INNOVATIVE SOLUTIONS
BY OPEN SOURCE EXPERTS

camp to camp

INNOVATIVE SOLUTIONS
BY OPEN SOURCE EXPERTS

GEOCOM 2022
AUTHENTIFICATION/AUTORISATIONS DANS GEORCHESTRA
ETAT DES LIEUX & NOUVEAUTÉS

Historique

camptocamp

- Cahier des charges initial:
  - CAS v3.3.3 (héritage ifremer Sextant ?)
  - OpenLDAP
- 2014: Passage en v4.0.x
- 2015: PPIGE-NPDC en v4.2, jamais remonté dans geOrchestra (version custom OpenIDv1, interopérabilité avec catalogue isogeo)
- 2021: Passage en v6.3.x + module provider Oauth2

Expérimentations & intégrations diverses

- Rennes-Métropole: interfaçage avec un Active-Directory / synchro AD → LDAP, puis "SP-trust-SP" entre extranet et intranet
- Expérimentations autour de shibboleth (CNRS / E. Chiarello)
- PPIGE: CAS4.2 / OpenIDv1 & attributs supplémentaires (Isogéo)
- INRA/INRAE: cascade de l'authentification OpenLDAP→AD via SASL (hauteloire, biotope, stdizier)
- OpenLDAP: overlay memberOf puis schémas spécifiques geOr
- GGE/DGE: partage d'infos avec applications tierces (data4citizen)
- Géo2France: ouvrir l'authentification geOrchestra via protocole Oauth2

Le cas particulier "Deutsche Telekom"

camptocamp

- Installation geOrchestra standard
- Utilisation de leur Active Directory corporate (CIAM)
- Retour sur l'OpenLDAP (autonomie des équipes)
- "On voudrait finalement un mélange des deux"
- Nouveaux cas d'usage: interfaçage avec un système existant ("ICU" basé sur keycloak / Oauth2 / OpenID-Connect)

⇒ motivations suffisantes pour une réécriture du SP

Deutsche-Telekom: security-proxy v2 ?

camptocamp

- Basé sur spring-cloud-gateway (microservices = serveurs HTTP qui ont besoin de se parler entre eux)
- SP actuel vieillissant
  - Écrit il y a plus de 10 ans
  - Proxy.java: +1130 lignes de code
  - Beaucoup de code custom pour "faire du http"
  - Nouveaux paradigmes (reactive programming) mais on reste dans l'univers "Spring"
- CAS n'est plus nécessaire / directement compatible

Conclusions

camptocamp

- CAS n'est pas une "mauvaise solution" en soi
  - "Couteau suisse" de l'authentification: interopérabilité++
  - Suffisamment "tordable" à la plupart des besoins / infras
  - Protocole "mûr"
  - Brique utilisée en production ailleurs
- On a mis du temps à migrer de v4 à v6
  - N'a jamais été une priorité dans la communauté
  - Fonctionnel satisfaisant
  - Webapp en v4 pas très responsive
  - Besoin de fournir d'autres protocoles d'authentification
- Possibilités d'aller vers plus de modularité dans geOrchestra ?
  - Brancher / débrancher des briques via configuration ?
  - Il y a souvent un existant, CAS+OpenLDAP viennent souvent en doublon


camptocamp
INNOVATIVE SOLUTIONS
BY OPEN SOURCE EXPERTS