

## Introduction à la notion de *Fédération de Services*



Pour le projet GEARS dont EIFEL est partenaire, la première brique d'un *système de fédération de services* va être proposé aux utilisateurs du pilote français qui démarre au mois de mai.

Cette première brique va consister à leur fournir un service de Single Sign On (SSO) ce qui va leur permettre de pouvoir naviguer entre le portail Plone et le groupe de travail mis à leur disposition par EIFEL, leur ePortfolio dans Elgg et le site Strategy Blueprint fournissant les contenus de formation du pilote, sans devoir s'identifier trois fois.



### Comment ça fonctionne ?

L'utilisateur va d'abord devoir s'authentifier sur Plone et le groupe de travail, dans Elgg et dans Strategy Blueprint.

A chacun des trois login et mots de passe propres aux trois environnements, sont associés des identifiants indépendants, fournis par un (ou plusieurs) fournisseur(s) d'identités (IDP, pour Identity Provider). L'utilisateur peut alors faire le choix de "fédérer" ses trois identités ce qui lui permet de circuler librement (sans s'identifier à nouveau) entre ces trois environnements.

Il est important de noter que seul l'utilisateur connaît ses identifiants et que chacun des systèmes reste complètement découplé par rapport aux autres.

EIFEL jouera le rôle d'IDP, sur la base d'Authentic, un service fondé sur la librairie open source LASSO développée par Entr'ouvert.

Le système IDP et les services proposés (Plone, Elgg et SB) auront au préalable défini ce que l'on appelle un cercle de confiance en échangeant différents paramètres ainsi que des certificats Internet (le même type de certificat que ceux qui sont utilisés pour signer des mails ou payer sur les systèmes de e-commerce).

Chaque utilisateur disposera également d'un compte avec un login et un mot de passe sur le système IDP. Il devra alors demander au système IDP de fédérer ces 4 logins.

Il y a 2 méthodes pour cela :

soit à la demande de l'utilisateur authentifié sur l'un des services concernés,  
soit à la demande de l'utilisateur authentifié sur l'IDP (la méthode n'est pas encore précisée pour notre système).

notre IDP, Authentic, créera alors une association entre ces différentes identités sans faire de copie locale des couples logins/mots de passe.

Les trois identités étant alors associées, l'utilisateur pourra, à partir d'une seule identification sur l'un des services ou sur l'IDP, naviguer entre Plone, Strategy Blueprint et Elgg.

## Quels sont les avantages d'un système de fédération d'identité par rapport à un système de SSO « normal » ?

Le SSO classique partage généralement le même login et mot de passe pour TOUS les services en même temps. Le gros désavantage est qu'en cas de piratage de cette identité, le pirate a accès à tous les services reliés par ce SSO, ce qui n'est pas le cas d'un système de fédération de services.

Liberty Alliance (LA) est un consortium industriel qui produit des spécifications dans le monde industriel, télécommunications, mobiles... et pas seulement pour l'éducation.

LA propose deux frameworks dont la fédération d'identité (ID-FF en terminologie LA) qui permet le SSO, c'est le niveau préalable à leur Web Services Framework (ID-WSF en terminologie LA). Voir le schéma N°1

Ce système ID-WSF permet de partager des attributs. Un attribut c'est par exemple, un élément de votre profil dans votre carnet d'adresse, de votre profil créé dans votre eportfolio, de votre profil personnel et/ou professionnel au sein de l'intranet de l'entreprise où vous travaillez, de votre fiche apprenant dans le LMS où vous êtes inscrit...

Ces attributs vont pouvoir être partagés à plusieurs niveaux.

### Exemple :

Vous renseignez votre carte de visite dans votre carnet d'adresse avec nom, prénom, email, téléphone... et tout ce que vous pensez intéressant comme données à fournir à vos correspondants.

Vous allez pouvoir transmettre TOUT ou PARTIE des informations de votre carte de visite au portail de votre entreprise, à un LMS pour suivre une formation sans avoir à compléter de nouveaux formulaires contenant les champs de cette carte.

A plus long terme, il sera même possible de partager avec une personne en particulier ces informations (c'est une évolution des spécifications en cours au sein de LA).

Les applications vont de l'éducation au commerce électronique en autorisant l'accès à ces services par votre mobile, votre ordinateur ou tout système communiquant supportant ces spécifications.

A ce jour, comme vous le savez, lorsque vous complétez un formulaire sur un site, le descriptif des informations stockées sur le serveur de l'entreprise du site est transmis à la CNIL qui s'assure que l'entreprise respecte les chartes de la Cnil et qu'elle vous accorde bien un droit de regard et de rectification ; c'est l'entreprise qui détient votre profil et peut donc l'utiliser pour que vous receviez des informations pas toujours pertinentes.

Avec le Web Services Framework, c'est vous qui transmettez une autorisation d'utilisation de certaines de vos données personnelles et à cette entreprise particulière, pas une autre. Lorsque vous décidez de supprimer cette autorisation, le système informatique de l'entreprise en question supprimera automatiquement les informations qu'il aurait pu dupliquer localement. Bien entendu cela n'évite pas un risque de détournement des informations par une personne mal intentionnée mais l'entreprise ne pourra plus demander de mise à jour de vos données personnelles aux autres services. Une telle demande serait automatiquement et immédiatement rejetée.

Une vraie révolution en terme de sécurité et d'appropriation de l'identité de chacun.

### Petit Historique :

Le système développé par Liberty Alliance est un exemple d'architecture SOA (Service Oriented Architecture) sécurisé. Voir schéma N°2.

Les gros opérateurs comme IBM, SUN, TIBCO, SAP et Microsoft ont bien sûr d'autres propositions d'architecture SOA, mais rarement en open source et surtout bien moins sécurisés (c'est pourquoi les principaux acteurs, excepté Microsoft, font partie du consortium LA).

Shibboleth est un autre système de fédération de service répandu dans l'éducation mais qui ne va pas aussi loin que LA. Il ne dispose pas du framework web service.

D'ailleurs, Internet2 qui supporte Shibboleth est maintenant membre du consortium Liberty Alliance.

Ces deux structures ont à l'origine utilisé un même standard SAML de l'OASIS (équivalent du W3C) pour construire leur framework de fédération de services, en travaillant chacun de leur côté. Ils ont enfin réuni leurs travaux autour d'une évolution majeure de SAML, la version 2, toujours hébergée au sein d'OASIS.

La roadmap de Shibboleth prévoit maintenant le support de SAML 2 ce qui lui permettra de fournir dans l'avenir (et en gérant l'évolution du parc existant) un système IDP conforme avec Liberty Alliance (la dernière version des spécifications LA étant déjà basée sur la version 2 de SAML).

## Liberty Alliance

### Liberty Identity Federation Framework (ID-FF)

S'authentifier une fois et être capable d'utiliser des services d'autres sites fédérés sans autre authentification complémentaire.

1

### Liberty Identity Services Interface Specifications (ID-SIS)

Spécifications web service pour la gestion des services basés sur les profils (profil personnel, profil employé..)

3

### Liberty Identity Web Services Framework (ID-WSF)

Comment trouver, décrire des services basés sur l'identité.  
Comment interagir avec ces services (politique d'accès prenant en compte des demandes d'accès aux données personnelles).

2

## Exemple d'architecture SOA

