

Gestion des utilisateurs

La plateforme est accessible aussi bien au personnel de Bioaster qu'à des personnes extérieures impliquées dans des projets collaboratifs de Bioaster. En fonction de son appartenance à une UTEC, une UTEM ou un projet, l'utilisateur se voit attribuer des droits sur des ressources/outils de calcul, des données, des modules ou des outils/applications.

User stories

[TLC] On va dire que je pinaille, mais je ne pense pas qu'on puisse appeler ces "phrases" des *user stories*. Celles-ci doivent en effet être de la forme :

As a (role), I want (feature), so that (benefit).

Pour prendre un exemple concret, on pourrait écrire :

En tant qu'administrateur, je veux pouvoir supprimer un compte utilisateur, de cette manière ce utilisateur ne pourra plus se logger.

Mais cela n'enlève rien à ton inventaire, c'est juste l'utilisation du terme *user stories* que je ne trouve pas approprié.

Authentification

Story	Référent / Vérificateur
Un utilisateur doit pouvoir s'authentifier avec un login/mot de passe	UTEC6
Un utilisateur doit pouvoir s'authentifier avec un certificat (StartSSL, CaCert, ...)	UTEC6
Un utilisateur doit pouvoir réinitialiser son mot de passe avec une confirmation envoyée par email	UTEC6
Un utilisateur doit être averti de la politique de gestion des cookies appliquée sur la plateforme	UTEC6
Un utilisateur doit pouvoir consulter les mentions légales applicables sur la plateforme	UTEC6

Gestion des droits, autorisation

Story	Référent / Vérificateur
Un utilisateur peut avoir accès à 0 ou à plusieurs applications	UTEC6

Story	Référent / Vérificateur
Un utilisateur doit pouvoir visualiser ses droits d'accès aux applications	UTEC6
Un utilisateur doit pouvoir faire une demande d'accès (en ligne) à une application	UTEC6
Un utilisateur peut être rattaché à 0 ou plusieurs UTECs	UTEC6
Un utilisateur peut être rattaché à 0 ou plusieurs UTEMs	UTEC6
Un utilisateur peut être rattaché à 0 ou plusieurs projets	UTEC6
Un utilisateur doit pouvoir explorer l'espace GPFS de ses UTECs/UTEMs/projets (lecture seule ?)	UTEC6
Chaque UTEC/UTEM/projet a au moins un utilisateur référent	UTEC6

Administration

Story	Référent / Vérificateur
Un utilisateur ne choisit pas son mot de passe, il est généré à partir d'algorithme qui en gère la complexité	UTEC6
Un utilisateur ne peut pas être supprimé. Si un utilisateur doit être supprimé, la date de suppression de son compte et la raison de suppression doivent être renseignées, le champ « actif » de son profil doit être positionné à « False »	UTEC6
L'utilisateur référant d'une entité est obligatoirement un employé de Bioaster	UTEC6
Un utilisateur référent à des droits d'administration des utilisateurs sur l'entité qu'il gère	UTEC6
Lorsqu'un utilisateur est rattaché ou détaché d'une entité (UTEC/UTEM/projet), l'utilisateur référant de l'entité est notifié par mail	UTEC6
Un administrateur doit pouvoir allouer/révoquer des droits sur une application à un utilisateur	UTEC6
Un administrateur doit pouvoir visualiser toutes les demandes de réinitialisation de mot de passe	UTEC6
Un administrateur doit pouvoir visualiser l'historique des connexions d'un utilisateur donné	UTEC6
Un administrateur doit pouvoir bloquer l'accès complet ou partiel (à une entité) à un utilisateur	UEC6

Dictionnaire et modèle de données

Structure d'un utilisateur :

Code	Libellé (en français)	Description	Format/Taille	Obligatoire	Domaine de valeur / Commentaires
id	Identifiant	Identifiant unique de l'utilisateur	Numérique	Oui	
first_name	Prénom	Prénom de l'utilisateur	Texte (100)	Oui	Ex : Anatole
last_name	Nom	Nom de l'utilisateur	Texte (100)	Oui	Ex : France

Code	Libellé (en français)	Description	Format/Taille	Obligatoire	Domaine de valeur / Commentaires
email	Email	Email de l'utilisateur. Si utilisateur Bioaster forcément @bioaster.org	Texte (256)	Oui	Format d'email valide (voir regexp/validator)
dn	Nom distinctif	Distinguished name du certificat de l'utilisateur	Texte (256)	Non	Sensé être unique car contient l'email. Todo : trouver regexp pour validateur
active	Utilisateur actif	Est-ce-que l'utilisateur a le droit de se connecter (ce champ servira à bloquer un utilisateur)	Booléen	Oui	
password	Mot de passe	Mot de passe d'authentification de l'utilisateur	Texte (8-12) ?	Oui	Imposer des règles de complexité ? Ne peut être généré que par un algorithme ?
last_update	Date de dernière modification	Date de dernière modification des données du profil de l'utilisateur	Date	Oui	Automatique
creation_date	Date de création	Date de la création du profil de l'utilisateur	Date	Oui	
supression_date	Date de suppression	Date de la suppression du profil de l'utilisateur	Date	Non	
suppression_reason	Motif de suppression	Motif pour lequel le compte a été supprimé	Texte (taille ?)	Non	Champ libre ou liste de valeur possible : bannissement, a quitté Bioaster, ...
super_user	Super utilisateur	Donne accès à toutes les applications avec tous les droits (réservé aux administrateurs)	Booléen	Oui	
phone_number	Numéro de téléphone	Numéro de téléphone de l'utilisateur	Texte	Non	Trouvé regexp ou validateur « phone number »

Code	Libellé (en français)	Description	Format/Taille	Obligatoire	Domaine de valeur / Commentaires
uid	Identifiant AFS	Identifiant AFS (uid) de l'utilisateur	Numérique	Non	Pour le montage à la volée de l'espace AFS. Ex : 1789
afs_login	Login AFS	Login AFS de l'utilisateur	texte (8 ?)	Non	Ex : pveyre
afs_path	Racine AFS	Répertoire racine de l'utilisateur sur l'espace AFS	Texte	Non	
corporate	Utilisateur Bioaster	L'utilisateur est-il un employé de Bioaster	Booléen	Non	

Structure d'une UTEC :

Code	Libellé (en français)	Description	Format/Taille	Obligatoire	Domaine de valeur / Commentaires
id	Identifiant	Identifiant unique de l'UTEC	Numérique	Oui	
code	Code	Code de l'UTEC	Texte	Oui	Exemple : UTEC-1
nom	Nom	Nom complet de l'UTEC	Texte	Oui	Exemple : Collections d'échantillons biologiques
gpfs_path	Racine GPFS	Répertoire racine de l'UTEC sur l'espace de stockage GPFS	Texte	Non	Ex : /sps/bioaster/UTEC1 ou juste const racine bioster + /UTEC1
email	Email	Alias mail de l'UTEC	Texte	Oui	Valideur mail

Structure d'une UTEM :

Code	Libellé (en français)	Description	Format/Taille	Obligatoire	Domaine de valeur / Commentaires
id	Identifiant	Identifiant unique de l'UTEM	Numérique	Oui	
code	Code	Code de l'UTEM	Texte	Oui	Exemple :
nom	Nom	Nom complet de l'UTEM	Texte	Oui	Exemple :
email	Email	Alias mail de l'UTEM	Texte	Non	Valideur mail

Peut-être faudrait-il penser à une table "Partner" aussi. (id, name, label/code [ex : "bmx_biospecimens"] pour faciliter les permissions car un partenaire peut être présent dans plusieurs projets mais les groupes de personnes du partenaire attachés aux projets ne sont pas forcément les mêmes et ne doivent donc pas forcément avoir accès à tous les projets, mail_referent)

Structure d'un projet :

Code	Libellé (en français)	Description	Format/Taille	Obligatoire	Domaine de valeur / Commentaires
id	Identifiant	Identifiant unique d'un projet	Numérique	Oui	
nom	Nom	Nom du projet	Texte	Oui	Ex : Realism
summary	Résumé	Texte de présentation du projet	Texte (long)	Oui	
gpfs_path	Racine GPFS	Répertoire racine du projet sur l'espace de stockage GPFS	Texte	?	Note : cf chemin cahier de laboratoire ?
corporate	Projet interne	Projet interne à Bioaster (sans partenaire extérieur)	Booléen	Oui	

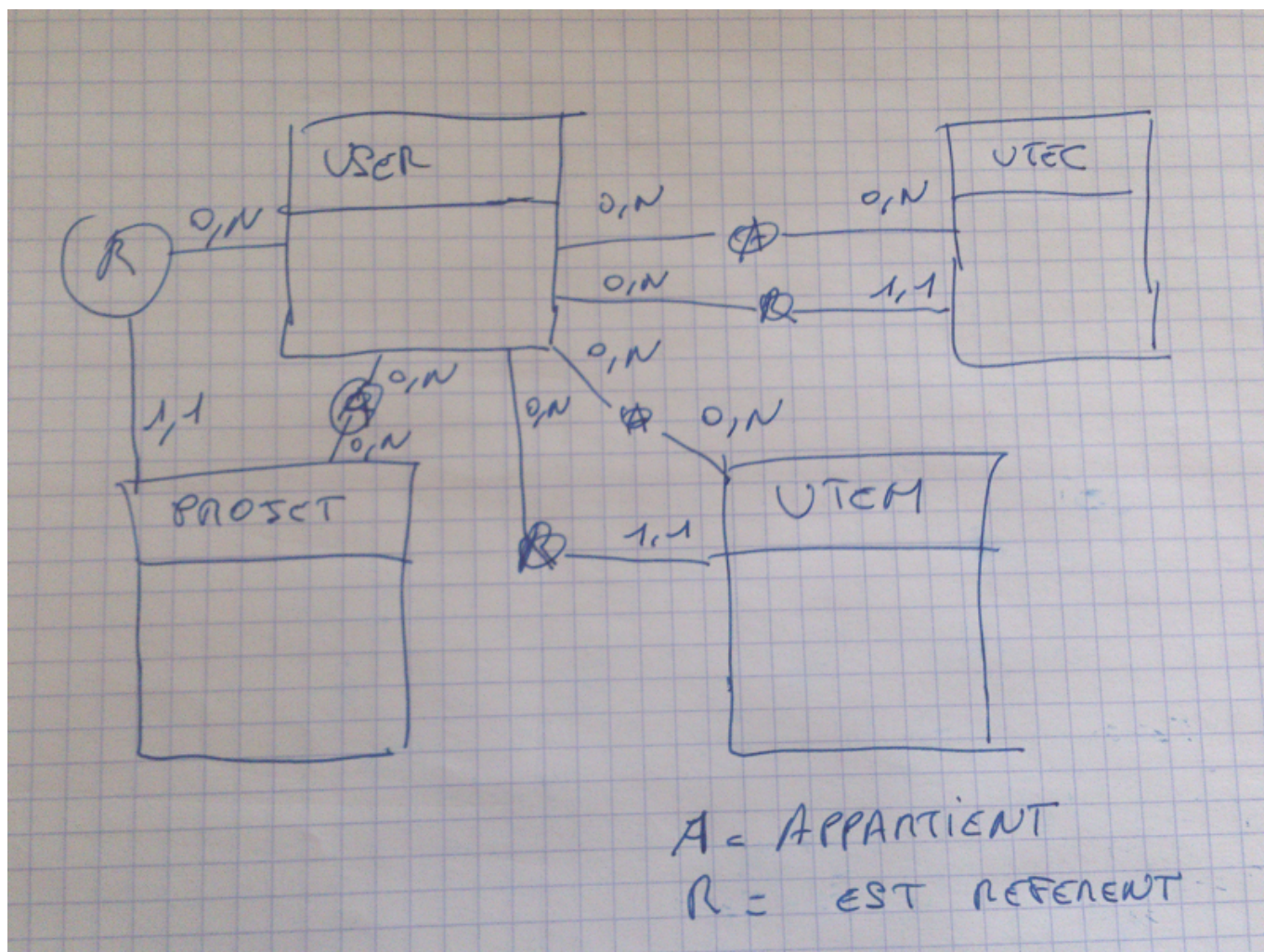
Faut-il descendre jusqu'au Work Package ?

Qui a besoin de quoi ?

Information	Application 1	Application 2	Application 3
email	1	1	1
nom	0	1	1
groupe	1	1	1
afs_path	0	0	1

Implémentation

MCD



Quelques pointeurs :

http://symfony.com/fr/doc/current/cookbook/security/entity_provider.html

<https://github.com/ztec/ZtecSecurityActiveDirectoryBundle>

<https://auth0.com/docs/server-platforms/symfony>

<http://m2mdas.github.io/blog/2013/11/21/integrate-hwioauthbundle-with-fosuserbundle/>

From:

<https://wiki.bioaster.org/> - **BIOASTER**

Permanent link:

https://wiki.bioaster.org/ut6/projets_internes/plateforme_bioinfo/gestion_utilisateur



Last update: **2015/04/27 17:07**