Université de Strasbourg

Spécification de l'annuaire d'établissement

Historique

Version	Date	Auteur	Modification
0.0	05/06/2008	Alain ZAMBONI	Rédaction initiale
0.1	12/06/2008	Alain ZAMBONI	Intégration des remarques de G. Brand, M. Legin et P. David
0.2	17/06/2008	Pierre DAVID	Intégration des remarques de C. Distel
0.3	24/06/2008	Alain ZAMBONI	Intégration des remarques de M. Legin (e.n.t.)
0.4	25/06/2008	Alain ZAMBONI	Intégrations des remarques du groupe de travail
0.5	26/06/2008	Alain ZAMBONI Emmanuel BLINDAUER	Recommandations SUPANN 2008 Corrections de M. Legin Ajout des chapitres « Active Directory »

Table des matières

1 Introduction

1.1 Contexte

La fusion des trois universités strasbourgeoises et de l'IUFM au premier janvier 2009 constitue une occasion unique de repenser l'architecture de l'annuaire LDAP défini et utilisé jusque là par divers services informatiques en place. Avec l'expérience accumulée dans la gestion de l'annuaire et grâce à une nouvelle Direction Informatique unifiée, les contraintes de dispersion qui pesaient jusqu'ici disparaissent et ouvrent la voie à une architecture d'annuaire simplifiée et homogène.

1.2 Objectifs et enjeux

Les objectifs de cet annuaire sont :

- d'assurer la cohérence des informations qui s'y trouvent ;
- de permettre leur utilisation transversale par l'ensemble des applications ;
- d'offrir aux composantes de l'UdS un service d'annuaire fiable et adapté à leurs besoins ;
- de gérer des services que l'UdS s'est engagée à offrir à des établissements partenaires (messagerie, wifi, e.n.t., applications pédagogiques, etc.) ;

La structure proposée est un annuaire unique sur lequel s'adossent tous les services, dans le but évident de simplifier les processus et d'en simplifier la gestion.

1.3 Objectif de ce document

Cette documentation est destinée à la fois aux concepteurs de l'annuaire et à ses utilisateurs, c'est à dire les concepteurs des applications utilisant l'annuaire. Elle a pour vocation de décrire précisément la structure de l'annuaire, les schémas utilisés et les valeurs des attributs.

2 Applications centralisées

La direction informatique de l'UdS offre de nombreux services centralisés au personnels et étudiants de l'université. Parmi eux, un certain nombre s'appuient fortement sur l'annuaire d'établissement.

2.1 Environnement Numérique de Travail (e.n.t.)

L'environnement numérique de travail propose aux personnels et étudiants de l'UdS d'accéder au travers d'un portail web sécurisé à un panel d'applications administratives et pédagogiques ainsi qu'à des informations ciblées.

2.1.1 Authentification

L'authentification est réalisée via un serveur CAS selon les identifiants et mot de passes stockés dans l'annuaire. De plus, l'activation ou non d'un compte e.n.t. est spécifiée au travers d'un attribut .

2.1.2 Profils

L'e.n.t. s'appuie fortement sur l'annuaire afin de construire de manière dynamique le portail personnalisé de l'utilisateur. Les attributs permettant l'identification de la personne sont stockées au sein de l'annuaire d'établissement.

2.2 Univ-R

En cours de rédaction.

2.3 Messagerie électronique

Un service de messagerie électronique centralisé est offert aux personnels et aux étudiants de l'UdS. Ce service s'appuie fortement sur l'annuaire d'établissement. Les interactions entre l'annuaire d'établissement et la messagerie électronique sont décrites ci-après.

2.3.1 Authentification

Les accès au serveur de messagerie pour la consultation (protocoles IMAP(S)/POP(S) ou webmail) ainsi que pour l'envoi de message sont authentifiés selon les identifiants (logins) et mots de passe stockés dans l'annuaire.

2.3.2 Adresses de messagerie

Toutes les adresses de messagerie valides sont déclarées dans l'annuaire. Ces adresses sont soit des adresses attribuées à une boîte aux lettres, soit des aliases de messagerie redirigeant vers une ou plusieurs autres adresses. Ces dernières peuvent appartenir à des domaines de messagerie hors du service de messagerie centralisé.

Les applications de routage de messagerie se connectent à l'annuaire d'établissement pour y résoudre les adresses de messagerie et déterminer si le message est à déposer dans une boîte aux lettres ou à transférer vers une ou plusieurs autres adresses.

2.3.3 Informations sur la boîte aux lettres électroniques

Pour permettre le dépôt et la lecture des messages, l'annuaire contient pour chaque boîte aux lettres un attribut indiquant le dossier de stockage des messages. Une limite d'espace disque autorisé est également déclarée pour chaque boîte.

Enfin, chaque boîte aux lettres peut se voir associer des filtres. Ceux-ci permettent d'effectuer des opérations automatiques sur les courriers entrants, tel qu'un déplacement automatique dans dossier. Ces filtres sont également stockés dans l'annuaire.

2.4 Listes de diffusion

Le service de listes de diffusion permet de créer des listes de messagerie offrant des fonctionnalités avancées : droits de postage, archivage, etc. Ce service est ouvert à l'ensemble de la communauté Osiris.

2.4.1 Authentification

Le serveur de listes de diffusion Sympa offre une interface de gestion graphique. L'accès à ce service requiert une authentification via un identifiant et un mot de passe, qui sont ceux contenus dans l'annuaire d'établissement.

2.4.2 Abonnement automatique

Les informations contenues dans l'annuaire d'établissement permettent de mettre en place un système d'abonnement automatique aux listes. Par exemple, les étudiants sont automatiquement inscrits aux listes de diffusions concernant leurs filières.

2.5 Accès réseaux Wifi et VPN

Pour faciliter la mobilité des utilisateurs, la direction informatique propose deux accès nomades au réseau Osiris. Le réseau sans-fil permet aux utilisateurs de se connecter au réseau Osiris en utilisant les ondes radio. Le service d'accès VPN permet quant à lui de se placer virtuellement dans le réseau Osiris quel que

soit son fournisseur d'accès Internet (à domicile ou depuis n'importe quel autre point de l'Internet).

2.5.1 Authentification

L'authentification à ces services est basée sur le couple identifiant et mot de passe de l'annuaire d'établissement.

2.5.2 Profils de connexion

Les utilisateurs de ces services peuvent être directement connectés à des sous-réseaux spécifiques, comme leur réseau de composante. Les attributs propres à chaque sous-réseau sont stockés dans l'annuaire, sous forme de profil. Les profils y sont également attribués aux utilisateurs. Les applications d'authentification s'adressent à l'annuaire pour obtenir ces associations et les informations concernant les profils de connexion.

2.6 Application « Cadic Intégral » du SCD de l'IUFM

L'application Cadic Intégral est utilisée au SCD de l'IUFM. Ses grandes fonctions sont :

- Portail Documentaire
- SIGB
- GED Administrative et Pédagogique

2.7 Active Directory

Active Directory (AD) est une technologie Microsoft dont l'implémentation contient en particulier un annuaire LDAP, mais aussi un serveur Kerberos pour l'authentification, et un serveur DNS. AD est l'outil structurant les « domaines » et « forêts ». Il permet également de déployer des logiciels et des configurations sur des objets (utilisateurs, ordinateurs, groupes).

Afin de faciliter la gestion des postes de travail Windows, la direction informatique offre un service de type Active Directory. Dans un soucis de cohérence, les authentifications sur le domaine Active Directory de l'UdS devront utiliser les identifiants de l'annuaire d'établissement.

2.8 Inscription aux activités sportives

L'application SiuapsWeb permet aux personnels et étudiants de s'inscrire à des activités sportives.

Afin de pouvoir proposer un paiement en ligne en adéquation avec le statut de la personne, cette application nécessite la présence de certains attributs dans le système d'information. Ceux ci sont définis au travers de la classe d'objet spécifique « udsSport ».

2.9 Annuaire fonctionnel

Pour une meilleure communication en interne comme vers l'extérieur, l'UdS doit disposer d'une application d'annuaire de type « Pages Jaunes ». Cette application permet la recherche de coordonnées des personnels de l'établissement (ou des personnels d'autres établissements hébergés dans les locaux) par leur nom, mais aussi par leur fonction au sein de l'université. Il est également possible de trouver les coordonnées des différents services et laboratoires.

L'annuaire d'établissement propose une structure de données permettant de stocker en son sein les informations nécessaires à la mise en place de cette application.

2.10 Téléphonie

La fusion des trois universités strasbourgeoise entraîne la fusion de trois systèmes téléphoniques différents. Un référentiel unique des numéros de téléphone attribués, indépendant des systèmes de téléphonie, est nécessaire pour préserver une interopérabilité entre ces derniers, et également pour offrir un service d'accueil téléphonique de qualité.

L'annuaire d'établissement a donc pour vocation de centraliser de manière abstraite les informations téléphoniques de l'UdS, et de s'interfacer avec les différents systèmes téléphoniques (en places ou à venir).

2.11 Composantes de l'UdS

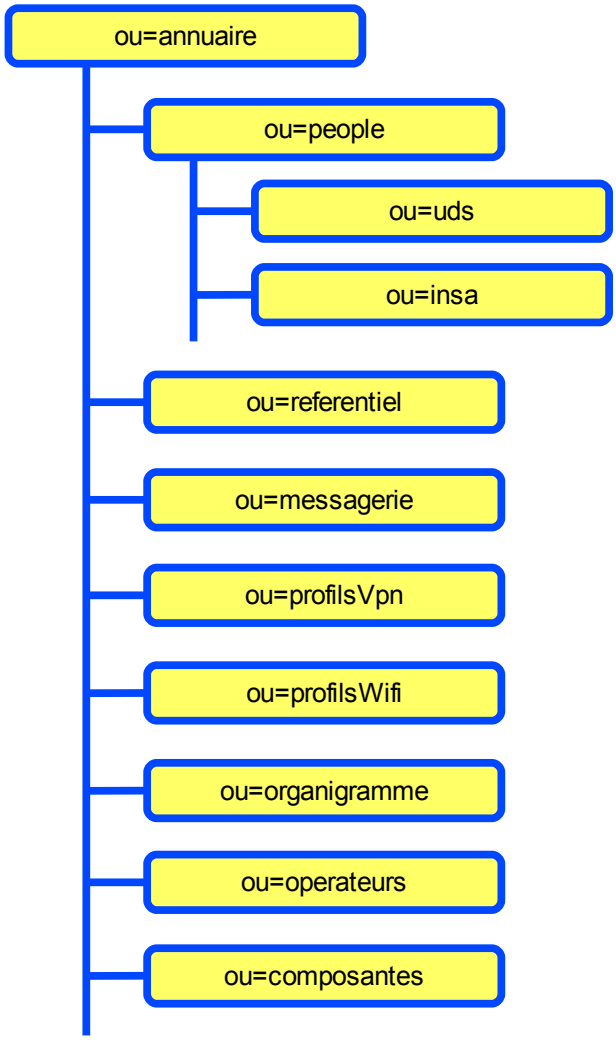
Afin de pouvoir offrir un service intégré pour l'utilisateur, les composantes peuvent interfacer leur système d'information avec l'annuaire d'établissement UdS. Ce point est traité en détail dans le chapitre 6.

3 Structure de l'annuaire d'établissement UdS

L'annuaire d'établissement est un annuaire multi-établissement : il doit pouvoir intégrer les utilisateurs des établissements d'enseignement supérieur et de recherche demandant à profiter de l'offre de service de la direction informatique.

Cet annuaire est aussi un annuaire applicatif : il contient des informations nécessaires au fonctionnement de services offerts par la direction informatique.

Afin de répondre à ces besoins, l'annuaire contient plusieurs branches, chacune contenant des informations de nature différente. Le contenu de ces différentes branches est expliqué plus spécifiquement dans les chapitres suivants.


ou=annuaire
ou=people
ou=uds
ou=insa
ou=referentiel
ou=messagerie
ou=profilsVpn
ou=profilsWifi
ou=organigramme
ou=operateurs
ou=composantes

4 Gestion des personnes

Chaque personne se voit attribuer un compte unique, quel que soit le nombre de fonctions qu'elle peut occuper au sein de l'université. Ainsi, un personnel également inscrit en tant qu'étudiant aura un seul compte, lui offrant accès aux applications réservées au personnel, mais également aux applications pédagogiques proposées aux étudiants.

4.1 Arborescence

Les personnes sont déclarées dans la branche « ou=people » de l'annuaire d'établissement. Cette branche est subdivisée : chaque établissement hébergé dans l'annuaire a sa sous-branche propre.

4.2 Les classes d'objets

Les schémas suivants détaillent la représentation utilisée pour stocker toutes les informations relatives à une personne dans l'annuaire.

4.2.1 Classe *inetOrgPerson*

Classe d'objet standard (RFC 2798) définissant une personne. Le détail des attributs contenus par cette classe peut être consulté dans les documents suivants :

- RFC-2798 de l'IETF : http://www.ietf.org/rfc/rfc2798.txt
- Recommandations SUPANN v1 : http://www.cru.fr/_media/documentation/supann/supann-v10.pdf
- Recommandations SUPANN 2008 : http://www.cru.fr/documentation/supann/2008/documentcomplet

4.2.2 Classe *eduPerson*

La classe *eduPerson* est issue des travaux d'un groupe de travail de l'association EDUCAUSE. Cette classe propose des attributs génériques permettant de définir une personne dans l'enseignement supérieur. L'utilisation de cette classe, plébiscitée par les recommandations SUPANN, s'inscrit dans une démarche d'harmonisation internationale des annuaires d'établissement de l'enseignement supérieur.

Le détail des attributs de cette classe peut être consulté dans les documents suivants :

- Site web EDUCAUSE : http://www.educause.edu/eduperson
- Recommandations SUPANN v1 : http://www.cru.fr/_media/documentation/supann/supann-v10.pdf
- Recommandations SUPANN 2008 : http://www.cru.fr/documentation/supann/2008/documentcomplet

Le tableau suivant présente les attributs issus de la classe edu*Person* qui seront utilisés dans l'annuaire UdS.

Nom	Mono ou multivalué	Obligatoire	Description
eduPersonAffiliation	Mu	N	Statut de la personne en fonction de la nomenclature suivante : ●student : étudiant inscrit dans l'établissement ●faculty : personnel géré ou hébergé par l'établissement assurant une activité d'enseignement ●employee : personnel géré ou hébergé par l'établissement assurant une activité autre que l'enseignement ou la recherche ●researcher : personne assurant une activité de recherche ●member : personne inscrite dans les bases de l'établissement ; s'ajoute aux profils student, faculty, employee et researcher ●affiliate : personne ne dépendant pas de l'établissement ●alum : ancien étudiant ayant gardé des liens avec l'établissement ●retired : personne retraitée ayant gardé des liens avec l'établissement ●emeritus : professeur ayant obtenu l'éméritat dans l'établissement ●library-walk-in : profil spécifique lié à la problématique des accès aux bibliothèques électroniques
eduPersonPrimaryAffiliation	Mo	N	Statut considéré comme principal (cf. nomenclature ci dessus)

4.2.3 Classe *supannPerson*

Les recommandations SUPANN ont pour but d'assurer la compatibilité des annuaires de l'enseignement supérieur aux niveaux national et international.

La classe d'objet *supannPerson* complète les classes *inetOrgPerson* et *eduPerson*. Elle ajoute des attributs génériques supplémentaires pour définir une personne.

Le détail des recommandations SUPANN peut être consulté dans les document suivant :

- Recommandations SUPANN v1 : http://www.cru.fr/_media/documentation/supann/supann-v10.pdf
- Recommandations SUPANN 2008 : http://www.cru.fr/documentation/supann/2008/documentcomplet

Le tableau suivant présente les attributs issus de la classe *supannPerson* qui seront utilisés dans l'annuaire UdS.

Nom	Mono ou multivalué	Obligatoire	Description
supannEtablissement	Mo	O	Établissement de rattachement administratif de la personne
supannCivilite	Mo	N	« M. », « Mme » ou « Mlle » (ne pas oublier le point après le M pour monsieur).
supannListeRouge	Mo	O	DOIT contenir une information sur le souhait de la personne de figurer en liste rouge. Booléen à VRAI pour les personnes figurant en liste rouge.
supannAutreTelephone	Mu	N	Téléphones fixes autres que le téléphone principal. Même syntaxe que TelephoneNumber.
supannEntiteAffectation	Mu	N	Représente la ou les affectations de la personne dans un établissement, une composante, un service, etc. Pour l'Uds, les valeurs utilisées sont celles du référentiel utilisé dans l' application Harpège.
supannEntiteAffectationPrincipale	Mo	N	Représente l'affectation principale de la personne dans l'établissement (composante, service, etc.). Pour l'Uds, les valeurs utilisées sont celles du référentiel utilisé dans l' application Harpège.
supannEmpId	Mo	N	Identifiant de l'employé dans le logiciel de gestion du personnel de l'établissement.
supannCodeINE	Mo	N	Cet attribut DOIT stocker le code INE pour les étudiants (voir sigles et glossaire).Il DOIT être renseigné si l'attribut eduPersonAffiliation contient student.
supannEtuId	Mo	N	Identifiant de l'étudiant dans le logiciel de gestion de scolarité de l'établissement.

4.2.4 Classe *udsPerson*

La classe d'objet *udsPerson* est la classe de base d'une personne de l'UdS. Elle propose les attributs nécessaires pour identifier une personne dans le système d'information de l'Université de Strasbourg. On retrouve dans cette classe certains attributs issus des classes *inetOrgPerson* et *eduPerson* dans le but de les rendre obligatoires.

Nom	Mono ou multivalué	Obligatoire	Description
uid	Mo	O	Login de l'utilisateur
givenName	Mo	O	Prénom de l'utilisateur
eduPersonAffiliation	Mu	O	Catégorie d'usager. Cf SUPANN
udsBirthdate	Mo	O	Date de naissance de la personne
udsBirthName	Mo	O	Nom de naissance de l'utilisateur Ce champ est uniquement rempli si le nom d'usage (sn) est différent du nom de naissance
udsCharterApproval	Mo	O	Booléen indiquant si la personne s'est engagée à respecter la charte d'utilisation des ressources informatiques de l'université
udsLab	Mu	N	Laboratoire(s) de recherche au(x)quel(s) est affectée la personne
udsEntActive	Mo	N	Booléen indiquant si la personne a activé son compte e.n.t.
udsNetManagerGroup	Mo	N	Groupe de gestionnaires réseaux ayant des droits sur l'administration de la personne
udsDataSource	Mu	O	Nom de la(les) base(s) source(s) dont l'entrée est issue. Valeurs possibles : APOGEE, HARPEGE, INSA, ENGEES, MANUEL La valeur « MANUEL » est utilisée lorsque les comptes ne sont pas rattachés à une base de données source. Les cas envisageables sont : - établissement sans annuaire d'établissement - comptes invités d'accès réseau (Wifi/VPN)
udsApogeeId	Mo	N	Index de la personne dans l'application Apogée. Attribué uniquement si udsDataSource vaut APOGEE
udsHarpegeId	Mo	N	Index de la personne dans l'application Harpège. Attribué uniquement si udsDataSource vaut HARPEGE
udsSourceDN	Mo	N	DN de référence dans l'annuaire INSA ou ENGEES si la personne est issue d'un de ces établissements. Attribué uniquement si udsDataSource a la valeur correspondante
udsFunctionDN	Mu	N	Attribue une ou plusieurs fonctions issues de l'annuaire fonctionnel à cette personne. Cf chapitre 5.1

4.2.5 Classe *udsEmployee*

La classe *udsEmployee* est attribuée aux personnels de l'université. Elle permet de renseigner les informations propres à ce statut issues de la base Harpège.

Nom	Mono ou multivalué	Obligatoire	Description
udsStatus	Mo	O	Statut de la personne : Titulaire, Vacataire, Contractuel

Nom	Mono ou multivalué	Obligatoire	Description
udsGrade	Mo	N	Grade de la personne
udsEndOfActivityDate	Mo	N	Date de fin d'activité en tant que personnel universitaire. Format date LDAP
udsSpeciality	Mo	N	Indique le code CNU pour les enseignants/chercheurs et la BAP pour les ITRF.

4.2.6 Classe *udsStudent*

La classe *udsStudent* est attribuée aux étudiants de l'université. Elle permet de renseigner les informations propres à ce statut issues de la base Apogée.

Les attributs obligatoires de cette classe peuvent être renseignés dès l'inscription administrative. C'est cette inscription qui est déterminante pour affecter le statut d'étudiant à une personne. Les autres attributs demandent que l'étudiant ait effectué son inscription pédagogique.

Nom	Mono ou multivalué	Obligatoire	Description
udsAcademicYear	Mo	O	Dernière année d'inscription de l'étudiant. Format : 4 chiffres. Ex: 2007 pour l'année scolaire 2007/2008
udsEtpIndex	Mu	O	Étape(s) à laquelle(auxquelles) est inscrit l'étudiant. Format code étape d'Apogée
udsMainDepartment	Mo	O	Composante principale d'inscription de l'étudiant
udsEndOfRightDate	Mo	N	Date de fin de droits étudiants. Format date LDAP
udsVetIndex	Mu	N	Version d'étape à laquelle(auxquelles) est inscrit l'étudiant
udsElpIndex	Mu	N	Élément(s) pédagogique(s) au(x)quel(s) est inscrit l'étudiant

4.2.7 Classe *udsTempTeacher*

Cette classe est une classe spécifique pour les enseignants vacataires. Elle est utilisée par les applications pédagogiques pour déterminer les droits d'accès.

Nom	Mono ou multivalué	Obligatoire	Description
udsTempTeacher	Mo	O	Date de fin de la vacation. Format date LDAP

4.2.8 Classe *udsSport*

Cette classe contient des attributs nécessaires à l'application SiuapsWeb. Elle permet de déterminer le montant des droits sportifs, et de savoir si la personne les a acquittés.

Nom	Mono ou multivalué	Obligatoire	Description
udsSportSubscription	Mo	O	Booléen déterminant si la personne a payé les droits sportifs
udsSportRate	Mo	N	Pour les personnels. Niveau de droit sportif (1, 2, etc.) en fonction de l'indice salarial. Les paliers sont fixés par le SIUAPS
udsScholar	Mo	N	Pour les étudiants. Booléen indiquant si l'étudiant est boursier
udsBaccalaureatYear	Mo	N	Année d'obtention du baccalauréat. Permet d'exempter les étudiants venant de réussir le bac des droits sportifs

4.2.9 Classe *udsMailAccount*

Cette classe contient les attributs nécessaires au service d'hébergement de messagerie. Elle offre les attributs définissant une boîte aux lettres.

Nom	Mono ou multivalué	Obligatoire	Description
udsMailDirectory	Mo	O	Indique le répertoire de stockage de la boîte aux lettres sur le(s) serveur(s) de messagerie
udsCanonicalAddress	Mo	O	Adresse de messagerie principale de la personne
udsAlternateAddress	Mu	N	Adresse(s) de messagerie secondaire(s) de la personne
udsQuota	Mo	N	Espace disque maximum en octets autorisé pour cette boîte aux lettres. La valeur doit se terminer avec « S » pour préciser que c'est une limite sur la taille de la boîte. Ex : 5Go → 5000000000S
udsMailFilter	Mo	N	Séquence de filtre de messagerie à appliquer aux messages à destination de cette boîte aux lettres. Cf. http://www-crc.u-strasbg.fr/osiris/services/bal/filtres-expert.html
udsMailLimitDate	Mo	N	Date d'expiration de la boîte aux lettres. Format date LDAP.

4.2.10 Classe *udsWifiProfile*

Cette classe contient les attributs autorisant la personne à se connecter au réseau sans-fil Osiris et permettant de la placer dans un sous-réseau spécifique. Une personne sans cette classe ne peut se connecter au réseau sans-fil.

Nom	Mono ou multivalué	Obligatoire	Description
udsRadiusProfileWifi	Mo	O	Profil Wifi de la personne, faisant référence à un profil déclaré dans la branche des profils wifi.
udsWifiLimitDate	Mo	N	Date d'expiration de l'accès au réseau sans-fil. Format date LDAP.

4.2.11 Classe *udsVpnProfile*

Cette classe contient les attributs autorisant la personne à utiliser le service d'accès à distance VPN et permettant de la placer dans un sous-réseau spécifique. Une personne sans cette classe ne peut utiliser ce service.

Nom	Mono ou multivalué	Obligatoire	Description
udsRadiusProfileVPN	Mo	O	Profil VPN de la personne, faisant référence à un profil déclaré dans la branche des profils VPN.
udsVPNLimitDate	Mo	N	Date d'expiration de l'accès au service VPN. Format date LDAP.

4.2.12 Classe *udsWebGroup*

Cette classe permet d'attribuer un ou plusieurs groupes web à une personne. Ces groupes pourront être utilisés par les serveurs web pour restreindre l'accès à certaines pages.

Nom	Mono ou multivalué	Obligatoire	Description
udsWebGroup	Mu	O	Groupe web au(x)quel(s) appartient la personne.

4.2.13 Classe *udsMailingList*

Cette classe permet de définir les listes de diffusions auxquelles la personne doit être abonnée.

Nom	Mono ou multivalué	Obligatoire	Description
udsMailingList	Mu	O	Listes de diffusion au(x)quelle(s) la personne sera abonnée.

4.2.14 Classe *udsScdIufm*

Cette classe, utilisée par l'application « Cadic Intégral » du SCD de l'IUFM, permet de définir les groupes auxquelles la personne appartient, et de définir des droits sur certains modules.

Nom	Mono ou multivalué	Obligatoire	Description
udsGrpCadicName	Mu	O	Liste des groupes au(x) quelle(s) la personne appartient afin de lui donner des droits sur des modules de l'application Cadic Intégral.

5 Structures annexes

5.1 Annuaire fonctionnel

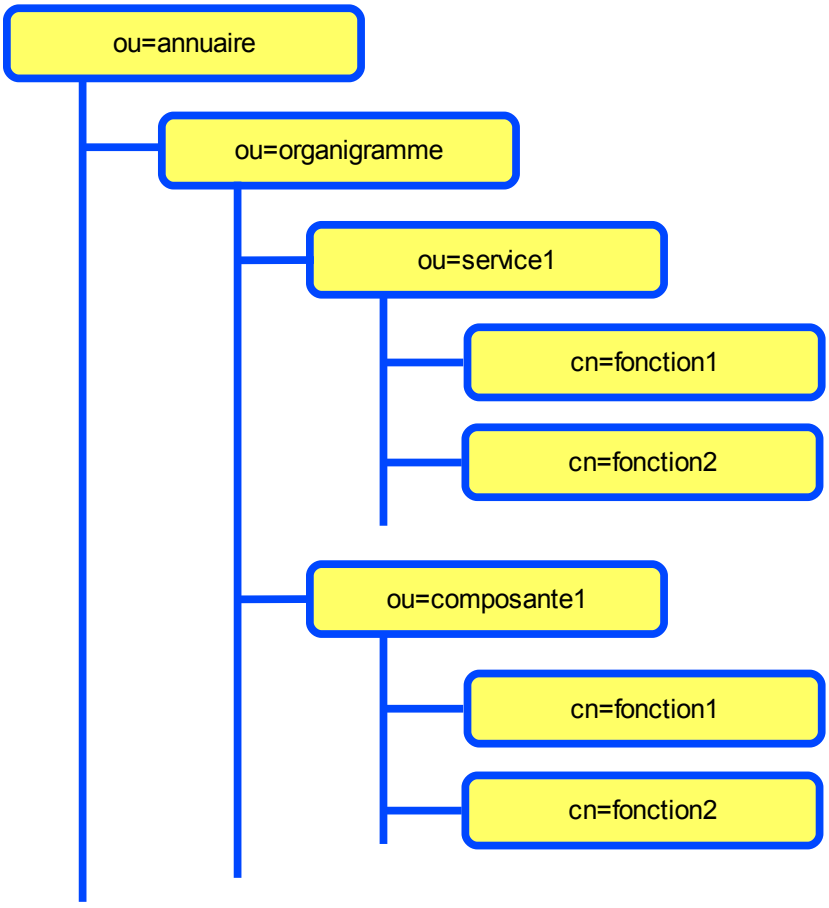
La structure d'annuaire fonctionnel référence les différentes fonctions de l'université de Strasbourg. Elle a vocation à être utilisé par avec une application de recherche, permettant de trouver les coordonnées des

personnels de l'université par leur nom ou leur fonction. Cette application permet également d'afficher les coordonnées de services, et de voir le rattachement des personnels à ceux-ci.

5.1.1 Sous-arborescence

La structure d'annuaire fonctionne est contenu dans la branche « ou=organigramme » de l'annuaire, directement sous la racine. Cette branche est subdivisée par service, composante ou laboratoire. Chaque entité aura donc sa sous-branche, dans laquelle pourront être listé les fonctions. Ces sous-branches pourront elle-même être subdivisées si nécessaire.

Les noms des entités seront les nouveaux noms courts du référentiel de l'UdS.



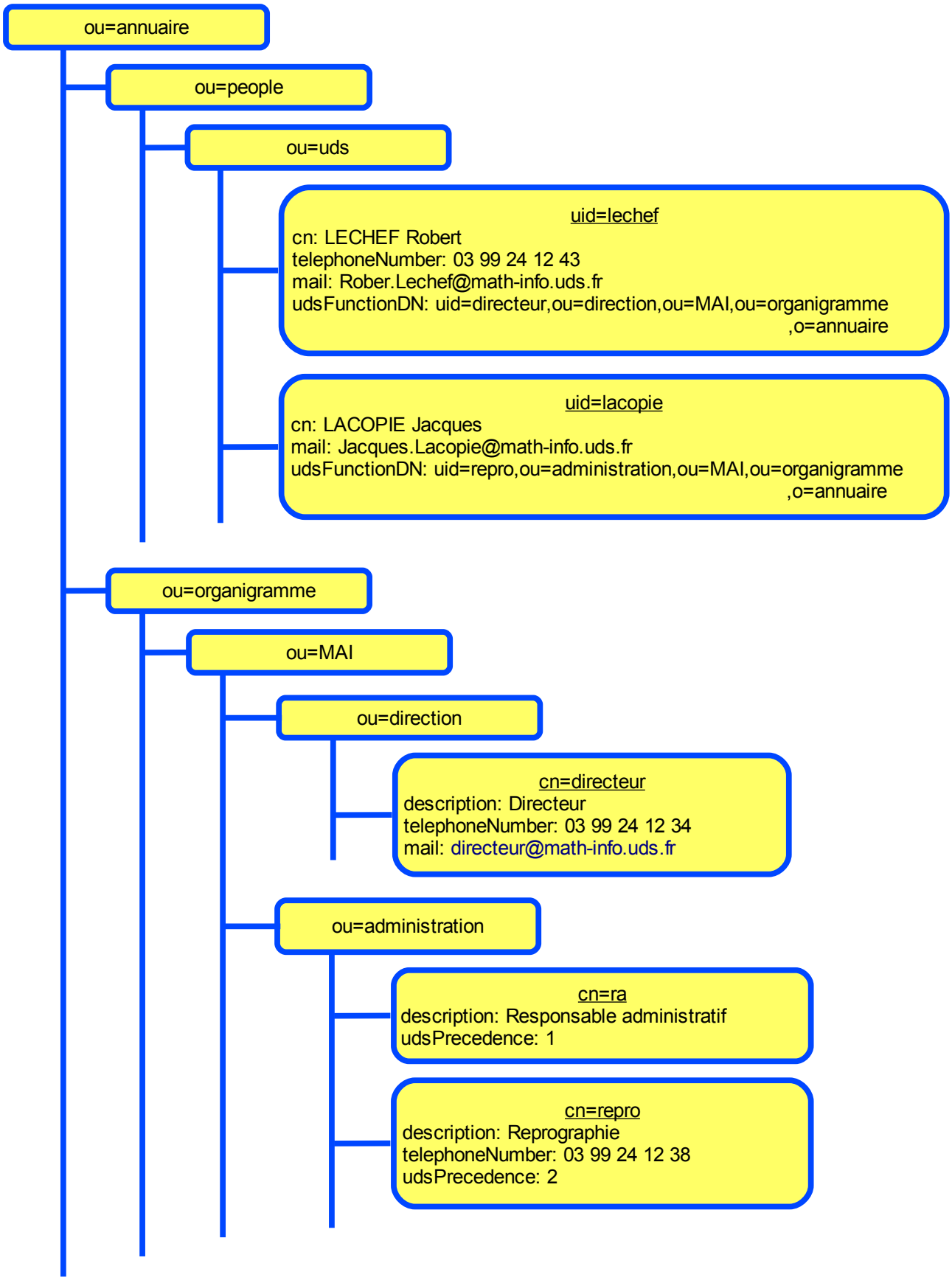
5.1.2 La classe udsFunction

Les caractéristiques d'une fonction sont définies dans la classe *udsFonction*. Plusieurs fonctions peuvent avoir le même identifiant ou nom, mais chacune reste unique au sein de son service/composante/laboratoire. Chaque fonction peut se voir attribué des informations de contact, indépendamment de celles qui sont propres aux personnes affectées à ces fonctions. Ces informations sont visibles dans l'application de consultation de l'annuaire fonctionnel en complément des informations de contact de la personne.

Nom	Mono ou multivalué	Obligatoire	Description
cn	Mo	O	Identifiant court de la fonction. Utilise l'attribut standard issu de la RFC 2256
description	Mo	O	Nom complet de la fonction. Utilise l'attribut standard issu de la RFC 1617
udsPrecedence	Mo	N	Valeur numérique permettant de trier applicativement l'affichage des fonctions dans une liste
telephoneNumber	Mo	N	Numéros de téléphone associés à cette fonction. Utilise l'attribut standard issu de la RFC 2256
mail	Mo	N	Adresse électronique associée à cette fonction. Utilise l'attribut standard issu de la RFC 1274 (rfc822Mailbox)

5.1.3 Exemple

Voici un exemple fictif de modélisation d'une composante ainsi que l'affectation de personnes aux fonctions déclarées.



5.2 Messagerie

Le service de messagerie nécessite le stockage de deux types d'informations en plus des boîtes aux lettres :

les aliases de messagerie, et la liste des domaines de messagerie hébergés.

Les aliases de messagerie sont les adresses de messagerie qui ne sont pas affectées directement à des boîtes aux lettres. Ces adresses redirigent les messages vers une ou plusieurs autres adresses, qui peuvent être hors du périmètre du service de messagerie centralisée.

5.2.1 Arborescence

Toutes les informations complémentaires relatives à la messagerie sont stockées dans la branche « ou=messagerie ». Cette branche est divisée en deux sous-branches :

- la branche « *ou=aliases* » qui contient tous les aliases
- la branche « *ou=domaines* » qui répertorie tous les domaines hébergés

Ces deux sous-branches ne sont pas elles-même subdivisées.

5.2.2 Classes d'objets

5.2.2.1 La classe *udsMailAlias*

Cette classe permet de déclarer des aliases. Elle est de type structurel, et peut donc être attribuée seule à un objet.

Nom	Mono ou multivalué	Obligatoire	Description
uid	Mo	O	Adresse de l'alias
udsForwardAddress	Mu	O	Adresse(s) destinataire(s) de l'alias
udsListManagedBy	Mo	N	Certains aliases peuvent être déclarés par des applications (ex: listes de diffusions). Lorsque c'est le cas, cet attribut indique le nom de l'application. Les aliases présentant cet attribut ne doivent pas être modifiés manuellement.

5.2.2.2 La classe *udsDomain*

Cette classe permet de déclarer des domaines. Elle est de type structurel, et peut donc être attribuée seule à un objet.

Nom	Mono ou multivalué	Obligatoire	Description
uid	Mo	O	Adresse de l'alias

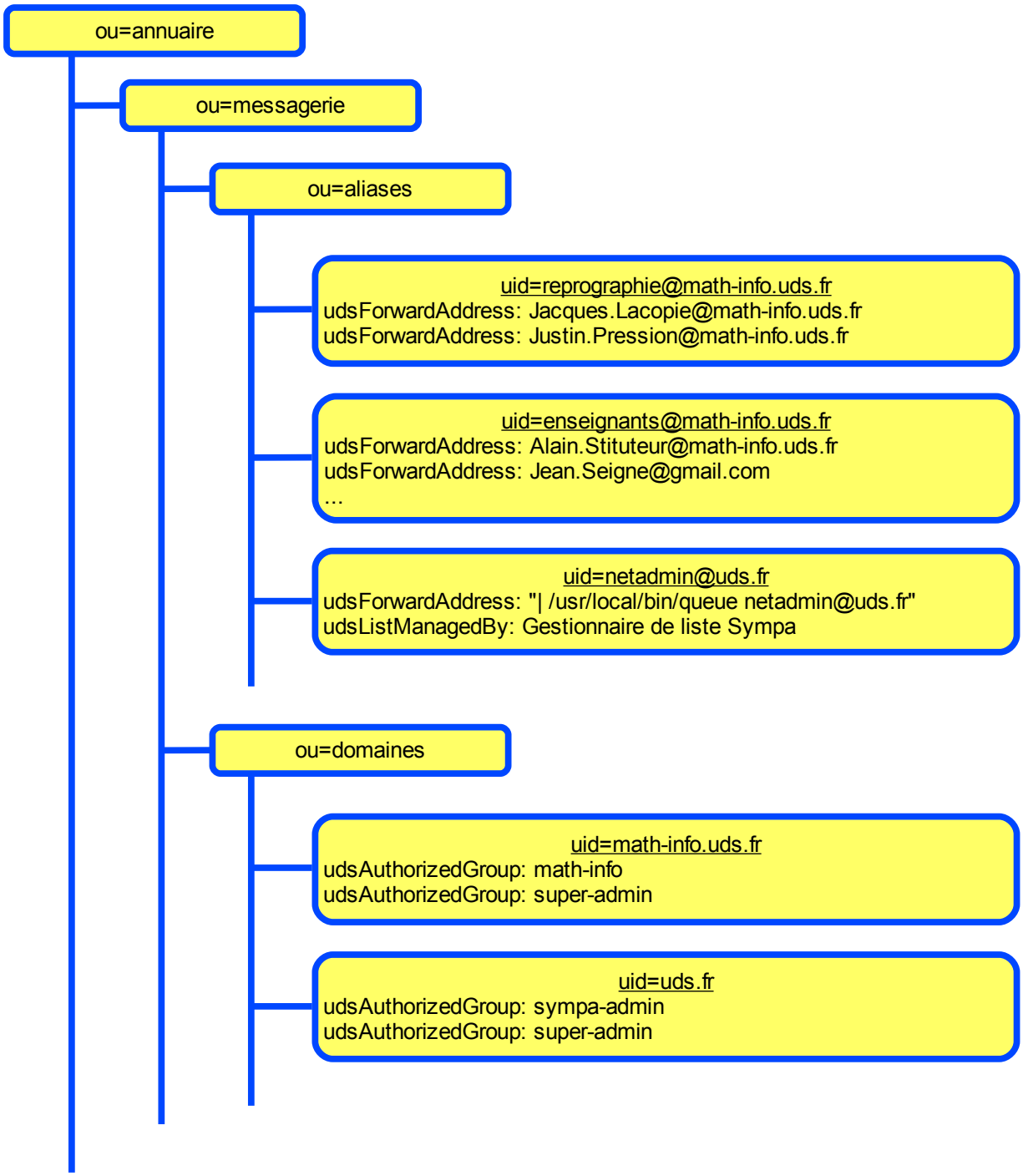
5.2.2.3 La classe *udsRights*

Cette classe est de type auxiliaire, et est donc forcément attribuée en supplément d'une classe structurelle. Elle est utilisée dans la définition des domaines et des profils Wifi et VPN. Elle permet de déclarer des groupes de correspondants autorisés à utiliser ces ressources. Les correspondants affectés aux groupes déclarés auront le droit de manipuler les adresses des domaines de messagerie concernés ou d'affecter les profils Wifi et VPN en questions.

Nom	Mono ou multivalué	Obligatoire	Description
udsAuthorizedGroup	Mu	O	Groupe(s) de correspondants réseaux autorisés à utiliser cette ressource (domaine de messagerie, Profils VPN ou Wifi)

5.2.3 Exemple

L'exemple fictif suivant présente quelques aliases et la déclaration des domaines associés.


ou=annuaire
ou=messagerie
ou=aliases
uid=reprographie@math-info.uds.fr
udsForwardAddress: Jacques.Lacopie@math-info.uds.fr
udsForwardAddress: Justin.Pression@math-info.uds.fr
uid=enseignants@math-info.uds.fr
udsForwardAddress: Alain.Stituteur@math-info.uds.fr
udsForwardAddress: Jean.Seigne@gmail.com
...
uid=netadmin@uds.fr
udsForwardAddress: "| /usr/local/bin/queue netadmin@uds.fr"
udsListManagedBy: Gestionnaire de liste Sympa
ou=domaines
uid=math-info.uds.fr
udsAuthorizedGroup: math-info
udsAuthorizedGroup: super-admin
uid=uds.fr
udsAuthorizedGroup: sympa-admin
udsAuthorizedGroup: super-admin

5.3 Profils Wifi

5.3.1 Arborescence

Toutes les définitions des profils Wifi sont stockées dans une branche « ou=profilsWifi », reliée à la racine de l'annuaire d'établissement. Il n'y a pas de subdivision en sous-branche.

5.3.2 Les classes d'objets

Les profils Wifi sont constitués de plusieurs classes d'objets. Parmi ces classes, la seule propre à l'UdS est la classe *udsRights* (cf paragraphe 5.2.2.3).

5.3.2.1 La classe *inetOrgPerson*

Quelques attributs de la classe standard *inetOrgPerson* sont utilisés.

Nom	Mono ou multivalué	Obligatoire	Description
uid	Mu	O	identifiant du profil. Par convention, les identifiants des profils Wifi débutent par « wifi- ».
sn	Mu	O	Nom du profil
cn	Mu	O	Description informative du profil

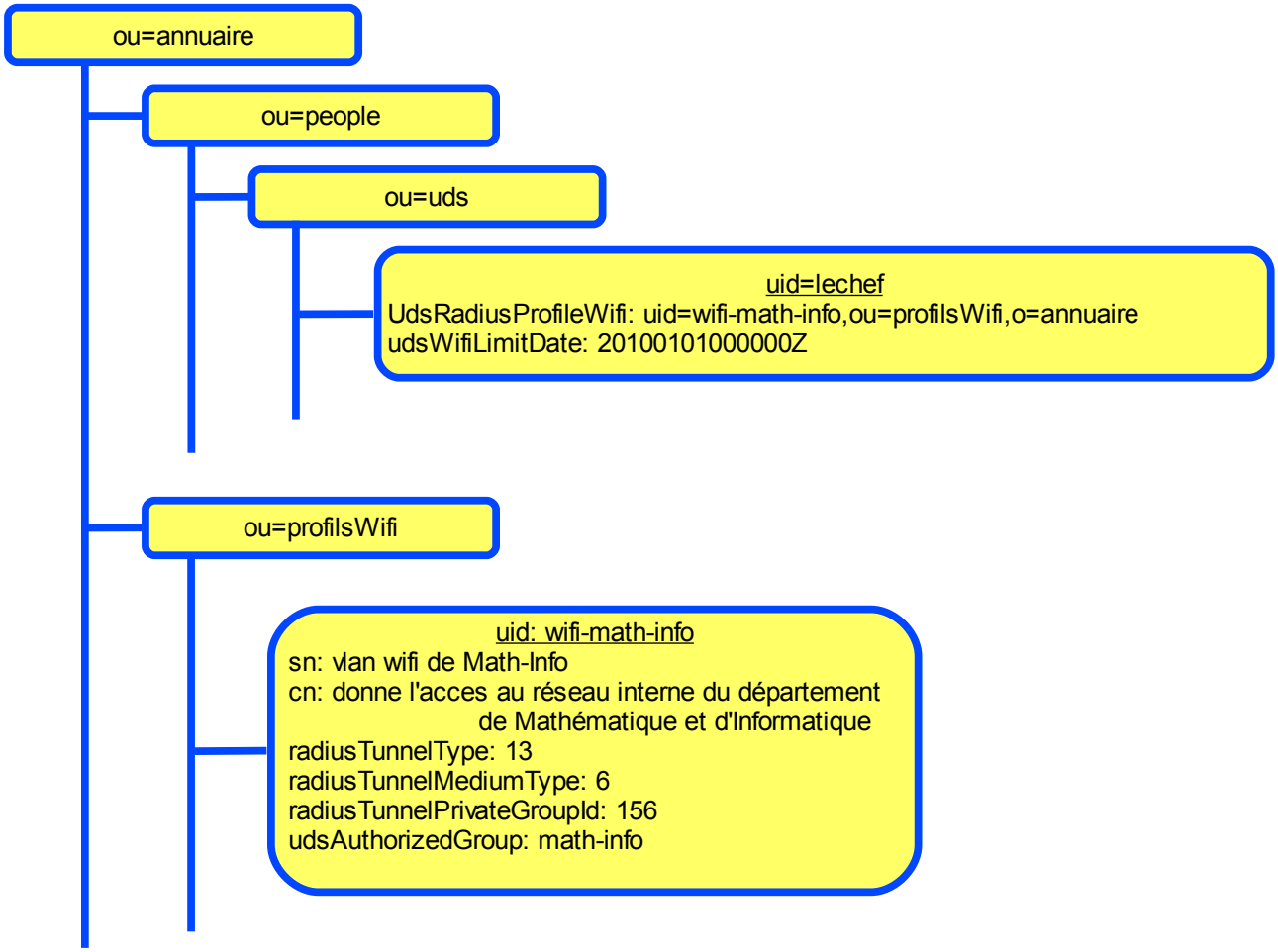
5.3.2.2 La classe *radiusProfile*

La classe applicative *radiusProfile* propose de nombreux attributs. Ceux utilisés dans les profils Wifi sont décrits dans le tableau ci-après.

Nom	Mono ou multivalué	Obligatoire	Description
radiusTunnelType	Mo	O	Valeur numérique indiquant le type de tunnel réseau utilisé. La valeur utilisée au sein d'Osiris est 13 pour spécifier l'utilisation de « réseaux virtuels » (VLAN).
radiusTunnelMediumType	Mo	O	Valeur numérique indiquant le protocole réseau du tunnel. La valeur utilisée au sein d'Osiris est 6 pour spécifier Ethernet.
radiusTunnelPrivateGroupId	Mo	O	Valeur numérique indiquant le numéro du réseau virtuel Ethernet..

5.3.3 Exemple

L'exemple suivant présente un profil Wifi et son attribution à un utilisateur.


ou=annuaire
ou=people
ou=uds
uid=lechef
UdsRadiusProfileWifi: uid=wifi-math-info,ou=profilsWifi,o=annuaire
udsWifiLimitDate: 20100101000000Z
ou=profilsWifi
uid: wifi-math-info
sn: vlan wifi de Math-Info
cn: donne l'acces au réseau interne du département
de Mathématique et d'Informatique
radiusTunnelType: 13
radiusTunnelMediumType: 6
radiusTunnelPrivateGroupId: 156
udsAuthorizedGroup: math-info

5.4 Profils VPN

5.4.1 Arborescence

Toutes les définitions des profils VPN sont stockées dans une branche « ou=profilsVpn », reliée à la racine de l'annuaire d'établissement. Il n'y a pas de subdivision en sous-branche.

5.4.2 Les classes d'objets

Les profils VPN sont constitués de plusieurs classes d'objets. Parmi ces classes, la seule propre à l'UdS est la classe *udsRights* (cf paragraphe 5.2.2.3).

5.4.2.1 La classe inetOrgPerson

Quelques attributs de la classe standard *inetOrgPerson* sont utilisés.

Nom	Mono ou multivalué	Obligatoire	Description
uid	Mu	O	Identifiant du profil. Par convention, les identifiants des profils Wifi débutent par « vpn- ».
sn	Mu	O	Nom du profil
cn	Mu	O	Description informative du profil

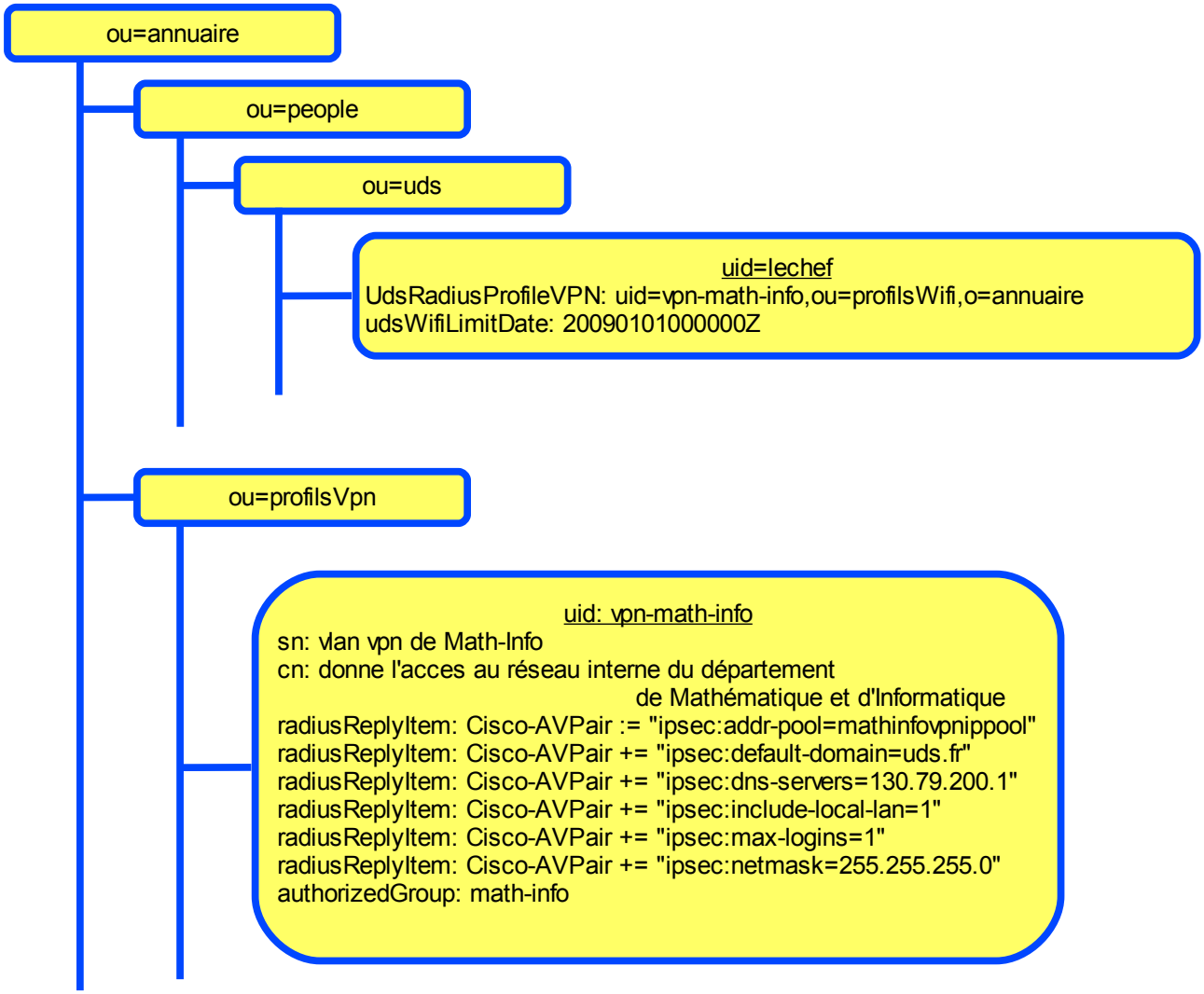
5.4.2.2 La classe radiusProfile

La classe applicative *radiusProfile* propose de nombreux attributs. Ceux utilisés dans les profils Wifi sont décrits dans le tableau ci-après.

Nom	Mono ou multivalué	Obligatoire	Description
radiusReplyItem	Mu	O	Méta-attribut contenant des paramètres de configuration (Cisco-AVPair) interprétés par le routeur VPN. Les différentes paramètres AVPair sont : ● ipsec:addr-pool = nom de l'espace d'adresses IP déclaré sur le routeur ● ipsec:default-domain = nom du domaine DNS ● ipsec:dns-servers = adresse du (des) serveur(s) DNS ● ipsec:include-local-lan = booléen. Si vrai, le client ne passera pas par le serveur VPN pour joindre son réseau local d'origine ● ipsec:max-logins = nombre de connexions simultanées autorisées par utilisateurs ● ipsec:netmask = masque de sous-réseau IP

5.4.3 Exemple

L'exemple suivant présente un profil VPN et son attribution à un utilisateur.


ou=annuaire
ou=people
ou=uds
uid=lechef
UdsRadiusProfileVPN: uid=vpn-math-info,ou=profilsWifi,o=annuaire
udsWifiLimitDate: 20090101000000Z
ou=profilsVpn
uid: vpn-math-info
sn: vlan vpn de Math-Info
cn: donne l'acces au réseau interne du département
de Mathématique et d'Informatique
radiusReplyItem: Cisco-AVPair := "ipsec:addr-pool=mathinfovpnippool"
radiusReplyItem: Cisco-AVPair += "ipsec:default-domain=uds.fr"
radiusReplyItem: Cisco-AVPair += "ipsec:dns-servers=130.79.200.1"
radiusReplyItem: Cisco-AVPair += "ipsec:include-local-lan=1"
radiusReplyItem: Cisco-AVPair += "ipsec:max-logins=1"
radiusReplyItem: Cisco-AVPair += "ipsec:netmask=255.255.255.0"
authorizedGroup: math-info

5.5 Structure du référentiel

Le référentiel de l'annuaire contient toutes les informations structurelles de référence relatives au fonctionnement de l'établissement : description des enseignements, des unités de recherche, des composantes, etc.

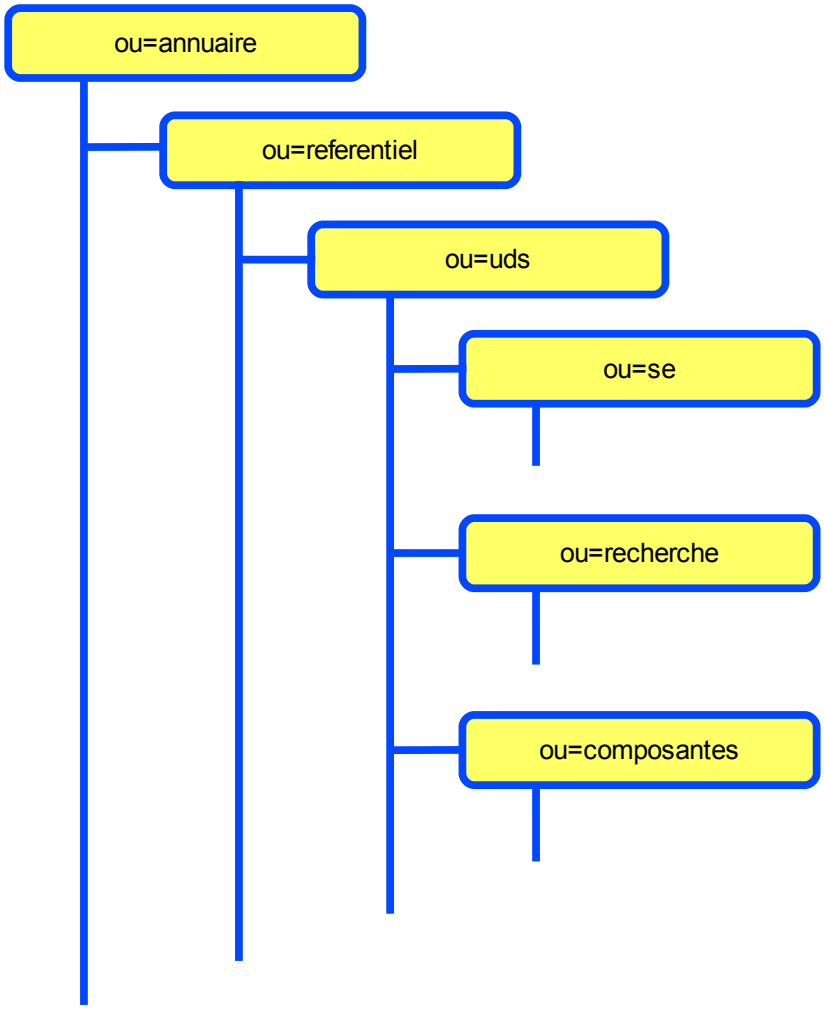
5.5.1 Arborescence

La branche « ou=referentiel » héberge l'ensemble de ces données. L'annuaire pouvant héberger des informations d'autres établissements pour leur offrir des services (par exemple la messagerie et les listes de diffusion étudiantes), une subdivision sur ce critère est effectuée. Les sous-branches ainsi créées sont nommées « ou=etab » (ex: ou=uds).

Chaque branche d'établissement est ensuite subdivisée en sous-branches pour chaque type d'information. Les contenants ainsi créés sont :

- « ou=se » : détaille la structure d'enseignement de l'établissement ;
- « ou=recherche » : détaille la structure de recherche ;
- « ou=composantes » : définis les composantes et services de l'établissement.

Dans le cas de l'UdS, ces informations sont issues des applications de gestion des ressources humaines (Harpège), de scolarité (Apogée), de gestion financière et comptable (Nabuco) et de gestion de la recherche (Graal).



5.5.2 Schémas

Les schémas concernant le référentiel sont en cours d'étude.

5.6 Autorisations d'accès à l'annuaire d'établissement

L'annuaire d'établissement de l'UdS contient de nombreuses informations sensibles, qui ne doivent pas être accessibles au public. C'est aussi la source principale d'informations pour de nombreuses applications. Enfin, c'est également une synthèse d'informations issues de plusieurs applications de gestion.

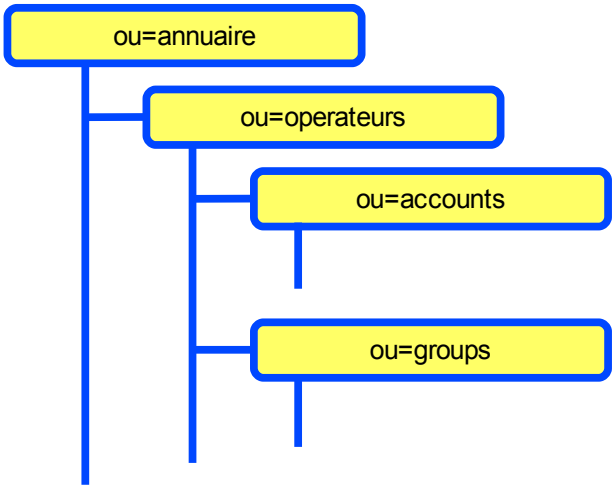
Les interactions des différentes applications avec l'annuaire sont donc nombreuses, mais doivent rester contrôlées. L'annuaire restreint donc les accès sur la base des « access-lists » du serveur LDAP. Ce système permet de réserver l'accès à des ressources uniquement sur certains critères (adresse IP, valeur d'un attribut, etc.), et de limiter le type d'accès (lecture, écriture, etc).

L'identification des accès à l'annuaire se fait par authentification des applications et des personnes. C'est sur l'identifiant fourni lors de l'authentification qu'est effectuée la restriction d'accès aux informations. L'annuaire contient donc une structure dédié à la déclaration des identifiants autorisés à y accéder.

5.6.1 Arborescence

La structure de données contenant les autorisations d'accès à l'annuaire se situe dans la branche « ou=operateurs ». Cette branche est subdivisée en deux sous-branches :

– « ou=accounts » : déclaration des identifiants de connexion à l'annuaire pour les applications.
– « ou=groups » : groupes d'utilisateurs issus de la branche « ou=people ». Les autorisations d'accès porteront sur ces groupes plutôt que sur les personnes individuelles.



5.6.2 Schémas

Les classes d'objets utilisés pour la déclaration de ces entrées sont des classes standards spécifiées en détail dans la RFC 2256.

5.6.2.1 la classe organizationalPerson

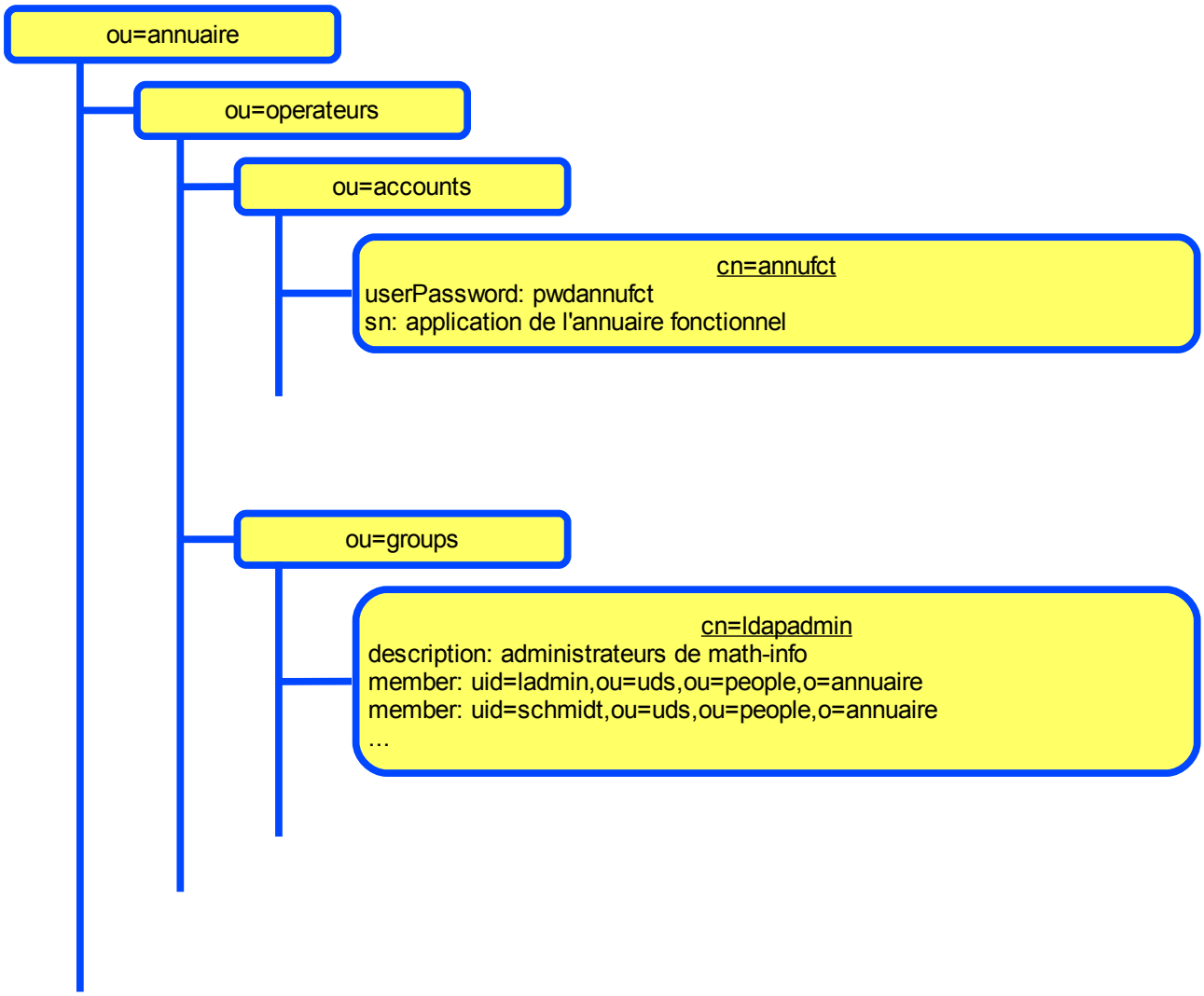
Cette classe est utilisée pour définir des entrées pour les applications.

5.6.2.2 la classe groupOfNames

Cette classe permet de créer des groupement d'entrées LDAP. Cette classe est utilisée dans la sous-branche « ou=groups » pour définir des groupes de personnes (via leur DN). Les access-list autorisent ensuite les groupes d'utilisateurs à accéder aux ressources.

5.6.3 Exemple

L'exemple suivant présente la déclaration d'un compte pour l'application d'annuaire fonctionnel, ainsi que la déclaration du groupe d'administrateurs de l'annuaire.


ou=annuaire
ou=operateurs
ou=accounts
cn=annufct
userPassword: pwdannufct
sn: application de l'annuaire fonctionnel
ou=groups
cn=ldapadmin
description: administrateurs de math-info
member: uid=ladmin,ou=uds,ou=people,o=annuaire
member: uid=schmidt,ou=uds,ou=people,o=annuaire
...

5.7 Téléphonie

Les structures de données concernant la téléphonie sont en cours d'étude.

5.8 Active Directory

L'objectif de proposer un identifiant unique dans le système d'information nécessite la prise en compte des postes de travail clients. Dans cette optique, le problème suivant se pose : le mot de passe chiffré de l'annuaire LDAP n'est pas utilisable directement par les sytèmes Microsoft pour authentifier les utilisateurs.

Plusieurs méthodes sont à l'étude pour résoudre cette incompatibilité :

1. Modification de la mire Windows pour authentifier sur le serveur LDAP UdS (application pGina : http://www.pgina.org)
2. Mise en place d'un serveur Kerberos, et approbation bidirectionelle des REALMS
3. Approbation du serveur Kerberos dans le cas des postes windows sans réseau AD (même configuration que l'approbation de domaine)
4. Migration des domaines AD vers samba 3 (Intégration fine à l'annuaire)
5. Utilisation de webservice pour la synchronisation de mots de passe entre l'annuaire LDAP et la base Active Directory

A part la solution 4, l'emploi d'outils d'approvisionnement complémentaires est nécessaire.

Les solutions 2 ou 3 permettent d'avoir un vrai référentiel unique de mot de passe, sans nécessiter la synchronisation de deux bases différentes. De plus, elles permettent d'offrir un vrai SSO complet dès l'ouverture de session. Le changement de mot de passe sur le poste client est possible, avec remontée automatique dans le référentiel.

La solution 4 permet de déléguer la gestion complète au serveur LDAP via un domaine samba.

6 Interaction avec les composantes

6.1 Objectifs

La mise en place du nouvel annuaire représente l'occasion de proposer aux composantes et aux laboratoires un nouveau service d'hébergement de leur annuaire local. Pour les composantes, l'intérêt est multiple :

- disposer d'une offre « clefs en main » d'hébergement d'annuaire, matérielle et logicielle ;
- disposer d'un hébergement performant et à haute disponibilité ;
- disposer de données en provenance directe des bases de gestion ;
- offrir un identifiant et un mot de passe uniques à tous les utilisateurs de la composante (personnels, étudiants, etc.) ;
- simplification des procédures de gestion des comptes : un seul annuaire à alimenter pour toutes les applications.

Pour l'établissement, l'adoption d'une telle offre d'hébergement constitue un environnement favorable pour améliorer la fiabilité des données présentes dans l'annuaire. Par ailleurs, une telle offre représente une économie d'échelle tant sur le plan humain que sur le plan matériel.

6.2 Schémas supportés

Un certain nombre de schémas applicatifs est proposé. Les applications concernées sont celles le plus souvent utilisées dans la gestion d'un système informatique de composante ou de laboratoire :

- NIS : gestion des utilisateurs sur systèmes UNIX (nis.schema et cosine.schema)
- Samba : Partage de données entre systèmes UNIX et Windows (samba.schema)
- Pykota : gestion des quotas d'impression (pykota.schema)
- Automount : montage NFS automatique sur un poste client (automount.schema)

Les demandes de schémas supplémentaires seront examinées au cas par cas.

6.3 La branche « ou=composantes »

Les données propres aux composantes sont stockées dans la branche « ou=composantes ». Chaque composante ou laboratoire utilisant l'annuaire d'établissement dispose de sa sous-branche spécifique. Celle-ci comporte d'office une branche « ou=people », contenant les utilisateurs de la composante. Ces derniers sont définis par une « adoption » des utilisateurs par la composante. Cette opération manuelle est effectuée par le(s) correspondant(s) informatiques de chaque composante.

Les informations d'authentification (identifiant et mot de passe), les informations d'état civil (nom, prénom, etc.) et les informations de contact (téléphone, adresse de messagerie, etc.) des utilisateurs adoptés sont répliquées et synchrones avec la branche « ou=people » principale.

Hormis pour ces informations, les correspondants réseau ont la possibilité de gérer le contenu de leur branche à leur guise (dans la limite des schémas supportés). Ils ont la possibilité d'ajouter des attributs aux personnes, de créer des branches supplémentaires pour y déclarer des paramètres applicatifs (ex: groupes POSIX).

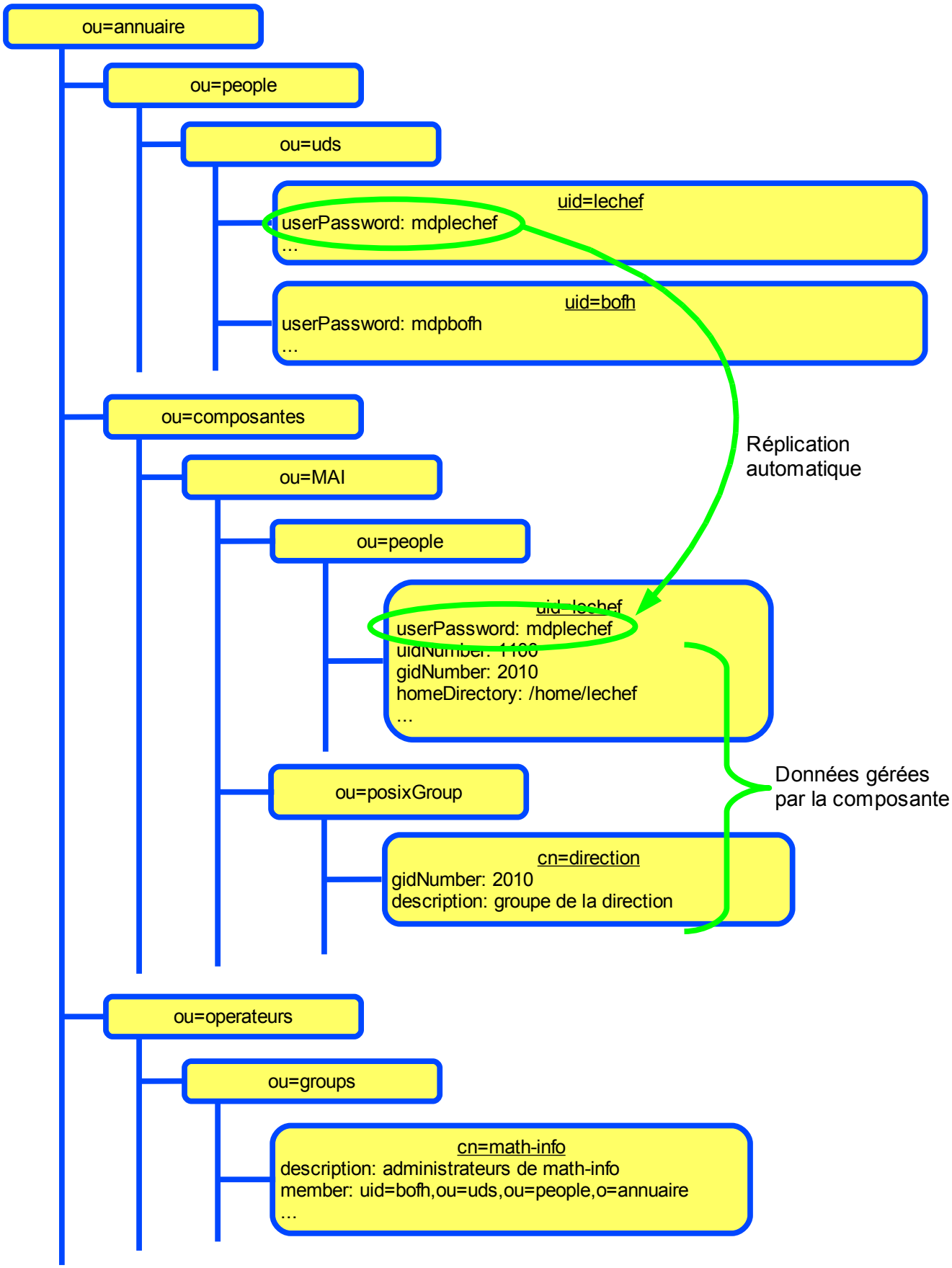
Une même personne peut être adoptée par plusieurs composantes différentes. Chaque composante pourra lui attribuer ses paramètres propres, sans interférer avec ceux des autres composantes.

6.4 Accès à l'annuaire

Les accès à l'annuaire sont effectués directement via le protocole LDAP. Les autorisations d'accès sont décrites dans le paragraphe 5.6.

6.5 Exemple

L'exemple fictif ci-après présente un aperçu de la sous-branche « ou =composantes », ainsi que l'affection d'un correspondant réseau au groupe autorisé à gérer les utilisateurs de sa composante.


ou=annuaire
ou=people
ou=uds
uid=lechef
userPassword: mdplechef
...
uid=bofh
userPassword: mdpbofh
...
ou=composantes
ou=MAI
ou=people
uid=lechef
userPassword: mdplechef
gidNumber: 2010
homeDirectory: /home/lechef
...
ou=posixGroup
cn=direction
gidNumber: 2010
description: groupe de la direction
ou=operateurs
ou=groups
cn=math-info
description: administrateurs de math-info
member: uid=bofh,ou=uds,ou=people,o=annuaire
...
Réplication automatique
Données gérées par la composante

7 Migration vers le nouvel annuaire d'établissement UdS

La situation actuelle (plusieurs annuaires dans les différents services et établissements) est appelée à perdurer tant que toutes les applications n'auront pas été migrées vers le nouvel annuaire décrit dans cette documentation.

Afin de faciliter la transition vers ce nouvel annuaire, celui-ci sera mis en production au plus tard le premier janvier 2009, tout en conservant les anciens annuaires. Dès la disponibilité du nouvel annuaire, les applications pourront progressivement être migrées.

Cette phase transitoire nécessaire pour la migration se terminera à la rentrée de septembre 2009, date à laquelle l'ancien annuaire source (actuellement hébergé au SIIG) sera arrêté, ainsi que les autres anciens annuaires. À cette date, l'intégralité des applications devra avoir été modifiée pour utiliser le nouvel annuaire.