ENCORA : Organisation et architecture de l'E.N.T. ENCORA

Christian Lenne
Département Réseau du C.I.C.G. / Université Joseph Fourier
351 Avenue de la Bibliothèque – Domaine Universitaire – BP 53 – 38041 Grenoble Cedex 9
Christian.LenneATgrenet.fr
date : 29 septembre 2003

Dominique Merle
SUN Microsystems – Professional Services
Dominique.MerleATsun.com

Stéphane Pichevin
SUN Microsystems – Professional Services
Stephane.PichevinATsun.com

Résumé

Le projet ENCORA est un des 4 projets retenus dans le cadre de l'appel d'offre FRT sur les Espaces Numériques de Travail (E.N.T.). Il est porté par le GIP CURA (Conférence Universitaire Rhône-Alpes) qui regroupe 13 établissements de la région en partenariat étroit avec deux industriels : SUN Microsystems et Ever Team. Le projet affiche très clairement le positionnement de services de l'ENT à deux niveaux : celui de chaque établissement et un niveau commun qui peut être interuniversitaire, voire régional.
Cet article présente, d'abord l'organisation du projet, sa démarche, les choix effectués et dans une deuxième partie présente les mécanismes utilisés pour la mise en place de l'ENT, l'architecture de ce dernier et donne des abaques pour calibrer l'ENT suivant les organisations et les populations traitées.

Mots clefs

Espace Numérique de Travail, Environnement Numérique de Travail, ENT, Portail, Authentification Unique, Single Sign One, SSO

1 Introduction

Le projet ENCORA (Environnement Numérique du Campus Ouvert Rhône Alpes) vise à la mise en place d'une architecture opérationnelle d'Espaces Numériques de Travail (ENT) permettant d'offrir des services à l'attention des acteurs de l'enseignement supérieur et la recherche : les étudiants, les personnels administratifs et techniques et les enseignants chercheurs. Il propose une architecture de base que nous appellerons socle sur lequel viennent se connecter des briques métier.
L'approche suivie a été de constituer un consortium composé du GIP CURA (Conférence Universitaire Rhône-Alpes) regroupant 13 établissements d'enseignement supérieur et de recherche, la société SUN Microsystems pour l'apport de sa technologie sur le socle de base et la société Ever Team pour sa technologie d'intégration de services métier et pour son expérience en portail documentaire et sa capacité de diffusion.
Cet article aborde 2 aspects différents visant à montrer, d'une part la démarche qui a conduit à l'affinage du projet et à sa définition précise, d'autre part l'approche plus technique expliquant l'architecture logique du socle et la description plus fine de la fonction de gestion de profils en relation avec l'annuaire LDAP Agalan/SupAnn.

2 Démarche

Après la notification par le ministère de la sélection du projet (été 2002), il a été nécessaire de travailler sur l'organisation et la mise en place d'un tel projet, vaste par ses aspects techniques et complexe dans sa géographie qui regroupe 13 établissements de différentes natures (scientifique, littéraire, pluridisciplinaire, …), d'organisations différentes et de culture technique différente. Nous nous attacherons ici à l'organisation mise en place pour établir le cahier des charges précis de la définition de l'ENT.

2.1 Recadrage du projet

Cette première période du projet a été consacrée à son recentrage en fonction des moyens globaux alloués. Cette période a été mise à profit pour, d'un côté préciser les accords de partenariat qui n'avaient pas été poussés jusqu'à leur terme, ce qui est normal dans une phase de proposition et d'un autre côté affiner le cahier des charges et l'architecture qui en découle.
Les discussions concernant les accords de partenariat ont porté sur le budget, les droits de propriété, le coût des licences logicielles pour le futur et les conditions de maintenance.
Concernant l'affinage du cahier des charges, le périmètre a été revu pour permettre une plus grande souplesse dans la mise en place des instances de l'ENT ENCORA. Ce travail a permis à un premier ensemble de 9 établissements sur les 13 que compte la CURA de se prononcer favorablement sur le montage final. Ce dernier prévoit la possibilité d'instanciation pour un établissement en particulier ou pour un ensemble d'établissements dont les relations liées à l'enseignement et à la recherche nécessitent des partages d'accès. En effet, il est fréquent sur une académie, d'avoir des filières d'enseignement ou des formations communes (en particulier au niveau des 2ème et 3ème cycles) ou d'avoir des enseignants qui interviennent dans plusieurs établissements. L'ENT peut alors se décliner selon une architecture permettant une identité propre de l'établissement dans la forme et dans la spécificité des formations qui pourront nécessiter des outils propres, mais également d'avoir des authentifications et des outils partagés. L'authentification se fera en prenant en compte les informations contenues dans l'annuaire LDAP des établissements. Cette mutualisation pourra, dans le futur, se mettre en place au niveau régional lorsque les interactions pédagogiques entre les établissements de l'académie de Grenoble et ceux de l'académie de Lyon seront plus développées.
Pour valider cette approche et prendre en compte les spécificités et modes de fonctionnement locaux, il a été décidé de mettre en place deux pilotes. Le premier pilote est une instanciation du socle technique fourni par SUN sur une plateforme Linux. Elle sera déployée pour l'université de Lyon 2. La seconde, instanciée pour un niveau mutualisé sur Grenoble, l'est sur une plateforme Solaris.
Concernant les briques métier, force est de constater la différence d'approches et donc d'utilisation d'outils, qui nécessite une implication de chaque établissement pour le développement ou l'adaptation des briques spécifiques à son organisation. L'apport d'Ever Team à ce niveau est la technologie EverSuite [1] qui va permettre d'intégrer dans le pilote grenoblois la brique « Offre de Formation » faisant l'objet du projet PROF développée pour la présentation de cette dernière lors du passage au LMD de deux des cinq établissements de l'académie de Grenoble. Ever Team va également mettre en place les connecteurs nécessaires à la consultation des bases documentaires locales. Il faut noter qu'un appel d'offre touchant au bureau virtuel étudiant est (à l'heure où l'article est écrit) en cours de publication de la part du Conseil Régional Rhône-Alpes. Ce dernier devrait normalement déboucher sur l'acquisition, sous une forme à préciser, d'un bureau virtuel s'intégrant harmonieusement dans l'ENT.

2.2 Organisation et spécifications générales

Le recadrage du projet, mais surtout l'affinage des fonctionnalités à mettre en place sur l'ENT final, ont conduit à rebâtir un nouveau cahier des charges. Pour avancer rapidement sur ce dernier, l'approche suivie dans le projet stratégique du portail Greco a été suivie[2]. Le découpage proposé dans la soumission de l'appel à projet a été révisé. Treize groupes de travail ont été formés pour préciser les besoins. L'ensemble de ces treize groupes a été scindé en deux paquets : le premier pour traiter des problèmes techniques et d'exploitation de l'ENT une fois en place, le second pour définir les fonctionnalités des différentes briques métier. Nous présentons rapidement les différents sous projets en commençant par les aspects métier qui ne seront pas repris dans cet article. Le nombre de participants indiqué ici précise le nombre de personnes ayant participé à la rédaction du cahier des charges. Les descriptions données dans cet article ont été prises, pour certaines, intégralement dans le document d'expression des besoins produit dans la phase de spécification.

- Bureau virtuel : un groupe de 7 personnes a défini les fonctions du bureau virtuel fourni dans l'ENT. Ce sous-projet spécifique fait l'objet d'un appel d'offre particulier piloté par le Conseil Régional Rhône-Alpes.
- Usages et bureautique (5 personnes) : la notion de bureautique et les usages associés dans un ENT peuvent couvrir un espace très variable en fonction du point de vue selon lequel on se place :
  - espace restreint aux suites de bureautique (c'est négliger le fait que les outils de bureautique servent pour la production administrative, scientifique et pédagogique)
  - espace très large couvrant l'ensemble des outils numériques de bureau utilisés pour la production, le suivi et la gestion de documents texte, graphiques ou multimédia.

  Il est prévu de pouvoir offrir les principales fonctions de bureautique : traitement de texte, tableur, création de présentations, traitement de dessins et images (pixmaps), traitement de dessins et images (vectoriel), construction de pages Web (statiques, dynamiques), atelier auteur (y compris production de « media riches » SMIL ou autres), outil de scénarisation, éditeur bas niveau, navigateur Web et à plus longue échéance des outils de traitement et de manipulation des sons et de la vidéo.

- Scolarité (11 personnes) : le groupe de travail a visé spécifiquement la définition, si nécessaire le développement, l'intégration et la mise en œuvre dans le portail de services liés aux opérations administratives de gestion de la scolarité des étudiants ; ils comprennent un volet information et un volet destiné à faciliter les procédures administratives et pédagogiques :
  - informations en amont sur les conditions, les procédures et les dates d'inscription à l'Université,
  - demandes de dossier, procédures de pré inscription ou d'inscription en ligne,
  - informations sur la rentrée,
  - informations sur les modalités de contrôle des connaissances, sur les règlements d'examens,
  - emplois du temps, dates d'examens,
  - accès au dossier étudiant, en particulier notes et résultats,
  - demandes de documents officiels (attestations et certificats divers, diplômes).
- Offre de formation, offre d'emploi et de stages (7 personnes) : les besoins exprimés par le groupe de travail a surtout porté sur l'analyse des outils existants en matière d'offre d'emploi et de stages dans différentes composantes d'établissements de la région. L'offre de formation doit intégrer le LMD. Concernant les établissements de l'académie de Grenoble, le projet d'offre de formation en est à la définition de la deuxième version (la première est en fonction depuis juillet dernier). Elle sera en ligne au printemps prochain. Bien entendu, cette « brique » a été pensée pour s'intégrer au socle ENCORA.
- Documentation (12 personnes) : l'objectif du groupe de travail était de décrire le contenu et les fonctionnalités de la " Bibliothèque " de l'espace numérique de travail ENCORA et plus particulièrement d'identifier les services mutualisables à l'échelle régionale et de définir un schéma d'interopérabilité entre l'offre documentaire d'ENCORA et celle des établissements. Les missions de la brique documentaire ont été identifiées comme suit :
  - gérer et communiquer des documents de différente nature,
  - participer à la recherche, à la diffusion et à la production de l'Information Scientifique et Technique,
  - former les utilisateurs aux nouvelles techniques d'accès à l'information,
  - fournir des outils permettant d'accéder à l'information.
- Vie apprenante : (12 personnes) : de nombreux systèmes de « E-learning » sont déjà en usages dans les différents établissements et écoles. Ils ont été estimés à une vingtaine. Ceci se traduit par un existant en terme de contenu pédagogique numérique hétérogène et difficile à migrer. Pour prendre en compte cette donnée, il a été décidé de limiter ENCORA à un ensemble de briques de services, de documentation et de moyens pour pourvoir intégrer au mieux les différentes plateformes existantes. C'est la notion « d'encorisation » qui a été mise en avant, sachant qu'un des problèmes qui se pose est la redondance et la cohérence de fonctions entre ces plateformes et le bureau virtuel (i.e. messagerie, forum, …).
- Vie universitaire (6 personnes) : sur cet aspect, le travail mené a plus été une analyse des pratiques car il y avait déjà 2 sites en place. Cet aspect informationnel couvre les informations et les services liés à la vie pratique de l'étudiant (logement, santé, culture, vie associative et culturelle, etc.), actualités et agendas de la vie universitaire, informations et services nécessaires aux futurs étudiants sur ces mêmes thèmes.

Pour les sous projets à dominante plus technique, l'expression des besoins s'est faite en 5 sous-projets, plus un à la charnière des deux groupes devant définir les grands principes de l'architecture externe et les interfaces ainsi que la taxonomie de la population concernée en les groupant par communautés et en leur associant des profils par défaut.

- Architecture externe, interface, communauté et profil utilisateurs : 12 personnes constituaient le groupe. Ce sous-projet avait la charge de concevoir, mettre en œuvre et évaluer l'Interface Homme Machine (IHM) des services du portail : il a défini les principes généraux de structuration du portail tel que la percevra l'utilisateur, son ergonomie et prend en compte l'accessibilité pour des utilisateurs ayant des contraintes particulières (handicap, langue, etc.).
- Infrastructure, architecture et intégration (11 personnes) : ce sous-projet, clé de voûte de l'ENT a eu pour objectif la définition et de la mise en place de l'architecture informatique (matérielle et logicielle) du portail. Il assure l'accès au portail pour tous les utilisateurs.
  Il a traité les problèmes d'intégration des composants, modules, outils développés ou fournis tels qu'ils ont été définis par les autres sous-projets. C'est ici que sont précisés les règles et standards à respecter pour qu'un module soit « intégrable », « inter opérable » ou simplement « accessible ». C'est aussi au niveau de ce sous-projet que sont définies les structures de conservation nécessaires au fonctionnement du portail (profils, annuaires, ...).
  Annuaire et gestion des groupes et usagers (5 personnes) : le modèle d'annuaire ENCORA retenu est celui de SupAnn [3], ceci, afin de permettre en fin de projet une instanciation possible du projet ENCORA à tout établissement suivant le schéma SupAnn recommandé par le ministère. L'annuaire SupAnn de l'établissement sera l'interconnexion pour le projet d'environnement numérique. En particulier les groupes seront répercutés dans l'annuaire SupAnn de manière automatique donc à la charge de l'établissement. Notons malgré tout, que l'annuaire en place dans tous les établissements de l'académie de Grenoble et à Lyon 2 est un annuaire SupAnn enrichi, plus exactement un annuaire AGALAN [4] constituant un sur ensemble de SupAnn dont il reprend les attributs. Cet annuaire sera utilisé par les mécanismes SSO

(identification unique) nécessaires aux identifications à travers les portails (portail d'établissement, portail ENCORA). L'annuaire permet la gestion des groupes et les droits associés, il permet la délégation de cette gestion. Les groupes pourront être constitués d'objets de même type situés dans plusieurs établissements.

- Point d'accès unique et authentification (9 personnes) : l'ENT offrant l'accès à des données personnelles il est nécessaire d'identifier les utilisateurs et de vérifier leur identité. A cet effet, on souhaite vivement une authentification unique pour l'ensemble des services, c'est-à-dire un seul mode d'authentification valable pour tous les services et une seule authentification par session d'utilisation de l'ENT. En revanche, l'ensemble des services ne sera pas accessible à tout le monde, et l'ENT gérera les autorisations. C'est le rôle du serveur de profils qui sera décrit plus longuement dans la deuxième partie.
- Organisation et mise en œuvre de l'environnement de production (6 personnes): la section 03 donne plus de détail sur la problématique d'exploitation d'un tel outil dans un contexte universitaire. Nous montrons dans cette section l'approche suivie.
- Industrialisation et déploiements : le groupe de 7 personnes a fixé le cadre pour établir des règles de calcul permettant à chaque établissement ou groupement d'établissements d'estimer les impacts de la mise en place des différents sous projets d'ENCORA sur son infrastructure réseau.

2.3 Architecture fonctionnelle

Le degré de mutualisation des ressources informatiques étant variable suivant les plaques métropolitaines en place (Lyon, Saint Etienne, Grenoble, Chambéry), l'architecture a été pensée pour permettre une grande souplesse dans le déploiement. La Figure 1montre la répartition des deux niveaux de portail : mutualisé et propre. Sur ce schéma, les boites en couleur dégradée (Portail et site institutionnel interuniversitaire) mettent en évidence les « agrégations » des deux niveaux de portail. Pour un établissement seul, les fonctions de serveur d'identité et la base de profil sont intégrées à l'environnement local.
Le site institutionnel interuniversitaire est facultatif, il n'est nécessaire que si le groupement d'établissements veut donner une visibilité à sa présence.
Le point d'entrée du portail est systématiquement celui du portail de l'établissement. Ceci permet un niveau de mutualisation allant du regroupement d'une entité à un regroupement de l'ensemble des acteurs de la région. Dans un premier temps, les deux pilotes mis en place vont permettre de valider cette architecture. En effet, l'université de Lyon 2 va déployer son portail, les établissements grenoblois vont quant à eux fournir un portail mutualisé.

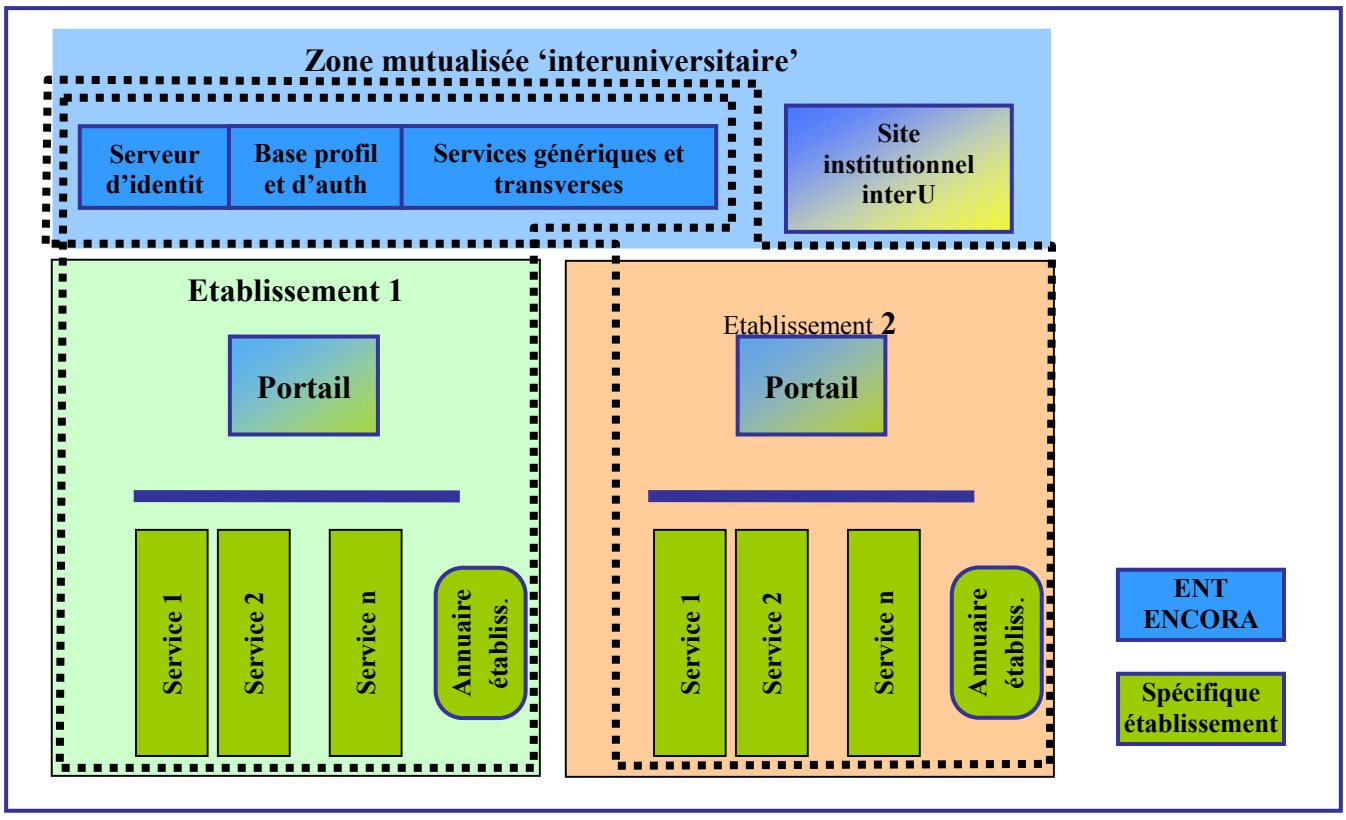

Figure 1 – *Architecture fonctionnelle de l'ENT*

3 Problématique de déploiement et d'exploitation

Lorsque l'on demande aux « utilisateurs » leur vision de la disponibilité d'un tel environnement, il y a un consensus : 24H/24, 7J/7, 365J/an. Prendre cette contrainte au pied de la lettre entraîne une architecture du système entièrement redondée et une organisation de l'exploitation complexe. Pour évaluer les besoins réels, nous avons cherché à préciser ces notions de disponibilité pour lesquelles une baisse même légère du niveau d'exigence modifie fortement l'architecture et l'exploitation. Par manque de place, nous ne donnons ici que les définitions de contraintes qui ont été retenues, tant sur la disponibilité que sur la qualification nécessaire des personnels en charge de l'exploitation. Pour chaque composant de l'ENT, nous avons ensuite attribué les contraintes supportables ce qui nous a permis d'en déduire les contraintes matérielles et l'organisation humaine à mettre en place.
Le mode de fonctionnement de nos établissements nécessite un découpage de la semaine en tranches horaire pendant lesquelles la disponibilité peut varier. En fonction des tranches horaires, la qualification des personnes en charge de l'exploitation peut être différente afin de pouvoir mettre en place des mécanismes d'astreinte, de sous-traitance, d'infogérance voire d'externalisation. Le tableau ci-dessous décrit le découpage pour couvrir les périodes de journée en jour ouvré, les nuits, le samedi matin ou le reste du week-end.

Indice	Explication abrégée	Caractéristique de la disponibilité
H1	Minuit-Minuit	Une intervention est possible dans les 2 heures
H2	8H-20H	Une intervention est possible quasi instantanément
H3	8H-12H 13H-18H	Une intervention est possible quasi instantanément
H4	8H-12H	Une intervention est possible dans les 2 heures
H5	18H-8H	Une intervention de type « presse-bouton » est possible dans l'heure.
H6	12H-8H	Une intervention de type « presse-bouton » est possible dans l'heure.

La définition de ces tranches horaires nous permet maintenant de définir des indices de priorité en précisant pour chacun d'entre eux leur signification. Ainsi, on trouvera qu'un indice de disponibilité dit de « 24H/24-7j/7 » autorise dans notre environnement, soit une indisponibilité courte due à une panne, soit à une indisponibilité due à un arrêt planifié du service, comme par exemple les évolutions de versions.

Indice	Explication abrégée	Caractéristique de la disponibilité
1	24H/24-7j/7	La disponibilité demandée est très grande. Il s'agit d'un service continu, hautement fiable. L'arrêt du système ne se fait que de façon programmée sur 3 jours par an. Le taux de panne ne peut excéder 3 jours cumulé par an ce qui correspond à un taux de disponibilité de 0,9835 (359/365). A cela il faut rajouter que la durée consécutive d'une panne ne peut excéder 8 heures. Le service s'entend sur la tranche horaire H1.
2	24H/24-6j/7	La disponibilité demandée reste forte. Il s'agit d'un service continu, très fiable. L'arrêt du système ne se fait que de façon programmée sur 3 jours par an. Le taux de panne ne peut pas excéder 3 jours cumulé par an ce qui correspond à un taux de disponibilité de 0,9835 (soit 359J/an). A cela, il faut rajouter que la durée consécutive d'une panne ne peut excéder 36 heures. Le service s'entend sur la tranche horaire H2 en jours ouvrés et en H4 le samedi.
3	Heures ouvrables	La disponibilité demandée est malgré tout forte. Il s'agit d'un service continu, fiable. L'arrêt du système ne se fait que de façon programmée sur 3 jours par an + une indisponibilité de service pendant des tranches horaires creuses pour des sauvegardes. La durée consécutive d'indisponibilité peut durer une nuit ou un week-end. Le service s'entend sur la tranche horaire H3 des jours ouvrés.
4	Au mieux	On fait au mieux durant les heures H3 en jours ouvrés. Moins de contraintes sont données pour les maintenances et les sauvegardes.

A partir de ces définitions, nous avons découpé l'ENT en ensemble de services (authentification, accès aux serveurs, outils de communication, outils de bureautique, sauvegarde / archivage, …) et nous avons demandé à la maîtrise d'ouvrage de définir l'indice de disponibilité à différentes échéances : Mise en place (T0), T0 + 24, T0 + 42 et T0 + 60 pour prendre en

compte les évolutions d'infrastructure nécessaires au niveau requis et étaler les investissements dans le temps. Nous avons également donné les contraintes imposées à l'établissement sur tout ce qui touche la fiabilité du réseau, des fluides (refroidissement, électricité), … pour être cohérent avec les exigences demandées. Il est inutile de vouloir une disponibilité permanente, par exemple si le courant est secouru par des onduleurs d'une durée de 30 mn ou si l'accès à la salle machine est impossible la nuit. Tous ces éléments ont été pris en compte pour arriver à un équilibre entre coût des équipements et exploitation. D'une manière générale, on peut dire qu'une forte disponibilité implique obligatoirement une redondance des équipements actifs (réseau ou serveur). Pour certaines fonctions, la solution s'impose (répartiteurs de charge, batterie de serveurs, …).

La suite de ce papier constitue la deuxième partie de l'article et s'attache plus particulièrement à donner les éléments techniques de l'ENT ENCORA.

4 Description générale

L'ENT est un espace constitué à la fois de composants nouveaux apportés par le projet ENCORA et d'un existant à intégrer et à rendre accessible.
Comme indiqué, le périmètre de l'ENT est à la fois vaste, évolutif et dépendant de chaque établissement. Nous proposons dans ce paragraphe de détailler les éléments apportés par le projet ENCORA et d'illustrer le principe d'intégration de services existants à l'ENT. Il est important de bien faire la distinction entre :
- le socle technique,
- les services d'ENCORA,
- les services existants.

4.1 Socle technique

Le socle technique est l'infrastructure permettant l'accès aux services de manière sécurisée et personnalisée. Il fournit en particulier les services de base suivants :
- une infrastructure d'intégration et de présentation de services Web sous forme de « portlet ». Cette infrastructure permet également d'intégrer des services de type client – serveur, moyennant quelques conditions sur les protocoles utilisés (utilisation d'un port fixe, Transport TCP),
- une présentation personnalisée :
  - par établissement : respect de la charte graphique et de l'identité visuelle,
  - par utilisateur : présentation des informations pertinentes pour un utilisateur, en fonction de ses droits et de ses préférences,
- accès sécurisé depuis l'établissement (**intranet**) ou depuis **Internet,**
- sécurisation de toutes les connexions par chiffrement (**SSL**),
- une utilisation des données utilisateurs de **l'annuaire LDAP d'établissement** respectant les préconisations SupAnn,
- un principe d'**authentification** suivant le principe « identifiant / mot de passe »,
- une solution d'authentification unique (**Single Sign On**) et de propagation de jeton de session,
- la gestion des **droits applicatifs** et la notion d'autorisation associée,
- la fourniture d'un outil de **gestion des utilisateurs** et des services intégrés,
- la possibilité d'effectuer de la **délégation d'administration** tant sur les données utilisateurs que sur les droits applicatifs,
- le **contrôle** de la durée des **sessions**, avec une personnalisation service par service,
- la capacité à **tracer** l'ensemble des accès via le socle.

Le socle technique repose sur l'offre logicielle Sun ONE, à savoir les produits suivants :
- Sun ONE Portal Server : présentation, personnalisation et intégration des services,
- Sun ONE Identity Server : gestion des droits applicatifs, authentification unique, interfaces de gestion,
- Sun ONE Directory Server : annuaire LDAP.

4.2 Les services d'ENCORA

Par essence, les services d'ENCORA sont amenés à s'enrichir et à évoluer. Nous présentons dans ce paragraphe les services de communication qui sont apparus comme ceux devant naturellement être présents dès la première version du projet.
Les services identifiés lors des réunions de travail sont les suivants :
- **messagerie**, avec un accès en interface Web (webmail) et un accès client lourd (protocole IMAP ou POP),

- annuaire de type « **Pages Blanches** », permettant des recherches sur l'annuaire de l'établissement suivant différents critères, voire interuniversitaire,
- **agenda** partagé permettant à la fois une gestion pratique (emplois du temps, salles de cours, …) mais également des événements extra universitaire (événements, séminaires, expositions, …) et la notification,
- **carnet d'adresses** personnelles stocké sur le serveur et accessible depuis une interface Web,
- Gestion de son compte : chaque utilisateur à la possibilité de modifier un certain nombre de ses propres attributs,
- **messagerie instantanée** (chat): il s'agit d'un outil de communication de plus en plus utilisé y compris dans les milieux professionnels,
- **espace de stockage** au sens large permettant en particulier de partager des espaces de travail. Cet espace de travail peut être accédé par différents protocoles et protégés par des règles d'accès,
- **page Web personnelle** : chaque utilisateur de l'ENT aura la possibilité de créer sa propre page Web,
- **canaux d'informations** : il s'agit de l'agrégation personnalisée d'informations disponibles sur l'intranet,
- **moteur de recherche** sur l'intranet,
- Possibilité de gérer des **groupes** : il s'agit d'un outil essentiel afin de créer des règles applicatives ou des communautés d'intérêts,
- Service de publication de contenu Web,
- Forum.

Ces services de communications peuvent être envisagés au sein strictement d'un établissement, mais également dans une logique interuniversitaire. Dans la première ébauche d'architecture, une solution à base de technologies Sun ONE pour fournir une partie des services (messagerie, calendrier, hébergement de pages personnelles ou plus généralement l'hébergement de sites Web, messagerie instantanée, Proxy cache pour la navigation Internet) et de produits libres (outils de publication comme SPIP, de listes de diffusion comme SYMPA, News, TWIKI, …) est envisagée.

4.3 Les services existants

Les services existants sont les plus nombreux et les plus variés. Dans une démarche fédérée rassemblant autant d'établissements d'origines aussi diverses, il est extrêmement délicat de recenser une liste de services existants consensuelle, et d'en extraire les plus représentatifs.
Les services existants correspondent à des applications du système d'informations qui ont vocation à être intégrés à l'ENT d'un point de vue fonctionnel. Les services concernés sont extrêmement divers et l'effort d'intégration au socle technique dépend de différents critères : technologies utilisées pour l'application, mécanisme d'authentification, modèle d'accès et droits applicatifs, niveau de présentation en terme d'interface graphique, …
Le choix des services à intégrer, le niveau d'intégration ainsi que le calendrier d'intégration appartiendra à chaque établissement de manière individuelle. Pour certaines applications que l'on retrouve dans différents établissements, Arpège ou Apogée par exemple, la mutualisation des efforts sera possible.
Les deux pilotes mentionnés en 2.3 correspondent à deux sélections personnalisées d'intégration de services.

5 Architecture générale

Le schéma d'architecture donné dans la Figure 2 est la représentation de l'implémentation du portail pour un établissement donné. Pour en simplifier la lecture, nous identifions trois zones principales que nous proposons de détailler par la suite :
- la zone établissement,
- la zone mutualisée interuniversitaire,
- la zone Internet.

Le schéma ci-dessous illustre cette architecture.

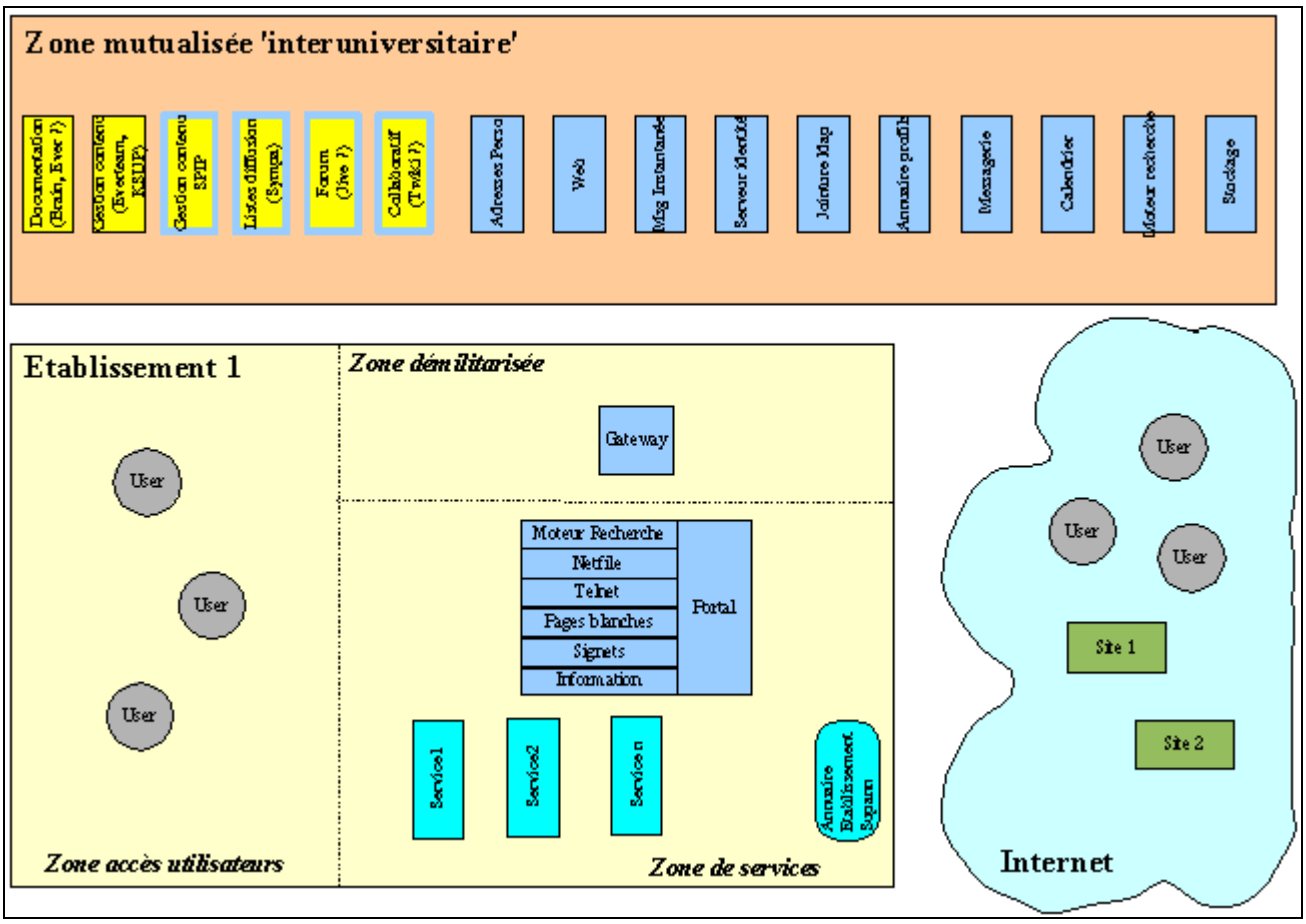

Figure 2 – *Architecture générale de l'ENT*

Nous détaillons maintenant les trois parties mises en évidence sur ce schéma à savoir, la partie établissement, la partie mutualisée et enfin tout ce qui touche l'internet.

5.1 Zone établissement

La zone établissement correspond à l'ensemble du système d'information de l'établissement. On présente ici les composants apportés par ENCORA dans l'établissement ainsi que leur positionnement. On présente également les interactions de ces nouveaux composants avec l'existant.
Classiquement, et de manière schématique, les systèmes d'information des établissements comportent 3 zones :

- une zone démilitarisée, ou DMZ, qui correspond au sas sécurisé, pour les connexions de l'établissement avec l'extérieur. On trouve dans cette zone des composants de sécurité et les données sensibles ne doivent pas exister dans cette zone,
- une zone de services qui correspond à la zone où les applications sont hébergées,
- une zone d'accès utilisateur qui correspond aux points de connexions des utilisateurs finaux.

Pour ENCORA, chaque établissement gère l'accès à son ENT et a ainsi la maîtrise de la sécurité.
Les utilisateurs peuvent se connecter à l'ENT soit depuis la zone d'accès utilisateurs, soit depuis Internet.
Toutes les connexions à l'ENT, quelle qu'en soit leur provenance, passent par la zone démilitarisée et sont prises en charge par le composant de sécurité, la « **gateway** », de Sun ONE Portal Server. La connexion entre l'utilisateur final et la gateway est chiffrée.
La gateway joue un rôle de reverse proxy et transmet les requêtes au composant de **portail**, Sun ONE Portal Server, qui se situe dans la zone de service de l'établissement. La connexion entre le portail et la gateway est en http et n'est donc pas chiffré puisqu'on est en zone de confiance.
Suite à l'authentification et à l'identification de l'utilisateur, le portail présente une vue personnalisée constituée d'un **agrégat de services et d'informations**.

Sun ONE portal Server se positionne comme couche de présentation, et n'a pas pour vocation de détenir le contenu qu'il présente. Il a donc un positionnement non intrusif sur le système d'informations et va extraire, et éventuellement remettre en forme, l'information ou le service là où elle/il se situe, à savoir dans la zone de service, dans la zone mutualisée interuniversitaire ou sur Internet. Le portail fournit lui-même un ensemble de services, représentés sur le schéma :

- moteur de recherche,
- « Netfile » : outil permettant de gérer les espaces de stockage hétérogènes et répartis, suivant le principe de « l'explorer »,
- « Telnet » : le portail propose nativement la possibilité de prendre l'accès en telnet de manière sécurisée à n'importe quelle machine de l'intranet. Cet outil repose sur la technologie de netlet,
- « pages blanches » : on peut utiliser un « portlet » classique du portail pour rendre ce service. Il est également possible d'intégrer un service Web déjà existant de l'établissement,
- signets : il s'agit d'un service standard de stockage de « favoris Web »,
- informations : « portlet » standard permettant de restituer le contenu d'une page Web au sein d'un portlet.

Le portail accède à l'information en utilisant en standard les protocoles requis par les services Web (HTTP, SOAP, …).
En synthèse, la zone établissement (Figure 3) héberge deux composants essentiels du socle technique : la gateway et le serveur de portail.

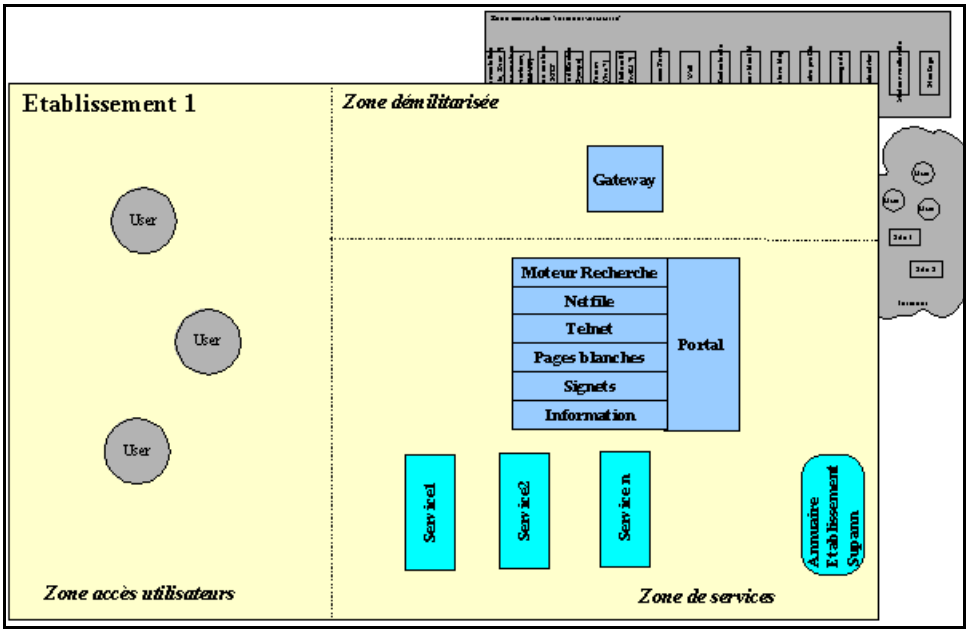

Figure 3 – *Architecture de la zone établissement*

5.2 Zone interuniversitaire

La zone mutualisée interuniversitaire (l) est par définition une zone transverse à l'ensemble des Etablissements.
Cette zone a pour vocation d'héberger :

- les nouveaux services apportés par ENCORA, dont font partie les services collaboratifs déjà décrits,
- les services, ou composants de services, destinés à une utilisation inter établissements.

Les services de la zone mutualisée interuniversitaire ne peuvent être accédés que par les portails d'établissements ou des services de l'ENT. Les utilisateurs finaux ne font aucun accès direct à ces services.

La mutualisation de cette zone présente un ensemble de bénéfices :

- une bonne qualité de service passe souvent par l'achat de matériel supplémentaire : commutateurs « intelligents », clusters, …,
- le partage de machine permet de rationaliser les investissements,
- l'exploitation de ces services demande à la fois des compétences particulières et également des notions d'astreinte,
- la limitation du nombre de sites et de machines simplifie globalement les opérations de maintenance évolutive.

Ce choix a néanmoins un certain nombre de contraintes :
- besoin en réseau entre les établissements et la zone mutualisée,
- organisation et localisation pour l'hébergement et l'exploitation de cette zone transverse.

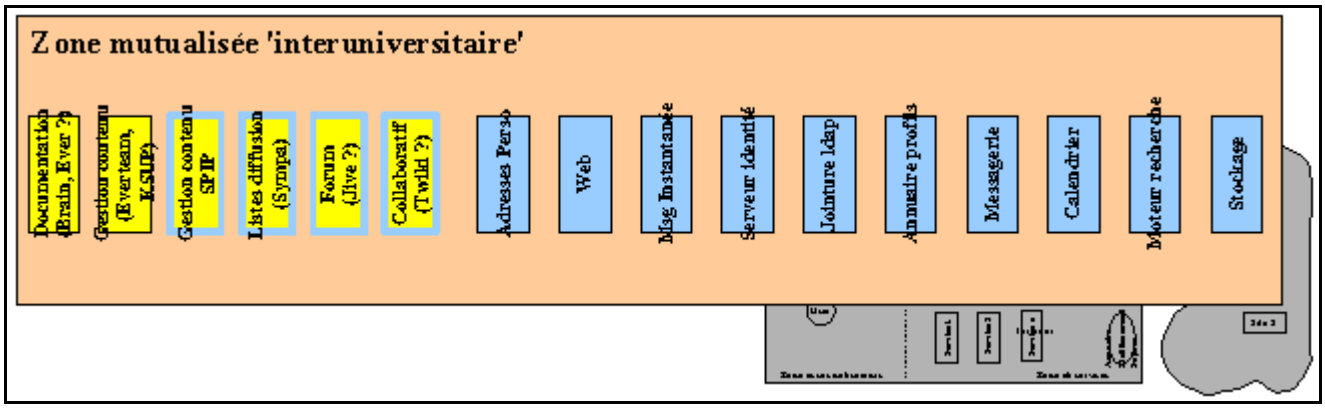

Figure 4 – *Services de la zone mutualisée*

Toutefois, il faut noter que les nouveaux services d'ENCORA sont proposés à chaque établissement mais ne sont pas imposés. Chaque établissement a la liberté de les utiliser ou pas. C'est en particulier vrai pour un service tel que le service de messagerie pour lequel l'établissement pourra soit poursuivre l'exploitation de son service actuel, soit se reposer sur la solution proposée par ENCORA.

5.3 Internet

La zone Internet est présentée à titre de zone d'interaction avec l'ENT. Les interactions sont à deux niveaux :
- point d'accès pour les utilisateurs : les utilisateurs pourront accéder à l'ensemble des services de l'ENT, de manière sécurisée, à partir de Internet,
- comme contenu restitué dans l'ENT : il est envisageable de créer des « portlet » qui présentent des contenus présents sur Internet, ou sur un réseau externe partenaire (extranet).

6 Structure technique de la couche de présentation

Sun ONE Portal Server est essentiellement constitué de deux composants logiciels, permettant la construction d'une architecture sécurisée pour l'ENT:
- la passerelle ou Gateway,
- le « Portal Server ».

6.1 Gateway

La Gateway fournit les fonctions de sécurité du portail, qui sont principalement :
- l'authentification bas niveau de la connexion (certificat serveur),
- la protection d'accès en fonction du statut de l'utilisateur (ex: non authentifié -> seules les pages de login sont accessibles) et des règles de session (ex: expiration des droits après une période définie d'inactivité),
- la gestion des autorisations associées en fonction des configurations propres à chaque utilisateur (URL policy),
- l'accès depuis Internet à des informations ou services présents sur l'Intranet (mécanisme de reverse proxy avec réécriture d'URL dans le protocole http),
- consultation de contenu HTML (via la réécriture d'URL dans les pages HTML - rproxy),
- accès à des services applicatifs de type client serveur (via le mécanisme de Netlet - eproxy).

Elle constitue le point d'accès unique à l'ENT depuis le poste client. La communication entre le poste client et la Gateway se fait exclusivement via un canal unique sécurisé sur un port bien identifié, combinant HTTPS (Secure Socket Layer) et flux netlet (MD5). La gateway se situe naturellement en zone démilitarisée.

La Netlet est une technologie spécifique destinée à intégrer au portail, de manière sécurisée, des connexions de type client-serveur en utilisant un procédé s'apparentant à du tunnelling comme le montre la Figure 5.
En l'occurrence, la Netlet est une applet Java certifiée qui se télécharge sur le poste client et ouvre, en local, un ou plusieurs port(s) TCP/IP en écoute.
Le client (lourd ou léger selon le cas) du service applicatif doit alors, être configuré spécifiquement afin de se connecter au service local fourni par l'applet, sur l'adresse IP 127.0.0.1 (localhost) et non pas sur le serveur auquel le poste est habituellement connecté.
La netlet se charge de chiffrer le flux et de le transférer à la Gateway, qui le déchiffre alors et le transmet jusqu'au serveur applicatif situé sur le réseau interne. Le flux en retour subit un traitement semblable (chiffrage par la Gateway et déchiffrage par la netlet).

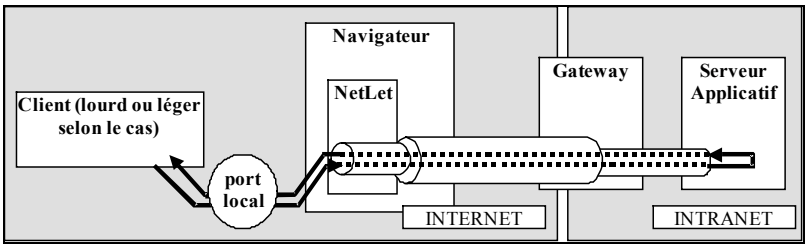

Figure 5 – *Principe de la technologie Netlet*

6.2 Portal Server

Le Portal Server est un serveur Web qui assume des fonctions de Portail, de Serveur d'Application et de Serveur d'administration :
- en tant que portail, il gère l'affichage des pages d'authentification, du desktop, des pages de personnalisation, d'aide et de service,
- en tant que serveur d'application, il inclut des services :
  - d'interface à des serveurs de mail POP3 et/ou IMAP4 (utilitaires NetMail),
  - de gestion de fichiers distants (utilitaires NetFile),
  - …
- en tant que serveur d'administration, il permet d'accéder aux fonctions de configuration, maintenance et exploitation du portail et de la gateway.

7 Gestion des identités

L'ENT ayant pour principe de base d'offrir des services personnalisés aux utilisateurs, une des problématiques qui en découle directement est la gestion de l'identité et des droits associés.
Cette problématique de gestion de l'identité des personnels et des étudiants, ainsi que, plus généralement, la problématique de gestion des communautés, est adressée par le composant Sun ONE Identity Server (Figure 6) qui permet :
- de gérer des utilisateurs et des communautés,
- d'affecter des services et des droits aux utilisateurs ou à des communautés,
- d'affecter des rôles,
- de gérer des organisations,
- de fournir un service de signature unique,
- d'affecter un niveau de sécurité en adéquation avec l'usager et les services accédés.

Le composant Identity Server s'appuie sur un standard de fait pour l'entrepôt des données utilisateurs: un annuaire de type LDAP.
Chaque usager du système d'informations est authentifié et identifié lors de l'accès à l'espace numérique. A partir de cette identité, répertoriée dans l'annuaire, Identity Server crée une session pour l'utilisateur, avec l'ensemble des droits qui lui sont associés. L'utilisateur peut alors accéder à l'ensemble des services auxquels il a droit, sans avoir à s'authentifier de nouveau et sans qu'il y ait de propagation de mot de passe sur le réseau : le jeton de session est utilisé comme identifiant et est interprété par les agents Identity Server, déployés sur les frontaux d'accès aux applications. Ce mécanisme de signature

unique peut être étendu sur des espaces multi domaines, par utilisation des spécifications Liberty Alliance, ce qui permet d'envisager des solutions de signature unique entre les établissements.
La gestion des rôles et de l'affectation des services aux usagers est assurée par « Identity Manager ». « Identity Manager » est un ensemble de services apporté aux administrateurs de l'ENT pour administrer les différentes organisations, groupes et politiques de sécurité. Il permet d'avoir différents niveaux d'administrateurs permettant, en particulier, de faire de la délégation de droits.

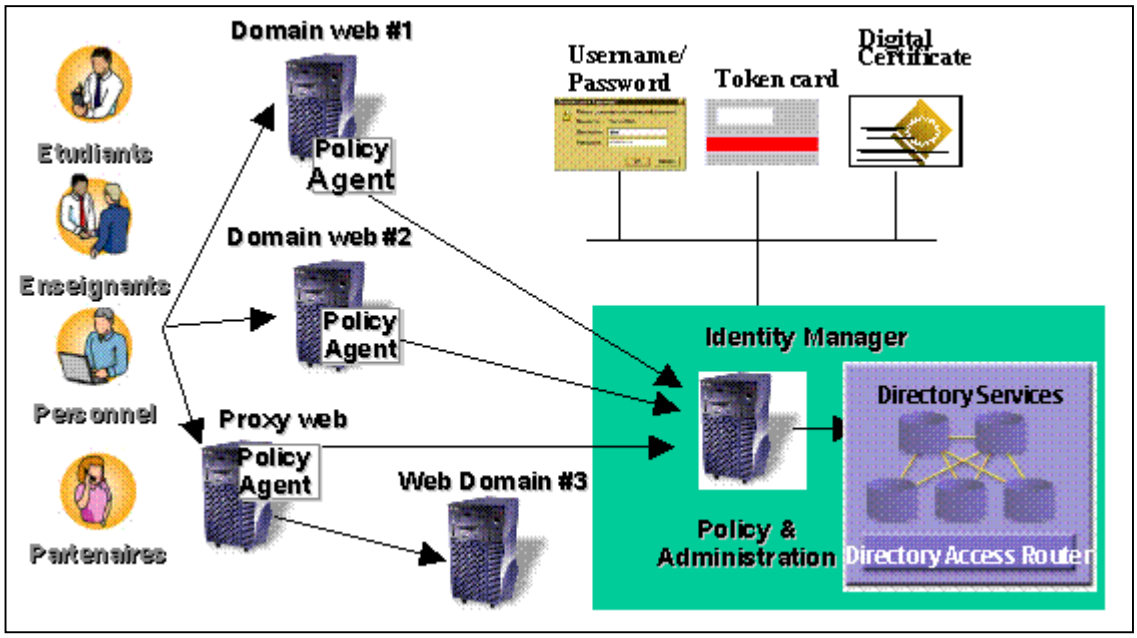

Figure 6 – *Principe de fonctionnement de l' « Identity Server »*

L'interface d'administration de Identity Server peut être complètement personnalisable en fonction des rôles, des identités, des établissements. La vue ci-dessous montre la possibilité de définir des organisations, de configurer les services, de surveiller les sessions et de fédérer l'identité sur Internet via Liberty.

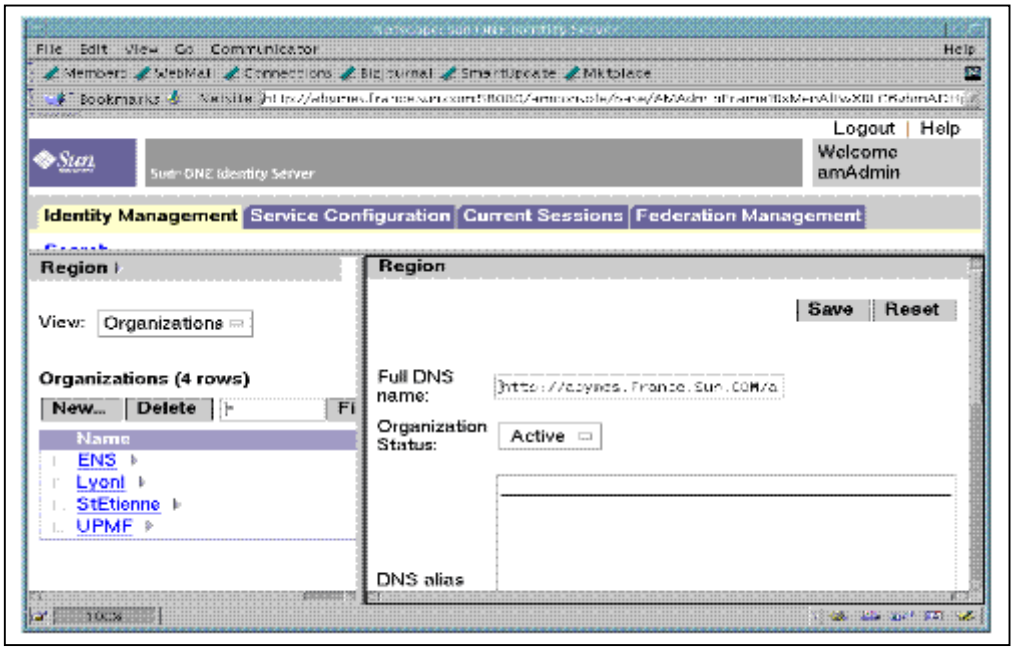

Figure 7 – *Interface d'administration de Identity Server*

8 Architecture physique

Une des difficultés pour le dimensionnement d'un ENT est sans doute le facteur d'échelle extrêmement variable suivant la taille de l'établissement (jusqu'à 200 000 utilisateurs potentiels) et l'utilisation qui en sera faite.
On se doit dès lors de définir des principes d'architecture et de dimensionnement évolutifs et capables d'absorber des charges importantes. Dans cet esprit, on utilise le savoir-faire acquis dans la mise en œuvre de portails d'information à gros volume d'usagers. Les principes retenus sont :

- la modularité: la capacité à intégrer des nouveaux composants logiciels ou matériels dans l'architecture,
- la « scalabilité » verticale: la capacité à monter en charge par simple rajout de puissance processeur dans une même machine,
- la « scalabilité » horizontale: la capacité à monter en charge par rajout de machine unitaire,
- la disponibilité: la capacité du système à rendre le service même en cas de panne d'un des composants matériels ou logiciels.

Ces différents principes permettront d'avoir un niveau de service constant pour l'usager quelle que soit la charge.

La Figure 8 présente le schéma d'une architecture matérielle de base permettant d'éviter les points de panne uniques. Nous en décrivons ici les mécanismes et nous présentons par la suite les moyens d'étendre cette architecture.

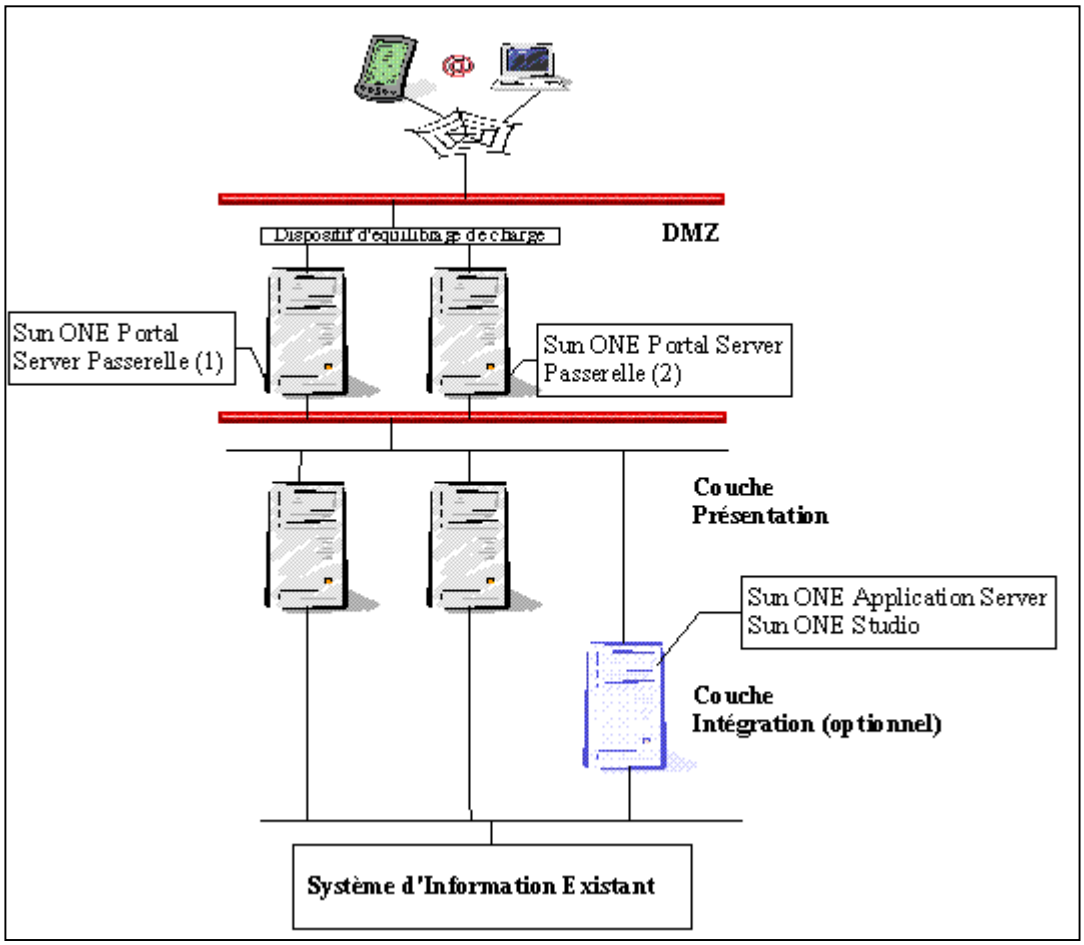

Figure 8 – *Architecture physique de base par établissement*

Les caractéristiques de l'architecture de base sont les suivantes :

- redondance de la passerelle (gateway) de portal Server : la répartition de charge et la reprise en cas de panne est assurée en amont pas un répartiteur de charge de type commutateur « intelligent »,

- le composant de portail est redondé de la même façon. Il n'est pas nécessaire d'incorporer de répartiteur supplémentaire : la gateway assure ce rôle de répartition vers les différentes instances de portail.

Ce modèle est extensible tant horizontalement que verticalement pour les deux composants en respectant les règles suivantes :
- gateway : au plus 4 CPU par machine,
- cœur de portail : au plus 12 CPU par instances.

La démarche de dimensionnement de l'infrastructure est la suivante :
- collecte des exigences et formulation d'hypothèses,
- établissement d'un dimensionnement primaire à l'aide d'abaques et de retours d'expériences,
- déploiement d'un pilote sur une infrastructure simplifiée,
- choix d'une stratégie d'architecture en fonction du retour d'expérience.

La *collecte des exigences* recouvre les aspects métiers, le nombre d'utilisateurs potentiels, actifs et simultanés, les temps de réponse demandés, le comportement des utilisateurs, les exigences en terme de performance, l'interaction avec les systèmes existants.
Ensuite on peut procéder au *premier dimensionnement* en utilisant le nombre de sessions concurrentes, le temps moyen entre les « hits », le temps de session moyen, les activités de recherche. A l'aide de ces éléments, des abaques sont utilisés pour faire un premier dimensionnement.
La *phase pilote* est le principe retenu dans le cadre d'ENCORA, Il permet d'avoir un premier retour d'expérience utilisateurs et fournit des informations sur la criticité des services ainsi que sur le modèle d'utilisation.
Enfin, on peut choisir une *stratégie d'architecture* qui se déclinera en trois modèles : « petits » établissements, établissements de taille « moyenne » et « larges » établissements.

9 Conclusion

Le projet ENCORA est un vaste projet qui a mis du temps à démarrer. Les premiers mois sont riches d'enseignement pour nous qui sommes informaticiens. On craignait en effet que regrouper des techniciens chevronnés avec des pratiques, des modes d'organisation et des convictions bien différentes déboucherait sur un projet « patchwork » répondant plus à un ensemble de solutions techniques différentes qu'à de réelles réponses à des besoins. Il n'en a rien été. Même si les réunions ont pu être vivantes☺, elles ont été très constructives et toujours détendues, à tel point qu'elles ont permis la définition d'une architecture commune, mutualisée au niveau de la région satisfaisant tout le monde.
Le plus dur reste maintenant à faire : non pas la réalisation technique, mais l'organisation humaine nécessaire à la mise à disposition des utilisateurs d'un tel outil qui touche en profondeur les habitudes des personnels administratifs et techniques des enseignants. C'est là, à notre avis, le plus gros challenge de l'arrivée des Espaces Numérique de Travail dans les établissements universitaires. Gageons que les établissements de la région Rhône-Alpes réussiront ce challenge. Les conditions de réussite sont déjà en place sur le plan technique et relationnel car elles ont pu s'établir lors de la phase de spécifications des besoins pour lesquels une centaine de personnes des différents établissements et de profils divers ont pu travailler ensemble.

Références

[1] EverSuite : http://www.ever-team.com/products/produits.html
[2] Christine LACOMBE, Pierre-Yves Cunin, The Portal of "GreCO-Universités", Virtual Campus Initiatives : 4th International Conference on New Educational Environments 2002 Lugano (Suisse) Mai 2002
[3] SupAnn : http://www.cru.fr/ldap/supann
[4] Agalan : http://www.agalan.org