# Privacy Preserving OAuth service using TEEs


## Titus ABELE

Travail de Bachelor 2023

Informatique et Systèmes de Communication – Informatique Logicielle

Professeur: Marcelo PASIN

Expert: Jämes MÉNÉTREY


## Description

L'authentification dans les services en ligne a évolué au cours de la dernière décennie. Aujourd'hui, il est possible pour une application client d'accéder à une ressource protégée en utilisant la norme Open Authorization (OAuth). Le propriétaire de la ressource peut ainsi accéder à la ressource sans avoir besoin d'utiliser les interfaces du fournisseur d'accès. Cela soulève des questions liées à la confidentialité et à la sécurité en ligne puisque les fournisseurs d'accès peuvent observer toutes les données relatives à la consultation des ressources même s'ils ne possèdent pas nécessairement les services clients que le propriétaire de la ressource a choisi d'utiliser.

Ce projet consiste à étudier la conceptualisation et la mise en œuvre d'un service d'autorisation aveugle. L'objectif est d'obscurcir les données entourant l'authentification fédérée à l'aide d'OAuth tout en augmentant de manière significative sa fiabilité. Ceci nécessite l'exécution d'un service d'autorisation OAuth à l'intérieur d'une enclave Intel SGX® dans un environnement d'exécution de confiance.

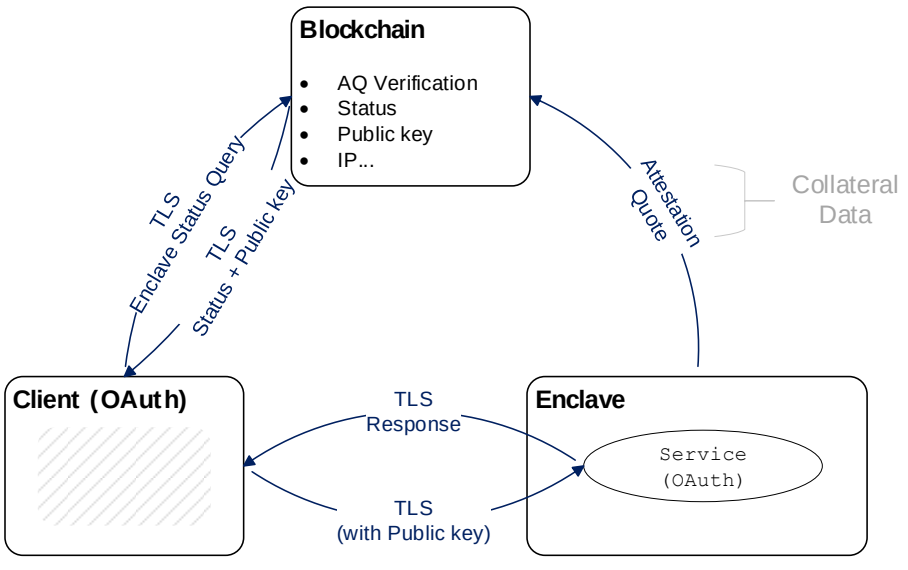
## Déroulement

En s'appuyant sur les environnements d'exécution de confiance, les enclaves Intel SGX et le réseau Integritee, le prototype vise à prouver qu'un service OAuth aveugle préservant la vie privée est réalisable. La norme OAuth prévoit l'utilisation de jetons pour fournir un accès sans justificatif à des ressources protégées. Pour obtenir un tel jeton, l'application cliente doit délivrer une autorisation (sous la forme d'informations d'identification de l'utilisateur dans le cas de ce prototype) et reçoit à son tour un jeton d'accès du serveur d'autorisation.

Une fois que le client a reçu un jeton d'accès, la ressource peut être demandée au serveur de ressources.

## Résultats

Le prototype est fonctionnel et prouve qu'un service d'autorisation OAuth peut effectivement être développé sur du matériel Intel SGX. Cependant, la technologie choisie, Integritee-Network, n'est peut-être pas la meilleure solution pour cette implémentation. Les solutions alternatives incluent le runtime TWINE WebAssembly ainsi qu'une enclave RISC-V Keystone pour l'exécution du service. Intel SGX s'est avéré être d'une nature plutôt complexe, et c'est le principal obstacle à sa popularité. Les problèmes rencontrés ne parviennent pas à rendre intéressante la confiance basée sur Intel. Bien qu'elles soient fonctionnelles, certaines caractéristiques essentielles sont encore absentes de la mise en œuvre. Notamment la sécurité de la couche transport, l'authentification multifactorielle et l'utilisation de bases de données appropriées. Ces trois caractéristiques augmenteraient considérablement la crédibilité et la facilité d'utilisation du prototype.




*Fonctionnement du Integritee-Network*

## Discussion : Conclusions et perspectives

La technologie choisie, bien qu'elle ne soit pas idéale, semble répondre de manière adéquate aux objectifs du projet. Les principales caractéristiques manquent encore en raison de l'absence de prise en charge des bibliothèques externes. Ces problèmes pourraient être résolus en changeant la technologie fondamentale utilisée pour les enclaves pour une norme plus ouverte telle que les enclaves Keystone de RISC-V. Cela permettrait d'améliorer considérablement les performances et la fiabilité.