Shibboleth.

# Fédération d'Identité

## SHIBBOLETH

Frederic.Soulier@univ-tlse1.fr

Université Toulouse 1 Sciences Sociales

CAPITOUL - 18/10/2007

# Plan

# Problématiques des systèmes d'information actuels

- Mobilité
  - Mobilité des utilisateurs accrue.
  - Augmentation des besoins d'Interconnexion entre établissements.

$\Rightarrow$ Evolution du périmètre du Système d'Information.

- Développement du web
  - Importance accrue des applications Web.
  - Multiplications des applications.

$\Rightarrow$ Multiplications des Authentifications

# Première réponse

- Mise en place de mécanismes de SSO
  - Accès aux ressources internes des établissements.
  - Quid des utilisateurs extérieurs aux entités ?
    - Comptes invités.
    - Création de comptes locaux.
    - Meta-Annuaires.

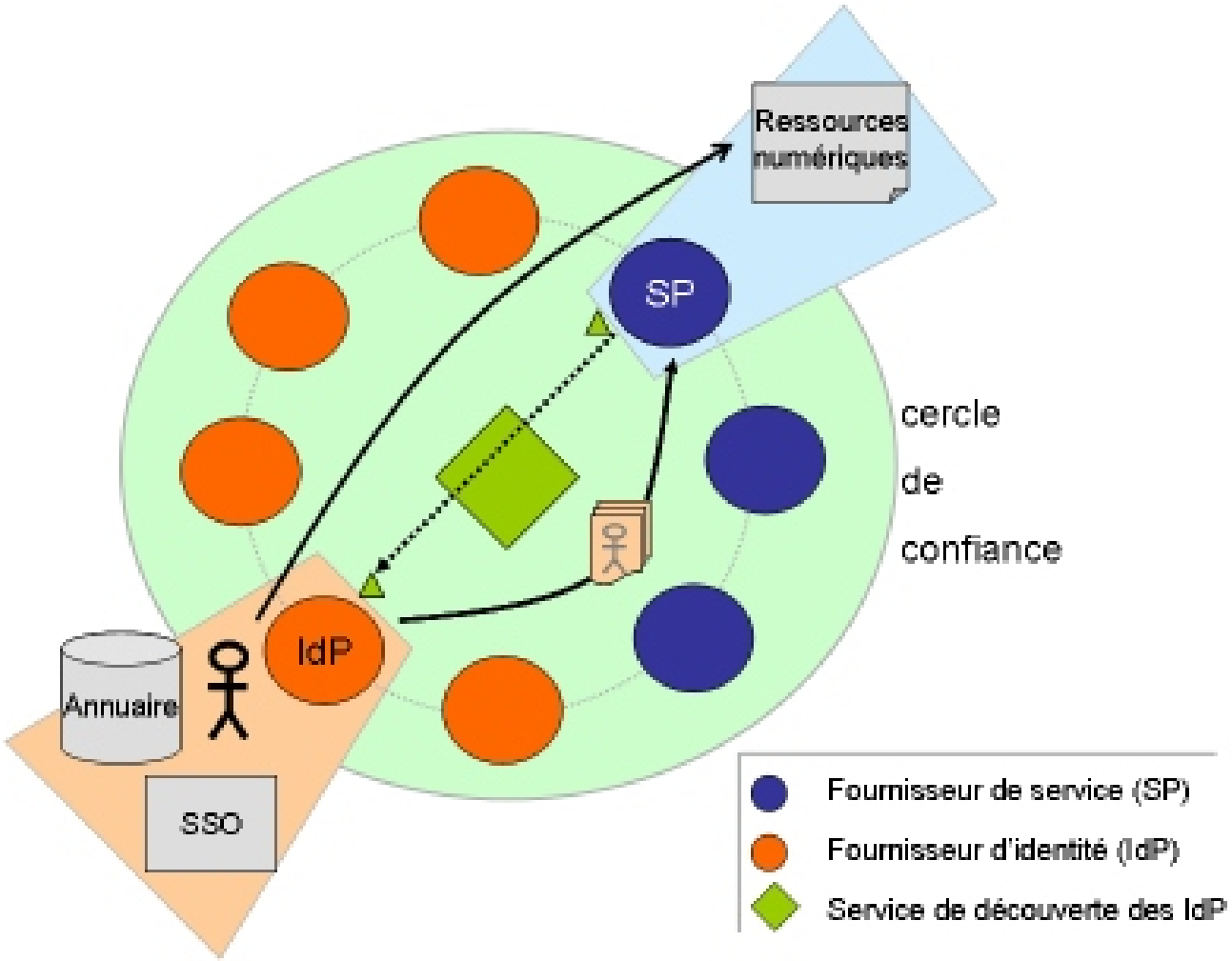
# Plan

# Fédération d'Identité
## Objectifs

Une Fédération d'identité pour atteindre 2 objectifs principaux :

1. Délégation de l'authentification
   - Utilisation du système d'Authentification de l'établissement d'origine de l'utilisateur.
2. Propagation des attributs utilisateurs
   - Diffusion, depuis l'établissement d'origine, d'attributs concernant l'utilisateur.
   - Notion d'autorisation.

# Fédération d'Identité
## Termes génériques (Sources CRU)



# Fédération d'Identité
## Atouts

Les principaux avantages :

- Disparition des comptes spécifiques pour les utilisateurs extérieurs.
  - Utilisation des comptes existants !
- Fiabilisation des données utilisateurs.
  - Qui mieux que l'établissement d'origine peut gérer le compte utilisateur ?
- Indépendance des système d'authentification.
  - Pas de modification des systèmes existants pour les établissements fournisseurs de service.

Le concept sous-jacent :

$\Rightarrow$ La CONFIANCE dans la Fédération !

# Fédération du CRU
## Aspect organisationnel

La fédération du CRU est constitué de plusieurs membres :

- Le CRU
  - Organisme fédérateur.
- Les fournisseurs d'identité (IdP) :
  - Etablissements de l'enseignement supérieur.
- Les fournisseurs de service (SP) :
  - Etablissements de l'enseignement supérieur.
  - Autres organismes publics.
  - Entreprises privées.

# Fédération du CRU
## Aspect technique

Le CRU assure les fonctions suivantes au sein de la fédération :

- Inscription des entités dans la fédération.
- Distribution des méta-données aux différents partenaires.
- Sécurisation des échanges au sein de la fédération avec sa PKI
  - Authentification.
  - Chiffrement.

Le CRU gère 2 fédérations :

- Fédération de test.
- Fédération pilote.

Pas de centralisation des échanges.
Utilisation du produit shibboleth pour implémenter la fédération.

# Plan

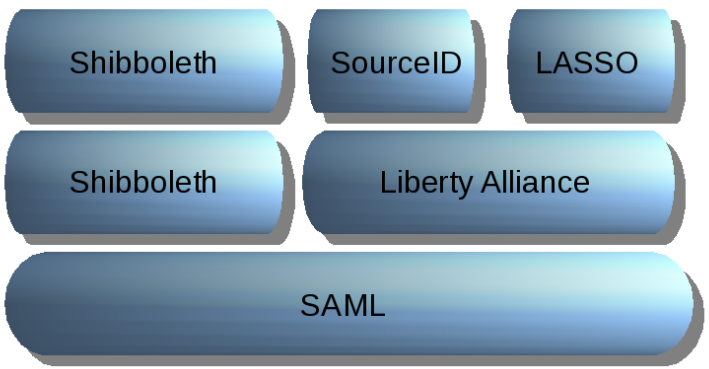
Shibboleth est un mot hébreu qui désigne une phrase ou un mot ne pouvant être prononcé correctement que par les membres d'un groupe donné.

## Un peu d'histoire . . .

Les éphraïmites auraient utilisé ce mot pour confondre leurs ennemis gileadites parmi les fuyards. Les gileadites n'étant pas capables de prononcer le phonème "sh", ils écorchaient là le dernier mot de leur vie...

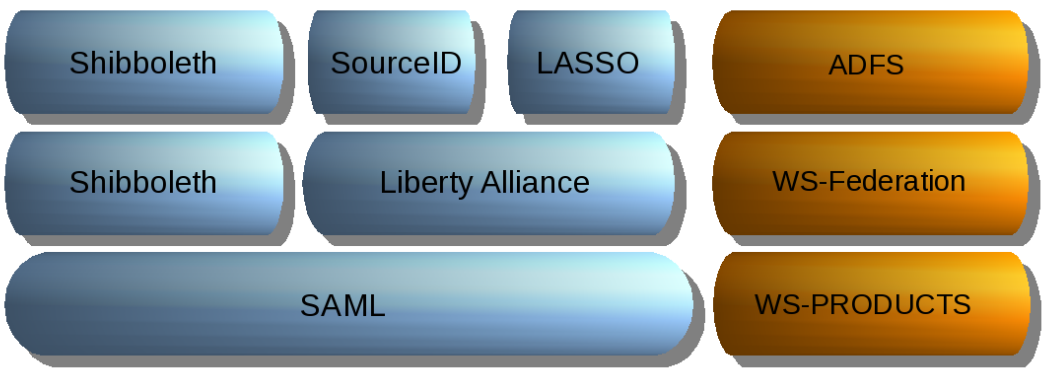
# Présentation
## Shibboleth : **Norme**/Implémentation

- Développé par Internet2
- Shibboleth est une norme basée sur SAML
  - SAML : Security Assertion Markup Language.
  - SAML : Protocole à fort niveau d'abstraction.
  - SAML : Echange d'assertions de sécurité entre différentes applications.
  - Fichiers XML.
- Shibboleth étend le protocole SAML
  - Authentification
  - Autorisations



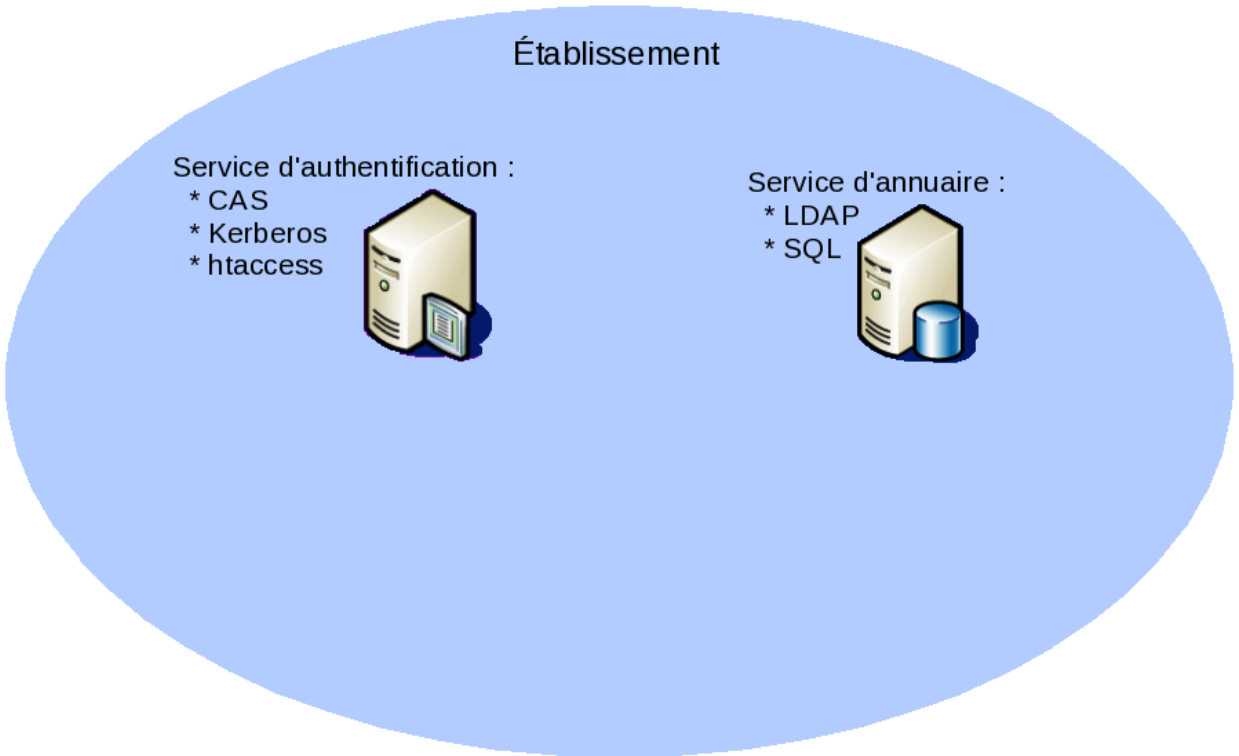
# Présentation
## Shibboleth : **Norme**/Implémentation

- Développé par Internet2
- Shibboleth est une norme basée sur SAML
  - SAML : Security Assertion Markup Language.
  - SAML : Protocole à fort niveau d'abstraction.
  - SAML : Echange d'assertions de sécurité entre différentes applications.
  - Fichiers XML.
- Shibboleth étend le protocole SAML
  - Authentification
  - Autorisations

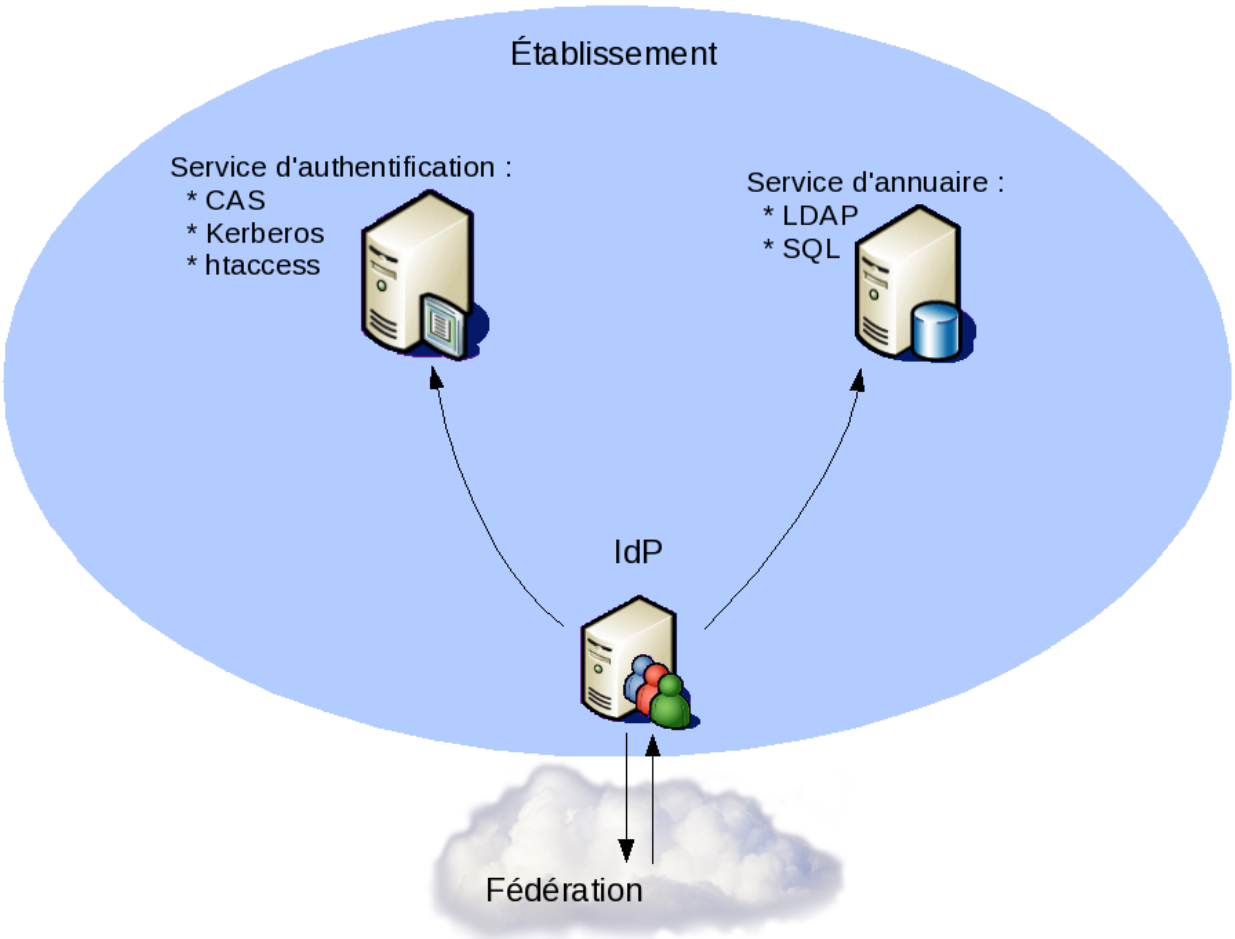


- Shibboleth propose 2 briques :
  - Une brique Fournisseur d'Identité.
  - Une brique Fournisseur de Service.

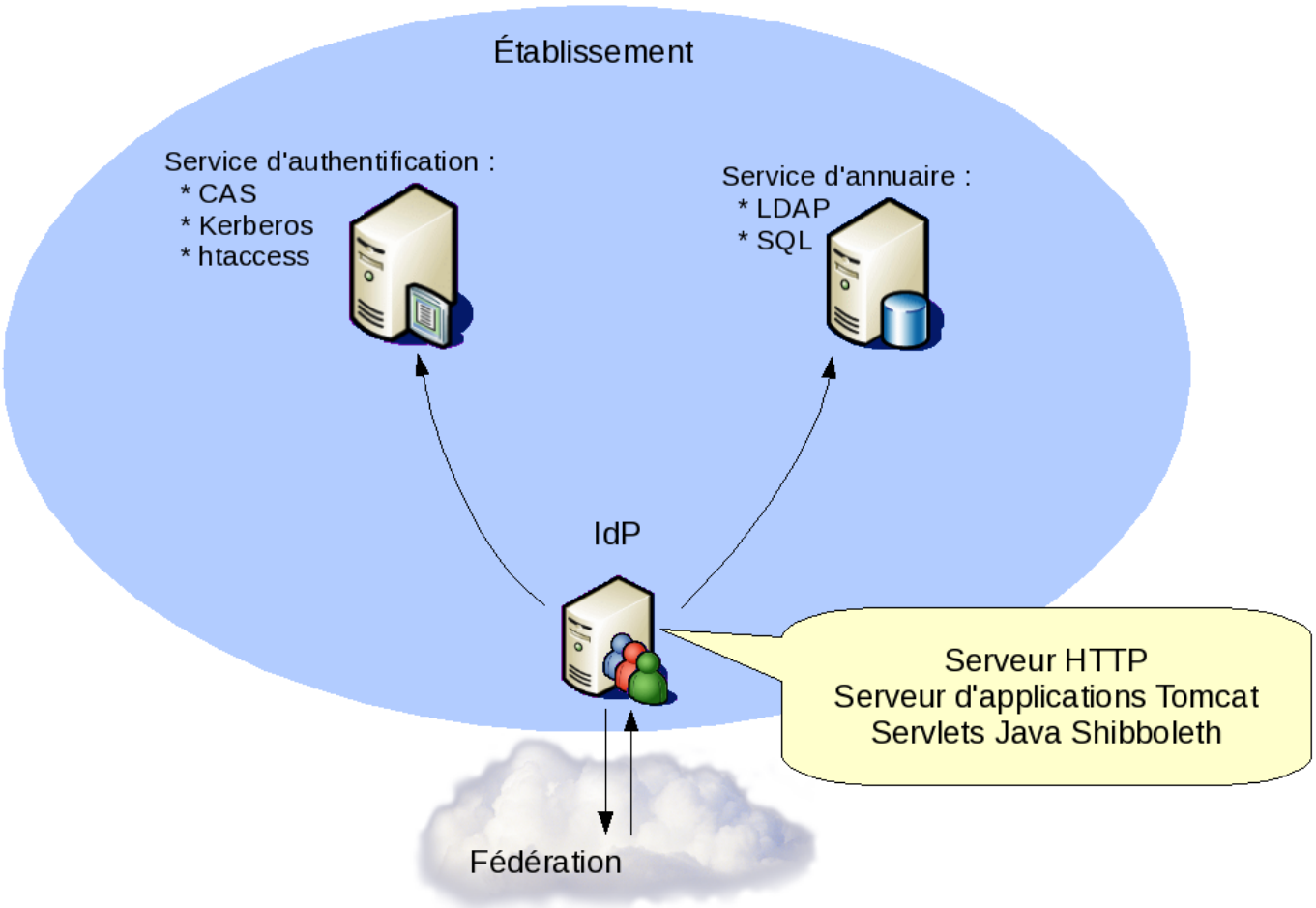
# Présentation
## Intégration dans le Système d'Information (Fournisseur d'Identité)



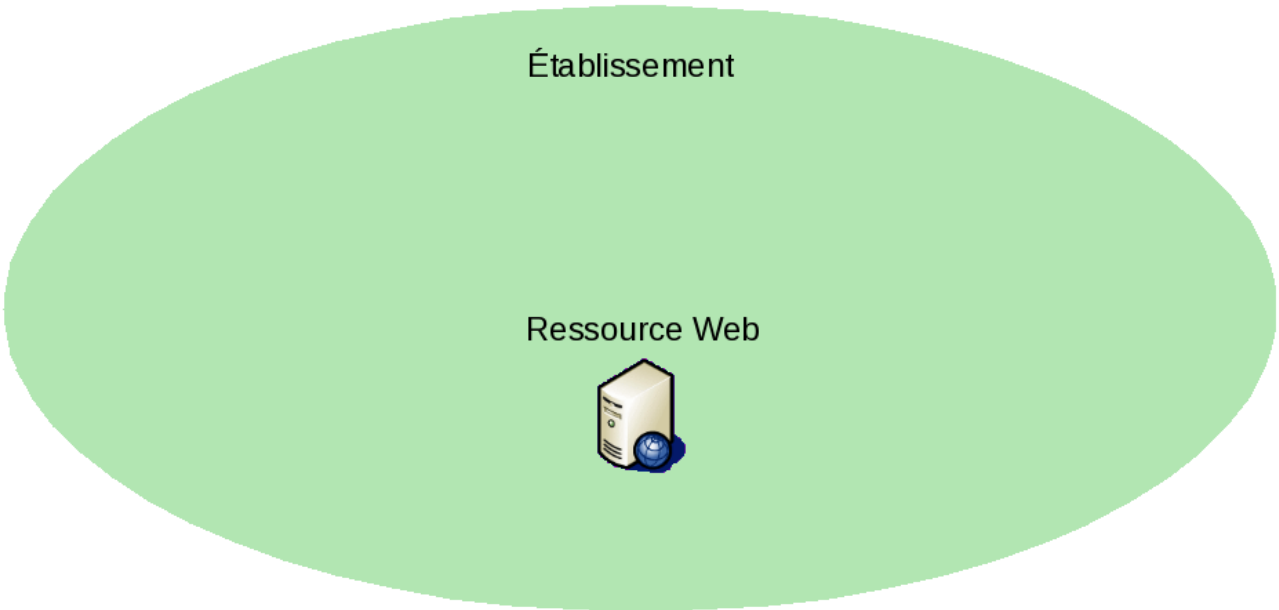
# Présentation
## Intégration dans le Système d'Information (Fournisseur d'Identité)



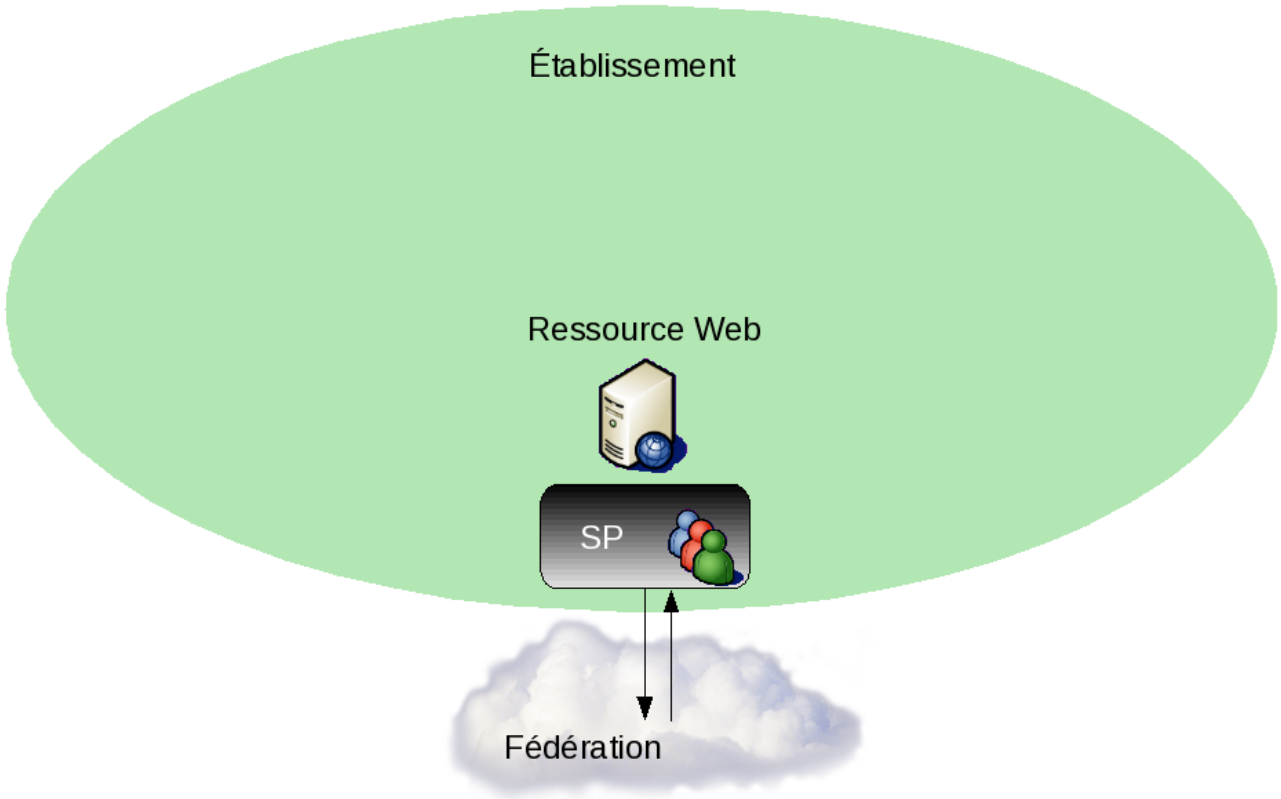
# Présentation
## Intégration dans le Système d'Information (Fournisseur d'Identité)



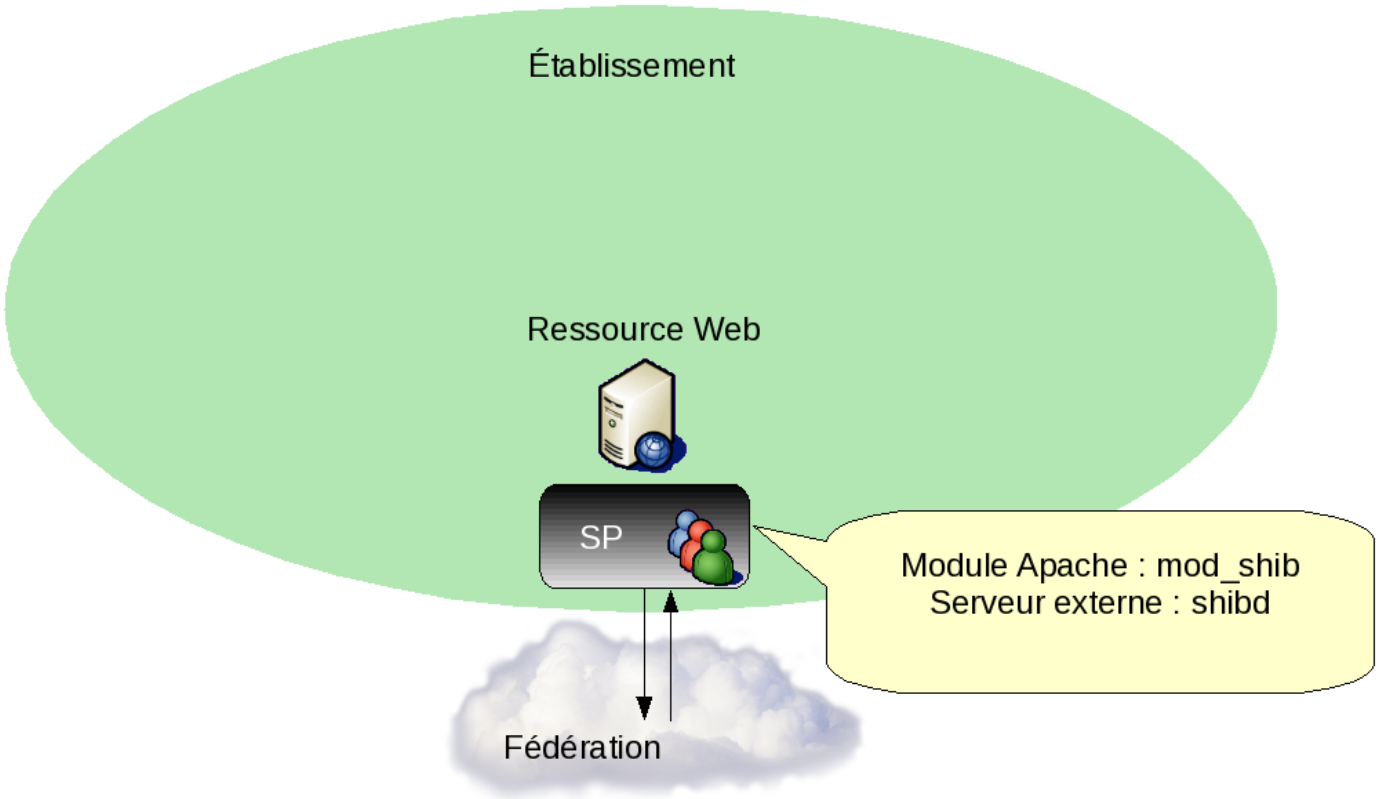
# Présentation
## Intégration dans le Système d'Information (Fournisseur de Service)



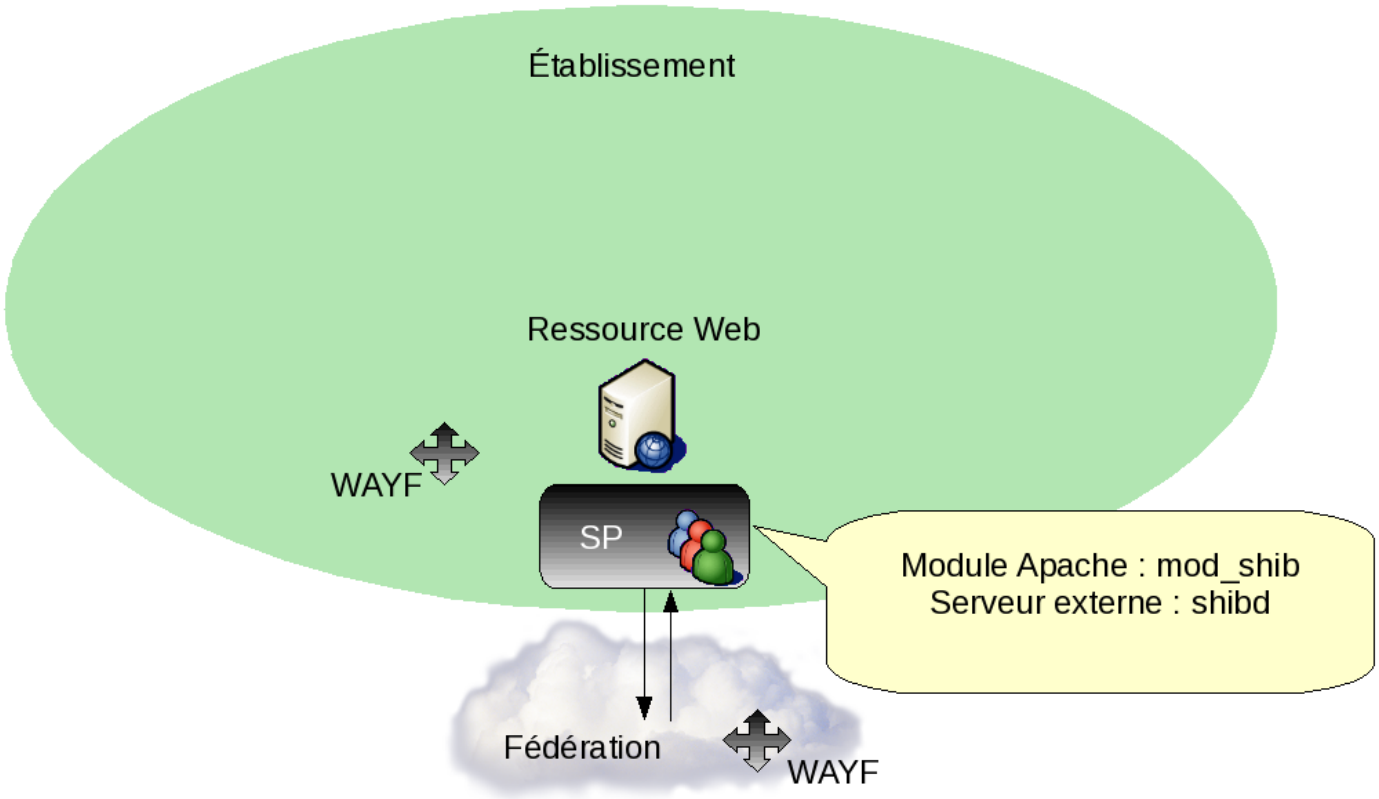
# Présentation
## Intégration dans le Système d'Information (Fournisseur de Service)



# Présentation
## Intégration dans le Système d'Information (Fournisseur de Service)



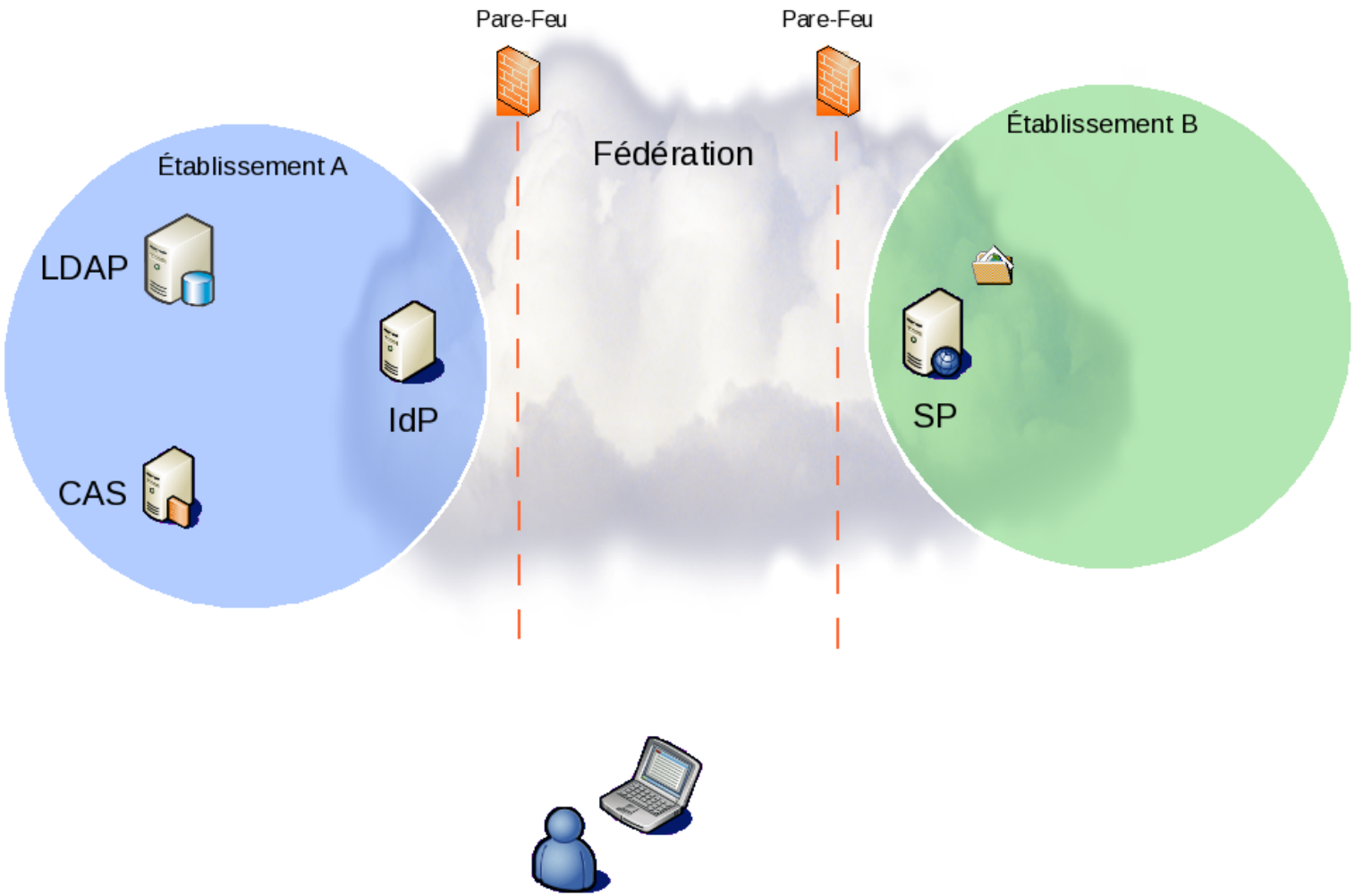
# Présentation
## Intégration dans le Système d'Information (Fournisseur de Service)



# Plan

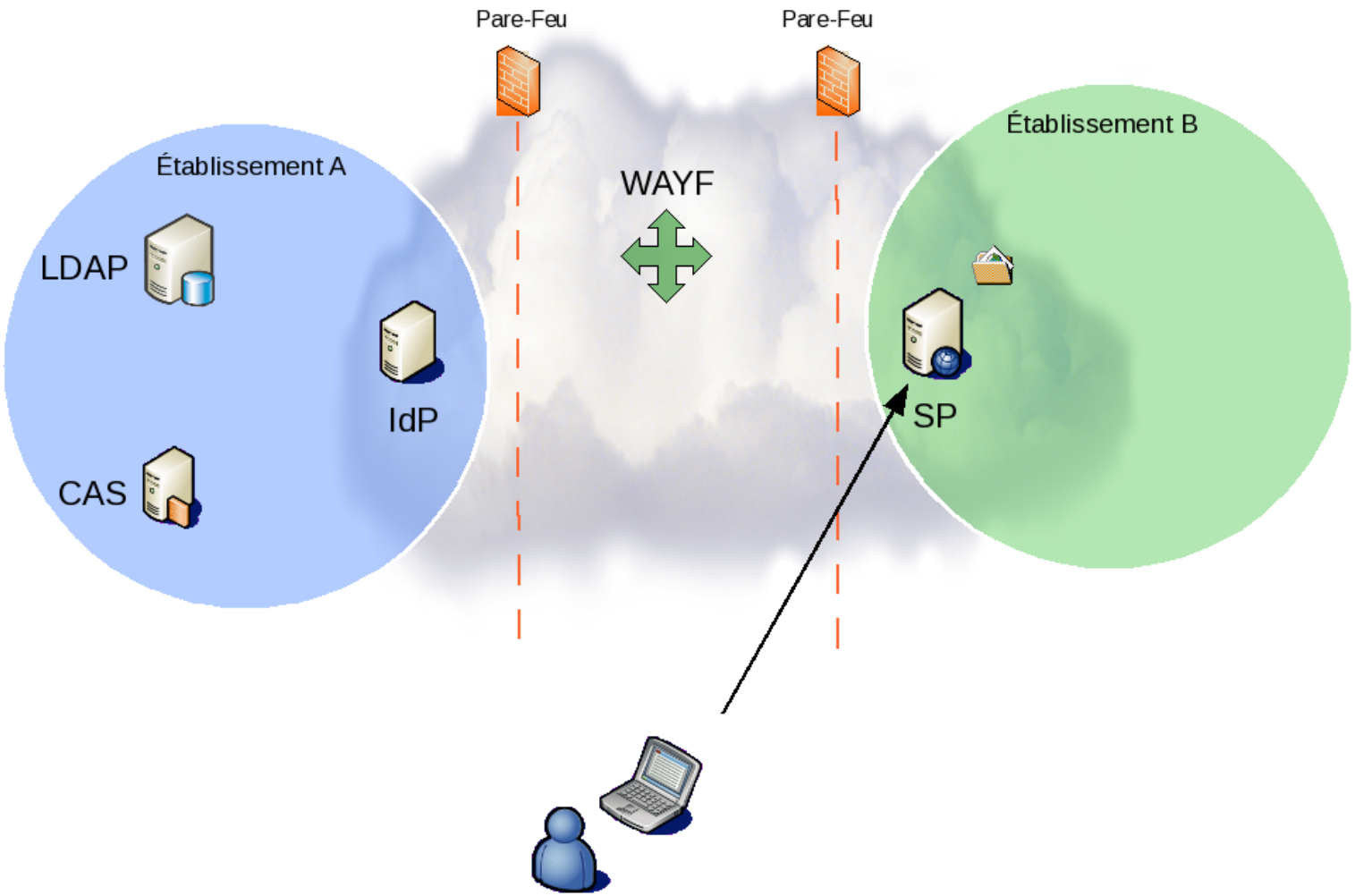
# Intéractions Client - SP - IdP

## Cinématique



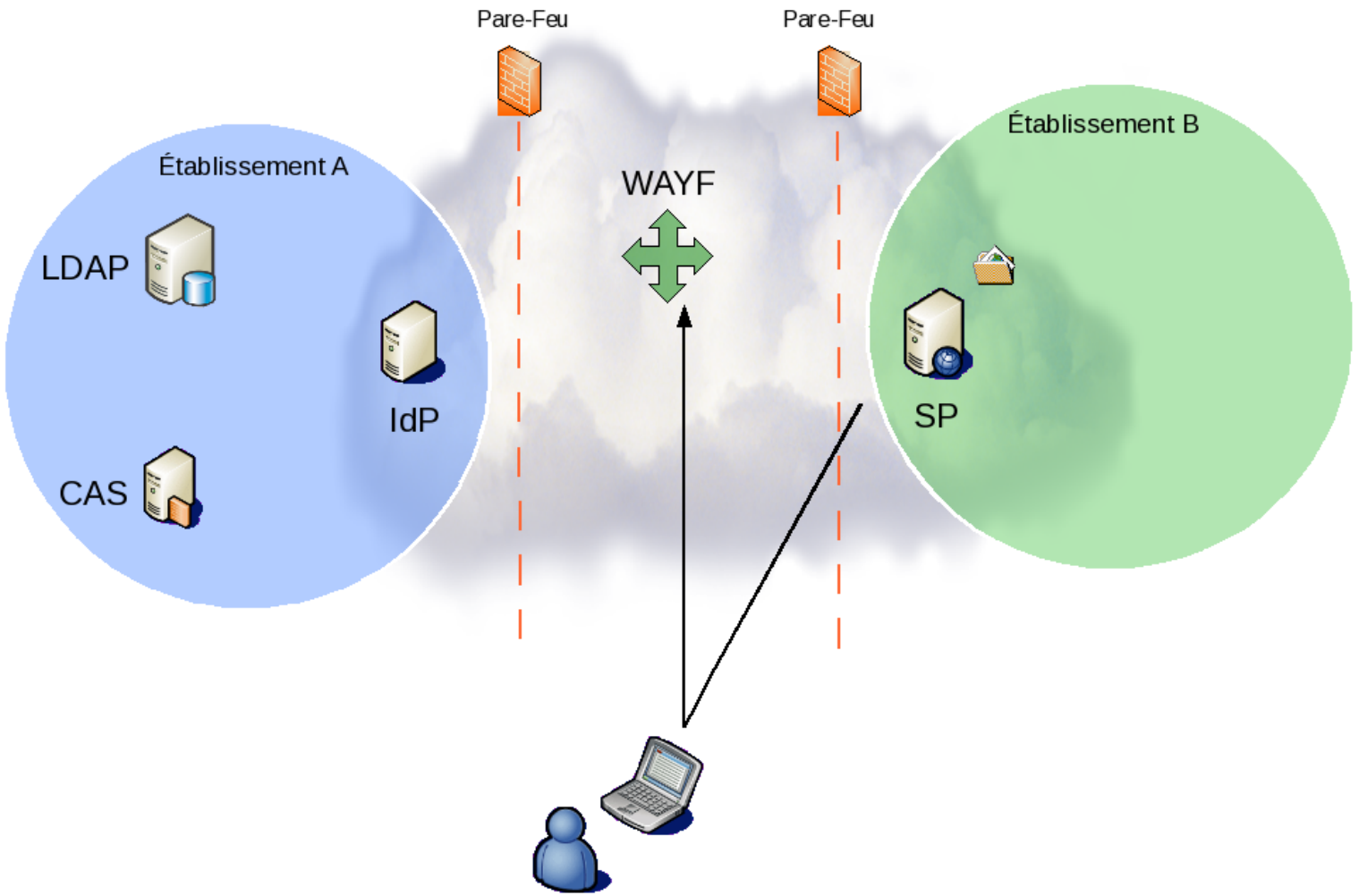
# Intéractions Client - SP - IdP

## Cinématique



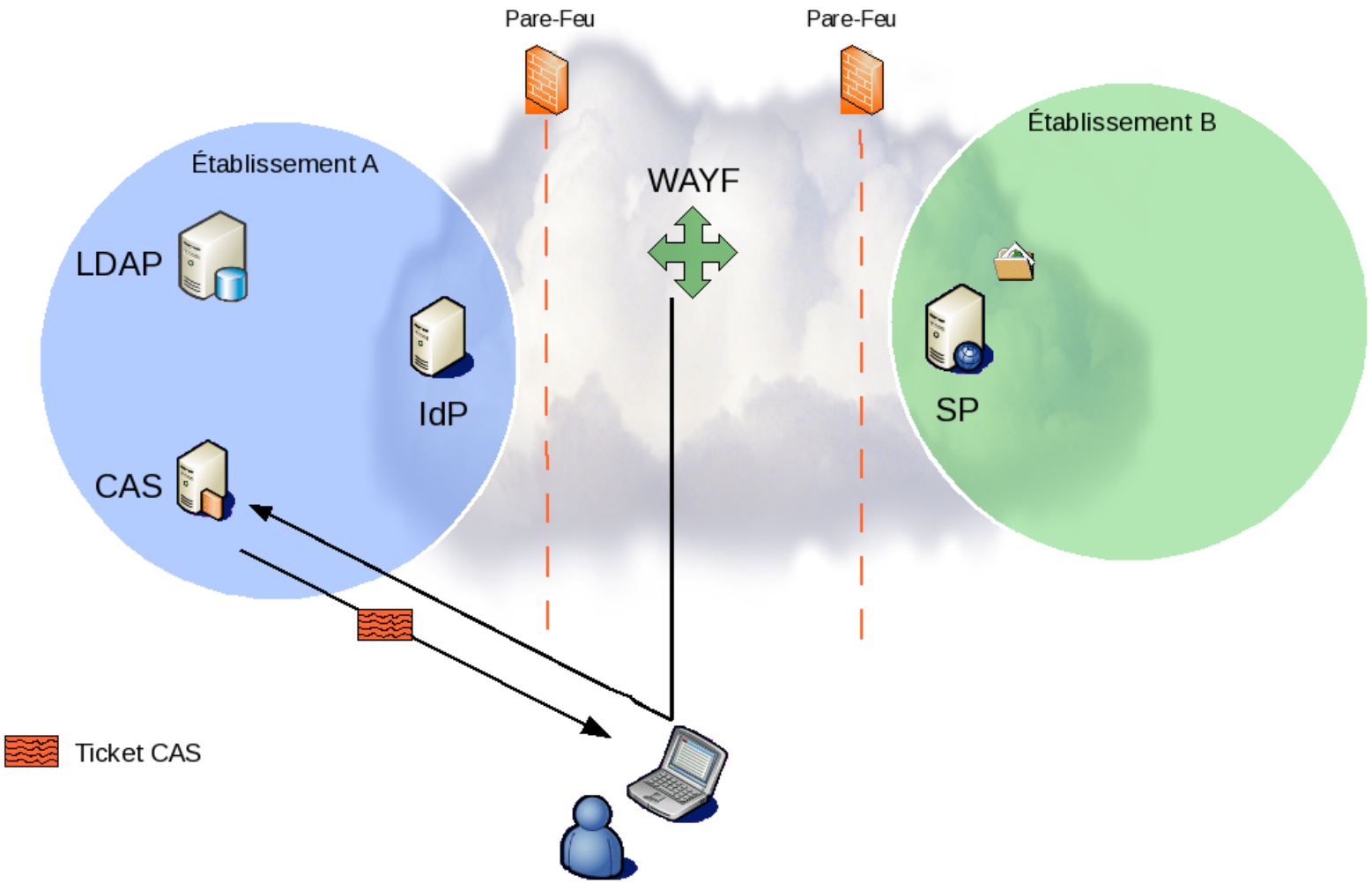
# Intéractions Client - SP - IdP

## Cinématique



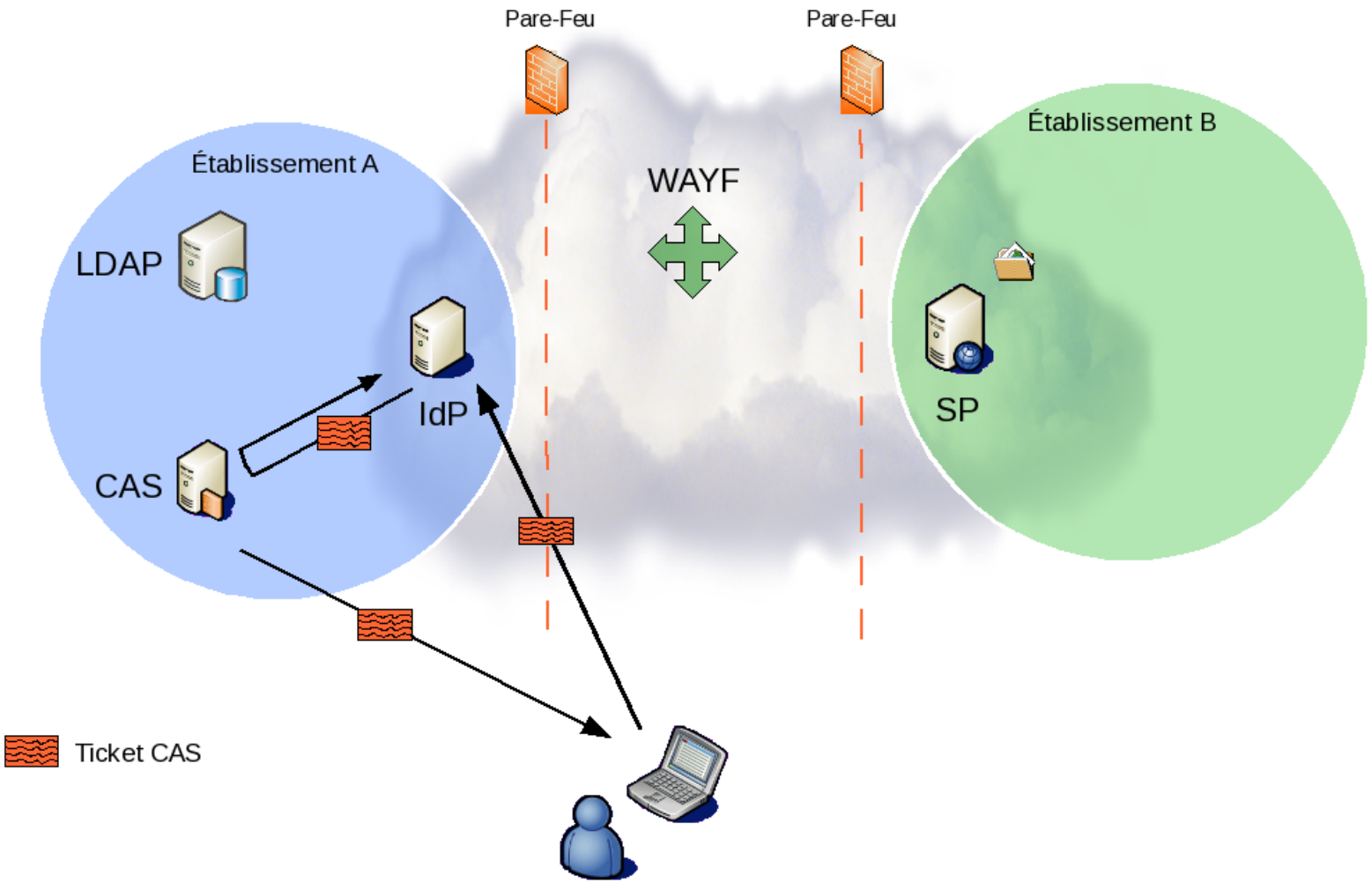
# Intéractions Client - SP - IdP

## Cinématique



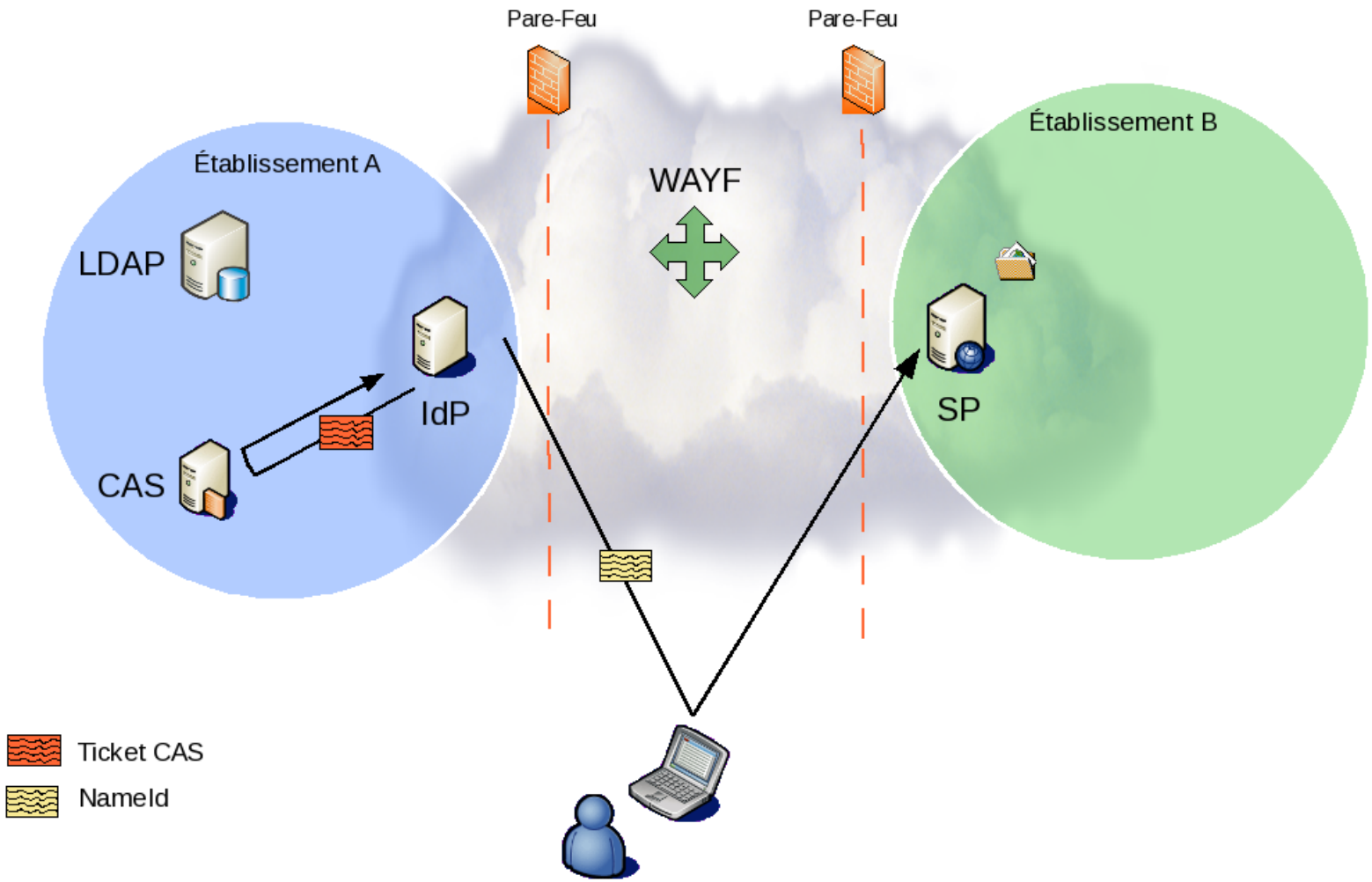
# Intéractions Client - SP - IdP

## Cinématique



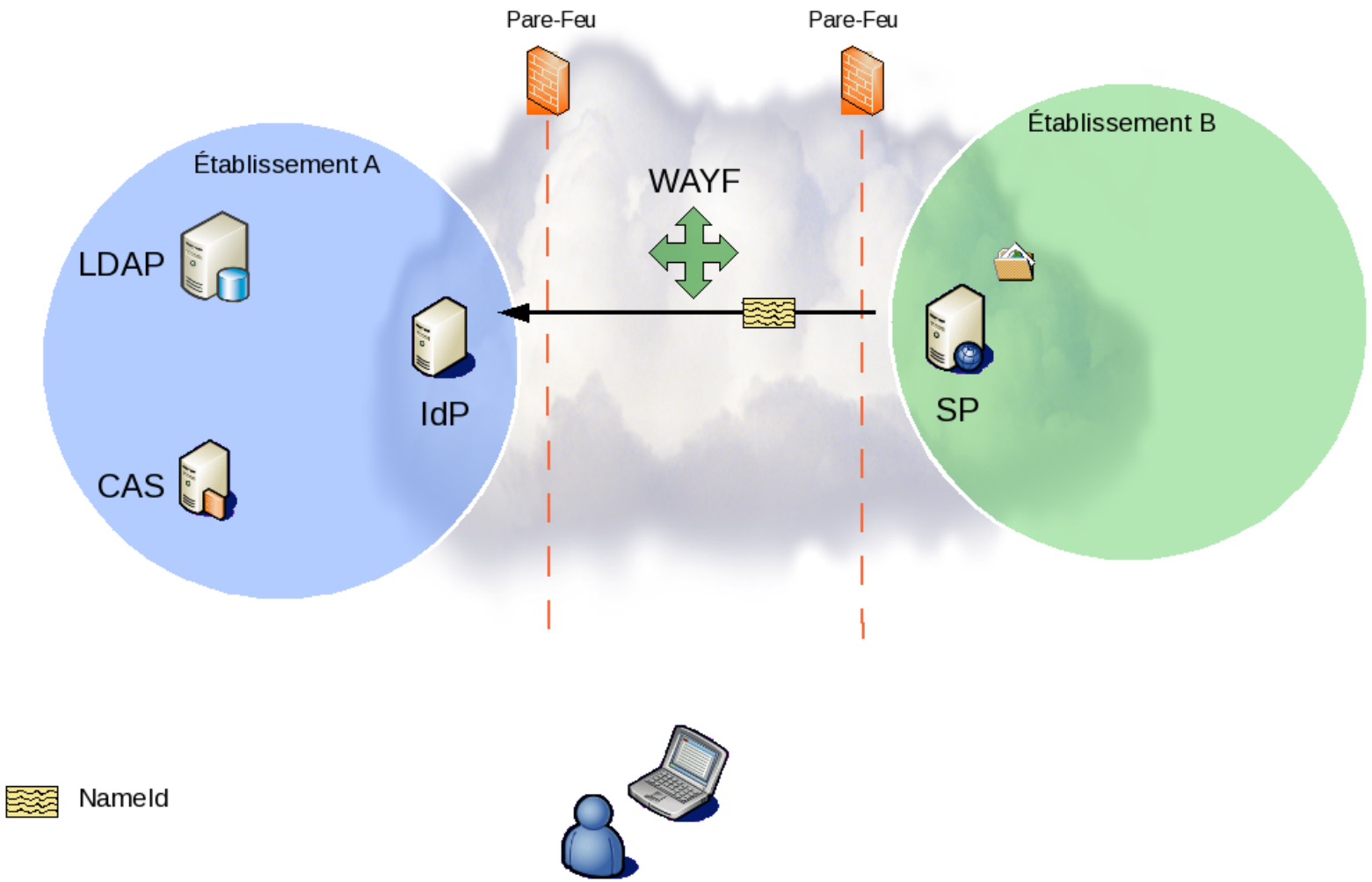
# Intéractions Client - SP - IdP

## Cinématique



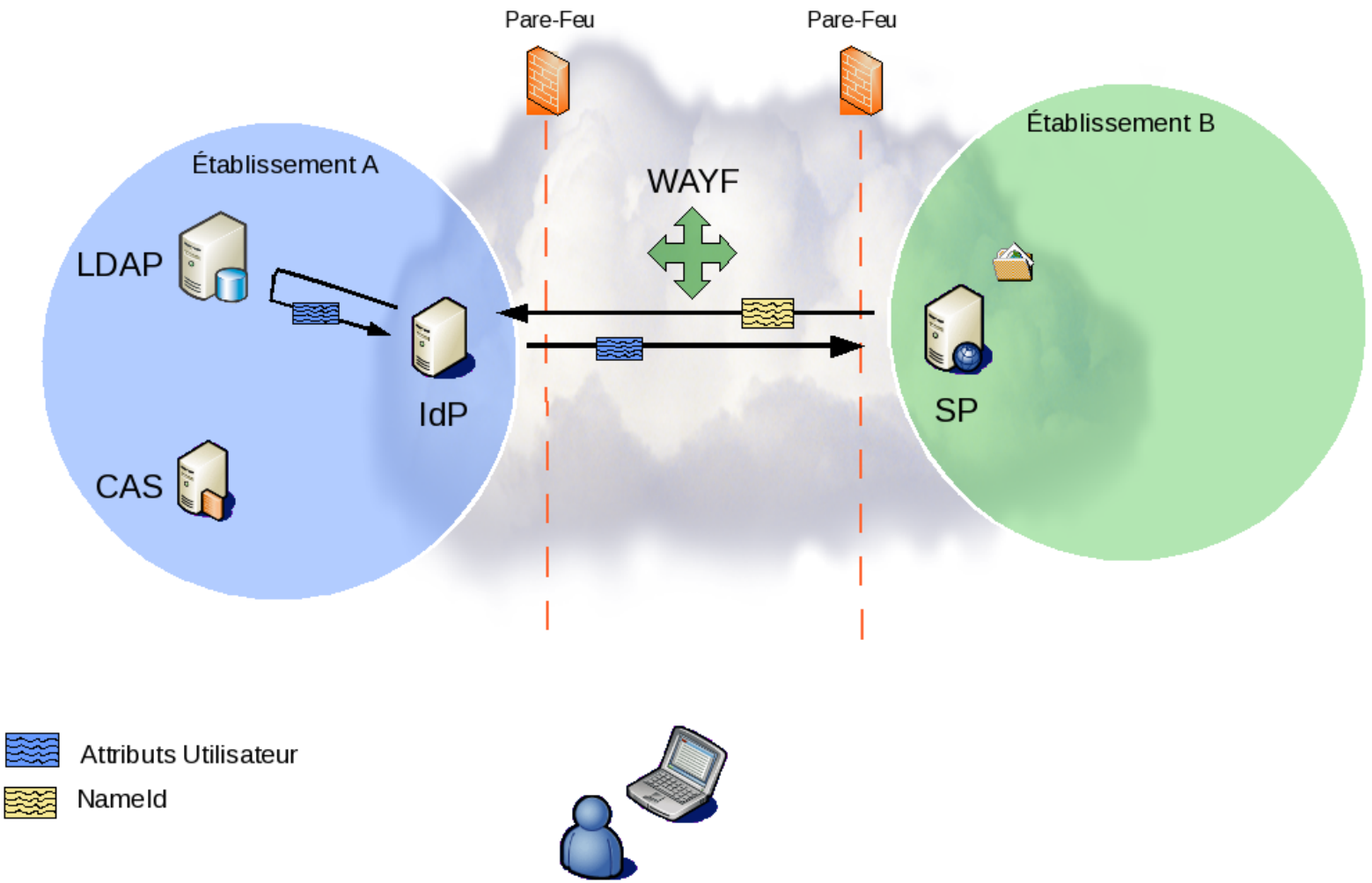
# Intéractions Client - SP - IdP

## Cinématique



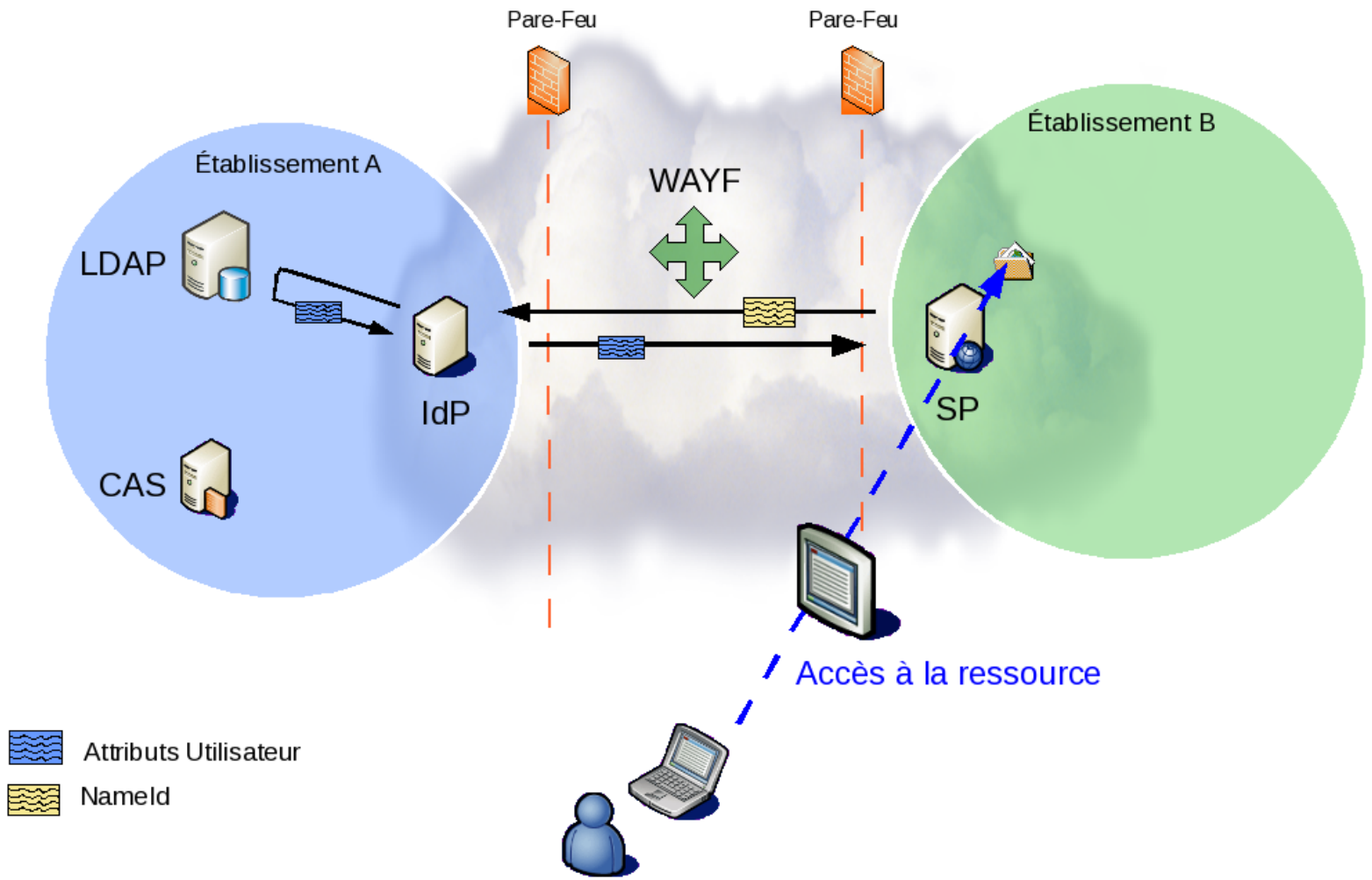
# Intéractions Client - SP - IdP

## Cinématique



# Intéractions Client - SP - IdP

## Cinématique



# Plan

# Mise en oeuvre à UT1
## Principales étapes du déploiement de l'Idp

- Demande de certificat pour le serveur.
- Installation du package shibboleth.
- Inscription dans la fédération de test.
- Validation du fonctionnement dans la fédération de test.
- Inscription dans la fédération pilote.
- Paramétrages pour interactions avec les fournisseurs de services.

# Mise en oeuvre à UT1
## Définition des attributs propageables

Liste prédéfinie d'attributs échangeables au sein de la fédération

- Espace de nommage commun => facilite les echanges IdP - SP.
- Attributs issus du schéma SUPANN.
- Possibilité de construction dynamique des attributs.

Exemple de défintion :

```
<!-- Attribut pour fournisseur de service EBSCO -->
<SimpleAttributeDefinition
        id="urn:mace:dir:attribute-def:eduPersonScopedAffiliation"
        smartScope="univ-tlse1.fr" sourceName="eduPersonAffiliation">
        <DataConnectorDependency requires="supann-univ-tlse1.fr"/>
</SimpleAttributeDefinition>
```

# Mise en oeuvre à UT1
## Restriction sur la propagation

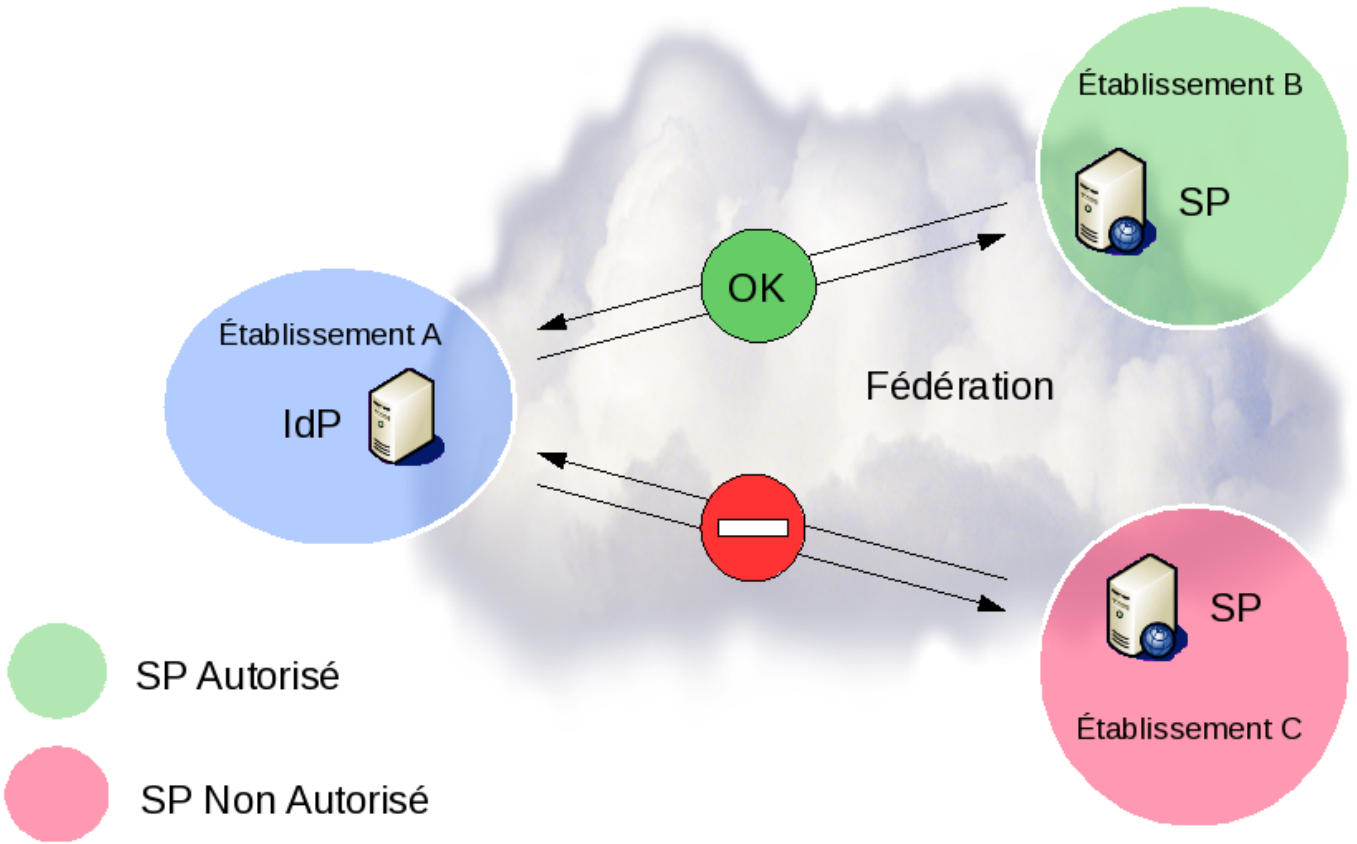
- Gestion de la propagation d'attributs.
- Définition en fonction des fournisseurs de services.
- Utilisation du système ARP.

Exemple de défintion :

```
<Rule>
 <Target>
        <Requester
        matchFunction="urn:mace:shibboleth:arp:matchFunction:exactShar">
        http://shibboleth.ebscohost.com
        </Requester>
 </Target>

 <Attribute
        name="urn:mace:dir:attribute-def:eduPersonScopedAffiliation">
   <AnyValue release="permit"/>
 </Attribute>
</Rule>
```

# Mise en oeuvre à UT1
## Restriction sur la propagation



# Plan

# Exemple simple
## Connexion au service EBSCO : Les problématiques

- EBSCO : Portail documentaire électronique payant.
- Souscription d'un abonnement annuel pour l'université Toulouse 1.
- Accés réservé aux membres de l'Université (Personnels/Etudiants).
- Problématique de la restriction d'accés pour EBSCO :
  - Compte générique pour l'Université Toulouse 1.
  - Restriction sur l'IP des clients.
- Problématique des utilisateurs :
  - Accés aux ressources uniquement depuis l'université.
  - Utilisation de solutions de type VPN.

# Exemple simple
## Connexion au service EBSCO : Utilisation de la fédération

DEMONSTRATION

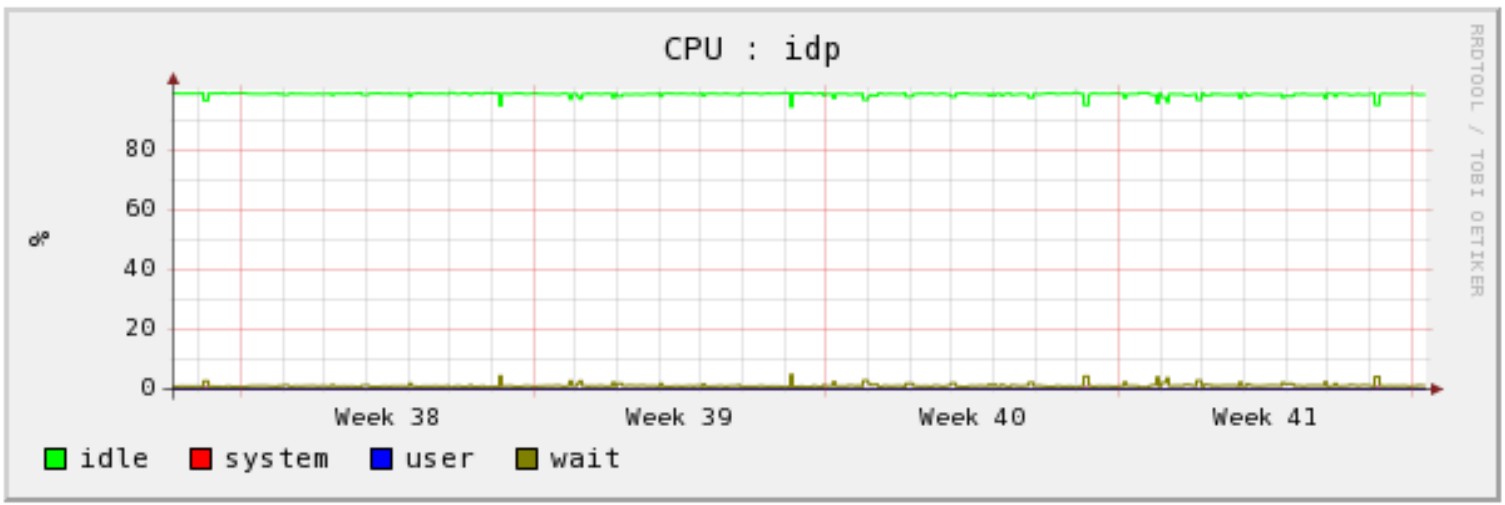
`http://search.ebscohost.com/login.aspx?authtype=shib`

# Plan

# Mise en oeuvre à UT1
## Hébèrgement

Service très peu gourmand en ressources.
Bon candidat à la virtualisation.

- Machine virtuelle Xen.
- Distribution Centos 5.
- 512 Mo de RAM

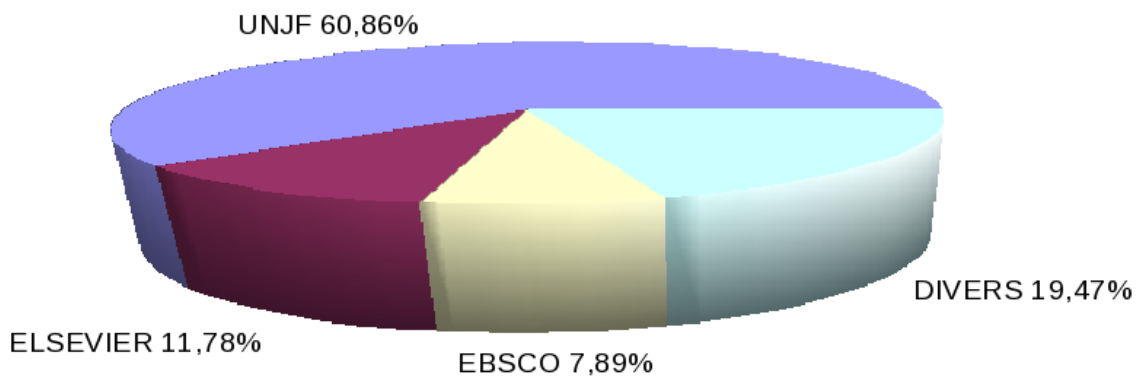



**Past Month**

# Les usages actuels
## Etat des lieux des accés

- Répartition des accés par population :
  - 91 % d'étudiants.
  - 9 % de personnels.

- Répartition des accés par fournisseurs de services :



# Plan

# Réflexions

- Réalisation d'une chaine de test complète du système d'authentification.
- Shibbolethisations de nouveaux services (Internes ou externes).
- Mise en haute disponibilité du service IdP ?
- Intérêt dans le cadre d'une UNR ?

# Plan

# Bilan

- Service à haute valeur ajoutée.
- Service peu couteux à mettre en place.
- Temps de déploiement lié à l'existant (< 3 jours).
- Perspectives Intéressantes liées au développement des SP.
- Ne permet pas de s'affranchir de référentiels à jour et de systèmes d'authentification sécurisés.
- Réelle satisfaction des utilisateurs.
  - Simplicité d'utilisation.
  - Mobilité favorisée.
  - Unifications des authentifications.