

J-EOLE

17-18 Octobre 2013

Evolutions Seshat / EoleSSO

Bruno Boiget - Christophe Léon

Evolutions Seshat / EoleSSO

- Contexte
- L'application eDispatcher
- EoleSSO – Nouvelles fonctionnalités
- Casification et fédération

Evolutions Seshat / EoleSSO

- Contexte
 - Dans le cadre de l'intégration des services académiques (dont les portails agents et téléservices) au sein des ENT, nous avons proposé un début de solution se basant sur le serveur Seshat et le service EoleSSO.
 - Un certain nombre de problèmes empêchaient une intégration complète. En particulier la problématique de fédération dans le cadre d'utilisateurs affectés à plusieurs établissements (responsables d'élèves).
 - En collaboration avec la mutualisation Envole, nous avons cherché une solution à ces problèmes.

Evolutions Seshat / EoleSSO

- L'application eDispatcher
 - Objectif : Créer un **point d'entrée central** au niveau académique pour l'accès aux ENT et au PIA (pour les élèves, parents, et personnels académiques).
 - Pré-requis
 - Scribes en établissement alimentés par **AAF**
 - **Réplication** d'annuaire et **féderation** entre les serveurs Scribes et Seshat. Les serveurs doivent être enregistrés sur **Zéphir**
 - **Fédération** entre Seshat et **FIM-AGENT / FIM-TS** suivant les fonctionnalités désirées

Evolutions Seshat / EoleSSO

- **eDispatcher** : Fonctionnement

- eDispatcher est protégé par le service EoleSSO de Seshat. L'utilisateur se **connecte sur l'application edispatcher** et est redirigé sur le serveur SSO pour s'**authentifier**.
- Il est alors **renvoyé sur l'application** avec les **attributs** nécessaires (un filtre et des attributs calculés sont installés par le paquet eole-dispatcher).
- Ces attributs permettent de calculer les **établissements d'affectation** de l'utilisateur et de retrouver l'adresse du **portail correspondant** (à l'aide de données envoyées par Zéphir)
- l'utilisateur choisit un établissement et une fédération est alors déclenchée vers le fournisseur de service correspondant. La **clé de fédération** est calculée en **fonction de ses attributs**, son **mode d'authentification**, et sa **provenance réseau**.

Evolutions Seshat / EoleSSO

- **EoleSSO** – nouvelles fonctionnalités
 - Fichiers d'**attributs calculés** renvoyant **plusieurs attributs**
 - Mise à disposition d'informations supplémentaires :
 - numéro établissement dans les méta données
 - Service à atteindre et niveau d'authentification dans les attributs de l'utilisateur
 - Désactivation de l'**auto-complétion** à l'authentification
 - Ajout d'un **mode liste blanche** pour les applications Casifiées (Pas de filtre par défaut, seules les applications déclarées reçoivent une réponse du serveur).
 - Présentation d'une URL spécifique en cas de **désynchronisation de clé OTP** (suite à des instabilités constatées sur la librairie PAM/RSA).

Evolutions Seshat / EoleSSO

- Protection d'applications (protocole CAS)
 - La Casification d'application PHP est documentée dans le wiki du projet **eole-php5-cas**
 - Des applications sont livrées par défaut sur Scibe (piwik, ajaxplorer, portail Posh, ...)
 - De nombreuses autres applications ont été prises en compte :
 - Voir le **site de la mutualisation Envole** (envole.ac-dijon.fr). Des rubriques sont dédiées aux applications gérées (par la mutualisation et hors mutualisation).
 - Le **projet envole-conf-sso** regroupe des connecteurs pour diverses ressources pédagogiques (cns, vocable, lesite.tv, ...)
<http://envole.ac-dijon.fr/wordpress/2013/04/29/connecteurs-sso>.

Evolutions Seshat / EoleSSO

- Fédération d'identité (protocole SAML 2)
 - La fédération avec les serveur **FIM-RSA** (portails agents et télé-services) a été mise en place dans plusieurs académies.
 - Des tests de fédération de Scribe avec d'autres ENT ont été expérimentés (**K-d'école**)
 - La fédération d'EoleSSO en tant que fournisseur de service avec un serveur **Shibboleth** (Educagri, enseignement agricole) est actuellement en cours d'expérimentation.
 - De nombreux autres produits utilisent le protocole SAML (SimpleSAMLphp, LemonLDAP::NG, ...)

Evolutions Seshat / EoleSSO

conclusion

- Les dernières modifications d'EoleSSO et de l'application Edispatcher permettent de résoudre les problèmes d'affectations multiples pour les parents et enseignants.
- Seshat permet de constituer un hub de fédération pouvant répondre à une grande partie des cas d'utilisation dans le cadre d'un PIA et d'un ENT.
- Une étude est actuellement en cours pour porter EoleSSO sur le serveur authentic2 et résoudre certains problèmes d'instabilité constatés lors de l'utilisateur du mode OTP.

Merci de votre attention

- Seshat
 - Documentation des modules : <http://eoleng.ac-dijon.fr/documentations/>
- EoleDispatcher
 - Projet : <http://dev-eole.ac-dijon.fr/projects/eole-dispatcher>
 - Documentation : <http://dev-eole.ac-dijon.fr/projects/eole-dispatcher/wiki>
- EoleSSO
 - Projet : <http://dev-eole.ac-dijon.fr/projects/eole-sso>
 - Documentation : <http://eoleng.ac-dijon.fr/documentations/old/EoleSSO/>
- Authentic 2
 - <http://www.entrouvert.com/identite-numerique/authentic-2/>
- Mutualisation Envole :
 - <http://envole.ac-dijon.fr>

Licence

- Documentation distribuée sous la licence « Creative Commons by-nc-sa 2.0-fr »

<http://creativecommons.org/licenses/by-nc-sa/2.0/fr/>