Annuaires pour l'enseignement supérieur et la recherche - Nouveautés *SupAnn*

Aï-Eng Bompoil
RENATER
23-25, rue Daviel
75013 Paris

Benoît Branciard
Direction du système d'information et des usages numériques
Centre Pierre Mendès France
90 rue de Tolbiac
75634 Paris Cedex 13

Pierre-Olivier Terrisse
Direction des Systèmes d'Information et du Numérique
2 rue de la Houssinière
BP 92208
44322 Nantes cedex

Sylvain Brachotte
Direction du Numérique Université de Lorraine
Sous-direction Infrastructures et Services
18-32 Rue Lionnois
54000 Nancy Cedex

Résumé

La mise en œuvre des recommandations SupAnn *(Annuaires pour l'enseignement supérieur) au sein des différentes structures d'enseignement supérieur et de recherche est aujourd'hui incontournable.*

L'offre toujours croissante de services et applications numériques a rendu nécessaire la mise en place d'un cadre de cohérence pour l'exploitation et l'échange des données de type annuaire, tant via les mécanismes de fédération d'identités que pour les usages locaux.

Les recommandations SupAnn *ambitionnent de définir un cadre technique et un vocabulaire commun répondant à ces besoins.*

Depuis la publication de la version 1 de SupAnn *en 2003 et ses mises à jour de 2008 et 2009, les évolutions des services numériques dans les établissements d'enseignement supérieur et de recherche engendrent de nouveaux besoins de structuration, d''échange et de maîtrise des données. La généralisation des référentiels, l'interconnexion à* FranceConnect*, ainsi que la mutualisation d'un nombre croissant d'applications nécessitent de faire évoluer le dialecte* SupAnn.

A cet effet, RENATER a relancé en octobre 2016 un groupe de travail réunissant des représentants d'établissements de l' enseignement supérieur et de la recherche.

Ses travaux ont mené à la publication en septembre 2018 d'une nouvelle version de SupAnn*, enrichissant la précédente sur trois axes :*

- *interopérabilité ;*
- *représentation de nouvelles informations ;*
- *rédactionnel et formalisme .*

Le poster proposé au JRES 2019 *offre une présentation de* SupAnn *et ses usages, de la version courante, des travaux en cours et à venir. Il présente les activités du groupe de travail.*

Cet échange privilégié permettra de découvrir SupAnn*, de s'y intéresser, de le commenter, et peut-être de s'investir dans ses prochaines évolutions.*

Mots-clefs

Annuaire, *LDAP*, *SAML*, *RENATER*, *Fédération Éducation-Recherche*, *FranceConnect*, *Mifare*, *RFC*, *SupAnn*, gestion d'identités, référentiels

1 Introduction

Nombreux sont les établissements qui font appel à *SupAnn* pour leurs annuaires ou leurs flux de données et se conforment à ses recommandations. Celles-ci font désormais partie des fondations des systèmes d'information de l'enseignement supérieur et de la recherche.

Cet article se propose de présenter *SupAnn*, le groupe de travail et les dernières nouveautés. Quatre parties le composent. La première partie rappelle la définition de *SupAnn*, ses objectifs, son champ d'application et son format. La seconde partie présente le groupe de travail et les évolutions apportées par la version 2018. Seront ensuite abordés les aspects pratiques: comment utiliser *SupAnn*, un scénario-type de déploiement, quelques exemples d'usage parmi lesquels la gestion d'un organigramme web, de listes de diffusion d'étudiants etc. Enfin, nous terminerons par les perspectives d'évolutions.

2 Qu'est-ce que *SupAnn*?

SupAnn est l'acronyme de « Annuaires pour le Supérieur ».

Il est né du besoin des établissements de l'enseignement supérieur et de la recherche de disposer d'un cadre commun pour la mise en œuvre de leurs annuaires respectifs, et s'est étendu au fil des évolutions technologies et organisationnelles.

Ci-dessous, les principaux objectifs qui ont motivé, et qui motivent toujours, le groupe de travail pour l'élaboration de *SupAnn* :

- favoriser la portabilité des logiciels utilisés en harmonisant les schémas d'annuaires ;
- homogénéiser le contenu des annuaires pour faciliter le portage des logiciel et progiciels interagissant avec eux ;
- converger vers des compétences internes similaires en matière d'annuaire au sein des établissements de l'enseignement supérieur et établir un langage commun entre les différents acteurs ;
- sensibiliser les établissements à la nécessité de mettre en œuvre un référentiel central afin de rationaliser et structurer les informations de référence pour leur dispositif d'authentification et de contrôle d'accès ;
- compléter les normes internationales existantes (*eduPerson*, *SCHAC*, *etc.*).

Depuis ses premières versions, *SupAnn* a vu son champ d'application s'élargir progressivement. À l'origine construit sur la base du protocole *LDAP*, qui reste encore son support privilégié, il a ensuite été étendu à *SAML*, qui est exploité par la fédération d'identités enseignement supérieur et recherche, et s'ouvre désormais à *FranceConnect*.

Les évolutions prennent désormais en compte les usages hors protocole *LDAP*, en considérant *SupAnn* comme un vocabulaire générique d'échange de données pouvant s'intégrer à n'importe quel mécanisme de fédération d'identités ou format structuré tel que *XML* ou *JSON*.

SupAnn est mis à disposition en ligne sous forme de *recommandations* sur le portail de *RENATER* [1].

Celles-ci définissent les notions propres à *SupAnn :* une arborescence *LDAP* normalisée, des classes d'objets, des types d'attributs et des formats de données, ainsi que le détail de leur usage. Elles introduisent également les éléments provenant d'autres standards (*RFC*, *eduPerson*, *etc.*) dont l'emploi est recommandé.

Les lecteurs trouveront également un ensemble de bonnes pratiques, des recommandations de gestion de la confidentialité des données et les références aux nomenclatures utilisées, qu'elles soient définies dans le cadre de *SupAnn* ou qu'elles proviennent de sources externes.

3 Le groupe de travail *SupAnn*

Le premier groupe de travail *SupAnn* a été constitué en 2002, copiloté par la Direction de la technologie, l'*AMUE* (Agence de Mutualisation des Universités et Établissements) et animé par le *CRU* (Comité Réseau des Universités), dans le cadre du schéma directeur des espaces numériques de travail (*SDET*). Il publie en 2003 les recommandations *SupAnn* v1. Cette première version propose une représentation élémentaire des *personnes* et des *groupes*.

En 2005, à la suite d'une enquête sur les usages, le travail reprend avec la mobilisation d'un groupe fonctionnel et d'un groupe technique. Ce dernier, animé par le *CRU*, fait appel aux contributions de la communauté des utilisateurs et aboutit à la publication des versions 2008 et 2009 des recommandations. Celles-ci complètent la v1 avec la représentation des *structures*, l'introduction du format *composite* répondant à la

problématique du cumul de profils, celle des *étiquettes* facilitant l'exploitation de nomenclatures multiples, la modélisation du profil *étudiant*, des *rôles* et *affectations* des personnels, ainsi que quelques corrections et de nouveaux attributs.

En 2016, *RENATER*, qui a repris les activités du *CRU*, réitère le processus d'appel à la communauté pour former un nouveau groupe de travail, en charge de répondre aux besoins laissés en suspens. Représentant 26 établissements d'enseignement et recherche (*RENATER*, universités, écoles d'ingénieurs et organismes de recherche), ce groupe est majoritairement constitué de responsables techniques et fonctionnels de la fédération d'identité, mais aussi des systèmes d'information et des annuaires d'établissements. Il œuvre pour faire évoluer les recommandations, dont la publication de la version 2018 est le premier résultat. Celle-ci propose plusieurs nouveautés, décrites ci-dessous, ainsi qu'une amélioration du formalisme rédactionnel et des enrichissements, comme la préconisation d'un niveau de visibilité pour chaque attribut, selon sa confidentialité.

L'animation des réunions et la coordination des travaux de ce nouveau groupe sont pilotés par *RENATER* avec la collaboration régulière des universités de Paris 1 Panthéon-Sorbonne et de Nantes.

Les réunions plénières sont organisées tous les quinze jours sous forme de visioconférences, et réunissent une dizaine de membres en moyenne.

Ceux-ci analysent les besoins issus de leur propre expérience de terrain ainsi que ceux remontés par la communauté, les priorisent, en étudient les modélisations possibles, conçoivent des implémentations techniques y répondant et enfin rédigent le résultat en vue de leur inclusion dans les recommandations.

Le groupe communique par ailleurs régulièrement lors des manifestations de la communauté enseignement supérieur et recherche (*JRES*, Journées fédération, etc.), afin de promouvoir *SupAnn*, présenter ses nouveautés et l'avancement des travaux en cours.

La composition de ce groupe n'est pas figée : des membres peuvent s'en retirer, parfois par manque de disponibilité ou du fait d'un éloignement de leur activité professionnelle avec la thématique *SupAnn*. À l'inverse, si vous souhaitez nous rejoindre afin d'apporter à l'équipe votre expérience, vos contributions et vos idées, toutes les bonnes volontés sont bienvenues. Après une première entrevue validant vos motivations et vos attentes, votre adhésion sera validée par l'équipe de coordination, actuellement constituée de 4 personnes.

Vous trouverez toutes les informations nécessaires sur la page de contact du groupe de travail [2].

4 Les nouveautés SupAnn 2018

4.1 Intégration avec *FranceConnect* et gestion de l'état civil

Cette évolution répond à un triple besoin :

- stocker dans l'annuaire l'*identité pivot* d'une personne (nom et prénoms d'état-civil, date et lieu de naissance, etc.), transmise par un fournisseur d'identités *FranceConnect* après validation par le *RNIPP* (répertoire national d'identification des personnes physiques) *;*
- conserver dans l'annuaire le lien avec une identité *FranceConnect*, indépendamment de ses attributs d'état-civil ;
- disposer, même hors contexte *FranceConnect*, d'attributs permettant une gestion de l'état-civil plus étendue que ce qui était disponible jusqu'alors.

À cet effet, plusieurs nouveaux éléments ont été définis :

- un jeu d'attributs pour représenter l'état-civil, dans le format exploité par *FranceConnect :* le nom de naissance, le code INSEE de la ville et du pays de naissance, les prénoms dans l'ordre de l'état-civil, enfin la date de naissance et le genre, au format *OpenID Connect* ;
- un attribut technique *supannFCSub* établissant le lien avec l'identité *FranceConnect* via le *SUB* (SUB*ject OpenID Connect*) ;
- une classe *supannFCPerson* regroupant l'ensemble des attributs ci-dessus.

Ces nouveaux attributs complètent ceux existants pour représenter l'état civil et facilitent l'interfaçage des établissements avec *FranceConnect*, par exemple dans un scénario de délégation de l'authentification, d'approvisionnement automatique des comptes ou de réconciliation d'identités à partir de l'identité pivot.

4.2 État et cycle de vie des ressources

Cette nouveauté 2018 permet de représenter les différents états et échéances du cycle de vie des ressources liées à une personne, de la création à la suppression en passant par différentes restrictions qui évoluent au fil du temps.

Une ressource peut être aussi bien le compte de l'utilisateur que l'accès à sa boite de messagerie électronique ou d'autres services selon le besoin des établissements.

L'état peut prendre trois valeurs : Actif, Inactif ou Suspendu. Un sous-état optionnel permet de préciser le motif pour lequel l'état a été positionné, en fonction des traitements souhaités. Par exemple : *SupannVerrouAdministratif*.

Le diagramme ci-dessous présente un exemple-type de cycle séquentiel des états et sous-états d'une ressource :

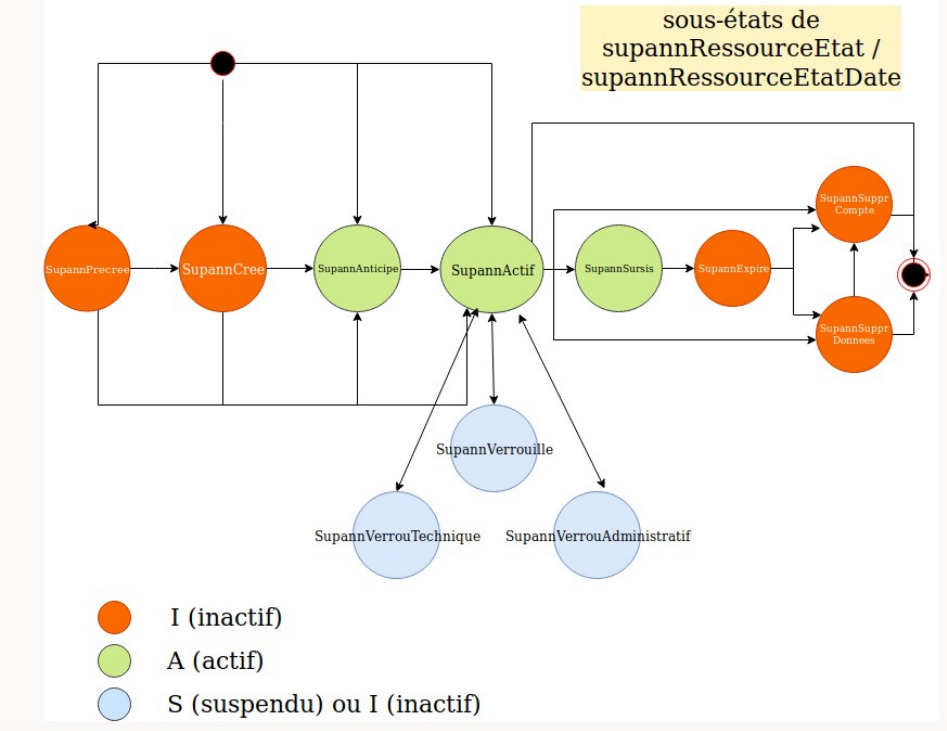

Figure 1 - cycle de vie d'une ressource

Deux nouveaux attributs étiquetés sont proposés pour représenter cette information. Le premier, *supannRessourceEtat*, représente l'état actuel de la ressource en fonction de son cycle de vie. Le second, *supannRessourceEtatDate*, le complète avec des dates de début et de fin.

Exemple de valuation pour un compte utilisateur actuellement actif, avec une date de début au 01/09/2019 et une date de fin au 01/09/2020 :

```
supannRessourceEtat: {COMPTE}A:SupannActif
supannRessourceEtatDate: {COMPTE}A:SupannActif:20190901:20200901
```

4.3 Gestion des cartes multi-services

L'objet de cette évolution est de représenter la carte multi-service, appelée également carte d'accès. Il s'agit le plus souvent d'une carte à puce sans contact normalisée *ISO 14443*, telle que la technologie *MIFARE* ou ses déclinaisons (*DESfire…*), permettant d'identifier son porteur au moyen d'identifiants uniques, notamment l'identifiant physique globalement unique (*UID*), mais aussi des codes applicatifs propres à l'établissement émetteur.

La disponibilité de ces informations dans *SupAnn* permet à des applications de les consommer d'une manière standardisée, soit au sein de l'établissement, le plus souvent

par le protocole *LDAP*, soit au travers de la fédération d'identités, via le protocole *SAML*, dans de cadre d'une coopération ou d'un regroupement d'établissements.

Cette diversité des technologies et des modes de consommation ont amené à décliner l'encodage des données sous plusieurs formes redondantes : attributs avec options, étiquetés, en décimal ou hexadécimal, avec les octets du plus fort au moins fort ou l'inverse, etc.

Nous y avons ajouté des indications sur la validité de la carte et ses échéances, son type et sa source, ainsi que deux attributs composites (*supannCMSAffectation* et *supannCMSAppAffectation*) permettant de gérer l'attribution de plusieurs cartes à une même personne.

Toutes ces données sont regroupées dans la classe auxiliaire *supannCMS*, apparue dans la première version de *SupAnn* 2018 [3].

Quelques cas d'usage :

- partage des codes de cartes multi-services entre établissements associés afin d'autoriser les étudiants à imprimer des documents sur un copieur à carte quel que soit le site géographique, en utilisant la fédération d'identités ;
- accès à la carte multi-service pour une application de bibliothèque universitaire via le protocole *LDAP ;*
- contrôle d'accès physique à des bâtiments, des salles… à partir des codes applicatifs stockés sur une zone privée de la carte, et de l'attribut *supannCMSAppId*.

Exemple d'entrée d'annuaire implémentant la classe *supannCMS :*

```
dn: uid=jdupont,ou=people,dc=univ-exemple,dc=fr
objectClass: supannPerson
objectClass: supannCMS
supannCMSId;x-mifare-xlsb: DEADBEEF000000
supannCMSId;x-mifare-xmsb: 000000EFBEADDE
supannCMSId;x-mifare-dlsb: 62678480394911744
supannCMSId;x-mifare-dmsb: 4022250974
supannCMSIdEtiquette: {MIFARE:XLSB}DEADBEEF000000
supannCMSIdEtiquette: {MIFARE:XMSB}000000EFBEADDE
supannCMSIdEtiquette: {MIFARE:DLSB}62678480394911744
supannCMSIdEtiquette: {MIFARE:DMSB}4022250974
supannCMSType: etudiant
supannCMSSource: unicampus@univ-exemple.fr
supannCMSDateFin: 20210201020000Z
supannCMSAffectation: [type=etudiant][format=MIFARE:XLSB]
    [id=DEADBEEF000000][valide=vrai][source=unicampus@univ-exemple.fr]
    [datefin=20210201020000Z]
```

4.4 Profil des *personnes ressources* et catégories de population

SupAnn 2008 avait défini d'une manière détaillée la représentation du *profil étudiant*, au moyen de l'attribut composite *supannEtuInscription* et des attributs élémentaires correspondants, alimentés depuis la base de gestion de la scolarité. Ce choix permettait une gestion efficace des *inscriptions multiples*, à savoir lorsqu'un étudiant, ou plus largement un apprenant, était inscrit simultanément à plusieurs formations.

Cependant, rien d'équivalent n'était défini pour les *personnes ressources*, c'est-à-dire celles contribuant professionnellement à l'activité de l'établissement, comme les enseignants, les personnels *BIATSS* ou les chercheurs. L'attribut *eduPersonAffiliation*, largement utilisé pour sélectionner les grandes catégories de population, ne permet par exemple pas de différencier un enseignant-chercheur (valeurs : *faculty, researcher, teacher, member, employee*) d'un chercheur hébergé (*faculty, researcher, member*) cumulant son activité avec des vacations d'enseignement (*teacher, member, employee*). De plus, si ces deux activités sont exercées dans des structures différentes, rien ne permettait de lier chaque structure avec l'activité concernée.

SupAnn 2018, dans sa révision 2, comble cette lacune avec l'introduction d'un attribut composite *supannEmpProfil*, qui corrèle les valeurs des attributs existants, contribuant à définir un profil professionnel : établissement, affiliation, corps, activité, entité d'affectation et son type. Ces champs sont complétés par une date de fin du profil, permettant par exemple de gérer un cycle de purge de données ou d'en déduire une échéance de fin de droits.

Suivant la même logique, un attribut *supannExtProfil* a été créé pour représenter le profil d'une *personne extérieure* (invité, visiteur, intervenant, prestataire, etc.).

Par analogie, une date de fin optionnelle a été ajoutée à *supannEtuInscription*, permettant de gérer efficacement l'hétérogénéité des dates de fin de formations.

Parallèlement à cette démarche, il était apparu nécessaire de mieux pouvoir définir chaque catégorie de population par un code unique, dans le prolongement du classement des valeurs du *eduPersonAffiliation* effectué dans *SupAnn* 2008 [4]. Une nouvelle nomenclature de *catégories de population* a donc été définie, après collecte minutieuse de multiples retours d'expérience. Un attribut multivalué *supannCodeProfil* a été conçu pour recueillir ces valeurs, et un champ correspondant a été inclus dans les attributs composites *supannEmpProfil, supannExtProfil* et *supannEtuInscription*, afin de faire de la catégorie de population l'un des éléments clés de chaque profil. Une notion de *pondération* des catégories de population a également été introduite, permettant d'identifier la catégorie principale en cas de profils multiples.

La figure ci-dessous montre, sous forme d'un extrait *LDIF*, comment pourraient être représentés les profils professionnels du chercheur hébergé, par ailleurs vacataire d'enseignement, évoqué précédemment. Les attributs élémentaires cumulent les valeurs des deux profils (ici : établissements *Univ. Paris 1* et *CNRS*, affiliations chercheur et enseignant, affectation à une structure de recherche et une composante, etc.), tandis que

l'attribut *supannEmpProfil* présente les valeurs séparées en deux profils distincts, l'un borné au 31/08/2020, et l'autre sans limite de durée.

```
dn: uid=jdupont,ou=people,dc=univ-paris1,dc=fr
supannEtablissement: {UAI}0753639Y
supannEtablissement: {UAI}0751717J
eduPersonAffiliation: faculty
eduPersonAffiliation: researcher
eduPersonAffiliation: teacher
eduPersonAffiliation: member
eduPersonAffiliation: employee
eduPersonPrimaryAffiliation: faculty
supannTypeEntiteAffectation: {SUPANN}S203
supannTypeEntiteAffectation: {SUPANN}S200
supannEntiteAffectationPrincipale: UR71
supannEntiteAffectation: UR71
supannEntiteAffectation: UF22
supannActivite: {CNU}0500
supannEmpCorps: {NCORPS}223
supannEmpCorps: {NCORPS}758
supannCodeProfil: {SUPANN}RHTCO
supannCodeProfil: {SUPANN}RGIE
supannEmpDateFin: 20200831220000Z
supannEmpProfil:
    [codeprofil={SUPANN}RHTCO][etab={UAI}0753639Y][affil=faculty]
    [corps={NCORPS}223][typeaffect={SUPANN}S203][affect=UR71]
supannEmpProfil:
    [codeprofil={SUPANN}RGIE][etab={UAI}0751717J][affil=teacher]
    [corps={NCORPS}758][typeaffect={SUPANN}S200][affect=UF22]
    [activite={CNU}0500][datefin=20200831220000Z]
```

Remarque : la formalisation des catégories de population n'est pas encore figée à la rédaction de ce document, quelques différences peuvent apparaître par rapport à la révision courante de SupAnn 2018, qui fait foi.

4.5 Données personnelles et consentement

Par nature, un annuaire peut contenir des informations personnelles pour la diffusion desquelles le règlement *RGPD* nous impose de recueillir le consentement préalable de l'intéressé. Il est utile de représenter cet accord dans le compte *SupAnn* de chaque personne représentée, afin de s'assurer du respect de ces choix personnels.

À partir du moment où la propagation des informations personnelles est contrôlée, il devient envisageable de représenter des données privées des utilisateurs afin de faciliter la communication en périphérie de l'établissement : numéros de téléphones personnels, adresses postales et de messagerie, etc. dans de nouveaux attributs étiquetés permettant une souplesse dans la présentation que n'avaient pas les anciens attributs. Quelques exemples :

```
supannTelephonePrive: {PERSO}+33 6…
supannTelephonePrive: {SMS}+33 6…
supannMailPrive: {SECOURS}mail@domaine
supannAdressePostalePrivee: {PERSO}10 rue Machin$75025
   Paris$France
```

L'attribut étiqueté *supannConsentement* permet d'indiquer, d'une manière aussi détaillée que nécessaire, les informations dont la personne a consenti la diffusion (par attribut, par classe ou par objet appartenant à une application), et pour quels usages (public, interne à l'établissement ou pour des applications explicitement définies).

Son format général est :

```
{QUELLE INFORMATION}QUEL USAGE
```

- *QUELLE INFORMATION* : de quelle information l'utilisateur consent la diffusion ;
- *QUEL USAGE* : pour quel usage ce consentement est donné.

Dans l'exemple suivant, la personne dont l'entrée est représentée consent à ce que :

- son adresse de messagerie privée de secours soit utilisée d'une manière interne à l'établissement (en cas de mot de passe perdu par exemple), mais pas diffusée à l'extérieur ;
- l'image *JPEG* contenant sa photo numérisée soit diffusée sans restrictions ;
- l'application de contrôle d'accès « CASTEL » accède à tous les attributs de la classe *supannCMS* ;
- l'application « *PSTAGES* » consulte l'objet de type « *CV* » géré par l'application nommée « *RESEAUPRO* ».

```
supannConsentement: {SUPANNMAILPRIVE:SECOURS}INTERNE
supannConsentement: {JPEGPHOTO}PUBLIC
supannConsentement: {CLASSE:SUPANNCMS}APPLI:CASTEL
supannConsentement: {APPLI:RESEAUPRO:CV}APPLI:PSTAGES
```

NB : l'attribut supannConsentement n'est pas encore figé dans la recommandation SupAnn.

5 Mode d'emploi de *SupAnn*

5.1 Comment utiliser *SupAnn* ?

Ces questions sont régulièrement posées lors des rencontres avec les responsables d'annuaires, quelques cas sont ici décrits pour illustrer certains usages de *SupAnn*.

Je dois mettre telle information dans mon annuaire, comment procéder ?

Consultez en premier lieu les recommandations *SupAnn*, notamment la liste des attributs, afin d'identifier les nomenclatures correspondant à votre besoin. À défaut, vous pouvez également consulter les normes internationales, notamment celles concernant les schémas *EduPerson* [5] et *SCHAC* [6]. Notez que les besoins les plus techniques (gestion de l'authentification, routage de messagerie, identifiants de sécurité…) ne sont pas intégralement couverts par *SupAnn :* référez-vous à la documentation de votre solution logicielle (*Active Directory*, *POSIX*, *Samba*, *Postfix, etc.*) pour certains schémas spécifiques. En tout dernier recours, vous pouvez créer des attributs personnalisés.

L'annuaire de mon établissement doit être compatible *SupAnn*. Faut-il vraiment renseigner les 89 attributs listés dans les recommandations ?

Il n'est pas utile d'implémenter l'ensemble des attributs de la recommandation. Focalisez-vous seulement sur ceux qui sont nécessaires à vos projets d'intégration.

Dans ma *COMUE* la mise en place d'une application de *SIGB* partagée est envisagée.

SupAnn permet la propagation des profils des utilisateurs (étudiants, enseignants, etc.) des établissements membres vers ce *SIGB* sous un format standardisé, au travers de la fédération d'identités ou de connexions aux annuaires *LDAP*.

Un prestataire auquel nous confions le développement d'une application externalisée a besoin d'identifier les disciplines des étudiants qui s'y connectent.

Lui fournir l'attribut *supannEtuSecteurDisciplinaire* par l'intermédiaire de la fédération d'identités.

De même, l'essentiel des informations ayant trait aux parcours universitaires des étudiants se trouvent représentées dans *SupAnn*, au chapitre « profil apprenant ». Par contre, des données plus spécifiques ou sujettes à changements rapides n'ont pas

vocation à figurer dans un annuaire : elles ne sont pas modélisées par *SupAnn*. Par exemple : les notes aux examens, les emplois du temps…

Je dois mettre en place *SupAnn*. Que dois-je faire ?

La mise œuvre *ex nihilo* d'un annuaire SupAnn se réalise typiquement en déroulant les étapes suivantes :

- inventorier les applications consommatrices de données, leurs besoins et leurs modes d'alimentation : les services intégrés à la fédération d'identités, les applications disposant de connecteurs au protocole *LDAP*, celles pouvant être alimentées par extractions, etc. ;
- répertorier les sources de données disponibles (applications de *GRH*, scolarité, etc), les informations qu'elles peuvent fournir, leur degré de qualité et définir les règles d'arbitrage entre elles ;
- inventorier les briques logicielles d'alimentation (connecteurs) à mettre en œuvre ou adapter, en fonction de l'existant, des ressources disponibles, du budget ou des délais : référentiel, outils d'*ETL*, développements à réaliser, etc. ;
- définir le jeu d'attributs découlant des besoins et des capacités des sources, identifier les transformations nécessaires (transcodages, reformatages, etc.) ;
- configurer les connecteurs pour ce jeu de données, avec les transformations éventuelles ;
- définir les règles de diffusion et d'accès à l'annuaire (via des *Access Lists LDAP*, des règles de pare-feu, etc.) en fonction des attributs retenus et des niveaux de visibilité recommandés ;
- déployer un annuaire *LDAP* de production, y appliquer le schéma *SupAnn* ou l'ajouter à un annuaire existant ;
- si besoin : dans le cadre de la fédération d'identités, mettre en place un fournisseur d'identités *Shibboleth* connecté à cet annuaire.

En pratique, les établissements partent le plus souvent d'un annuaire existant qui doit être modifié pour appliquer les recommandations *SupAnn*. Ils procèdent par une migration en douceur où l'ancienne implémentation est progressivement abandonnée. Des instances *LDAP* de pré-production ou de maquettage, dont on s'assure du confinement rigoureux, sont par ailleurs souvent indispensables pour mener à bien ce déploiement avant mise en production.

5.2 Pour quels usages ? Dans le détail… des recommandations à la carte

Quelques exemples de ce qu'il est possible de représenter dans un annuaire *SupAnn*.

5.2.1 Représenter l'organigramme de l'établissement

Les structures de l'établissement sont représentées dans la branche *ou=Structures*, située elle-même sous la racine de l'arborescence. Il est possible de représenter aussi bien les structures organisationnelles (UFR, unités de recherche, directions, services, etc.) que des entités plus abstraites ou transversales : instances électives, projets, cellules de coordination, etc.

La première entrée à implémenter concerne l'établissement lui-même.

Chacune des entités est identifiée par un attribut *supannCodeEntite* qui l'identifie d'une manière unique par un code propre au système d'information de l'établissement. On indique également son libellé court dans l'attribut *ou (organizationalUnit)*, et un libellé plus explicite dans l'attribut *description*. Les liens hiérarchiques entre les entités sont représentés par l'attribut *supannCodeEntiteParent* qui référence l'entrée de niveau supérieur, tandis qu'une classification par type est possible au moyen de l'attribut *supannTypeEntite*. Par ailleurs, les personnes affectées dans chaque structure ou y exerçant des fonctions peuvent être identifiées par recherche sur leurs attributs *supannEntiteAffectation*, *supannEntiteAffectationPrincipale* ou *supannRoleEntite*.

Une application web locale de type « annuaire » peut exploiter l'ensemble de ces informations, sous forme de requêtes *LDAP*, afin de publier un organigramme dynamique de l'établissement, basé sur les données en temps réel issues de l'annuaire.

5.2.2 Attribuer des droits à des personnes en fonction de leurs profils

De nombreux droits d'accès peuvent être déduits de combinaisons d'attributs de personnes définissant leurs profils, statuts ou rôles. En premier lieu l'attribut *eduPersonAffiliation* ou plus finement le nouvel attribut *supannCodeProfil*, ou bien encore les attributs définissant les fonctions : *supannRoleGenerique* et *supannRoleEntite*. Des applications ont la possibilité d'exploiter ces attributs afin d'accorder des permissions, au moyen de filtres *LDAP* ou par comparaison des valeurs renvoyées par le fournisseur d'identités dans le cadre de la fédération.

5.2.3 Générer des listes de diffusion d'étudiants par formation

L'attribut *supannEtuInscription* peut entrer dans la constitution de filtres *LDAP* alimentant des listes de diffusion, avec de nombreuses possibilités de sélection : par composante, par niveau (licence, master, doctorat, etc.), par *étape*, par discipline, par année universitaire…

L'exemple ci-dessous illustre la configuration d'une liste de diffusion par *étape* et année universitaire dans le gestionnaire de listes *Sympa :*

```
include_ldap_query
name LDAP 01A1-2019
attrs mail
filter (&(supannEtuInscription=*[anneeinsc=2019]*
    [etape={UAI:0751717J}01A1]*)(supannRessourceEtat={MAIL}A*))
host ldap1.univ-exemple.fr,ldap2.univ-exemple.fr
user cn=sympa,ou=admin,dc=univ-exemple,dc=fr
passwd XXXXX
suffix ou=people,dc=univ-exemple,dc=fr
timeout 180
scope one
select first
```

Ici, la liste abonne les étudiants dont la boite aux lettres électronique est active et qui sont inscrits en 2019-2020 dans la formation 01A1 de l'établissement dont le code UAI est 0751717J.

On remarquera que le bon fonctionnement du filtre sur un attribut composite, ici *supannEtuInscription*, est basé sur le respect de l'ordre d'apparition des éléments entre crochets, à l'intérieur de la valeur de cet attribut.

5.2.4 Je ne trouve pas de quoi répondre à mon besoin !

Si le besoin est spécifique à l'établissement, il est toujours possible d'ajouter des attributs locaux aux entrées d'un annuaire *SupAnn*. Mais s'il s'agit d'informations pouvant être partagées, n'hésitez pas à soumettre vos idées au groupe de travail afin d'étudier une éventuelle future intégration à *SupAnn*. La demande fera l'objet d'une analyse approfondie le cas échéant. Pour cela, vous trouverez les informations nécessaires sur la page de contact du groupe de travail [2].

5.3 Conclusion

SupAnn est un travail continu visant à intégrer les nouvelles exigences du système d'informations. La révision 2 de sa version 2018 sera publiée à la fin de l'année 2019.

Les besoins suivants ont d'ores et déjà été identifiés, et constituent des perspectives potentielles d'évolutions :

- la modélisation des locaux : définir un modèle de données simplifié, issu par exemple de celui utilisé par les outils de gestion du patrimoine (ex : *BIM*, *Building Information Modeling*), pour que ces informations (liste de sites, bâtiments, étages, bureaux…) puissent être associées à des personnes, soient affichables dans un annuaire web et soient accessibles à des solutions de suivi de tickets (ex : *GLPI*, *Request Tracker*) ou des applications de *GMAO* potentiellement externalisées chez un prestataire et intégrées à la fédération d'identités ;
- la modélisation des formations : faire en sorte que les codes d'*étapes*, de diplômes ou d'éléments pédagogiques référencés dans le *supannEtuInscription* puissent correspondre à des entrées d'annuaire contenant leurs libellés, descriptions, hiérarchie, etc. Ces entrées pourraient être utilisées pour affichage dans un annuaire web (présenter le libellé en français d'une étape à laquelle est inscrit un étudiant), ou exploitées par des applications de type cours en ligne (ex. : *Moodle*) pour la constitution de hiérarchies de groupes ;
- d'une façon plus générale, introduire la notion de tables de nomenclatures, faisant correspondre à tout code utilisé dans un attribut donné une entrée contenant les libellés et descriptions correspondantes, ainsi qu'un ensemble d'éléments descriptifs génériques (parenté, coordonnées…).

Le futur dépendra des priorités arbitrées par le groupe de travail, de son analyse et des retours des utilisateurs, en gardant à l'esprit les principes fondamentaux de *SupAnn* : cohérence, rigueur, transversalité et si possible… pérennité !

Annexe

Sigles et acronymes :

- LDAP : Lightweight Directory Access Protocol
- LDIF : LDAP Data Interchange Format
- SAML : Security Assertion Markup Language
- CRU : Comité Réseau des Universités
- AMUE : Agence de mutualisation des universités et des établissements
- ETL : Export, Transform, Load (outil d'extraction et de transformation de données)
- GMAO : Gestion de Maintenance Assistée par Ordinateur
- GRH : Gestion des Ressources Humaines
- RGPD : Règlement Général sur la Protection des Données
- SCHAC : SCHema for Academia
- SIGB : Système Intégré de Gestion de Bibliothèque

Bibliographie

[1] Recommandations SupAnn, RENATER : https://services.renater.fr/documentation/supann/

[2] Adresse de contact du groupe SupAnn : https://services.renater.fr/documentation/supann/supann2018/presentation

[3] La carte multi-service dans les recommandations SupAnn : https://services.renater.fr/documentation/supann/supann2018/recommandations2018/personnes/carte-ms

[4] Les différentes catégories de personnes à l'université, SupAnn 2008 : https://services.renater.fr/documentation/supann/evolepa

[5] eduPerson : https://wiki.refeds.org/display/STAN/eduPerson

[6] SCHAC : https://wiki.refeds.org/display/STAN/SCHAC