29-31 mai 2024

Gestion des identités en mode SAAS

Forum OASIS-OKAPI – Session 5

OASIS-OKAPI

Jeudi 30 mai 2024

Authenfication SSO

L'authentification Single Sign On est un processus d'authentification permettant à des utilisateurs d'accéder de manière sécurisée à de multiples applications, à l'aide d'un jeu unique d'identifiant et de mot de passe.

Centralisation des accès (1)

Une fois l'authentification SSO mise en place, les employés d'une entreprise pourront accéder à toutes les applications et tous les sites web disponibles au sein de leur entreprise en s'enregistrant une seule fois.

Centralisation des accès (2)

En d'autres termes, l'authentification SSO permet d'accéder à plusieurs systèmes en se connectant à un système unique, plutôt que de démultiplier les identifiants et mots de passe sur l'ensemble des applications.

Collaboration entre 2 entités

Ce processus d'authentification est rendu possible grâce à la relation de confiance établie entre deux entités : l'identity provider (IdP) qui est un gestionnaire d'identité numérique et l'application à laquelle un utilisateur souhaite accéder, le service provider (SP).

Protocole de communication

La communication entre ces deux entités s'effectue via un standard informatique permettant l'échange d'informations liées à la sécurité : les assertions OIDC (Open Id Connect).

Etapes de la connexion

Voici les différentes étapes de la connexion SSO :

1. L'utilisateur accède au service provider (SP) depuis Internet
2. Le service provider envoie une requête à l'identity provider
3. L'utilisateur est invité à renseigner les identifiants de l'identity provider (nom d'utilisateur + mot de passe)
4. Le fournisseur d'identité valide les identifiants (ou non) et envoie à son tour une assertion OIDC au service provider attestant de la validité de l'authentification
5. Le service provider autorise la connexion de l'utilisateur
6. L'utilisateur peut profiter du service auquel il souhaitait accéder

Mise en œuvre (1)

- Le service provider OASIS-OKAPI peut communiquer avec les 2 identity provider :
  - AZURE-AD
  - Keycloak

Mise en œuvre (2)

- La mise en place est réalisée au terme d'une collaboration étroite entre :
  - DSI
  - TWS

Exploitation

Tous les utilisateurs, qu'ils soient en consultation ou non, sont nommément identifiés.