



Les comptes UNR

**Boris VALERA
& Louis CHANOUHA**

11 octobre 2018

sommaire



Génèse

- Finalité et principe de fonctionnement
- Calcul de l'unrCleld
- Mécanique interne
- Cas pratique du SCOUT (et autres)

Génèse

❑ Début du projet autour de 2007

- Création du PRES Université de Toulouse
- Mise en œuvre d'un mécanisme complexe d'alimentation en fin 2008

❑ Mise en œuvre de projets autour du numérique

- Mise en place d'une authentification CAS
- Mise en place d'un Bureau Universitaire Toulousain (BUT)
- Création d'un annuaire UNR

❑ Chronologie

- 2009 : Lancement de l'annuaire et du CAS UNR
- 2011 : Mise en place de Shibboleth
- 2016 : Refonte de l'architecture et du fonctionnement
- 2016 : Adaptations pour gérer le routage de messagerie SCOUT
- 2017 : réécriture complète des processus d'alimentation
- 2018 : l'année de la stabilisation

sommaire

- Génèse
- Finalité et principe de fonctionnement
- Calcul de l'unrCleld
- Mécanique interne
- Cas pratique du SCOUT (et autres)

Finalité et principe de fonctionnement

❑ Objectif

- Offrir un annuaire complet de tous les membres de l'Université Fédérale Toulouse Midi-Pyrénées
- Faciliter le travail en inter-universitaire
- Se centre sur la personne et non les comptes informatiques
 - ✓ Faire en sorte que toutes les identités d'une personnes soient regroupées
- Mutualiser et offrir de nouveaux services

❑ Principe

- Les établissements fournissent une liste d'attributs pour les utilisateurs qu'ils souhaitent remonter
- Un processus central fusionne ces données dans un seul annuaire
- On repère les comptes d'une même personne et on agrège ses données

- Échanges par fichier Idif

Principe de fonctionnement

☐ Usage des 4 branches

Utilisateurs	Comptes de services	Groupes	Listes de diffusion
<ul style="list-style-type: none">• Authentification• Annuaire• Politique d'accès	<ul style="list-style-type: none">• pour le SCOUT• BAL partagées	<ul style="list-style-type: none">• pour le SCOUT• pour les politiques d'accès	<ul style="list-style-type: none">• Pour le SCOUT• mails uniquement

- **Seul la branche « utilisateurs » est obligatoire pour l'intégration**
 - ✓ Unicité des personnes sur cette branche
- **Peu d'informations privées stockées (nom/prénom/identifiant/affectation/adresse(s) mail)**
 - ✓ **Pas de mot de passe**

☐ Alimentation

- **Établissements déposent leurs données (fichiers LDIF) sur un serveur de dépôt**
- **Un script met à jour régulièrement à jour l'annuaire UNR (du lundi au vendredi, de 8h à 17h à la dixième minute de chaque heure)**
 - ✓ Instantanéité de la création des comptes ? Via Webservice
- **Met à jour le SCOUT (depuis février 2018)**

sommaire

- Génèse
- Finalité et principe de fonctionnement
- Calcul de l'unrCleld
- Mécanique interne
- Cas pratique du SCOUT (et autres)

Calcul de l'unrCleId

❑ **Spécifications**

- Hash basé sur : nom, prénom et date de naissance

❑ **Problèmes sur la génération**

- Respect des règles de hashage
- Qualité des données en entrée
- Choix/Disponibilité des données en entrée

- Une nouvelle version des spécifications est en cours de préparation

❑ **Problème sur le compte**

- Problèmes d'affectation du compte à un établissement principal de rattachement
- Changement de contexte qui perturbe les utilisateurs

Calcul de l'unrCleId

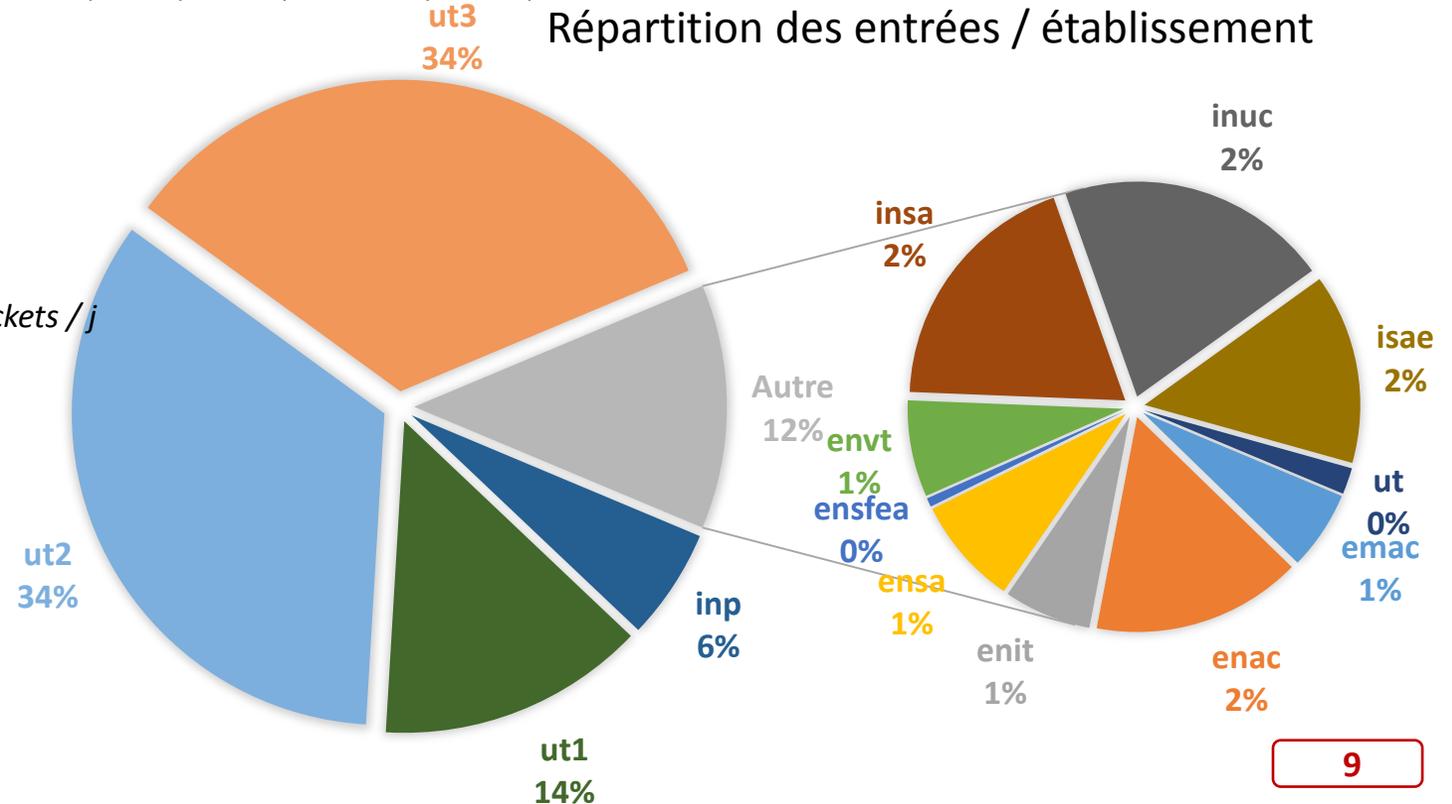
☐ Usage du service

- **Services inter-universitaires:** SCOUT, SICD (Alma, Archipel), Élections, SGC, Prismes, Toulbox, Support...
- **Service d'authentification exclusif:** UT2J, ENVT, COMUE
- **Annuaire:** listes de diffusion, SCOUT...

☐ Quelques chiffres

- **14 établissements** sur l'annuaire en avril 2018
 - ✓ UT1, UT2J, UPS, INSA, INUC, ISAE, COMUE, EMAC, ENAC, ENIT, ENSA, ENSFEA, ENVT, INP
 - ✓ Restent environ 5 établissements

- **176000 entrées** (utilisateurs)
 - ✓ dont **138000 étudiants** (17% personnels)
 - ✓ Dont 2% comptes multi-affectés
- **Annuaire LDAP:** 410000 connexions / j (05/12)
- **CAS** > 30000 connexions / j, > 60000 validations de tickets / j
 - ✓ 55 services UNR
 - ✓ 55 UT2J
 - ✓ 22 COMUE
 - ✓ 14 ENVT



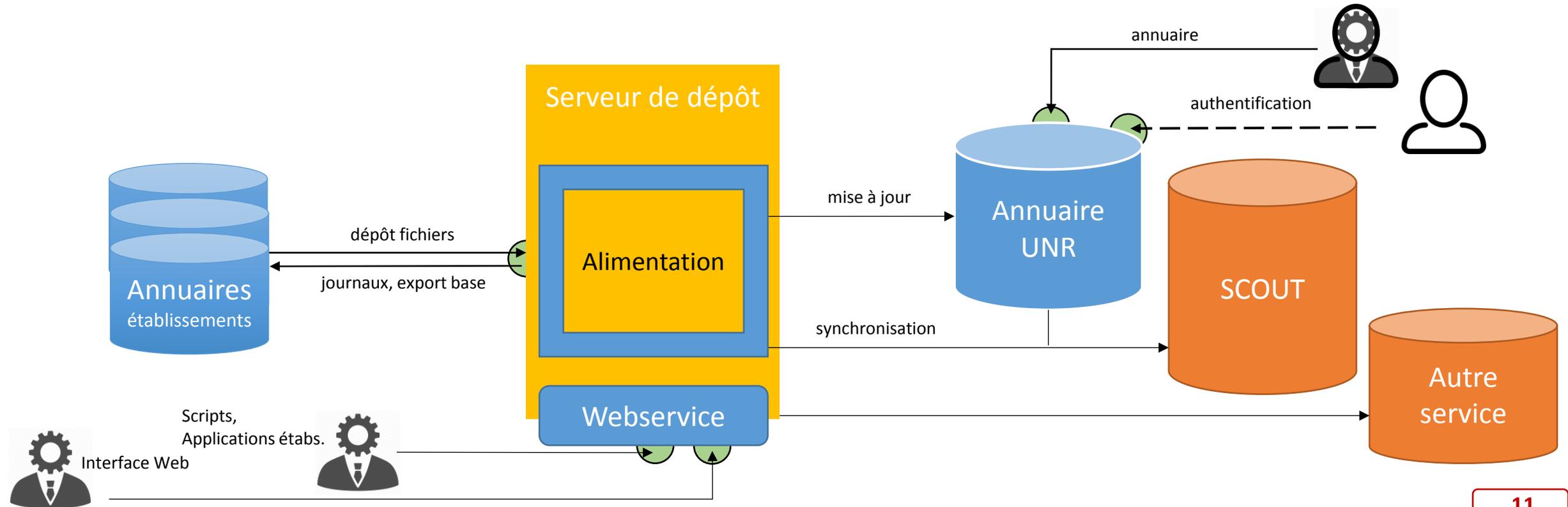
sommaire

- Génèse
- Finalité et principe de fonctionnement
- Calcul de l'unrCleld
- Mécanique interne
- Cas pratique du SCOUT (et autres)

Mécanique interne

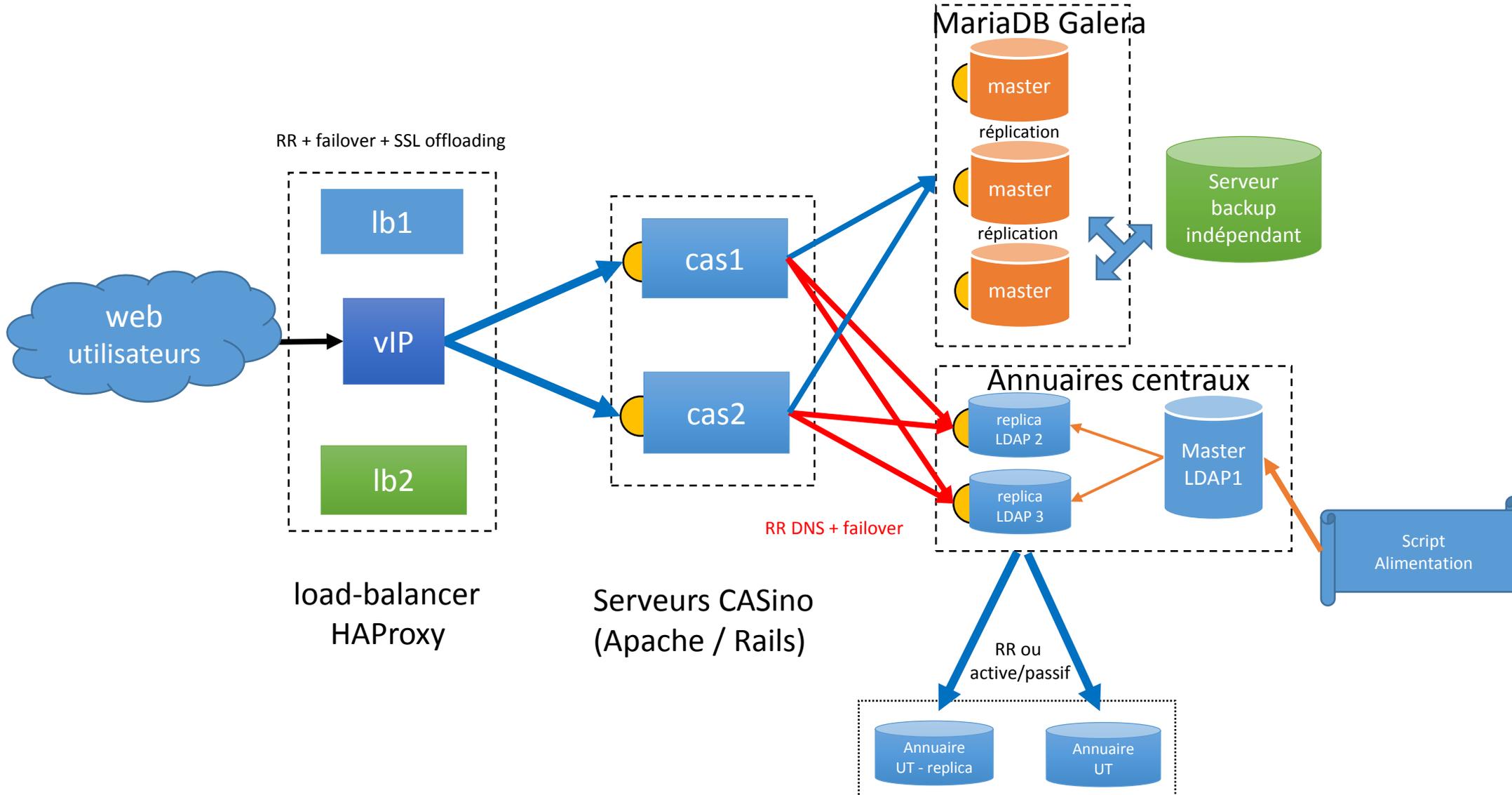
☐ Interfaces de communication

1. **Serveur de dépôt:** mise à jour données, lectures journaux, export annuaire
2. **Interface d'administration:** reporting et opérations
3. **Webservice UNR (REST):** reporting et opérations
 - Création de compte, changement d'affectation, synchronisation...



Mécanique interne

❑ Architecture détaillée: présentation Capitoul du 13 octobre 2016 (Florent Lartet & Louis Chanouha)



Mécanisme interne : Fusion des comptes

❑ Fusion des comptes

➤ Objectif : une personne = un compte = un identifiant

✓ Intérêt

- Un seul compte pour chaque application dans l'UFTMiP (études/carrière)
- Diminution des licences logicielles à payer
- Vote unique
- Centré sur la personne et non le compte

✓ Sélection sur unrCleId

➤ 1 affectation principale et des secondaire(s)

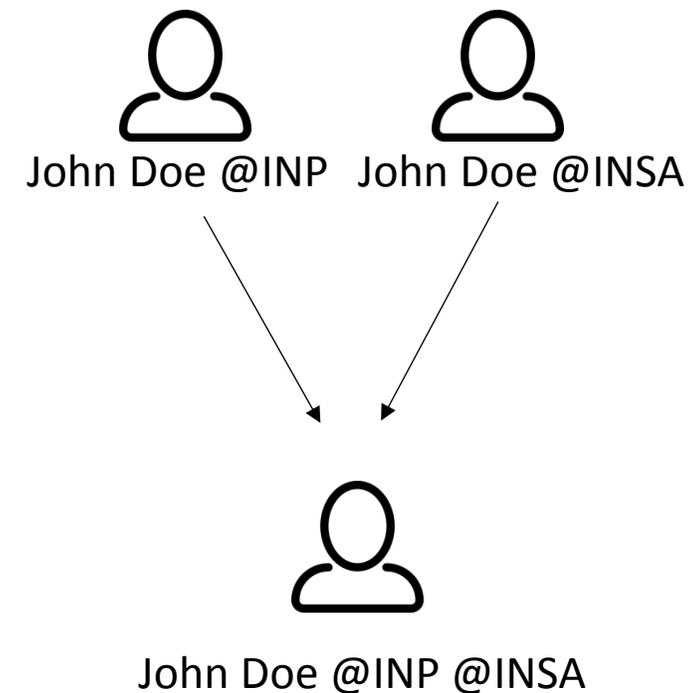
✓ Règle générale = l'affectation principale est conservée tant que possible (depuis 2016)

- Sauf disparition de l'affectation principale

➤ Changement d'affectation manuel possible (webservice, ticket)

➤ Lors d'un changement d'affectation

- ✓ Compte SCOUT automatiquement renommé, synchronisé & affecté au nouvel établissement
- ✓ Envoi de notifications mail



Mécanique interne : Cycle de vie

- Durée de rétention des comptes**
- Durée initiale de vie du compte**
- Mot de passe**
 - **Complexité**
 - **Réutilisation des anciens**
 - **Durée de vie**

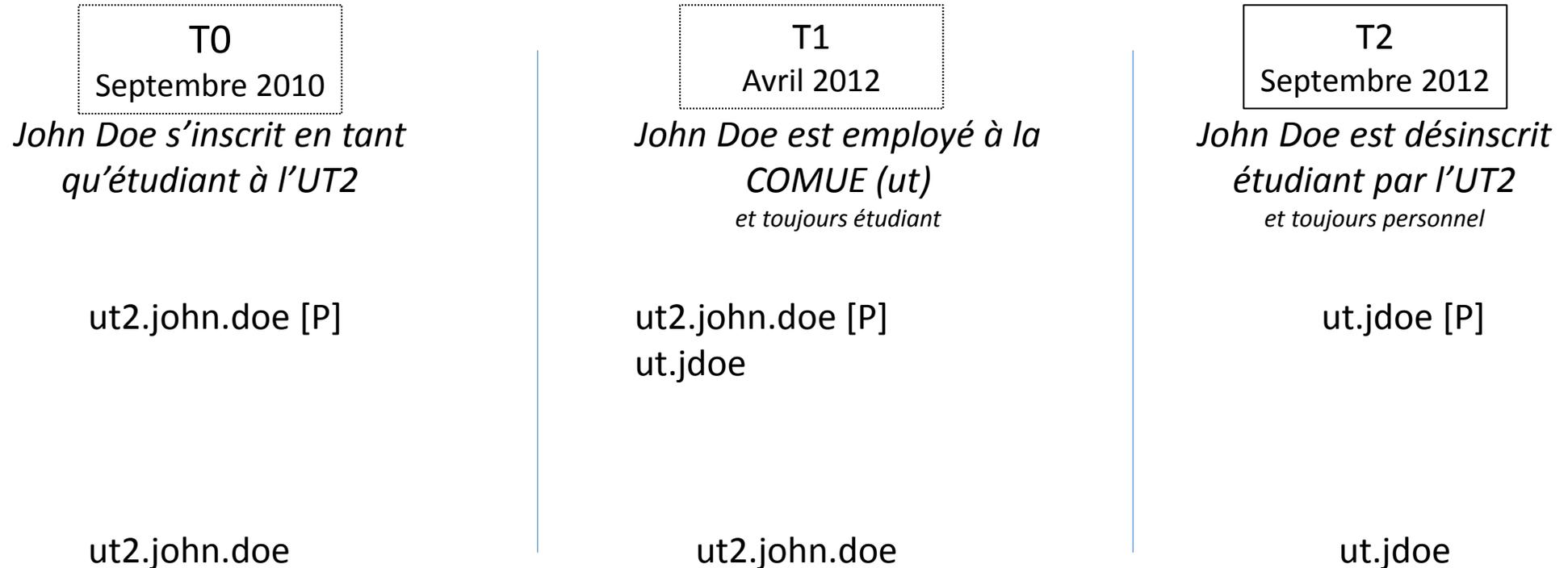
➔ **Paramètres des établissements**

sommaire

- Génèse
- Finalité et principe de fonctionnement
- Calcul de l'unrCleld
- Mécanique interne
- Cas pratique du SCOUT (et autres)

Cas pratique du SCOUT

❑ La fusion des comptes par l'exemple



Intervention manuelle:
Bascule
ut2.john.doe => ut.jdoe
Par équipe UNR ou
établissement d'accueil (UT)

Cas pratique du SCOUT

- Les données suivent l'utilisateur**
- Fusion des adresses d'envoi**
- Un seul compte dans l'application pour toutes les activités**
 - **Pas besoin de se déconnecter pour travailler dans un autre groupe de travail**
 - **On invite le bon compte quelle que soit l'identité utilisée**
- Toutes les authentifications mènent au compte**
- Une seule licence utilisateur à payer**
- Simplicité de gestion des stagiaires**

- Il faut inclure le SCOUT dans les processus d'arrivée et surtout de départ**
 - **Qui prend la main sur les groupes administrés ?**
 - **À qui transférer la propriété des données ?**
 - **Quelles données doivent être supprimées, transférées, oubliées ?**
 - **Comme pour toute donnée liée à un utilisateur...**

Autres cas pratiques

Gestion des bibliothèques

- Migration du systèmes de gestion sur Alma
- Une personne = un emprunteur

Systèmes de votes électroniques

- Une personne = un vote

Conclusion

- Projet pas « uniquement technique »**
- Gros bénéfices de la fusion pour les utilisateurs**
- Des complexités mais des solutions**
- Amélioration continue du système**
- La solution parfaite existe-t-elle ?**

Done is better than perfect !

Des questions ?

