Le contexte, les objectifs

La renaissance du groupe de travail Supann

- Né en 2003, Supann normalise le contenu des annuaires LDAP dans le monde de l'enseignement supérieur / recherche français.
- Après avoir publié Supann 2009, le comité Supann est entré dans un long sommeil... pour se réveiller en 2016 ; nous avons reformé le groupe.
- Depuis ses premières versions, SupAnn a vu son champ d'application s'élargir progressivement. Il était à l'origine uniquement focalisé sur LDAP ; puis sont apparus de nouveaux usages, comme les services de la fédération d'identités, et désormais France Connect.
- Des points d'implémentation demandaient à être détaillés.
- Première publication de la nouvelle mouture de Supann en 2018, mises à jours en 2019.

Les objectifs de Supann

- Proposer aux établissements un cadre de cohérence.
- Favoriser la portabilité des logiciels.
- Une meilleure homogénéité des contenus.
- Converger vers de compétences internes similaires, parler le même vocabulaire.
- Sensibiliser les établissements à la nécessité de mettre en œuvre un référentiel central.

Les questions qui reviennent souvent

Je dois mettre en place Supann : que dois-je faire ?

- Supann est plus un couteau suisse qu'un règlement à suivre à la lettre.
- Il évite d'implémenter des classes /attributs propriétaires.
- Il propose une représentation des informations liées aux comptes.
- Supann propose des bonnes pratiques mais n'impose aucune méthode d'alimentation de d'annuaire.
- Un schéma pour OpenLDAP est proposé.

Pourquoi autant d'attributs ?

- Supann présente aujourd'hui 89 attributs, presque tous facultatifs.
- Beaucoup ~~de redondance~~ de dénormalisations !

  - pas de formes normales : ce n'est pas une table SQL ;
  - il n'est donc pas recommandé que SupAnn soit le référentiel source des utilisateurs ;
  - différents usages (LDAP, fédération d'identités) entraînent différentes représentations.

Exemple : supannCMSId, supannCMSIdEtiquette

Nouveautés

Une nouveauté de 2018 : la CMS

- La Carte Multi-Services (CMS) au standard Mifare / DESFire s'est imposée dans presque tous les établissements.
- De nouveaux usages sont possibles en lien avec la fédération d'identités afin d'échanger les informations qui se trouvent sur ces cartes entre établissements.
- Pour cela, il faut normaliser leur représentation.

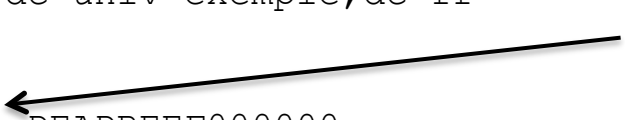
  ▶ la classe supannCMS

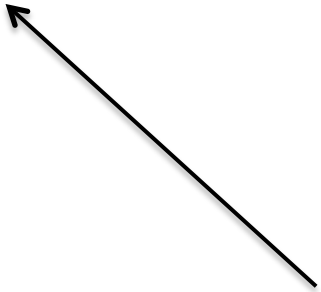
Une nouveauté de 2018 : la CMS

- La classe supannCMS présente 9 attributs
- Certaines informations sont présentées d'une manière redondante afin de couvrir tous les cas d'usage :
  - avec Shibboleth : avec des étiquettes
  - avec un client LDAP : avec des options
  - encodages multiples
- Par exemple : supannCMSId / supannCMSIdEtiquette

Une nouveauté de 2018 : la CMS

```
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
```





Une nouveauté de 2018 : France Connect

- France Connect est un dispositif proposé par l'État reposant sur la norme OpenID Connect. Il permet à un utilisateur de s'identifier à partir d'un fournisseur d'identité à un fournisseur de service du service Public possédant le bouton FranceConnect.
- Il nécessite de déployer une "identité pivot" constituée du genre, date de naissance, prénoms, nom de naissance, code INSEE de la ville de naissance, code INSEE du pays de naissance : représentation de l'état civil.
- Un attribut technique : le "sub" (subject), clé de croisement et témoin de conformité FC -> supannFCSub

Autres nouveautés

- Les options d'attributs ;
- La représentation du cycle de vie des comptes ;
- La gestion des profils multiples (personnes ressources, apprenants, hébergés).

À venir

- Des attributs pour modéliser le recueil du consentement à la diffusion d'informations personnelles (ou professionnelles ou estudiantines), ainsi que la représentation des données personnelles (photo, téléphones, adresse postale et mail personnels...)
- Recommandations d'alimentation et d'intégration au SI
- Recommandations d'architecture technique : réplication, sauvegarde, ACLs, indexation, instances multiples, intégration ActiveDirectory, gestion de l'authentification…