camp
tocamp

INNOVATIVE SOLUTIONS
BY OPEN SOURCE EXPERTS

# Intégration de Fournisseurs d'identité tiers

## Retours d'expérience

# Problématiques

- Choix techniques dans geOrchestra
  - OpenLDAP
  - CAS

- Les organisations ont généralement des existants
  - Annuaires utilisateurs déjà en place
  - Parfois des fournisseurs d'identité disponibles (Oauth2, SAMLv2, ...)

- Comment on s'interface avec ?
  - Synchronisation entre LDAPs (scripts)
  - SASL (cascade authentification d'un LDAP à l'autre)
  - Connexion directe sur des webservices (OIDC/Oauth2, ...)

# Deutsche Telekom

- geOrchestra-gateway: Déjà présentée les années précédentes
- Utilisation d'un fournisseur compatible OpenID-Connect
- Mapping des rôles: OpenLDAP & CAS devenu superflu, pas d'adhérence sur les composants existants geOrchestra

# Renater (INRAE)

- Intégration de la fédération d'identité "Renater"
- Pas support client SAMLv2 pour la gateway
- Intégration via un composant en amont (apache-httpd / mod_mellon)
- utilisation des en-têtes HTTP renvoyés par apache, la gateway se basant dessus pour finaliser l'authentification ("sp-trust-sp")

# MEL (FranceConnect et Oauth2)

- FranceConnect: Quelques spécificités, mais globalement compatible OpenID-Connect

- Fournisseur d'identité compatible Oauth2: La gateway supporte déjà ce protocole

# DT vs MEL / INRAE ?

- Possibilité de configurer la gateway pour créer des comptes provenant de fournisseurs tiers dans le LDAP geOrchestra

- Permet à l'administrateur de plateforme de continuer à administrer les utilisateurs externes (pas possible chez DT mais pas demandé non plus)

# CAS: quel avenir dans geOrchestra ?

- CAS est utilisé depuis le début du projet
- Supporte un certain nombre de protocoles d'authentification
  - Aussi bien en client
  - Qu'en serveur
  - ⇒ véritable couteau suisse de l'authentification
- Piste pas nécessairement explorée, mais pourrait potentiellement répondre à certains usages / Interopérabilité++
- A l'inverse: Utilisation du CAS geOrchestra pour s'authentifier sur des applis tierces (geo2france / eXo)


INNOVATIVE SOLUTIONS
BY OPEN SOURCE EXPERTS