Protocole d'expérimentation FDI-LEEX

Période d'expérimentation :

Date de début : Date de fin :

Membres du groupe :

- **feldma_l / dev**
- **diallo_p / asys**
- **places_m / devops**
- **lombar_j / asys**

Contexte d'expérimentation :

Architecture Microservices sur Kubernetes (backend) et 2 sites clients (une boutique et un site applicatif). Infrastructure utilisée dans le cadre du GPE de places_m & feldma_l en IOT. Un focus particulier a été voulu sur la sécurité du produit.

Objet du protocole :

Comparaison de différents protocoles d'authentification SAML et OAuth2 pour des microservices.
En parallèle, discussion sur les différents providers (google, microsoft, keycloak) pour mieux comprendre et maîtriser la mise en place d'un système de sécurité robuste et fiable.

Objectifs détaillés :

L'objectif est de mettre en place certaines des solutions les plus répandues pour avoir un réel retour d'expérience et nous permettre de choisir au mieux ce qui nous convient.
Les différentes comparaisons mises en place porteront principalement sur la facilité de mise en place et les performances en conditions réelles. Résistance à la surcharge, robustesse et fiabilité sont des éléments clés, qu'il faut prendre en compte dans les moindres détails.
Comparaison des fonctionnalités (théorique), facilité d'implémentation et de maintenance (théorique), rapidité d'exécution (un script avec des timestamps), coûts (théorique) et expérience utilisateur (cf fuite des users sur un form).

Environnement de test :

- OAuth, SAML, Python
- Google, Microsoft (et Keycloak)

Protocole d'expérimentation :

Produire 2 POC (3 si on a le temps): 1 avec OAuth et l'autre avec SAML. Avec ceci, discuter de la facilité de mise en place, la modularité des différentes solutions, les coûts des infrastructures associées.
Réalisation des mini "stress tests" pour évaluer les performances. Plusieurs calls successifs sur les différents systèmes mis en place et extraction d'une moyenne de temps d'exécution pour chacun d'eux.
Vérification de la persistance des données finales.

Documentation :

Concernant le systèmes de single sign_on :

https://fr.wikipedia.org/wiki/Authentification_unique

À propos des différents systèmes à tester et à mettre en place :

https://oauth.net/

https://oauth.net/code/python/

https://blog.authlib.org/2020/fastapi-google-login

https://www.keycloak.org/

https://developers.google.com/identity/protocols/oauth2

https://docs.microsoft.com/fr-fr/azure/active-directory/develop/active-directory-v2-protocols

Extension possible du sujet, perspectives d'évolutions :

Si on compare que les providers classiques (Google, Microsoft), on pourra proposer une implémentation auto-hébergée. Sinon, on trouve un autre protocole à étudier.

Pour les perspectives d'évolution : suggérer un modèle de droits concret

Notes de synthèse / Observations :

Listez ici les points positifs et les points de vigilances que vous avez pu observer durant vos expérimentations.

- Risques
- Evolutions futures
- Impacts
- Taille du groupe
- La communauté
- La documentation
- Facilité de prise en mains