Séminaire EOLE
Dijon
23-24 Octobre 2008

Eole SSO

Sommaire

- Présentation du projet
- Protocoles supportés
- Fonctionnalités spécifiques
- Expérimentations
- Intégration dans Eole-2.2
- Evolutions

Présentation du projet

- Motivations
  - Single Sign On : saisie de mot de passe unique.
  - Fédérer l'authentification d'un ensemble d'applications.
  - Maîtrise du produit pour son adaptation en fonction des besoins et de l'évolution du système d'information.
- Choix
  - Développement en python / framework TwistedMatrix.
  - Support de plusieurs protocoles pour faciliter l'intégration des applications.
  - Guichet d'authentification au niveau de l'établissement.

Protocoles supportés

- CAS 2
  - Support du protocole CAS 1 ou 2
  - Ajout de la gestion du mode proxy (cas 2 uniquement)
- OpenID 2.0
  - Support de l'authentification par le protocole OpenID 2
  - Extension Eole permettant la communication d'attributs
- SAML 2
  - Support de l'authentification en mode Idp initiated
  - Support du single Logout (sous certaines conditions)

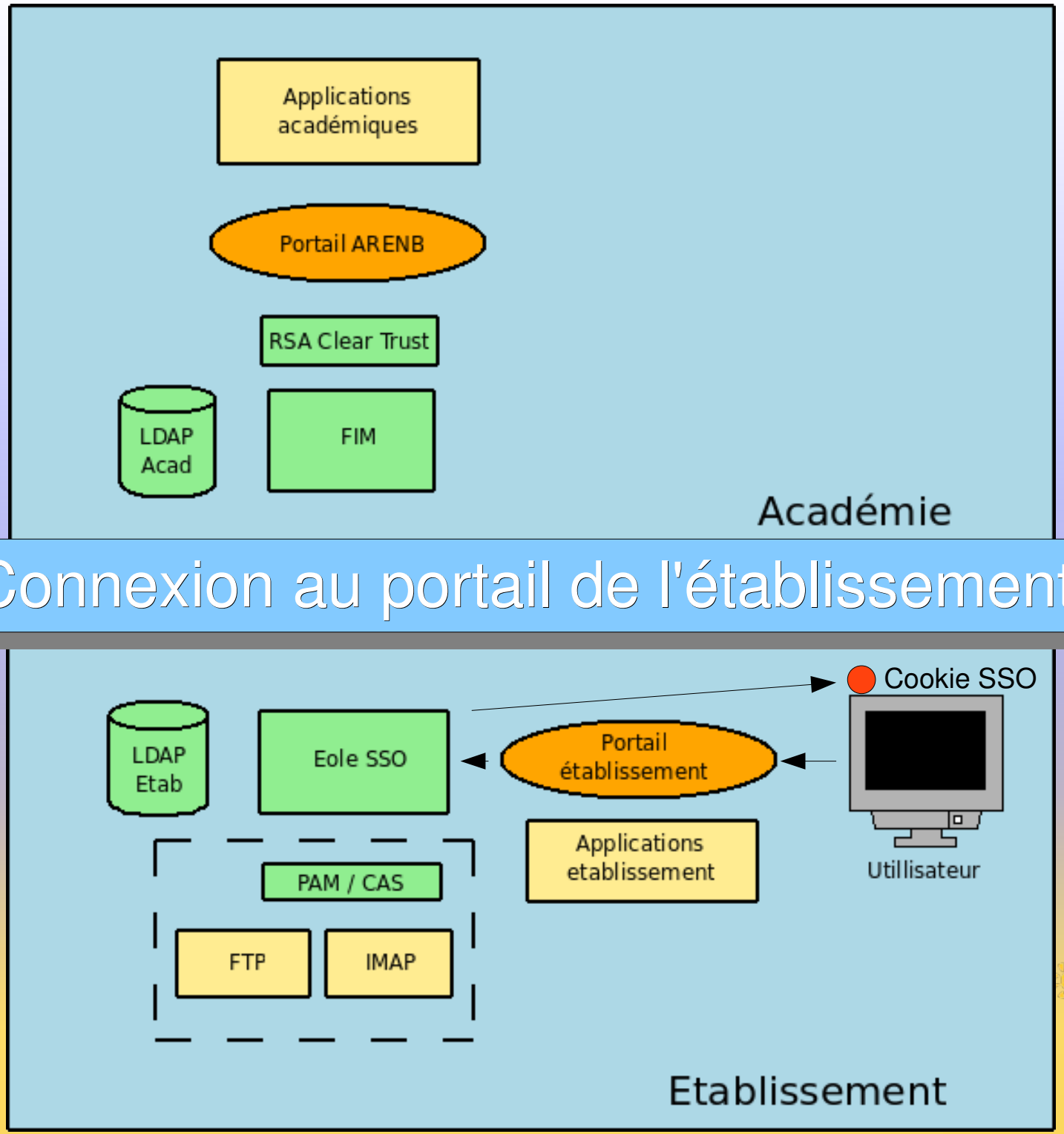
Fonctionnalités spécifiques

- Gestion d'un serveur parent
  - Possibilité de remonter sur un deuxième serveur Eole-SSO pour authentifier l'utilisateur (par ex au niveau académique).
- Ajout / Filtrage d'attributs calculés
  - Personnalisation des données renvoyées par le serveur (ex : calcul d'un profil utilisateur en fonction des attributs récupérés sur un serveur LDAP).
  - Définition d'applications en fonction de leur url, et choix des attributs à renvoyer à celles-ci.
- Client phpCAS modifié
  - Modification de la librairie pour gérer l'envoi d'attributs.

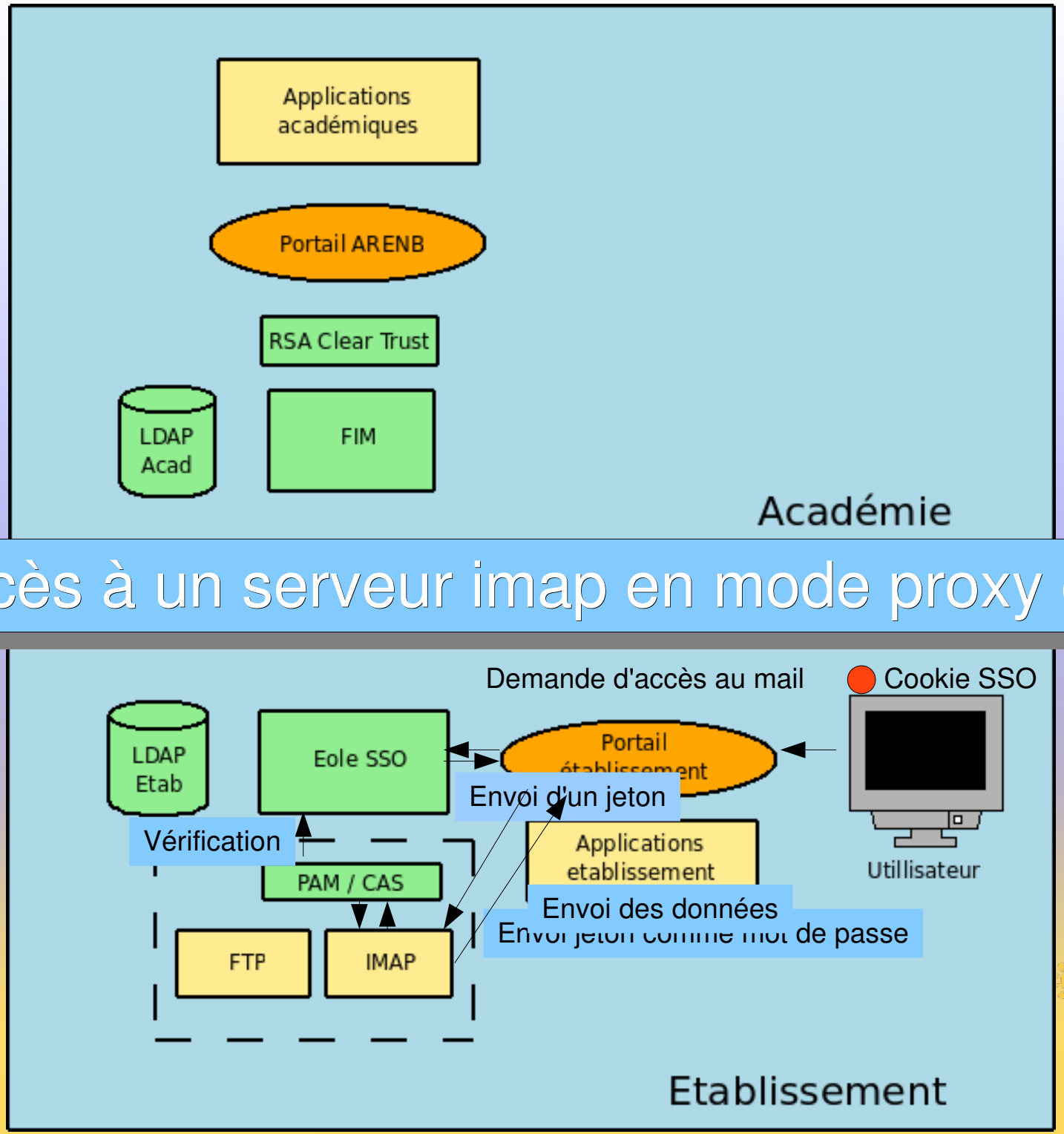
Expérimentations

- CASification d'applications PHP
  - Tests réalisés sur les applications gepi, grr, cartable en ligne, ...
- Accès à des services non web en mode proxy
  - Accès à imap via Squirrelmail
  - Accès ftp via WebShare
- Expérimentation SAML2
  - Accès au portail ARENB par l'intermédiaire de FIM
  - Tests avec la librairie SimpleSamlPHP

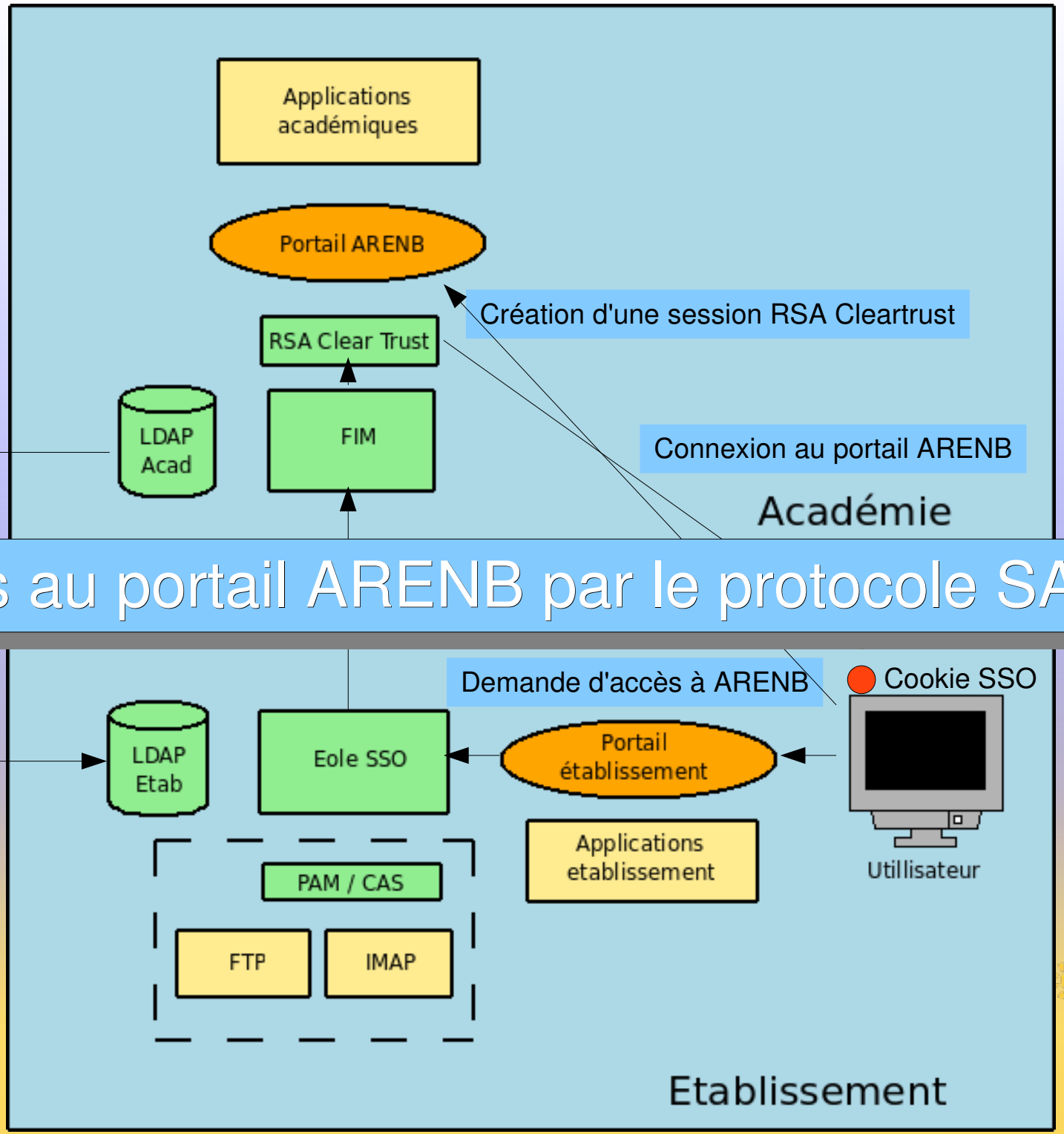
Connexion au portail de l'établissement



Accès à un serveur imap en mode proxy cas



Accès au portail ARENB par le protocole SAML



Intégration dans Eole-2.2

- Utilisation standard
  - Activation du service eole-sso dans gen_config
  - Utilisation du service sso dans l'ead2
- Scribe 2.2 : Application pré configurées
  - Choix dans gen_config : utilisation du service sso pour les applications du serveur.
  - Active automatiquement l'authentification unique sur les applications web et les services ftp et imap

Evolutions/Développements

- Developpement
  - Consolidation du code et des cinématiques des protocoles
- Intégration
  - Librairies et de documents pour faciliter l'adaptation d'applications dans différents langages.
  - Mise à jour des annuaires établissement pour permettre la jointure avec les annuaires académiques.
- Saml
  - Gérer le traitement de requêtes d'authentification.
  - Mise en place d'une pki (académique/Agriates ?) pour sécuriser les échanges et faciliter le déploiement.

Informations utiles

- Page wiki Eole SSO : http:/eole.orion.education.fr/wiki/index.php/EoleSSO
- Page sur l'expérimentation SSO/FIM : http:/eole.orion.education.fr/wiki/index.php/EoleSSOFim
- Le projet CAS : http://www.ja-sig.org/products/cas/
- Oasis / Spécifications SAML : http://www.oasis-open.org/specs/index.php#saml
- OpenID : http://openid.net http://www.openidfrance.fr

Merci de votre attention