

MENJVA

MESR

DÉFINITION ET CONCEPTION DE L'ANNUAIRE ENT

*Cahier des charges de l'annuaire ENT
(document principal)*



Sujet : Ce document constitue le cahier des charges pour la fourniture
d'une solution d'annuaire pour l'ENT.

Référence : AnnuaireENT_v1.54

Version : 1.54

Date : 6 mai 2011

Nb pages : 75

FICHE DE CONTROLE DU DOCUMENT

Suivi des versions

Version	Date	Class.	Rédacteur	Modification
1.02	13/07/2005	DR	Solucom	Première diffusion restreinte
1.09	02/05/2006	P	Solucom	<i>[Document de travail]</i> Mise à jour des modalités d'alimentation depuis le SI MENESR Corrections mineures
1.50	18/12/2006	P	Solucom	Version stabilisée
1.51	22/03/2007	P	Solucom	Corrections mineures sur les attributs LDAP
1.52	30/04/2007	P	Solucom	Corrections mineures sur les attributs LDAP Les annexes deviennent des documents indépendants
1.52a	02/07/2007	P	Solucom	Modifications sur l'attribut <i>personalTitle</i> Précision sur le préfixe de la clé de jointure
1.52b	07/11/2007	P	Solucom	Corrections mineures d'écarts entre les annexes 2 et 3
1.53	06/05/2011	P	IBM	Modifications mineures sur les attributs LDAP

Classification (Class.) : P : Public – DR : Diffusion Restreinte – C : Confidentiel

TABLE DES MATIERES

1.	INTRODUCTION	6
2.	PRESENTATION GENERALE DE L'ANNUAIRE ENT	8
2.1.	QU'EST-CE QUE L'ANNUAIRE ENT ?	8
2.2.	PRINCIPES DIRECTEURS DE L'ANNUAIRE ENT	9
2.3.	VUE D'ENSEMBLE DE L'ANNUAIRE ENT	10
3.	CONTENU DE L'ANNUAIRE ENT	12
3.1.	PERIMETRE DES DONNEES	12
3.2.	MODELE DE SECURITE	13
3.3.	CARACTERISATION DES PERSONNES	17
4.	SCHEMA ET DIT DE L'ANNUAIRE ENT.....	27
4.1.	PREAMBULE	27
4.2.	DESCRIPTION DES CLASSES D'OBJET DE L'ANNUAIRE ENT	28
4.3.	DIT DE L'ANNUAIRE ENT	42
4.4.	ATTRIBUTS PARTICULIERS.....	43
5.	ARCHITECTURE TECHNIQUE DE L'ANNUAIRE ENT	47
5.1.	PRINCIPES D'ARCHITECTURE.....	47
5.2.	ARCHITECTURE – OPTION 1.....	48
5.3.	ARCHITECTURE – OPTION 2.....	49
5.4.	ARCHITECTURE – OPTION 3.....	50
6.	ANNUAIRE ET ACCES INTER-ENT	52
7.	SERVICES DE L'ANNUAIRE ENT	56
7.1.	SERVICES DE GESTION	56
7.2.	SERVICES D'ACCES	63
7.3.	SERVICES TECHNIQUES	66
7.4.	API DE SERVICE	68
8.	EXIGENCES SUR L'ANNUAIRE ENT	69
9.	ORGANISATION ET PROCESSUS TYPES DE GESTION DE L'ANNUAIRE ENT	71
9.1.	ORGANISATION TYPE DE LA GESTION DES DROITS D'ACCES.....	71
9.2.	PROCESSUS TYPE DE GESTION.....	72

LISTE DES ILLUSTRATIONS

Figure 1 : Architecture fonctionnelle de la solution d'annuaire ENT	10
Figure 2 : Modèle de sécurité de l'annuaire ENT	13
Figure 3 : Exemple de gestion des droits sur une application de l'ENT	15
Figure 4 : Caractérisation des personnes de l'annuaire ENT	17
Figure 5 : Caractérisation d'un Élève	18
Figure 6 : Caractérisation d'une Personnes en relation avec un élève.....	19
Figure 7 : Caractérisation d'un Enseignant	20
Figure 8 : Caractérisation d'un Non enseignant	21
Figure 9 : Caractérisation d'un Personnel extérieur	22
Figure 10 : Caractérisation d'un Tuteur de stage ou maître d'apprentissage	23
Figure 11 : Caractérisation d'un Responsable d'entreprise	24
Figure 12 : Schéma LDAP de l'annuaire ENT	31
Figure 13 : DIT de l'annuaire ENT	42
Figure 14 : Solution d'architecture de l'annuaire ENT	48
Figure 15 : Architecture – Option 1	49
Figure 16 : Architecture – Option 2	50
Figure 17 : Architecture – Option 3	51
Figure 18 : Accès d'un utilisateur à une application d'un autre ENT	53

CONVENTIONS TYPOGRAPHIQUES

Cette mise en forme indique les recommandations faites au porteur de projet afin d'adapter le cahier des charges à ses besoins. Il s'agira notamment de compléter ou préciser certaines attentes en fonction de son projet ENT.

Cette mise en forme indique une précision complémentaire adressée au porteur sur les principes de ce document. Ces précisions pourront être supprimées du cahier des charges définitif.

Cette mise en forme indique au lecteur un point d'attention particulièrement important.

1. INTRODUCTION

OBJET DU DOCUMENT

Le porteur choisira une des deux formulations proposées ci-dessous en fonction de l'objet du document :

Ce document constitue une annexe au cahier des charges de l'ENT. Il définit le cahier des charges de l'annuaire ENT.

Ce document définit le cahier des charges de l'annuaire ENT.

Ce document a été élaboré à partir du cadre générique issu des travaux du Ministère de l'Éducation Nationale, de l'Enseignement Supérieur et de la Recherche (MENESR) et de la Caisse des Dépôts et Consignations (CDC). Il a été complété par les exigences spécifiques au projet **[NOM_PROJET_ENT]**.

PLAN DU DOCUMENT

Ce document est composé des parties suivantes :

- Le chapitre 2 présente une vue d'ensemble de l'annuaire ENT et précise ses principes directeurs.
- Le chapitre 3 décrit le contenu de l'annuaire ENT en termes de périmètre couvert, de modèle de sécurité et de caractérisation des personnes.
- Le chapitre 4 décrit le schéma LDAP et le DIT de l'annuaire ENT, et précise comment sont gérés certains objets ou attributs particuliers.
- Le chapitre 5 définit les principes d'architecture de l'annuaire ENT et les options envisageables.
- Le chapitre 6 présente les besoins d'accès inter-ENT et définit le fonctionnement de la solution à mettre en œuvre.
- Le chapitre 7 décrit les services attendus de l'annuaire ENT, notamment en termes de gestion et d'accès.
- Le chapitre 8 définit les exigences attendues de l'annuaire ENT.
- Le chapitre 9 décrit l'organisation et les processus de gestion types de l'annuaire ENT.

ANNEXES (DOCUMENTS INDEPENDANTS)

- L'Annexe 1 présente le glossaire du cahier des charges et le lexique des notions spécifiques aux MENESR (référence : Glossaire_v1.52).
- L'Annexe 2 décrit les caractéristiques des personnes et des structures de l'annuaire ENT (référence : PersonnesStructures_v1.52).

- L'Annexe 3 définit le schéma LDAP de l'annuaire ENT et les nomenclatures utilisées pour chaque attribut (référence : SchemaLDAP_v1.52).
- L'Annexe 4/4bis présente les modalités d'alimentation de l'annuaire ENT depuis le SI du MENESR (référence : AlimentationMENESR_v1.52).
- L'Annexe 5 donne la liste des codes identifiants les différents projets ENT (référence : CodesProjets_v1.52).

DOCUMENTS DE REFERENCE

[1] Documents de spécification d'un socle ENT, MENESR/CDC/DICTAO, v2.0 (31/10/2005), <http://www2.educnet.education.fr/sections/services/ent/sdet/>.

Le porteur pourra remplacer les documents de référence susmentionnés par le cahier des charges de son ENT.

[2] Recommandations pour la gestion de l'Authentification-Autorisation-SSO : AAS (annexe du Schéma Directeur des Espaces numériques de Travail), MENJVA, v3.0 (2011), <http://www.educnet.education.fr/services/ent/sdet> (sur Eduscol à partir du 1^{er} septembre 2011).

[3] Base Centrale des Nomenclatures du MENESR, <http://www.infocentre.education.fr/bcn/>.

Notons que le cahier des charges a été constitué en s'appuyant sur des travaux connexes ayant abouti aux résultats suivants :

- Documents sur l'Annuaire Fédérateur MENESR, <http://www.orion.education.fr/dpma-a3>.
- PRISME-Lorraine : Cahier des clauses techniques particulières, Conseil Régional de Lorraine.
- Recommandations pour les annuaires de l'enseignement supérieur : SUPANN, MENESR, v1.0, <http://www.cru.fr/ldap/supann/recomm/SUPANN-V10.pdf>.
- Schémas d'annuaires et schémas de registres de ressources numériques interopérables pour les administrations, ADAE (ex-ATICA), février 2003, http://www.adele.gouv.fr/sdae/upload/documents/Annexe_4a_schemas_annuaires_interoperables.pdf.

2. PRESENTATION GENERALE DE L'ANNUAIRE ENT

2.1. QU'EST-CE QUE L'ANNUAIRE ENT ?

Dans le cadre des Espaces Numériques de Travail de **l'enseignement secondaire**, l'annuaire ENT est l'annuaire des personnes et des structures en relation avec le Ministère de l'Éducation Nationale, le Ministère de l'Agriculture et les collectivités locales. Il comprend notamment les élèves, les parents d'élèves, les enseignants, les personnels administratifs...

L'annuaire ENT présente la spécificité que certaines personnes peuvent appartenir à plusieurs catégories. Par exemple, un enseignant peut également être parent d'un élève ou encore assurer des fonctions administratives dans un établissement, en tant que chef d'établissement notamment. L'annuaire ENT doit permettre de gérer une unique identité tout en autorisant le cumul des catégories.

Différents projets d'ENT pour l'enseignement secondaire sont ou seront lancés sous le pilotage des collectivités locales en collaboration avec le MENESR. Chaque projet ENT, et donc **chaque annuaire d'ENT**, couvre couramment un **périmètre départemental ou régional**, soit les personnes et structures du périmètre concerné.

Par défaut, le **chef d'établissement** est le **propriétaire** des données de l'annuaire sur le périmètre de son établissement (*cette responsabilité peut être répartie au sein de l'équipe de direction de l'établissement, voire déléguée à d'autres acteurs*).

L'annuaire ENT permet directement ou à travers d'autres services d'offrir les fonctions suivantes :

- **Des services de sécurité**, tels que l'authentification des utilisateurs de l'ENT sur les applications de l'ENT et le contrôle de leur accès à ces applications. Cela recouvre la notion « d'annuaire de sécurité ENT ».
- **Des services d'accès à des informations**, qui caractérisent et qualifient les personnes ou les structures en relation avec l'ENT et recouvrent la notion « d'annuaire fonctionnel ENT ».

Dans la suite du document, seul le terme « annuaire ENT » sera utilisé.

En complément, l'annuaire ENT embarque des services de gestion des identités et d'administration des droits ou habilitations.

Ces services sont offerts exclusivement aux utilisateurs de l'ENT et aux applications reposant sur le socle ENT. Dans ce cas, les applications du socle ne gèreront pas en propre les données qui sont déjà disponibles dans l'annuaire ENT.

Des accès croisés sont attendus entre différents ENT. Il s'agit alors de permettre à un utilisateur d'un ENT d'accéder à des applications hébergées par un autre ENT. Pour y parvenir, il est nécessaire de définir un **cadre d'interopérabilité** entre les ENT.

Conformément à l'arrêté du 30/11/2006 relatif aux ENT¹, le Système d'Information (SI) du MENESR constitue une source autoritaire majeure pour les données de l'annuaire ENT². Des interfaces locales pourront si nécessaire être mises en place avec l'annuaire ENT. Enfin, l'annuaire ENT n'a pas, de son côté, vocation à alimenter les référentiels de différents SI.

2.2. PRINCIPES DIRECTEURS DE L'ANNUAIRE ENT

Les principaux objectifs poursuivis à travers la définition du cahier des charges de l'annuaire ENT sont les suivants :

- **Faciliter au maximum la construction des ENT** en définissant et en standardisant l'annuaire ENT pour tous les projets ENT.
- **Garantir le fonctionnement de l'ENT** (couverture des services minimum attendus, niveau de sécurité, niveau de performances...) et permettre **les accès inter-ENT** souhaités (ou avec des services tiers).

Ces objectifs sont à atteindre dans un environnement où les éléments contextuels suivants sont à prendre en compte :

*Les projets ENT sont multiples, sur des périmètres différents. En conséquence, ils doivent généralement prendre en compte des **spécificités** qui leur sont propres. Le cahier des charges n'a certainement pas été exhaustif dans la prise en compte de la **multiplicité des attentes**.*

*Enfin, ces besoins multiples vont nécessairement **évoluer dans le temps**.*

L'approche suivante a alors été privilégiée :

- Tous les besoins connus et conformes au cadre de l'annuaire ENT sont pris en compte en proposant un **modèle riche et des normes pour ce modèle** (*logique de faciliter la construction*).
- Dans ce modèle, seul **un minimum³ est obligatoire** et doit absolument respecter les normes proposées (*il s'agit d'un cadre à respecter pour garantir le fonctionnement de l'ENT et les accès inter-ENT*).
- Chaque ENT dispose **d'espaces de liberté propres** autour du minimum à respecter ; ces espaces de liberté concernent l'utilisation, l'ajout ou la suppression de certaines informations de l'annuaire, l'utilisation ou non des normes proposées ou encore la mise en place de tel ou tel service (*prise en compte des spécificités locales et de leurs évolutions dans le temps*).

■

¹ Arrêté du 30 novembre 2006 portant création, au sein du Ministère de l'Éducation Nationale, de l'Enseignement Supérieur et de la Recherche, d'un traitement de données à caractère personnel relatif aux Espaces Numériques de Travail (ENT), publié au Journal Officiel du 13 décembre 2006.

² Les modalités d'alimentation de l'annuaire ENT depuis le SI du MENESR sont détaillées à l'Annexe 4.

³ Notons que le minimum est défini dans la suite du document par :

- Les identifiants pour les entrées utilisateurs, profils des utilisateurs et applications.
- Les attributs ou caractéristiques obligatoires dans l'annuaire ENT pour toutes les entrées (cf. chapitre 4.2).
- Les données normées de l'annuaire permettant l'accès inter-ENT (cf. chapitre 6).
- Les services de base de l'annuaire (cf. chapitre 7).

2.3. VUE D'ENSEMBLE DE L'ANNUAIRE ENT

L'annuaire ENT ou la solution d'annuaire ENT se compose de plusieurs briques fonctionnelles représentées ci-dessous.

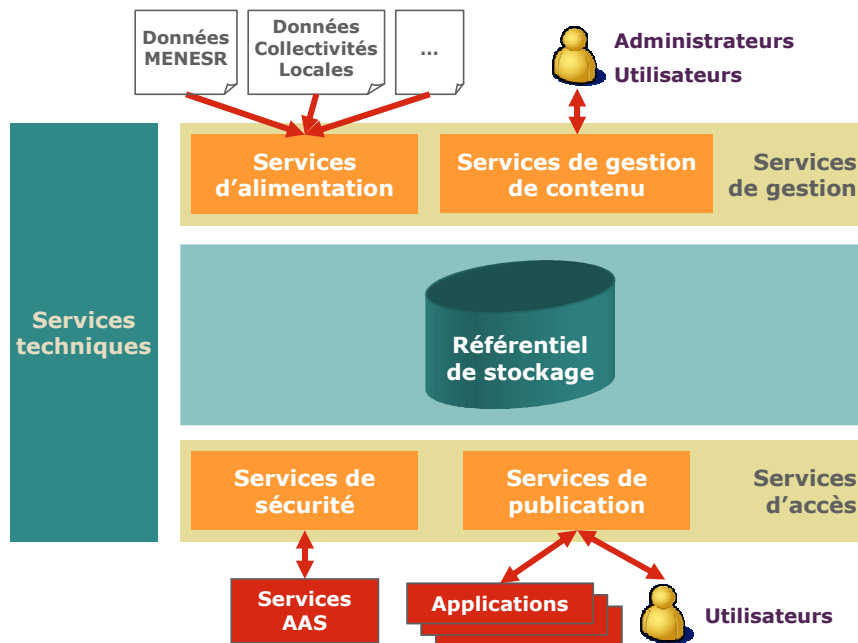


Figure 1 : Architecture fonctionnelle de la solution d'annuaire ENT

Les briques fonctionnelles sont les suivantes :

- Un référentiel de stockage contenant l'ensemble des données / informations sur les personnes et les structures sur le périmètre couvert. Il propose plusieurs API d'accès à son contenu.
- Des services de gestion :
 - ▶ Les services d'alimentation permettent de peupler et de mettre à jour l'annuaire ENT à partir de différentes sources de données.
 - ▶ Les services de gestion de contenu permettent aux administrateurs et aux utilisateurs de modifier certaines informations contenues dans le référentiel.
- Des services d'accès :
 - ▶ Les services de sécurité de l'annuaire ENT sont utilisés par les services AAS (Authentification-Autorisation-SSO) pour répondre aux requêtes d'authentification et d'autorisation.
 - ▶ Les services de publication sont utilisés par les applications pour récupérer des informations partagées entre les applications et permettent aux utilisateurs de visualiser le contenu de l'annuaire ENT.
- Des services techniques assurant la supervision, la gestion des traces et des audits, les sauvegardes et les restaurations.

Les attentes vis-à-vis de chacune de ces briques fonctionnelles sont détaillées dans la suite du document.

Notons que cette vue logique de l'annuaire ENT ne présume pas des orientations techniques qui doivent être proposées par le soumissionnaire. Il n'est pas exclu qu'une même solution couvre plusieurs briques fonctionnelles. Le soumissionnaire précisera et justifiera dans sa réponse les orientations techniques qu'il a choisies.

3. CONTENU DE L'ANNUAIRE ENT

3.1. PERIMETRE DES DONNEES

Le périmètre doit être adapté par le porteur en fonction des populations, des structures et des usages prévus par le projet ENT. Exemples : couverture des lycées uniquement, des Centres de Formation des Apprentis (CFA), des établissements agricoles...

Le périmètre couvert par l'annuaire ENT du projet **[NOM_PROJET_ENT]** regroupe l'ensemble des personnes et des structures liées à l'enseignement secondaire pour le périmètre suivant : **A compléter par le porteur : départements et régions concernés**.

CATEGORIES DE PERSONNES

Les catégories de personnes concernées par l'annuaire ENT sont les suivantes :

- Les **élèves** du secondaire scolarisés dans le périmètre du projet.
- Les **personnes en relation avec les élèves** du secondaire scolarisés dans le périmètre du projet.

Couvre a minima les personnes exerçant l'autorité parentale, les personnes hébergeant un élève, les responsables financiers, les correspondants en cas d'urgence.

- Les **enseignants** du secondaire exerçant dans le périmètre du projet.
- Les **non enseignants rattachés administrativement à des services académiques** et exerçant une activité au sein d'un établissement du secondaire dans le périmètre du projet.

Couvre a minima les corps d'inspection et les personnels détachés du rectorat.

- Les **non enseignants rattachés administrativement à une collectivité locale** et exerçant une activité au sein d'un établissement du secondaire dans le périmètre du projet.

Couvre a minima les techniciens et ouvriers de service.

- Les **non enseignants rattachés administrativement à un établissement d'enseignement** du secondaire situé dans le périmètre du projet.

Couvre a minima les chefs d'établissement, certains personnels administratifs ainsi que les personnes des établissements privés.

- Les **personnels extérieurs** recrutés par un établissement d'enseignement secondaire dans le périmètre du projet.

Couvre a minima les prestataires.

- Les **tuteurs de stage et maîtres d'apprentissage** des élèves du secondaire scolarisés dans le périmètre du projet.
- Les **responsables des entreprises partenaires** des établissements d'enseignement secondaire et des services académiques dans le périmètre du projet.

CATEGORIES DE STRUCTURES

Les structures concernées par l'annuaire ENT du projet sont les suivantes :

- Les **établissements d'enseignement** secondaire appartenant au périmètre du projet. Il peut s'agir de tout ou partie des structures d'enseignement référencées par le MENESR et disposant à ce titre d'un numéro UAI (ex-RNE).

Couvre a minima les collèges et les lycées généraux, techniques et professionnels, qu'ils soient publics ou privés.

- Les **services académiques** appartenant au périmètre du projet.

Couvre a minima le rectorat et les services départementaux.

- Les **collectivités locales** appartenant au périmètre du projet.

Couvre a minima les conseils régionaux et les conseils généraux.

- Les **entreprises partenaires** des établissements d'enseignement secondaire et des services académiques appartenant au périmètre du projet.

Couvre a minima les entreprises accueillant des élèves de l'académie en stage ou en apprentissage, les entreprises formant des apprentis, les Chambres de Commerce et d'Industrie et les partenaires socio-culturels.

3.2. MODELE DE SECURITE

Le modèle de sécurité de l'annuaire ENT est représenté sur la figure ci-dessous.

Chaque élément est décrit dans la suite du chapitre.

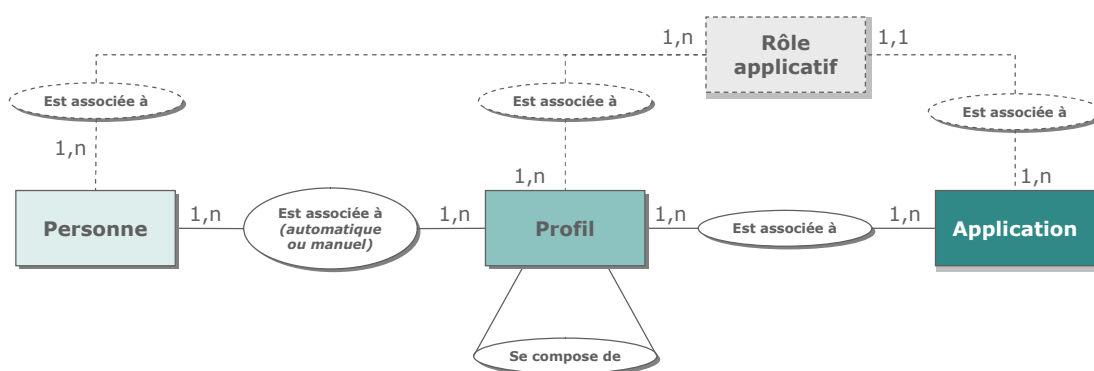


Figure 2 : Modèle de sécurité de l'annuaire ENT

« PERSONNE »

Une Personne est un membre d'une des catégories de personnes définies sur le périmètre adressé par l'annuaire ENT.

Une Personne peut être associée à plusieurs Profils.

Une Personne peut être directement associée (si nécessaire) à plusieurs Rôles applicatifs.

« PROFIL »

Un Profil est un objet de sécurité permettant le regroupement de Personnes selon des caractéristiques particulières propres à la Personne afin de faciliter les actes d'administration.

Un Profil peut être peuplé selon trois modes :

- « Mode Automatique » : une règle de peuplement détermine dynamiquement les Personnes qui appartiennent à un Profil.

Une règle de peuplement automatique d'un Profil correspond à une expression logique sur des couples « attribut / valeur ». Toute Personne dont les attributs vérifient l'expression logique est automatiquement affectée au Profil.

Exemple de règle de peuplement d'un profil correspondant aux élèves de Première et de Terminale technologiques :

(classe d'objet = « Élève ») ET (filière = « Technologique ») ET (niveau = « Première ») OU (niveau = « Terminale »)

Seuls les attributs marqués par une croix dans la colonne « Autorisa. » du tableau de l'Annexe 2 peuvent être utilisés pour définir des règles de peuplement.

Le porteur pourra, s'il le souhaite, baser les règles de peuplement sur des attributs supplémentaires et donc modifier en fonction la liste donnée en Annexe 2. La réplication filtrée (cf. chapitre 5.1) devra être adaptée en conséquence.

- « Mode Discrétionnaire » : les gestionnaires affectent manuellement des Personnes à un Profil.
- « Mode Mixte » : les deux modes précédents sont utilisés pour peupler le Profil.

Les Profils peuvent également être imbriqués (un Profil peut regrouper d'autres Profils) ou exclusifs (cf. chapitre 7.1.2).

La liste des Profils d'une Personne peut également être utilisée dans la règle de peuplement.

Exemple de règle de peuplement d'un profil regroupant l'ensemble du personnel administratif :

(profil = « Secrétariat ») ET (profil = « Personnel de direction »)

« APPLICATION »

Une Application désigne tout service applicatif proposé aux Personnes et utilisant les services du socle ENT.

Les Applications utilisent tout d'abord les services AAS pour contrôler l'authentification d'une Personne en vérifiant la validité des identifiants et des moyens d'authentification présentés.

Les Applications utilisent ensuite les services AAS pour contrôler l'accès de la Personne à l'Application. Les services AAS permettent de vérifier :

- La valeur de certains attributs de la Personne.

Les applications peuvent baser leurs autorisations sur certains attributs du modèle. Ces attributs sont marqués par une croix dans la colonne « Autorisa. » de l'Annexe 2.

Le porteur pourra, s'il le souhaite, baser les autorisations sur des attributs supplémentaires et donc modifier en fonction la liste donnée en Annexe 2. La réplication filtrée (cf. chapitre 5.1) devra être adaptée en conséquence.

- Et/ou l'appartenance de la Personne à au moins un des Profils liés à l'Application.

L'Application utilise les Profils pour définir des droits d'accès macroscopiques.

« ROLE APPLICATIF »

Une Application peut également définir des Rôles applicatifs dans l'annuaire ENT. Un Rôle applicatif donne accès à un ensemble de fonctionnalités au sein de l'application pour laquelle a été défini le Rôle applicatif.

Un Rôle applicatif n'est défini que pour une Application. Un Rôle applicatif peut être associé à plusieurs Profils et plusieurs Personnes directement.

La gestion de droits plus fins reste du ressort des Applications.

EXEMPLE

Le porteur pourra, s'il le souhaite, supprimer ou adapter cet exemple.

Une application de gestion du budget de l'établissement déclare dans l'annuaire ENT des rôles applicatifs, qui pour l'application ont la signification suivante :

- « Responsable » : a accès à toutes les fonctions de l'application.
- « Gestionnaire » : a accès aux fonctions de visualisation et de modification.
- « Utilisateur » : a accès à la fonction de visualisation.

Les profils « Personnels de direction » et « Personnels d'intendance » sont associés au rôle « Responsable », le profil « Personnels administratifs » est associé au rôle « Gestionnaire » et le profil « Conseillers d'éducation » est associé au rôle « Utilisateur ». Le rôle applicatif « Responsable » est directement attribué à une des personnes.

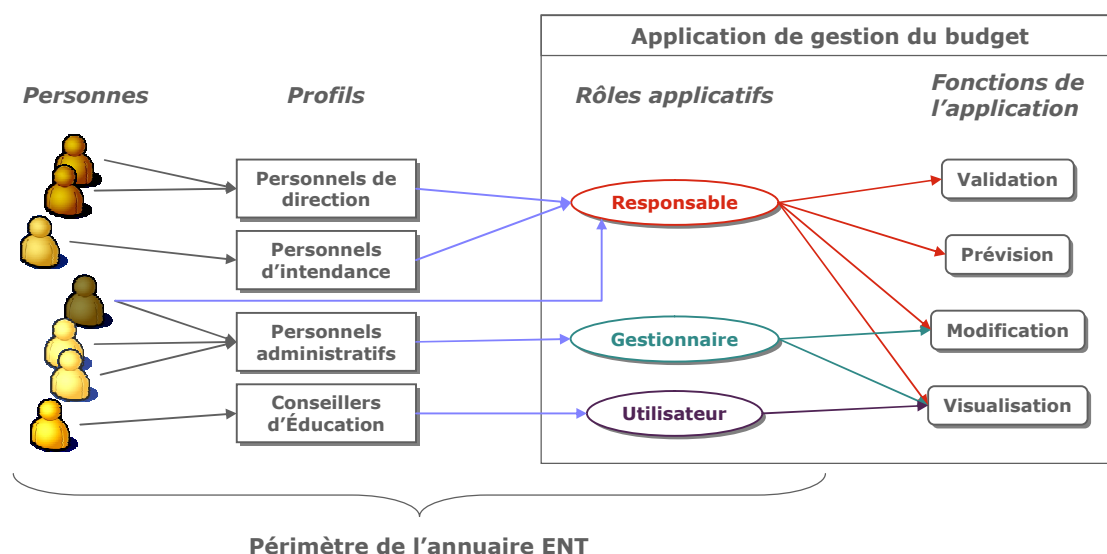


Figure 3 : Exemple de gestion des droits sur une application de l'ENT

REMARQUES

(1) : Le présent document est basé sur les spécifications du socle ENT et des fonctions standard attendues des services AAS. A ce stade, il ne tient pas compte de fonctionnalités spécifiques portées par les services AAS proposés par le soumissionnaire, par exemple challenges, prise en compte de la période d'accès dans l'autorisation, de la typologie d'accès, fonction de suspension d'utilisateurs après échecs...

Le soumissionnaire précisera les impacts de ces fonctions sur le modèle de données de l'annuaire.

(2) : Le modèle présenté peut éventuellement être adapté ou limité en fonction des implémentations proposées par le soumissionnaire :

- Exemples de limitations : pas d'utilisation des groupes dynamiques, limitation de la taille des groupes statiques...
- Exemples d'adaptations : utilisation de la classe d'objet ou d'une combinaison d'attributs existants pour déterminer l'appartenance à un profil partagé⁴... Des solutions différentes pourront notamment être proposées en fonction des catégories de personnes, du fait des différences de volumétrie et de la possibilité ou non d'utiliser la classe d'objet pour déterminer l'appartenance à un profil.

Le soumissionnaire précisera donc, en fonction des capacités des services AAS qu'il propose et de l'impact de la volumétrie sur les performances (cf. chapitre 8), les limitations et les adaptations proposées sur le modèle de sécurité.

⁴ Cf. chapitre 6.

3.3. CARACTERISATION DES PERSONNES

Ce chapitre définit les catégories de personnes et de structures de l'annuaire ENT qui ont été présentées au chapitre 3.1.

Le modèle ci-après prend en compte le fait qu'une personne puisse appartenir à plusieurs catégories. Il peut s'agir par exemple d'un enseignant qui est également parent d'un élève ou encore d'un enseignant qui assure des fonctions administratives dans un établissement (chef d'établissement notamment).

La figure suivante est une illustration de la caractérisation des personnes de l'annuaire ENT.

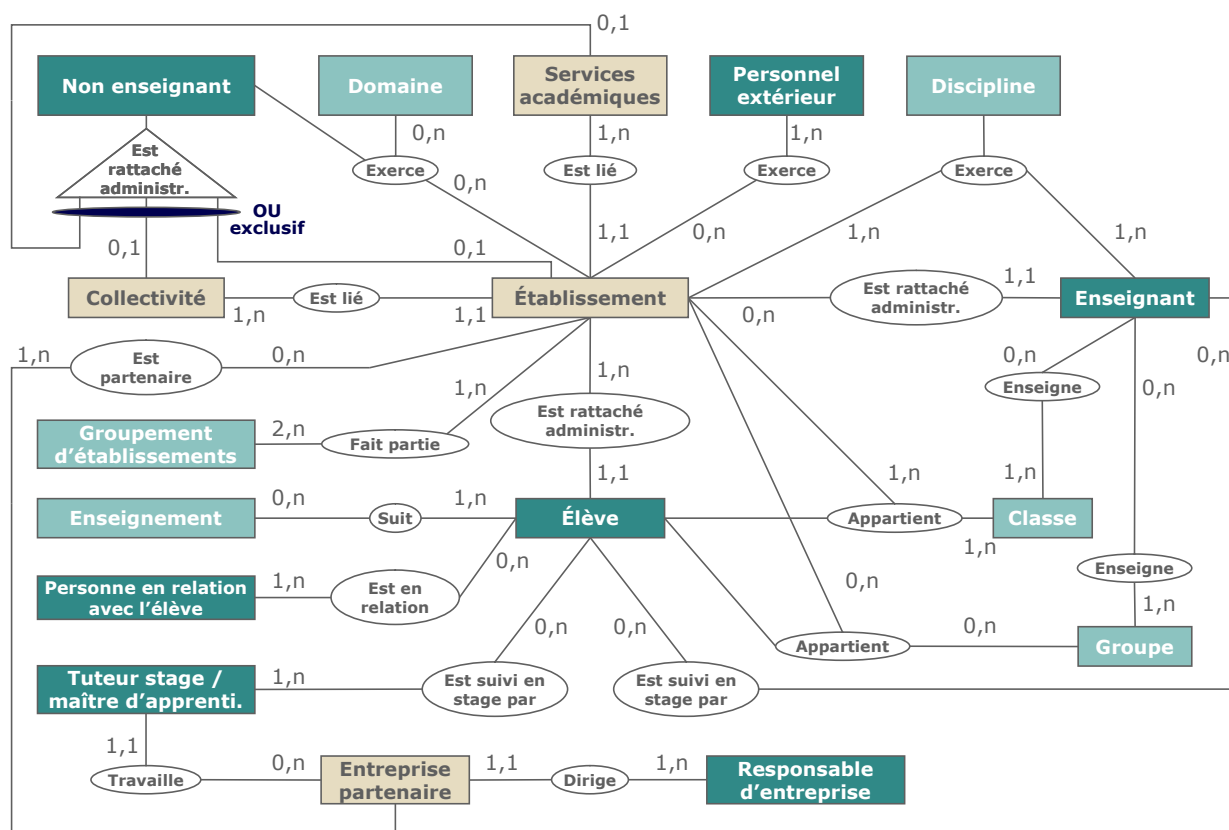


Figure 4 : Caractérisation des personnes de l'annuaire ENT

Les paragraphes ci-après expliquent les relations entre les différents éléments du modèle.

Une description détaillée de chaque élément du modèle d'information est donnée à l'Annexe 2.

DESCRIPTION DES PERSONNES

Élève

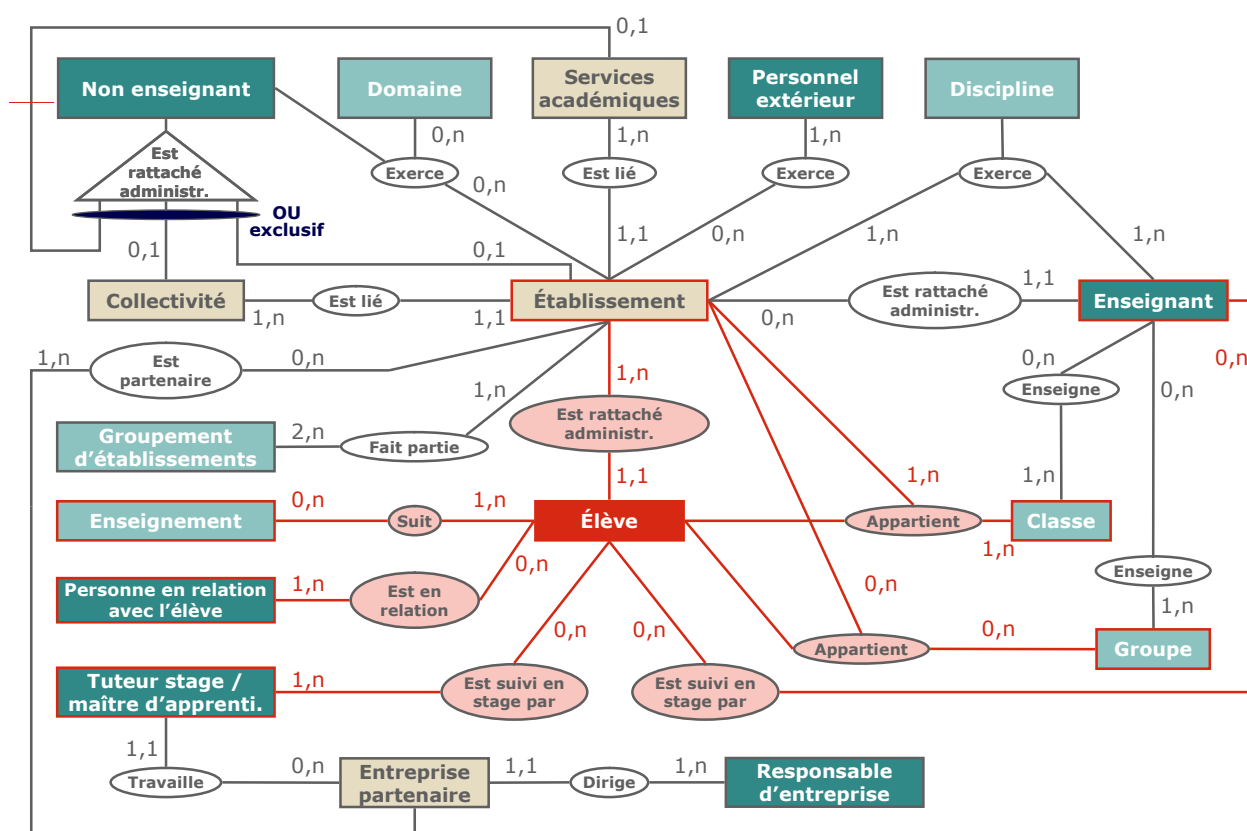


Figure 5 : Caractérisation d'un Élève

Un **Élève** est rattaché administrativement à un et un seul **Établissement**.

Un **Élève** est en relation avec zéro (élève majeur), une, ou plusieurs **Personnes en relation** avec l'élève.

Un **Élève** suit un ou plusieurs **Enseignements**.

Un **Élève** effectue zéro ou un stage/apprentissage simultanément. Pour ce stage/apprentissage, il est suivi par un ou plusieurs **Enseignants**, et un ou plusieurs **Tuteurs de stage ou maîtres d'apprentissage**. **Parmi les Enseignants qui suivent l'Élève durant son stage/apprentissage, un seul est responsable de l'Élève.**

Un **Élève** appartient à zéro, un, ou plusieurs **Groupes**. Ces **Groupes** peuvent se trouver dans des **Établissements** différents.

Un **Élève** appartient au moins à une **Classe**. Un **Élève** peut appartenir à plusieurs **Classes**, **mais à une seule Classe par Établissement**.

Remarque : Dans certains cas, un élève peut être amené à utiliser plusieurs ENT. En effet, si un élève suit des enseignements dans un établissement autre que son établissement de rattachement administratif et que les deux établissements ne sont pas « couverts » par le même ENT, cet élève est géré dans les deux ENT. Ce besoin d'accès à de multiples ENT peut également concerner, dans d'autres rares cas, des enseignants, des personnes en relation avec l'élève ou des non enseignants.

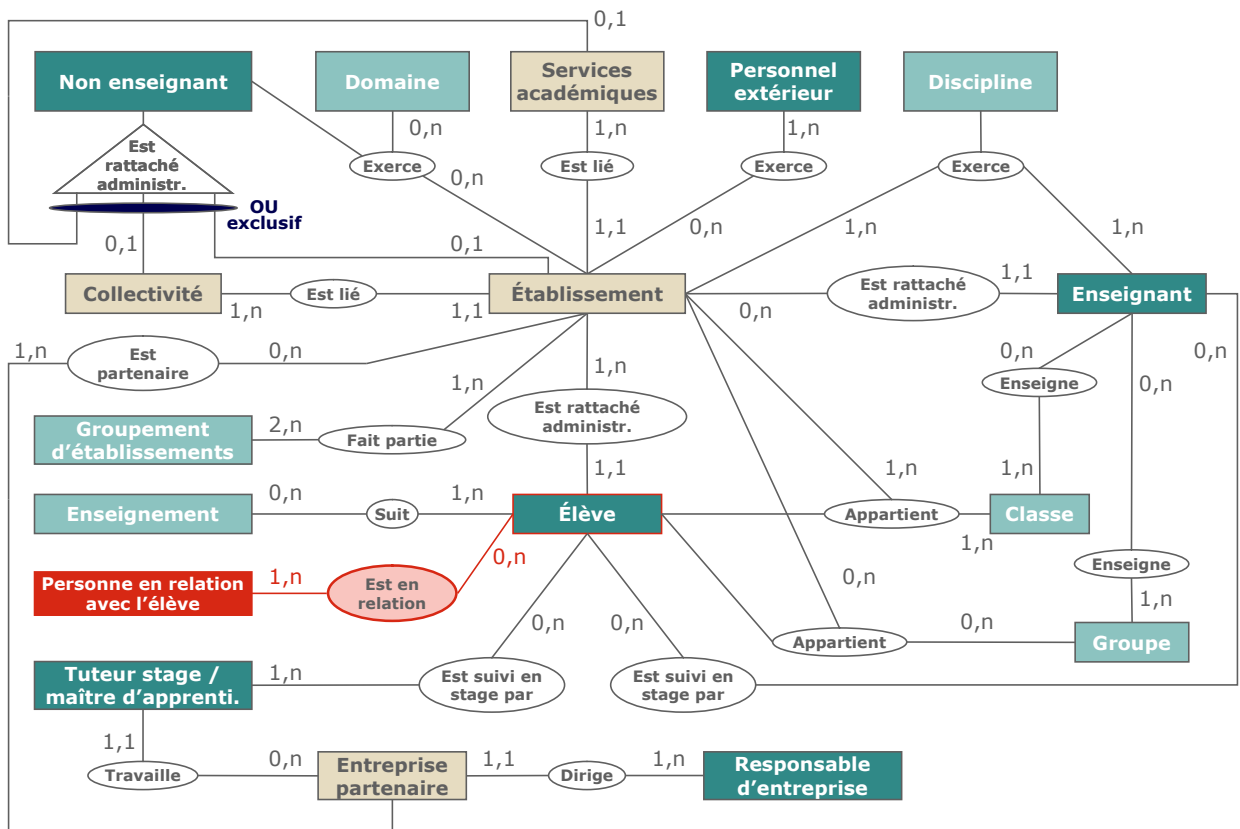
Personne en relation avec l'élève

Figure 6 : Caractérisation d'une Personnes en relation avec un élève

Une *Personne en relation avec l'élève* est en relation avec un ou plusieurs *Élèves*.

Enseignant

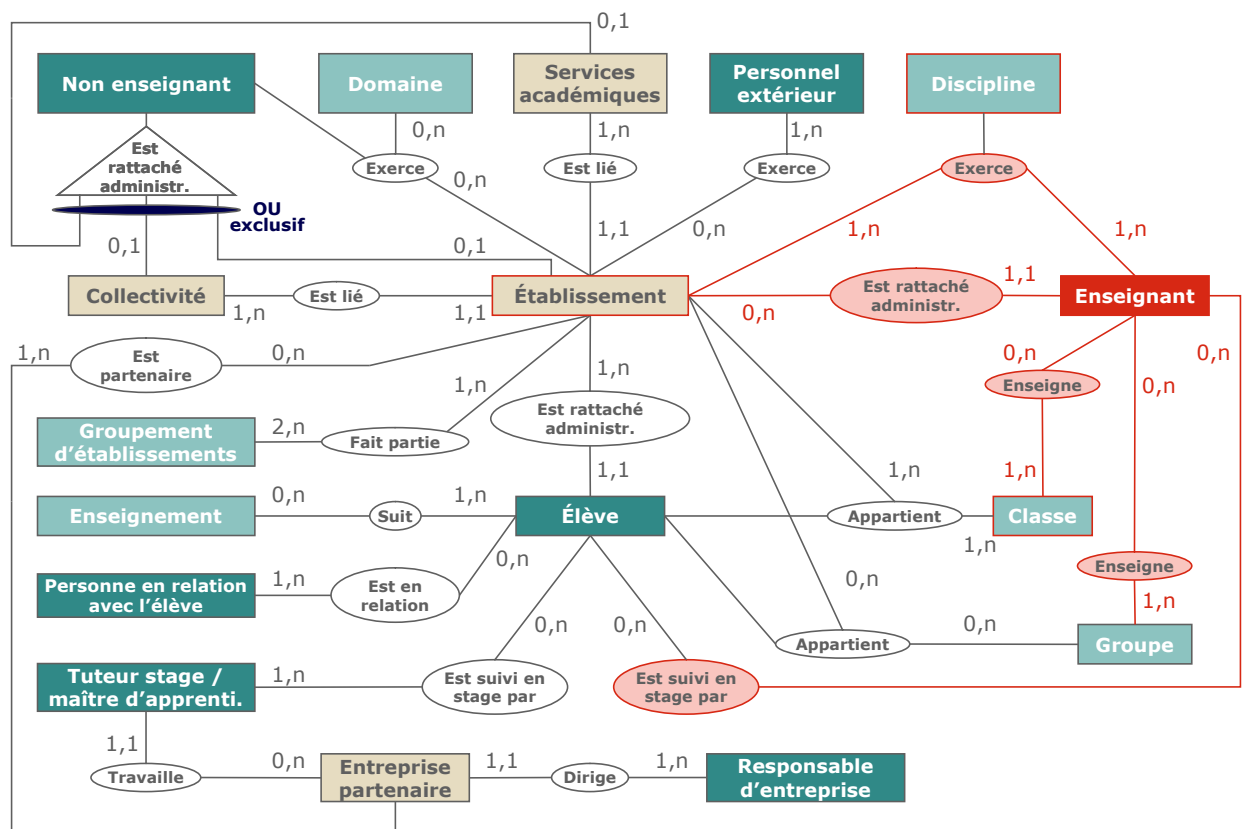


Figure 7 : Caractérisation d'un Enseignant

Un *Enseignant* est rattaché administrativement à un et un seul *Établissement*.

Un *Enseignant* exerce une ou plusieurs *Disciplines* dans un ou plusieurs *Établissements*.

Un *Enseignant* enseigne dans zéro, une, ou plusieurs *Classes*.

Un *Enseignant* enseigne dans zéro, un, ou plusieurs *Groupes*.

Un *Enseignant* suit zéro, un, ou plusieurs *Élèves* durant leur stage/apprentissage. **Parmi les *Enseignants* qui suivent un *Élève* durant son stage/apprentissage, un seul est responsable de l'*Élève*.**

Non enseignant

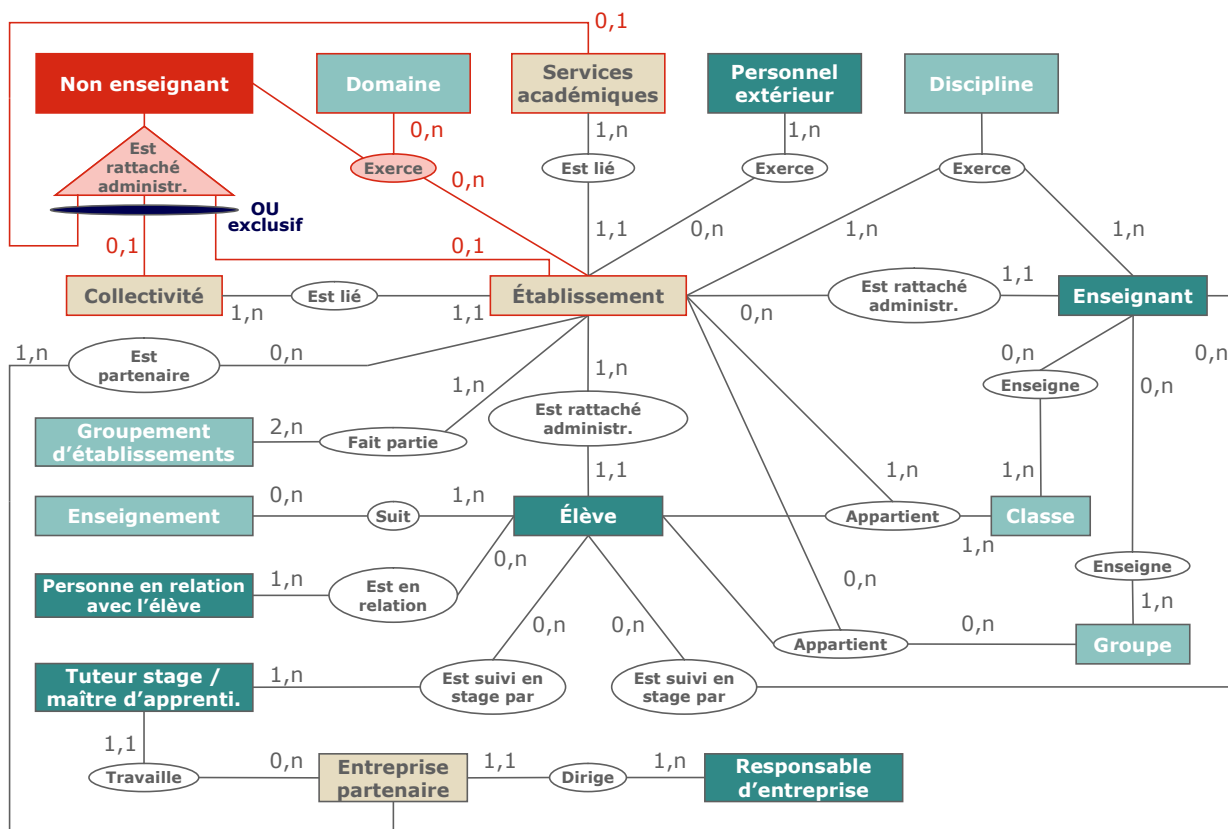


Figure 8 : Caractérisation d'un Non enseignant

Un *Non enseignant* peut exercer une activité dans un ou plusieurs *Domaines*, dans un ou plusieurs *Établissements*.

Un *Non enseignant* est lié soit à une et une seule *Collectivité locale*, soit à un et un seul ensemble de *Services académiques*, soit à un et un seul *Établissement*.

Personnel extérieur

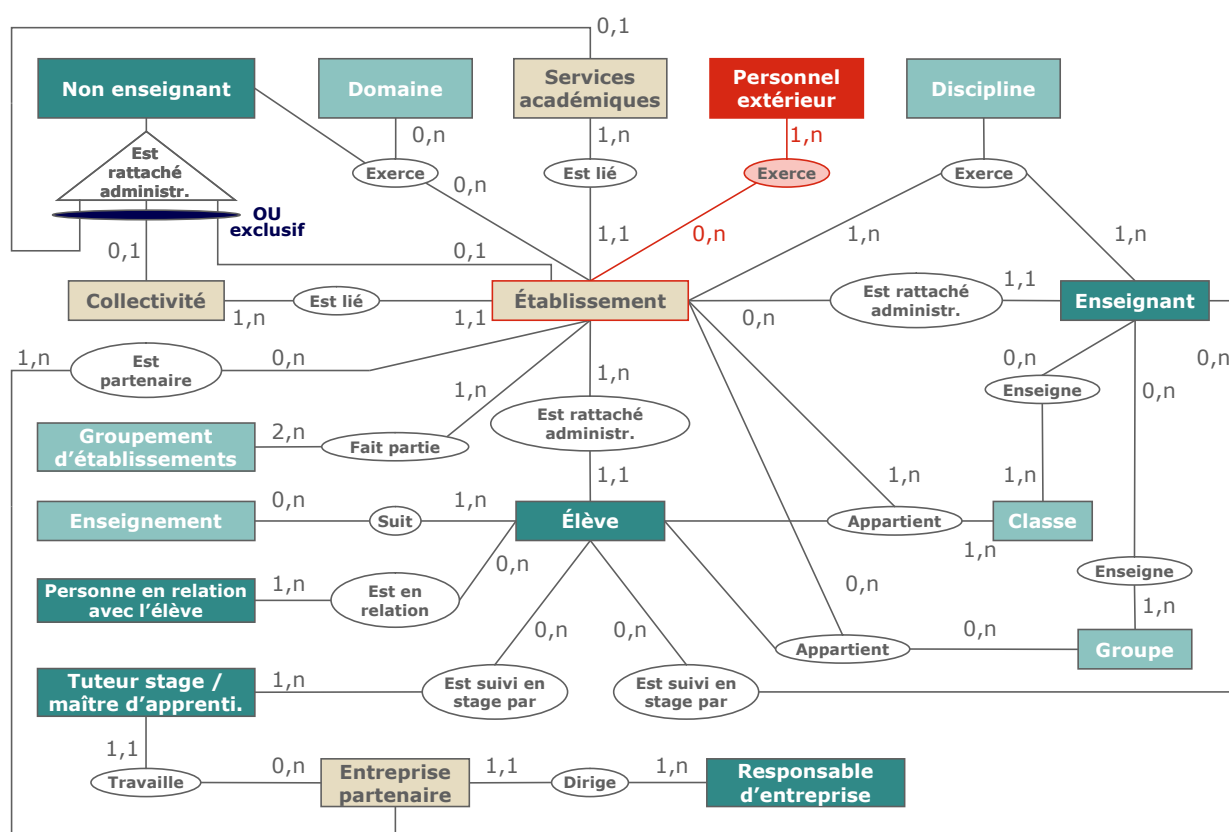


Figure 9 : Caractérisation d'un Personnel extérieur

Un *Personnel extérieur* exerce une activité dans un ou plusieurs *Établissements*.

Tuteur de stage ou maître d'apprentissage

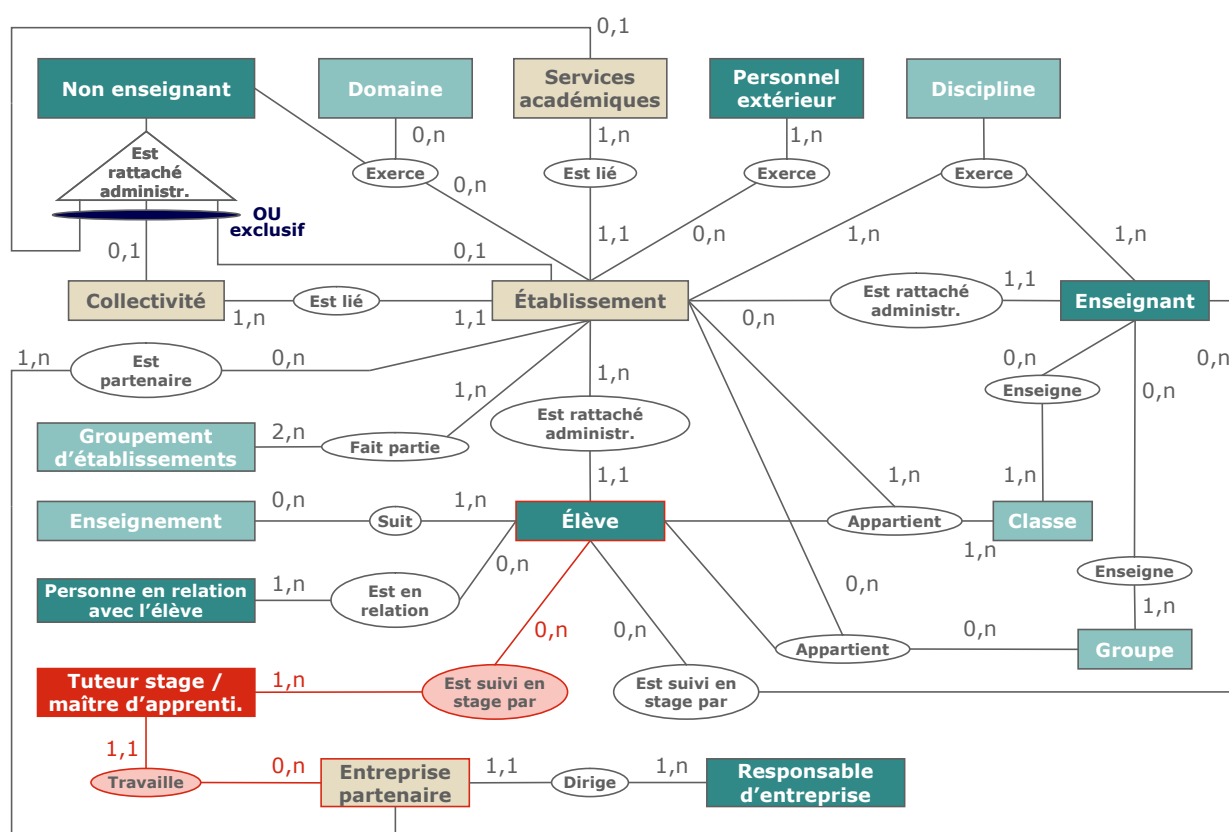


Figure 10 : Caractérisation d'un Tuteur de stage ou maître d'apprentissage

Un *Tuteur de stage ou maître d'apprentissage* suit un ou plusieurs *Élèves* durant leur stage/apprentissage.

Un *Tuteur de stage ou maître d'apprentissage* travaille dans une *Entreprise partenaire*.

Diagramme de base de données relationnelles pour un établissement scolaire. Les entités sont représentées par des rectangles, les relations par des ovales, et les spécialisations par des triangles.

Entités et leurs attributs (suggérés) :

- Non enseignant** (Entité)
- Collectivité** (Entité)
- Groupement d'établissements** (Entité)
- Enseignement** (Entité)
- Personne en relation avec l'élève** (Entité)
- Tuteur stage / maître d'apprenti** (Entité)
- Établissement** (Entité)
- Élève** (Entité)
- Entreprise partenaire** (Entité)
- Services académiques** (Entité)
- Personnel extérieur** (Entité)
- Discipline** (Entité)
- Enseignant** (Entité)
- Classe** (Entité)
- Groupe** (Entité)

Relations et cardinalités :

- Non enseignant** (0,1) **Est rattaché administr.** (0,1) **Collectivité** (1,n) **OU exclusif**
- Collectivité** (1,n) **Est lié** (1,1) **Établissement** (1,1)
- Groupement d'établissements** (2,n) **Fait partie** (1,n) **Établissement** (1,n)
- Enseignement** (0,n) **Suit** (1,n) **Élève** (0,n)
- Personne en relation avec l'élève** (1,n) **Est en relation** (0,n) **Élève** (0,n)
- Tuteur stage / maître d'apprenti** (1,n) **Est suivi en stage par** (0,n) **Élève** (0,n)
- Élève** (0,n) **Est suivi en stage par** (0,n) **Entreprise partenaire** (1,1)
- Services académiques** (1,n) **Est lié** (1,1) **Établissement** (1,1)
- Personnel extérieur** (1,n) **Exerce** (0,n) **Établissement** (1,n)
- Discipline** (1,n) **Exerce** (1,n) **Établissement** (1,n)
- Établissement** (0,n) **Est rattaché administr.** (1,1) **Enseignant** (0,n)
- Enseignant** (0,n) **Enseigne** (1,n) **Classe** (1,n)
- Enseignant** (0,n) **Enseigne** (1,n) **Groupe** (1,n)
- Établissement** (1,n) **Appartient** (0,n) **Classe** (1,n)
- Établissement** (1,n) **Appartient** (0,n) **Groupe** (0,n)
- Entreprise partenaire** (1,1) **Dirige** (1,n) **Responsable d'entreprise** (1,n)
- Entreprise partenaire** (0,n) **Travaille** (1,1) **Tuteur stage / maître d'apprenti** (1,1)

Un *Responsable d'entreprise* est responsable d'une ou plusieurs *Entreprises partenaires*.

Établissement

Un *Établissement* est lié à une et une seule *Collectivité locale*.

À un *Établissement* sont rattachés administrativement zéro, un, ou plusieurs *Non enseignants*.

Dans un *Établissement*, zéro, un, ou plusieurs *Personnels extérieurs* peuvent exercer une activité.

Dans un *Établissement* sont exercées une ou plusieurs *Disciplines* par un ou plusieurs *Enseignants*.

Un *Établissement* possède une ou plusieurs *Classes*.

Un *Établissement* possède zéro, un, ou plusieurs *Groupes*.

Un *Établissement* fait partie de zéro, un, ou plusieurs *Groupements d'établissements*.

Un *Établissement* est partenaire d'une ou plusieurs *Entreprises partenaires*.

Collectivité locale

Une *Collectivité locale* est liée à un ou plusieurs *Établissements*.

A une *Collectivité locale* sont rattachés administrativement zéro, un ou plusieurs *Non enseignants*.

Services académiques

Un ensemble de *Services académiques* est liée à un ou plusieurs *Établissements*.

A un ensemble de *Services académiques* sont rattachés administrativement zéro, un ou plusieurs *Non enseignants*.

Entreprise partenaire

Une *Entreprise partenaire* est dirigée par un et un seul *Responsable d'entreprise*.

Une *Entreprise partenaire* est partenaire d'un ou plusieurs *Établissements*.

Dans une *Entreprise partenaire* travaillent zéro, un ou plusieurs *Tuteurs de stage ou maîtres d'apprentissage*.

DESCRIPTION DES AUTRES TYPES DE DONNEES LIES AUX PERSONNES

Domaine

Un *Domaine* peut correspondre à l'activité d'un ou plusieurs *Non enseignants* dans un ou plusieurs *Établissements*.

Discipline

Une *Discipline* peut être exercée par un ou plusieurs *Enseignants* dans un ou plusieurs *Établissements*.

Classe

Une *Classe* appartient à un et un seul *Établissement*.

Une *Classe* regroupe un ou plusieurs *Élèves* qui peuvent être rattachés administrativement à des *Établissements* différents.

Une *Classe* reçoit l'*Enseignement* d'un ou plusieurs *Enseignants*.

Groupe

Un *Groupe* appartient à un et un seul *Établissement*.

Un *Groupe* regroupe zéro, un, ou plusieurs *Élèves* qui peuvent être rattachés administrativement à des *Établissements* différents.

Un *Groupe* reçoit l'*Enseignement* d'un ou plusieurs *Enseignants*.

Enseignement

Un *Enseignement* est suivi par zéro, un, ou plusieurs *Élèves*.

Groupement d'établissements

Un *Groupement d'établissements* regroupe deux ou plus *Établissements*. Le terme *Groupement d'établissements* inclut les bassins de formation, les cités scolaires et les GRETA.

CONTRAINTES D'INTEGRITE

Des contraintes d'intégrité sur les données de l'annuaire ENT viennent compléter la description présentée ci-dessus. Ces contraintes sont les suivantes :

- [CI-1] Au plus deux *Personnes en relation avec l'élève* exercent l'autorité parentale sur cet *Élève*.
- [CI-2] Au moins une *Personne en relation avec l'élève* exerce l'autorité parentale sur un *Élève* mineur.
- [CI-3] Sur décision d'un *Élève* majeur, il est possible qu'aucune *Personne en relation avec l'élève* n'exerce l'autorité parentale sur lui.
- [CI-4] Il existe au plus un professeur principal par *Classe*.
- [CI-5] Un professeur principal d'une classe donnée enseigne nécessairement au moins une discipline à cette *Classe*.
- [CI-6] Il existe au plus deux *Élèves* délégués par *Classe*.
- [CI-7] Un *Élève* délégué de classe doit nécessairement faire partie de la *Classe* dont il est le délégué.
- [CI-8] Le contact ENT par défaut d'un établissement est le chef d'établissement de cet établissement.

Le porteur pourra éventuellement compléter cette liste si d'autres contraintes d'intégrité doivent être prises en compte.

4. SCHEMA ET DIT DE L'ANNUAIRE ENT

4.1. PREAMBULE

ORIENTATION TECHNOLOGIQUE

L'annuaire ENT doit répondre à des requêtes correspondant à différents usages :

- Des requêtes d'authentification / autorisation.
- Des requêtes de consultation.
- Des requêtes de mise à jour / gestion.

L'annuaire ENT s'appuie sur plusieurs référentiels typés par usage (cf. chapitre 5) :

- Un référentiel pour les mises à jour, la gestion et la consultation d'informations.
- Un référentiel pour l'authentification et l'autorisation des utilisateurs.

Tous ces référentiels sont des annuaires compatibles LDAP v3.

Quelques éléments ayant guidé ce choix :

- *LDAP est utilisé en standard pour des référentiels de sécurité (devant offrir des services d'authentification / autorisation).*
- *Le choix de LDAP pour l'ensemble des référentiels typés par usage permet d'assurer une cohérence technologique entre les différents référentiels et de faciliter la mise en œuvre des flux de synchronisation.*

Le soumissionnaire pourra cependant proposer et justifier une solution technique alternative pour les référentiels. Il devra alors décrire l'ensemble des modifications à apporter, notamment au modèle et à l'architecture technique.

ORGANISATION DES OID DE L'ANNUAIRE ENT

Ce chapitre est à compléter par le porteur.

(1) Si le porteur possède ou souhaite posséder un OID propre pour son organisation⁵, celui-ci sera utilisé comme arc principal pour l'identification des éléments du schéma LDAP. La règle de hiérarchisation est la suivante :

<OID porteur>. <projet>. <type usage>. <portée>. <type d'élément>. <incrément>

avec :

*<OID porteur> : OID attribué au porteur de projet ENT, soit « **A COMPLETER** »*

<projet> : vaut « 1 » pour le projet ENT

<usage> : vaut « 1 » pour l'annuaire ENT

⁵ Une demande d'OID peut être effectuée auprès de l'IANA ou de l'AFNOR.

<portée> : définit s'il s'agit d'un objet commun aux ENT ou d'une extension locale

« 1 » : objet du modèle commun à tous les ENT

« 2 » : extension locale de schéma

<type d'élément> : définit le type d'élément identifié

« 1 » : attribut

« 2 » : classe d'objet

<incrément> : nombre à incrémenter pour chaque objet créé

Les valeurs de <incrément> à utiliser pour les classes et les attributs du modèle de l'annuaire ENT sont données en Annexe 3.

(2) Une demande d'utilisation de l'OID du MENESR est en cours de validation. Si le MENESR propose d'utiliser son OID, le porteur pourra décider de l'utiliser. Dans ce cas, la règle de hiérarchisation présentée ci-dessus devra être adaptée à celle du MENESR.

(3) Sinon, le porteur utilisera l'OID de son choix et utilisera la règle de hiérarchisation présentée ci-dessus.

NOMENCLATURES

Les nomenclatures correspondant aux attributs du schéma LDAP sont données en Annexe 3.

Le porteur devra préciser les nomenclatures qu'il souhaite partager au niveau de tout l'ENT. Dans le cas contraire, hors nomenclature à portée nationale, la nomenclature sera propre à un établissement et non partagée dans l'ENT.

4.2. DESCRIPTION DES CLASSES D'OBJET DE L'ANNUAIRE ENT

Remarques :

- Des précisions sur les notions liées à la scolarité (MEF, matières, n°UAI...) sont données dans la partie « Lexique MENESR » de l'Annexe 1.
- Sauf mention contraire, les « classes » dont il est question dans ce chapitre sont des classes au sens LDAP.

4.2.1. Gestion des objets de l'annuaire ENT

PERSONNES APPARTENANT A PLUSIEURS CATEGORIES DE PERSONNES

Une personne peut appartenir à plusieurs catégories de personnes. Il peut s'agir par exemple d'un enseignant qui est également parent d'un élève.

L'entrée de l'annuaire ENT représentant une telle personne doit disposer de l'ensemble des caractéristiques propres à chacune des catégories de la personne.

C'est pourquoi le schéma de l'annuaire ENT est basé sur l'utilisation de **classes LDAP auxiliaires**, qui permettent de compléter une entrée de l'annuaire ENT avec des attributs spécifiques. En cumulant plusieurs classes auxiliaires sur l'entrée d'une même personne, celle-ci disposera de tous les attributs nécessaires en fonction des catégories de personnes auxquelles elle appartient.

Exemple de création d'un enseignant qui est également parent d'un élève :

- *Un objet est créé à partir de la classe ENTPerson. L'objet dispose ainsi des attributs communs à tous les utilisateurs de l'ENT.*
- *La personne étant enseignante, il faut ajouter la classe auxiliaire ENTAuxEnseignant à l'objet. Celui-ci dispose alors d'attributs tels que les disciplines enseignées, les classes dont la personne est professeur principal...*
- *Étant également parent, il faut ajouter la classe auxiliaire ENTAuxPersRelEleve à l'objet. Celui-ci dispose alors d'attributs tels que les élèves en responsabilité...*

Il n'est pas possible de restreindre les classes LDAP structurelles que peut venir compléter une classe auxiliaire. Un contrôle d'intégrité devra donc être assuré au niveau des services de gestion de contenu afin de ne permettre l'ajout de classes auxiliaires qu'à la classe structurelle *ENTPerson*. Les élèves (classe *ENTEleve*) ne peuvent en effet pas appartenir à plusieurs catégories.

Par ailleurs, l'ENT pourra offrir aux utilisateurs un service permettant de réconcilier les identités distinctes qu'ils possèdent dans chacune des catégories (cf. [SRV-3] au chapitre 7.1.1).

PERSONNES EXERÇANT DANS PLUSIEURS ETABLISSEMENTS

Certaines personnes exercent leur activité dans plusieurs établissements : des élèves suivent des cours dans plusieurs établissements, des personnels administratifs dépendant d'une collectivité locale possèdent des fonctions dans un établissement d'enseignement...

En conséquence, ces personnes accèdent à plusieurs ENT d'établissement. Selon les cas, ces ENT relèvent du même projet ENT ou de projets différents (les possibilités de rapprochement des comptes sont donc différentes cf. chapitre 6 page 52).

Il est donc nécessaire de distinguer la structure de rattachement administratif et la ou les structures d'exercice. C'est pourquoi tout utilisateur de l'ENT possède l'attribut « *ENTPersonStructRattach* » pour désigner la structure de rattachement administratif. Les structures d'exercice doivent par contre être déduites de l'attribut « *ENTPersonFonctions* ».

QUALIFICATION DES RELATIONS MULTIPLES ENTRE OBJETS DE L'ANNUAIRE ENT

Une certaine complexité peut apparaître dans le schéma LDAP lorsqu'il est nécessaire de qualifier des relations « n – n » entre objets. Exemple : « *Comment qualifier la relation entre un élève et une personne, sachant qu'un élève peut être en relation avec plusieurs personnes dont le rôle est différent, et qu'une personne peut être en relation avec plusieurs élèves et jouer un rôle différent vis-à-vis de chaque élève ?* »

Lorsqu'il existe une liste fermée des qualités décrivant une relation, il est possible de créer un attribut par qualité. Cet attribut pointe sur la personne concernée.

C'est le cas pour un élève et son père, un élève et sa mère et un élève et les personnes qui exercent l'autorité parentale.

Par contre, lorsque les qualités ne sont pas définies, deux attributs sont créés par relation : un attribut pointant sur la personne concernée et un attribut indiquant la qualité associée à cette personne.

C'est la raison pour laquelle les attributs « ENTElevePersRelEleve1 », « ENTEleveQualitePersRelEleve1 », « ENTElevePersRelEleve2 » et « ENTEleveQualitePersRelEleve2 » ont été créés. Ils permettent de définir librement la relation entre un élève et deux personnes autres que ses parents ou ses tuteurs légaux. Il peut s'agir par exemple du responsable financier de l'élève.

Afin de qualifier d'éventuelles relations supplémentaires concernant un *Élève*, il est possible d'utiliser la classe *ENTRelEleve*. Une instance de ce groupe doit être créée pour chaque relation entre chaque couple « *Élève – Personne en relation avec l'élève* ». Un attribut du groupe permet de qualifier cette relation. Il conviendra toutefois d'être attentif au volume d'entrées supplémentaires générées dans l'annuaire ENT par cette solution.

ADULTES EN FORMATION CONTINUE

Les adultes en formation continue ne sont pas pris en compte dans le schéma proposé. Si le porteur souhaite les intégrer au périmètre couvert par l'ENT, il devra :

- *ajouter une classe auxiliaire « ENTAuxFormationContinue » ;*
- *déterminer les attributs nécessaires pour cette classe ;*
- *assurer l'alimentation de cette nouvelle catégorie de personnes.*

4.2.2. Schéma LDAP

Les classes LDAP standard sont utilisées autant que possible afin de faciliter la mise en place d'applications génériques. Les attributs non disponibles dans le schéma standard sont ajoutés dans des classes dédiées à l'ENT par extension du schéma.

Le schéma LDAP de l'annuaire ENT est représenté sur la Figure 12. Les différentes classes sont décrites dans la suite du chapitre et sont reprises à **[l'Annexe 3](#)**.

Le récapitulatif des attributs par catégorie de personnes ou de structures est donné à **[l'Annexe 2](#)**. Notons que le caractère facultatif ou obligatoire d'un attribut hérité peut varier en fonction de la catégorie de personnes ou de structures.

Remarque : Des attributs à caractère technique pourront être ajoutés au schéma LDAP afin de couvrir les besoins des services AAS (utilisateur suspendu, date de validité, « challenges »...).

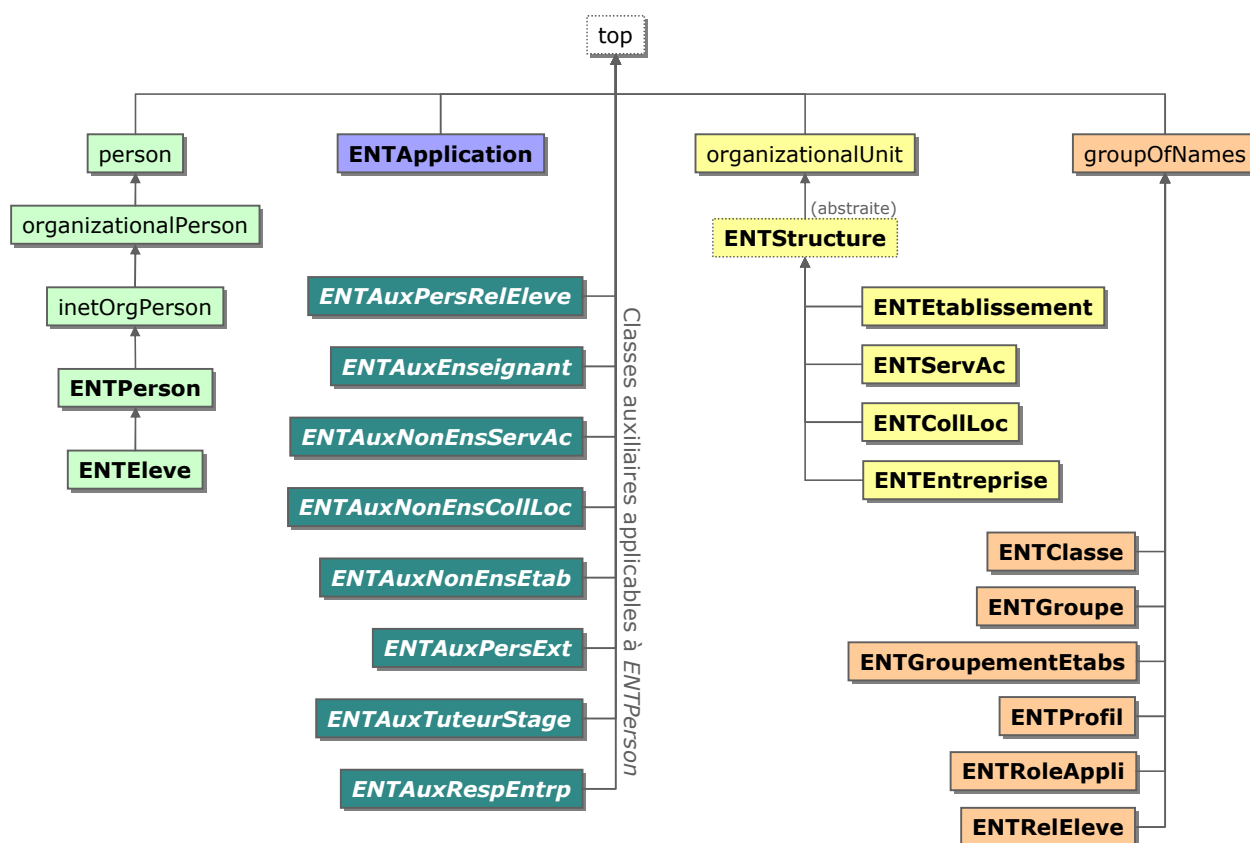


Figure 12 : Schéma LDAP de l'annuaire ENT

4.2.3. Classes relatives aux personnes

CLASSES *PERSON*, *ORGANIZATIONALPERSON* ET *INETORGPERSO*

Les classes *person*, *organizationalPerson* et *inetOrgPerson* sont des classes LDAP standard qui servent de base pour décrire des personnes. Les attributs correspondants sont donnés dans le tableau ci-dessous.

Les attributs grisés ne sont pas utilisés par le modèle d'information de l'annuaire ENT.

Les cellules en italique correspondent à des contraintes spécifiques à l'annuaire ENT sur les propriétés des attributs. Ces contraintes d'intégrité devront être contrôlées par les services de gestion de contenu en plus de celles mentionnées au chapitre 3.3. Exemple : le standard LDAP autorise l'attribut « *telephoneNumber* » à être multi-valué alors que dans le modèle de l'annuaire ENT cet attribut doit être mono-valué.

C. ⁶	Attribut LDAP	Description	Obl / Fac ⁷	Mo / Mu ⁸
Person	cn	Nom canonique de l'objet	Obl	Mo
	sn	Nom d'usage	Obl	Mo
	userPassword	Mot de passe de connexion à l'ENT	Obl	Mo
	seeAlso			

⁶ C. : classe LDAP.

⁷ Obl / Fac : indique si l'attribut doit obligatoirement être renseigné (Obl) ou s'il peut être laissé vide (Fac).

⁸ Mo / Mu : indique si l'attribut est mono-valué (Mo) ou multi-valué (Mu).

C. ⁶	Attribut LDAP	Description	Obl / Fac ⁷	Mo / Mu ⁸
	description			
	telephoneNumber	Numéro de téléphone fixe professionnel	Fac	Mo
organizationalPerson	title	Titre	Fac	Mo
	x121Address			
	registeredAddress			
	destinationIndicator			
	preferredDeliveryMethod			
	telexNumber			
	telexTerminalIdentifier			
	internationaliSDNNNumber			
	facsimileTelephoneNumber	Numéro de fax professionnel	Fac	Mo
	street			
	postOfficeBox			
	postalCode			
	postalAddress			
	physicalDeliveryOfficeName			
	ou			
	st			
	l			
inetOrgPerson	audio			
	businessCategory			
	carLicense			
	departmentNumber			
	displayName	Nom et prénom accentués	Obl	Mo
	employeeNumber			
	employeeType			
	givenName	Prénom usuel	Obl	Mo
	homePhone	Numéro de téléphone fixe personnel	Fac	Mo
	homePostalAddress			
	Initials			
	jpegPhoto	Photographie	Fac	Mo
	labeledURI			
	mail	Adresse e-mail	Fac	Mo
	manager			
	Mobile	Numéro de téléphone mobile	Fac	Mo
	o			
	pager			
	photo			
	roomNumber	Numéro de bureau	Fac	Mo
	secretary			
	uid	Identifiant interne à l'ENT	Obl	Mo
	userCertificates			
	x500UniqueIdentifier			
	preferredLanguage			
	userSMIMECertificate			
	userPKCS12			

Les classes *person*, *organizationalPerson* et *inetOrgPerson* ne doivent pas être instanciées dans l'annuaire ENT.

CLASSE *ENTPERSON*

La classe *ENTPerson* hérite de la classe *inetOrgPerson* et ajoute les attributs communs à toutes les personnes de l'ENT. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
personalTitle	Civilité	Fac	Mo
ENTPersonAutresPrenoms	Autres prénoms que le prénom usuel	Fac	Mu
ENTPersonNomPatro	Nom patronymique	Fac	Mo
ENTPersonSexe	Sexe	Fac	Mo
ENTPersonCentresInteret	Centres d'intérêt par établissement	Fac	Mu
ENTPersonAdresse	Adresse personnelle - champ libre	Fac	Mo
ENTPersonCodePostal	Adresse personnelle - code postal	Fac	Mo
ENTPersonVille	Adresse personnelle - ville	Fac	Mo
ENTPersonPays	Adresse personnelle - pays	Fac	Mo
ENTPersonLogin	Login (identifiant de connexion à l'ENT)	Obl	Mo
ENTPersonAlias	Alias	Fac	Mo
ENTPersonJointure	Clés de jointure	Obl	Mu
ENTPersonStructRattach	Structure de rattachement	Fac	Mo
ENTPersonFonctions	Fonctions et disciplines de poste associées dans des structures	Fac	Mu
ENTPersonDateNaissance	Date de naissance	Fac	Mo
ENTPersonProfils	Profils associés	Fac	Mu

L'attribut « *ENTPersonProfils* » doit être mis à jour lors de l'attribution ou du retrait d'un profil à une personne.

L'attribut « *ENTPersonFonctions* » doit être utilisé pour déterminer l'ensemble des établissements d'exercices d'un enseignant, l'attribut « *ENTPersonStructRattach* » fournissant uniquement l'établissement de rattachement administratif de l'enseignant.

La classe *ENTPerson* peut être complétée par une ou plusieurs des classes auxiliaires définies dans le modèle. Ces classes auxiliaires sont détaillées dans la suite du chapitre.

CLASSE *ENTELEVE*

La classe *ENTEleve* hérite de la classe *ENTPerson* et ajoute les attributs relatifs à la catégorie de personnes « Élèves ». Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTEleveVilleNaissance	Ville de naissance	Fac	Mo
ENTEleveDeptNaissance	Département de naissance	Fac	Mo
ENTElevePaysNaissance	Pays de naissance	Fac	Mo
ENTEleveParents	Parents	Fac	Mu
ENTElevePere ⁹	Père	Fac	Mo
ENTEleveMere ⁹	Mère	Fac	Mo
ENTEleveAutoriteParentale	Personnes exerçant l'autorité parentale	Fac	Mu
ENTElevePersRelEleve1	Autre personne en relation avec l'élève - 1	Fac	Mo
ENTEleveQualitePersRelEleve1	Qualité autre personne en relation avec l'élève 1	Fac	Mo
ENTElevePersRelEleve2	Autre personne en relation avec l'élève - 2	Fac	Mo

⁹ Attribut présent pour des raisons de rétro-compatibilité. Cet attribut ne devrait pas faire partie de la structure de l'annuaire ENT. Notons qu'il pourra être supprimé dans une future mise à jour majeure du cahier des charges.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTEleveQualitePersRelEleve2	Qualité autre personne en relation avec l'élève 2	Fac	Mo
ENTEleveBoursier	Boursier	Fac	Mo
ENTEleveRegime	Régime établissement de rattachement	Fac	Mo
ENTEleveTransport	Transport scolaire	Fac	Mo
ENTEleveStatutEleve	"Statut" de l'élève	Obl	Mo
ENTEleveMEF	MEF	Obl	Mo
ENTEleveLibelleMEF	Libellé MEF	Obl	Mo
ENTEleveMEFRattach	MEF de rattachement	Fac	Mo
ENTEleveCodeNivFormation	Code du niveau de formation	Obl	Mo
ENTEleveNivFormation	Niveau de formation	Obl	Mo
ENTEleveFiliere	Filière	Obl	Mo
ENTEleveNivFormationDiplome	Niveau de formation du diplôme	Fac	Mo
ENTEleveSpecialite	Spécialité	Fac	Mo
ENTEleveEnseignements	Enseignements	Obl	Mu
ENTEleveStructRattachId	Identifiant de l'élève dans SCONET	Obl	Mo
ENTEleveClasses	Établissements et classe associée	Obl	Mu
ENTEleveGroupes	Établissements et groupes associés	Obl	Mu
ENTEleveEnsRespStage	Enseignant responsable de stage	Fac	Mo
ENTEleveEnsTutStage	Enseignants tuteurs de stage	Fac	Mu
ENTEleveEntrTutStage	Tuteur de stage / Maître d'apprentissage	Fac	Mo
ENTEleveEntrAutres	Autres personnes de l'entreprise suivant l'élève en stage	Fac	Mu
ENTEleveDelegClasse	Élève délégué de classe	Fac	Mo
ENTEleveDelegAutres	Élève délégué autres	Fac	Mu
ENTEleveMajeur	Majeur	Obl	Mo
ENTEleveMajeurAnticipe	Majeur anticipé	Fac	Mo

L'attribut « ENTEleveClasses » doit être utilisé pour déterminer l'ensemble des établissements d'un élève, l'attribut « ENTPersonStructRattach » fournissant uniquement l'établissement de rattachement administratif de l'élève.

CLASSE *ENTAuxPersRelEleve*

La classe *ENTAuxPersRelEleve* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Personnes en relation avec les élèves*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxPersRelEleveEleve	Élèves concernés	Obl	Mu
ENTAuxPersRelEleveRepresentant	Représentant des parents d'élèves	Fac	Mu

La classe auxiliaire *ENTAuxPersRelEleve* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

CLASSE *ENTAuxEnseignant*

La classe *ENTAuxEnseignant* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Enseignants*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxEnsDisciplinesPoste ⁹	Disciplines de poste et catégorie de discipline de poste associée	Fac	Mu
ENTAuxEnsCategoDiscipline	Catégories de discipline de poste	Fac	Mu
ENTAuxEnsMEF	Codes MEF et libellé associé pour chaque établissement	Fac	Mu
ENTAuxEnsMatiereEnseignEtab	Établissement et matières enseignées	Fac	Mu
ENTAuxEnsClasses	Établissement et classes associées	Fac	Mu
ENTAuxEnsGroupes	Établissement et groupes associés	Fac	Mu
ENTAuxEnsClassesPrincipal	Établissement et classe associée dont la personne est professeur principal	Fac	Mu
ENTAuxEnsRespStage	Élèves stagiaires en responsabilité	Fac	Mu
ENTAuxEnsTutStage	Élèves stagiaires suivis	Fac	Mu

La classe auxiliaire *ENTAuxEnseignant* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

L'attribut *ENTAuxEnsCategoDiscipline* fournit des codes pivots pour les disciplines d'enseignements uniquement. Il n'existe pas de pivots pour les autres fonctions.

CLASSE *ENTAuxNonEnsServAc*

La classe *ENTAuxNonEnsServAc* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Non enseignants rattachés administrativement aux services académiques*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxNonEnsServAcService	Service	Fac	Mo
ENTAuxNonEnsServAcDomaineEtab	Établissements d'exercice et domaines associés	Fac	Mu
ENTAuxNonEnsServAcDomaineRegroupEtabs	Regroupement d'établissements d'exercice et domaines associés	Fac	Mu

La classe auxiliaire *ENTAuxNonEnsServAc* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

CLASSE *ENTAuxNonEnsCollLoc*

La classe *ENTAuxNonEnsCollLoc* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Non enseignants rattachés administrativement à une collectivité locale*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxNonEnsCollLocService	Service	Fac	Mo
ENTAuxNonEnsCollLocDomaineEtab	Établissements d'exercice et domaines associés	Fac	Mu
ENTAuxNonEnsCollLocDomaineRegroupEtabs	Regroupement d'établissements d'exercice et domaines associés	Fac	Mu

La classe auxiliaire *ENTAuxNonEnsCollLoc* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

CLASSE *ENTNonEnsEtab*

La classe *ENTAuxNonEnsEtab* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Non enseignants rattachés administrativement à un établissement d'enseignement*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxNonEnsEtabService	Service	Fac	Mo

La classe auxiliaire *ENTAuxNonEnsEtab* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

CLASSE *ENTAuxPersExt*

La classe *ENTAuxPersExt* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Personnels extérieurs*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxPersExtService	Service	Fac	Mo

La classe auxiliaire *ENTAuxPersExt* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

CLASSE *ENTAuxTuteurStage*

La classe *ENTAuxTuteurStage* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Tuteurs de stage et maîtres d'apprentissage*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxTuteurStageSociete	Société	Obl	Mo
ENTAuxTuteurStageEleves	Élevés suivis en stage ou en apprentissage	Obl	Mu

La classe auxiliaire *ENTAuxTuteurStage* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

CLASSE *ENTAuxRespEntrp*

La classe *ENTAuxRespEntrp* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Responsables des entreprises partenaires*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxRespEntrpSociete	Société	Obl	Mo

La classe auxiliaire *ENTAuxRespEntrp* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

4.2.4. Classes relatives aux structures

CLASSE *ORGANIZATIONALUNIT*

La classe *organizationalUnit* est une classe LDAP standard qui sert de base pour décrire des structures. Les attributs sont donnés dans le tableau ci-dessous.

Les attributs grisés ne sont pas utilisés par le modèle d'information de l'annuaire ENT.

Les cellules en italique correspondent à des restrictions spécifiques à l'annuaire ENT sur les propriétés d'attributs. Ces contraintes d'intégrité devront être contrôlées par les services de gestion de contenu en plus de celles mentionnées au chapitre 3.3.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ou			
description			
preferredDeliveryMethod			
searchGuide			
st			
businessCategory			
telexNumber			
l	Adresse professionnelle - ville	Fac	<i>Mo</i>
seeAlso			
telephoneNumber	Numéro de téléphone	Fac	<i>Mo</i>
physicalDeliveryOfficeName			
postalCode	Adresse professionnelle - code postal	Fac	<i>Mo</i>
internationalISDNNumber			
x121Address			
userPassword			
registeredAddress			
street	Adresse professionnelle - champ libre	Fac	<i>Mo</i>
postalAddress			
facsimileTelephoneNumber	Numéro de fax	Fac	<i>Mo</i>
teletexTerminalIdentifier			
postOfficeBox	Adresse professionnelle - boîte postale	Fac	<i>Mo</i>
destinationIndicator			

CLASSE *ENTSTRUCTURE*

La classe *ENTStructure* est une classe abstraite qui hérite de la classe *organizationalUnit* et la complète avec les attributs communs à toutes les structures de l'ENT. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTStructureJointure	Nom courant / Raison sociale	Obl	Mu
ENTStructureTypeStruct	Type de structure	Fac	Mo
ENTStructureNomCourant	Nom courant / Raison sociale	Obl	Mo
ENTStructureResponsable	Responsable	Fac	Mo
ENTStructureSIREN	Numéro de SIREN / SIRET	Obl	Mo
ENTStructureEmail	Adresse e-mail	Fac	Mo
ENTStructureSiteWeb	Site web	Fac	Mo
ENTStructureContactENT	Contact ENT	Fac	Mo
ENTStructureUAI	Numéro UAI	Fac	Mo

La classe abstraite *ENTStructure* ne peut pas être instanciée.

CLASSE *ENTEtablissement*

La classe *ENTEtablissement* complète la classe *ENTStructure* avec les attributs relatifs à la catégorie de structures *Établissements d'enseignement*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTEtablissementMinistereTutelle	Ministère de tutelle	Obl	Mo
ENTEtablissementContrat	Contrat	Obl	Mo
ENTEtablissementStructRattachAdmin	Structures de rattachement administratif	Fac	Mu
ENTEtablissementStructRattachFcti	Structures de rattachement fonctionnel	Fac	Mu
ENTEtablissementBassin	Bassin de formation	Fac	Mo

CLASSE *ENTServAc*

La classe *ENTServAc* complète la classe *ENTStructure* avec les attributs relatifs à la catégorie de structures *Services académiques*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTServAcAcademie	Académie	Obl	Mo

CLASSE *ENTCollLoc*

La classe *ENTCollLoc* complète la classe *ENTStructure* avec les attributs relatifs à la catégorie de structures *Collectivité locale*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTCollLocLieuGeographique	Région ou département	Obl	Mo

CLASSE *ENTEntreprise*

La classe *ENTEntreprise* complète la classe *ENTStructure* avec les attributs relatifs à la catégorie de structures *Entreprises partenaires*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTEntrepriseEtabs	Établissements partenaires	Obl	Mu

4.2.5. Classes relatives aux groupes d'entrées de l'annuaire ENT

CLASSE *GROUPOfNames*

La classe *groupOfNames* est une classe LDAP standard qui sert de base pour décrire des groupes d'entrées de l'annuaire ENT (groupes de personnes, de structures, de groupes...). Les attributs correspondants sont donnés dans le tableau ci-dessous.

Les attributs grisés ne sont pas utilisés par le modèle d'information de l'annuaire ENT.

Les cellules en italique correspondent à des restrictions spécifiques à l'annuaire ENT sur les propriétés d'attributs. Ces contraintes d'intégrité devront être contrôlées par les services de gestion de contenu en plus de celles mentionnées au chapitre 3.3.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
cn	Nom du groupe	Obl	Mo
businessCategory			
seeAlso			
owner	Propriétaire du groupe	Fac	Mo
ou			
o			
description	Description du groupe	Fac	Mo
member	Membres du groupe	Fac	Mu

CLASSE *ENTCLASSE*

Remarque : il est ici question de la « classe LDAP » représentant une « classe d'élèves ».

La classe *ENTClasse* hérite de la classe *groupOfNames* et ajoute les attributs relatifs aux classes des élèves. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
(aucun attribut supplémentaire pour la classe <i>ENTClasse</i>)			

Les classes sont définies par établissement d'enseignement. L'attribut « owner », hérité de *groupOfNames*, correspond au « dn » de l'établissement d'enseignement pour lequel est définie la classe.

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » des élèves de la classe.

L'attribut « cn » doit désigner de façon unique une classe sur le périmètre de l'ENT. La règle de construction proposée est la suivante : le nom d'une classe doit être préfixé du numéro SIREN de l'établissement d'enseignement pour lequel elle est définie, suivi d'un « _ ».
Exemple : 123456789_3eme2

Le porteur pourra éventuellement définir sa propre règle de construction.

CLASSE *ENTGROUPE*

La classe *ENTGroupe* hérite de la classe *groupOfNames* et ajoute les attributs relatifs aux groupes d'élèves. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
(aucun attribut supplémentaire pour la classe <i>ENTGroupe</i>)			

Les groupes d'élèves sont définis par établissement d'enseignement. L'attribut « owner », hérité de *groupOfNames*, correspond au « dn » de l'établissement d'enseignement pour lequel est défini le groupe.

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » des élèves du groupe.

L'attribut « cn » doit désigner de façon unique un groupe d'élèves sur le périmètre de l'ENT. La règle de construction proposée est la suivante : le nom du groupe d'élèves doit être préfixé du numéro SIREN de l'établissement d'enseignement pour lequel il est défini, suivi d'un « _ ». Exemple : 123456789_latin2

Le porteur pourra éventuellement définir sa propre règle de construction.

CLASSE *ENTGROUPEMENTETABS*

La classe *ENTGroupeMENTEtabs* hérite de la classe *groupOfNames* et ajoute les attributs relatifs aux groupements d'établissements (bassins de formation, cités scolaires, GRETA). Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
(aucun attribut supplémentaire pour la classe <i>ENTGroupeMENTEtabs</i>)			

L'attribut « owner », hérité de *groupOfNames*, n'est pas renseigné. *Le porteur pourra préciser cet attribut s'il le souhaite.*

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » des établissements qui constituent le regroupement.

L'attribut « cn » doit désigner de façon unique un groupement d'établissements sur le périmètre de l'ENT.

CLASSE *ENTPROFIL*

La classe *ENTProfil* hérite de la classe *groupOfNames* et ajoute les attributs relatifs aux profils décrits dans le modèle de sécurité de l'annuaire ENT. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTProfilPeuplement	Règle de peuplement	Fac	Mo

Il existe deux types de profils :

- Les profils partagés au niveau national (cf. chapitre 6) et qui sont donc transverses à un ENT.

Dans ce cas, l'attribut « owner », hérité de *groupOfNames*, n'est pas renseigné.

- Les profils définis sur le périmètre d'une structure (établissement notamment).

Dans ce cas, l'attribut « owner », hérité de *groupOfNames*, correspond au « dn » de l'établissement d'enseignement qui a défini le profil.

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » des personnes associées à ce profil.

L'attribut « cn » doit désigner de façon unique un groupement d'établissements sur le périmètre de l'ENT. La règle de construction est la suivante :

- Les profils partagés au niveau national sont préfixés par « National_ ».
- Les profils définis par des structures sont préfixés par le numéro SIREN de la structure suivi de « _ ».

Des informations complémentaires sur les règles de peuplement des profils sont données au chapitre 3.2.

CLASSE *ENTROLEAPPLI*

La classe *ENTRoleAppli* hérite de la classe *groupOfNames* et ajoute les attributs relatifs aux rôles applicatifs décrits dans le modèle de sécurité de l'annuaire ENT. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTRoleAppliProfils	Profils associés	Fac	Mu

Un rôle applicatif est défini par rapport à une application donnée. L'attribut « owner », hérité de *groupOfNames*, correspond au « dn » de l'application qui a défini le rôle applicatif. Cet attribut doit nécessairement être renseigné.

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » des personnes associées à ce rôle applicatif.

CLASSE *ENTRELEVE*

La classe *ENTRelEleve* hérite de la classe *groupOfNames* et ajoute les attributs relatifs à une relation entre un *Élève* et une *Personne en relation avec l'élève*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
(aucun attribut supplémentaire pour la classe <i>ENTRelEleve</i>)			

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » d'un seul *Eleve* et d'une seule *Personne en relation avec l'élève*.

L'attribut « description », hérité de *groupOfNames*, qualifie la relation entre l'*Eleve* et la *Personne en relation avec l'élève*.

Remarque : Il est nécessaire de créer un groupe par relation que l'on veut représenter.

4.2.6. Classe relative aux applications

CLASSE *ENTAPPLICATION*

La classe *ENTApplication* hérite directement de la classe *top* et décrit les applications qui utilisent l'annuaire ENT. Ces applications peuvent reposer ou non sur le socle ENT. Les attributs sont donnés dans le tableau ci-dessous.

Les cellules en italique correspondent à des restrictions spécifiques à l'annuaire ENT sur les propriétés d'attributs. Ces contraintes d'intégrité devront être contrôlées par les services de gestion de contenu en plus de celles mentionnées au chapitre 3.3.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTApplicationId	Identifiant	Obl	Mo
userPassword	Mot de passe	Obl	Mo
ENTApplicationNom	Nom	Obl	Mo
ENTApplicationDesc	Description	Fac	Mo
ENTApplicationCatego	Catégorie	Obl	Mu

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTApplicationProprietaire	Propriétaire de l'application	Fac	Mo
ENTApplicationProfils	Profils utilisés par l'application	Fac	Mu
ENTApplicationRolesAppli	Rôles applicatifs utilisés par l'application	Fac	Mu

La classe *ENTApplication* possède un identifiant et un mot de passe qui permettent à l'annuaire ENT d'authentifier l'application sur l'ENT.

4.3. DIT DE L'ANNUAIRE ENT

4.3.1. Racine

Le porteur indiquera la racine qu'il souhaite mettre en place pour l'annuaire ENT. La seule contrainte est de faire référence au nom du projet ENT dans la racine.

Exemple de racine possible pour le projet PRISME : « dc=prisme-lorraine, dc=net »

4.3.2. Arborescence

L'organisation retenue pour le DIT est une organisation à plat. Dans cette organisation, tous les objets de l'annuaire ENT sont classés dans des catégories directement rattachées à la racine.

Les catégories sont :

- *personnes* : liste des personnes.
Contient des objets des classes *ENTPerson* et *ENTEleve*.
- *structures* : liste des structures.
Contient des objets des classes *ENTetablissement*, *ENTServAc*, *ENTCollLoc* et *ENTentreprise*.
- *groupes* : liste des groupes.
Contient les objets des classes *ENTClasse*, *ENTGroupe*, *ENTGroupementEtabs*, *ENTProfil*, *ENTRoleAppli* et *ENTRelEleve*.
- *applications* : liste des applications utilisant l'annuaire ENT.
Contient les objets de la classe *ENTApplication*.

Des contraintes applicatives, notamment par rapport aux services AAS, pourraient imposer d'utiliser des termes anglais pour les branches personnes (people) et groupes (groups). Le porteur modifiera en conséquence le DIT de l'annuaire ENT ou laissera éventuellement cette liberté au soumissionnaire.

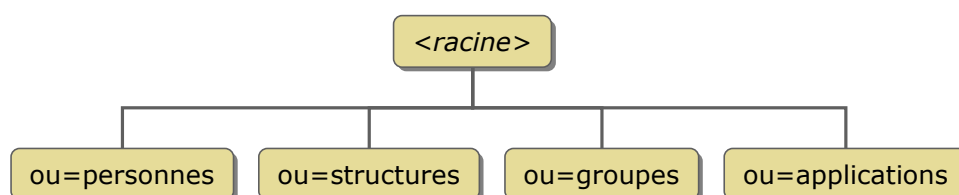


Figure 13 : DIT de l'annuaire ENT

Compte tenu du nombre de personnes au sein de l'ENT, les risques d'homonymie sont très présents. C'est pourquoi l'attribut « cn », tel qu'il est construit, ne pourra pas être utilisé comme RDN (*Relative Distinguished Name*) des personnes. Des précisions sont données au chapitre 4.4.

Le soumissionnaire pourra proposer et justifier une organisation plus hiérarchique en précisant les impacts éventuels sur le schéma et notamment comment les personnes exerçant dans plusieurs établissements sont alors gérées (cf. chapitre 4.2.1). Il précisera également si des ACL sont positionnées sur certaines branches.

4.4. ATTRIBUTS PARTICULIERS

4.4.1. Identifiant unique des personnes sur l'annuaire ENT

Toute entrée appartenant à la classe *inetOrgPerson* ou à une classe qui en hérite possède un attribut « uid ». Cet attribut représente l'identifiant interne à l'ENT et doit être unique sur le périmètre national.

FORMAT DE L'IDENTIFIANT UNIQUE

Cet identifiant est de la forme « LxxCi iii » avec :

- L et C : Lettre et chiffre du code projet ENT.

A partir de l'Annexe 5, il s'agira pour le porteur de choisir le code projet à utiliser et d'assurer la cohérence de ce choix dans le temps.

Exemple : si le projet couvre le périmètre de la région Alsace, le porteur utilisera le code projet « A 0 ». Par contre, si le projet ne concerne que le Bas-Rhin, le code « A 1 » sera utilisé.

Le code ENT pour le projet INOM_PROJET_ENT est : « A compléter par le porteur en fonction du tableau en Annexe 5 ».

- xx et iii : 2 lettres et 4 chiffres à générer pour chaque entrée (6 760 000 combinaisons possibles).

SERVICE DE GENERATION DE L'IDENTIFIANT

Le service de génération de l'identifiant fait partie des services à implémenter et doit suivre les principes de fonctionnement suivants :

- Respect du format présenté ci-dessus.
- Utilisation du code projet ENT pour les caractères L et C.
- Génération des caractères xx et iii sur la base des attributs discriminants suivants :
 - ▶ le nom d'usage ;
 - ▶ le prénom usuel ;
 - ▶ la date de naissance (si celle-ci est connue).

Remarque : Les attributs complémentaires suivants peuvent être utilisés pour résoudre les cas d'homonymie (deux personnes possédant les mêmes valeurs pour tous les attributs discriminants) :

- ▶ les autres prénoms ;
- ▶ le nom patronymique.

- Renvoi de l'identifiant déjà généré si les mêmes attributs discriminants sont présentés.

Remarque : Un utilisateur qui changerait d'ENT (suite à un déménagement par exemple) se verrait attribuer un nouvel identifiant pour le nouvel ENT.

Le porteur déterminera si l'identifiant d'un utilisateur supprimé peut être réutilisé, et si oui, au bout de combien de temps. Notons que la réutilisation d'un identifiant peut présenter un risque de confusion d'identité vis-à-vis d'un tiers.

4.4.2. Login

Toute entrée appartenant à la classe *ENTPerson* ou à une classe qui en hérite possède un attribut « *ENTPersonLogin* » qui correspond à l'identifiant de connexion à l'ENT.

Cet identifiant de connexion doit être unique sur le périmètre de l'ENT. Cette unicité doit également prendre en compte les valeurs d'alias existants (cf. chapitre suivant).

Le porteur pourra supprimer la phrase précédente si la fonctionnalité d'alias n'est pas proposée.

FORMAT DU LOGIN

Le porteur pourra choisir parmi les propositions suivantes la règle de construction du login qu'il souhaite adopter :

- *prenom.nomXX*, où *XX* est un incrément garantissant l'unicité ;
- *pnomXX*, où *XX* est un incrément garantissant l'unicité ;
- « *uid* » ;
- *identifiant institutionnel* (pour les populations qui en dispose et si celui-ci est transmis par le MENESR en tant que clé de jointure) ;
- *autre proposition*.

SERVICE DE GENERATION DU LOGIN

Selon le format de login choisi par le porteur, un service de génération du login peut être nécessaire (notamment en cas d'incrément garantissant l'unicité). Le porteur indiquera ici les principes de fonctionnement attendus pour ce service.

4.4.3. Alias

Le schéma LDAP proposé permet de créer un seul alias pour chaque utilisateur. Il devra être adapté si le porteur :

- *ne souhaite pas offrir cette fonctionnalité ;*
- *ou souhaite que les utilisateurs disposent de plusieurs alias.*

Ce chapitre pourra être supprimé si le porteur ne souhaite pas offrir cette fonctionnalité.

Toute entrée appartenant à la classe *ENTPerson* ou à une classe qui en hérite possède un attribut « *ENTPersonAlias* » qui correspond à un identifiant alternatif de connexion à l'ENT. Celui-ci peut donc être utilisé à la place de « *ENTPersonLogin* ».

L'alias offre aux utilisateurs la possibilité de choisir un identifiant de connexion plus facile à retenir que celui qui est fourni automatiquement. La règle de création de l'alias est la suivante : un alias donné est attribué à la première personne qui en fait la demande.

Cet alias doit être unique sur le périmètre de l'ENT. Cette unicité doit également prendre en compte les valeurs des identifiants de connexion existants (cf. chapitre précédent).

Le porteur pourra définir, s'il le souhaite, des contraintes s'appliquant sur le format des alias.

Le service permettant à un utilisateur de se créer un alias est décrit au chapitre 7.1.2.

4.4.4. « cn » des personnes

Le *Common Name*, ou « cn », des utilisateurs est construit comme suit :

- nom d'usage (en majuscules sans caractères diacritiques) ;
- suivi d'un espace ;
- suivi du prénom usuel (en minuscule, sauf la première lettre, et avec caractères diacritiques).

Les lettres entrelacées sont séparées et les traits d'union et les apostrophes sont remplacés par des espaces.

Exemple : *DE LA FONTAINE Jean Pierre*

Remarque : L'unicité d'un « cn » dans la branche *people* n'est pas garantie. Il ne sera donc pas utilisé dans la construction du « dn ».

Le porteur pourra éventuellement proposer une autre règle de construction du « cn ».

4.4.5. Photographie

Toute entrée appartenant à la classe *inetOrgPerson* ou à une classe qui en hérite possède un attribut « *jpegPhoto* ». Cet attribut permet de stocker une photographie au format JPEG ; il n'est utilisé que pour certaines catégories de personnes.

Le stockage de ces photographies au sein de l'ENT représente un volume de données conséquent qui peut impacter fortement les performances de l'annuaire ENT.

Des indications volumétriques sont données au chapitre 8. À partir de ces informations, le soumissionnaire indiquera s'il est préférable de stocker les photographies dans l'annuaire ENT ou au sein d'un support de stockage externe.

Dans le deuxième cas, l'annuaire ENT ne conservera que le chemin permettant d'accéder au fichier.

Dans tous les cas, un contrôle sur la taille maximum des photographies sera nécessaire.

4.4.6. Construction du « dn »

Chaque entrée de l'annuaire est référencée de manière unique dans le DIT par son « dn » (*Distinguished Name*). Il s'agit du chemin d'accès à l'entrée depuis le sommet de l'arbre.

La construction du « dn » est la suivante :

- Le « dn » des entrées représentant des personnes sera basé sur l'attribut « uid ».
- Le « dn » des entrées représentant des structures d'établissement sera basé sur l'attribut « ENTStructureUAI ».
- Le « dn » des entrées représentant les autres structures sera basé sur l'attribut « ENTStructureSIREN ».
- Le « dn » des entrées représentant des groupes sera basé sur l'attribut « cn ».
- Le « dn » des entrées représentant des applications sera basé sur l'attribut « ENTApplicationId ».

4.4.7. Clé de jointure

Afin d'assurer la correspondance entre les objets personnes et structures des sources autoritaires et ceux stockés dans l'annuaire ENT, il est nécessaire de disposer d'un identifiant commun jouant le rôle de clé de jointure.

Chaque source autoritaire fournit donc une clé de jointure persistante, qui permet d'identifier de manière unique chaque personne et chaque structure au fil des alimentations successives, et donc de suivre le cycle de vie des objets (modification des attributs et suppression). **Cette clé de jointure doit notamment être pérenne d'une année scolaire sur l'autre.**

Une même entrée personne ou structure dans l'annuaire ENT doit cependant disposer d'une clé de jointure pour chacune des sources autoritaires qui permettent d'alimenter un ou plusieurs des ses attributs.

Les clés de jointure sont stockées dans l'annuaire ENT grâce aux attributs multi-valués « ENTPersonJointure » (pour les personnes) et « ENTStructureJointure » (pour les structures). Ils sont construits comme suit :

- Identifiant de la source autoritaire. Les identifiants sont les suivants :
 - Alimentation manuelle depuis l'ENT : identifiant = « ENT ».
 - Alimentation depuis le SI du MENESR : identifiant = « AC- » + nom de l'académie.
 - Autres sources d'alimentation : identifiant librement défini par chaque projet ENT.
- Suivi du caractère « \$ ».
- Suivi de la clé de jointure fournie par la source autoritaire pour désigner l'objet.

NB : Ce champ est distinct de l'identifiant unique des personnes sur l'annuaire ENT, défini au chapitre 4.4.1.

5. ARCHITECTURE TECHNIQUE DE L'ANNUAIRE ENT

Plusieurs exigences et éléments de contexte ont servi à bâtir l'architecture technique de l'annuaire ENT :

- Les besoins en termes d'usage de l'annuaire : mise à jour, gestion, authentification / autorisation, consultation.
- La répartition géographique des sources d'alimentation, notamment celles du MENESR.
- Le périmètre minimum couvert par un ENT (à savoir un département).
- La volumétrie attendue.

Sur la base de ces éléments, une solution d'architecture a été définie. Cette architecture est présentée en détails au chapitre 5.1.

Cette solution peut être déclinée en trois options afin de garantir des niveaux de disponibilité et de partage de charge en adéquation avec les exigences de qualité de service.

Le soumissionnaire préconisera l'option la plus pertinente au regard de son offre technique et des éléments de volumétrie présentés au chapitre 8. Par défaut, l'option à retenir sera la première.

Le porteur pourra cependant choisir d'imposer une des options aux soumissionnaires.

5.1. PRINCIPES D'ARCHITECTURE

La solution d'architecture (Figure 14) repose sur la séparation de l'annuaire ENT en deux référentiels typés par usage :

- Un référentiel pour les mises à jour, la gestion et la consultation d'informations.
- Un référentiel pour l'authentification et l'autorisation des utilisateurs.

Quelques éléments de justification :

- *Les performances du référentiel d'authentification et d'autorisation ne sont pas impactées par les requêtes de consultation et les accès en écriture lors des mises à jour.*
- *Cette séparation permet d'appliquer des procédures d'exploitation adaptées aux exigences de qualité de service de chacun des référentiels (plus fortes pour un référentiel d'authentification / autorisation que pour un référentiel de consultation).*

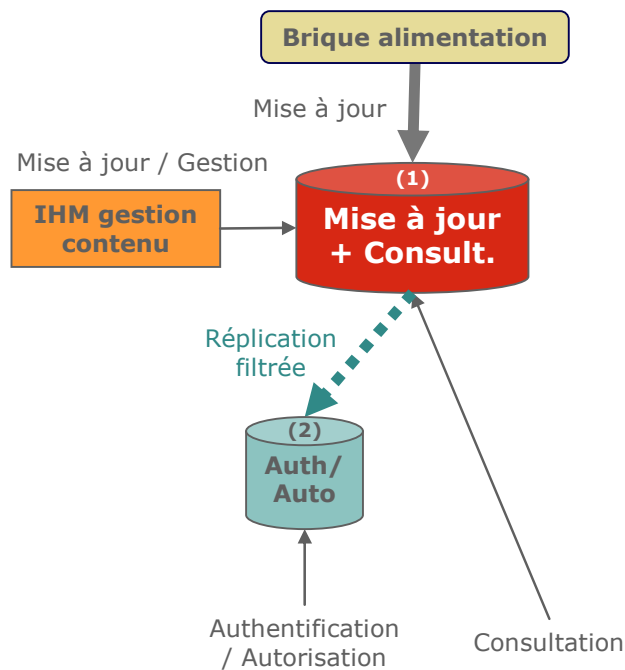


Figure 14 : Solution d'architecture de l'annuaire ENT

La brique d'alimentation correspond au composant technique du service d'alimentation chargé de la mise à jour automatique de l'annuaire ENT (cf. chapitre 7.1.1). Les mises à jour depuis cette brique, ainsi que les mises à jour manuelles depuis l'IHM de gestion de contenu, sont réalisées sur le référentiel (1). Celui-ci traite également les requêtes de consultation, en provenance des applications.

Le référentiel (2) est dédié aux requêtes d'authentification et d'autorisation. Il est alimenté par réplication filtrée depuis le référentiel (1). Seuls les attributs utiles à la gestion des autorisations sont répliqués dans le référentiel (2). Ces attributs sont marqués par une croix dans la colonne « Autorisa. » du tableau de l'Annexe 5.

INDEXATION DE L'ANNUAIRE ENT

Afin d'améliorer le temps de réponse aux requêtes effectuées sur l'annuaire ENT, des index doivent être créés sur certains attributs.

Le référentiel de « mise à jour, gestion et consultation » et le référentiel « d'authentification / autorisation » pourront disposer d'index différents.

Il est notamment recommandé de créer des index sur les attributs suivants : « uid », « login », « alias », « ENTPersonStructRattach ».

5.2. ARCHITECTURE – OPTION 1

La première option (Figure 15) correspond à une mise en œuvre minimaliste de la haute-disponibilité sur la solution d'architecture présentée précédemment.

La haute-disponibilité repose sur la mise en place d'un référentiel (1') de secours. Il s'agit d'une réplication totale du référentiel (1) de mise à jour et de consultation.

Les applications ne s'adressent qu'à un proxy LDAP (ou un commutateur de niveau 7/Applicatif) dont le rôle est de répartir les requêtes en fonction de leur type :

- Les requêtes de consultation sont dirigées vers le référentiel (1).
- Les requêtes d'authentification / autorisation sont dirigées vers le référentiel (2).

Remarque : Un proxy LDAP offre cependant des fonctions plus avancées permettant d'optimiser les performances (ex. : gestion de cache).

Si un des référentiels (1) ou (2) ne répond pas, le proxy LDAP (ou le commutateur de niveau 7) redirige les requêtes vers le référentiel (1') de secours.

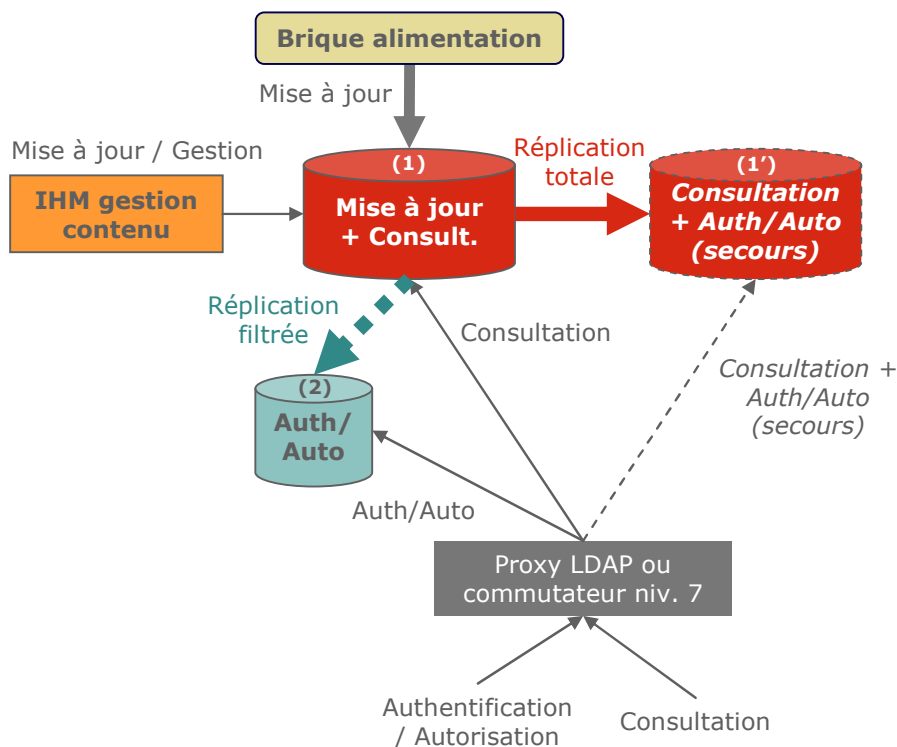


Figure 15 : Architecture – Option 1

Remarques :

- Si le référentiel (1) de mise à jour et de consultation est indisponible, il ne sera plus possible de mettre à jour l'annuaire ENT, que ce soit automatiquement ou via l'IHM de gestion de contenu.
- Si les référentiels (1) et (2) sont indisponibles en même temps, toutes les requêtes seront redirigées sur le même référentiel (1') de secours, avec un risque de dégradation des performances.

5.3. ARCHITECTURE – OPTION 2

L'option 2 (Figure 16) complète l'option 1. La redirection des requêtes par un proxy LDAP (ou un commutateur niveau 7) est reprise. Cependant, cette option permet en plus d'assurer la haute-disponibilité pour les actes de mises à jour et de gestion via l'IHM de gestion de contenu.

L'IHM de gestion de contenu est redondée et les requêtes correspondantes passent désormais par le proxy LDAP (ou commutateur niveau 7). En fonctionnement nominal, ces requêtes sont dirigées vers le référentiel (1) de mise à jour et de consultation. Si celui-ci n'est pas disponible, elles sont alors redirigées vers le référentiel (1') de secours.

Afin que les modifications apportées au référentiel (1') de secours lors d'un dysfonctionnement soient prises en compte dans le référentiel (1), une réplication totale multi-maîtres est mise en place entre les référentiels (1) et (1').

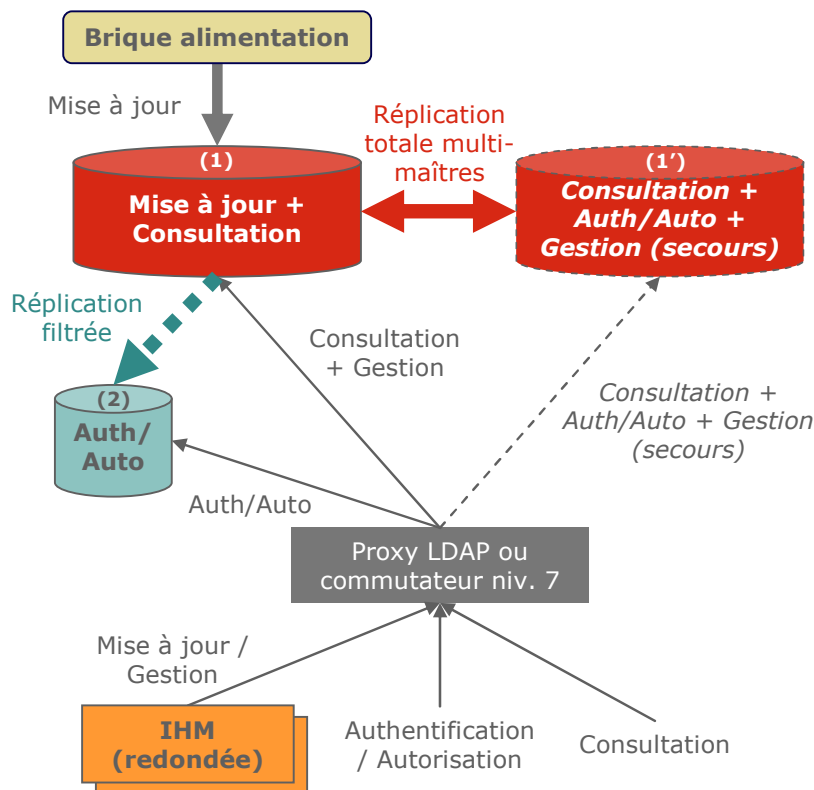


Figure 16 : Architecture – Option 2

Remarques :

- Si le référentiel (1) de mise à jour et de consultation est indisponible, il ne sera plus possible de mettre à jour l'annuaire ENT via la brique d'alimentation.
- Les modifications apportées au référentiel (1') lors d'un fonctionnement en mode secours ne seront répercutées sur le référentiel (2) d'authentification / autorisation que lorsque le référentiel (1) sera de nouveau opérationnel.

5.4. ARCHITECTURE – OPTION 3

L'option 3 (Figure 17) généralise la haute-disponibilité à tous les composants de l'architecture et ajoute la répartition de charge. Elle est constituée des éléments suivants :

- Deux référentiels de mise à jour, consultation et gestion : (1) et (1'). Une réplication totale multi-maîtres est mise en place entre ces deux référentiels.
- Deux référentiels d'authentification / autorisation : (2) et (2'). Une réplication totale multi-maîtres est mise en place entre ces deux référentiels. Ils sont alimentés par réplication filtrée, respectivement depuis les référentiels (1) et (1').

- Un commutateur niveau 7, secouru en *Heartbeat*, répartit les requêtes de mise à jour / gestion, d'authentification / autorisation et de consultation sur deux proxies LDAP en fonction de leur charge.
- Chaque proxy LDAP n'est relié qu'à un seul référentiel de mise à jour, consultation et gestion ((1) ou (1')) et un seul référentiel d'authentification / autorisation ((2) ou (2')). Le proxy redirige alors les requêtes vers le référentiel adéquat.

Les applications et l'IHM de gestion de contenu ne s'adressent qu'au commutateur.

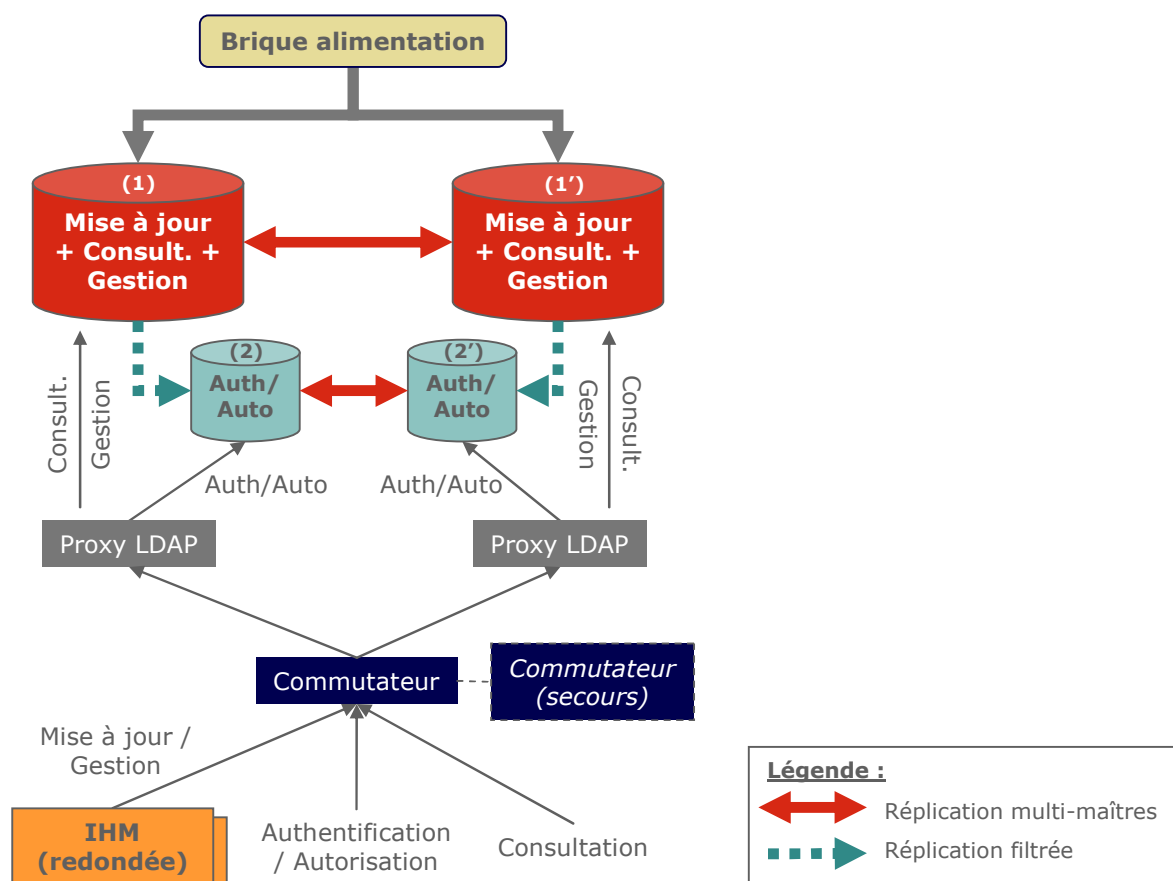


Figure 17 : Architecture – Option 3

Remarque : Cette architecture pourrait permettre de localiser sur deux sites différents les référentiels (1)–(2) et (1')–(2').

6. ANNUAIRE ET ACCES INTER-ENT

BESOINS A COUVRIR

L'annuaire d'un ENT contribue à offrir des services d'identification/authentification et d'autorisation des utilisateurs de cet ENT sur les applications qu'il héberge.

Au-delà de ces accès « locaux », d'autres services sont attendus :

- Accès *croisés* : il s'agit de permettre l'accès des utilisateurs d'un ENT à des applications tierces sans obliger les utilisateurs à se signer de nouveau s'ils ont déjà été authentifiés sur leur ENT.

Ces applications sont des applications hébergées par un autre ENT ou proposées par un tiers. Elles ont une couverture nationale.

Dans le cas d'accès aux applications d'un tiers, les caractéristiques suivantes doivent être respectées :

- ▶ Un utilisateur donné doit toujours se présenter avec la même identité afin de suivre et tracer ses accès dans la durée.
 - ▶ La preuve d'authentification présentée à l'application proposée par le tiers ne doit porter aucune information susceptible de pouvoir identifier nommément la personne accédante (notion de préservation de l'anonymat).
- Accès *multi-ENT* : il s'agit de permettre à des utilisateurs qui sont sur de multiples ENT d'accéder aux applications de ces différents ENT sans obliger ces utilisateurs à se signer de nouveau s'ils ont déjà été authentifiés sur un de leurs ENT.

Notons que ces besoins d'interopérabilité ne concernent que des fonctions de sécurité : identification/authentification et autorisation.

Le tableau suivant précise par catégorie de personnes les besoins à couvrir ainsi qu'un premier niveau d'information sur le volume d'utilisateurs concernés.

Catégorie de personnes	Besoins à couvrir	
	Accès croisés	Accès multi-ENT
Élève	Oui	Oui (quelques centaines ou milliers sur le périmètre national)
Enseignant	Oui	Oui (quelques centaines ou milliers sur le périmètre national)
Personne en relation avec l'élève	Oui	Oui (quelques centaines sur le périmètre national)
Non enseignant rattaché à des services académiques	Oui	Oui (quelques centaines sur le périmètre national)
Non enseignant rattaché à une collectivité locale	Oui	Oui (quelques centaines sur le périmètre national)
Non enseignant rattaché à un établissement	Oui	Oui (quelques centaines sur le périmètre national)
Personnel extérieur	Sans objet	
Tuteur de stage / Maître d'apprentissage		
Responsable d'entreprise		

PRINCIPES DE LA SOLUTION A METTRE EN PLACE

La couverture de ces besoins nécessite la mise en œuvre d'un environnement d'interopérabilité entre **les services AAS des ENT** et ceux de l'environnement hébergeant l'application accédée.

Le principe retenu pour répondre à ces attentes est décrit dans le document [2] ; il s'appuie sur la mise en place de services de type « fédération d'identités » et d'une relation de « confiance » entre les environnements.

La figure suivante illustre la solution dans le cas d'un utilisateur d'un ENT 1 accédant à une application de l'ENT 2 – accès croisés.

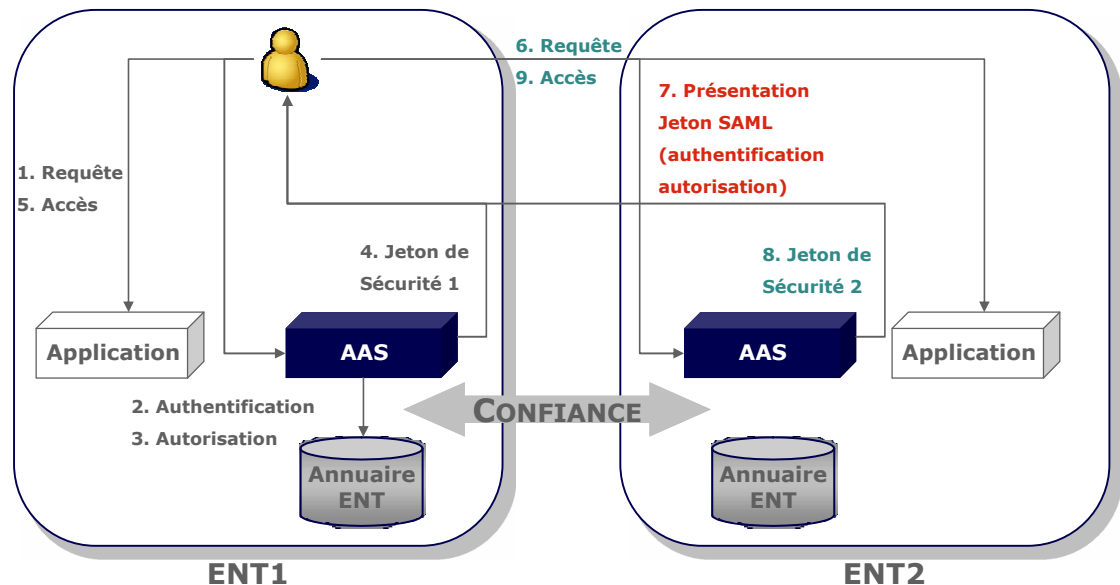


Figure 18 : Accès d'un utilisateur à une application d'un autre ENT

La cinématique des accès est la suivante :

1. Tentative d'accès à une application de l'ENT 1.
2. L'utilisateur non authentifié est redirigé vers le service AAS de l'ENT 1 ; il s'authentifie en présentant son identifiant et son mot de passe.
3. Le service AAS vérifie via son modèle de sécurité mis en œuvre que l'utilisateur est autorisé à accéder à l'application.
4. Le service AAS de l'ENT 1 fournit un jeton de sécurité porteur d'informations d'identité de l'utilisateur (preuve d'authentification, identifiant et éventuellement d'attributs) à l'utilisateur (ce jeton sera présenté par l'utilisateur à toutes les applications de l'ENT 1, de manière transparente pour l'utilisateur, et permettra généralement à l'utilisateur d'éviter de se signer de nouveau).
5. L'utilisateur accède à l'application en présentant ce jeton de sécurité.
6. Tentative d'accès à une application de l'ENT 2.

7. Le service AAS de l'ENT 2 identifie que l'application en question nécessite la présentation d'un jeton de sécurité différent (sur la base d'un format pivot mis en place à travers la relation de confiance entre l'ENT 1 et l'ENT 2). Puis, il fournit ce jeton à l'utilisateur qui le présente alors à l'application de l'ENT 2. Ce jeton présenté porte des informations permettant de prouver l'identité de l'accédant (authentification sur l'ENT 2) et d'autres caractéristiques propres à l'utilisateur (ces informations ont un sens pour les services AAS de l'ENT 2, elles permettent d'autoriser l'accès à l'application).
8. Si l'utilisateur est authentifié et autorisé, il reçoit un jeton de sécurité fourni par le service AAS de l'ENT 2.
9. L'utilisateur accède à l'application en présentant ce jeton de sécurité.

Notons que la fédération des identités multiples des personnes de l'ENT dans divers environnements de la sphère publique n'est pas couverte dans le présent cahier des charges. Néanmoins, tous les éléments de l'annuaire sont normés pour le permettre à terme.

FONCTIONS ATTENDUES SUR L'ANNUAIRE

Pour contribuer à la mise en place de cette solution, l'annuaire ENT va donc offrir les fonctions suivantes :

- Fourniture de l'identifiant interne à l'ENT d'un utilisateur, qui pourra selon le cas être anonymisé par les services AAS (cf. chapitre 4.4.1 pour la définition de l'identifiant interne).

L'identifiant possède les caractéristiques suivantes :

- Il est unique sur un périmètre national.
- Il est géré localement sur l'ENT.

Notons qu'il n'est pas invariant dans le temps. En cas de changement d'ENT, l'utilisateur se verra attribuer un nouvel identifiant ; ses accès à des services tiers ne pourront alors être suivis.

- Mise en place systématique au sein de chaque ENT des profils à portée nationale et fourniture des profils d'un utilisateur.

Ces profils à portée nationale sont les suivants :

Identifiant du profil	Description du périmètre
National_1	Élève
National_2	Responsable d'un élève (parent, tuteur légal)
National_3	Enseignant
National_4	Personnel de direction de l'établissement
National_5	Personnel de vie scolaire travaillant dans l'établissement
National_6	Personnel administratif, technique ou d'encadrement travaillant dans l'établissement
National_7	Personnel de rectorat, de DRAF, de collectivité locale, d'inspection académique

Ils permettront à un administrateur de donner des droits d'accès à une application en se basant sur ces profils et ainsi autoriser les accès (par exemple, autoriser les utilisateurs ayant le profil « Élève » à consulter une encyclopédie). Les informations de profils seront présentées par l'accédant dans le jeton de sécurité, ce qui permettra de l'autoriser.

Ces profils ont les caractéristiques suivantes :

- ▶ Ils ne peuvent être supprimés de l'annuaire.
- ▶ Leurs identifiants ne peuvent être modifiés localement dans l'annuaire sans contrôle préalable.
- ▶ Ils sont par défaut peuplés automatiquement en fonction de la valeur d'un ou plusieurs attributs caractérisant les personnes. Ils peuvent être complétés de manière discrétionnaire.

Les règles de peuplement par catégorie de personnes peuvent être précisées par le porteur.

- Fourniture des informations suivantes sur un utilisateur :

Catégorie de personnes	Informations à transmettre (identifiant et description)
Élève	Académie / Établissement / « Statut » de l'élève / Niveau de formation / Filière / Enseignements (plusieurs fois si dans plusieurs établissements dépendant du même projet ENT)
Enseignant	Académie / Établissement / Matières enseignées (plusieurs fois si dans plusieurs établissements dépendant du même projet ENT)
Personne en relation avec l'élève	Établissement
Non enseignant rattaché à des services académiques	Établissement
Non enseignant rattaché à une collectivité locale	Établissement
Non enseignant rattaché à un établissement	Établissement
Personnel Académique	Structure
Personnel Collectivité	Structure

Ces informations ont les caractéristiques suivantes :

- ▶ Elles doivent être obligatoirement renseignées dans l'annuaire.
- ▶ Leur nomenclature ne peut être localement modifiée dans l'annuaire sans contrôle préalable : il s'agit de nomenclatures nationales qui doivent nécessairement être utilisées.

Notons que :

- *La solution proposée impose pour couvrir le besoin d'accès multi-ENT les contraintes suivantes :*
 - ▶ *Un utilisateur est géré sur un et un seul ENT, à choisir parmi ceux auxquels il appartient.*
 - ▶ *Il doit s'authentifier au préalable sur l'ENT sur lequel il est géré avant d'accéder à des applications d'un autre ENT.*

Il n'est pas demandé au soumissionnaire de couvrir ces contraintes via la fourniture d'une solution, elles le seront via des mesures organisationnelles et opérationnelles.

- *Le soumissionnaire pourra éventuellement proposer une solution basée sur des synchronisations entre les annuaires des différents environnements en précisant les services proposés notamment pour la synchronisation des mots de passe. Cette solution sera alors considérée comme dégradée.*

7. SERVICES DE L'ANNUAIRE ENT

Cette partie décrit l'ensemble des services attendus pour l'annuaire ENT.

Le soumissionnaire détaillera, pour chaque fonctionnalité, le mode de fonctionnement de sa solution et les principes de mise en œuvre (pré-requis, développements et paramétrages nécessaires...). Une distinction claire devra être effectuée entre les fonctionnalités natives (ne nécessitant qu'un paramétrage), les fonctionnalités à développer, et les fonctionnalités non prises en charge.

Le porteur pourra, en fonction de ses besoins, ne pas faire figurer dans son cahier des charges certaines fonctionnalités présentées ci-après, ou a contrario ajouter certaines fonctionnalités manquantes.

Par ailleurs, le porteur précisera les éléments suivants :

- Charte graphique et gabarit des IHM.*
- Cinématique / dynamique des pages.*

7.1. SERVICES DE GESTION

7.1.1. Services d'alimentation

[SRV-1] Alimentation depuis un fichier

Deux types d'alimentation par fichiers sont envisageables :

- **Alimentation depuis un fichier XML fourni par le MENESR.**

Le fichier XML fourni par le MENESR comporte les objets personnes et structures gérés par le MENESR ainsi que leurs caractéristiques. Le format de ce fichier est détaillé à l'Annexe 4.

- **Alimentation depuis un fichier fourni par une autre source externe.**

Le soumissionnaire proposera a minima un connecteur permettant l'alimentation de l'annuaire ENT à partir de fichiers plats.

Le porteur pourra éventuellement compléter ce chapitre avec les informations concernant les autres sources d'alimentation. Les fichiers en question pourront être de type XML, DSML, CSV, LDIF...

Les services d'alimentation doivent :

- Permettre de créer, modifier, et supprimer des personnes et des structures, et leurs attributs dans l'annuaire ENT, à partir des données fournies dans le fichier plat, en définissant des règles de synchronisation et de jointure.
- Permettre de définir les fréquences d'alimentation.
- Permettre de suspendre une alimentation à tout moment.

- Implémenter des mécanismes de contrôle du format des fichiers en entrée, de gestion des erreurs (reprises), de gestion des doublons, de vérification des règles de synchronisation, de vérification des contraintes d'intégrité définies au chapitre 3.3.

Les contraintes d'intégrité liées à une limite quantitative (exemple : nombre maximum d'élèves délégués par classe) devront être paramétrables.

- Implémenter des notifications d'alertes en cas d'erreur ou de non respect de règles ou de contraintes.

Ces alertes pourront être classées en différents niveaux. Selon le niveau d'alerte, le mécanisme d'alimentation pourra ou non être stoppé.

Le porteur pourra préciser les niveaux d'alertes et les processus associés qu'il souhaite mettre en œuvre, ou laisser à la discrétion du soumissionnaire le fait d'effectuer des propositions en ce sens.

Remarque : L'alimentation des mots de passe ne fait pas partie des fonctions attendues pour les services d'alimentation.

[SRV-2] Règles de gestion de l'alimentation

Les services d'alimentation doivent prendre en compte des règles de gestion de l'alimentation, et nomment :

- des règles de transformation de la casse des attributs alimentés ;
- des règles de construction des clés de jointure (cf. chapitre 4.4.7) ;
- des règles de répartition des objets alimentés entre les différentes catégories de personnes et de structures gérées au sein de l'annuaire ENT ;
- des règles de transformation des références (entre objets alimentés) en *dn* pointant vers des objets de l'annuaire ENT.

Exemple : l'attribut « ENTElevePere » d'un objet *ENTEleve* doit référencer un objet *ENTAuxPersRelEleve* présent dans l'annuaire ENT.

Les règles de gestion pourront être **spécifiques à chaque source autoritaire**. Les règles concernant l'alimentation depuis le SI du MENESR sont décrites à l'Annexe 4.

Le porteur pourra compléter ce chapitre avec des règles de gestion complémentaires, notamment par rapport à d'autres sources d'alimentation que le SI du MENESR.

[SRV-3] Réconciliation des informations issues de différentes sources autoritaires

Les informations concernant une même personne physique peuvent provenir de différentes sources autoritaires, notamment lorsqu'une personne appartient à plusieurs catégories de personnes. Ainsi, les informations d'un parent d'élève travaillant pour une collectivité locale proviendront à la fois du SI du MENESR et du SI de la collectivité.

Afin que chaque personne physique puisse disposer d'un seul compte sur l'annuaire ENT (et donc d'un seul identifiant de connexion), les services d'alimentation doivent permettre de réconcilier les informations issues des différentes sources autoritaires. Cette réconciliation ne pourra se faire qu'à l'initiative de la personne concernée.

Pour tout objet « Personne », le principe de réconciliation est le suivant :

- La personne se connecte à l'ENT à l'aide d'un de ses comptes, <compte1>, puis accède au service de réconciliation.

- L'ENT demande à la personne :
 - de saisir à nouveau le mot de passe de <compte1> ;
 - de saisir l'identifiant de connexion (login) et le mot de passe du ou des comptes qui doivent être réconciliés avec <compte1> ;
 - de choisir le compte de référence parmi <compte1> et les autres comptes. Ce compte de référence détermine :
 - L'identifiant de connexion et le mot de passe qui seront utilisés pour les prochains accès à l'ENT ;
 - Les informations qui seront conservées en cas de divergence entre les différentes sources (nom de famille orthographié différemment par exemple).
- Après vérification des identifiants de connexion et des mots de passe, l'ENT :
 - ajoute les informations provenant des différents comptes au compte de référence ;
 - conserve l'ensemble des clés de jointure ;
 - rappelle à la personne l'unique identifiant de connexion qui doit désormais être utilisé.

Remarque : Pour une même source autoritaire, une même personne physique peut être vues comme deux objets différents, et donc être alimentée sous deux clés de jointure différentes. Une réconciliation sera donc nécessaire également dans ce cas (cf. Annexe 4 pour l'alimentation depuis le SI du MENESR).

7.1.2. Services de gestion de contenu

[SRV-4] Environnement de gestion central et unique

Le service de gestion de contenu doit proposer un environnement de gestion central et unique donnant accès aux fonctions de gestion des entrées de l'annuaire ENT.

L'accès à l'environnement de gestion des entrées est réservé aux administrateurs centraux et locaux, et aux utilisateurs. Ils doivent se signer par la fourniture d'un couple « identifiant / mot de passe ».

[SRV-5] Gestion des personnes et des structures

Le service de gestion de contenu doit permettre d'appliquer des opérations (création, modification, suppression) sur les personnes et les structures de l'annuaire ENT :

- Gestion des d'entrées correspondant à des personnes :
 - Création / suppression d'entrées.
 - Modification des attributs d'une entrée.
 - Ajout / suppression d'une catégorie à une personne.
- Gestion des d'entrées correspondant à des structures :
 - Création / suppression d'entrées.
 - Modification des attributs d'une entrée.

Le service de gestion de contenu doit notamment contrôler les contraintes d'intégrité mentionnées au chapitre 3.3 et permettre de gérer les multiples relations d'un élève avec des personnes en relation avec les élèves.

Ces différentes opérations seront par ailleurs implémentées en conformité avec les contraintes d'intégrité présentées aux chapitres 3.3 et 4.2.1.

Remarques :

- Ces fonctions seront notamment utilisées pour compléter le peuplement de l'annuaire ENT avec les catégories de personnes et de structures qui ne sont pas alimentées automatiquement.
- Toute donnée issue de l'alimentation MENESR n'est pas modifiable dans l'interface de gestion de contenu, à l'exception de certains attributs mentionnés dans la colonne « Alimentation » du tableau de l'Annexe 2. Ces attributs sont en effet initialisés par l'alimentation MENESR puis proposés en self-service (civilité, email...).

[SRV-6] Gestion des nomenclatures

Le service de gestion de contenu doit offrir une fonction de gestion des nomenclatures. Ce service consiste en l'implémentation et en la gestion d'une table de nomenclature locale permettant d'associer chaque attribut ne disposant pas d'une nomenclature nationale à une nomenclature définie localement.

[SRV-7] Gestion des listes rouges

L'outil de gestion de contenu doit permettre de gérer des listes rouges d'utilisateurs.

Ces utilisateurs n'apparaîtront pas dans les pages blanches. Les informations sur ces utilisateurs serviront uniquement à déterminer leurs habilitations.

Remarque : Cette fonctionnalité sera notamment utilisée dans le cas d'élèves placés sous protection juridique.

[SRV-8] Gestion des groupes de personnes / groupes de structures

Cette fonction offre la possibilité de gérer des groupes de personnes (classes, groupes de langue...) et des groupes de structures (regroupement d'établissements...).

- Création / suppression d'entrées.
- Modification de la liste des membres (ajout / suppression de membres)

Ces groupes peuvent être peuplés de trois manières :

- Discrétionnaire : le groupe est peuplé / dépeuplé manuellement par l'administrateur.
- Automatique : le groupe est peuplé / dépeuplé automatiquement en fonction de règles de peuplement basées sur des combinaisons de valeurs des attributs des personnes ou structures.
- Mixte : à la fois discrétionnaire et automatique.

Il est également possible de créer des groupes de groupes. Les objets peuplés peuvent être des groupes ou des personnes (ou structures). Le nombre de récursivité n'est pas limité.

[SRV-9] Gestion des profils

Cette fonction offre la possibilité de gérer des profils.

- Création / suppression.
- Modification de la liste des membres (ajout / suppression de membres).

Ces profils peuvent être peuplés de trois manières :

- Discrétionnaire : le profil est peuplé / dépeuplé manuellement par l'administrateur.
- Automatique : le profil est peuplé / dépeuplé automatiquement en fonction de règles de peuplement basées sur des combinaisons de valeurs des attributs des personnes.
- Mixte : à la fois discrétionnaire et automatique.

Il est également possible de créer des profils de profils. Les objets peuplés peuvent être des groupes ou des personnes. Le nombre de récursivité n'est pas limité.

Un profil peut être exclusif. Une personne associée à un profil exclusif ne peut être associée à tout autre profil ou à certains profils.

Un profil peut hériter d'un profil existant. L'ensemble des attributs du profil hérité est alors associé automatiquement au profil héritant, dont notamment la liste des personnes membres du profil et les rôles applicatifs associés.

[SRV-10] Gestion des rôles applicatifs

Cette fonction offre la possibilité de gérer des rôles applicatifs.

- Création / suppression.
- Association à une application.
- Gestion de l'association à un ou plusieurs profils.

Remarque : Une personne peut directement être associée à un rôle applicatif, soit de manière discrétionnaire, soit de manière automatique, sans l'intermédiaire d'un profil associé à ce rôle.

[SRV-11] Gestion des applications

Sur son périmètre d'administration, un administrateur peut créer, modifier, supprimer une application.

Une application peut être associée à zéro, un, ou plusieurs rôles applicatifs.

Remarque : Certains éléments caractérisant les applications sont liées aux services AAS implémentés, et ne sont pas intégrés à ce document (exemples : période d'accès, typologie d'accès, modes d'authentification...).

[SRV-12] Délégation des droits d'accès aux données de l'annuaire ENT

Des droits d'accès en lecture / écriture sont positionnés sur les objets et attributs de l'annuaire ENT.

Des périmètres distincts d'administration sont définis pour chaque administrateur (délégation ou répartition de l'administration des utilisateurs).

Les périmètres suivants peuvent être définis :

- Des portées d'administration : objets et attributs de ces objets.
- Des actions d'administration sur ces portées :
 - ▶ Droits : lecture, création, modification, suppression de données.
 - ▶ Capacité à déléguer ces droits :
 - à une ou plusieurs personnes (de manière discrétionnaire, par appartenance à un groupe...);
 - sur une période donnée (date d'effet / date de fin) ;

- attribution de tout ou partie des droits dont on dispose ;
- attribution de la capacité de déléguer tout ou partie de ces droits à d'autres personnes.

Des recouvrements de périmètres entre administrateurs sont possibles.

Un niveau hiérarchique est associé à chaque administrateur. Un administrateur de niveau n peut annuler toutes les actions réalisées par les administrateurs de niveau inférieur ou modifier toutes les données accessibles par les administrateurs de niveau inférieur.

Un administrateur peut ainsi définir les droits d'un utilisateur sur les attributs le caractérisant (lecture / écriture / capacité de délégation d'administration sur ses attributs).

Exemple d'implémentation : définitions

Ces différents services permettent par exemple de décliner l'organisation suivante, selon quatre niveaux : administrateur central, propriétaire, gestionnaire, utilisateur.

1. *L'administrateur central a en charge la création et la gestion des objets transverses à l'ENT tels que les profils partagés, et les rôles applicatifs et les applications transverses.*
2. *Les propriétaires possèdent les droits en écriture sur les objets de leur périmètre, et définissent pour chacun des attributs d'un type d'objet :*
 - *les gestionnaires et leurs droits (lecture / écriture) ;*
 - *la capacité à déléguer ces droits.*
3. *Les gestionnaires sont responsables de la gestion / mise à jour des objets / attributs.*
4. *Un utilisateur est un gestionnaire particulier, n'ayant des droits d'écriture et de capacité à déléguer un droit en lecture ou en écriture uniquement sur ses attributs.*

Notons que le porteur doit présenter au chapitre 9.1 l'organisation retenue dans le cadre de son projet ENT.

Remarque : Au regard du schéma d'annuaire (cf. chapitre 4.2) et de l'organisation de la gestion du contenu envisagée (cf. chapitre 9.2), le soumissionnaire précisera s'il est envisageable de positionner des ACL de premier niveau directement sur l'annuaire, ou si l'ensemble de ces droits devra être géré au niveau des services de gestion de contenu. Dans le premier cas, il précisera quelles ACL doivent être positionnées.

[SRV-13] Délégation des droits d'accès sur les applications

Une personne, sous réserve qu'elle soit autorisée à le faire, doit pouvoir déléguer tout ou partie de ses droits d'accès à une ou plusieurs applications, et ce de manière temporaire.

Une délégation temporaire de droits se caractérise par :

- Une liste de personnes à qui les droits (tout ou partie des droits possédés) sont délégués (liste discrétionnaire, liste basée sur un groupe de personnes ou sur un profil).
- Une période donnée : une date d'effet et une date de fin de cette délégation pour chaque personne déléguée.
- La capacité pour chaque personne déléguée de déléguer elle-même à d'autres personnes tout ou partie de ces droits.

[SRV-14] Gestion des suspensions

Le service de gestion offre la capacité de suspendre les personnes.

Lorsqu'une personne est suspendue, toutes ses caractéristiques sont conservées (attributs, liens...) mais la personne ne peut pas accéder aux applications de l'ENT.

Il est également possible de positionner pour toute personne une date d'activation et une date de fin de validité. En fonction de ces dates, des traitements de suspension ou de notification de suspension peuvent être lancés.

Il est possible de réactiver une personne suspendue.

[SRV-15] Import / export de fichiers

Le service de gestion de contenu doit permettre :

- d'importer un fichier afin de peupler l'annuaire ENT ;
- d'exporter dans un fichier des entrées sélectionnées.

Les formats de fichier devant être pris en charge sont les suivants : CSV, LDIF, XML.

[SRV-16] Outil de workflow

Les processus définis au chapitre 9.2 doivent être informatisés. Pour ce faire, les fonctions de *workflow* suivantes sont attendues :

- Une interface graphique et simple d'utilisation permettant de créer et de gérer les *workflows* relatifs aux processus de l'ENT.
- La capacité à gérer les fonctionnalités classiques de *workflow* : validation en série, en parallèle, escalade en cas de non traitement dans les délais impartis, champs à renseigner de façon obligatoire ou facultative pour valider une étape du *workflow*, envoi de notification par mail, envoi de mail prédéfini selon la ressource traitée, édition d'état papier...

[SRV-17] Changement de mot de passe

Le service de gestion de contenu doit permettre aux utilisateurs de modifier leur mot de passe. Cette action nécessite :

- de saisir l'ancien mot de passe ;
- de saisir et confirmer le nouveau mot de passe.

Les mots de passe ne doivent pas être stockés en clair. Ils devraient être stockés de manière chiffrée et irréversible, éventuellement sous forme d'empreintes numériques (cf. document [2]).

[SRV-18] Création / modification / suppression de l'alias

Le porteur pourra supprimer cette fonctionnalité s'il ne souhaite pas la proposer.

Un utilisateur peut se créer, s'il le souhaite, un alias de connexion l'ENT. Il ne peut disposer que d'un seul alias. La règle retenue pour la création des alias sur le périmètre de l'ENT est la suivante : « premier arrivé, premier servi ».

Le porteur pourra envisager de demander au soumissionnaire la mise en œuvre d'un workflow spécifique de validation des demandes d'alias afin d'empêcher l'utilisation de noms d'alias réservés, vulgaires, pouvant induire en erreur...

[SRV-19] Demande de modification de ses propres informations

Le service de gestion de contenu doit permettre à une personne de demander des modifications sur certains de ses attributs non accessibles en écriture : changement de coordonnées, erreur de saisie... via l'utilisation d'un *workflow*.

La fiche de l'utilisateur passe alors en mode « édition ». Les modifications ne sont pas inscrites dans l'annuaire ENT mais transmises à la personne définie dans le *workflow*.

7.2. SERVICES D'ACCES

7.2.1. Services de sécurité

Ce chapitre présente les services de sécurité utilisés par les services AAS.

En fonction des services AAS retenus, le porteur pourra étendre la couverture fonctionnelle de ces services. En effet, seuls les services fondamentaux d'authentification et d'autorisation sont demandés par la suite.

Au regard des services demandés, le soumissionnaire indiquera les extensions de schéma LDAP nécessaires et les éventuels impacts sur l'architecture technique.

[SRV-20] Gestion de l'authentification

Lors de l'accès d'une personne à une application de l'ENT, les services AAS vérifient au travers d'une requête d'authentification la validité du couple « identifiant de connexion / mot de passe » dans l'annuaire ENT.

- Paramètres d'entrée : identifiant de connexion / mot de passe
- Paramètres de sortie : OK / NOK.

Remarque : L'utilisation d'un alias de connexion est possible.

Le porteur pourra supprimer cette remarque s'il ne souhaite pas proposer la fonctionnalité d'alias.

[SRV-21] Gestion de l'impersonnation

Le porteur pourra supprimer cette fonctionnalité s'il ne souhaite pas la proposer.

Une personne, lorsqu'elle souhaite accéder à une application pour laquelle elle possède plusieurs « rôles », peut choisir, lors de la phase d'authentification, avec quel rôle elle se connecte. Elle retrouve alors uniquement l'environnement applicatif et les droits associés au rôle choisi.

Remarque : Cette fonction peut nécessiter l'utilisation de comptes « tampon ». Le soumissionnaire détaillera la solution technique proposée.

[SRV-22] Gestion de l'autorisation

Lors de l'accès d'une personne à une application de l'ENT, les services AAS vérifie au travers d'une requête d'autorisation si la personne est autorisée à accéder à l'application demandée.

Le contrôle d'autorisation sur une application peut être réalisé sur la valeur d'un attribut de la personne, sur l'appartenance de la personne à un profil, sur l'appartenance de la personne à un rôle applicatif. Il ne peut se baser que sur un sous-ensemble défini des objets et attributs de l'annuaire ENT. Cette liste est précisée en Annexe 2.

Aussi, plusieurs types de requête sont envisageables :

- Requête autorisation de type 1 :
 - Paramètres d'entrée : identifiant de connexion de la personne / identifiant d'attribut / valeur d'attribut.
 - Paramètres de sortie : OK / NOK.
- Requête autorisation de type 2 :
 - Paramètres d'entrée : identifiant de connexion de la personne / identifiant de profil.
 - Paramètres de sortie : OK / NOK.
- Requête autorisation de type 3 :
 - Paramètres d'entrée : identifiant de connexion de la personne / identifiant de rôle applicatif.
 - Paramètres de sortie : OK / NOK.
- Requête autorisation de type 4 :
 - Paramètres d'entrée : identifiant de connexion de la personne.
 - Paramètres de sortie : liste des profils associés à la personne.
- Requête autorisation de type 5 :
 - Paramètres d'entrée : identifiant de connexion de la personne.
 - Paramètres de sortie : liste des rôles applicatifs associés à la personne.

7.2.2. Services de publication

[SRV-23] Publication pour les applications

Les applications de l'ENT, en cohérence avec leurs droits d'accès aux données de l'annuaire ENT, peuvent interroger l'annuaire ENT pour récupérer tout ou partie des caractéristiques d'une personne, d'une structure, la liste des membres d'un profil...

[SRV-24] Pages Blanches

Une personne peut consulter les fiches des autres personnes de l'ENT. Ces fiches pourraient comporter les zones suivantes afin d'organiser les informations :

- Informations civiles.
- Coordonnées personnelles.
- Coordonnées professionnelles.
- Informations administratives.

- Scolarité.
- Divers.

En fonction de ses droits, une personne ne pourra consulter que certaines informations sur les fiches des autres personnes.

Lorsque les attributs des fiches font référence à des entrées de l'annuaire ENT (des personnes, des structures, des classes, des groupes...), des liens hypertextes doivent permettre d'accéder aux fiches correspondant à ces entrées.

[SRV-25] Pages Jaunes

Une personne peut consulter les fiches des structures gérées par l'ENT. Ces fiches pourraient comporter les zones suivantes afin d'organiser les informations :

- Informations légales.
- Coordonnées géographiques.
- Coordonnées du standard.
- Divers.

Toutes les informations des fiches des structures sont consultables librement par toutes les personnes de l'ENT. Le porteur pourra éventuellement amender cette remarque.

Le service de consultation doit également permettre d'accéder aux fiches correspondant aux différents groupes de l'annuaire ENT (classes, groupes, regroupements d'établissements...) afin d'obtenir la liste des membres de ces groupes.

[SRV-26] Navigation

Les Pages Blanches doivent proposer une navigation arborescente avec affichage sur la zone principale de l'IHM de la fiche sélectionnée. Les arborescences suivantes doivent être proposées a minima :

- Par établissement, puis par catégorie de personnes, puis par ordre alphabétique.
- Pour un établissement, par catégorie de personnes, puis par ordre alphabétique.
- Par structure (établissement, services académiques, collectivité locale), puis par catégorie de personnes (consolidation).

[SRV-27] Recherche

La recherche constitue une fonctionnalité particulièrement importante du service de gestion de contenu. Ce dernier doit en effet permettre à la fois une recherche très ciblée et une recherche beaucoup plus générale.

Les recherches peuvent porter sur les différents attributs des catégories de personnes et notamment le nom, le prénom, la structure de rattachement, le niveau scolaire...

Pour les attributs dont la nomenclature définit une liste fermée, l'interface doit proposer des listes de choix en plus d'un champ libre.

L'outil doit permettre l'utilisation d'expressions logiques pour constituer des requêtes de recherche.

Des requêtes « standard » doivent également être proposées aux utilisateurs. La liste ci-dessous donne quelques exemples de requêtes qui pourraient être proposées :

- Rechercher toutes les personnes de la catégorie *<liste de catégories>* dans l'établissement *<liste d'établissements>*.
- Rechercher toutes les personnes de la catégorie *<liste de catégories>* liées à la classe/groupe *<liste des classes/groupes>*.
- Rechercher tous les *<catégorie de personnes>* dans l'établissement *<liste d'établissements>*.
- Rechercher tous les enseignants [respectivement les élèves] qui enseignent [respectivement qui suivent] l'enseignement *<liste d'enseignements>*.
- Rechercher toutes les personnes qui exercent la fonction ou le domaine *<liste de fonctions/domaines>*.

Le résultat de la recherche doit être présenté sous forme de tableau ou de liste. Un lien doit permettre de consulter la fiche correspondant à chacune des entrées retournées en résultat de la recherche.

La notion de « panier » doit être implémentée par l'outil de gestion de contenu. Ce terme désigne la capacité à conserver des entrées du résultat d'une requête pour effectuer des actions postérieures (exemples : envoi d'e-mail ou impression de chacune des fiches correspondantes...).

[SRV-28] Édition

Il est possible d'exporter une fiche, le résultat d'une recherche ou toutes les fiches issues d'une recherche dans un fichier, en précisant notamment :

- les fiches à exporter par rapport au résultat d'une recherche (quelles personnes, quelles structures) ;
- les attributs à exporter pour chaque fiche.

Les formats de fichier devant être pris en charge sont les suivants : PDF, CSV.

[SRV-29] Impression

Une fiche « Personne », une fiche « Structure », le résultat d'une recherche ou toutes les fiches issues d'une recherche peuvent être imprimées.

7.3. SERVICES TECHNIQUES

[SRV-30] Gestion des traces et historisation

Toute action ou activité doit être tracée et stockée dans des journaux, et en particulier :

- Flux d'alimentation de l'annuaire :
 - ▶ Type de flux.
 - ▶ Date de début et date de fin de l'accès.
 - ▶ Actes de gestion réalisés : actions, données.
- Accès des utilisateurs avec leur compte :
 - ▶ Identifiant de la personne.
 - ▶ Date de début et date de fin de l'accès.
 - ▶ Identifiant des applications accédées, durée de connexion par application.

- Actions de gestion des administrateurs :
 - ▶ Identifiant de la personne.
 - ▶ Date de début et date de fin de l'accès.
 - ▶ Actes de gestion réalisés : actions, données.
- Accès aux journaux et actions sur les journaux :
 - ▶ Identifiant du compte.
 - ▶ Date de début et date de fin de l'accès.
 - ▶ Actes réalisés : actions, données.
- Tentatives d'accès infructueuses :
 - ▶ Identifiant de la personne.
 - ▶ Date.
 - ▶ Motifs de l'échec.

[SRV-31] Journaux d'accès

L'accès aux journaux est soumis à une authentification et un contrôle d'autorisation. Les administrateurs habilités doivent se signer par la fourniture d'un couple « identifiant de connexion / mot de passe ».

Le système offre une fonction de gestion des journaux permettant d'archiver les journaux, de les visualiser, de réaliser des tris sur la base de toutes les informations qu'ils contiennent (identifiant de personne, applications accédées...), de les éditer ou de réaliser des exports.

Chaque administrateur habilité doit avoir la possibilité de se créer ses propres fonctions de tris en choisissant les critères et le format de représentation des résultats. Des fonctions de recherche mono-critère ou multi-critères sur les informations contenues dans les journaux sont mises à la disposition des administrateurs.

[SRV-32] Audit et reporting

Le service d'audit et reporting doit fournir une vision centralisée des habilitations des utilisateurs au travers de tableaux de synthèse. Ces tableaux doivent notamment présenter les informations suivantes :

- Utilisateurs appartenant à un profil ou à un rôle applicatif ; profils et rôles applicatifs d'un utilisateur.
- Rôles applicatifs associés à un profil ; profils associés à un rôle applicatif.
- Applications utilisant un profil ou un rôle applicatif ; rôles applicatifs et profils utilisés par une application.
- Personnes accédant à une application.
- ...

[SRV-33] Supervision

La solution mettra en œuvre des fonctionnalités permettant la détection automatique des erreurs de fonctionnement de la solution. Ces erreurs seront alors tracées automatiquement, la localisation du fichier de trace pouvant être paramétrée.

Le soumissionnaire précisera les outils de supervision supportés par sa solution, les modalités de cette compatibilité et la typologie des incidents pouvant être générés, par composant.

[SRV-34] Administration et pilotage

La solution mettra en œuvre une administration technique centralisée de la solution.

Le soumissionnaire détaillera les moyens mis en œuvre pour cette administration et, si la solution nécessite d'ordonnancer certains travaux, détaillera les outils d'ordonnancement supportés par la solution proposée.

[SRV-35] Sauvegarde / archivage

La solution mettra en œuvre des fonctionnalités de sauvegarde. Ces fonctionnalités permettront :

- des sauvegardes à intervalle régulier paramétrable et cela sans arrêt du service ;
- des restaurations déclenchées manuellement et cela sans arrêt du service.

Ce service devra également offrir des fonctions paramétrables d'archivage des données.

Le soumissionnaire précisera sur la base de son expérience l'ensemble des données à sauvegarder par composant de la solution, et les outils de sauvegarde supportés par sa solution et les modalités de cette compatibilité.

7.4. API DE SERVICE

[SRV-36] API de service

L'ensemble des services présentés précédemment doivent être accessibles via des API développées en C ou JAVA.

[SRV-37] Couche de services

En option, le soumissionnaire pourra proposer la réalisation d'une couche de services permettant de rendre les applications indépendantes du modèle de données de l'annuaire ENT, limitant ainsi les impacts en cas d'évolution de celui-ci.

Il devra choisir une méthode d'implémentation de la couche de services (de préférence basée sur une architecture « Web Services » à l'aide des techniques SOAP / WSDL / UDDI) et fournir un schéma d'architecture technique expliquant la mise en place de cette couche de services.

8. EXIGENCES SUR L'ANNUAIRE ENT

[EX-1] Volumétrie

Le volume des données stockées dans l'annuaire ENT est un élément structurant pour la définition de l'architecture technique. Ainsi, le porteur indiquera précisément, pour les années à venir, le périmètre couvert par le projet ENT afin que le soumissionnaire puisse établir une réponse argumentée du dimensionnement de sa solution :

- Nombre d'élèves concernés par le projet.
- Nombre d'établissements concernés par le projet.
- Etc.

Les éléments de volumétrie et les hypothèses d'accès donnés dans ce chapitre peuvent permettre au soumissionnaire de déterminer l'option d'intégration des exigences de disponibilité et de la répartition de charge la plus adaptée pour respecter les temps de réponse exigés pour l'ENT.

À titre d'illustration, les hypothèses suivantes peuvent être considérées :

- Pour 100 élèves, on compte :
 - ▶ 125 responsables d'élève ;
 - ▶ 10 enseignants ;
 - ▶ 5 non enseignants.
- Les autres catégories de personnes représentent une quantité non significative.

Pour 1 élève inscrit dans l'ENT, il y a donc environ $(100 + 125 + 10 + 5) / 100 = 2,4$ personnes.

[EX-2] Intégration dans l'existant

La solution proposée devra s'intégrer, autant que faire se peut, sans interférence avec l'existant technique (supervision, sauvegarde, exploitation...).

Le porteur précisera cet existant technique ou fera référence à sa description réalisée dans le document [1].

[EX-3] Référentiel technique

La solution proposée devra être conforme au référentiel technique en termes de systèmes et de plate-forme utilisés.

Le porteur précisera ce référentiel technique ou fera référence à sa description réalisée dans le document [1].

[EX-4] Performances sur les requêtes des services de sécurité

Le niveau de qualité de service exigé est plus élevé pour le référentiel d'authentification / autorisation. L'objectif est donc de s'assurer que les requêtes sur ce référentiel pourront être traitées dans les temps.

Les premières expérimentations laissent entrevoir les hypothèses présentées ci-après. Le porteur pourra les compléter ou les modifier au vu de son expérience.

Les hypothèses sur la période chargée sont les suivantes :

- Environ 25% de la population d'un établissement d'enseignement est amenée à se connecter à l'ENT. Les catégories de personnes concernées sont les élèves, les enseignants, les non enseignants rattachés administrativement aux services académiques, les non enseignants rattachés administrativement à une collectivité locale, les non enseignants rattachés administrativement à un établissement et les personnels extérieurs.
- Durant une session d'un utilisateur de l'ENT, 6 requêtes sont effectuées en moyenne sur le référentiel d'authentification / autorisation : 1 requête d'authentification et 5 requêtes d'autorisation.

La solution proposée par le soumissionnaire devra maintenir un temps de réponse à chacune des requêtes d'authentification / autorisation inférieur à une (1) seconde.

Le soumissionnaire précisera par ailleurs les impacts techniques potentiels en cas de doublement des hypothèses d'accès, les mêmes exigences en termes de performance étant conservées.

[EX-5] Performances sur les requêtes des services de publication

Pour chaque requête des services de publication, la solution proposée par le soumissionnaire devra maintenir un temps de réponse inférieur à deux (2) secondes.

[EX-6] Disponibilité

La durée cumulée d'indisponibilité de la solution d'annuaire est inférieure à 8 heures par an. Cette durée est déterminée, hors maintenance, 7 jours sur 7 et 24 heures sur 24.

Le nombre maximum d'indisponibilités de la solution d'annuaire est de 3 fois par an.

La durée maximale d'une indisponibilité de la solution d'annuaire est de 4 heures. Cette durée est déterminée, hors maintenance, sur les jours ouvrés de 07h00 à 20h00.

[EX-7] Hébergement

Il est prévu d'héberger l'annuaire ENT sur **A compléter par le porteur : quel site ? quelles responsabilités pour l'exploitant du site ? quels services d'exploitation sur le site ?...**

Certains établissements pourraient cependant souhaiter héberger physiquement les données qui les concernent. Le soumissionnaire précisera quelles adaptations devraient alors être apportées au modèle et à l'architecture afin de prendre en compte ce besoin et quels impacts pourraient en découler. De même, il précisera les moyens d'administration et d'exploitation à mettre en œuvre.

Le porteur pourra supprimer ce paragraphe si la possibilité d'hébergement n'est pas offerte aux établissements.

[EX-8] Exigences communes à tout le socle

La solution d'annuaire devra satisfaire aux exigences définies pour l'ensemble du socle ENT.

Le porteur pourra compléter ce chapitre avec les exigences qu'il jugera nécessaires.

9. ORGANISATION ET PROCESSUS TYPES DE GESTION DE L'ANNUAIRE ENT

L'objectif de cette partie est de donner aux soumissionnaires une vision détaillée des processus pressentis pour l'annuaire ENT. La solution proposée devra être capable de gérer ces processus et d'intégrer de manière simple (paramétrage et interface graphique) de nouveaux processus du même type et leur déclinaison en workflow.

Ce chapitre ne présente qu'un exemple possible d'organisation.

Le porteur devra ainsi préciser les rôles des différents acteurs et les processus de gestion, en s'appuyant le cas échéant sur les propositions ci-dessous.

9.1. ORGANISATION TYPE DE LA GESTION DES DROITS D'ACCES

9.1.1. Acteurs

L'organisation de la gestion des droits d'accès aux données de l'annuaire ENT peut reposer sur les acteurs présentés ci-dessous.

ADMINISTRATEUR CENTRAL

L'administrateur central de l'annuaire ENT a accès en écriture sur les objets de type « profil partagé », « rôle applicatif » et « application » transverses à l'ENT.

Il est ainsi en charge de la création de ces objets et de leur mise à jour.

PROPRIETAIRES ET GESTIONNAIRES LOCAUX

Le chef d'établissement est le propriétaire de l'ensemble des données sur son périmètre de responsabilité. Les populations concernées correspondent à l'ensemble des personnes rattachées administrativement à l'établissement ou exerçant une fonction dans l'établissement.

Ainsi, le chef d'établissement possède un accès en écriture sur les objets de type « personne », « structure », « profil local à l'établissement », « rôle applicatif local à l'établissement », « application locale à l'établissement », et peut notamment inscrire une personne dans un profil.

Il peut déléguer tout ou partie de ses droits sur ces données à des gestionnaires locaux (par exemple, les personnels administratifs).

9.1.2. Définition des droits d'accès

L'article 4 de l'arrêté du 30/11/2006 relatif aux ENT¹ définit les principes de gestion des droits d'accès aux données de l'annuaire ENT. Les recommandations du MENESR pour la déclinaison de ces principes sont présentées à l'Annexe 2.

9.2. PROCESSUS TYPE DE GESTION

9.2.1. Gestion des personnes

INSCRIPTION D'UNE PERSONNE

Plusieurs modes d'inscription d'une personne dans l'annuaire ENT peuvent être envisagés.

Inscription automatique

La création d'une personne dans l'annuaire ENT est réalisée automatiquement depuis les sources d'alimentation. Si une entrée est identifiée comme nouvelle dans la source alors qu'elle est déjà présente dans l'annuaire ENT, une anomalie est déclenchée.

Inscription manuelle par la structure de rattachement

Pour les catégories de personnes qui ne sont pas alimentées automatiquement, la création est réalisée manuellement dans l'annuaire ENT via l'interface de gestion de contenu prévue à cet effet (cf. service [SRV-5]). Cette alimentation manuelle est réalisée par le propriétaire ou par un gestionnaire délégué, en charge de l'établissement de rattachement administratif de la personne à créer.

Inscription individuelle

L'inscription individuelle consiste en une demande engagée par la personne auprès d'un gestionnaire de l'établissement ou du propriétaire, au travers d'un *workflow* où la personne renseigne les informations nécessaires à sa création dans l'annuaire ENT. Une fois ces informations validées par le gestionnaire, la personne est créée dans l'annuaire.

Le porteur adaptera ou complétera éventuellement les modes d'inscription proposés en fonction de ses attentes.

Quel que soit le mode d'inscription, l'activation du compte est réalisée à la première connexion de la personne, sous réserve de son acceptation explicite.

SUPPRESSION D'UNE PERSONNE

Le porteur doit préciser ici les actions à effectuer lorsqu'une personne est supprimée du référentiel source. Ces actions peuvent dépendre des catégories de personnes concernées. Exemples :

- Suppression directe de l'entrée.*
- Suspension de l'entrée et suppression automatique au bout d'une durée déterminée.*
- Conservation de l'entrée pendant quelques mois puis suppression (permet aux utilisateurs de disposer des ressources pendant quelques mois supplémentaires, notamment afin de récupérer leurs données).*

MODIFICATION D'UNE PERSONNE

Les modifications des attributs d'une personne suivent les modes d'inscription envisageables pour la personne, à savoir une modification automatique via l'alimentation depuis des référentiels externes, une modification manuelle sur demande de l'utilisateur et réalisée soit directement par lui-même, soit par le gestionnaire, ou une modification manuelle réalisée directement par le gestionnaire.

9.2.2. Gestion des structures

AJOUT D'UNE STRUCTURE

La création d'une structure est réalisée automatiquement pour toutes les nouvelles entrées des sources d'alimentation autoritaires.

Pour les catégories de structures qui ne sont pas alimentées automatiquement, la création est réalisée manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. service [SRV-5]). Cette alimentation manuelle pourra être réalisée par le propriétaire ou un gestionnaire délégué.

SUPPRESSION D'UNE STRUCTURE

Le porteur doit préciser ici les actions à effectuer lorsqu'une structure est supprimée d'un référentiel source. Ces actions peuvent dépendre des catégories de structures concernées. Exemples :

- *Suppression directe de l'entrée.*
- *Suspension de l'entrée et suppression automatique au bout d'une durée déterminée.*
- *Conservation de l'entrée pendant quelques mois puis suppression (permet aux utilisateurs de cette structure de disposer des ressources pendant quelques mois supplémentaires, notamment afin de récupérer leurs données).*

9.2.3. Gestion des profils

AJOUT D'UN PROFIL

La création des profils est réalisée manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. service [SRV-9]).

Un propriétaire ou un gestionnaire délégué peut uniquement créer des profils locaux sur son périmètre de responsabilité.

L'administrateur central de l'annuaire ENT peut créer des profils partagés, dont la portée sera transverse à tout l'ENT.

Remarque : L'ajout d'un profil partagé n'a de sens que s'il est réellement partagé entre tous les ENT.

SUPPRESSION D'UN PROFIL

La suppression des profils est réalisée manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. service [SRV-9]).

Un propriétaire ou un gestionnaire délégué peut uniquement supprimer des profils locaux à son périmètre de responsabilité.

L'administrateur central de l'annuaire ENT peut supprimer des profils partagés, dont la portée est transverse à tout l'ENT.

Remarque : La suppression d'un profil partagé empêchera d'assurer l'interopérabilité avec les autres ENT. Cette action est donc déconseillée.

PEUPLEMENT / DEPEUPLEMENT MANUEL D'UN PROFIL

Le peuplement des profils est réalisé manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. service [SRV-9]).

Un propriétaire ou un gestionnaire délégué peut uniquement peupler un profil avec des personnes appartenant à son périmètre de responsabilité. Il pourra peupler tout profil partagé et tout profil local à son périmètre de responsabilité.

Le dépeuplement d'un profil suit les mêmes règles que le peuplement.

9.2.4. Gestion des applications et des rôles applicatifs

AJOUT D'UNE APPLICATION OU D'UN RÔLE APPLICATIF

La création d'une application ou d'un rôle applicatif est réalisée manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. services [SRV-10] et [SRV-11]).

Un propriétaire ou un gestionnaire délégué peut uniquement créer des applications et des rôles applicatifs locaux sur son périmètre de responsabilité.

L'administrateur central de l'annuaire ENT peut créer des applications et des rôles applicatifs transverses à tout l'ENT.

SUPPRESSION D'UNE APPLICATION OU D'UN RÔLE APPLICATIF

La suppression d'une application ou d'un rôle applicatif est réalisée manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. services [SRV-10] et [SRV-11]).

Un propriétaire ou un gestionnaire délégué peut uniquement supprimer des applications et des rôles applicatifs locaux à son périmètre de responsabilité.

L'administrateur central de l'annuaire ENT peut supprimer des applications ou des rôles applicatifs transverses à tout l'ENT.

Remarque : La suppression d'une application entraîne la suppression de tous les rôles applicatifs associés à cette application.

PEUPLEMENT / DEPEUPLEMENT MANUEL D'UN ROLE APPLICATIF

Le peuplement d'un rôle applicatif est réalisé manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. service [SRV-10]).

Un propriétaire ou un gestionnaire délégué peut uniquement peupler un rôle applicatif avec des personnes ou des profils appartenant à son périmètre de responsabilité. Il pourra peupler tout rôle applicatif associé à une application transverse ou locale à son périmètre de responsabilité.

Le dépeuplement d'un rôle applicatif suit les mêmes règles que le peuplement.