Séminaire EOLE
Dijon
23/24 novembre 2011

Architecture Envole/EoleSSO

Sommaire

- Présentation du socle Envole
- EoleSSO : modes de fonctionnement
- Fédération et gestion des annuaires
- Accès aux services académiques / Télé services
- Choix du mode d'accès
- ENT Réunion
- Evolutions
- Informations utiles

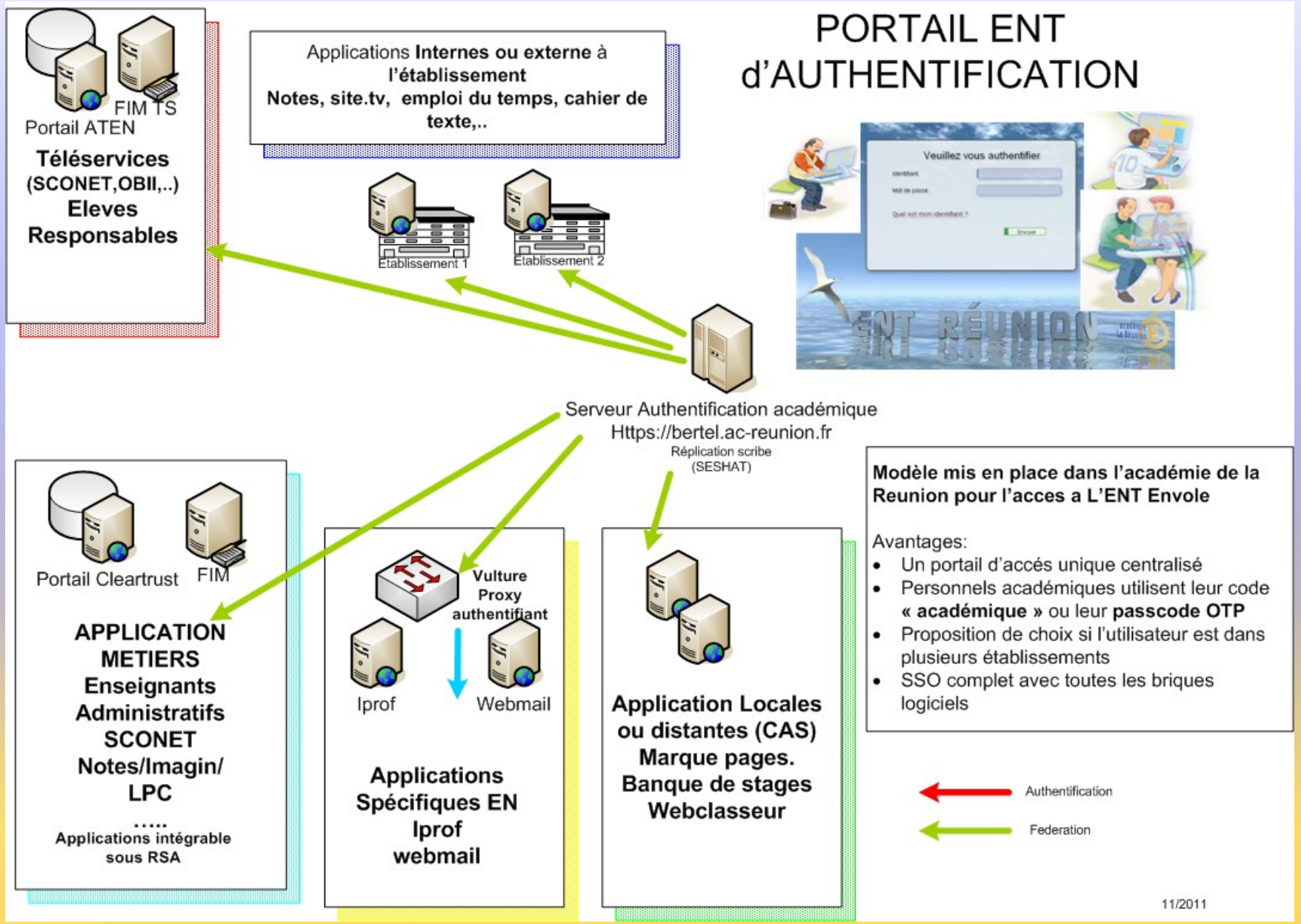
Le socle Envole

- Portail Posh
  - Portail web 2.0
  - Intégration de services hétérogènes dans une interface
  - Personnalisable par l'utilisateur
  - Authentification centralisée grâce au service SSO
- Serveur EoleSSO
  - Support de plusieurs protocoles pour faciliter l'intégration des applications (CAS / SAML).
  - Fonctions de contrôle des attributs transmis
  - Possibilité de fédération avec d'autres produits grâce au protocole SAML

Modes de fonctionnement

- Fournisseur d'identité
  - Vérifie l'identité de l'utilisateur
  - Passerelle vers les services protégés par d'autres systèmes d'authentification en académie (RSA/FIM), ou vers des applications/portails d'éditeurs tiers (Universalis-edu, CNS, ...).
- Fournisseur de Service
  - Protection de l'accès aux applications locales (ex: Scribe en établissement/Seshat en académie);
  - Fédération avec des fournisseurs d'identité à travers le protocole SAMLv2 (après échange de méta-données).

Exemple de mise en œuvre



Annuaires et fédération

- Gestion des annuaires
  - Un annuaire par établissement (Scribe)
  - Annuaire consolidé des établissements (Seshat)
  - Annuaires externes configurables (Académique, ...)
- Réplication / gestion des identifiants
  - Mise en place de la réplication entre Scribe et Seshat
  - Fédération entre Scribe et Seshat (FederationKey)
  - Gestion des homonymes sur la mire EoleSSO (proposition d'un choix à l'utilisateur)

Accès aux services académiques

- Fédération avec FIM/RSA
  - Utilisation du protocole SAML
  - Lien de confiance établi par échange de métadonnées
- Authentification par clé OTP
  - Vérification auprès du serveur RSA via un module PAM (l'adresse de Seshat doit être autorisée comme agent dans la configuration du serveur RSA)
  - Mode de gestion des identifiants OTP gérables pour chaque annuaire (désactivés, identiques à l'identifiant annuaire, configurables par l'utilisateur)

Accès aux télé services

- Gestion du vecteur de fédération
  - Fédération de type SAML avec un vecteur composé (FrEduVecteur, cf annexe d'interconnexion ENT/TS)
  - Vecteur calculé et stocké sur le serveur Seshat (procédure journalière).
  - Récupéré par EoleSSO en tant qu'attribut calculé.
- Pré-requis
  - Annuaires Scribe répliqués sur Seshat.
  - Import des données depuis AAF (attribut eleveId nécessaire pour retrouver les élèves liés aux responsables)

Choix du mode d'accès

- Authentification en établissement (Scribe)
  - Accès limité aux applications académiques (pas d'accès OTP)
- Authentification en académie (Seshat)
  - Aide à la connexion pour l'utilisateur et redirection automatique vers l'ENT établissement (page frontale et dispatcher sur Seshat) ;
  - Comportement après la déconnexion de l'ENT (établissement) configurable dans le cas d'une fédération depuis Seshat.

Choix du mode d'accès

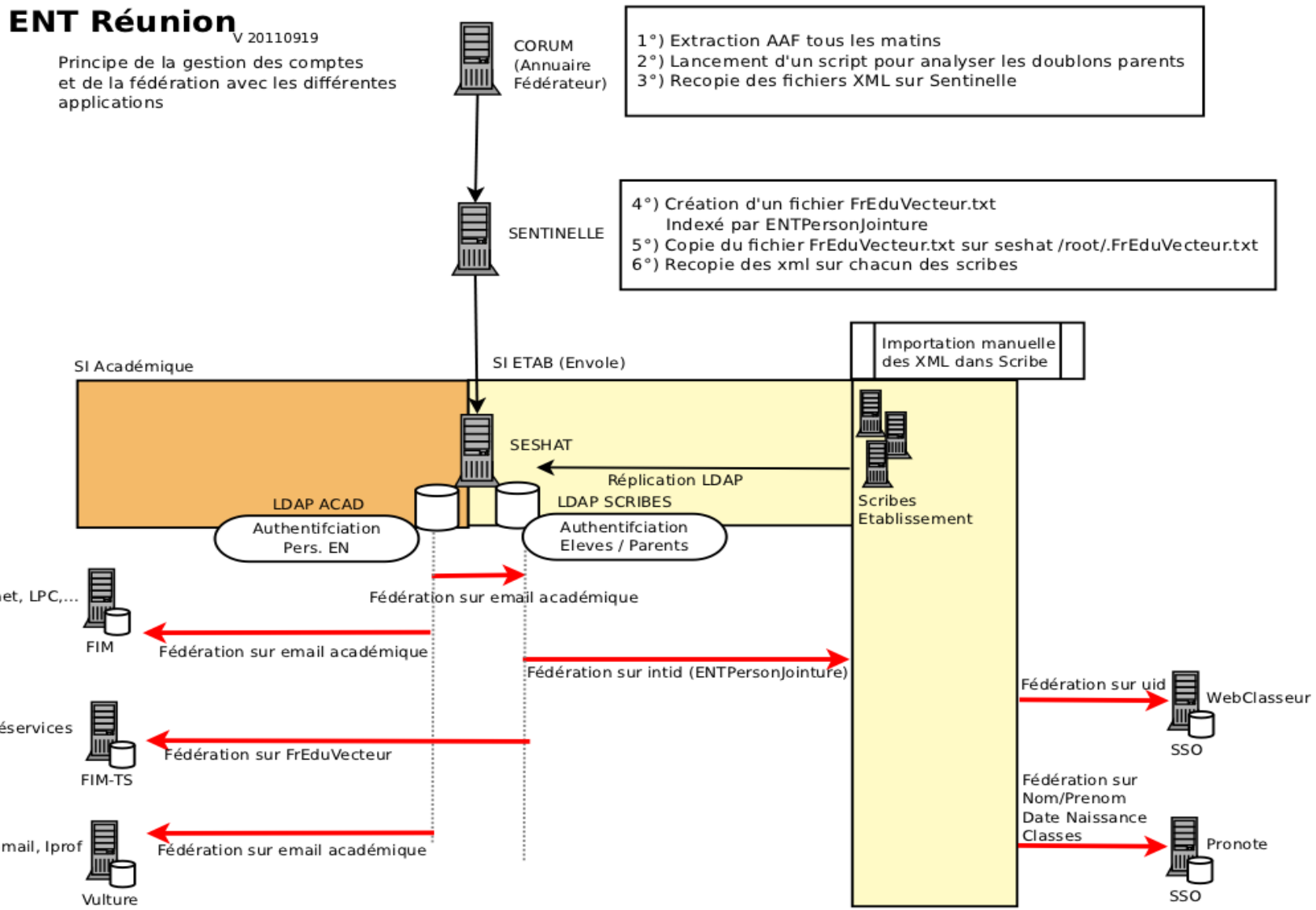
- Configuration des associations
  - /usr/share/sso/attribute_sets/associations.ini (permet de définir des options différentes pour chaque fournisseur d'identité reconnu).

```
[urn:fi:ac-monacad:et-seshat.ac-monacad:1.0]
# accepte les assertions provenant de seshat
allow_idp = true
# autorise seshat à initier la connexion
allow_idp_initiated = false
# utilise un jeu d'attribut particulier
attribute_set = jeu_perso_1
# service par défaut en mode fournisseur de service
default_service = https://etab.monacad/posh
# url ou rediriger après une déconnexion du portail établissement
default_logout_url = https://etab.monacad:8443/discovery?idp_ident=seshat



~
~
~
~
~
~
~
"/tmp/test.ini" 14L, 488C écrit(s)                    14,0-1        Tout
```

ENT Réunion

- Gestion des homonymes
- Dispatcher sur Seshat (Affectations multiples)
- Nouveau plugin « desktop »
- Fédération des services académiques et des télé services
- Point sur le déploiement
- Site dédié pour la connexion ENT.
- Statistiques consolidées sur les usages

ENT Réunion


ENT Réunion
V 20110919
Principe de la gestion des comptes et de la fédération avec les différentes applications
CORUM (Annuaire Fédérateur)
1°) Extraction AAF tous les matins
2°) Lancement d'un script pour analyser les doublons parents
3°) Recopie des fichiers XML sur Sentinelle
SENTINELLE
4°) Création d'un fichier FrEduVecteur.txt
Indexé par ENTPersonJointure
5°) Copie du fichier FrEduVecteur.txt sur seshat /root/.FrEduVecteur.txt
6°) Recopie des xml sur chacun des scribes
SI Académique
SI ETAB (Envole)
Importation manuelle des XML dans Scribe
SESHAT
Réplication LDAP
LDAP ACAD
Authentifciation Pers. EN
LDAP SCRIBES
Authentifciation Eleves / Parents
Scribes Etablissement
Sconet, LPC,...
FIM
Fédération sur email académique
Fédération sur email académique
Fédération sur intid (ENTPersonJointure)
Fédération sur uid
WebClasseur
SSO
Téléservices
FIM-TS
Fédération sur FrEduVecteur
Fédération sur Nom/Prenom Date Naissance Classes
Pronote
SSO
Webmail, Iprof
Vulture
Fédération sur email académique

Evolutions

- Nouvelle version du portail (Posh 3) sur Eole 2.3.
- Utilisation de la libraire Lasso (implémentation libre des standards Liberty Alliance, conforme SAML v2), en cours d'intégration.
- Intégration des adaptations faites à la Réunion.
- Annuaire global Seshat (import AAF).

Informations utiles

- Documentation : http://eoleng.ac-dijon.fr/documentations/EoleSSO/
- EoleSSO/OTP : ftp://eoleng.ac-dijon.fr/pub/Documentations/presentations/octobre2010/eole_sso.pdf
- EoleSSO/SAML : ftp://eoleng.ac-dijon.fr/pub/Documentations/presentations/Octobre2009/eole_sso.pdf
- Oasis / Spécifications SAML : http://www.oasis-open.org/specs/index.php#saml
- Lasso : http://lasso.entrouvert.org

Merci de votre attention