Secured access to a corporate eHealth community through social media identities

Domaine spécialisé: IT Security
Chargé: Dr. Emmanuel Benoist
Expert: Andreas Spichiger
Partenaire du projet: GSMN Privatklinik Obach, Solothurn

L'authentification dans le domaine médicale est un sujet important, l'utilisation du Single Sign-On permet de faciliter l'accès aux données importantes pour les médecins. Dans ce projet, plusieurs moyens de connexions via des réseaux sociaux ont été étudiés ainsi que la façon de les intégrer dans l'environnement de l'entreprise. Pour la réalisation, L'Identity Server de WSO2 est utilisé comme intermédiaire entre l'application et les différents Identity Providers.

Introduction

L'authentification dans les entreprises est un sujet important, en particulier dans le domaine médicale, où une perte de temps pour accéder à des informations critiques peut être une question de vie ou de mort.
L'utilisation du Single Sign-On est une première approche pour diminuer le taux d'oublie/perte de mot de passe. Mettre à disposition des médecins la possibilité de se connecter à leur compte via des médias sociaux accélère justement l'accès aux données.

But de la thèse

Le but de la thèse est de permettre aux utilisateurs de s'authentifier via différents Identity Providers (IdPs) : la base de données interne, Google, Facebook, une base de données Shibboleth ou la SuisseID.
L'intégration de l'application dans l'environnement de l'entreprise est un des points clés de ce travail.
L'utilisation et la configuration de l'Identity Server de WSO2 comme intermédiaire entre l'application et les différents Identity Providers sont une partie importante de ce projet.
Les utilisateurs accèdent à l'application principale. Celle-ci joue le rôle de Service Provider et leur permet de choisir un mode de login. Le mode choisi entraîne la redirection de l'utilisateur vers la page de login correspondante.

L'authentification est alors réalisée du côté de l'Identity Provider sélectionné, puis l'application principale reçoit, en retour, les attributs demandés de l'utilisateur concerné.

Réalisation

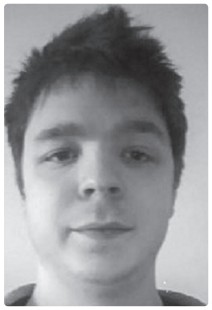
Pour communiquer avec le Service Provider, l'Identity Server de WSO2 privilégie le langage SAML. Les Identity Providers, eux, n'utilisent pas systématiquement ce langage : Google et Facebook utilisent respectivement OpenID et OAuth2, alors que Shibboleth et la SuisseID utilisent SAML. Les échanges sont cryptés au moyen de SSL. Les attributs récupérés auprès des différents IdPs sont utilisés pour gérer les comptes des utilisateurs pour l'application concernée.

Résultats

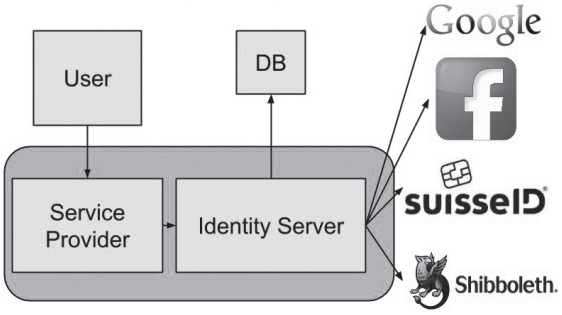
Les utilisateurs, ainsi connectés via leur compte externe, sont alors enregistrés dans la base de données interne et peuvent ensuite modifier certaines informations. La gestion fine des droits est, quant à elle, assurée par un administrateur, via une console dédiée.

Perspectives

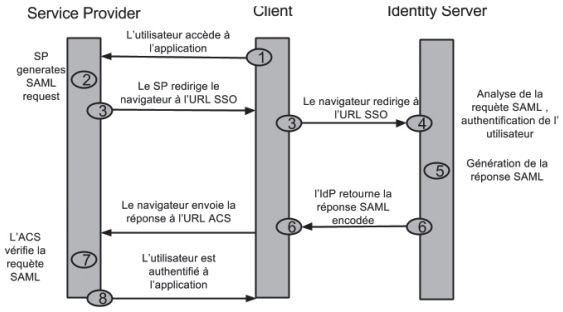
Le provisioning ultérieur d'autres Identity Providers s'appuie sur la même logique. La veine est ainsi ouverte.



Malic Maraachli



Composants du projet



Communication SAML entre l'application et l'Identity Server de WSO2