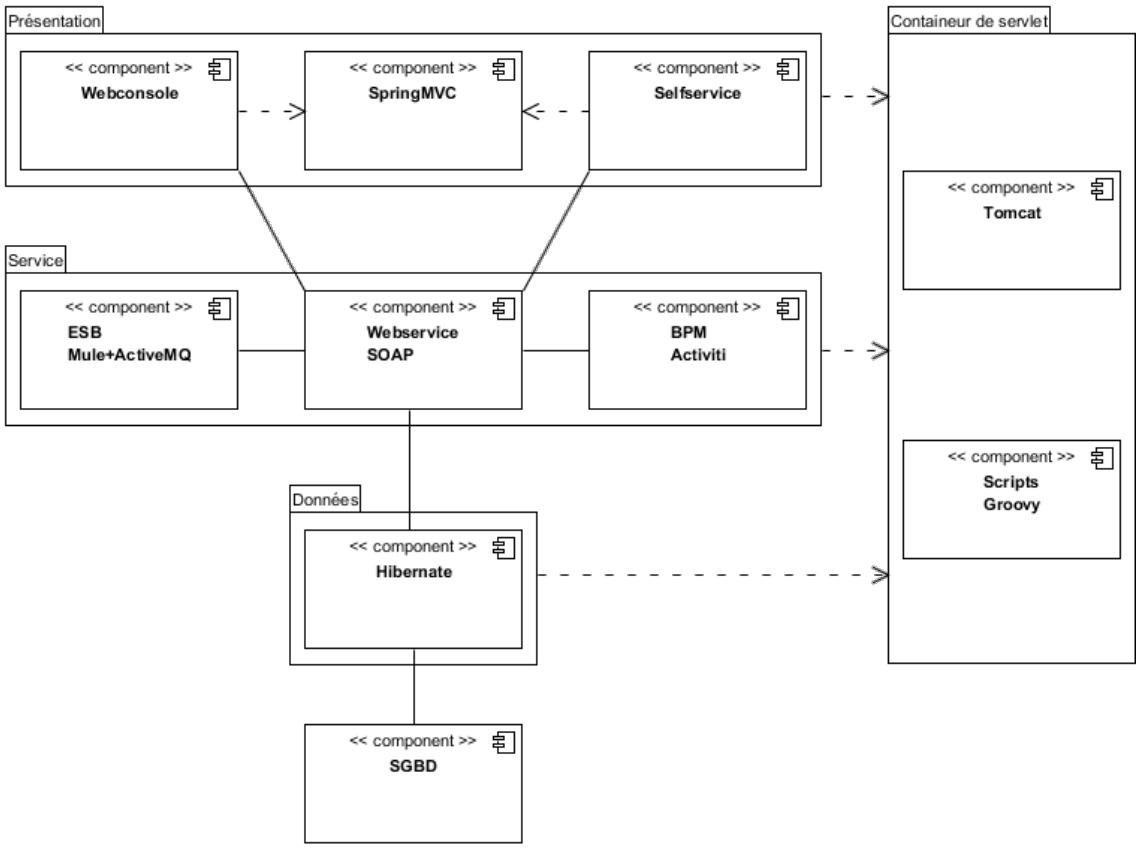


Figure 84 - Architecture de la solution OpenIAM Identity Management

V.5.3.1 Stockage des données

La couche « stockage de données » ne peut être assurée que par le SGBDR MySQL pour la version communautaire qui est utilisée lors de cette étude alors que la version commerciale permet d'utiliser les moteurs Oracle RDBMS et Microsoft SQLServer. La couche ORM va évoluer dans la prochaine version majeure de Hibernate vers le standard JPA.

La couche « présentation » de la solution comporte une console d'administration disponible via l'application « webconsole » ainsi qu'une application « selfservice » dédiée aux utilisateurs du système d'information de l'organisation.

V.5.3.2 Services

La couche « service » repose sur un bus de messages (ESB : « Enterprise Service Bus » en anglais) Mule qui distribue les appels envoyés par les couches « présentation » et « stockage » à des webservices au format SOAP. Ainsi, chaque élément peut envoyer ou recevoir des informations par ce biais et demander la réalisation d'une action à un autre composant au travers d'un webservice. De ce fait, chaque composant peut être exécuté par un containeur de servlet indépendant, ce qui permet d'accroitre la capacité de traitement de la solution. De plus, l'indépendance des différentes

couches permet à chaque élément d'évoluer à des rythmes différents. Ainsi, des changements correctifs ou fonctionnels développés sur un élément n'ont pas d'impact sur les autres composants.

Les webservices fournis par OpenIAM font appels à des scripts Groovy pour exécuter les traitements. Cependant, les appels aux webservices sont indépendants des langages de programmation employés. Ainsi, de nouvelles fonctionnalités peuvent être développées dans des langages de programmation autres que Java, ce qui peut permettre de réutiliser des outils déjà présents dans le système d'information du CNRS.

Par ailleurs, le moteur Activiti de gestion des processus métier (BPM : « Business Process Management » en anglais) permet de piloter l'enchainement des tâches de gestion des identités nécessitant l'intervention d'une personne. Un processus peut être déclenché par différents types d'évènements tels que d'une demande d'approbation, une demande d'accès ou une demande de génération de rapport d'audit. Il peut alors interagir avec les webservices d'identité comme les connecteurs aux ressources ou d'autres services de l'organisation. En effet, le moteur BPM peut être configuré pour être à l'écoute de différentes sources d'informations telles qu'une adresse de courrier électronique dont la réception d'un message déclenche une action. Le moteur est évidemment préconfiguré pour travailler avec le bus de messages d'OpenIAM.

V.5.3.3 Présentation

La couche « présentation » est constituée de deux outils distincts pouvant être déployés dans le même conteneur de servlet ou indépendamment sur des serveurs distincts différents de ceux où les autres couches ont été installées. Ces deux interfaces graphiques sont développées avec la plate-forme « Modèle-Vue-Contrôleur » (MVC) Spring MVC.

L'application d'administration permet aux comptes identifiés comme administrateur de gérer tous les aspects liés aux identités, ce qui inclut, les comptes utilisateurs, les rôles, les groupes, les modes d'authentification et les processus métier. Ainsi pour les comptes utilisateur, les fonctionnalités offertes sont la création, la désactivation, l'activation et la suppression mais également la définition des attributs de l'identité, l'attribution de rôles, l'assignation à des groupes et la consultation de l'historique.

L'application « self-service » est utilisable par l'ensemble des utilisateurs du système d'information du CNRS. Elle permet à tout utilisateur de mettre à jour ses informations. Elle fournit également un module de gestion des mots de passe qui permet de le réinitialiser, mais aussi de déverrouiller ou réactiver son compte utilisateur. L'application offre également un module de gestion par délégation qui permet sans utiliser la console d'administration de modifier les informations et les attributions de comptes utilisateurs pour lesquels l'administration a été déléguée

à certaines personnes. Un module permet également à un utilisateur reconnu de demander la création d'un utilisateur envoyant alors une requête pour approbation aux personnes autorisées.

V.5.3.4 Audit

La solution OpenIAM fournit des outils d'audit. Ainsi, chaque évènement reçu ou envoyé par le bus de message est journalisé dans la base de données. Un webservice existe nativement pour pouvoir exporter ces informations vers un système tiers.

Par ailleurs OpenIAM fournit des modèles de rapport au format Eclispe BIRT. La génération et l'affichage de tels rapports ne fait donc pas partie des composants d'OpenIAM, mais nécessite une infrastructure annexe. Les rapports fournis en standards permettent d'afficher les informations traitées par le bus de message, les tentatives de connexion, la liste des utilisateurs inactifs, les tentatives de changement de mot de passe, la liste des rôles, les détails d'activation et de désactivation des utilisateurs et la liste de l'ensemble des utilisateurs.

V.5.3.5 Connecteurs

La solution OpenIAM peut se connecter à différentes ressources pour ajouter et supprimer des comptes utilisateurs aux travers de connecteurs non intrusifs. En effet, ils ne nécessitent pas le déploiement d'agent dans les systèmes cibles. De plus, conformément à l'ensemble des composants, les connecteurs sont des webservices, ce qui facilite le développement d'une nouvelle interface de connexion.

OpenIAM fournit nativement des connecteurs pour les annuaires LDAP, Active Directory, les applications « Google Apps », les serveurs Linux, les comptes utilisateurs des bases de données Oracle. Il est également possible de modifier le contenu d'une table de base de données ou de faire appel à un script groovy.

V.5.4 Rétrospective de l'itération

L'étape de configuration a nécessité la modification du fichier « securityconf.properties », ce qui n'était pas indiquée dans la documentation. Cependant, le problème était évoqué dans un des sujets ouverts dans le forum. Bien que la documentation n'a pas été mise à jour suite à la question, cette situation prouve qu'il est possible d'obtenir rapidement des réponses par l'équipe de développement.

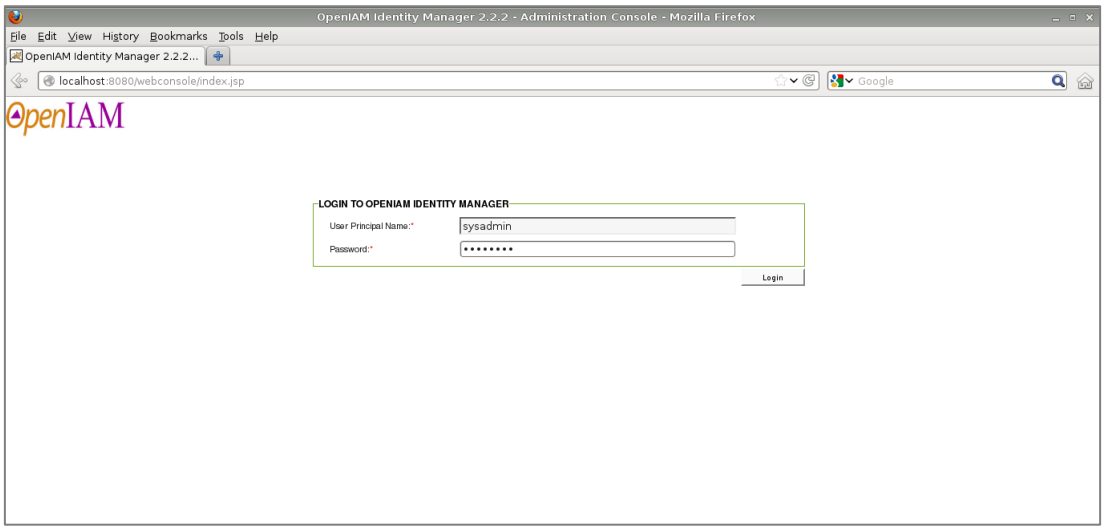


Figure 85 - Ecran de connexion à la console d'administration d'OpenIAM

Par ailleurs, le module page blanche doit être adapté pour être conforme aux obligations de la loi française Informatique et Libertés (cf. paragraphe « Cadre réglementaire »). En effet, nativement, celui-ci ne permet pas de soustraire des comptes à la recherche. Hors, toute personne le désirant, peut demander le retrait de son compte de la liste visible de tous. Cette modification n'étant pas prévue dans le cadre de cette étude, elle pourra être prise en compte dans un sprint ultérieur.

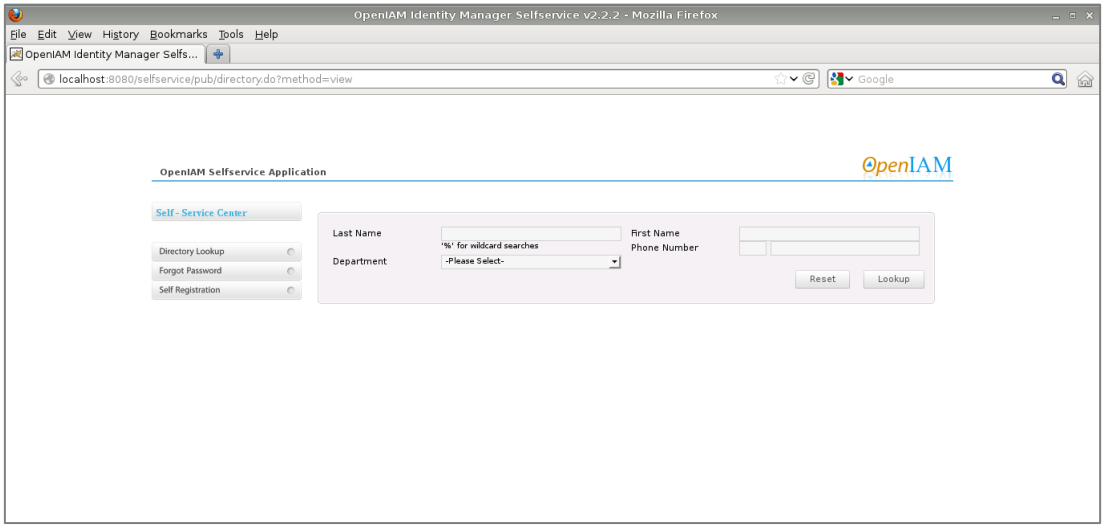


Figure 86 - Ecran de l'application page blanche d'OpenIAM self-service

De plus, l'interface graphique de la console d'administration et de l'application self-service n'est disponible qu'en anglais. Bien qu'il semble possible d'internationaliser certains paramètres d'affichage, notamment pour le libeller des attributs, aucune traduction ne semble livrée nativement pour l'ensemble de l'interface. L'aspect traduction pourra faire l'objet d'une itération à part entière.

Une autre itération pourra être envisagée sur la sécurité des webservices. En effet, les webservices sont accessibles par une adresse URL. Il faudra donc s'assurer que leur utilisation est légitime. Pour cela, la solution pourra consister à les protéger par Janus.

V.6 Itération 3 – Construction du référentiel des identités

V.6.1 Sprint backlog

L'objectif de cette itération est d'initialiser les données de l'outil avec les données présentes dans Labintel. La User story correspondante peut être exprimée selon la phrase « En tant qu'architecte du système d'information, je veux construire un référentiel d'identités alimenté avec les données de Labintel ». La première tâche consistera à alimenter le référentiel de l'outil avec les données Labintel en respectant le modèle d'identité fourni par défaut par OpenIAM Identity Management. Dans le langage des outils de gestion des identités et des accès, ce processus s'appelle « synchronisation ». Une seconde phase devra étendre le modèle de d'identités pour prendre en charge un plus grand nombre d'informations présentes dans Labintel et mettre à jour les informations chargées précédemment.

V.6.2 Modèle des identités

Par défaut, dans OpenIAM Identity Management, une personne est définie selon la RFC 2798. Cette dernière décrit la classe « InetOrgPerson » dont héritent les classes « cnrsPerson » et « refUser » qui sont utilisées respectivement dans les annuaires « Central » et « Référentiel ». La classe « eduPerson » définie par le consortium Internet2 pour représenter les personnes présentes sur un campus universitaire hérite également de « InetOrgPerson » et est parente de son équivalente française, la classe « supannPerson » décrite dans la norme supAnn 2009.

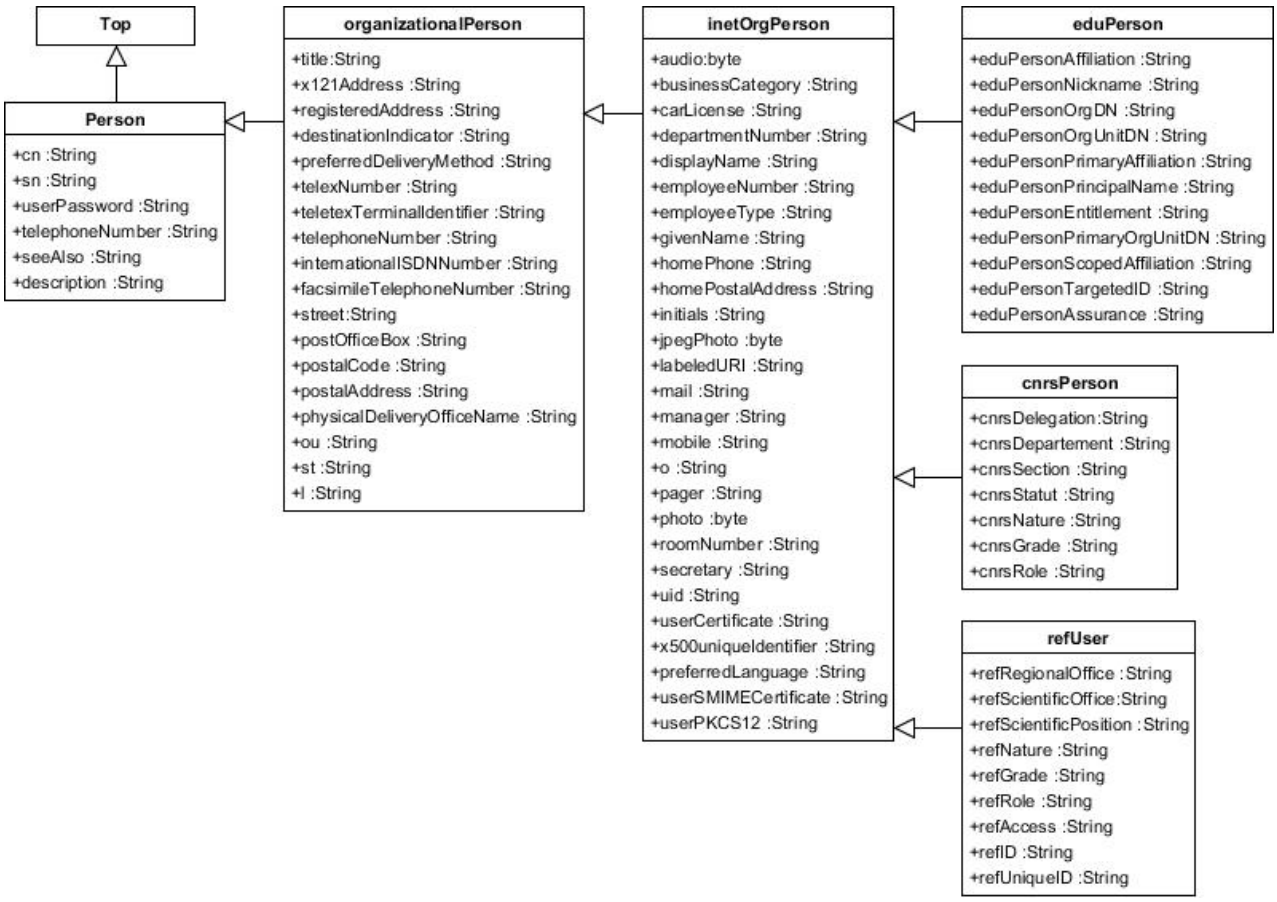


Figure 87 - Diagramme de classe de définition des identités

De plus, des informations techniques sur les comptes utilisateurs manipulées par Janus et DMAS sont stockées dans les classes « cnrsSystemInfo » et « refSystemInfo » respectivement implémentées dans les annuaires « Central » et « Référentiel ». Dans ce dernier, l'attribut booléen « refUnauthenticable » est utilisé pour déterminer si un compte est habilité à s'authentifier dans Janus, dans quel cas la valeur est positionnée à « false ». Actuellement, l'information est utilisée uniquement pour s'assurer qu'une adresse de courrier électronique ne puisse servir à authentifier qu'un seul compte. En effet, dans le cas où une telle adresse est partagée par plusieurs comptes, seul le premier créé sera reconnu.

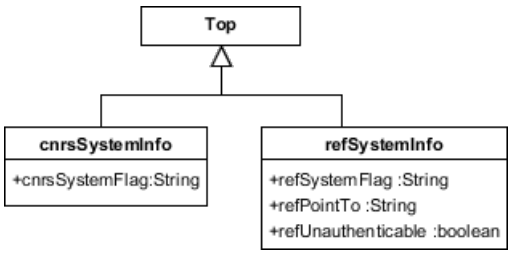


Figure 88 - Diagramme de classe de définition des informations techniques

Par ailleurs, la solution OpenIAM Identity Management permet également de prendre en compte l'organisation d'affection de l'utilisateur. Celle-ci est décrite par la classe

« OrganizationUnit » définie dans la RFC 2798. Dans l'annuaire « Central », cette classe est étendue par la classe « cnrsOrganizationalUnit ». Dans l'annuaire « Référentiel », il n'existe pas de classe dédiée à la description des unités. Ces informations sont renseignées dans chaque compte utilisateur.

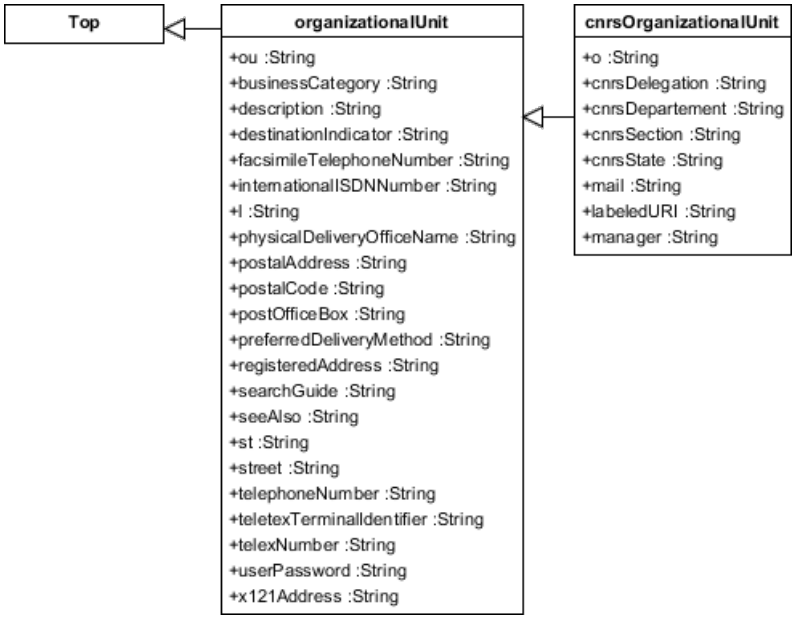


Figure 89 - Diagramme de classe de définition des organisations

Bien que disponibles dans Labintel et faisant partie des caractéristiques d'une identité, la synchronisation active de la classe « OrganizationalUnit » ne fait pas partie du périmètre de cette itération. A l'instar de l'annuaire « Référentiel », certaines informations relatives à l'unité pourront être chargées dans des attributs spécifiques.

Tous les attributs de la classe « InetOrgPerson » n'ayant pas d'équivalent dans Labintel, seul un nombre restreint sera implémenté dans le cadre de la présente étude. Les attributs retenus sont ceux obligatoires de la classe « Person » :

- « sn » pour le nom de famille,
- « cn » pour le nom complet.

Les attributs retenus de la classe « OrganizationalPerson » sont :

- « title » pour la fonction exercée,
- « street » pour la rue,
- « postalcode » pour le code postal,
- « l », pour la localité,
- « ou » pour le nom de l'unité.

Les attributs retenus de la classe « InetOrgPerson » sont :

- « employeeNumber » pour le numéro d'employé,

- « employeeType » pour le type d'emploi,
- « givenName » pour le prénom,
- « mail » pour l'adresse de courrier électronique,
- « o » pour le nom de l'organisation.

Les attributs propres au CNRS présents dans les deux types d'annuaires retenus sont :

- « regionalOffice » qui correspond à la délégation régionale de rattachement,
- « scientificOffice » qui correspond à l'institut d'appartenance de l'unité.

Dans Labintel, les données nécessaires sont stockées dans les tables « uni » (unités), « imp_uni » (implantations), « ttl_uni » (tutlles), « typ_per » (types de personnel), « ntu_per » (natures de personnel), « typ_ntu_per » (types de nature de personnel), « per » (personnels), « dr » (délégations régionales) et « ds » (départements scientifiques) ainsi que dans la vue vue_eta (établissements) mise à disposition par l'application « Référentiel des partenaires ».

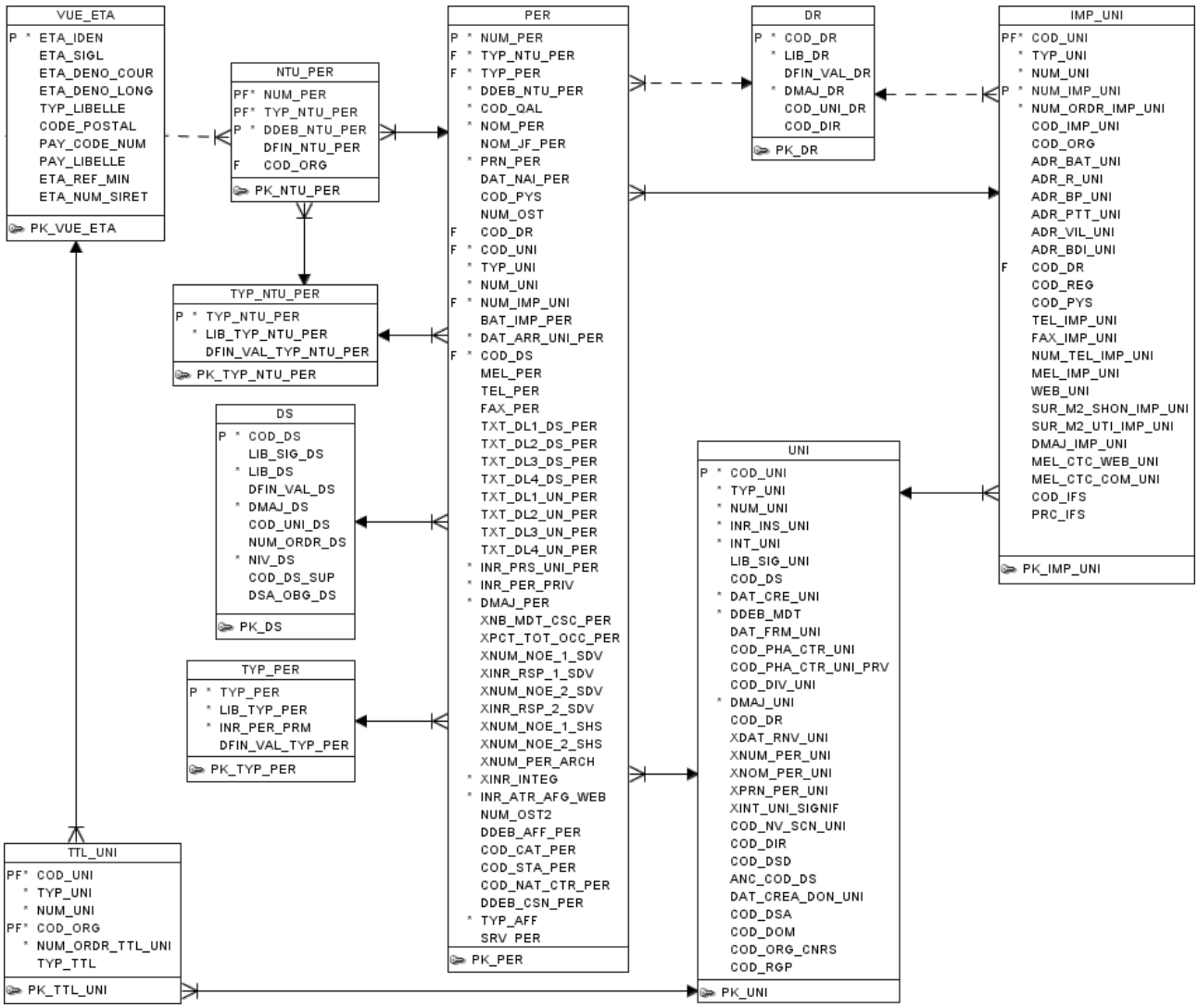


Figure 90 - Modèle de physique de données de Labintel pour les identités

V.6.3 Environnement de développement

Comme évoqué lors de l'itération précédente, OpenIAM utilise plusieurs projets de la communauté Springsource, dont Spring MVC et le langage Groovy. De ce fait, l'outil de développement privilégié est Spring Tool Suite qui est basé sur Eclipse.

Les binaires livrés par OpenIAM intégrant le conteneur de servlet Tomcat et déployés dans la machine virtuelle sont complétés par un environnement dédié au développement qui comprend les classes sources Java extraites depuis le site GIT. Spring Tool Suite permet de télécharger l'ensemble des fichiers nécessaires grâce à l'outil d'automatisation Maven.

V.6.4 Extension du modèle de données

Comme évoqué précédemment, les classes « cnrsPerson » et « refUser » étendent la classe « InetOrgPerson ». Cependant, l'application OpenIAM ne permet pas de mettre en œuvre la notion d'héritage. De ce fait, comme il est impossible de réaliser des classes enfant, il faut développer

chaque classe individuellement en reprenant pour chacune l'ensemble des attributs communs. Cela implique également qu'une modification du modèle de la classe parente « InetOrgPerson » ne sera pas répercutée dans les classes spécifiques au CNRS. Dans le cadre de la présente étude, cette difficulté peut être contournée en ajoutant des attributs au schéma initial sans formalisme spécifique à une des classes CNRS. La définition d'attributs supplémentaires ne pouvant pas être réalisée au travers de la console d'administration, ces informations sont saisies directement dans la table « metadata_element » de la base de données du référentiel OpenIAM. Le nom de l'attribut étant affiché directement dans la console d'administration, la lisibilité peut s'en trouver diminuer. Il faut donc veiller à utiliser un nom d'attribut métier et non purement technique pour faciliter l'utilisation de la console pour les utilisateurs. De plus, le contenu de ces attributs peut poser un problème d'exhaustivité des informations. En effet, par exemple, dans le cas de l'attribut concernant la délégation régionale de rattachement, il serait souhaitable de disposer de son code qui est employé couramment au sein du CNRS et de son nom complet. Hors, si l'information peut être présentée sous le format « *code* (*nom complet*) » qui est facilement compréhensible, cela peut poser des difficultés ultérieurement lorsque ces données seront traitées pour être chargées dans des annuaires LDAP par exemple. En effet, l'information doit être analysée puis déstructurée pour la reconstruire sous un autre format. De ce fait, il est préférable de pouvoir disposer d'un attribut dédié à l'affichage dans la console d'administration et dans l'application self-service puis de deux attributs techniques liés au code et au nom complet de l'unité qui présentent les données telles qu'elles sont stockées dans Labintel.

Par ailleurs, l'absence de notion d'héritage peut être source de difficultés pour définir un autre type d'identité qui pourrait partager des attributs communs avec les classes du CNRS. Ce cas peut notamment se présenter pour les prestataires ou des personnes extérieures aux partenariats établis par le CNRS pour lesquels il n'est pas utile de disposer de tous les attributs, tels que l'organisme de rattachement, mais qui pourraient nécessiter d'autres attributs tels que le moyen de contacter la personne dans l'unité et au sein de son organisation d'origine.

V.6.5 Initialisation du référentiel

Comme évoqué dans le paragraphe « Gestion des identités », le cycle de vie d'une identité inclue la création, la mise à jour et la suppression des informations qui lui sont liées. La phase de création peut être réalisée par différents moyens dans l'outil OpenIAM Identity Management. La synchronisation active permet de mettre en place un système de surveillance d'un système source pour mettre à jour le référentiel et les systèmes cibles à intervalle régulier. La console d'administration permet à un administrateur de saisir des informations sur un nouvel utilisateur. Ce dernier peut également demander sa création dans le référentiel par l'application de self-service.

Ces deux modes de saisies génèrent le déclanchement d'un processus métier de validation de la demande de création. En outre il est également possible de développer une nouvelle interface de création d'utilisateur.

Le périmètre de cette itération étant la population présente dans Labintel, il est préférable de mettre en place un système de lecture de la base de données par synchronisation active. Le service de synchronisation fait alors appel à un script groovy dédié qui transformera les données issues de Labintel pour les charger en tant qu'utilisateur dans le référentiel. Pour cela, une vue est créée spécifiquement dans la base de données de Labintel pour renvoyer l'ensemble des informations nécessaires.

```
CREATE OR REPLACE VIEW VUE_AFFECTATION AS
SELECT PER.PRN_PER, PER.NOM_PER, PER.NUM_PER, PER.COD_UNI, PER.TYP_PER, PER.MEL_PER,
       DR.COD_DR, DR.LIB_DR, DS.COD_DS, DS.LIB_DS,
       VUE_ETA.ETA_DENO_LONG, VUE_ETA.ETA_SIGL, VUE_ETA.ETA_IDEN,
       TYP_PER.LIB_TYP_PER, TYP_NTU_PER.LIB_TYP_NTU_PER,
       UNI.INT_UNI, IMP_UNI.ADR_R_UNI, IMP_UNI.ADR_PTT_UNI,
       NVL(ADR_BDI_UNI,ADR_VIL_UNI) AS ADR_VIL_UNI,
       PER.INR_PRS_UNI_PER
FROM UNI, IMP_UNI, TYP_PER, NTU_PER, TYP_NTU_PER, VUE_ETA, PER, DR, DS
WHERE PER.COD_UNI=UNI.COD_UNI
  AND PER.COD_UNI=IMP_UNI.COD_UNI
  AND PER.NUM_IMP_UNI=IMP_UNI.NUM_IMP_UNI
  AND PER.TYP_PER=TYP_PER.TYP_PER
  AND PER.TYP_NTU_PER=NTU_PER.TYP_NTU_PER
  AND NTU_PER.TYP_NTU_PER=TYP_NTU_PER.TYP_NTU_PER
  AND PER.NUM_PER=NTU_PER.NUM_PER
  AND NVL(NTU_PER.COD_ORG,130)=VUE_ETA.ETA_IDEN
  AND PER.COD_DR=DR.COD_DR
  AND UNI.COD_DS=DS.COD_DS
```

Figure 91 - Vue d'extraction des affectations « VUE_AFFECTATION »

La classe groovy de validation « ValidateSrcLabRecord » développée spécifiquement permet de s'assurer que les informations issues de Labintel peuvent être lues correctement. Pour cela, dans un premier temps, chaque colonne est testée pour vérifier qu'elle contient une valeur. Après la phase de test d'initialisation où le nombre de lignes renvoyées par la requête est limité, il sera possible d'alléger ce test afin de diminuer les temps de validation et améliorer le temps total de chargement. Enfin, la classe groovy de transformation « TransformSrcLabRecord » développée spécifiquement traite chaque ligne extraite individuellement réalisant la transformation d'une colonne vers un attribut de la classe « User » pour chaque ligne parcourue comme dans l'extrait suivant :

```
Attribute attrVal = null;
Map<String,Attribute> columnMap =  rowObj.getColumnMap();
// nom->sn
attrVal = columnMap.get("NOM_PER");
if (!isNull(attrVal)) {
	pUser.setLastName(attrVal.getValue().toUpperCase());
}
// fonction->title
attrVal = columnMap.get("LIB_TYP_NTU_PER");
if (!isNull(attrVal)) {
	pUser.setTitle(attrVal.getValue());
}
```

Figure 92 - Classe TransformSrcLabRecord.groovy : extrait de la méthode de transformation

Un traitement particulier concerne l'adresse de courrier électronique. En effet, comme évoqué précédemment, cette information est utilisée en tant qu'identifiant dans le système d'information du CNRS. Dans OpenIAM, l'identifiant est défini pour un périmètre applicatif, qui correspond dans la terminologie OpenIAM à une identité. La notion d'utilisateur correspondant alors à une personne. Une identité doit être créée par exemple pour permettre à un utilisateur d'accéder aux fonctionnalités de l'application self-service qui nécessite une authentification. La classe groovy de transformation est donc adaptée afin de prendre en compte cette caractéristique. Pour cela, il faut définir l'identifiant du compte pour le domaine de sécurité de l'application de self-service. Ce dernier est celui qui est affecté par défaut grâce au code suivant :

```
// mail
attrVal = columnMap.get("MEL_PER");
if (!isNull(attrVal)) {
	def emailStr = attrVal.getValue();
	List<Login> newPrincipalList = new ArrayList<Login>();
	Login lg = new Login();
	lg.id = new LoginId("USR_SEC_DOMAIN", emailStr, "0");
	newPrincipalList.add(lg);
	setPrincipalList(newPrincipalList);
}
```

Figure 93 - Classe TransformSrcLabRecord.groovy : traitement relatif aux identifiants

Afin de faciliter la lisibilité des informations dans l'application Web d'administration, les données de type « employeetype » extraites de la table « TYP_PER » de Labintel sont chargées dans la table « STATUS » de la base de données du référentiel OpenIAM. Bien qu'il n'y ait pas de synchronisation active envisagée dans le cadre de l'étude, les données extraites de la vue « VUE_ETA » de Labintel relatives aux établissements de recherche sont chargées en tant qu'organisation dans la table « COMPANY » du référentiel d'OpenIAM afin d'offrir une meilleure lisibilité des informations dans l'application. De même, pour faciliter la lecture du nom de l'unité d'affectation, les données relatives aux attributs « deptName » et « deptCd » extraites de la table « UNI » de Labintel sont chargées en tant que département dans la table « COMPANY ». La prise

en compte de ce type d'information dans OpenIAM montre de possibles difficultés pour une itération ultérieure pour la gestion des unités. En effet, OpenIAM prévoit une notion de dépendance entre le département et l'organisation. Hors, une unité peut avoir plusieurs tutelles, ce qui correspond dans le modèle proposé par OpenIAM à un département qui appartiendrait à plusieurs organisations, ce qui n'est pas possible au travers de l'outil OpenIAM. Comme la gestion des établissements et des unités n'est pas comprise dans le périmètre de cette étude, aucune solution n'est étudiée dans la présente itération. Le contournement mis en place consiste à définir comme organisme parent la première tutelle de l'unité.

Dans un premier temps, pour le chargement initial, seules les affectations en cours sont extraites de Labintel, ce qui représente plus de cent vingt cinq mille comptes utilisateurs. La reprise de l'historique complet ne sera envisageable que dans un environnement de production performant, car cela représente trois cent quatre-vingt quinze mille comptes supplémentaires inactifs. La vue est donc adaptée en conséquence pour ne lister que les affectations où la personne est actuellement en activité.

V.6.6 Mise à jour des données

L'écran de définition de la synchronisation permet de configurer le script de transformation pour qu'il s'exécute en mode incrémental. Dans ce cas, les comptes sont mis à jour uniquement s'ils ont été modifiés dans l'application source. Pour cela, la requête SQL de la vue d'extraction des comptes doit contenir une colonne contenant l'information de dernière modification. Cette information est disponible dans la colonne « DMAJ_PER » de la table « PER ». Les comptes sont alors mis à jour si la valeur de la colonne « DMAJ_PER » est supérieure à la date de la dernière synchronisation. La colonne « NUM_PER », qui stocke l'identifiant technique unique de chaque affectation, est utilisée pour réaliser la comparaison entre les comptes déjà créés dans le référentiel OpenIAM et les affectations présentes dans Labintel.

A l'instar des annuaires « Central » et « Référentiel », les utilisateurs sont activés dans le référentiel OpenIAM si et seulement si la personne est décrite comme présente en unité (valeur de la colonne « INR_PRS_UNI_PER » de la table « PER » de Labintel est égale à « 1 »). Une entrée est automatiquement désactivée si elle ne remplit plus cette condition ou si l'enregistrement est supprimé de Labintel.

```
// presence en unite->activation du compte
attrVal = columnMap.get("INR_PRS_UNI_PER");
if (!isNull(attrVal)) {
	if (attrVal.getValue().equals("1")) {
		pUser.setStatus(UserStatusEnum.ACTIVE);
	}else {
		pUser.setStatus(UserStatusEnum.INACTIVE);
	}
}
```

Figure 94 - Classe TransformSrcLabRecord.groovy : traitement de la présence en unité

Comme évoqué précédemment, l'adresse de courrier électronique doit être utilisée en tant qu'identifiant dans les applications OpenIAM. De ce fait, la mise à jour de celle-ci doit être répercutée dans l'ensemble des domaines de sécurité en plus des adresses de contact. Pour cela, la liste des identités doit être reconstruite avec la nouvelle valeur de courriel.

```
attrVal = columnMap.get("MEL_PER");
if (!isNull(attrVal)) {
	def emailStr = attrVal.getValue();
	// modifie chaque login
	List<Login> currentEmlList = getPrincipalList();
	if (currentEmlList != null && currentEmlList.size()>0) {
		List<Login> newPrincipalList = new ArrayList<Login>();
		for (Login lg :currentEmlList) {
			def id=lg.getId();
			Login newLogin = new Login();
			newLogin.id = new LoginId(id.getDomainId(),
						emailStr,
						id.getManagedSysId());
			newPrincipalList.add(newLogin);
		}
		setPrincipalList(newPrincipalList);
	}
}
```

Figure 95 - Classe TransformSrcLabRecord.groovy : mise à jour des identifiants

Par ailleurs, nativement, la synchronisation peut être exécutée automatiquement quotidiennement, toutes les heures, tous les quarts d'heure, toutes les cinq minutes ou toutes les minutes. Actuellement, l'outil DMAS est capable de propager les mises à jour de Labintel vers les annuaires en moins de cinq secondes après la validation par la personne gestionnaire de l'unité. Cela peut donc constituer une régression par rapport à l'existant pour l'utilisateur final. Une itération ultérieure pourrait prendre en charge ce problème. En effet, il est possible de modifier le code source de l'application qui exécute le bus pour ajouter un intervalle inférieur à la minute.

Une synchronisation complète peut être envisagée afin de s'assurer que les informations sont à jour et que les seules les personnes en activité ont un compte actif. La synchronisation définie lors de la tâche précédente doit donc être conservée et paramétrée pour s'exécuter quotidiennement en mode complet. Parallèlement, une seconde tâche équivalente doit être créée où le mode de synchronisation sera positionné comme incrémental et l'intervalle le plus faible possible.

V.6.7 Rétrospective de l'itération

Le référentiel OpenIAM étant alimenté et sa mise à jour étant développée, l'objectif de l'itération est pleinement rempli. Cependant, cette phase de développement a permis d'entrevoir des limites à l'outil.

En effet, pour valider la synchronisation, la population de test initiale a été limitée dans un premier temps à une unique affectation pour ensuite être ouverte à la population de la DSI du CNRS (unité « MOY1678 ») qui compte cent vingt quatre personnes en activité. Enfin le périmètre a été plus largement ouvert. Même avec un faible volume de comptes, des ralentissements se font sentir. Cette situation est due au modèle de données des organisations dans OpenIAM. En effet, les organismes et les départements sont stockés dans la même table « COMPANY » du référentiel, la colonne « PARENT_ID » étant alors renseignée uniquement pour les départements et divisions avec l'identifiant de l'organisme d'appartenance. L'analyse des requêtes lentes montre alors qu'aucun index n'est utilisé. Cependant, la création d'index n'a pas permis d'améliorer les temps de réponse. En effet, la recherche de compte passe par une requête de recherche des organisations, ce qui correspond aux lignes de la table « COMPANY » pour lesquelles la colonne « PARENT_ID » est vide. Hors ce dernier critère ne permet pas d'utiliser un index même s'il existe car les valeurs vides ne peuvent pas être indexées. De ce fait, des lenteurs se produisent sur tous les écrans qui doivent afficher au moins le nom d'une organisation, tels que la recherche de comptes où une liste déroulante d'établissements est affichée. OpenIAM n'est donc pas prévu pour gérer plus de dix neuf milles organismes et presque six mille unités. Ce problème a été remonté aux développeurs. Une solution sera proposée dans les versions à venir.

Par ailleurs, le planificateur de tâche interne à l'outil OpenIAM, basé sur Quartz, offre la possibilité de fixer la fréquence parmi un choix de cinq valeurs allant de la minute à vingt-quatre heures. Hors, l'outil DMAS actuellement employé par la DSI du CNRS est capable de propager une identité depuis l'application Labintel vers un référentiel en moins de cinq secondes. De ce fait, l'utilisation de l'outil OpenIAM fait perdre à l'utilisateur la vision de propagation immédiate des mises à jour d'identité. Pour cela, il serait possible de diminuer l'intervalle en modifiant le code source de l'application. Une autre solution qui propagerait l'information en temps réel consisterai à modifier Labintel pour qu'il envoie un message sur le bus OpenIAM déclenchant ainsi immédiatement le traitement de synchronisation lors des validations d'opérations dans Labintel. Ceci pourra faire l'objet d'une itération.

Bien que cela ne fasse pas partie du périmètre de l'étude, il n'est pas possible de synchroniser OpenIAM avec la base de données du référentiel des partenaires. Pour cela il faut obligatoirement réaliser l'extraction d'information depuis un fichier texte au format CSV.

V.7 Itération 4 – Gestion des rôles

V.7.1 Sprint backlog

L'itération a pour but de développer les différents aspects relatifs aux rôles, depuis la création jusqu'à la gestion de son cycle de vie. Le périmètre de l'étude est restreint aux rôles évoqués lors du recueil des besoins pour les applications CORE et Simbad. En outre, le profil de directeur d'unité tient une place importance dans le système d'information du CNRS. Entre autres, dans Simbad il est un gestionnaire par défaut, de même que dans Labintel. Le sprint doit donc permettre de mettre en place l'automatisation de la gestion du rôle de directeur d'unité (DU).

Ces deux types de rôles, l'un dont la gestion est manuelle et l'autre dont la gestion est automatisée par des processus métiers, impliquent des tâches distinctes ayant des user stories différentes. Ainsi, pour la gestion des rôles applicatifs pour Simbad et CORE les user stories sont « En tant qu'utilisateur, je veux demander l'accès à une application » qui peut se traduire par « En tant qu'utilisateur, je veux demander qu'on me donne un rôle », « En tant qu'utilisateur responsable d'une application, je veux valider l'octroi des rôles sous ma responsabilité », « En tant qu'utilisateur, je veux voir la liste des rôles qui me sont attribués ». Pour le profil DU, les user stories sont « En tant qu'administrateur, je veux automatiser l'attribution du rôle DU » et « En tant qu'administrateur, je veux révoquer le rôle DU ».

V.7.2 Rôles applicatifs CORE et Simbad

Comme évoqué précédemment, les rôles applicatifs CORE sont affectés aux personnes en délégation pour leur permettre de valider les demandes de création d'espace CORE et/ou d'administrer un espace CORE. Il est donc nécessaire de prévoir deux types de rôles (validation et administration) associés à un périmètre (la délégation régionale). Bien qu'il soit possible de définir des attributs aux rôles, il n'est pas possible d'instancier un rôle avec différentes valeurs d'attributs. De plus, une personne peut avoir à intervenir, en création ou modification, sur un site dont l'unité n'appartient pas à la délégation. Il n'est donc pas possible de déduire le périmètre d'après la délégation régionale d'affectation de la personne déductible de l'attribut « Regional Office ». De ce fait, il est nécessaire de déclarer autant de rôles distincts que de délégations régionales. Par conséquent pour CORE, il est nécessaire de créer dix-neuf rôles de validation et autant d'administration.

Pour Simbad, les rôles identifiés comme devant être gérés en dehors de l'application sont le gestionnaire de profil et le valideur. Ces activités devant être assurées par une personne de l'unité, le périmètre associé aux rôles correspondants est donc réduit à l'unité d'affectation du compte. De

ce fait, il n'est pas nécessaire de créer autant de rôles que d'unités. Par ailleurs, le profil DU est également utilisé par Simbad, mais sa gestion fait l'objet d'une tâche dédiée.

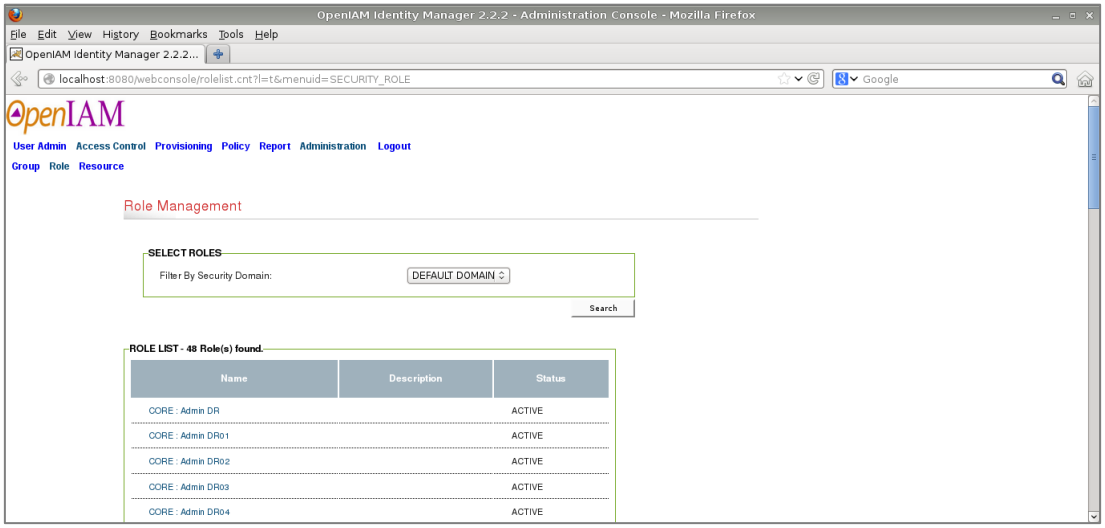


Figure 96 - Ecran de gestion des rôles dans OpenIAM

Concernant la gestion du cycle de vie de ces différents rôles, l'outil OpenIAM en version communautaire 2.2 ne permet de mettre en place des processus de gestion des demandes utilisateurs liées aux rôles. En effet, le développement de tels flux métiers n'est possible qu'avec la version payante. De ce fait, il n'est pas possible dans le cadre de la présente étude de réaliser une solution répondant aux user stories « En tant qu'utilisateur, je veux demander qu'on me donne un rôle », « En tant qu'utilisateur responsable d'une application, je veux valider l'octroi des rôles sous ma responsabilité ».

V.7.3 Profil « DU »

Comme évoqué précédemment, le profil DU est une information issue des référentiels du système d'information du CNRS. En effet, la gestion d'une unité est confiée à une personne pour un mandat renouvelable une fois. Dans le système d'information du CNRS, le processus de nomination d'un directeur d'unité repose sur deux prérequis. Le premier impose que l'unité soit positionnée comme active dans le référentiel des structures de Labintel. Le second prérequis exige que la fiche agent de l'affectation de la personne dans l'unité soit déjà saisie dans Labintel avec une adresse de courrier électronique dédiée, puisqu'elle sert d'identifiant. Lorsque ces besoins sont satisfaits, le processus de nomination peut se dérouler peut se dérouler jusqu'au positionnement des attributs « CnrsRole » à « DU – *code unité* » et « RefRole » à « du=*code unité* » respectivement dans les annuaires « Central » et « Référentiel ».

Lors de la nomination d'un directeur, une fiche agent a donc été préalablement créée dans Labintel. De ce fait, le compte utilisateur sous-jacent est connu du référentiel OpenIAM par la tâche

de synchronisation développée dans l'itération précédente. Ensuite la fiche agent est modifiée pour prendre en compte le changement de poste. Il est donc possible de détecter la création d'un nouveau mandat de responsable en corroborant les informations avec la fiche agent du nouveau responsable.

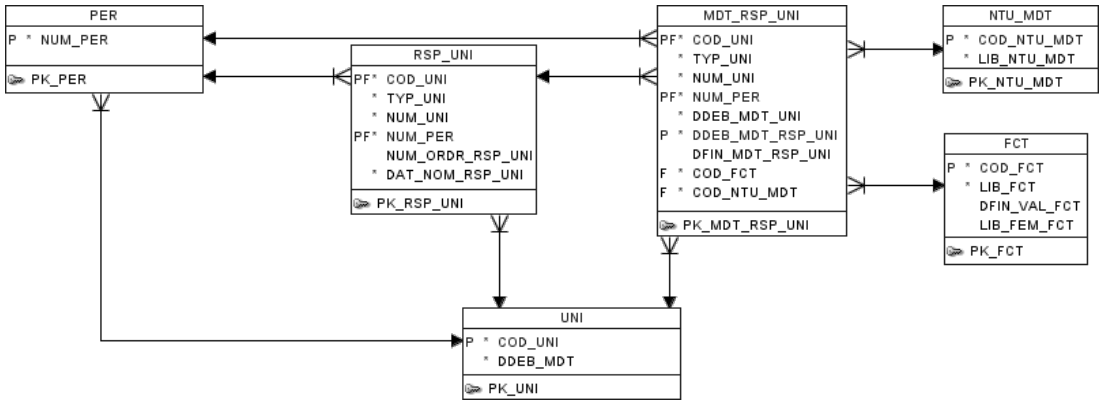


Figure 97 - Modèle de physique de données de Labintel pour les mandats de responsable

Il est donc possible d'utiliser une vue spécifique aux mandats pour permettre de lister les directeurs d'unité et donc de déterminer les comptes qui doivent recevoir le rôle DU. La vue « V_DIR » qui existe dans la base de données de Labintel permet de lister les responsables, mais elle ne dispose pas de la colonne « DMAJ_PER » permettant de détecter les mises à jour. Il est donc nécessaire de développer une vue dédiée à la gestion du rôle DU. Sachant que les informations relatives aux comptes sont prises en charge par le script de synchronisation développé lors de l'itération précédente. La seule donnée nécessaire de la table « PER » est « NUM_PER » pour permettre la réconciliation entre les comptes existants dans les référentiels et les comptes liés aux mandats. La seconde information nécessaire est le code de l'unité exploitable depuis la colonne « COD_UNI ».

```
CREATE OR REPLACE VIEW VUE_DU AS
SELECT PER.NUM_PER, MDT_RSP_UNI.COD_UNI, RSP_UNI.NUM_ORDR_RSP_UNI, PER.DMAJ_PER
FROM PER, RSP_UNI, MDT_RSP_UNI
WHERE PER.NUM_PER = RSP_UNI.NUM_PER
AND MDT_RSP_UNI.NUM_PER = RSP_UNI.NUM_PER
AND MDT_RSP_UNI.COD_UNI = RSP_UNI.COD_UNI
AND MDT_RSP_UNI.COD_FCT = 'D'
AND TRUNC(SYSDATE) BETWEEN MDT_RSP_UNI.DDEB_MDT_RSP_UNI AND
NVL(MDT_RSP_UNI.DFIN_MDT_RSP_UNI,TRUNC(SYSDATE)+1);
```

Figure 98 - Vue d'extraction des mandats de responsable d'unité « VUE_DU »

Dans le script d'affectation du rôle DU, il n'est pas nécessaire de vérifier que le compte utilisateur est déjà connu puisque c'est un prérequis du processus métier pour la saisie du mandat. Cependant, il est préférable de s'assurer qu'il existe déjà dans le référentiel. Dans le cas contraire, cela implique que l'affectation du nouveau directeur n'est pas encore prise en compte. D'où la

nécessité de synchroniser régulièrement l'ensemble des comptes pour contourner d'éventuelles défaillances.

La mise à jour du compte utilisateur génère une difficulté de synchronisation. En effet, les scripts de synchronisation des comptes utilisateurs et d'attribution du rôle DU peuvent entrer en conflit s'ils sont en mode incrémental. Le premier des deux qui prend en compte la modification de Labintel, positionne dans le référentiel OpenIAM la date de mise à jour du compte. De ce fait, pour l'autre script, le compte a déjà été mis à jour, ce qui empêche le déroulement de ce script pour ce compte. Une solution peut consister à fusionner les deux vues, pour lister l'ensemble des informations nécessaires en une seule fois.

```
CREATE OR REPLACE VIEW VUE_IDENTITE AS
SELECT VUE_AFFECTATION.*, VUE_DU.NUM_PER AS NUM_RSP, VUE_DU.NUM_ORDR_RSP_UNI,
GREATEST(VUE_AFFECTATION.DMAJ_PER,VUE_DU.DMAJ_PER) AS DMAJ_IDENTITE
FROM VUE_AFFECTATION,VUE_DU
WHERE VUE_AFFECTATION.COD_UNI=VUE_DU.COD_UNI
```

Figure 99 - Vue d'extraction des identités « VUE_IDENTITE »

Par ailleurs, dans OpenIAM, il est possible d'indiquer pour chaque compte qui est le manager. Il est donc envisageable de définir cette information pour chaque compte affecté à l'unité qui a un nouveau directeur, sauf, évidemment, pour le directeur lui-même. Dans ce cas, pour forcer la mise à jour du compte avec cette information, la date de mise à jour peut être positionnée à la plus récente entre celle du compte et celle de l'affectation du nouveau directeur. Pour déterminer si le compte en cours de traitement est celui du directeur, il suffit de comparer les valeurs de « NUM_PER » du compte et du directeur. Si c'est la même valeur, alors le compte est celui du directeur qui doit alors recevoir le rôle DU. Dans le cas contraire, l'information relative au responsable peut être positionnée pour le compte.

```
// num_rsp->manager ou role
attrVal = columnMap.get("NUM_RSP");
if (!isNull(attrVal)) {
	if (attrVal.getValue().equals(pUser.getEmployeeId())) {
		// compte DU
		// ajout de rôle DU si présent en unité
		if (pUser.status == UserStatusEnum.ACTIVE) {
			List<Role> roleList = pUser.getMemberOfRoles();
			if (roleList == null) {
				roleList = new ArrayList<Role>();
			}
			RoleId id = new RoleId("USR_SEC_DOMAIN", "DU");
			Role r = new Role();
			r.setId(id);
			if (!isInRole(userRoleList,  id)) {
				roleList.add(r);
			pUser.setMemberOfRoles(roleList);
		}
	} else {
		pUser.setManagerId(attrVal.getValue());
```

```
        }
}
```

Figure 100 - Classe TransformSrcLabRecord.groovy : attribution du rôle DU

Comme évoqué précédemment, le directeur d'unité a la possibilité d'intervenir dans l'attribution de rôles. Aussi, dans OpenIAM, une identité peut être ajoutée au compte pour que le responsable puisse accéder à la console d'administration et ainsi pouvoir gérer les rôles du personnel de son unité.

Par ailleurs, en fin de mandat, le rôle DU doit être retiré automatiquement du compte. En effet, il est préférable de retirer l'information de responsable d'unité quand l'affectation prend fin, même si le compte est désactivé. Dans ce cas, il est possible de mettre en place une classe groovy dédiée qui parcours régulièrement l'ensemble des mandats et vérifie que le rôle est bien retiré de la liste des attributions. Pour cela, le script peut s'appuyer sur la table « MDT_RSP_UNI » déjà utilisée dans la vue « VUE_DU ». Afin de s'assurer qu'un compte ne soit pas pris en compte par ce traitement avant celui de la classe groovy « TransformSrcLabRecord », il faut déterminer un enchainement où celui-ci est exécuté en mode complet avant la nouvelle classe groovy « TransformSrcDURecord ».

V.7.4 Rétrospective de l'itération

En version 2.2 communautaire, il n'est pas possible de développer des flux liés à la gestion du cycle de vie qui puissent être réalisables au travers de l'application self-service. Cependant, la version communautaire 2.3 devrait intégrer cette fonctionnalité, ce qui démontre que le besoin est clairement identifié par l'équipe de développement et qu'il est jugé important.

Pour les rôles qui sont associés à un périmètre tel que l'unité ou la délégation régionale, la liste d'affichage dans l'outil pour l'attribution peut être longue. Cela peut donc être une source d'erreur, car il devient facile de se tromper de case à cocher dans la liste. Dans ce cas, une itération peut être envisagée pour modifier l'affichage des rôles disponibles. Il serait envisageable de faire le choix du rôle à attribuer ou à demander en deux étapes. La première consisterait à choisir le rôle et la seconde à rechercher son périmètre (délégation régionale, unité, …).

Par ailleurs, la création et la manipulation des rôles a permis de mettre en avant des limites concernant les notions de hiérarchie et d'héritage. Ces deux types de lien entre rôles existent dans le modèle OpenIAM. En effet, les informations relatives peuvent être saisies dans l'application et elles sont alors stockées dans la base de données. Mais elles ne sont pas encore exploitées. Ces fonctionnalités sont envisagées dans une version 3.

V.8 Itération 5 – Approvisionnement des ressources cibles

V.8.1 Sprint backlog

L'objectif de l'itération est de pouvoir simuler l'alimentation de l'annuaire « Référentiel » et de la base de comptes de l'application Simbad. Les user stories sous-jacentes sont « En tant qu'administrateur, je veux provisionner et mettre à jour les comptes dans un annuaire LDAP au format « Référentiel » » et « En tant qu'administrateur, je veux provisionner et mettre à jour les comptes dans les tables d'une base de données Oracle ».

V.8.2 Modèle d'approvisionnement

OpenIAM permet de gérer les accès par RBAC. En effet, dans l'outil OpenIAM, la notion de rôle est le moyen qui permet de déterminer quelles sont les ressources auxquelles un compte utilisateur peut accéder. Ainsi pour chaque rôle, il est possible de définir quelles sont les ressources qui sont impactées lors de l'attribution ou du retrait à un compte utilisateur. L'attribution d'un rôle à un compte utilisateur déclenche dans OpenIAM un processus d'approvisionnement. Celui-ci enregistre alors le compte dans les ressources (bases de données locales de comptes ou annuaires par exemple) qui sont liées au rôle.

Parallèlement, pour chaque ressource, il est nécessaire de définir une politique de correspondances d'attributs. Ainsi pour chaque attribut défini dans la ressource cible, il est possible de développer des classes groovy de règles de transformation des informations présentes dans le référentiel OpenIAM.

OpenIAM propose également un processus de réconciliation. Celui-ci permet de mettre à jour le référentiel OpenIAM lorsque des modifications sont réalisées dans la ressource. Ainsi, si un utilisateur est créé dans l'application, ce nouveau compte est remonté dans OpenIAM. Cependant, afin de garder le contrôle sur la création des comptes utilisateurs, il est préférable d'avoir un unique canal de création de compte.

V.8.2.1 Alimentation d'une base de données

Comme évoqué précédemment, dans les applications du système d'information du CNRS, l'identifiant utilisé est l'adresse électronique. La base de données créée pour simuler l'application Simbad prend en compte cette spécificité. La table des utilisateurs posséde une colonne « LOGIN » qui doit être renseignée avec les adresses de courrier électroniques des utilisateurs.

Cette phase de simulation a permis de soulever plusieurs problèmes. En effet, la plus grande difficulté a été remontée lors de l'étape de cartographie de la gestion des identités au CNRS : lorsque la personne change d'adresse de courrier électronique, elle perd tous ses accès, car les applications ne sont pas conçues pour gérer le changement d'identifiant. Ce problème est également présent dans OpenIAM. En effet, l'outil se base sur l'identifiant applicatif pour mettre à jour les comptes dans les ressources impactées. Hors, comme l'écran suivant le montre, OpenIAM s'appuie sur un attribut « principal » pour établir la liaison entre un compte OpenIAM et un compte applicatif.

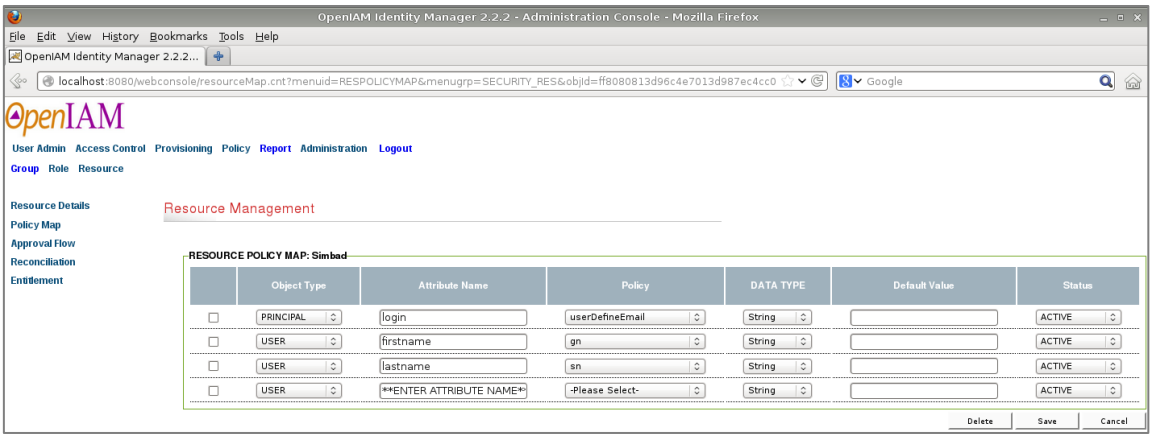


Figure 101 - Ecran de gestion de la politique de correspondance d'informations dans OpenIAM

Hors, suite à un changement de valeur de l'identifiant, OpenIAM n'est plus en mesure d'établir la liaison entre le compte dans le référentiel et le compte applicatif dans la ressource. Pour pouvoir palier à ce problème, il est nécessaire d'ajouter une information supplémentaire dans les tables d'utilisateurs des applications. Dans ce cas, il est alors possible d'utiliser l'attribut « userid » du référentiel OpenIAM comme clé de référence. En effet, OpenIAM affecte un identifiant technique unique lors de la création d'un compte. En l'utilisant également dans les tables de comptes des ressources, OpenIAM est alors capable de mettre à jour l'identifiant de connexion applicatif.

Une seconde difficulté est due au manque de souplesse du modèle RBAC. En effet, pour certains comptes, l'adresse électronique n'est pas renseignée dans Labintel. Ce cas perturbe le modèle d'approvisionnement, car cette information sert d'identifiant. Hors, pour résoudre le problème, il suffirait de pouvoir ajouter une contrainte. Dans ce cas, un compte ne peut être habilité et reconnue par une ressource que s'il appartient à un rôle déterminé et si son compte rempli toutes les conditions, dont la présence d'une adresse électronique, ce qui se rapproche du modèle CRBAC. Dans le cadre de l'application Simbad, cela se traduit par le fait que le rôle DU ne doit alors pas être la condition pour qu'un compte soit enregistré dans l'application. En effet, le rôle de gestionnaire de profil est affecté par défaut aux directeurs d'unité, mais il peut être délégué à d'autres personnes de l'unité. Dans ce cas, par défaut, le rôle « Gestionnaire de profil Simbad » est attribué aux

responsables d'unité qui ont une adresse électronique valide. De plus, le rôle DU ne doit plus être associé à une ressource. De ce fait, chaque nouvelle application dont l'accès pourrait être basé sur le rôle DU, doit disposer d'un rôle propre correspondant, ce qui implique une modification de la classe de synchronisation.

```
if (pUser.status == UserStatusEnum.ACTIVE) {
	List<Role> roleList = pUser.getMemberOfRoles();
	if (roleList == null) {
		roleList = new ArrayList<Role>();
	}
	if (pUser.getEmail()!=null) {
		roleID = new RoleId("USR_SEC_DOMAIN", "GestionnaireProfilSimbad");
		role = new Role();
		role.setId(roleID);
			if (!isInRole(userRoleList,  roleID)) {
				roleList.add(role);
			}
			pUser.setMemberOfRoles(roleList);
	}
}
```

Figure 102 - Classe TransformSrcLabRecord.groovy : attribution du rôle « Gestionnaire de profil Simbad »

Ce cas particulier correspond à la définition des notions de rôles et de profils. Ainsi le profil métier « Directeur d'unité » donne droit à un ensemble de rôles applicatifs, dont celui de « Gestionnaire de profil » dans le contexte de l'application Simbad.

Pour la gestion des accès, OpenIAM ne permet pas de gérer l'attribution des rôles dans les applications. En effet, il n'est pas possible de définir qu'une seule table cible dans la configuration du connecteur à la ressource. De ce fait, il n'est pas possible d'alimenter en plus une table qui lie un compte utilisateur à des rôles. En corollaire, un flux de réconciliation ne permettrait pas de faire remonter dans OpenIAM les droits qui sont donnés à un compte utilisateur.

V.8.2.2 Alimentation d'un annuaire LDAP

Tous les comptes créés par synchronisation avec Labintel doivent être enregistrés dans les annuaires LDAP « Central » et « Référentiel ». Afin de respecter le modèle RBAC, ces deux ressources sont chacune associée à un rôle distinct. Afin de rester conforme aux règles régissant la création d'un compte dans un annuaire, un compte ne peut être créé que si la personne est décrite comme présente en unité et n'est pas du type personnel privé. La seconde information n'étant pas prise en compte, la vue « VUE_IDENTITE » doit donc être adaptée pour présenter la colonne « INR_PER_PRIV » de la table « PER ». Si le compte remplit ces conditions, les rôles techniques « LDAP Central » et « LDAP Référentiel » lui sont automatiquement attribués. Par contre, l'alimentation de l'annuaire « SAP » repose sur d'autres conditions. En effet, les utilisateurs SAP sont les titulaires du CNRS, les directeurs d'unité et les comptes possédant le rôle « Utilisateur

SAP ». Finalement, le référencement d'un compte dans l'annuaire « SAP » peut reposer uniquement sur l'attribution du rôle « Utilisateur SAP ». Ce dernier peut alors être attribué automatiquement aux titulaires CNRS et les directeurs d'unité.

Comme précisé lors l'étape de cartographie, les comptes utilisateurs doivent être créés sous la racine « ou=people, dc=cnrs, dc=fr ». La branche « CNRS » contient les titulaires CNRS, la branche « EXTER » contient les titulaires non CNRS et la branche « TEMP » contient les non titulaires payés par le CNRS. Pour mettre en œuvre cette répartition, il suffit d'utiliser une correspondance d'informations pour l'attribut cible « ou ».

```
def listNatureCnrs = new HashSet( [ 'ITA CNRS', 'chercheur CNRS' ] );
def listCodePermanentNature = new HashSet( [ 'chercheur','enseignant-
chercheur','ingénieur de recherche','ingénieur','technicien/administratif' ] );

def isCNRS         = listNatureCnrs.contains( user.title );
def isPermanent = listCodePermanentNature.contains( user.employeeType )

def subBranch = "temp";
if ( isPermanent ) {
       if ( isCNRS ) {
              subBranch = "cnrs";
       } else {
              subBranch = "exter";
       }
}

output=subBranch;
```

Figure 103 - Classe de correspondance « ou.groovy »

Par ailleurs, pour les annuaires LDAP, l'identifiant technique est l'attribut « uid » décrit dans la RFC 4519. Il peut être construit automatiquement lors de la synchronisation avec Labintel et être enregistré dans un attribut dédié afin de s'assurer que la valeur soit la même dans tous les annuaires. La valeur est composée du prénom et du nom de la personne. Si cette valeur existe déjà, une extension numérique est ajoutée et éventuellement incrémentée tant qu'une valeur existe.

```
def uid = pUser.firstName.replaceAll("\\s", ".") + "." +
       pUser.lastName.replaceAll("\\s", "."); //remplace les espaces par des points
def ctr = 1;
def origUid = uid;
//Verifie si uid existe deja
while ( loginManager.loginExists( "USR_SEC_DOMAIN", uid, 0 )) {
       strCtrSize = String.valueOf(ctr);
       uid=origUid + ctr;
       ctr++;
}
```

Figure 104 - Classe TransformSrcLabRecord.groovy : construction simplifiée de l'attribut « uid »

Les attributs utilisés pour limiter les accès à une application sont « CnrsRole » et « RefRole » respectivement pour les annuaires « Central » et « Référentiel ». Pour le profil DU,

l'attribut « CnrsRole » est positionné à la valeur « DU – *code unité* » dans l'annuaire central et « RefRole » à « du=*code unité* » dans l'annuaire référentiel. Les rôles applicatifs CORE de validation et d'administration sont respectivement représentés dans l'annuaire « Référentiel » par les attributs « {Core}validDr=*code DR* » et « {Core}adminDR=*code DR* ». Pour Simbad, le rôle de valideur est « {Simbad}valideur:unite=*code unité* » et le rôle de gestionnaire de profil est « {Simbad}gestionnaireProfil:unite=*code unité* ».

V.8.3 Rétrospective de l'itération

La tâche consistant à alimenter une table de compte dans une base de données a permis de mettre en évidence les difficultés liées au choix de l'identifiant pour le système d'information du CNRS. Cependant, un contournement est envisageable en utilisant une colonne technique correspondant aux identifiants techniques générés par l'outil OpenIAM.

Pour les annuaires LDAP, l'identifiant technique d'un compte est son « uid ». Pour le périmètre du démonstrateur, les valeurs ont été construites sans tenir compte de celles qui existent dans les annuaires LDAP actuellement déployés. De ce fait, dans le cadre de l'installation dans le contexte du système d'information du CNRS, les « uid » existants devraient être synchronisés avec le référentiel OpenIAM lors de la phase d'initialisation.

Par ailleurs, le modèle RBAC impose de créer des rôles sans signification métier pour l'alimentation des annuaires LDAP. Cela peut permettre de déterminer, lors d'un audit, si la présence d'un compte dans un annuaire est légitime. Les comptes créés directement dans un annuaire sans avoir utiliser l'outil peuvent ainsi être détectés par comparaison avec la liste des comptes possédant le rôle nécessaire.

V.9 Itération 6 – Désactivation de comptes

V.9.1 Sprint backlog

L'objectif de l'itération est de développer la gestion complète du cycle de vie des comptes après l'étape d'approvisionnement. Ainsi, lorsqu'une affectation arrive à échéance, le compte sous-jacent doit être rendu inactif. Ce cas de figure correspond à la user story « En tant qu'administrateur, je veux qu'un compte soit inutilisable quand la personne n'est plus présente dans son unité d'affectation ».

V.9.2 Fin de présence en unité dans Labintel

Dans le cas où l'affectation d'une personne dans une unité prend fin, la personne ne doit plus être en mesure de se connecter aux ressources du système d'information du CNRS. Cela implique que le compte ne soit plus utilisable auprès des systèmes d'authentification, à savoir les annuaires LDAP « Central », « Référentiel » et « SAP ». Pour Janus, l'attribut « refUnauthenticable » permet d'empêcher un compte d'être utilisé. Cependant, cette information n'est pas disponible dans les annuaires « Central » et « SAP ». De ce fait, il est préférable d'intervenir au niveau de l'attribution des rôles. Les trois rôles relatifs aux annuaires doivent donc être retirés de tous les comptes inactifs. Cela présente également l'avantage que l'information d'approvisionnement soit disponible pour les audits et visible au travers de l'application. En outre, aucun autre rôle ne doit être retiré. Ainsi, en cas de réactivation du compte, tous les droits applicatifs dans les différentes ressources sont inchangés. Par contre, le rôle DU fait exception. En effet, du point de vue métier, lorsque la mission de direction de l'unité prend fin, la personne n'a plus le profil « Directeur d'unité ». De ce fait, le rôle DU ainsi que tous les dérivés, tels que « Gestionnaire de profil » doivent être retirés.

V.9.3 Rétrospective de l'itération

La désactivation de comptes est facilitée par l'utilisation du modèle RBAC. En effet, le retrait des rôles techniques correspondant à chaque ressource responsable de l'authentification permet d'empêcher les accès au système d'information à partir d'un compte inactif. Par contre, la conservation des rôles applicatifs permet de restituer les droits d'utilisation en cas de réactivation du compte.

V.10 Itération 7 – Délégation d'habilitation

V.10.1 Sprint backlog

Actuellement, lorsqu'un directeur d'unité souhaite déléguer certaines de ses activités, il divulgue son mot de passe à la personne qui doit exercer ses fonctions pendant son absence. L'objectif de cette itération est d'éviter ce comportement afin d'assurer la sécurité du système d'information. La user story est donc « En tant qu'utilisateur, je veux partager mes accréditations à un autre utilisateur pendant une période limitée ».

V.10.2 Développement d'un workflow de délégation de gestion d'un rôle

Le développement de workflow n'est pas possible dans la version communautaire 2.2. Cette fonctionnalité est disponible avec la version payante ou avec la version communautaire 2.3.

V.11 Itération 8 – Compte temporaire

V.11.1 Sprint backlog

L'objectif de cette itération est de développer les processus liés aux différents types de comptes liés à des missions à durée déterminée. Cela concerne autant les emplois ayant un contrat à durée déterminée, que les contrats de prestation externe. Ces deux cas de gestion impliquent les deux user stories distinctes suivantes : « En tant qu'administrateur, je veux qu'une personne recrutée en contrat à durée déterminée puisse utiliser les ressources adéquates dès le début de son contrat » et « En tant que responsable applicatif, je veux qu'un intervenant ne travaillant pas pour une unité du CNRS puisse se connecter à l'application ».

V.11.2 Gestion des contrats à durée déterminée issus de Labintel

L'approvisionnement des affectations depuis Labintel a été développée lors des premières itérations, de même que la désactivation automatique lorsque l'affectation prend fin. L'aspect de gestion des contrats à durée déterminée par synchronisation avec Labintel ne nécessite donc pas de développement spécifique. En effet, à la date de fin d'affectation, la personne est positionnée comme n'étant plus présente en unité dans Labintel. De ce fait, bien que le contrat possède l'information de date de fin, il n'est pas nécessaire de modifier le processus de synchronisation pour le prendre en compte. Cependant, il serait souhaitable que la personne puisse être opérationnelle dès son arrivée dans l'unité. Hors, pour les personnes employées par le CNRS l'affectation n'est visible dans Labintel qu'après retour du procès verbal d'installation. Cela signifie que la personne est présente en unité, mais qu'aucun compte ne peut lui être attribué dès son arrivée. Pour pallier à ce problème, il faut avoir accès aux données présentes dans SIRHUS. OpenIAM ne disposant pas de connecteur pour SAP, il n'est pas possible d'anticiper la création de compte dans le cadre du périmètre de la présente étude. Par contre, OpenIAM dispose d'un connecteur pour les webservices. Aussi, en faisant évoluer le format pivot issu du demi-flux SIRHUS pour rendre visibles toutes les fiches, actives ou non validées, il serait envisageable de pouvoir créer un compte par anticipation. Ensuite, il serait nécessaire alors de développer un processus de réconciliation avec Labintel pour pouvoir attribuer l'attribut « NUM_PER » au compte déjà créé.

En outre, l'itération liée à la désactivation des comptes a permis de développer le retrait automatique des rôles liés aux annuaires.

Par ailleurs, lorsqu'une affectation prend fin et par conséquent que le compte est rendu inactif, il doit être automatiquement supprimé dans les annuaires. Par contre, puisqu'il a conservé les rôles relatifs aux annuaires, dès sa réactivation, il est à nouveau créé dans les annuaires avec

tous ses rôles applicatifs. A cette fin, les ressources LDAP doivent être paramétrées pour supprimer un compte lorsque l'évènement de désactivation est levé.

Pour les contrats à durée déterminée CNRS, en cas de renouvellement du contrat, la fiche agent dans Labintel reste la même et conserve donc la même valeur d'attribut « NUM_PER ». Dans ce cas, le compte conserve les rôles qui lui étaient attribués. Par contre, l'activation automatique du compte dans Labintel est également soumise à la saisie du procès verbal d'installation. Cependant, comme le compte existe déjà, un administrateur peut activer le compte manuellement. Il faut alors prévoir un processus de demande d'activation, ce qui n'est pas possible dans le cadre de la présente étude. En revanche, si la personne obtient un nouveau contrat pour une affectation différente, le compte qu'elle va utiliser ne peux pas et ne doit pas reprendre les rôles par défaut acquis précédemment. Par contre, il peut être utile de conserver les accréditations liées à l'ancienne affectation au cas où la mission à réaliser soit la même. Dans ce cas, il est possible de reproduire l'ensemble des rôles sur la nouvelle affectation.
Comme évoqué lors de la description du cycle de vie des identités au CNRS, pour les personnes en contrat à durée déterminée issues d'autres organismes, les affectations sont liées à la notion de séjour. En cas de renouvellement du contrat, un séjour est ajouté dans la fiche Labintel de l'agent non-CNRS. Cela permet de conserver la même valeur de « NUM_PER ». La personne peut donc continuer à utiliser le même compte dès qu'il est marqué comme présent dans l'unité.

V.11.3 Gestion des contrats de missions non gérées par Labintel

Les personnes ayant besoin d'accéder à des ressources CNRS mais qui ne sont pas saisies dans Labintel sont intégrées dans le fournisseur d'identité « Janus-Ext ». L'alimentation des comptes dans la branche « foreigner » de l'annuaire « Référentiel » ne peut pas être automatisée. Par contre, la demande de création de compte peut être saisie au travers de l'application OpenIAM self-service. Dans ce cas, le processus doit inclure automatiquement une demande d'enregistrement auprès du fournisseur d'identité « Janus-Ext ». Dans OpenIAM, il est possible d'associer une création de compte par l'application self-service à une ressource. Cependant, pour des raisons de lisibilité, il est préférable que le compte soit associé à un rôle spécifique à l'annuaire « Référentiel » pour la branche « foreigner ». Ainsi, le processus de création manuelle de comptes doit inclure l'attribution automatique du rôle « Janus-Ext ». De plus, la demande de création doit inclure une date de début de mission et une date de fin. Si aucune date de fin n'est spécifiée, il est nécessaire qu'une date limite par défaut soit attribuée. La PSSI du CNRS ne fournit pas de période maximum autorisée. Elle sera donc à définir en concertation avec le RSSI du CNRS. Les comptes existants doivent être soumis à la même restriction. De ce fait, les comptes externes doivent être intégrés dans

le référentiel OpenIAM pour leur attribuer une date de fin. Cette étape de réconciliation permettra de désactiver les comptes inutilisés à la fin de la période autorisée.

V.11.4 Rétrospective de l'itération

Pour les comptes issus de la synchronisation avec Labintel, aucun développement spécifique n'est nécessaire. Cependant, il faut envisager la modification du demi-flux EAI d'extraction de SIRHUS pour rendre visibles les fiches agent non validées. Ainsi, il serait possible d'anticiper la création de comptes et rendre les personnes opérationnelles dès leur arrivée en unité. Par ailleurs, il serait souhaitable de pouvoir améliorer la qualité des données pour les fiches agent créées dans Labintel pour le personnel extérieur. Cela permettrait d'éviter d'augmenter inutilement le nombre de comptes utilisateurs.

Pour les personnes externes, le processus de création des comptes affecte un rôle spécifique au fournisseur d'identité « Janus-Ext ». De plus, ce type de compte, qui inclut les comptes existants, doit obligatoirement posséder une date de fin de mission. Hors, ces comptes ne sont pas soumis à la déclaration CNIL de Labintel, car ils sont en dehors de son périmètre. Il devient donc nécessaire de réaliser une déclaration spécifique à la gestion des identités et des accès du système d'information du CNRS.

V.12 Rétrospective du démonstrateur

Les itérations relatives au choix et à l'implémentation d'une architecture FLOSS ont permis de mettre en évidence que l'utilisation d'une méthode reconnue est nécessaire afin de pouvoir caractériser l'environnement tant organisationnel que technique du projet de l'outil. Le choix de définir une méthode propre a induit un retard de presque un mois. Par contre, le choix d'une méthode reconnue telle que QSOS a permis de sélectionner un projet qui évolue régulièrement et dont l'équipe est attentive aux besoins des utilisateurs. Cependant, la fiche de sélection d'un outil doit évoluer pour intégrer des critères supplémentaires permettant d'effectuer une comparaison avec l'existant composé des outils DMAS et IHM.

En outre, bien que les cas d'utilisations choisis étaient simples, ils ont permis d'approcher les difficultés potentielles de cas d'utilisation plus complexes. De ce fait, si un autre outil doit être évalué, il est possible d'utiliser les mêmes cas d'utilisation. Dans le cas du test d'une nouvelle version d'OpenIAM ou d'un autre outil de gestion des identités et des accès, il est possible de réutiliser les différents éléments développés au cours de cette étude, car le code source de l'application n'a pas été modifié.

Ainsi, l'itération « Construction du référentiel des identités » montre qu'il faut modifier la fiche d'évaluation pour la fréquence de synchronisation. Les notes attribuées doivent alors être définies selon les critères suivants : 2 pour une fréquence inférieure à dix secondes, 1 pour une fréquence comprise en dix secondes et une minute et 0 pour une fréquence supérieure. De plus, le service de page blanche doit pouvoir gérer les demandes de retrait conformément à la loi informatique et liberté. Par contre, après discussion avec les développeurs, j'ai saisi la demande de fonctionnalité « IDMAPPS-563 - Define inheritance in user type » qui doit être développée en version 3.0. En outre, une vue spécifique a été développée pour l'application Labintel. Elle rassemble l'ensemble des informations nécessaires à la construction des identités. Celle-ci pourra servir de source unique, alors qu'actuellement le recueil d'information nécessite plusieurs requêtes.

L'itération pour la gestion des rôles a permis de mettre en œuvre la distinction entre les notions de profils et de rôles. L'attribution de rôles applicatifs dans les bases de comptes a pu être automatisée pour le profil « Directeur d'unité ». Le modèle ABAC actuellement mis en œuvre permet uniquement le positionnement d'attributs dans les annuaires. En outre, ce sprint a permis de mettre en évidence que la possibilité de développer un processus de demande de rôle est un aspect important qui n'est pas géré actuellement par OpenIAM. Le coefficient affecté à ce critère doit être augmenté.

L'itération d'approvisionnement des ressources cibles a permis de trouver une solution pour mettre à jour les identifiants basés sur les adresses électroniques dans les bases de compte des ressources

cibles. Il est en effet possible d'ajouter un identifiant technique caché dans les tables des ressources cibles correspondant à l'identifiant technique du compte dans l'outil de gestion des identités et des accès. De plus, chaque transformation étant réalisée dans un script différent, il est facile de réutiliser ou réinterpréter le code développé pour un autre outil.
L'itération de désactivation de comptes a permis de démontrer que le modèle RBAC permet de rendre inaccessible l'accès aux ressources tout en conservant l'état d'un compte pour faciliter sa réactivation. Comme pour le sprint précédent, les scripts groovy mis en œuvre pourront être réutilisés lors de développements avec d'autres solutions.

Finalement, seuls les cas d'utilisation impliquant les acteurs d'administration ont pu être développés. OpenIAM est donc capable de remplacer les outils existants, pour « maximiser l'intégration des fonctionnalités au sein d'un même outil » comme stipulé dans le schéma directeur de la DSI du CNRS. Par contre, les user stories concernant les utilisateurs du système d'information du CNRS n'ont pu être que faiblement implémentées. En effet, l'outil n'offre pas la possibilité de développer des processus de demande et d'attribution de rôles. De même, l'itération pour la délégation d'habilitation n'a pas pu être mise en œuvre car la fonctionnalité n'existe pas en version 2.2 communautaire. OpenIAM ne permet donc pas de mettre en place des processus de gestion pour les comptes utilisateurs nécessitant des interventions humaines.
De plus, le modèle OpenIAM ne permet pas de prendre en compte les services dépendant de plusieurs organisations. Hors les unités multi-tutelles représentent plus de la moitié des unités prises en compte dans Labintel.
Ces différents cas d'utilisation devant être obligatoirement pris en charge à moyen terme, l'outil OpenIAM ne peut pas être une solution envisageable pour répondre aux besoins du CNRS.

Conclusion

Gouvernance des identités

Bien que le projet Janus eut pour ambition en 2009 de prendre en charge la gestion des identités et des accès, l'étude de cette thématique ne fut lancée qu'en 2011. En effet, la gestion des identités et des accès est un domaine qui est en train de se construire. Actuellement, peu de standards existent, ce qui augmente la complexité des projets de gestion des identités et des accès. Pour preuve, la norme ISO-24760 ne fut publiée qu'en 2011. Pour le projet du CNRS, il fut donc nécessaire de commencer par établir un dictionnaire des concepts manipulés afin de s'assurer que tous les acteurs partagent un langage commun. L'étape de cartographie a permis de mettre en évidence que la notion de personne n'est prise en compte que pour un tiers de la population des utilisateurs du système d'information du CNRS. La grande majorité des utilisateurs est associée à la notion d'affectation. La gestion des identités n'est donc pas intégrée dans la politique d'urbanisation du système d'information. Pour palier à ce manque et comprendre les interactions, il fut nécessaire de rencontrer des gestionnaires des ressources humaines et des responsables régionaux des systèmes d'informations. Ainsi, les identités sont actuellement liées aux affectations dans les unités et décorrélées des personnes. Cela implique des pertes d'informations qui peuvent être nécessaires aux applications du système d'information du CNRS. Cette situation est à l'origine des problèmes récurrents rencontrés par les applications nationales du système d'information. Le CNRS ne dispose pas de toutes les informations nécessaires pour associer les cent vingt milles comptes utilisateurs du fournisseur d'identité Janus à des personnes physiques. Cette étape à approfondir sera nécessaire pour améliorer la gestion des identités. Paradoxalement, la fédération « Éducation-Recherche » a permis de faciliter l'authentification des personnels extérieurs, mais a aggravé le problème de qualité des données. C'est pour cette raison qu'il est généralement conseillé de commencer un projet de gestion des identités et des accès par l'aspect identité et non par la gestion des accès.

En outre, l'augmentation du périmètre des comptes utilisateurs doit être prise en compte par une déclaration CNIL indépendante de celle de Labintel, comme c'est le cas actuellement pour le référentiel du fournisseur d'identité du CNRS. L'ouverture du système d'information aux partenaires du CNRS implique de nouveaux traitements qui doivent être pris en compte dans une déclaration CNIL spécifique ou mise à jour.

Par ailleurs, pour répondre aux besoins de réactivité pour rendre les personnels recrutés opérationnels au plus tôt, il sera nécessaire de modifier les flux d'information. Les rencontres avec les responsables applicatifs de la DSI du CNRS ont permis de mettre en évidence que les problèmes n'étaient pas d'ordre technique mais organisationnel. En ce sens, j'ai travaillé avec l'équipe

responsable de l'EAI et le responsable de l'application SIRHUS pour faire évoluer le demi-flux d'extraction. L'objectif est de rendre visible toutes les fiches agents, même celle en attente de validation, afin de pouvoir anticiper la création de comptes sous contrôle d'une personne autorisée. Cette solution pouvant résoudre d'autres problèmes dans le système d'information, la modification du demi-flux est en cours de planification.

L'ensemble des connaissances et compétences acquises tout au long de cette étude m'ont permis de participer à différents travaux pilotés par la DSI du CNRS. Ainsi, j'ai pu intégrer un groupe de travail mené par l'équipe responsable de l'urbanisation sur le thème « Flux de personnes ».

Au-delà du développement d'un outil, l'étude a permis de mettre en évidence des problèmes de sécurité dus aux processus métier actuellement en place et à l'absence d'une gouvernance des identités et des accès.

De plus, la cartographie réalisée a été intégrée dans un document de référence livré en annexe de tous les cahier des charges pour les appels d'offres relatifs aux annuaires ou aux outils Shibboleth mis en œuvre par la DSI du CNRS. Ainsi, les sociétés candidates ont connaissance de l'environnement CNRS de gestion des comptes pour les applications nationales.

Application de gestion des identités

Le développement du démonstrateur avait pour but de vérifier la faisabilité de la reprise de l'architecture existante par un outil Free/Libre Open Source et de l'étendre à la gestion des rôles et des accès pour les applications du système d'information du CNRS. La première difficulté rencontrée fut de trouver une méthode fiable pour choisir un projet candidat. Ensuite, le choix d'OpenIAM a permis de répondre majoritairement aux objectifs fixés lors de la phase de recueil des besoins. Cependant, chaque itération a permis de mettre en évidence des difficultés de réalisation. L'outil n'est en effet pas conçu pour gérer l'appartenance d'une unité à plusieurs tutelles. Il ne permet pas également de répondre aux besoins de gestion de processus de demande, d'attribution ou de délégation. OpenIAM en version communautaire 2.2 ne peut donc pas être une solution de support à la gestion globale des identités et des accès pour le personnel des unités du CNRS. En effet, pour répondre à l'ensemble des besoins, le coup induit par la modification de la version communautaire 2.2 représente un cout proche d'un développement spécifique complet. De plus, la version OpenIAM 2.3 était prévue pour novembre 2012. Elle a ensuite été repoussée de mois en mois à décembre, janvier puis février. Elle fut finalement mise à disposition en mars 2013. La société semble avoir eu des difficultés à finaliser cette mise à jour. Les capacités de l'organisation ne sont pas donc pas celle attendues. La présente étude a permis d'établir que le marché Open Source de la gestion des identités et des accès n'offre que des solutions en cours de développement.

Les offres FLOSS doivent donc encore évoluer pour atteindre le niveau que proposait l'éditeur Sun avec son outil Sun IdM avant son rachat par Oracle.

Un critère supplémentaire souhaité par la sécurité des systèmes d'information du CNRS est de pouvoir bénéficier d'un support de proximité, ou au moins assuré par un organisme français. Cette offre locale n'existe pas pour OpenIAM, contrairement à d'autres outils libres dans d'autres domaines tels que l'annuaire OpenLDAP. Le besoin d'accompagnement par un prestataire français peut être ajouté comme critère de la fiche d'identité des outils Open Source, permettant ainsi par la méthode QSOS de ne pas sélectionner les projets non pris en charge par au moins un de ses partenaires en France.

Cependant, l'outil OpenIAM pourra être déployé pour des contextes moins sensibles que le domaine du fournisseur d'identité Janus. Par exemple, il est envisageable de le mettre en œuvre pour la gestion des comptes utilisés pour les concours en ligne. Les bases de comptes de ces applications doivent être vidées après chaque concours. L'application de self-service pourrait être utilisée pour que les candidats se créent un compte et gèrent leurs informations de connexion. Ces informations seraient provisionnées vers un fournisseur d'identité dédié à ce domaine d'activité. Cela permettrait d'éviter de développer les briques de gestion des comptes pour chaque application en dehors du périmètre de Janus ou de la fédération d'identité.

Bien que poussée par la circulaire publiée le 19 septembre 2012 par le Premier Ministre français Jean-Marc Ayrault sur le bon usage des logiciels libres dans l'administration française, la mise en œuvre des logiciels Open Source ne doit pas être automatique, comme stipulée en page neuf de l'annexe jointe à cette circulaire. Ceci est le cas des outils Open Source étudiés qui n'ont pas permis de répondre à l'ensemble des besoins, plusieurs autres possibilités sont envisageables. Continuer à investir dans les outils développés en interne, DMAS et IHM, est la solution envisagée en attendant l'émergence d'une solution complète adéquate.

Parallèlement, l'examen des outils commerciaux est facilité par l'utilisation des grilles d'évaluation rédigées lors de la présente étude. De plus, les cas d'utilisation sélectionnés ayant permis de mettre en évidence les difficultés à répondre à l'ensemble des besoins du CNRS, ils peuvent être mis à profit pour développer un nouveau démonstrateur. Ensuite, la décision d'achat reposera sur la comparaison de son coût d'acquisition et de mise en conformité avec le format CNRS par rapport à un développement interne. Dans ce cadre, j'ai réalisé avec l'éditeur Oracle un démonstrateur basé sur l'outil Oracle Identity Management. L'installation, la configuration, le développement d'une synchronisation, la configuration de rôles et l'approvisionnement d'un annuaire LDAP et d'une base de données équivalent à celui réalisé dans l'itération 5 ont rencontré des difficultés, mais ont permis de montrer la maturité et une plus grande complétude du produit. Ce travail a pu être

accompli en une semaine seulement parce que de nombreux écueils avaient été soulevés par l'étude des outils FLOSS.

Par ailleurs, depuis la réalisation de la sélection lors du second sprint de « Définition de l'architecture cible », l'ensemble des projets a évolué. Ainsi, Kuali a développé huit nouvelles versions, dont la première intègre notamment un correctif aux problèmes rencontrés avec le SGBDR MySQL. Evolveum a également publié une nouvelle version majeure de MidPoint, mais la structure du projet et le nombre de clients n'ont pas évolué. Le projet Apache Syncope n'est plus en mode incubateur. Malgré des mises à jour mensuelles, la version 1.1 planifiée pour fin 2012 n'est disponible que depuis fin mars 2013. OpenIAM a terminé la version 2.3 qui intègre entre autres la possibilité de réaliser des processus de demande et d'attribution de rôle. ForgeRock a également publié une mise à jour majeure de l'ensemble de ses outils. De plus, son vice-président, A. Foster a été élu « President of the Board of Trustees » pour l'Initiative Kantara et nommé au directoire de l'Institute of Electrical and Electronics Engineers (IEEE). Cette marque de confiance des communautés d'experts et Free/Libre Open Source envers le vice-président de ForgeRock, ainsi que la présence de la société en France montrent que l'offre mérite d'être réévaluée, ou au moins suivie.

Une solution à envisager est d'investir avec des établissements partenaires de la recherche dans l'un de ces outils FLOSS pour l'aider à respecter sa feuille de route et pour réaliser en parallèle les fonctionnalités spécifiques au CNRS. Le code source ainsi développé serait alors reversé à la communauté.

Bibliographie

Références documentaires

[1] M.R. Nami, A. Malekpour. Virtual Organizations : Trends and Models. Dans IFIP International Federation for Information Processing, Volume 288; *Intelligent Information Processing IV*, Zhongzhi Shi, E. Mercier-Laurent, D. Leake, pages 190–199, 2008

[2] J. Magiera, A. Pawlak. Security Frameworks for virtual organizations. Dans *Organizations: Systems and Practices*. Springer, pages 133-148, 2005

[3] A. Sigogneau, S. Landel. *2010, une année avec le CNRS, données chiffrées et indicateurs*. CNRS, 33 pages, 2011

[4] Denis Guthleben. *Histoire du CNRS de 1939 à nos jours.* Armand Colin, 480 pages, 2003

[5] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, S. Pope. Trust Requirements in Identity Management. *Australasian Information Security Workshop 2005* volume 44, pages 99-108, 2005

[6] *ISO/IEC 24760-1:2011(E)*. ISO/IEC, 20 pages, 2011

[7] E. Bertino, K. Takahashi. *Identity Management: Concepts, technologies and systems*. Artech House, 194 pages, 2010

[8] A. Balat, R. Bergeron, A. Butel, M. Cottreau, F. Depierre, G. Khouberman, L. Mourer, W. Poloczanski. *Gestion des identités*. CLUSIF, 63 pages, 2007

[9] G. Harry. *Failles de sécurité des applications Web*. CNRS, 38 pages, 2012

[10] D. F. Ferraiolo, D. R. Kuhn, R. Chandramouli. *Role-Based Access Control, Second Edition*. Artech House, 381 pages, 2007

[11] F. Cuppens, N. Cuppens-Boulahia. Les modèles de sécurité. Dans *Sécurité des systèmes d'information, (Traité IC2, série Réseaux et télécoms)*. Hermès, pages 13-48, 2006

[12] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, R. Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security* v.4 n.3, pages 224-274, 2001

[13] M. Frank, J. M. Buhmann , D. Basin. On the definition of role mining. Dans *Proceeding of the 15th ACM symposium on Access control models and technologies*, pages 35-44, 2010

[14] L. Wang, D. Wijesekera, S. Jajodia. A logic-based framework for attribute based access control. Dans *Proceedings of the 2004 ACM workshop on Formal methods in security engineering*, pages 45-55, 2004

[15] G. Chamoret, F. Chavoutier, M. Copitet, J-P Godard, P. Grassart, J. Mauferon, L. Mourer, T. Ramard, G. Remy. *La réforme BÂLE 2, une présentation générale*. CLUSIF, 28 pages, 2004

[16] L. Audibert. *UML 2 de l'apprentissage à la pratique*. Ellipses, 298 pages, 2009

[17] W. W. Royce. Managing the Development of Large Software Systems : concepts and techniques. Dans *Proceedings of the 9th international conference on Software Engineering*, pages 1-9, 1970

[18] J. McDermid, K. Ripken. Life cycle support in the Ada environment. *ACM SIGAda Ada Letters*, v.III n.1, pages 57-62, 1983

[19] K. Beck. *Test Driven Development: By Example*. Pearson Education, 240 pages, 2002

[20] B. W. Boehm. A Spiral Model of Software Development and Enhancement. *ACM SIGSOFT Software Engineering Notes*, Volume 11 n.4, pages 14-24, 1986

[21] A. Cockburn. *Agile software development*. Addison-Wesley Longman Publishing Co., 278 pages, 2002

[22] *ISO/CEI 27002:2005(F)*. ISO/IEC, 130 pages, 2005

[23] P. Carpenter, E. Perkins. *Magic Quadrant for User Administration/Provisionning*. Gartner Inc., 42 pages, 2011

[24] M. Phillips, S. Shrum. *Which CMMI Model Is for You?*. Software Engineering Institute, Carnegie Mellon University, 4 pages, 2011

[25] Equipe produit CMMI. *CMMI pour le développement, version 1.3*. Software Engineering Institute, Carnegie Mellon University, 570 pages, 2010

[26] H. Glazer, J. Dalton, D. Anderson, M. Konrad, S. Shrum. *CMMI or Agile: Why Not Embrace Both!*. Software Engineering Institute, Carnegie Mellon University, 45 pages, 2008

[27] K.-J. Stol, M. Ali Babar. A Comparison Framework for Open Source Software Evaluation Methods. Dans *Open Source Software: New Horizons*, pages 389-394, 2010

[28] F.-W. Duijnhouwer, C. Duijnhouwer. *Open Source. Maturity Model*, Capgemini Expert Letter, 2003

[29] B. Golden. *Succeeding with Open Source*. Addison-Wesley Professional, 272 pages, 2004

[30] R. Semeteys, O. Pilot, L. Baudrillard, G. Le Bouder. *Méthode de Qualification et de Sélection de logiciels Open Source (QSOS) version 1.6*. Atos Origin, 36 pages, 2006

[31] A. Wasserman, M. Pal, C. Chan. *Business Readiness Rating for Open Source, BRR Whitepaper 2005 Request For Comments 1*. OpenBRR.org, 22 pages, 2005

[32] M. Wittmann, R. Nambakam, G. Ruffati, S. Oltolina, E. Petrinja, F. Ortega, V. Malheiros, D. Tosi. *Working Document 6.3.1 - CMM-like model for OSS*. Qualipso, 140 pages, 2009

Références Web

- Bearing Point. *Améliorer la gestion de l'identité et des droits, quels gains pour une DRH ?*, disponible sur : http://blogrh.bearingpoint.com (consulté le 23/04/2012)
- CIFER. *Community Identity Framework for Education and Research*, disponible sur : http://ciferproject.org (consulté le 03/09/2012)
- ConnId. *Framework for simplifying provisioning*, disponible sur : https://code.google.com/p/connid (consulté le 03/09/2012)
- Evolveum. *Open projects. Reliable technology. Useful systems.*, disponible sur : http://evolveum.com (consulté le 03/09/2012)
- Renater. *Fédération Éducation-Recherche*, disponible sur : https://federation.renater.fr (consulté le 25/04/2012)
- FreeMind. *FreeMind - free mind mapping software*, disponible sur : http://freemind.sourceforge.net (consulté le 24/10/2012)
- CNRS. *IGC CNRS*, disponible sur : https://igc.services.cnrs.fr/Doc/ (consulté le 03/09/2012)
- Apache. *Apache Syncope*, disponible sur : http://incubator.apache.org/syncope/ (consulté le 03/09/2012)
- CNRS. *Le projet Janus*, disponible sur : https://janus.dsi.cnrs.fr/Documentation/ (consulté le 25/04/2012)
- Kuali. *Kuali Identity Management*, disponible sur : http://kuali.org/rice/modules/kim (consulté le 03/09/2012)
- Internet2. *Middleware*, disponible sur : http://middleware.internet2.edu (consulté le 03/09/2012)
- ForgeRock. *OpenIDM project*, disponible sur : http://openidm.forgerock.org/ (consulté le 03/09/2012)
- Tirasa. *Syncope*, disponible sur : http://syncope.tirasa.net (consulté le 01/08/2012)
- Jasig. *What is OpenRegistry?*, disponible sur : https://wiki.jasig.org/display/OR/Home (consulté le 03/09/2012)
- CLUSIF. *Club de la Sécurité de l'Information Français*, disponible sur : http://www.clusif.asso.fr (consulté le 25/04/2012)
- CNRS. *Bienvenue au CNRS*, disponible sur : http://www.cnrs.fr (consulté le 23/04/2012)

- Comité Réseau des Universités. *Intégration du CRU à Renater*, disponible sur : https://www.cru.fr (consulté le 03/09/2012)
- Educause. *What is Educause ?*, disponible sur : http://www.educause.edu (consulté le 03/09/2012)
- Gartner. *Top 10 Information Management Trends*, disponible sur : http://www.gartner.com (consulté le 31/07/2012)
- ITFACTO. *Conformité des accès : Identités, annuaire, SSO*, disponible sur : http://www.guidescomparatifs.com/Conformite_des_acces_identites_annuaire_mot_de_passe.asp (consulté le 10/08/2012)
- Identropy. *The Identropy Blog*, disponible sur : http://www.identropy.com/blog/ (consulté le 24/04/2012)
- ISO. *We're ISO, the International Organization for Standardization. We develop and publish International Standards.*, disponible sur : http://www.iso.org (consulté le 25/04/2012)
- Linagora. *Logiciels et Services Open Source pour réussir les grands projets du libre !*, http://www.linagora.com (consulté le 03/09/2012)
- nLight. *Open Source Identity Management Systems*, disponible sur : http://www.nlight.eu/documents/open-source-idm/ (consulté le 23/03/2012)
- Black Duck Software, Inc. *Discover, Track and Compare Open Source*, disponible sur : https://www.ohloh.net (consulté le 03/09/2012)
- The Open Group. *The Open Group's member organizations work to establish open, vendor-neutral IT standards and certifications in a variety of subject areas critical to the enterprise.* disponible sur : http://www.opengroup.org (consulté le 09/05/2012)
- OpenIAM. *Identity & Access Management for the Enterprise*, disponible sur : http://www.openiam.com (consulté le 09/05/2012)
- Qualipso. *Trust and Quality in Open Source Systems*, disponible sur : http://www.qualipso.org (consulté le 25/09/2012)
- Atos Origin. *Collaborative technological watch Qualification and Selection of Opensource Software*, disponible sur : http://www.qsos.org (consulté le 25/09/2012)
- Agence Nationale de le Sécurité des Systèmes d'Information. *Portail de la sécurité informatique*, disponible sur : http://www.securite-informatique.gouv.fr (consulté le 25/04/2012)
- Carnegie Mellon Software Engineering Institute. *Welcome to the Software Engineering Institute*, disponible sur : http://www.sei.cmu.edu (consulté le 24/09/2012)
- Spring. *What is Spring?*, disponible sur : http://www.springsource.org/ (consulté le 01/10/2012)

- Agence Nationale de le Sécurité des Systèmes d'Information. *Actualités, guides, publications*, disponible su*r :* http://www.ssi.gouv.fr (consulté le 25/04/2012)

Source des icônes libres de droits d'utilisations : http://findicons.com

Table des annexes

Annexe 1

The Manifesto for Agile Software Development

Seventeen anarchists agree:

We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

- Individuals and interactions over processes and tools.
- Working software over comprehensive documentation.
- Customer collaboration over contract negotiation.
- Responding to change over following a plan. That is, while we value the items on the right, we value the items on the left more.

We follow the following principles:

- Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.
- Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.
- Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.
- Business people and developers work together daily throughout the project.
- Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.
- The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.
- Working software is the primary measure of progress.
- Agile processes promote sustainable development. The sponsors, developers and users should be able to maintain a constant pace indefinitely.
- Continuous attention to technical excellence and good design enhances agility.
- Simplicity.the art of maximizing the amount of work not done.is essential.

- The best architectures, requirements and designs emerge from self-organizing teams.
- At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.

Kent Beck, Mike Beedle, Arie van Bennekum, Alistair Cockburn, Ward Cunningham, Martin Fowler, James Grenning, Jim Highsmith, Andrew Hunt, Ron Jeffries, Jon Kern, Brian Marick, Robert C. Martin, Steve Mellor, Ken Schwaber, Jeff Sutherland, Dave Thomas
www.agileAlliance.org

Annexe 2

ISO 24760

(Table des matières)

Annexe 3

ISO-27002

(Table des matières – Chapitre 11)

Annexe 4

Carte heuristique QSOS de maturité

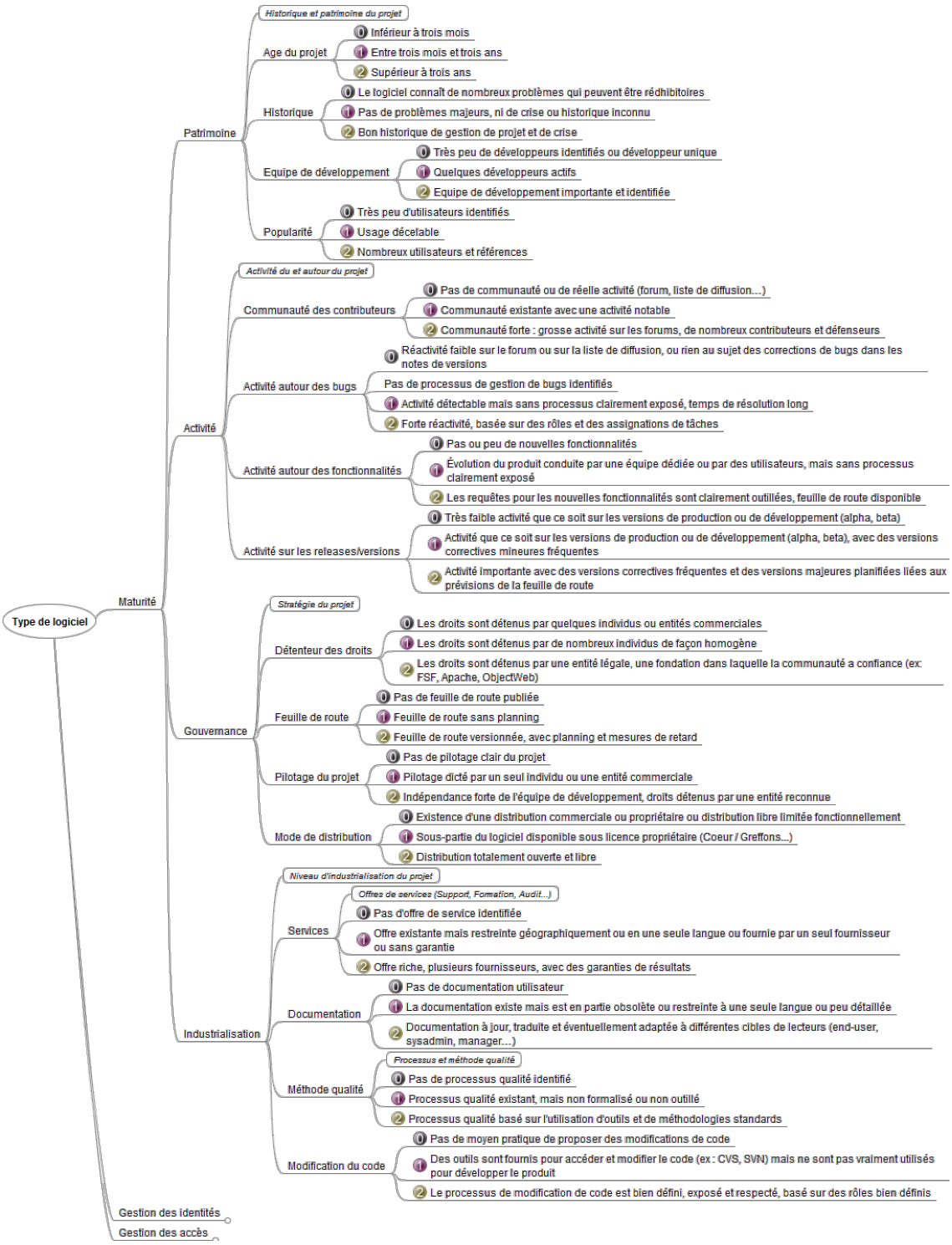


Figure 105 - Carte heuristique QSOS de maturité

(source : http://www.qsos.org)

Annexe 5

Grille d'évaluation technique

Les critères de la grille d'évaluation sont issus en partie du cahier des charges de gouvernance des accès mis à disposition gratuitement par la société guidescomparatifs.com.

1. Gestion des identités

Tableau XXVIII - Grille d'évaluation technique : Référentiel intégré

Critères	Compléments	Coefficient
La solution peut-elle utiliser un référentiel intégré ?	Annuaire LDAP Base de données relationnelle Autres :	4
La solution est-elle compatible SAML ?	Compatible CAS, Sihbboleth ?	4

Tableau XXIX - Grille d'évaluation technique : Connecteurs

Critères	Compléments	Coefficient
Quels sont les connecteurs vers d'autres annuaires supportés ?	Active Directory Microsoft Exchange NIS OpenLDAP V3 Autres:	5
Quels sont les connecteurs fichiers supportés ?	Attribute-value pair text files Delimited text file Fixed-width text files LDIF Autres :	4
Quels sont les connecteurs bases de données supportés ?	Microsoft SQL Server Oracle Database MySQL PostgreSQL Autres	5

Critères	Compléments	Coefficient
Quels sont les autres connecteurs supportés ?	DSML 2.0 SAP Autres	2
Peut-on développer ses propres connecteurs ?		5
La solution permet-elle de détecter des changements dans les sources de données ?		4

Tableau XXX - Grille d'évaluation technique : Transformation

Critères	Compléments	Coefficient
La solution permet-elle de traiter les données en entrée et en sortie d'un connecteur ?	Concaténation de chaîne Opérations arithmétiques Extraction de chaînes Autres :	5
Quel langage de programmation est supporté pour le traitement des données ?	Perl PHP C, C++ C# Visual Basic C#.Net XSLT Java JavaScript Autres	4

Tableau XXXI - Grille d'évaluation technique : Provisioning

Critères	Compléments	Coefficient
La synchronisation des informations est-elle gérée par la solution ?	De manière événementielle Nécessite des actions manuelles Autre(s) :	5
La solution permet-elle de créer, supprimer et modifier des entrées dans les applications via les connecteurs ?		2

Critères	Compléments	Coefficient
La solution permet-elle de mettre en place un processus de création, modification ou suppression des comptes applicatif au travers des différents connecteurs (par exemple, création de l'entrée dans l'application de ressources humaines en premier, puis dans Active Directory, puis dans Novell Netware) ?	Par configuration graphique Par programmation au niveau des règles de jointure et de transformation	5
La solution permet-elle de créer des comptes en masse ?		2
La solution permet-elle d'anticiper la création de compte ?		2
La solution permet-elle la création de comptes de test ?		2
La solution permet-elle de propager les informations rapidement ?	En moins de 30s En temps réel Sur évènement	5
La solution permet-elle de désactiver temporairement un utilisateur ou un groupe (pas d'authentification possible) ?	Période de désactivation Désactivation d'un utilisateur Désactivation d'un groupe ou d'un rôle Autre(s)	5

2. Gestion des accès

Tableau XXXII - Grille d'évaluation technique : Gestion des rôles

Critères	Compléments	Coefficient
La solution supporte-t-elle des rôles ?	Groupe dynamique Groupe dynamique avec mise à jour automatique d'un attribut pour tous les utilisateurs	4
La solution permet-elle de renommer les rôles selon un langage métier ?		2
La solution permet-elle de prendre en compte la séparation des responsabilités dans la définition des rôles ?		1
La solution permet-elle de définir des exceptions à l'intérieur de rôles paramétrés ?		3
La solution permet-elle de gérer l'intégrité référentielle (suppression automatique d'un membre d'un groupe en cas de		2

Critères	Compléments	Coefficient
suppression de l'entrée utilisateur associée) ?		

Tableau XXXIII - Grille d'évaluation technique : Gestion des habilitations

Critères	Compléments	Coefficient
La solution permet-elle d'envoyer régulièrement aux utilisateurs une revue des utilisateurs sous leur responsabilité, afin de leur faire valider ou invalider les accès de leur équipe ?	Peut-on définir -la fréquence ? -la forme ? -le périmètre ? Autre(s) paramètre(s)	3
La solution est-elle en mesure de mettre en œuvre des processus d'escalade dans le processus de certification des habilitations ?	Exemple: pour procédure provisoire de délégation lors de l'absence du DU	2
La solution produit-elle un reporting sur les revues d'habilitation ?		2
La solution permet-elle de générer des alertes ?	Temps donné au processus de certification Niveaux d'habilitations Habilitations exceptionnelles Autre(s) :	3
Lors de l'autorisation d'une personne à accéder à une application, une fonction de workflow est-elle disponible pour informer et faire valider par les personnes habilitées l'autorisation de cet accès ?		4

Tableau XXXIV - Grille d'évaluation technique : Gestion des mots de passe

Critères	Compléments	Coefficient
La solution permet-elle de chiffrer les mots de passe ?	Uniquement stocké dans LDAP	5
La solution gère-t-elle l'historique du mot de passe ?		2
Si Oui, peut-on paramétrer la limite de l'historique (par exemple, 10 derniers)		2
La solution permet-elle de gérer le changement du mot de passe ?	Sésame V2	5

Critères	Compléments	Coefficient
Si Oui, peut-on forcer le changement du mot de passe à la première connexion ?		1
En cas de gestion de mot de passe, peut-on forcer le changement du mot de passe régulièrement ?		1
La solution gère-t-elle l'expiration du mot de passe ?		1
La solution permet-elle de contrôler le contenu du mot de passe ?	Sésame V2	5
La solution permet-t-elle le blocage d'un compte en cas d'erreur de mot de passe ?	Nombre de tentatives Délai entre deux tentatives Autres :	1
La solution pert-elle de synchroniser les mots de passe avec Active Directory ?	Sésame V2	4

Tableau XXXV - Grille d'évaluation technique : Contrôle et traçabilité

Critères	Compléments	Coefficient
La solution dispose-t-elle de fonctions de traçabilité ?	Peut-on définir -la fréquence ? -la forme ? -le périmètre ? Autre(s) paramètre(s)	4
Quels sont les événements couverts par le module de traçabilité ?	Authentification Gestion de mot de passe Workflow d'approbation Modification de rôle Autre(s)	2
Quel est le mode de gestion du module de supervision/traçabilité ?	Traçabilité passive Gestion d'événement / réactivité sur événement	3
Dans le cas d'une gestion réactive sur événement, quel est le périmètre couvert par le déclenchement d'action ?	Echec sur identification (par exemple 3 échecs + 1 réussite sur 1 minute peuvent laisser supposer une tentative d'intrusion) Autre(s)	2
Quelles sont les actions possibles déclenchées par le module de supervision actif ?	Envoi de mail Déconnexion d'accès	3

Critères	Compléments	Coefficient
	Autre(s)	
La solution dispose-t-elle de modèles de rapports prédéfinis ?		1

Liste des figures

Liste des tableaux

Gestion des identités et des accès pour le système d'information du CNRS

Mémoire d'Ingénieur C.N.A.M., Paris 2013

RESUME

Le CNRS souhaite se doter d'un outil pour mettre en œuvre telle politique de gestion des identités et des accès. L'objectif est de garantir que chaque personne qui travaille pour l'établissement bénéficie des moyens nécessaires pour réaliser sa mission.

L'étude de faisabilité de ce projet est l'occasion de définir un langage commun relatif aux concepts manipulés et d'établir une cartographie des processus existants qui sont impliqués dans l'administration des comptes utilisateurs.

Ce mémoire s'attache à présenter les différents aspects de ce projet, depuis l'étude de l'état de l'art jusqu'au choix d'une solution et à la réalisation d'un démonstrateur.

Mots clés : gestion des identités et des accès, identité, sécurité, compte, utilisateur, open source, maturité

SUMMARY

CNRS wants to acquire software to implement an identity and access management governance. The goal is to ensure that each person who works for the organisation has the capacity to achieve his mission.

The feasibility study of this project is an opportunity to define a common language for the handled concepts and to establish a mapping of the existing processes involved in the user account management.

This engineer report plans to present the various aspects of this project, since the study of the state of the art until the selection of the solution and the development of a proof of concepts.

Keywords: identity and access management, identity, security, account, user, open source, maturity