Service Technologies Systèmes Information

ENVOLE 1.5

Calendrier Envole

Service Technologies Systèmes Information

RSA FIM

Modification du SSO EOLE 2.2 (PAM-CAS, CT
EOLE V 2.2 RC

RSA FIM + module additionnel

Packaging et préparation de la diffusion

EOLE V 2.2 intégrant EnvOLE 1.5

1 septembre 2008
EOLE V 2.1

Dev. Version 1.5

1 avril 2008
V 1.13
sur EOLE V 2.0

10 octobre 2008
V 1.15 RC
sur EOLE V 2.0

Prise en compte du SSO EOLE 2,2 (PAM-CAS) et cassification des services de base

Premier rapport d'audit sécurité (2/10), lancement des corrections

15/12

Version 1.15 Envole

- SSO Gibii et Mathenpoche, CNS, SiteTV, KNE...
- Statistiques d'utilisation
- Interface d'administration :
  - Sauvegarde bases et fichiers, effacement des bases
  - Mise en ligne de la charte d'utilisation
  - Saisie simplifiée des liens vers les ressources
  - Bascule vers les comptes "meta_"
  - ...
- Véritable gestionnaire de fichier (ergonomie, diaporama, balladodiffusion, commentaires...)
  - Webshare à la place de SmbWebClient
- Webcalendar : affichage retravaillé, améliorations
- Cahier de texte en ligne : version 3.0.7
- GRR : version 1.9.4 (ou 1.9.5 si disponible)
- Multi-blog : WordPress Mu version 1.5 (Wordpress 2.5)

Version 1.5 Envole, EOLE V2.2, RSAFIM +Module additionnel

- Sécurité :
  - Liaison authentification Envole et SSO Académique RSA CT (utilise les fonctionnalité EOLE 2.2 et le module additionnel de RSA FIM en cours de qualification)
  - Liaison authentification Envole et SSO Local (CAS, PAM-CAS..., cassification de tous les services de base : gestion de fichiers, etc...)
  - Audit de sécurité et amélioration consécutives
- Diffusion EOLE :
  - Packaging
  - Prise de connaissance par l'équipe EOLE pour gérer la diffusion auprès des autres académies

Service Technologies Systèmes Information

GESTION IDENTITE DE L EDUCATION NATIONALE

1. Rappels et définitions en matière de gestion des identités et des habilitations
2. Présentation des composants à mettre en place
3. Démarches de mise en œuvre et principes fondamentaux

Que signifie « identité » ?

- L'identité numérique est l'équivoque de l'identité physique dans le monde numérique (système d'information, portail applicatif, etc.), et vice versa.
- Exemples :
  - Personne physique ↔ Login utilisateur
  - Machine ↔ Nom DNS d'un serveur, adresse IP
  - Téléphone ↔ Numéro de téléphone
- L'identification consiste associer une personne physique, un composant ou un élément logiciel à une identité numérique.
- L'identificati[illegible] de faire des actions sur tout ou partie [illegible] système d'information, portail :

Accéder

S'inscrire

Ouvrir des droits

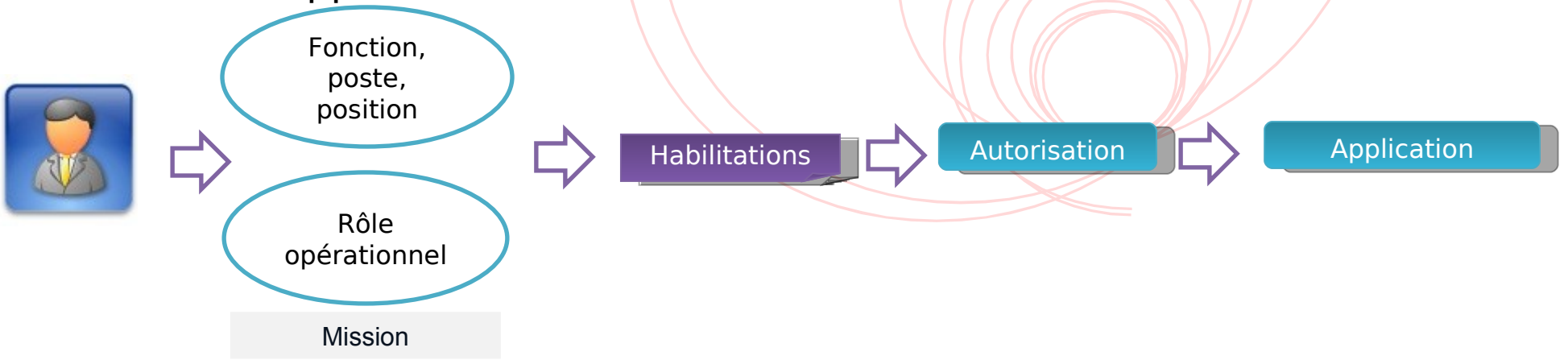
Créer, modifier, désactiver, révoquer, supprimer

S'engager

Signer

Qu'entend-on par « habilitation »?

- **Les habilitations correspondent aux droits d'accès associés à un utilisateur.**
- **Elles peuvent concerner une ou plusieurs ressources**
- **Elles sont définies en fonction :**
  - Du contexte de l'utilisateur
  - De sa fonction, son poste dans l'organisation
  - Opérationnel (Exemple : le RSSI ou l'administrateur d'une application)



GESTION IDENTITE DE L EDUCATION NATIONALE

1. Rappels et définition en matière de gestion des identités et des habilitations
2. Présentation des composants à mettre en place
3. Démarches de mise en œuvre et principes fondamentaux

Service Technologies Systèmes Information

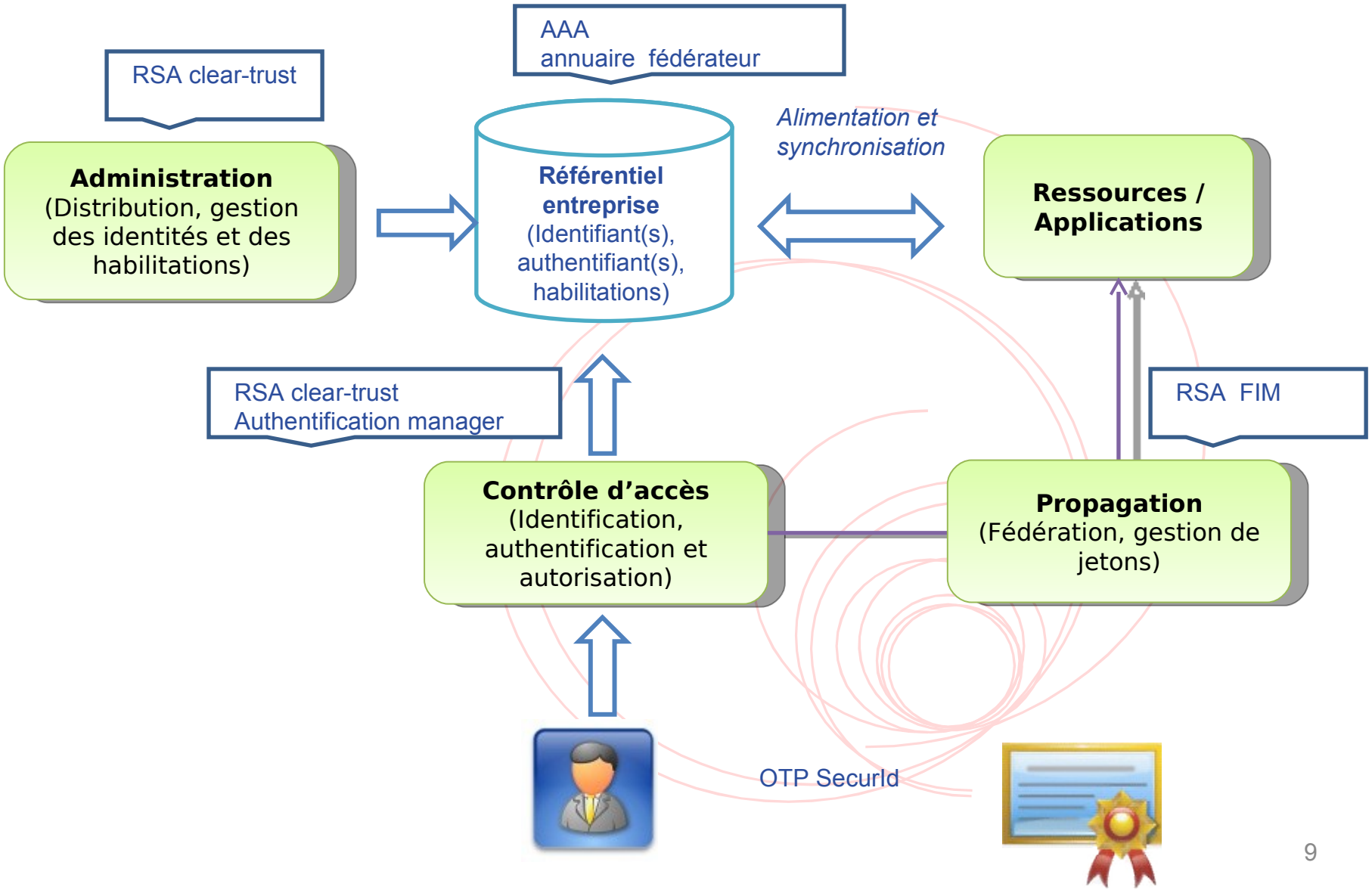
Etat des lieux

- Annuaire (LDAP sun Académique Annuaire Fédérateur)
- RSA Gestion des accès protection url
- Delegce Gestion des autorisations (moteur de délégations)
- Arenb portail d’accès agent. (Généralisation aux applications nationales)
- FIM fédération (Fournisseur d’identité, Fournisseur de Services) Gospel BE1D
- OTP (accès nominatif sécurisé aux applications) BE1D Sconet notes

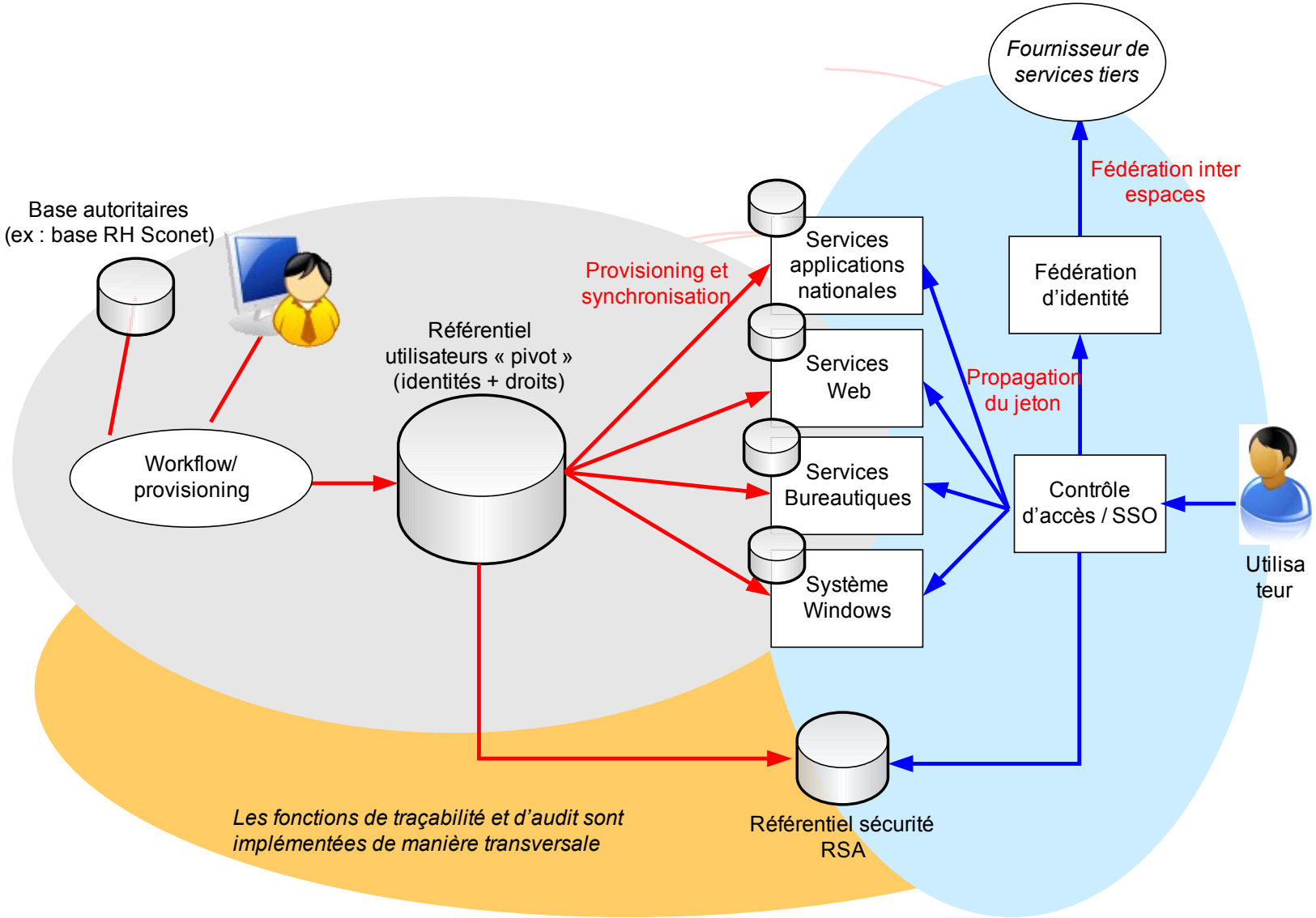
Objectifs d'évolution des infrastructures de gestion des identités et des habilitations

- **Homogénéiser la gestion des identités et des habilitations (travaux en cours PIA)**
  - Contrôle du circuit de gestion du cycle de vie des identités et des habilitations de bout en bout
  - Consolidation des informations
  - Construction d'un référentiel d'entreprise
  - Mise en place d'outils de synchronisation des référentiels du SI
- **Renforcer le contrôle d'accès**
  - Authentification forte (OTP certificats (dématérialisation de documents)
  - Mise en cohérence des habilitations
- **Faciliter l'accès aux application**
  - Mise en place d'un service d'authentification central
  - Mise en place d'un service de gestion de jetons (SSO)
    - Au sein d'un unique espace de confiance (expliquer)
    - Entre plusieurs espace de confiance (Fédération d'identité)

Les composantes nécessaires à la gestion de l'identité et des accès

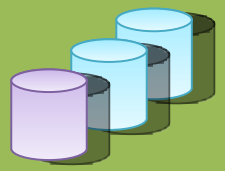


Les différentes démarches



Mise en œuvre d'un référentiel éducation nationale

Bases RH
Base partenaires
Fichiers clients
…



Informations sur la personne (organisationnel)

Alimentation automatisée

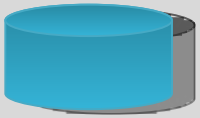
Alimentation manuelle

Référentiel MEN

Alimentation et synchronisation des référentiels applicatifs

Définition et gestion de la politique d'habilitation

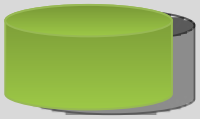
Politique d'habilitation



Messagerie

Windows / Linux

Référentiel sécurité

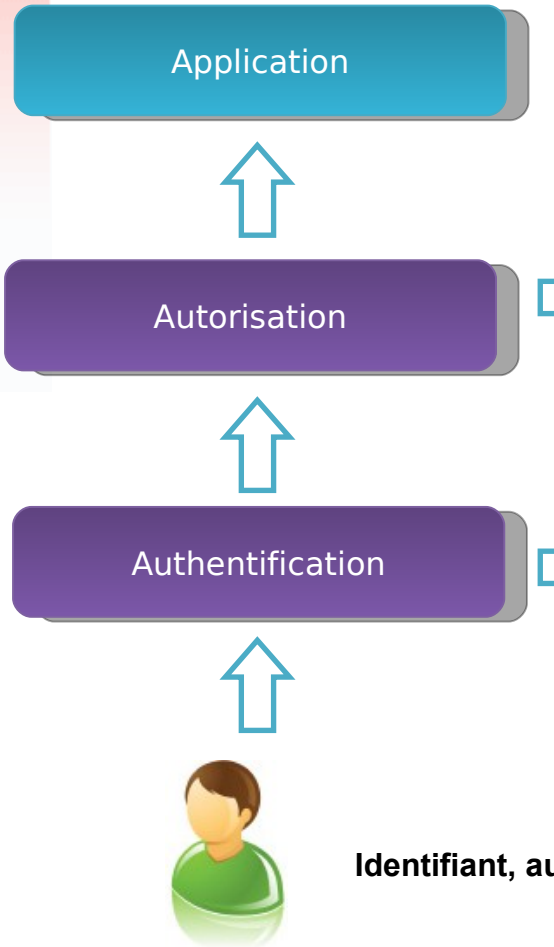


Référentiel applicatif

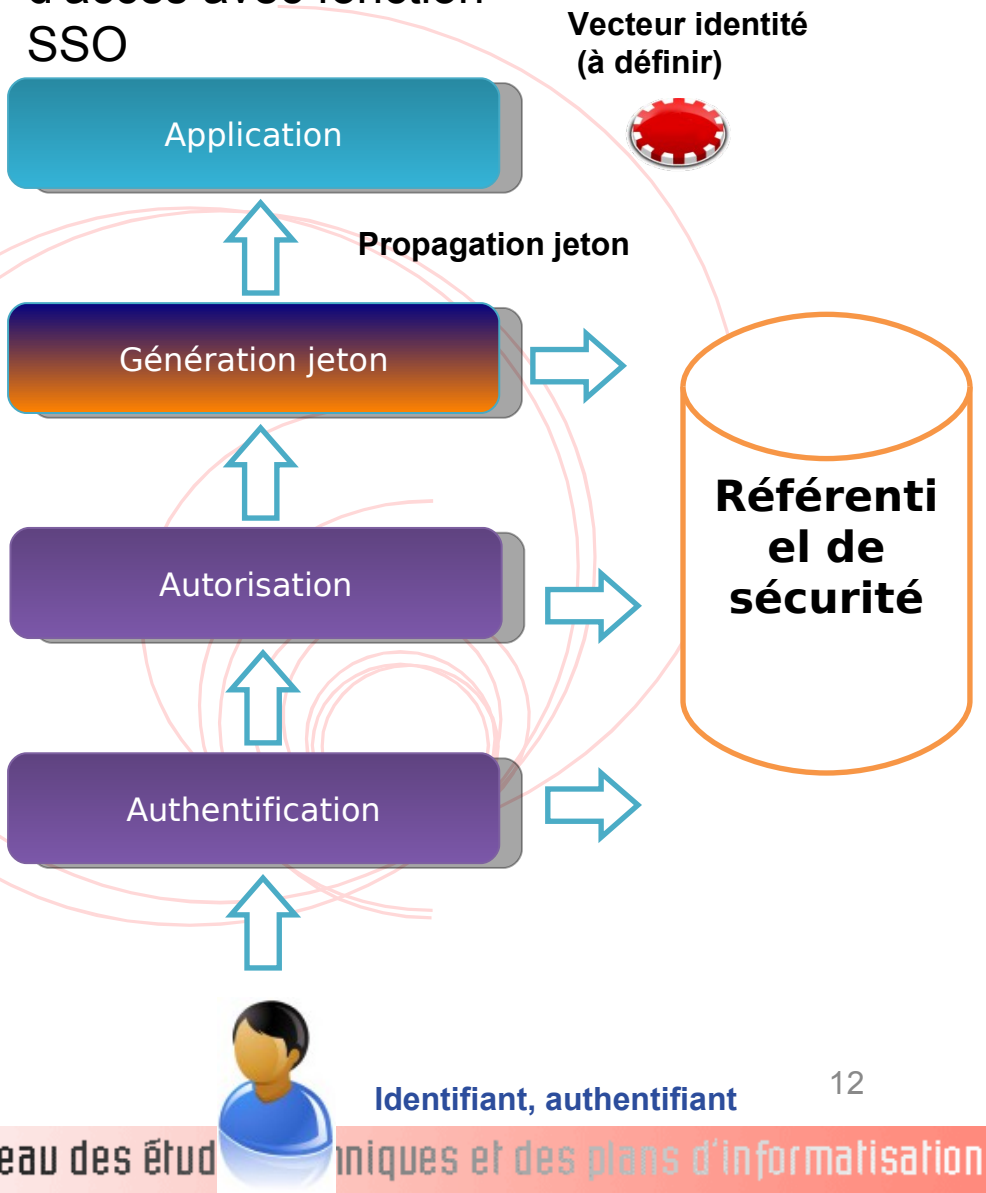
Informations relatives aux comptes (IT)

Mise en œuvre de fonction de contrôle d'accès

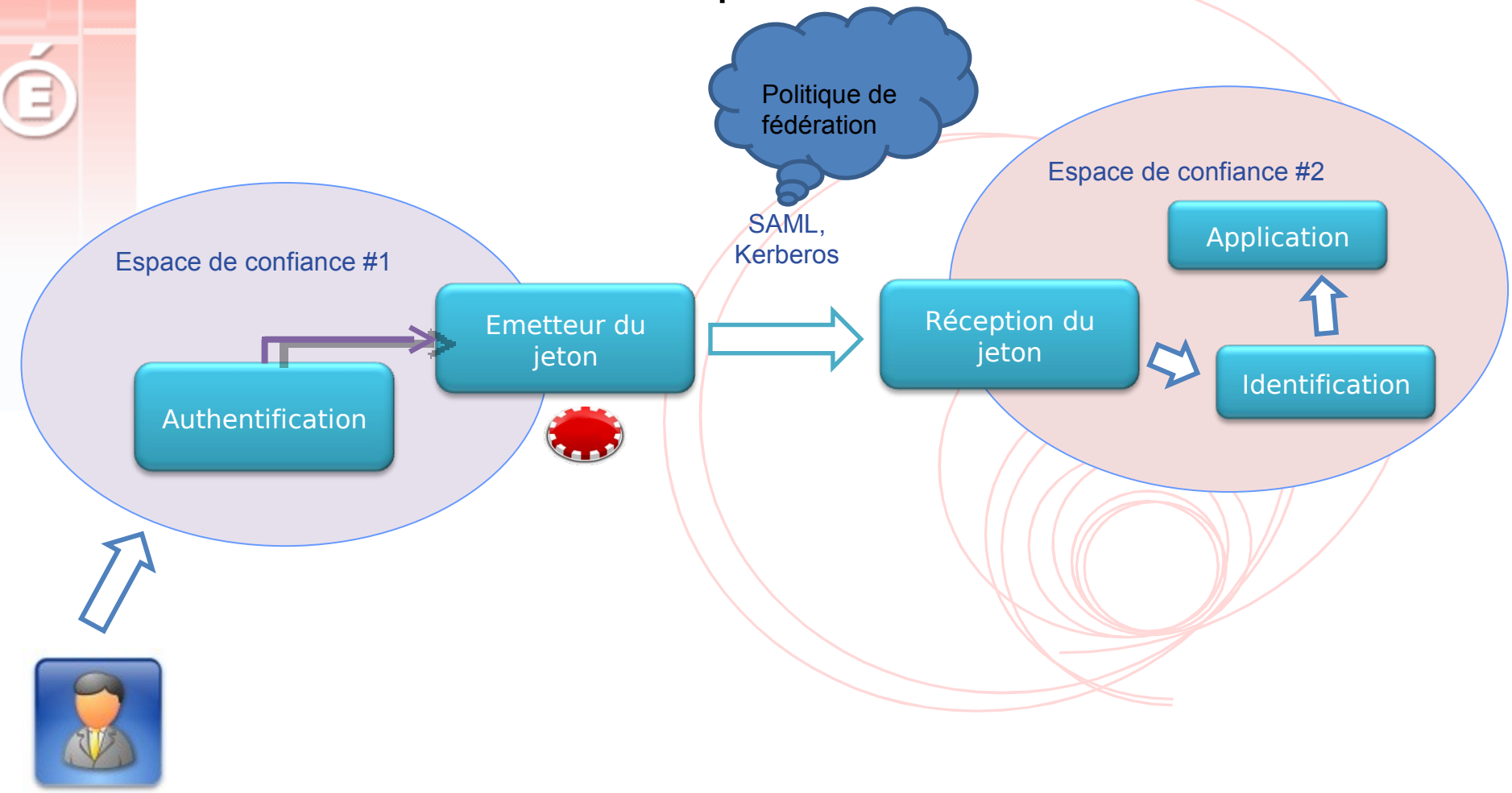
Scénario 1 : Contrôle d'accès traditionnel



Scénario 2 : Contrôle d'accès avec fonction SSO

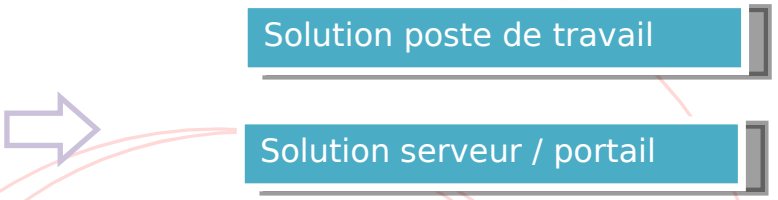


Fédération entre espaces de confiance

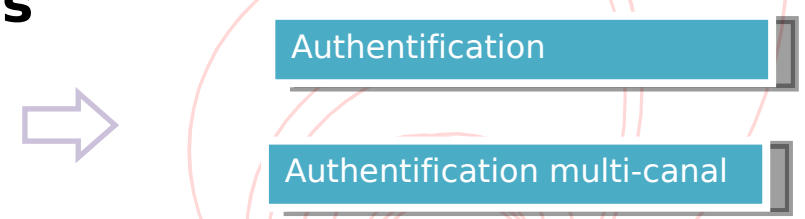


Pré-requis à la mise en place de fonctions de contrôle d'accès

- **Déterminer la nature des applications**
  - Web vs client/serveur
  - 1 tiers vs nTiers

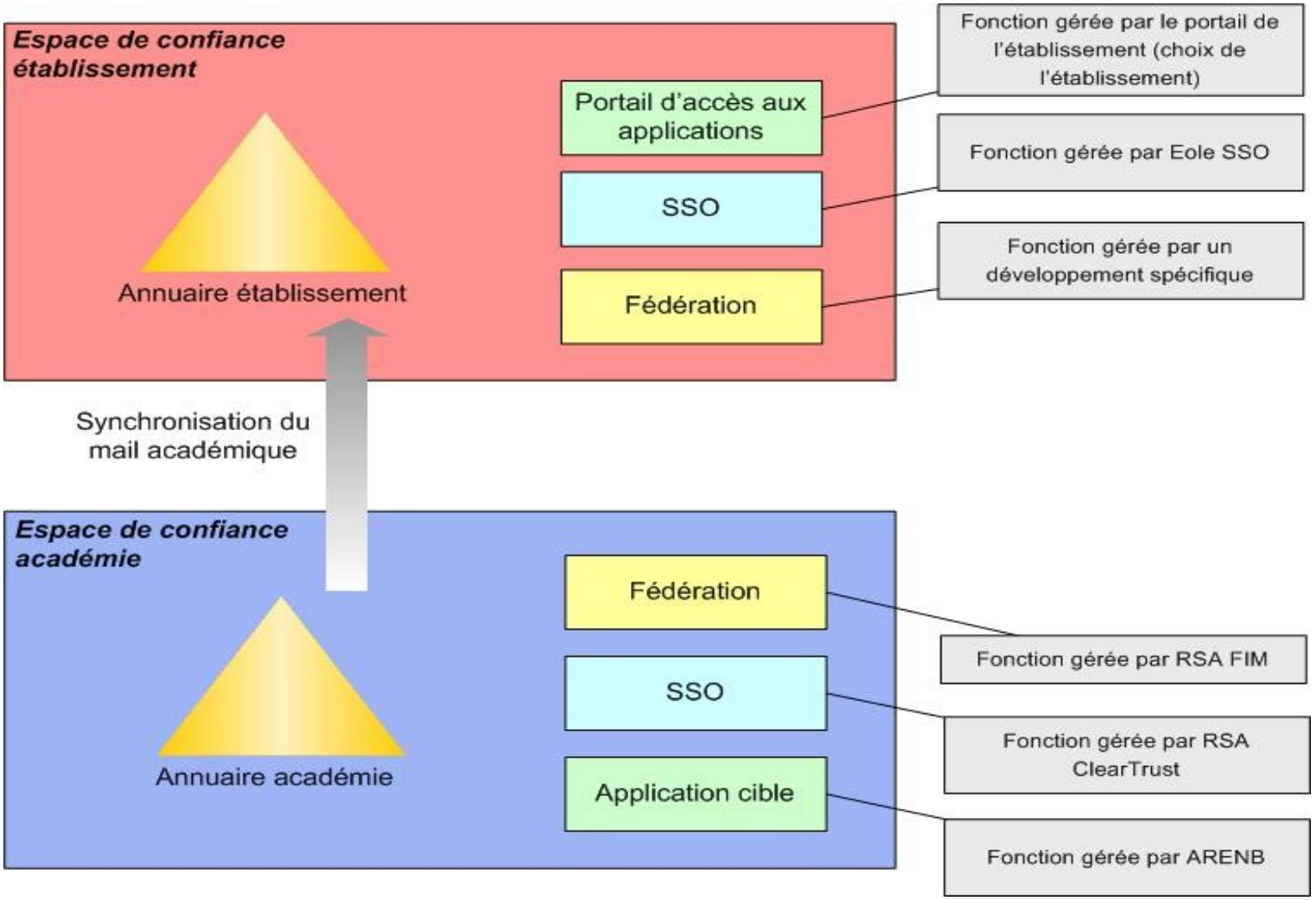


- **Identifier les acteurs (politique d'habilitation)**
- **Déterminer le niveau d'authentification attendu et les technologies envisagées**
  - Mot de passe
  - OTP
  - Certificat
  - Biométrie



- **Déterminer les principes de passage de jeton aux applications en fonction des contraintes applicatives**
  - Niveau d'intrusion possible au niveau des application
  - Compatibilités avec les technologie de propagation de jeton (Liberty Alliance, Kerberos, SAML, WSS, etc.)

EC Etablissement / Académie



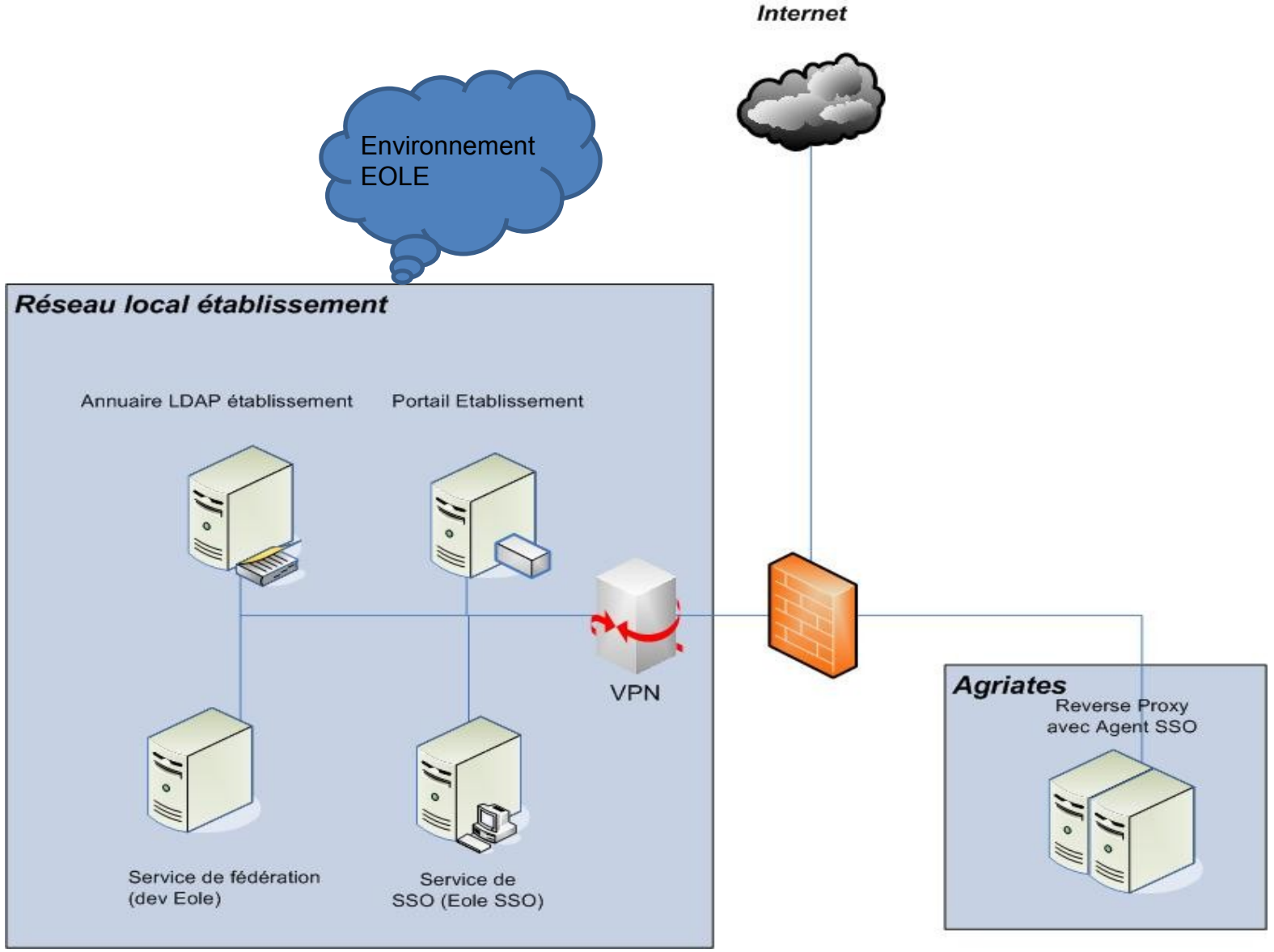
Service Technologies Systèmes Information

GESTION IDENTITE DE L EDUCATION NATIONALE

1. Rappels et définition en matière de gestion des identités et des habilitations
2. Présentation des composantes à mettre en place
3. Démarches de mise en œuvre et principes fondamentaux

Architecture technique espace de confiance primaire

<u>Note :</u> L'architecture du réseau local d'établissement indique les briques fonctionnelles utilisées. Le nombre de machine physique peut varier suivant les établissements.



Architecture technique espace de confiance secondaire

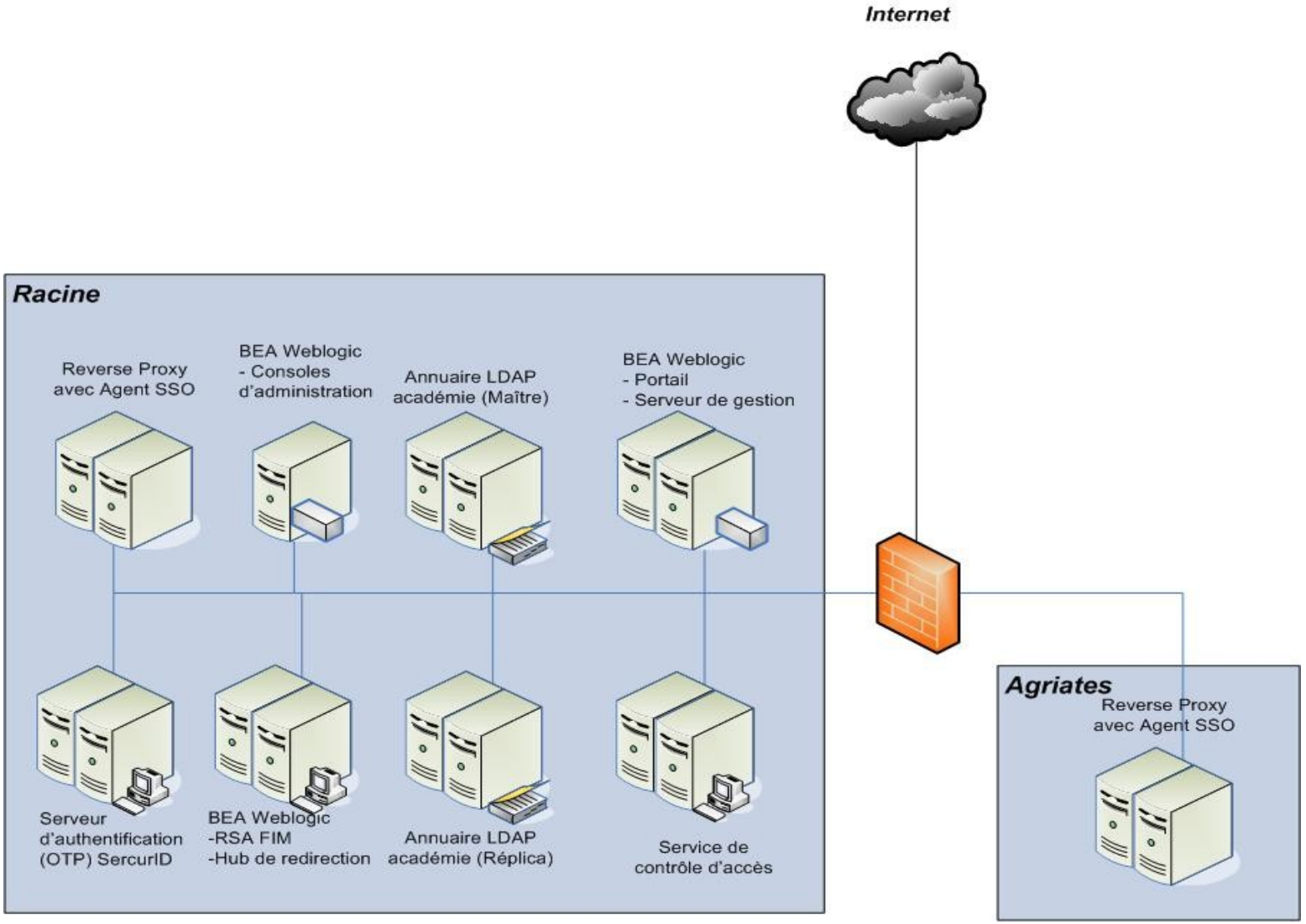
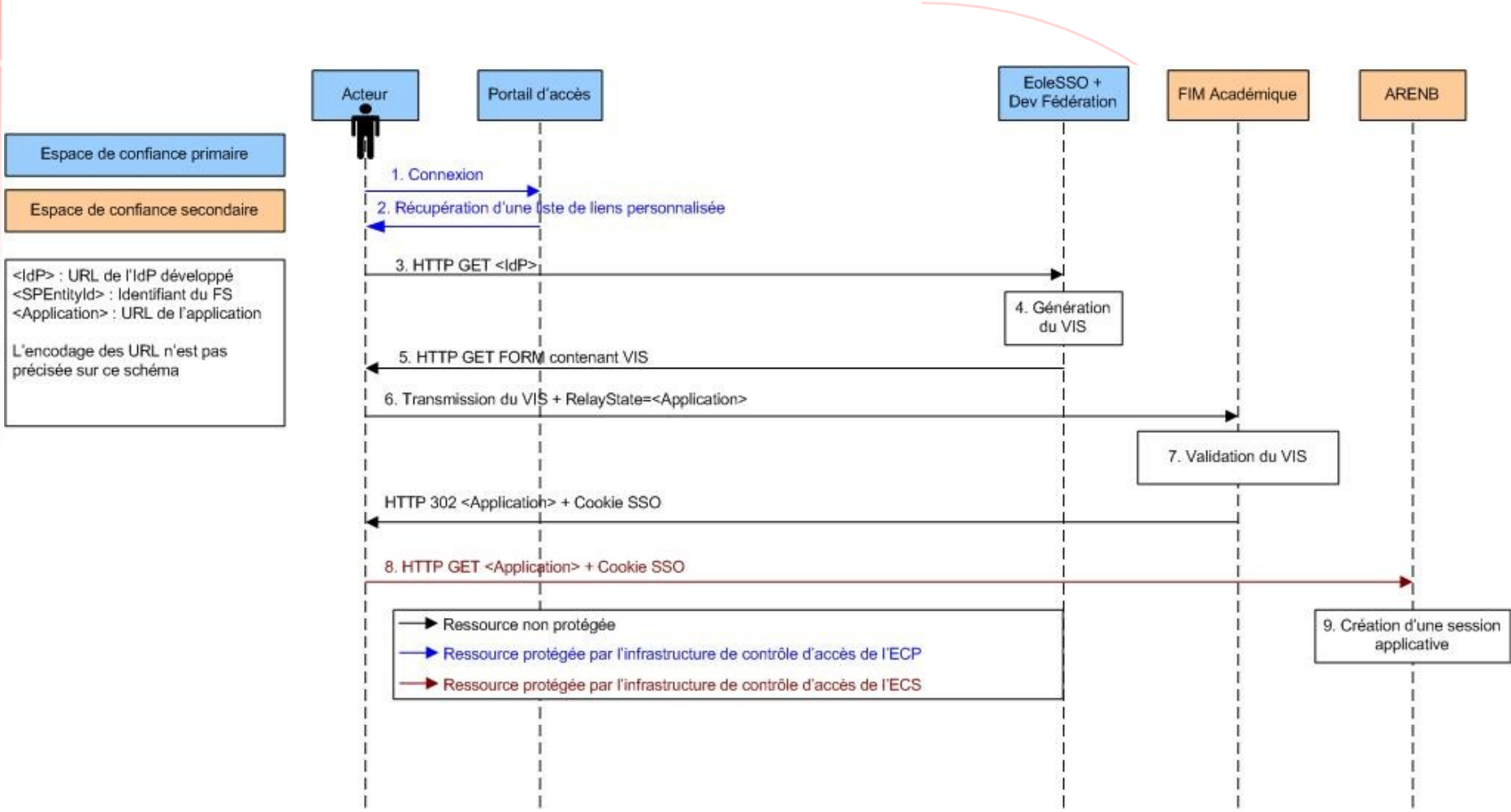
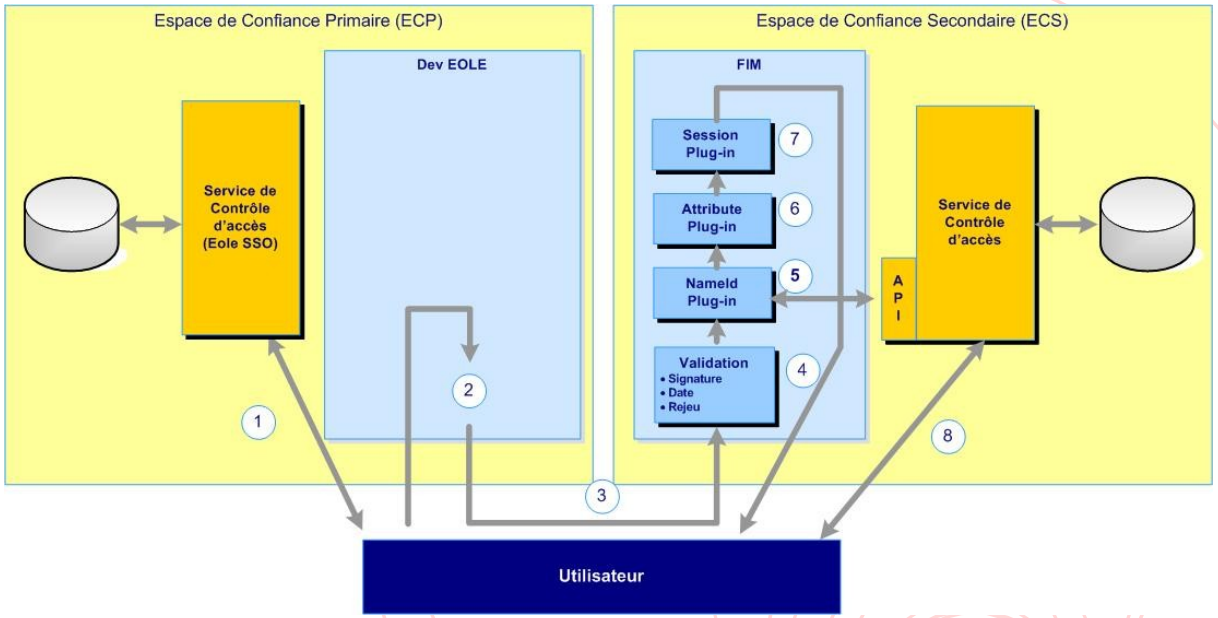


Diagramme de séquence d'accès à ARENB depuis le portail établissement

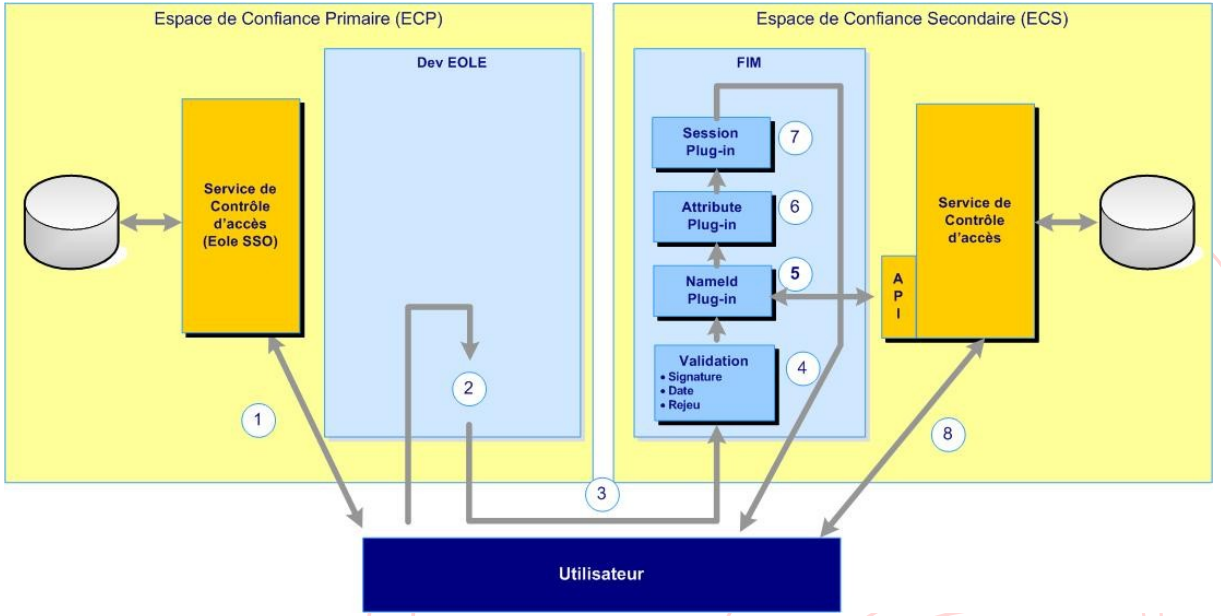


Ce schéma détaille en fait les étapes de la cinématique de connexion en mode IdP-initiated au niveau de FIM 1/2



•L'utilisateur est authentifié auprès du serveur Eole SSO de son académie. Il dispose donc d'une session valide dans l'ECP;
•L'utilisateur décide d'accéder à l'ECS. Le jeton d'authentification est généré;
•L'utilisateur envoie à l'aide de la méthode POST l'assertion SAML ainsi générée au FIM du FS ;
•Validation du jeton par FIM

Ce schéma détaille en fait les étapes de la cinématique de connexion en mode IdP-initiated au niveau de FIM: 2/2



Le NameID Plug-in du FS est chargé de réaliser le chaînage de entre l'identité locale à l'ECS et l'identité présente dans l'assertion. Dans notre cas, il s'agira de trouver le DN de l'utilisateur à partir de son adresse mail. Cette opération est effectuée à l'aide de l'Admin API de ClearTrust

L'Attribute Plug-in du FS va renseigner les informations concernant cet utilisateur à partir des attributs présents dans l'assertion en peuplant les propriétés de ClearTrust au travers de l'Admin API de ClearTrust. Dans notre cas, aucun attribut ne sera modifié

Le Session Plug-in du FS va générer un jeton d'authentification dans l'ECS et le renvoyer à l'utilisateur. L'utilisateur possédera alors un jeton d'authentification valide dans l'ECS ;
L'utilisateur peut maintenant se connecter aux systèmes protégés dans l'ECS. Dans le cas présent, l'utilisateur est redirigé vers la page de sélection de l'établissement.

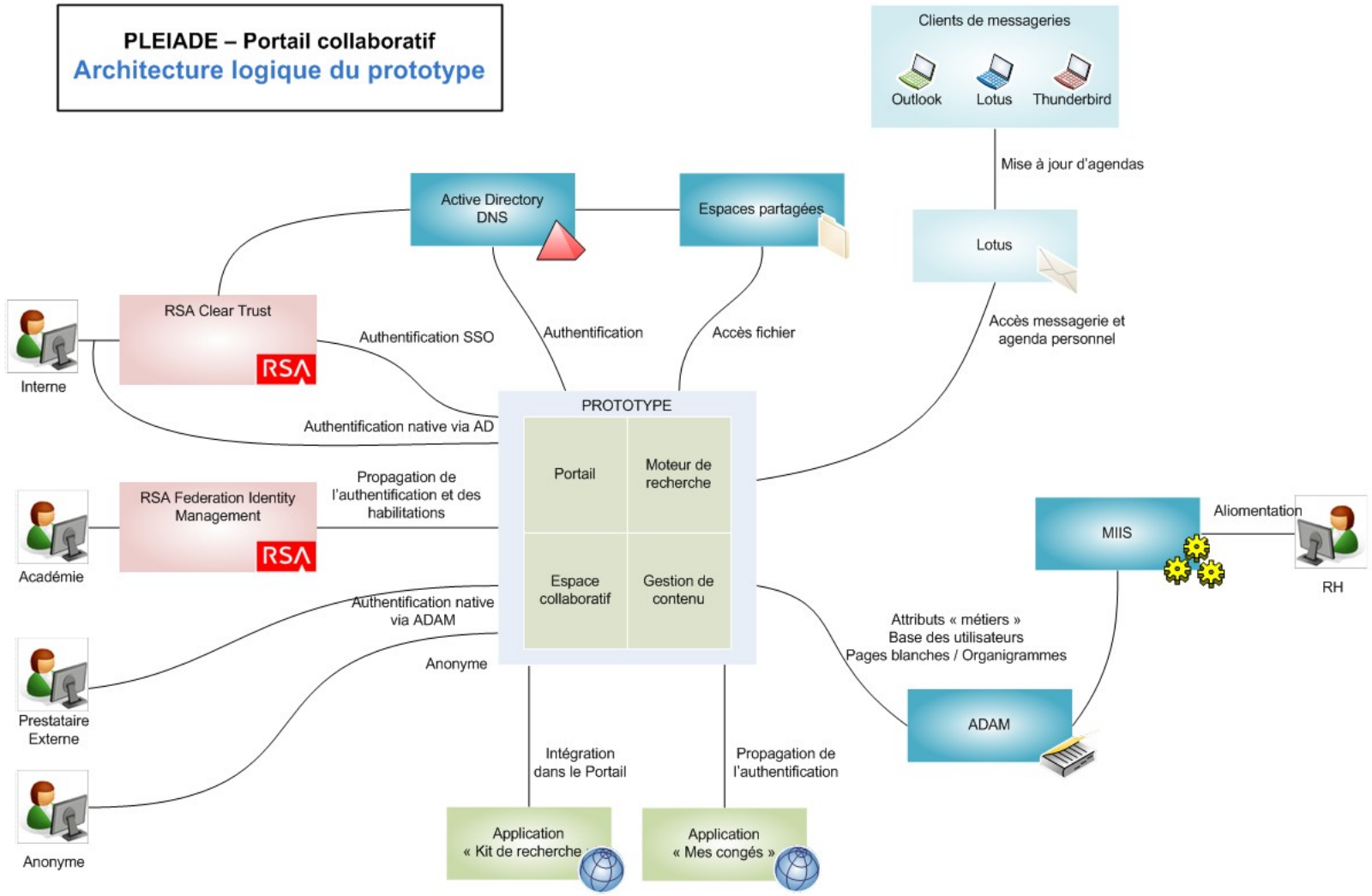
Service Technologies Systèmes Information

AUTRE CAS D'ARCHITECTURE

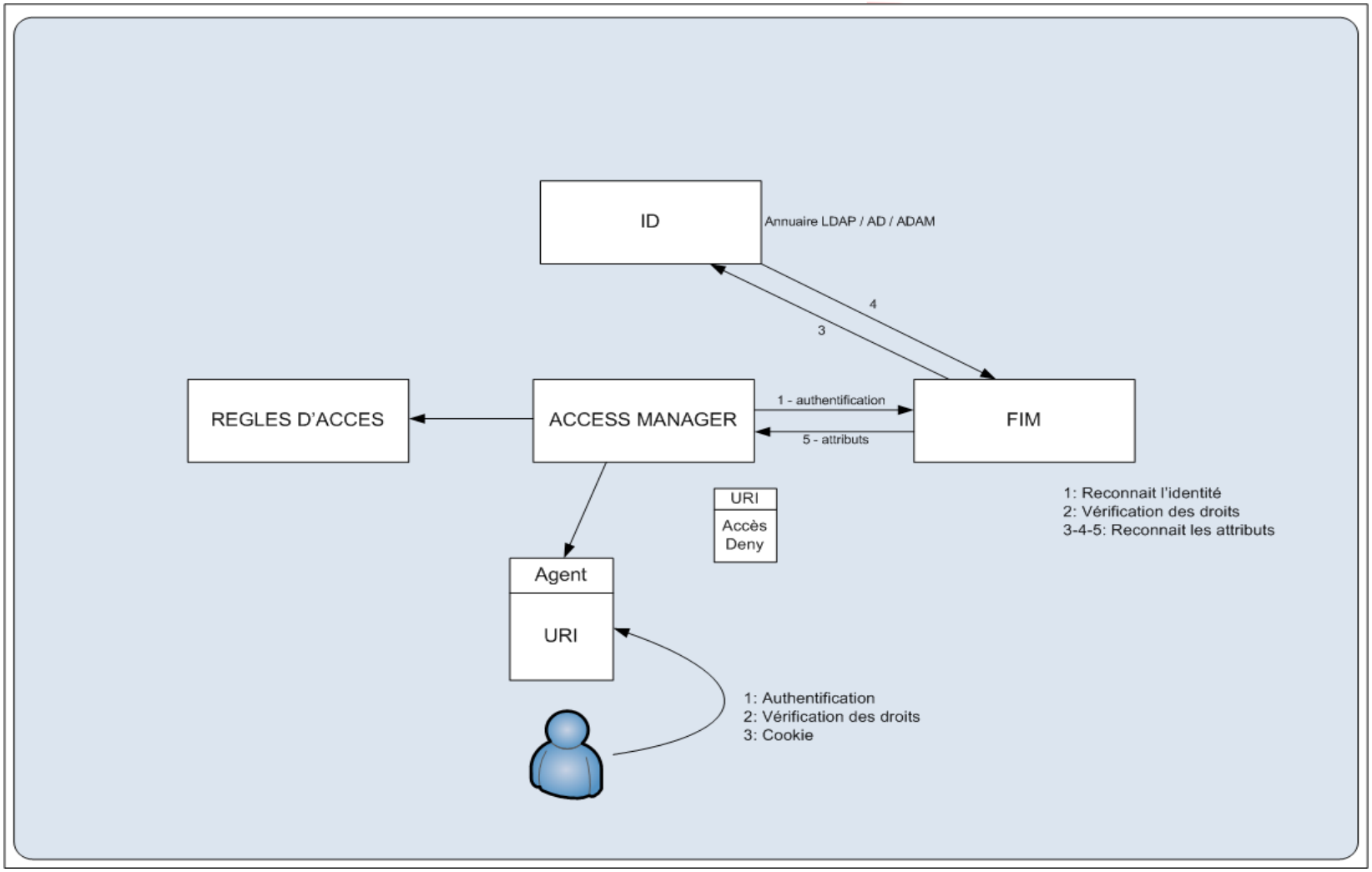
PORTAIL ACADEMIQUE GUICHET D'IDENTITE VERS PLEIADE PORTAIL ADMINISTRATION CENTRALE

SSO DE BOUT EN BOUT

Architecture RSA / MOSS 2007



Le cookie doit véhiculer les informations identité et autorisations



TRAVAUX EN COURS SSO et FEDERATION

- RSA vers CAS (DIJON PÔLE EOLE)
- RSA vers MICROSOFT (POC PLEIADE)
- RSA vers IBM (POC PLEIADE)
- RSA FIM vers Shibboleth (207 universités et centres de recherches) travaux avec académie de Rennes
- RSA intégration portail PIA JBOSS (en cours)

Glossaire

- EC : Espace de Confiance
- ECP : Espace de Confiance Primaire
- ECS : Espace de Confiance Secondaire
- EJB : Enterprise Java Beans
- FI : Fournisseur d'Identité
- FIM : Federated Identity Manager
- FS : Fournisseur de Services
- IGC : Infrastructure de Gestion de Clé
- SAML : Security Assertion Markup Language
- SLO : Single Log-Out
- SOAP : Simple Object Access Protocol
- SSL : Secure Sockets Layers
- SSO : Single Sign-On
- VI : Vecteur d'Identification