Séminaire EOLE
Dijon
19-20 Octobre 2010

Eole SSO

Sommaire

- Présentation du projet
- Modes de fonctionnement
- Schéma type
- Prise en compte de SecurID (OTP)
- Perspectives
- Informations utiles

Présentation du projet

- Motivations
  - Répondre à la problématique de l'authentification des applications d'un portail (Saisie de mot de passe unique);
  - Maîtrise du produit pour son adaptation en fonction des besoins et de l'évolution du système d'information.
- Fonctionnalités
  - Support de plusieurs protocoles (CAS / SAML / OpenID) pour faciliter l'intégration des applications et la fédération avec des partenaires tiers;
  - Fonctions de contrôle des attributs transmis;
  - Intégration d'une authentification forte par clé OTP.

Modes de fonctionnement

- Fournisseur d'identité
  - Passerelle vers les services protégés par d'autres systèmes d'authentification en académie (RSA/FIM);
  - Gestion de l'authentification auprès d'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 d'autres fournisseurs d'identité à travers le protocole SAMLv2 (après échange de méta-données).

Schéma type

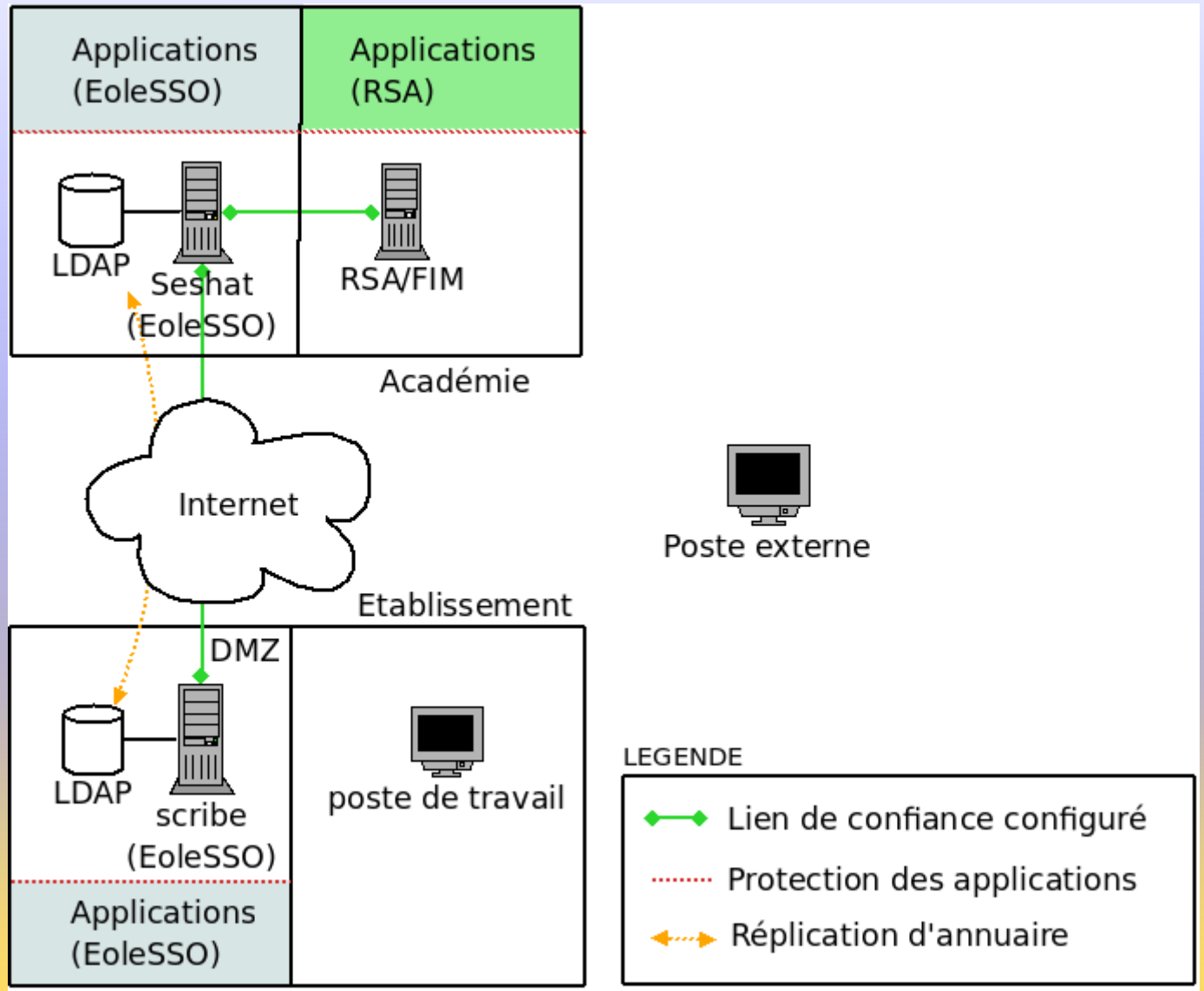

Applications (EoleSSO)
Applications (RSA)
LDAP
Seshat (EoleSSO)
RSA/FIM
Académie
Internet
Poste externe
Etablissement
DMZ
LDAP
scribe (EoleSSO)
poste de travail
Applications (EoleSSO)
LEGENDE
Lien de confiance configuré
Protection des applications
Réplication d'annuaire

Schéma type (session locale)

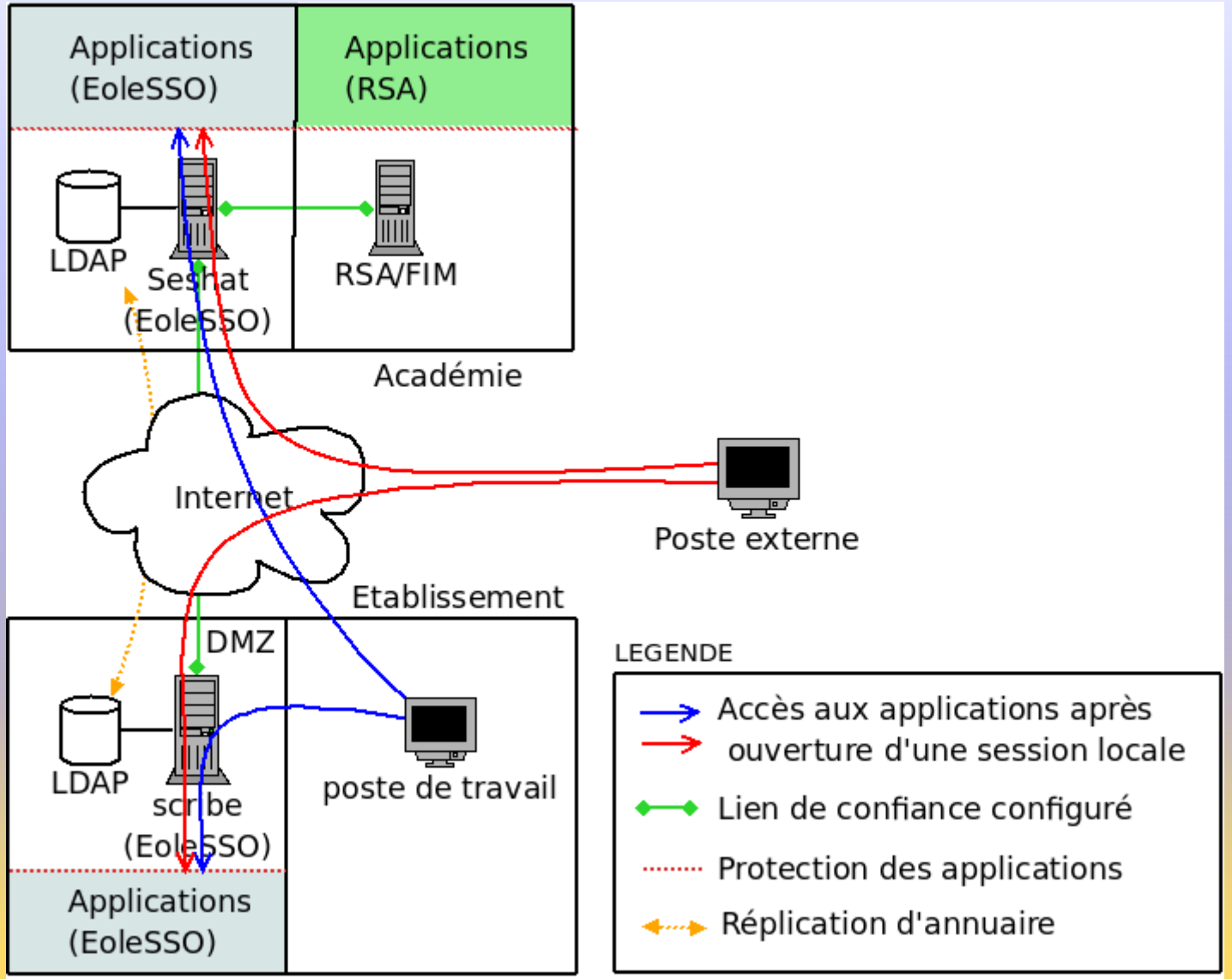
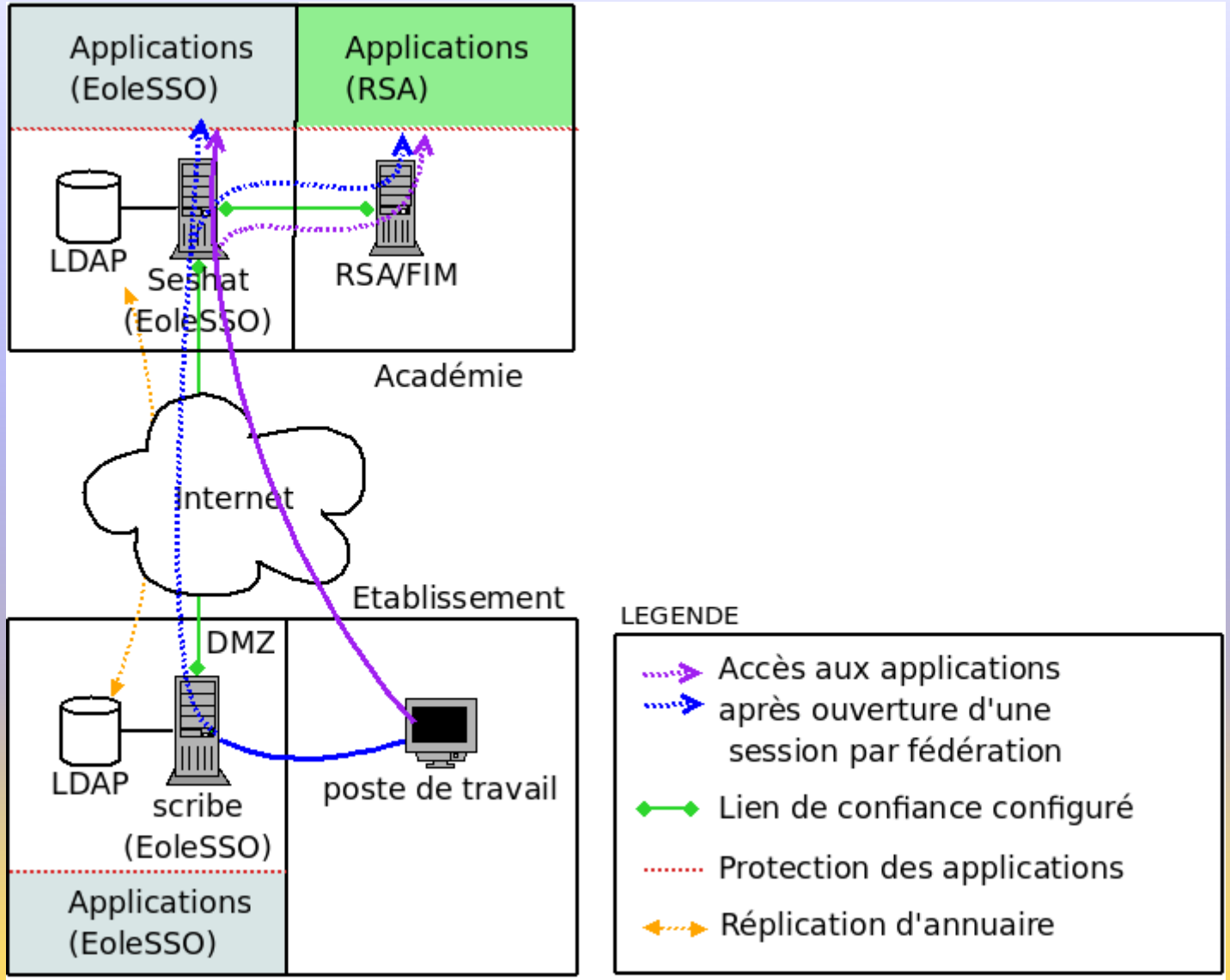


Schéma type (fédération)

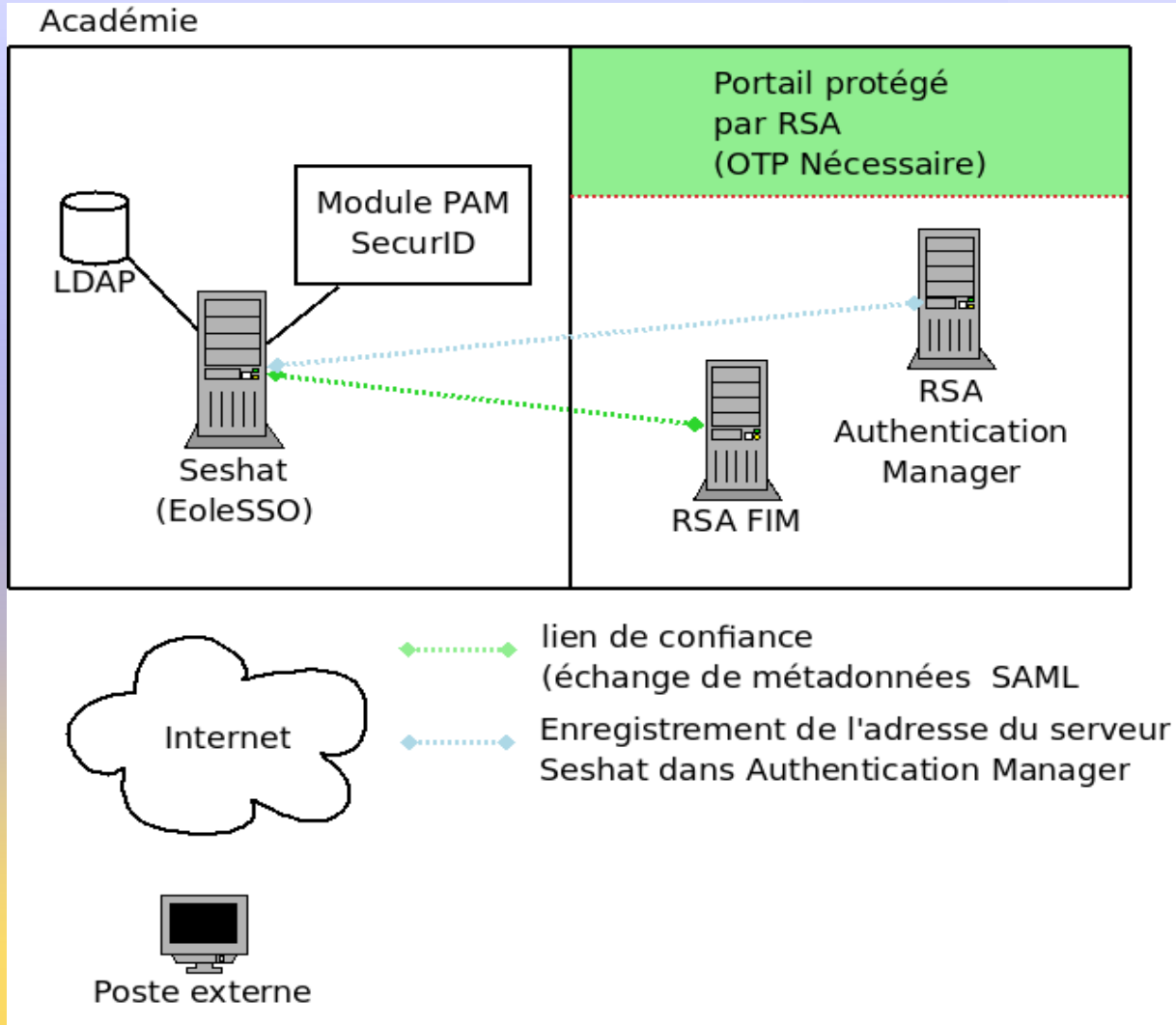


Prise en compte de SecurID (OTP)

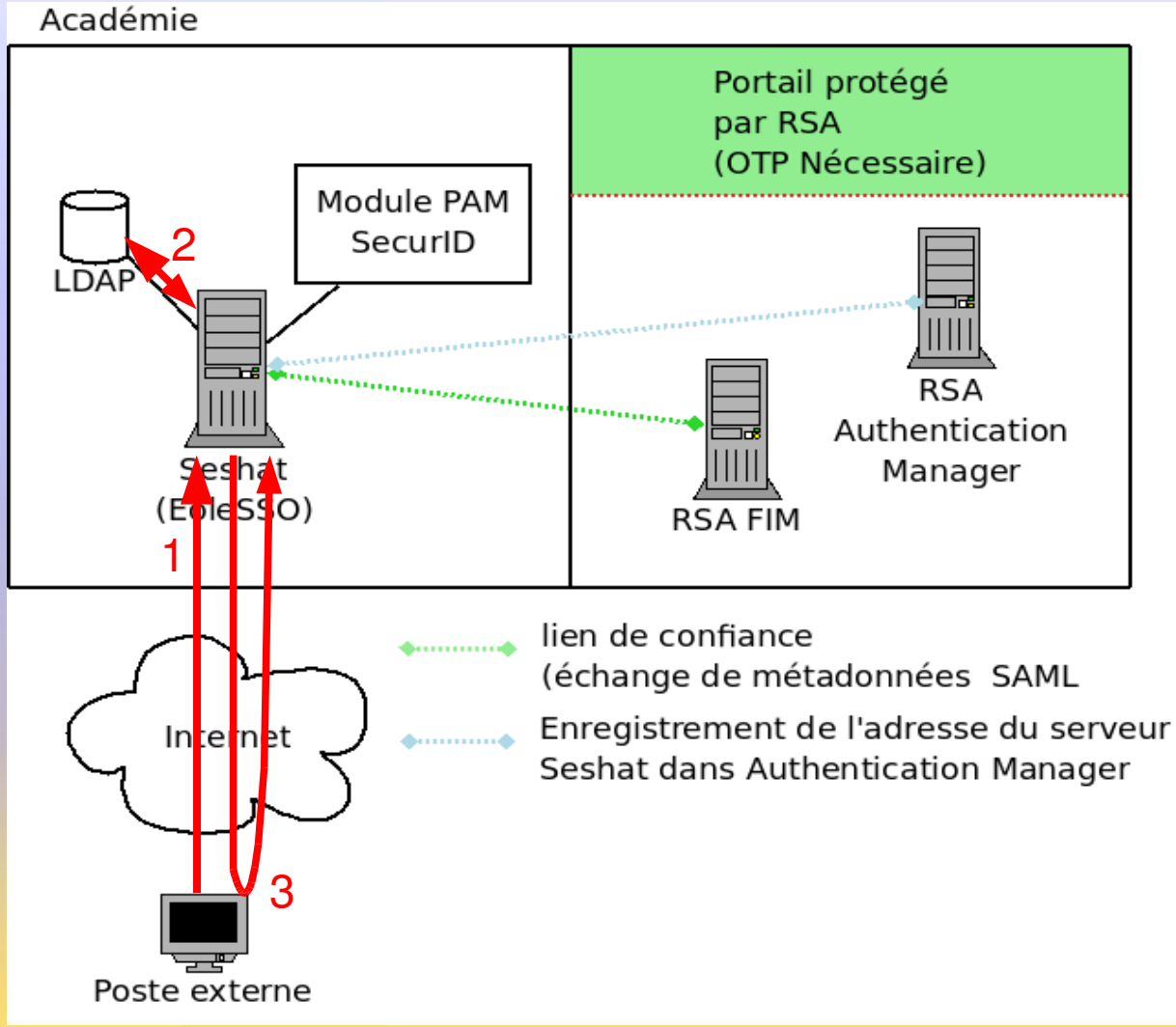
- Vérification du mot de passe OTP à l'ouverture de la session SSO;
- Transmission du niveau d'authentification (Mot de Passe classique ou OTP) lors de l'émission d'assertions SAML en tant que fournisseur d'identité;
- Nécessite d'enregistrer sur le serveur RSA l'adresse de chaque serveur autorisé à vérifier l'authentification (notion d'agent).

Prise en compte de SecurID (OTP)

- Configuration préalable
  - Installation sur Seshat du module PAM SecurID (+ fichier sdconf.rec du serveur OTP);
  - Enregistrement de l'adresse de Seshat dans la liste des sondes autorisées;
  - Ajouter SecurID dans la politique associée (FIMConfig).

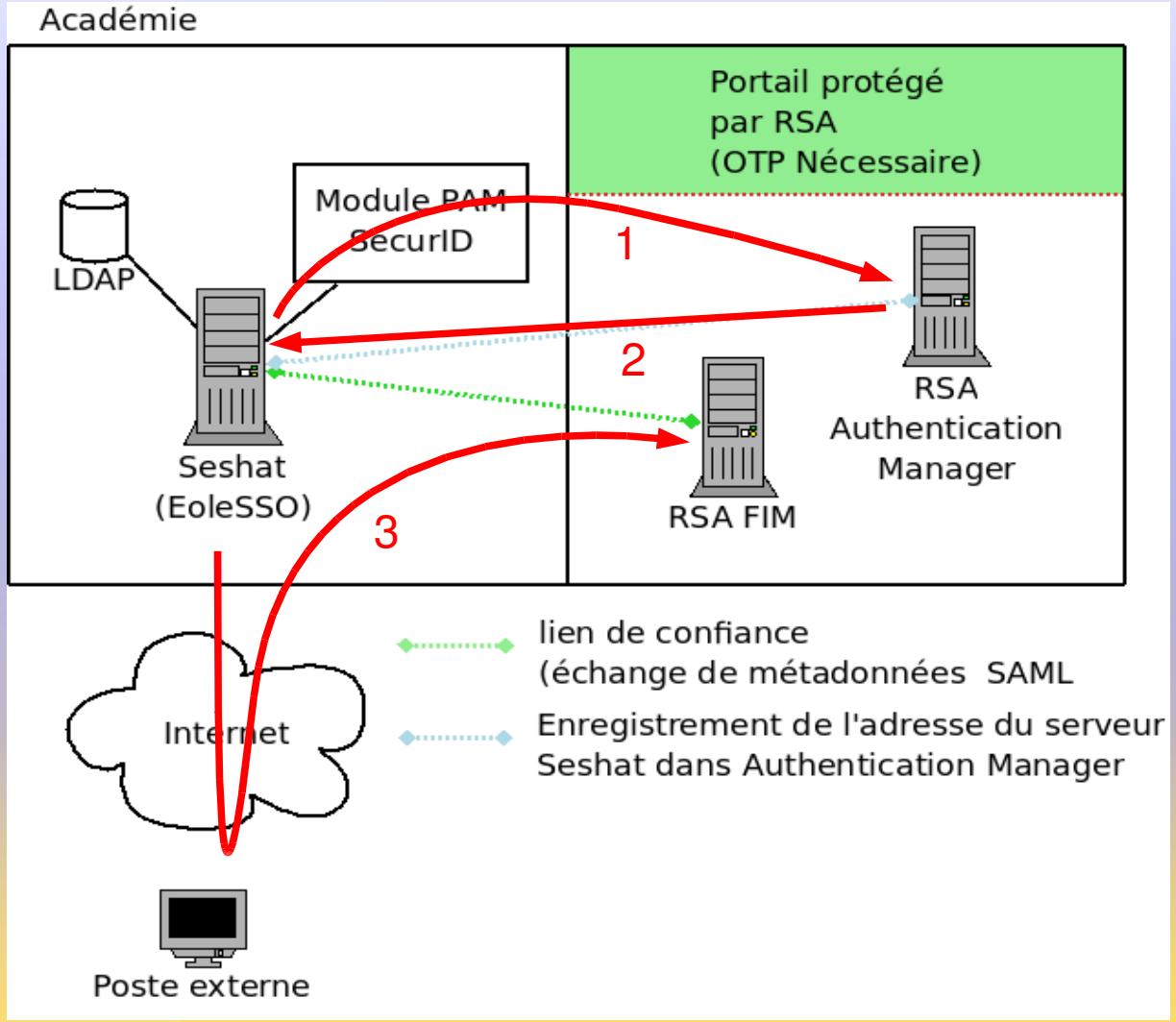


Prise en compte de SecurID (OTP)



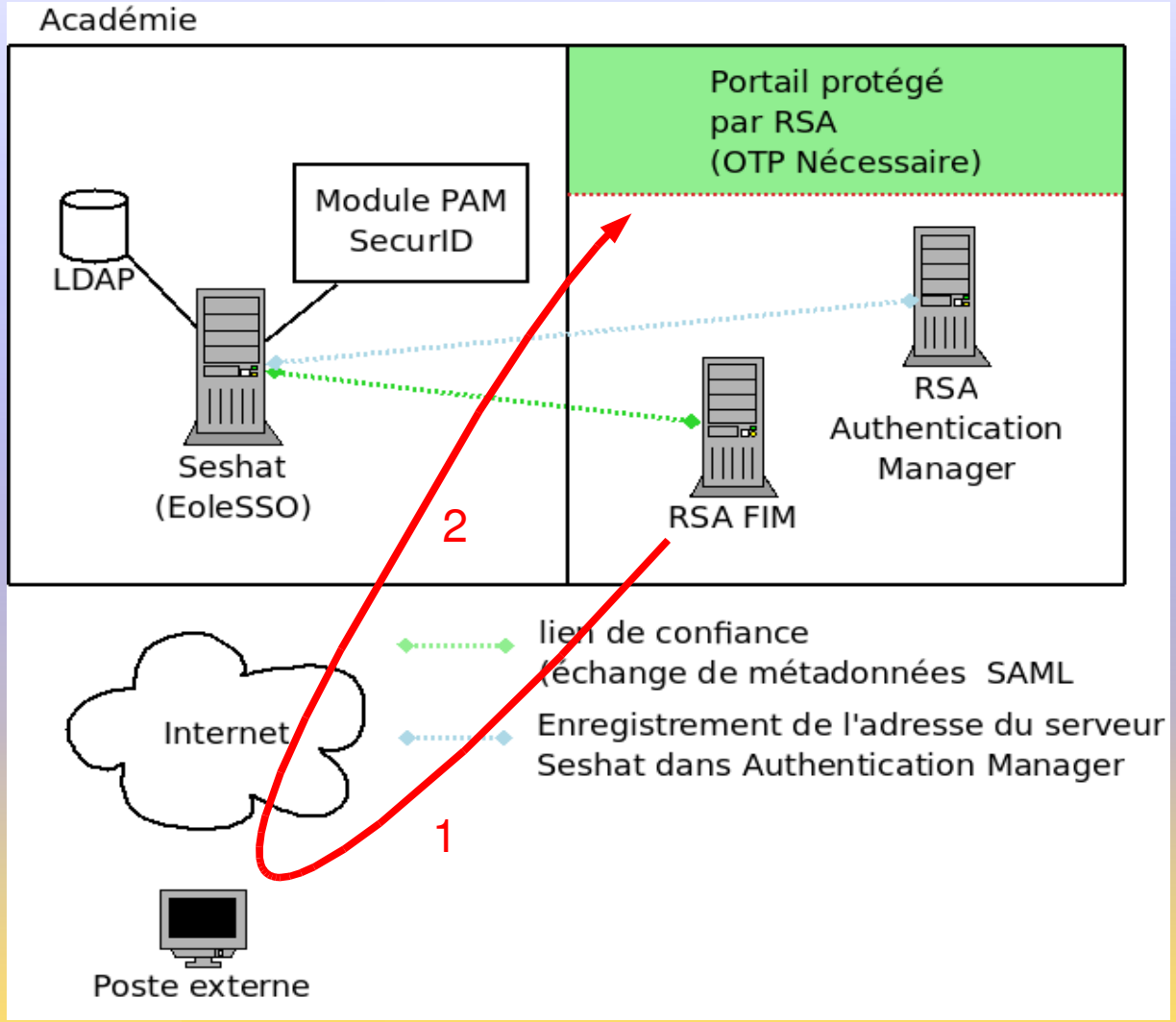
- Demande auprès du service EoleSSO
  1. Saisie login/mot de passe (ldap local) + mot de passe OTP;
  2. Validation des identifiants ldap;
  3. Création session SSO (cookie) et redirection sur la procédure SecurID.

Prise en compte de SecurID (OTP)



- Validation des identifiants OTP
  1. Envoi du login OTP + mot de passe fourni au module PAM;
  2. Si le résultat est valide, on modifie le niveau de sécurité de la session;
  3. Redirection sur FIM avec une assertion spécifique.

Prise en compte de SecurID (OTP)



- Accès à la ressource
  1. FIM vérifie l'assertion et crée une session (cookie valide sur le domaine académique);
  2. L'utilisateur est redirigé sur le portail (adresse passée à FIM en paramètre avec l'assertion).

Prise en compte de SecurID (OTP)

- Impact sur les assertions SAML

```
−<ns1:AuthnStatement AuthnInstant="2010-10-18T09:24:12Z" SessionIndex="[redacted]-
7d519f7737a514a0307099b30230319f9c9a614df7dfb0a7579c67bb">
  <ns1:SubjectLocality Address="[redacted]" DNSName="[redacted]"/>
 −<ns1:AuthnContext>
  −<ns1:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </ns1:AuthnContextClassRef>
  </ns1:AuthnContext>
</ns1:AuthnStatement>
```

```
−<ns1:AuthnStatement AuthnInstant="2010-10-18T09:29:58Z" SessionIndex="ST-[redacted]-
02070ea857f77ece1ea10e4b30428bf6d1e387f74801953f322d8800">
  <ns1:SubjectLocality Address="[redacted]" DNSName="[redacted]"/>
 −<ns1:AuthnContext>
  −<ns1:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
    </ns1:AuthnContextClassRef>
  </ns1:AuthnContext>
</ns1:AuthnStatement>
```

Perspectives

- OTP: gestion des identifiants (enregistrement de l'identifiant OTP par l'utilisateur à la première utilisation).
- Gérer le cas où l'accès à OTP est déployé sur un serveur SSO distant (ex: Scribe -> Seshat).
- Améliorer la gestion de la configuration.
- Correction de la gestion d'OpenID ? (pas de demandes actuellement).

Informations utiles

- Documentation: http:/eoleng.ac-dijon.fr/documentations/EoleSSO/
- 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