

Authentification unique - Single Sign On (SSO)

Ressources

- [SimpleSAMLphp](#) : SSO en PHP clé en main
- [Exemple de SSO simple en PHP](#)
- [Différences entre SAML et OAuth](#)
- [Marques pages sur le SSO](#)
- [Fonctionnement du SSO Google](#)

Choix du protocole de SSO

SAML 2 semble être un bon choix car il permet de transférer les informations concernant l'utilisateur. Cependant, ayant été défini en 2005, il [ne prend pas en compte le cas des applications mobiles ou web utilisant AJAX](#). OAuth 2 datant de 2012 prend en compte ce type de situation mais ne permet pas de récupérer en une seule étape les informations liées à l'utilisateur... Pour résoudre le problème du passage d'informations concernant l'identité de l'utilisateur avec OAuth 2, l'utilisation de [OpenID Connect](#) semble être la solution.

Solution OAuth 2 et OpenID Connect

- Serveur OAuth 2 et OpenID Connect en PHP : <https://github.com/bshaffer/oauth2-server-php>

Solution de Drupal pour réaliser un SSO

[Drupal propose](#) de créer des sous-domaines pour chaque site faisant parti du SSO. Cela permet de les faire tous pointer vers un seul script sso.php pour connecter ou déconnecter l'utilisateur de l'ensemble des sites. Le système consiste lors de la connexion/déconnexion de réaliser une chaîne de redirection visitant chaque site en question pour y modifier le cookie contenant les informations de connexion. Le serveur OpenID Connect/OAuth 2 dont se sert Drupal est basé sur le code du [oauth2-server-php](#) indiqué ci-dessus.

Définitions

WebSSO

Le WebSSO se consacre à l'authentification unique pour les applications Web, c'est-à-dire des applications client-serveur dont le client est un navigateur Web ([Source](#))

Identity Provider (IdP) [Fournisseur d'identités]

Service vérifiant l'identité d'un utilisateur et fournissant les informations d'authentications au fournisseur de service.

Service Provider (SP) [Fournisseur de services]

Un fournisseur de service est par exemple une application web qui va déléguer l'authentification de l'utilisateur à un fournisseur d'identité.

Authentification

L'authentification est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une personne ou d'un ordinateur afin d'autoriser l'accès de cette entité à des ressources ([Source](#)). Généralement, l'utilisation d'un couple login & mot de passe permet de réaliser l'authentification.

Identification

Moyen de « connaître » l'identité d'une entité, souvent à l'aide d'un identifiant tel qu'un nom d'utilisateur (login). À ne pas confondre avec le contrôle d'identité (ou authentification) qui permet de vérifier cette identité ([Source](#)).

From:
<https://memos.clapas.org/> - **Memos**

Permanent link:
<https://memos.clapas.org/informatique/developpement/memos/sso>

Last update: **2020/05/22 19:55**

