# Shad facilite les accès des utilisateurs finaux internes de l'État fédéral

**Un accès sûr est fondamental pour toute application informatique de l'État. Par ailleurs, il est très laborieux de dresser et gérer une liste d'utilisateurs pour chaque produit de l'e-governement. Le G-Cloud Shared Directory (ShaD) offre dès lors une solution unique d'authentification.**
**"Le G-Cloud ShaD concilie une infrastructure d'authentification centrale avec une gestion décentralisée des utilisateurs.", explique Luc Coppens, Directeur ICT au Service fédéral des pensions.**

*Luc Coppens, Directeur ICT, Service fédéral des pensions : "La première étape est l'identification classique, avec nom d'utilisateur et mot de passe, basée sur les données reprises dans la liste des utilisateurs de l'institution."*

Cela semble un problème informatique trivial : identifier les utilisateurs finaux en ligne, ajouter des utilisateurs et gérer leurs droits d'accès. Et ce pour chaque application. Néanmoins, le but n'est pas d'avoir des listes d'accès distinctes pour chaque application et institution. C'est un véritable obstacle pour des services communs. Sans compter que cela constitue un facteur de coûts inutile et un risque permanent en termes de sécurité.

"Pour le site web du moteur pension ou la plateforme collaborative BeConnected, des fonctionnaires de plusieurs institutions travaillent ensemble. Mettre en place une gestion des accès "ad hoc" avec autant d'organisations relève de la folie. Lorsque nous voulions partager la même application avec deux ou trois institutions, il y avait donc deux ou trois solutions techniques différentes. Une solution meilleure, générique s'imposait donc. Nous y avons nous-même contribué.", explique Luc Coppens, Directeur ICT au Service fédéral des pensions (SFP).
"Après consultation d'autres institutions, fédérales et dans la sécurité sociale, il est apparu qu'il était préférable de partir des listes d'utilisateurs (répertoires) existantes de chaque institution. C'est ce que nous avons donc fait.", confie Luc Coppens. C'est ainsi qu'est né Shared Directory (ShaD), un service G-Cloud générique pour l'authentification et, à terme, l'autorisation.

## La gestion des utilisateurs reste décentralisée

"La première étape vers le 'Cloud', également vers le Public Cloud, c'est toujours l'identité.", indique Bart Billiet, solutions architect au Service fédéral des pensions. Le répertoire personnel de l'institution doit être l'unique source de vérité. Le service G-Cloud ShaD chapeaute les listes des utilisateurs par institution. "Les institutions conservent la gestion des utilisateurs. Si vous créez un nouvel utilisateur, celui-ci devient connu pour les applications du G-Cloud, et est aussi immédiatement désactivé lorsque la personne quitte l'institution. Le but est que chaque institution puisse assurer cette gestion seule, que celle-ci ne soit pas centralisée."

"Le modèle de fédération, par lequel nous avons commencé, est le plus beau modèle. Les applications sont seulement "reliées" au service ShaD et donc facilement intégrables, en particulier les applications web.", poursuit Bart Billiet. "De plus en plus d'applications supportent les 'claims', une technique selon laquelle l'application n'assure plus elle-même le contrôle de l'identité. L'utilisateur se légitime auprès du répertoire de l'institution. Le service de fédération ShaD enregistre l'identité que l'utilisateur final "revendique" et transmet l'information à l'application. Au besoin, nous aidons d'autres institutions à adapter leurs applications à cette technique."

## Plusieurs formes et variantes

"La première étape est l'identification classique, avec nom d'utilisateur et mot de passe, basée sur les données reprises dans la liste des utilisateurs de l'institution.", ajoute Luc Coppens. "La technique des 'claims' est vivement recommandée pour les applications web de dernière génération. Parallèlement, nous supportons deux autres solutions, pour des technologies spécifiques: il y a un service

Suite >

*Bart Billiet, solutions architect, Service fédéral des pensions : "Pour l'utilisateur final, l'identification doit encore se faire de façon transparente."*

ShaD pour Office 365 et les services connexes, tandis qu'un autre service ShaD supporte spécifiquement le G-Cloud UCC-as-a-Service, avec Skype for Business et Exchange comme applications principales. L'architecture de ShaD est la seule qui supporte ces applications et est le fruit d'une concertation avec des spécialistes du métier de l'Europe et des États-Unis."

"Pour l'utilisateur final, l'identification doit encore se faire de façon transparente. Vous ne devez pas avoir de mot de passe distinct pour chaque application.", souligne Bart Billiet. "L'application la plus connue aujourd'hui est probablement le Moteur salarial, qui permet à plus de 12.000 collaborateurs d'une dizaine d'institutions publiques de la sécurité sociale de consulter leurs fiches de salaire électroniquement", confirme Luc Coppens, "ou le portail de connaissances BeConnected, l'outil de traduction BabelFed, ou encore des services G-Cloud techniques comme VM-as-a-Service, Backup-as-a-Service et GITLab." L'intégration la plus poussée concerne UCCaaS et l'accès à la plateforme fédérale de connaissances BeConnected."

"Pour des applications plus anciennes, une solution est en cours d'élaboration. Il faut ici examiner au cas par cas si la liaison est rentable. Il se peut que Shad ne soit pas toujours la meilleure solution, en particulier pour l'administration de systèmes ou pour des applications très spécifiques. Nous continuerons à nous focaliser sur l'utilisateur final, classique."

## Tourné vers l'avenir grâce aux standards ouverts

Bien que les services ShaD reposent sur une technologie commerciale, ils peuvent être reliés à différentes applications. "Le service de fédération repose entièrement sur des standards ouverts, plus particulièrement SAML v2. Les applications que nous avons reliées aujourd'hui sont souvent open source. Les spécialistes techniques de ce monde ont également insisté pour utiliser ShaD. On voit ainsi que les mondes de Windows et Linux peuvent coexister paisiblement.", conclut Luc Coppens.

## À propos du G-Cloud Shared Directory (ShaD)

ShaD (Shared Directory) est la solution centrale d'authentification pour les services du G-Cloud, qui permet aux utilisateurs internes de différentes institutions publiques de démontrer leur identité pour se connecter et à chaque institution publique de préserver la responsabilité de son propre répertoire local.
ShaD a été créé dans les buts suivants :

- Identifier facilement les utilisateurs internes de différentes institutions.
- Offrir la possibilité de centraliser des applications communes avec une identification basée sur le répertoire de chaque institution.
- La gestion des comptes utilisateurs reste dans chaque institution.
- Réduire à un minimum l'impact sur l'Active Directory (AD) existant des institutions.

Sur la base du type d'application, plusieurs modèles d'authentification sont aujourd'hui supportés :

- ShaD Federation Services : offre un Single-Sign-On dans les applications basées sur les "claims".
- ShaD UCCaaS : offre un Single-Sign-On pour Skype For Business & Exchange UCCaaS services. Architecture en collaboration avec Microsoft et Dimension Data, implémentation par Dimension Data.
- ShaD Online : procure une connectivité avec Azure AD et l'identification des utilisateurs dans Office 365. Autorise des fonctionnalités hybrides dans UCCaaS pour Skype, où les services peuvent être utilisés de façon transparente entre UCCaaS et Office 365.

Dans le ShaD et le G-Cloud, nous travaillons à une fonctionnalité additionnelle (ex. ShaD Domain Services, une solution d'authentification pour les applications plus anciennes) et au développement d'une vision et des composants nécessaires pour permettre aux utilisateurs d'accéder aux services de façon sûre et contrôlée.

## Plus d'informations

Contactez-nous via
shad@gcloud.belgium.be