UsersHub - Solution de Gestion des identités et accès (GIA)

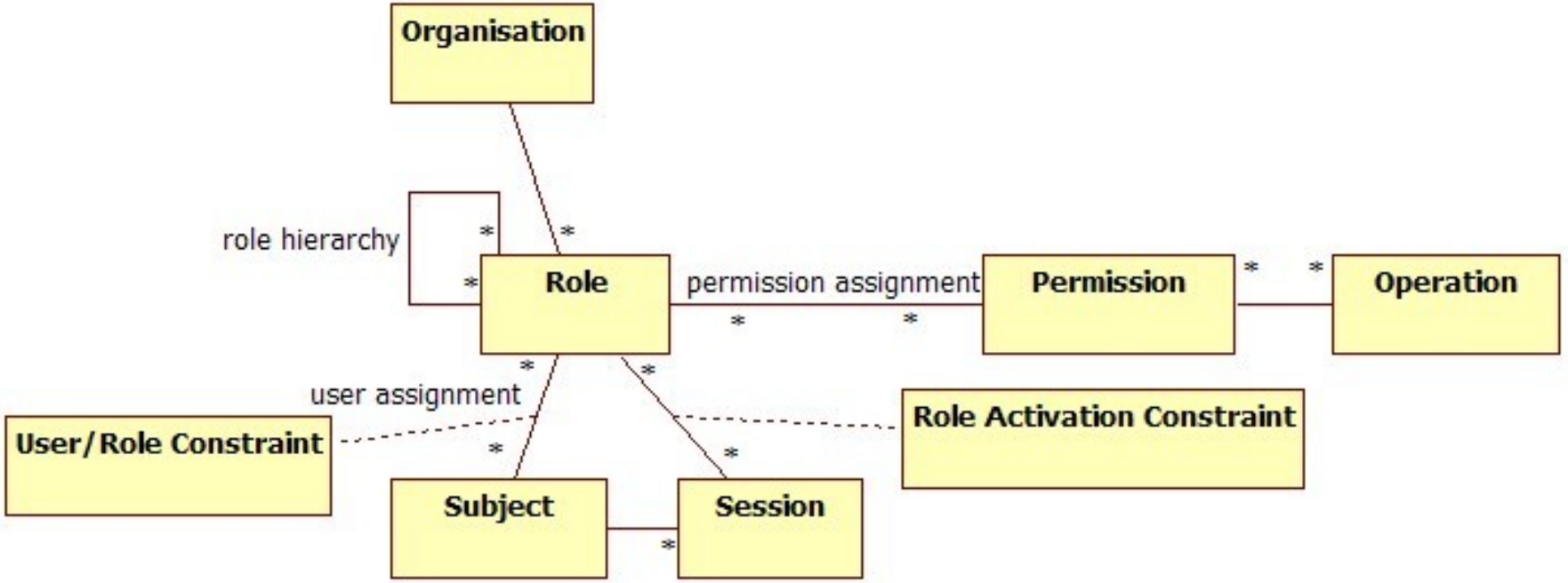
Identity and Access Management (IAM)

Les objectifs de ce type d'outil sont :

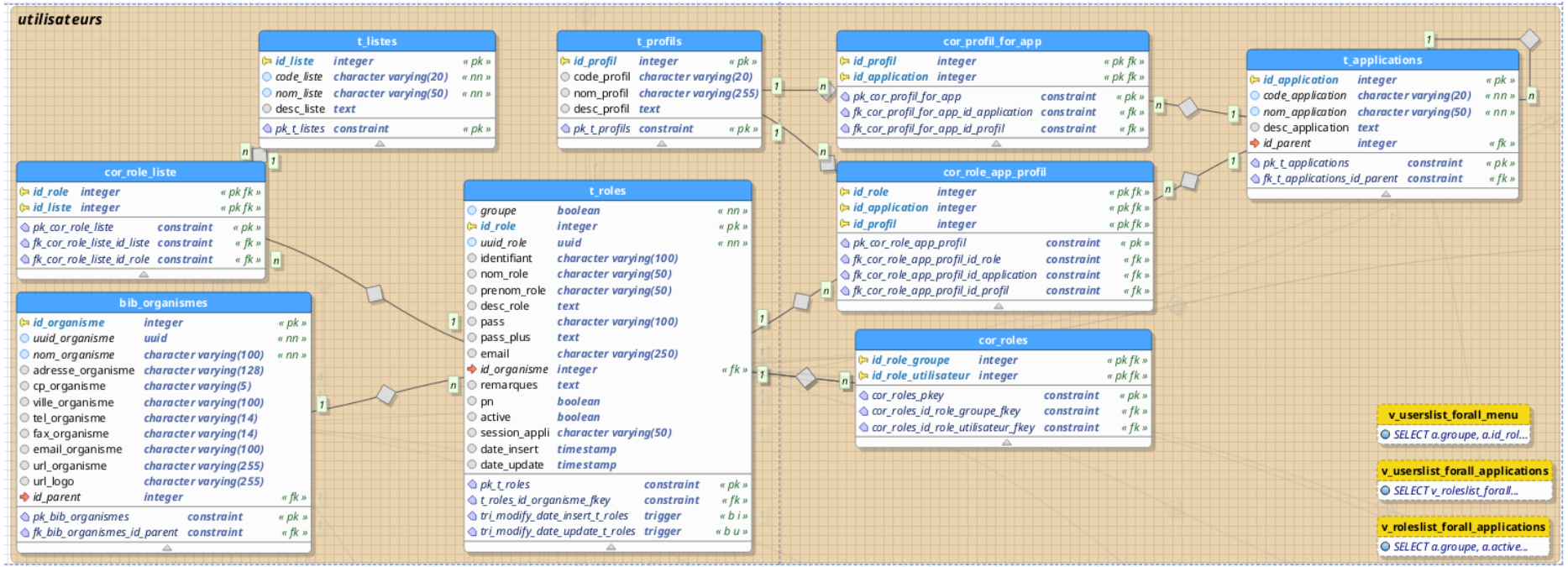
- L'***identification*** : représentation de l'identité d'un utilisateur à l'aide d'un *identifiant* fournit au système.
- L'***authentification*** : couple *identifiant/mot de passe* permet de créer une session entre l'utilisateur et le système.
- L'***autorisation*** : vérification du droit de l'utilisateur à accéder à une ressource.
- La ***gestion de l'utilisateur*** : consultation, ajout, modification, suppression des utilisateurs, des groupes et des rôles.
- être un ***annuaire central*** d'utilisateurs

Modèle classique du Contrôle d’accès basé sur les rôles

Role Based Access Control (RBAC)



Modèle actuel de UsersHub



UsersHub - Différences avec un GIA

- Gestion des **permissions non incluse** => déportée dans les applis “chapeau” (GeoNature, Geotrek)

  => mais présence de la **notion d’application =>** permet la gestion d’accès par appli

- 3 notions *profil*, *liste* et *groupe* équivalant à la notion de *rôle* : **profil** ⇔ **groupe** ⇔ **liste** ⇔ **rôle**
- Pas de nécessité d’une sécurité très poussée (double facteur d’authentification par exemple)
- GeoNature est “DB First” => nécessite le schéma “Utilisateurs” de UsersHub
- Difficultés à remplacer UsersHub par un autre GIA :
  - synchro schéma DB à maintenir => module d’authentification sur mesure.
  - les API doivent rester standard : JWT, SSO...

Besoins des SINP régionaux

Un utilisateur doit pouvoir **demander des accès aux observations précises** pour :

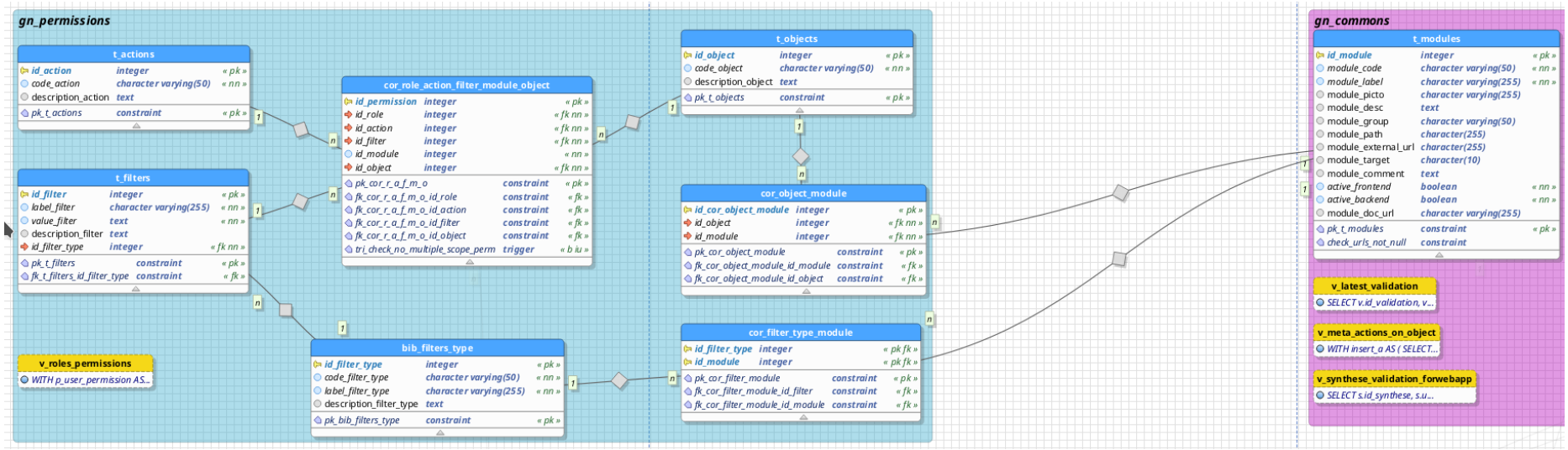
- les **jeux de données privées** avec des niveaux de diffusion
- les **observations sensibles**

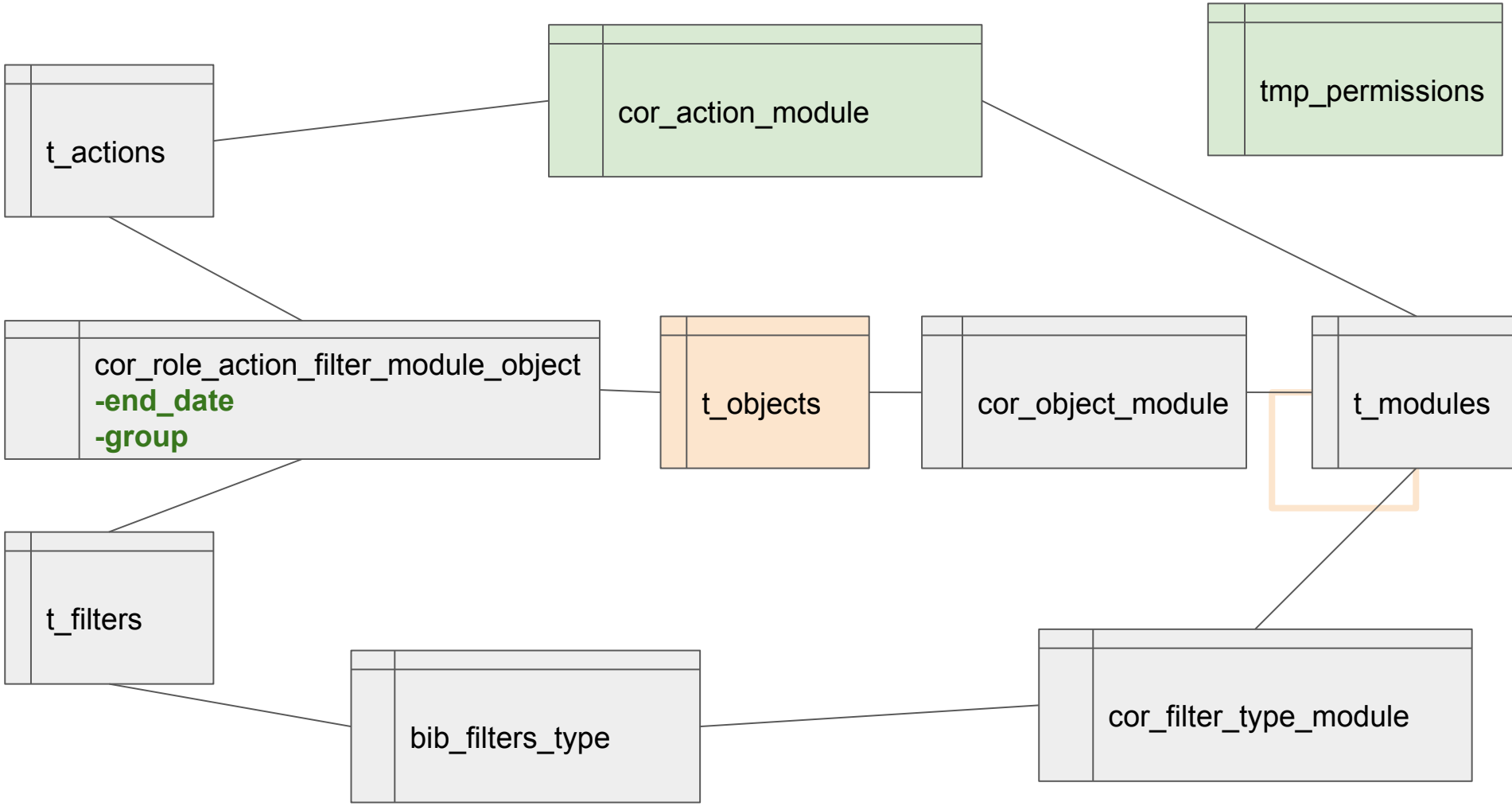
Possibilité de **limiter l'accès aux observations géo-confidentielles** par :

- **zone(s) géographique(s)**
- **taxon(s)**
- **date de fin**

Demandes forcément "**motivées**" => utilisateur doit préciser le cadre (projet, type d'étude, durée...)

Modèle actuel des permissions de GeoNature




t_actions
cor_action_module
tmp_permissions
cor_role_action_filter_module_object
-end_date
-group
t_objects
cor_object_module
t_modules
t_filters
bib_filters_type
cor_filter_type_module

Interface de gestion des permissions

Dans la base de données, un module est associé à : des actions, des filtres, des objets.

Principe de l'interface : pour un module donné, l'utilisateur pourra choisir une action (=> CRUVED), un objet (=> ressources) et y associer des filtres (geo, taxo, portée,...).

Problème : possibilité d'obtenir des combinaisons qui ne sont pas utilisées dans le module.

Solution : prédéfinir des combinaisons par module (?)