RENATER
CONNECTEUR DE SAVOIRS

La fédération d'identités, pourquoi et comment ?

Olivier Salaün, RENATER
ANF Mathrice 2014

RENATER

- Opérateur du réseau enseignement et recherche
- Sécurité
  - Le CERT RENATER
  - Animation réseau des RSSI
  - Certificats TCS
  - Fédération Education-Recherche
- Services applicatifs
  - Eduroam, eduspot
  - RENAvisio
  - Universalistes, FileSender, Partage, Antispam
  - Sympa, Sourcesup

RENATER

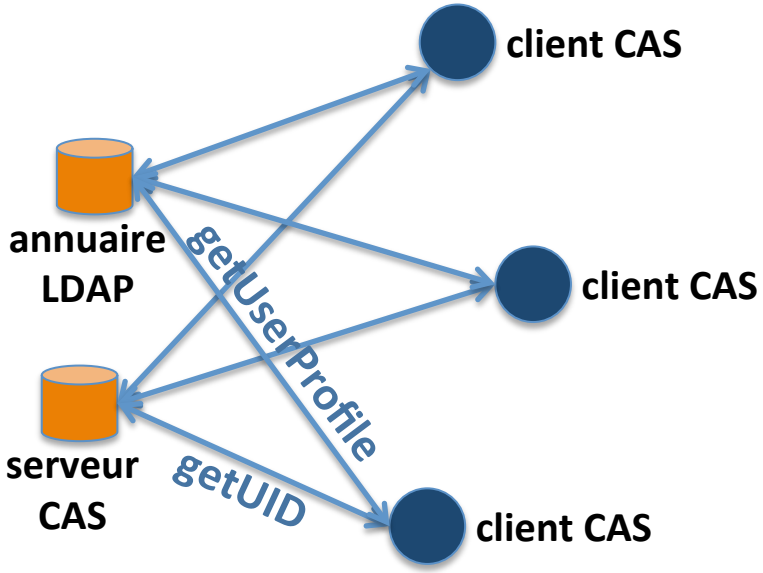
- Autres activités
  - Formations (Fédération, IPv6, Sympa)
  - Organisation des JRES
  - Relations internationales (GEANT, TERENA)
- En savoir plus
  - http://www.renater.fr
- Contact
  - support@renater.fr

Le menu...

1. l'authentification pour des services nationaux
2. fédération d'identités, principes de fonctionnement
3. l'envers du décor
4. le cercle de confiance
5. mettre en oeuvre la fédération d'identités
6. ressources proposées par RENATER
7. Moonshot, service d'autorisation

Gérer l'authentification pour des services nationaux

- CAS, le SSO d'établissement
  - utilisation en interne
  - cas d'utilisation : ENT, CMS, Webmail, etc



Gérer l'authentification pour des services nationaux

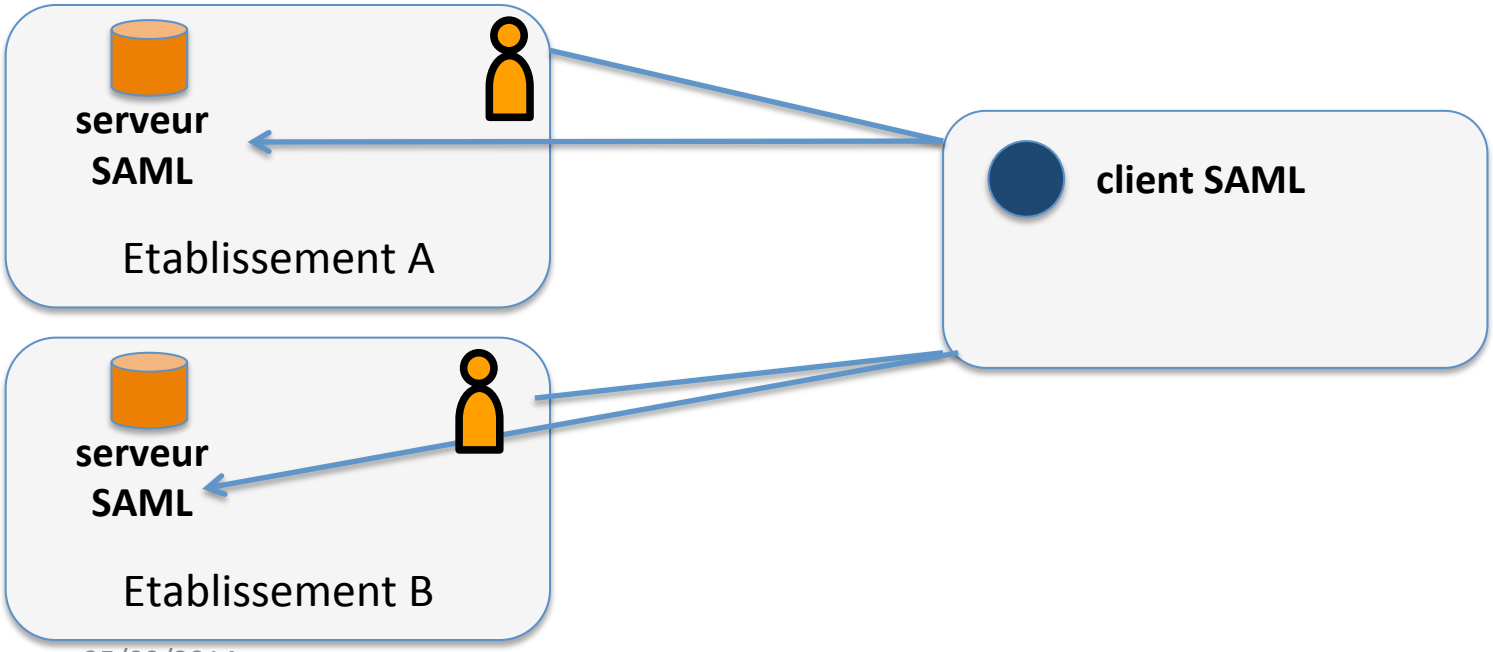
- Les situations plus complexes
  - éditeur de documentation élec (Ex : Elsevier)
  - services mutualisés en région (Ex : PRES, UNR)
  - services nationaux mutualisés (Ex : RENATER, Ministère, Esup)
  - services de communautés (Ex : Mathrice)
  - services de communautés internationales

Gérer l'authentification pour des services nationaux

- Ce qu'il manque à CAS pour passer à l'échelle
  - un client CAS ne connait qu'un seul serveur CAS
  - pas de normalisation de l'accès aux attributs utilisateurs
  - contrôler qui peut interroger le serveur CAS

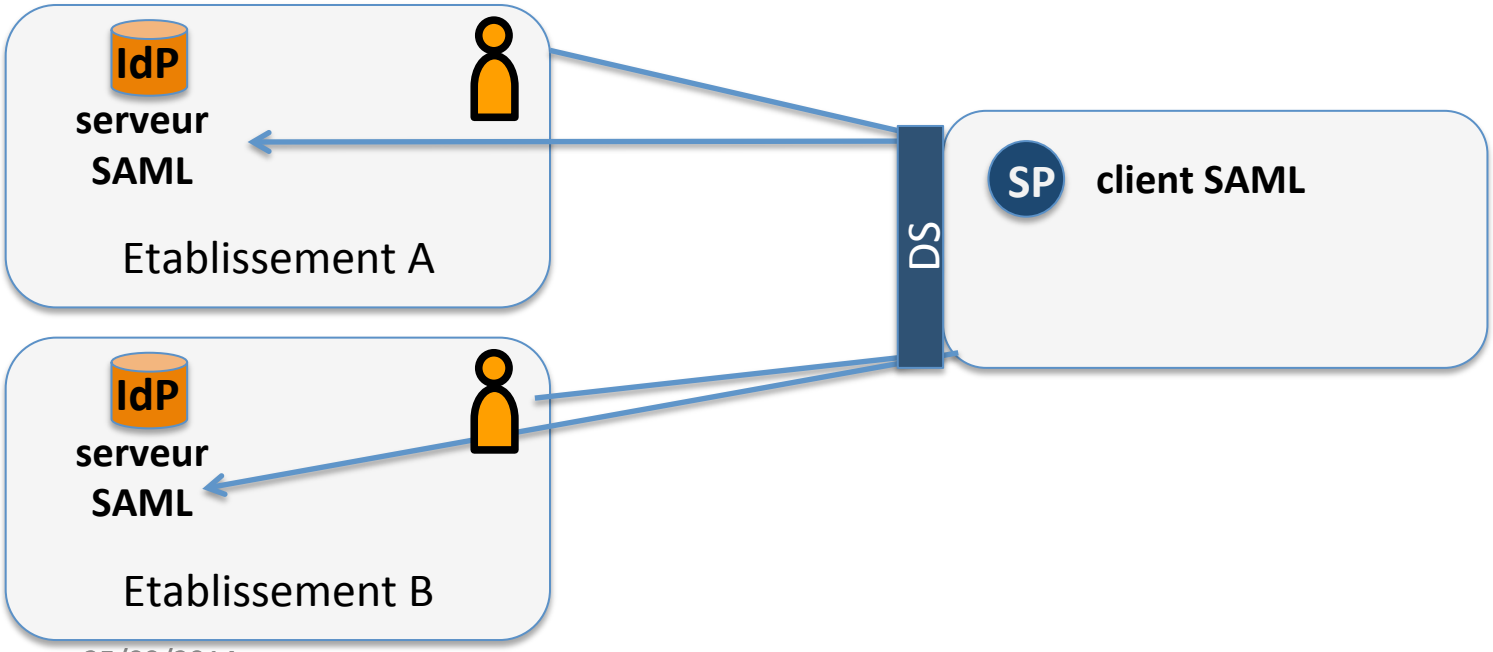
Fédération d'identités
Principes de fonctionnement

- un client SAML délègue l'authentification à un serveur SAML autoritatif pour l'utilisateur
- le client SAML connait la liste des serveurs SAML
- l'utilisateur ne divulgue pas ses éléments d'authentification au client SAML



Terminologie SAML

- Fournisseur d'identités ou IdP
- Fournisseur de service ou SP
- Service de découverte ou DS/WAYF



Principe de fonctionnement le fournisseur d'identités (IdP)

- Authentification de l'utilisateur
  - Peut être un client CAS
  - Preuve d'authentification = assertion SAML
  - Session utilisateur
- Transmet le profil de l'utilisateur
  - Via le protocole SAML2
  - Données issues des référentiels (LDAP ou SQL)
  - Richesse du profil utilisateur paramétrable

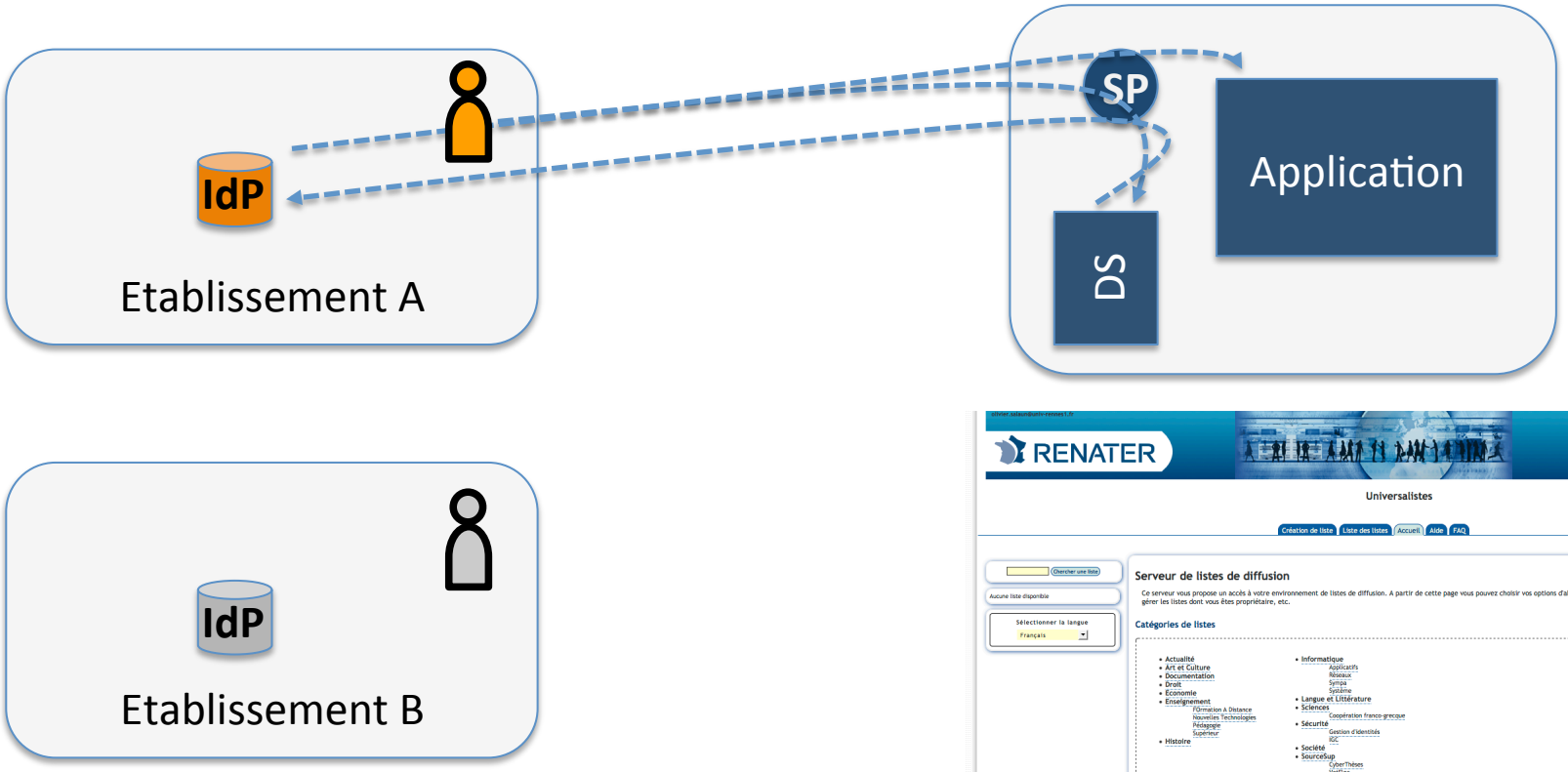
Principe de fonctionnement le fournisseur de service (SP)

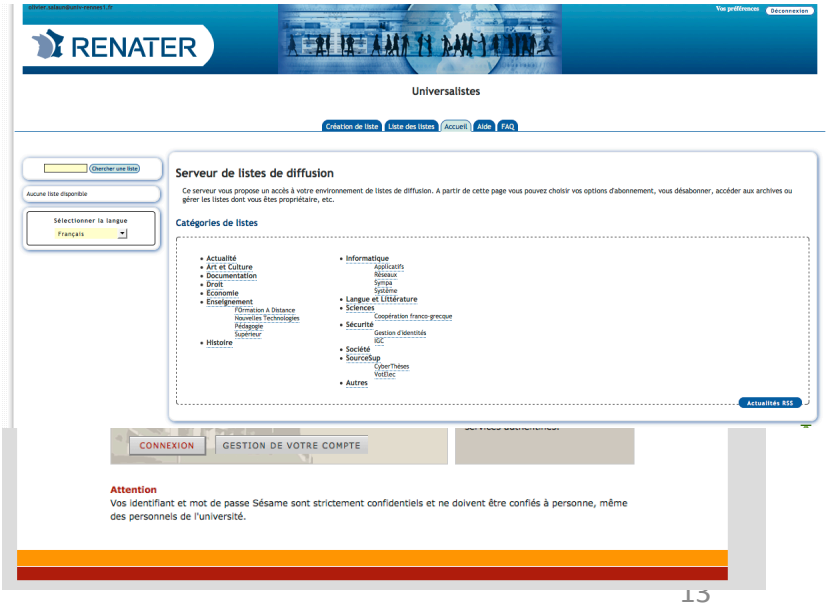
- en amont d'une application
  - API varie selon implémentation SP
- renvoie l'utilisateur vers son IdP
  - passage par le service de découverte (DS/WAYF)
  - retour de l'IdP avec un profil utilisateur
  - Session utilisateur
- gestion du contrôle d'accès
  - dans l'application
  - à partir des attributs utilisateur reçus

Demonstration

- https://filesender.renater.fr/
- https://antispam.renater.fr/
- http://www.sciencedirect.com/
- https://neugrid4you.eu/

Le workflow d'authentification





L'envers du décor
le service de découverte (DS/WAYF)

- fonction d'orientation de l'utilisateur
  - vers son IdP
- fonctionnement
  - menu déroulant
  - search as you type
  - pré-sélection
- qui l'opère ?
  - RENATER
  - ou l'établissement gérant l'application cible

L'envers du décor
le protocole SAML

- Protocole d'authentification
  - normalisé par le consortium OASIS
  - basé sur XML
- Fonctionnalités
  - Assertions d'authentification
  - Assertions d'échange d'attributs
  - Signature et chiffrement
- Version 2.0
  - publié en 2005
  - Interopérabilité possible avec les produits SAML 2

L'envers du décor
les méta-données SAML

- fichier descriptif d'une entité SAML
  - un SP, un IdP
  - un ensemble de SPs et d'IdPs
- permet les échanges entre entités SAML
  - délégation de l'authentification
  - signature/chiffrement des assertions
- contenu d'un fichier de méta-données
  - Identifiant de l'entité, URL, certificat, profils SAML supportés, contacts, description,...
- Exemple
  - https://federation.renater.fr/test/renater-test-metadata.xml

Le cercle de confiance

- terminologie
  - fédération = cercle de confiance
  - ex : fédération Education-Recherche
- constitution
  - des SPs
  - des IdPs
- résout la problématique des relations bilatérales
- les membres du cercle de confiance partagent
  - un niveau de confiance
  - un cadre technique
  - des méta-données SAML

La fédération Education-Recherche https://federation.renater.fr/

- un cercle de confiance
  - pour la communauté E/R française
  - opéré par le RENATER
- Concrètement c'est :
  - les chartes membre/partenaire,
    - articulation avec SAGA
  - le cadre technique,
    - SAML2, Supann 2009
  - les méta-données SAML + filtres d'attributs
  - le guichet de la fédération
  - les outils de test

Qui utilise la fédération ?

https://federation.renater.fr/registry?action=view_all&federation=renater

- 227 fournisseurs d'identités
  - uniquement des établissement E/R français
- 521 services fédérés
  - incluant des services commerciaux
  - typologie
    - ressources documentaires
    - e-learning
    - outils collaboratifs
    - accès Wi-Fi
    - applications métier mutalisées
    - distribution de logiciel

D’autres cercles de confiance

- D’autres fédérations E/R
  - dans 46 pays
  - https://refeds.org/resources/resources_list.html
- eduGAIN inter-fédération
  - une inter-connexion de fédérations E/R
  - http://edugain.org/
  - inscription depuis le guichet RENATER
    - par défaut pour les IdP
    - optionnelle pour les SP
- gérer une fédération, hébergée par RENATER
  - principe : fédération as a service
  - via le guichet RENATER
  - https://services.renater.fr/federation/docs/fiches/fed-locale

Le guichet de la fédération RENATER les fonctionnalités

- enregistrement d'un SP/IdP
  - dans fédération de Test
  - dans fédération Education-Recherche
- publication des données
  - génération des méta-données
  - affichage des IdP/SP sur le site de la fédération
- processus de validation
  - délégué aux contacts fédération des organismes

Le guichet de la fédération
Qui y accède ?

- les contacts techniques des entités SAML déclarées
  - inscription d'une entité SAML (SP, IdP)
  - édition des informations techniques
- les contacts fédération des organismes membres
  - vue synthétique des entités SAML
  - validation des inscriptions, mises à jour

Le guichet de la fédération https://federation.renater.fr/registry

Espace contact fédération - Validation des entités SAML

- sp / annuaire pages blanches TMSP php_shibbolisé -
- sp / http://trombi.it-sudparis.eu/ -

Description de l'entité SAML			Fédérations disponibles			
Type	Intitulé et identifiant	Organisme de rattachement	Fédération de Test	Fédération Education-Recherche	Fédération de l'Université Paris Saclay	Fédération Institut Mines Telecom
idp	IDP-Partenaires https://idpext.tem-tsp.eu/idp/shibboleth	Telecom & Management sud Paris	●	●	●	●
idp	Telecom SudParis et Telecom Management https://idpr.tem-tsp.eu/idp/shibboleth	Telecom & Management sud Paris	●	●	●	●
idp	Telecom et Management SudParis v2.3.3 https://idp.it-sudparis.eu/idp/shibboleth	Telecom & Management sud Paris	●	●	●	●
idp	idp-imt1-bc-ups https://idp-imt1-bc.tem-tsp.eu/idp/shibboleth	Telecom & Management sud Paris	●	●	●	●
sp	Blogs M & T SudParis https://wp.tem-tsp.eu/shibboleth	Telecom & Management sud Paris	●	●	●	●
sp	Institut Telecom - Blogs Tet M SudParis https://blog.it-sudparis.eu/	Telecom & Management sud Paris	●	●	●	●
sp	Mines-Telecom CMS https://mutuel.mines-telecom.fr/sp	Telecom & Management sud Paris	●	●	●	●
sp	Pages WEB publiques users https://www-public.it-sudparis.eu	Telecom & Management sud Paris	●	●	●	●
sp	Portail Captif Eduspot -Télécom Ecole de Management & Télécom SudParis https://portail.tem-tsp.eu/authsaml2/metadata	Telecom & Management sud Paris	●	●	●	●
sp	Telecom et Management SudParis Webspace https://www-public.it-sudparis.eu/shibboleth	Telecom & Management sud Paris	●	●	●	●
sp	Université Paris Saclay - Wikis https://wups.tem-tsp.eu/sp	Telecom & Management sud Paris	●	●	●	●
sp	annuaire pages blanches TMSP php_shibbolisé https://annu.it-sudparis.eu/	Telecom & Management sud Paris	●	⛔	⛔	⛔
sp	http://trombi.it-sudparis.eu/ https://trombi.it-sudparis.eu	Telecom & Management sud Paris	●	⛔	⛔	⛔

Mise en oeuvre
les étapes

1. mettre en place les briques techniques
2. branchement au système d'information
3. inscription auprès de RENATER

Les implémentations SAML

- un large choix
  - Shibboleth, SimpleSAMLPhp, EZProxy, modMellon, OIOSaml, OpenSSO
- spécifications SAML2 complexes
  - interopérabilité pas toujours garantie
  - sauf à définir un cadre technique
    - Ex : http://saml2int.org/

Les implémentations SAML Shibboleth

- Une implémentation du protocole SAML
  - logiciel open source
  - http://shibboleth.net
  - issu de la communauté E/R
    - d'abord aux USA
    - aujourd'hui un consortium
- Trois logiciels
  - Shibboleth IdP
  - Shibboleth SP
  - Shibboleth DS (pas utilisé par RENATER)

Les implémentations SAML Shibboleth

- atouts
  - très configurables
  - éprouvé (depuis 2003)
- bien adaptés au contexte E/R
- implémentation de référence pour RENATER
  - supports de formation pour Shibboleth
  - modèles de configuration pour Shibboleth
  - assistance via liste federation-utilisateurs
  - RENATER contribue financièrement au consortium

Mise en oeuvre d'un IdP Shibboleth

- une instance par organisme
- choix de l'implémentation
  - Shibboleth
    - 99% des IdP dans la fédération Education-Reherche
- technologie
  - servlet Java
- articulation avec CAS
  - optionnel (via un filtre Tomcat)
  - d'autres handler d'authentification proposés

Mise en oeuvre d'un IdP Shibboleth

- articulation avec le référentiel utilisateurs
  - connecteurs LDAP, SQL
  - fonctions de mapping (intitulé attribut ou valeur)
  - fonctions de transformation
- tester
  - SP de test de RENATER
  - fédération de test de RENATER
- passage en production
  - activation service fédération pour votre organisme
    - via le service SAGA
  - inscription dans la Fédération Education-Recherche
    - via le guichet de la fédération
  - configuration de l'IdP
    - utilisation des méta-données SAML

Mise en oeuvre d'un SP Shibboleth

- en amont d'une application web
  - une instance dédiée
  - ou mutualisation via un reverse-proxy
- choix de l'implémentation
  - Shibboleth
    - 90% des SP dans la fédération Education-Reherche
- technologie
  - module Apache (ou IIS) + un démon
  - RPMs disponibles

Mise en oeuvre d'un IdP Shibboleth

- adapter l'application web
  - pour exploiter des variables d'environnement
    - notamment REMOTE-USER
- déployer un service de découverte (DS/WAYF)
  - dédié à l'application ou mutualisé
- tester
  - IdP de test de RENATER
  - fédération de test de RENATER
- passage en production
  - activation service fédération pour votre organisme
    - via le service SAGA
  - inscription dans la Fédération Education-Recherche
    - via le guichet de la fédération
  - configuration du SP
    - utilisation des méta-données SAML

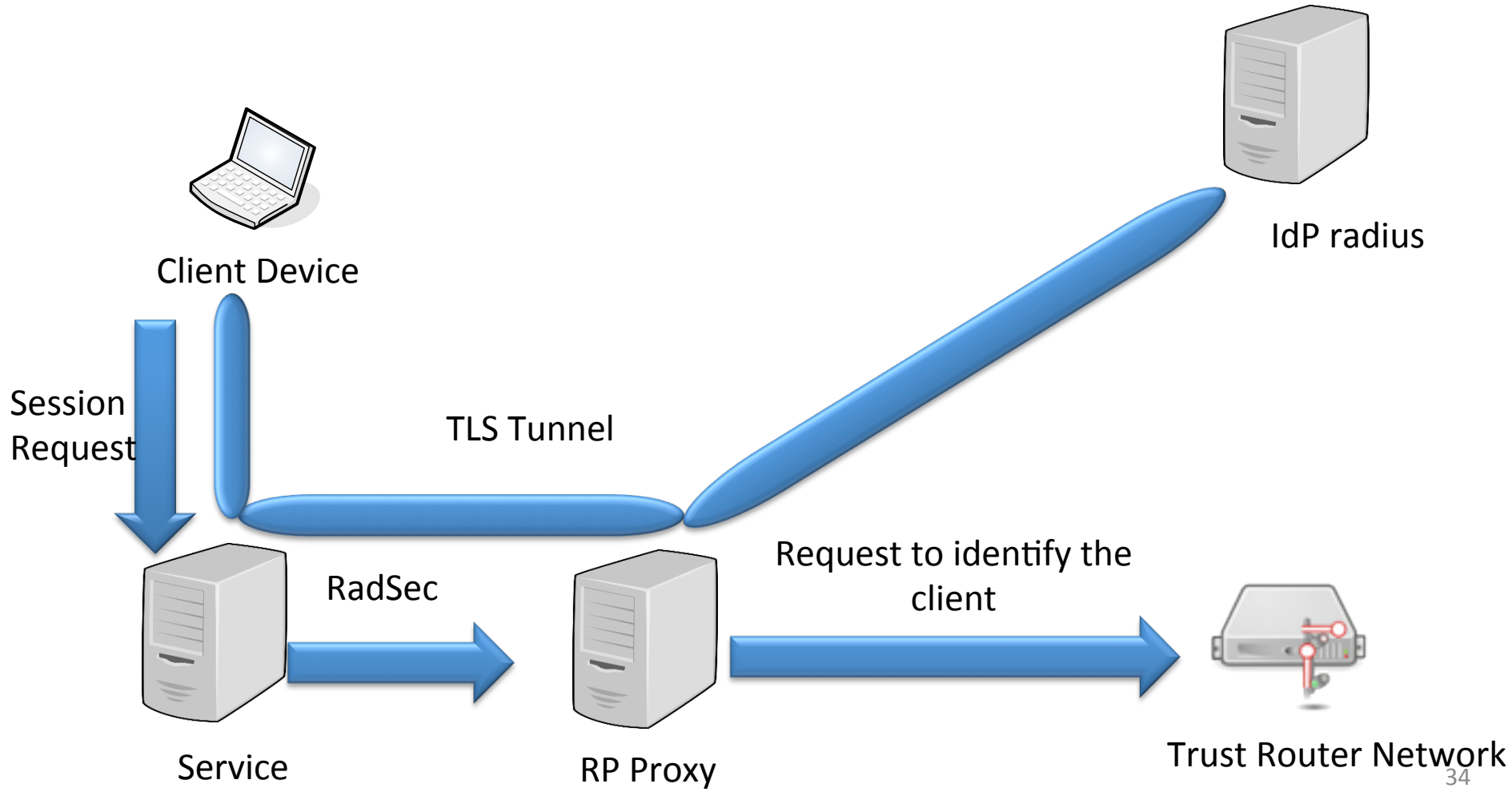
RENATER met à votre disposition

- le site de la fédération
  - https://federation.renater.fr
- des services de test
  - IdP, SP, WAYF, fédération
- des documentation d'installation
- une liste de discussion
  - federation-utilisateurs@listes.renater.fr
- des formations régulières
  - prochaine : début 2015

Moonshot
https://community.ja.net/groups/moonshot

- principe de Moonshot
  - utiliser les comptes institutionnels des établissements
  - pour des applications non web
- parallèle avec
  - fédération d'identités
  - eduroam
- Technologies
  - authentification Radius
  - autorisation basée sur SAML
  - implémentation cliente : GSS-API

Moonshot architecture



Moonshot contexte

- projet GEANT (réseau académique pan-européen)
  - initiative JANET (réseau académique UK)
  - en phase pilote
- standardisation technologie en cours
  - RFC 7055 du groupe IETF ABFAB
    - Application Bridging for Federated Access Beyond web
- RENATER
  - travail en cours
  - projet de mise en oeuvre d'un Trust Router national
    - 2015

Moonshot
Mise en oeuvre pour un établissement

- identifier les applications
  - compatibles GSS-API
- déployer un client Moonshot
  - en amont de l'application
- disposer d'un IdP SAML2
- disposer d'un serveur Radius
  - utilisant RadSec

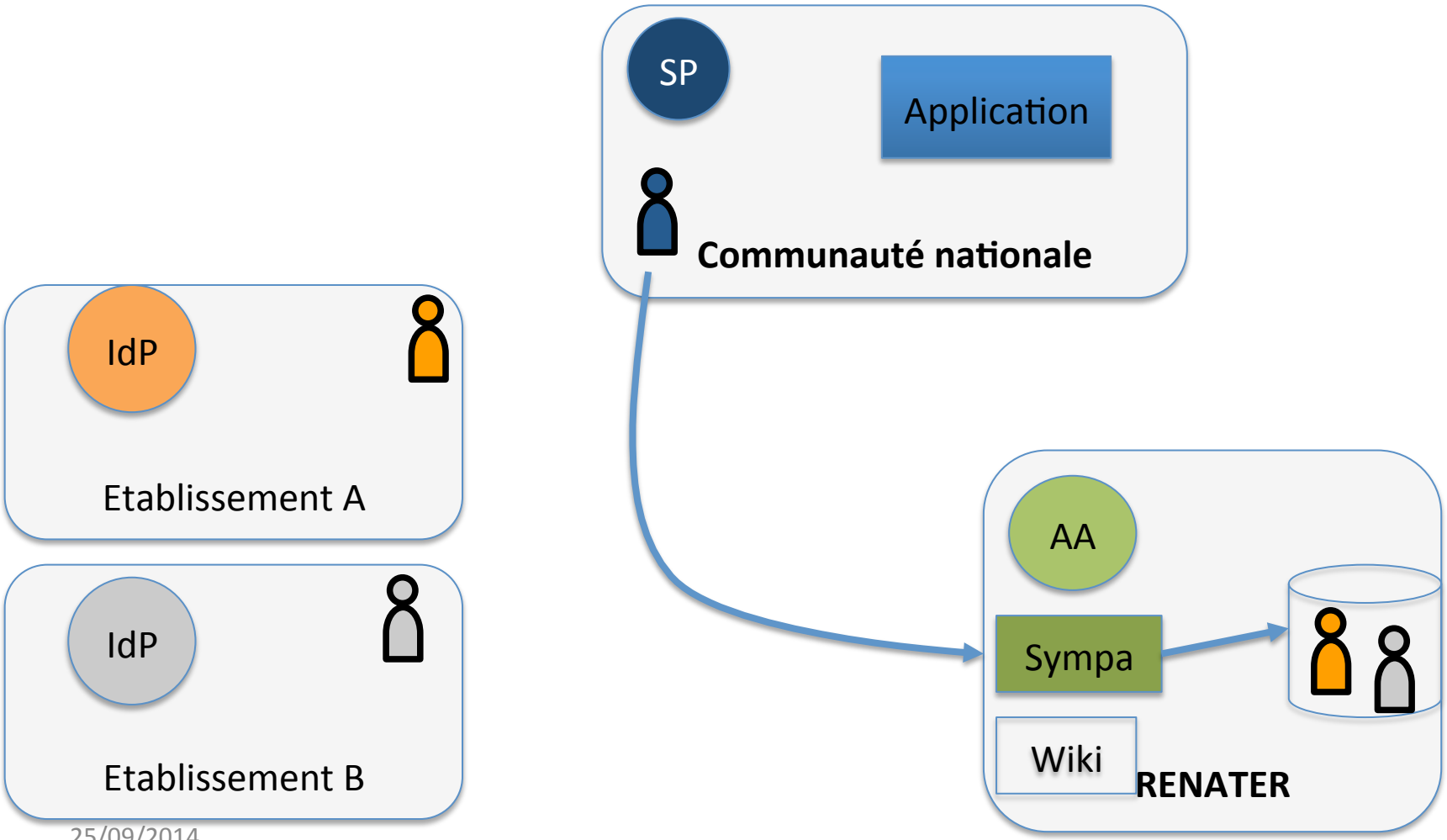
Un service d'autorisation basé sur des groupes

- Expression de besoin de quelques groupes d'utilisateur
- Maquette mise en place fin 2013
- Phase pilote en cours
  - pas encore de nom pour le service
  - pas encore de documentation officielle
- Mathrice
  - ça pourrait correspondre à vos cas d'utilisation

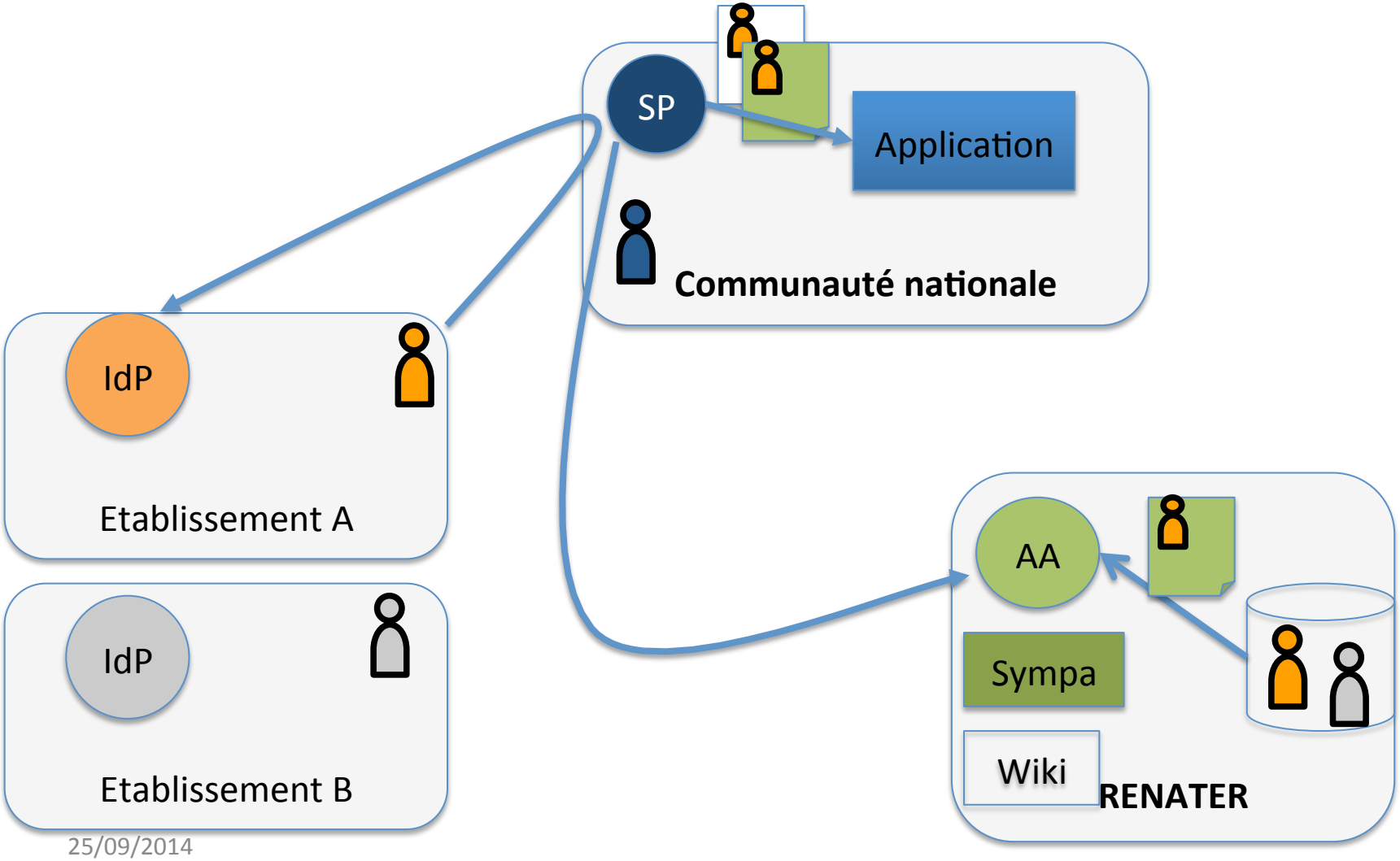
Service d'autorisation RENATER
Principe de fonctionnement

- permettre un contrôle d'accès unifié
  - à plusieurs applications
  - pour une population issue de différents organismes
- le référentiel de groupes
  - est géré par un serveur de groupe
  - avec le logiciel Sympa
  - interrogé via le protocole SAML
    - Attribute Authority
- intégration applicative
  - non intrusive
  - configuration du SP pour interroger le référentiel de groupes

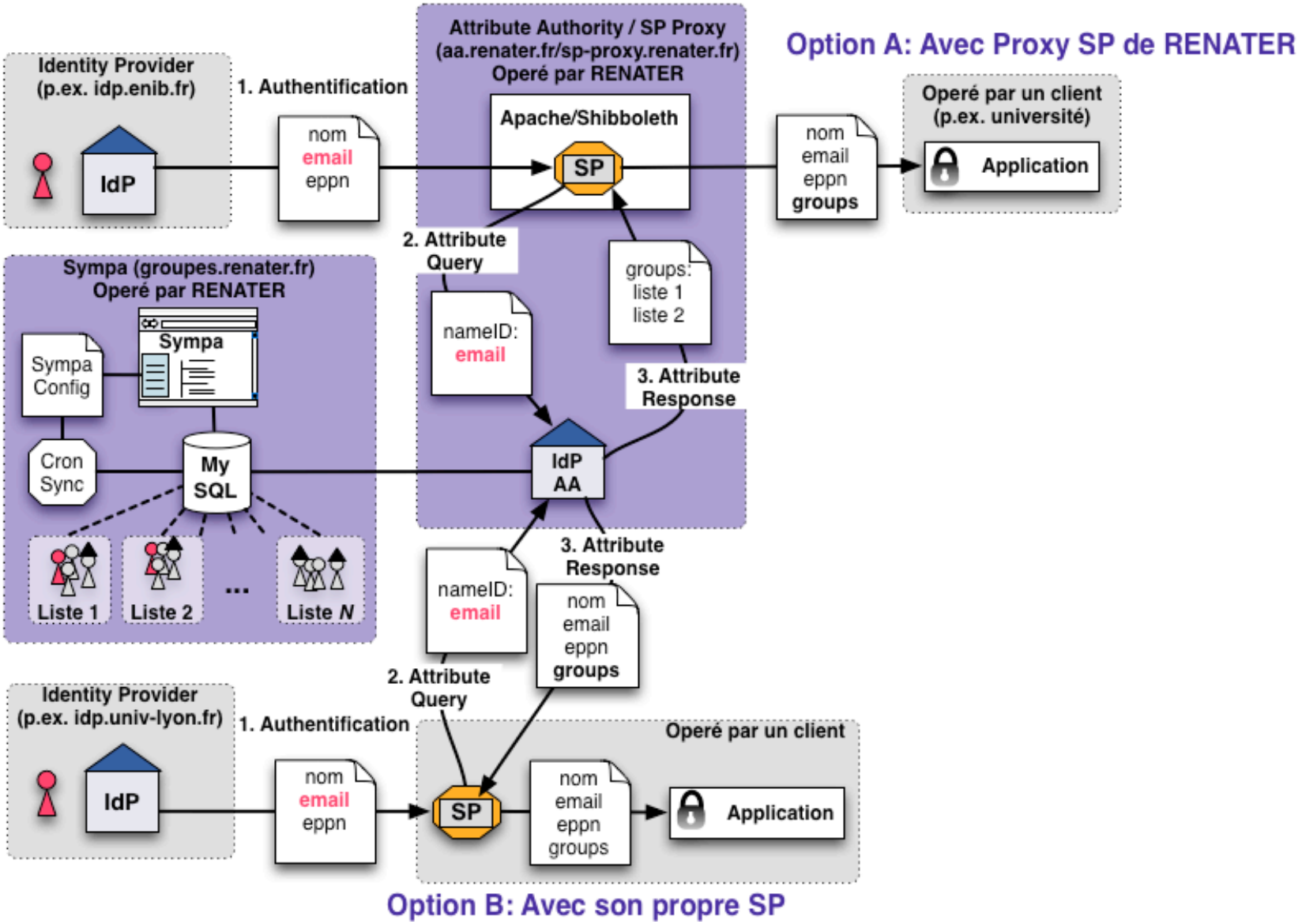
Service d'autorisation RENATER
Alimentation des groupes



Service d'autorisation RENATER
Contrôle d'accès



Service d'autorisation - Architecture



Service d'autorisation
Workflow pour mise en place

Un gestionnaire (G) d'application décide d'utiliser le service d'autorisation de RENATER

1. G crée un groupe (liste) sur Universalistes
   - Un paramètre allowed_sps indique les identifiants des SPs autorisés à voir ce groupe
2. G alimente les membres du groupe
   - Soit par abonnement (statiquement)
   - Soit inclusion source de données externe (dynamique)
3. G configure le SP (en amont de l'application)
   - Interrogation de l'attribute authority de RENATER
4. G définit une règle de contrôle d'accès
   - Soit au niveau Apache
   - Soit au niveau de l'application

Service d'autorisation
Vu de l'utilisateur

- Il accède classiquement à l'application
- Il s'authentifie auprès de son IdP
- Il doit être référencé dans le groupe Sympa

Service d'autorisation
Configuration du SP

```
<AttributeResolver type="Chaining">
   <AttributeResolver type="Query" subjectMatch="true" />
   <AttributeResolver type="SimpleAggregation" attributeId="mail"
            format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
     <Entity>https://sympa.example.org/idp/shibboleth</Entity>
   </AttributeResolver>
</AttributeResolver>
```

- documentation
  - https://services.renater.fr/federation/docs/fiches/sympa_attribute_provider

Service d'autorisation
Qui gère quoi ?

- RENATER gère
  - l'Attribute Autority
  - le serveur Sympa
- Le gestionnaire d'application gère
  - le SP en amont de l'application
  - les règles de contrôle d'accès dans son application
  - les membres de son groupe