RENATER
CONNECTEUR DE SAVOIRS

Un service d'autorisation pour les groupes (VOs) avec Sympa

Jean-François Guezou, RENATER

Journées SUCCES, 6 novembre 2015, Paris

RENATER
CONNECTEUR DE SAVOIRS

Sommaire

GIP RENATER

Un groupement d'intérêt public
Les organismes membres
Les missions
Le réseau
Les services

Le service d'autorisation pour VO

La fédération d'identités
L'Autorité d'Attributs
La plate-forme Sympa
La fonction SympaAA
Des Ressources

RENATER
CONNECTEUR DE SAVOIRS

GIP RENATER

Les organismes membres

Géosciences pour une Terre durable
brgm

cea
DE LA RECHERCHE À L'INDUSTRIE

irstea

cirad
LA RECHERCHE AGRONOMIQUE POUR LE DÉVELOPPEMENT

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

INRA
SCIENCE & IMPACT

Inria
INVENTEURS DU MONDE NUMÉRIQUE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE
DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

Instituts thématiques
Inserm
Institut national de la santé et de la recherche médicale

IRD
Institut de recherche pour le développement

cnrs
dépasser les frontières

Conférence des présidents d'université

ONERA
THE FRENCH AEROSPACE LAB

GIP RENATER

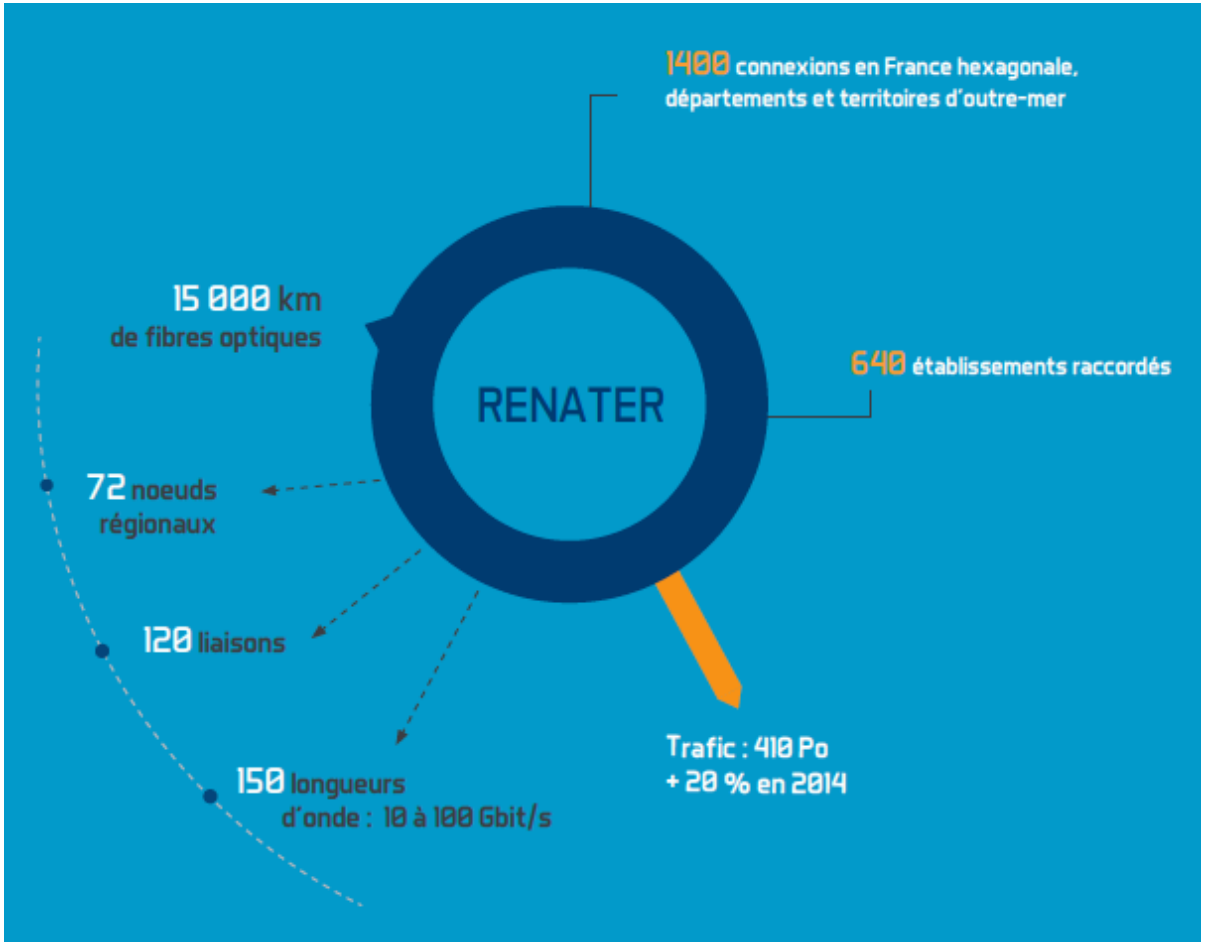
Les Missions

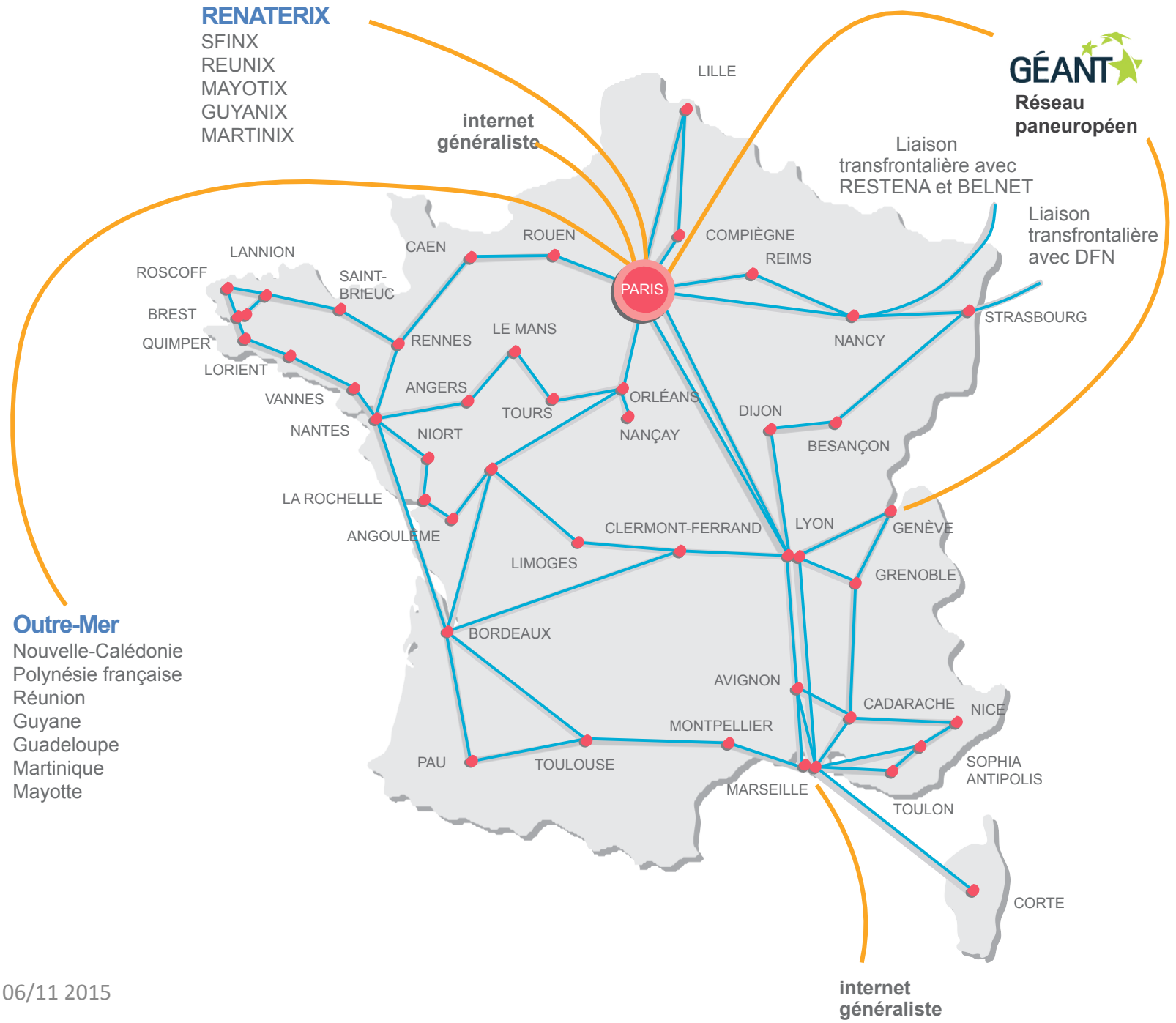
Offrir un réseau et des services de haute qualité, performants, sécurisés et innovants pour les besoins de la Communauté Enseignement/Recherche.

- Maîtrise d'ouvrage d'un réseau de communications pour la recherche, le développement technologique et l'enseignement
- Maîtrise d'ouvrage des services de communication (gestion des adresses, DNS,..)
- Garantir la disponibilité et la non altération des données
- Aider au développement des réseaux de collecte et à leur interconnexion nationale
- Assurer les communications avec les NRENs des autres pays

Le Réseau

Une Infrastructure fiable, robuste et sécurisée



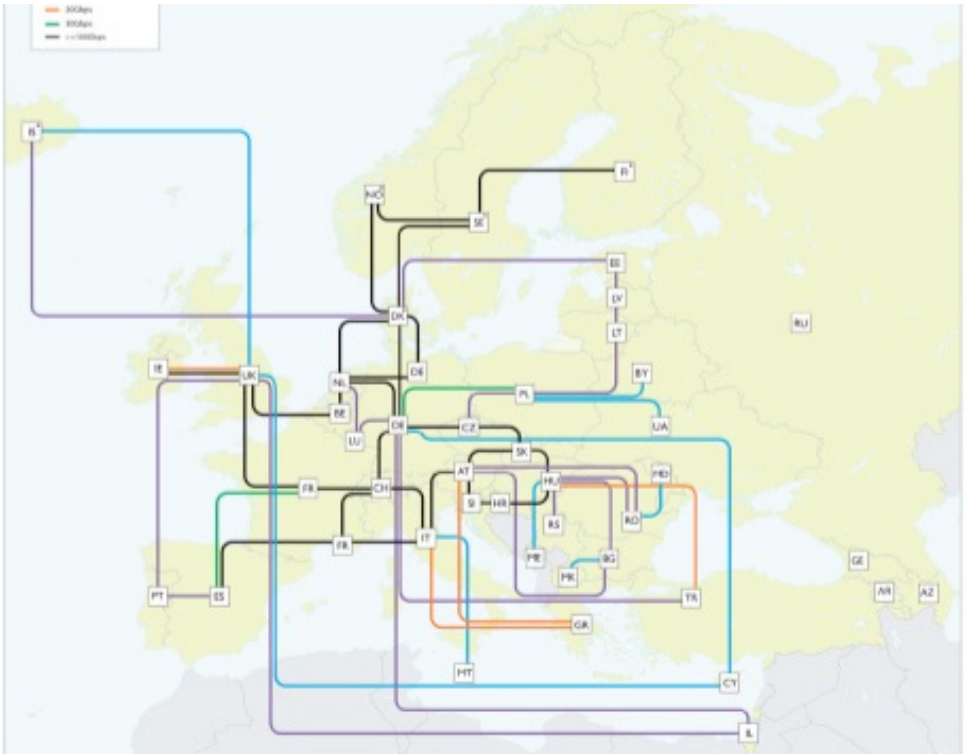

RENATERIX
SFINX
REUNIX
MAYOTIX
GUYANIX
MARTINIX
internet généraliste
GÉANT
Réseau paneuropéen
Liaison transfrontalière avec RESTENA et BELNET
Liaison transfrontalière avec DFN
Outre-Mer
Nouvelle-Calédonie
Polynésie française
Réunion
Guyane
Guadeloupe
Martinique
Mayotte
internet généraliste
LILLE
ROUEN
CAEN
COMPIÈGNE
REIMS
PARIS
LANNION
ROSCOFF
SAINT-BRIEUC
BREST
QUIMPER
LORIENT
RENNES
LE MANS
NANCY
STRASBOURG
VANNES
ANGERS
TOURS
ORLÉANS
NANÇAY
DIJON
NANTES
NIORT
BESANÇON
LA ROCHELLE
ANGOULÊME
CLERMONT-FERRAND
LYON
GENÈVE
LIMOGES
GRENOBLE
BORDEAUX
AVIGNON
CADARACHE
NICE
MONTPELLIER
PAU
TOULOUSE
SOPHIA ANTIPOLIS
MARSEILLE
TOULON
CORTE

RENATER
CONNECTEUR DE SAVOIRS

Le Réseau, L'Europe,…

GÉANT
ASSOCIATION

Architecture globalisée
au niveau européen et mondial



GÉANT, le réseau de recherche et d'éducation paneuropéen interconnecte 37 réseaux de recherche et d'enseignement nationaux de l'Europe (NREN). Ensemble, ils connectent plus de 50 millions d'utilisateurs à 10 000 institutions à travers l'Europe.

RENATER est raccordé à GEANT via 2 liaisons de 20 Gbit/s l'une de Paris et l'autre de Genève.

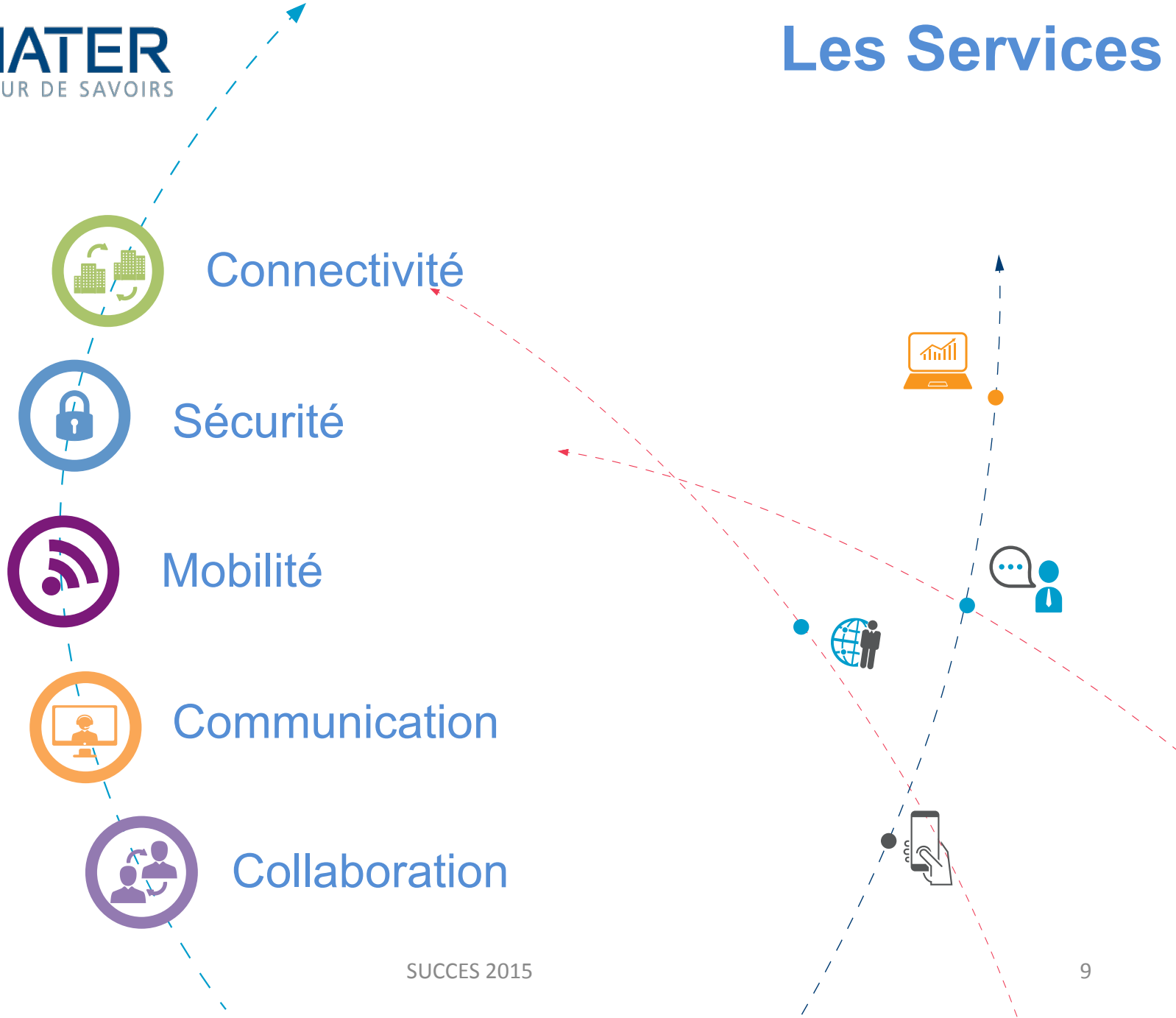
Le Réseau, L'Europe,…

GÉANT PROJECT
www.geant.net

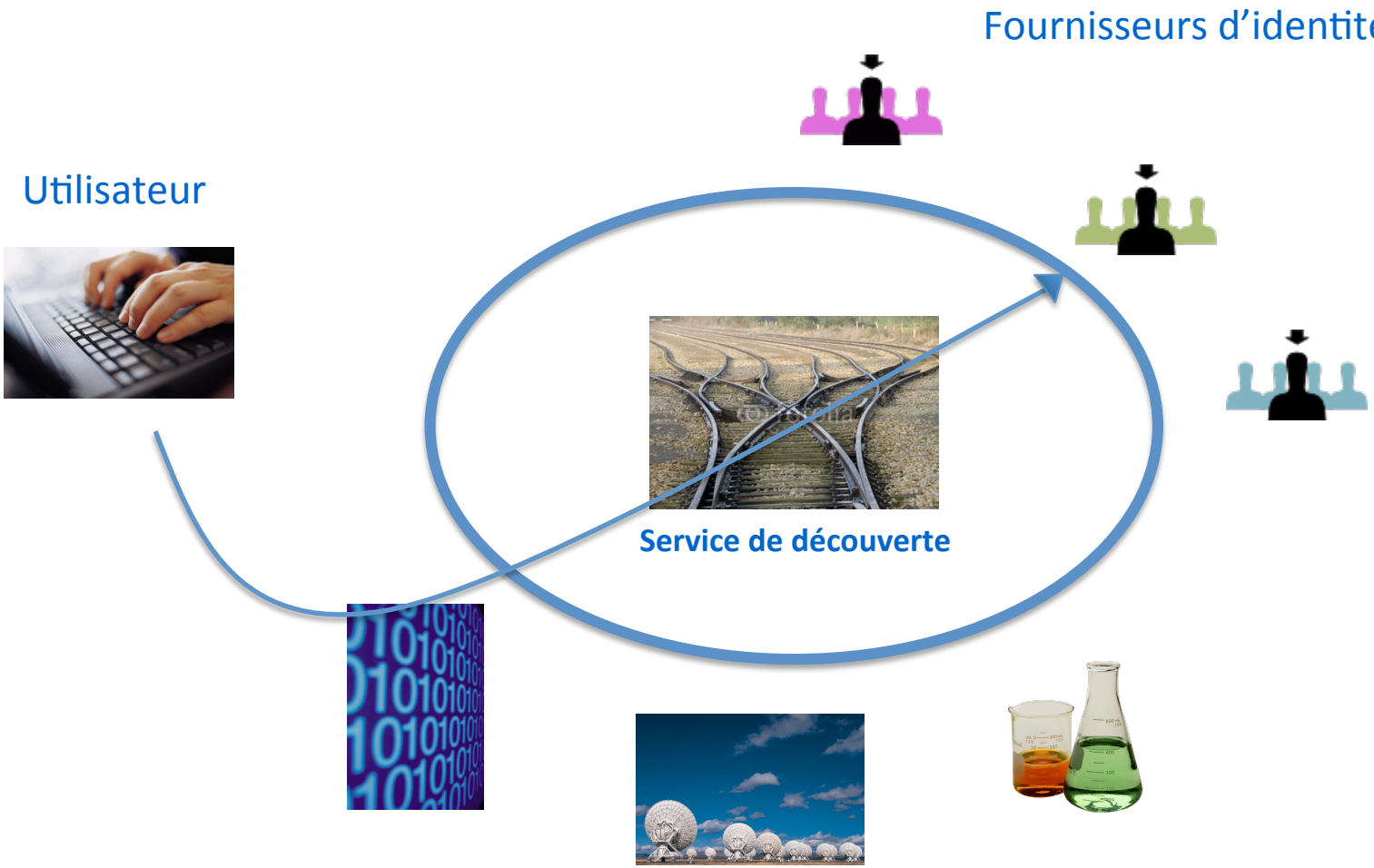
connect • communicate • collaborate

GÉANT is co-funded by the European Union within its 7th RSD Framework Programme.

Les Services

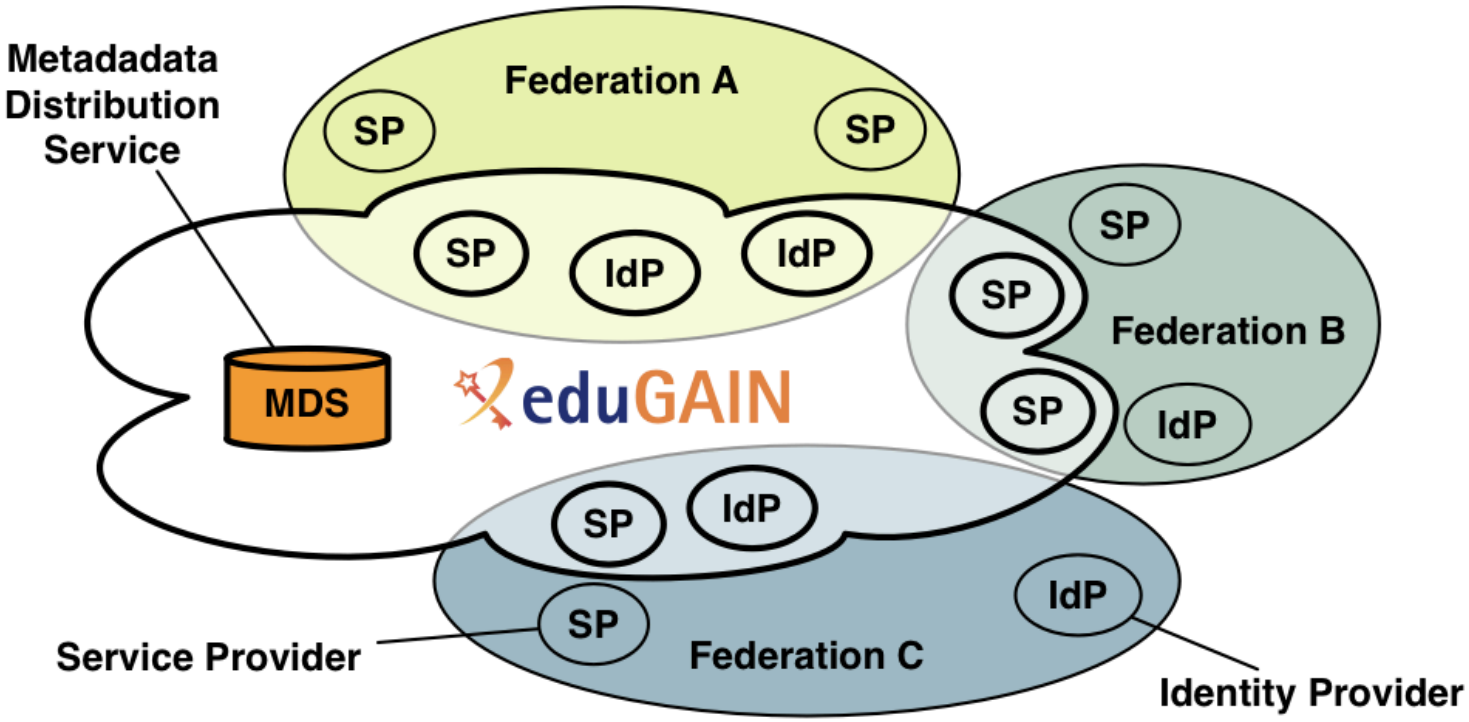


La fédération d'identités



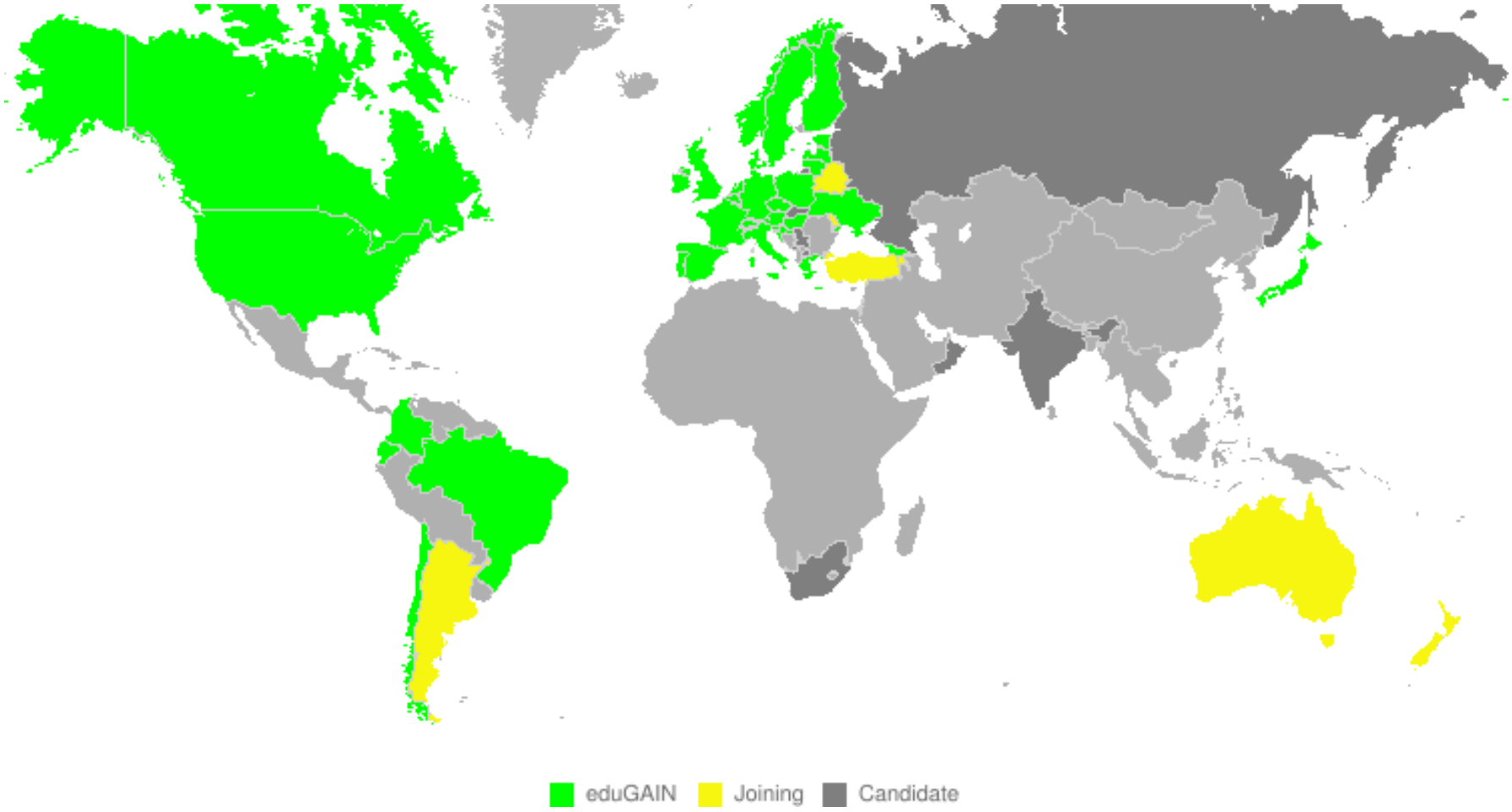
RENATER
CONNECTEUR DE SAVOIRS

eduGAIN

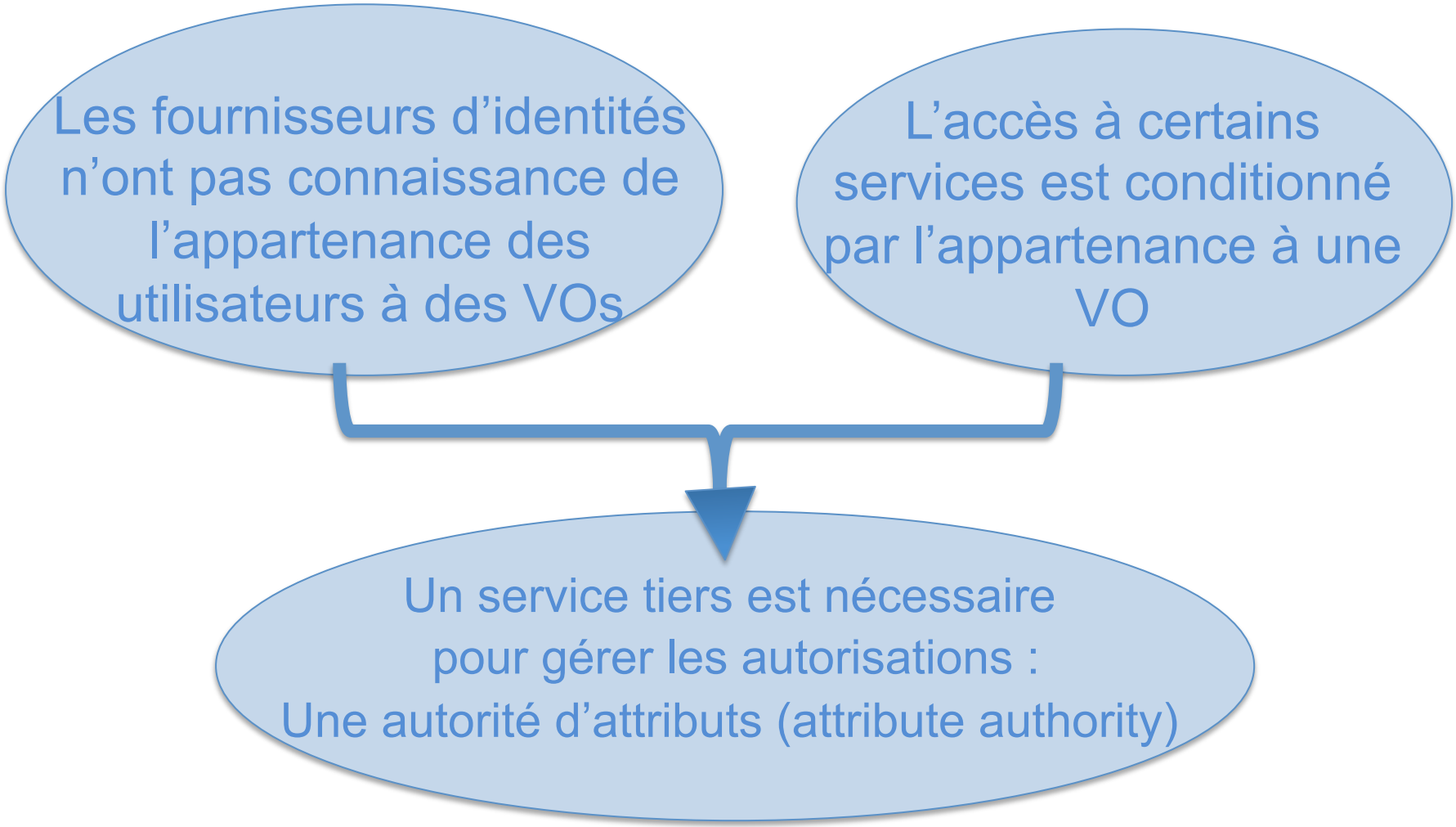


RENATER
CONNECTEUR DE SAVOIRS

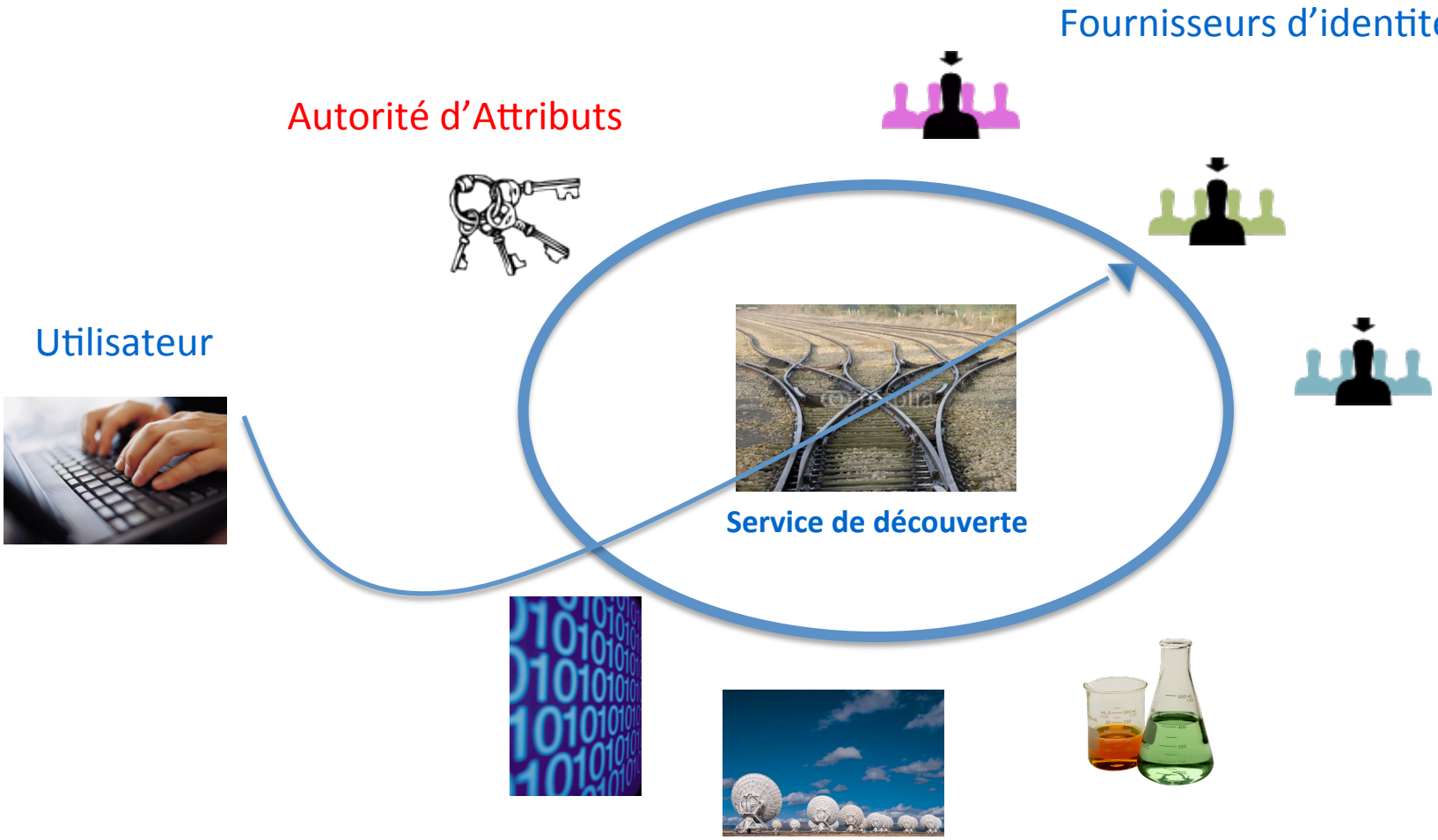
eduGAIN



Limites


Les fournisseurs d'identités n'ont pas connaissance de l'appartenance des utilisateurs à des VOs
L'accès à certains services est conditionné par l'appartenance à une VO
Un service tiers est nécessaire pour gérer les autorisations :
Une autorité d'attributs (attribute authority)

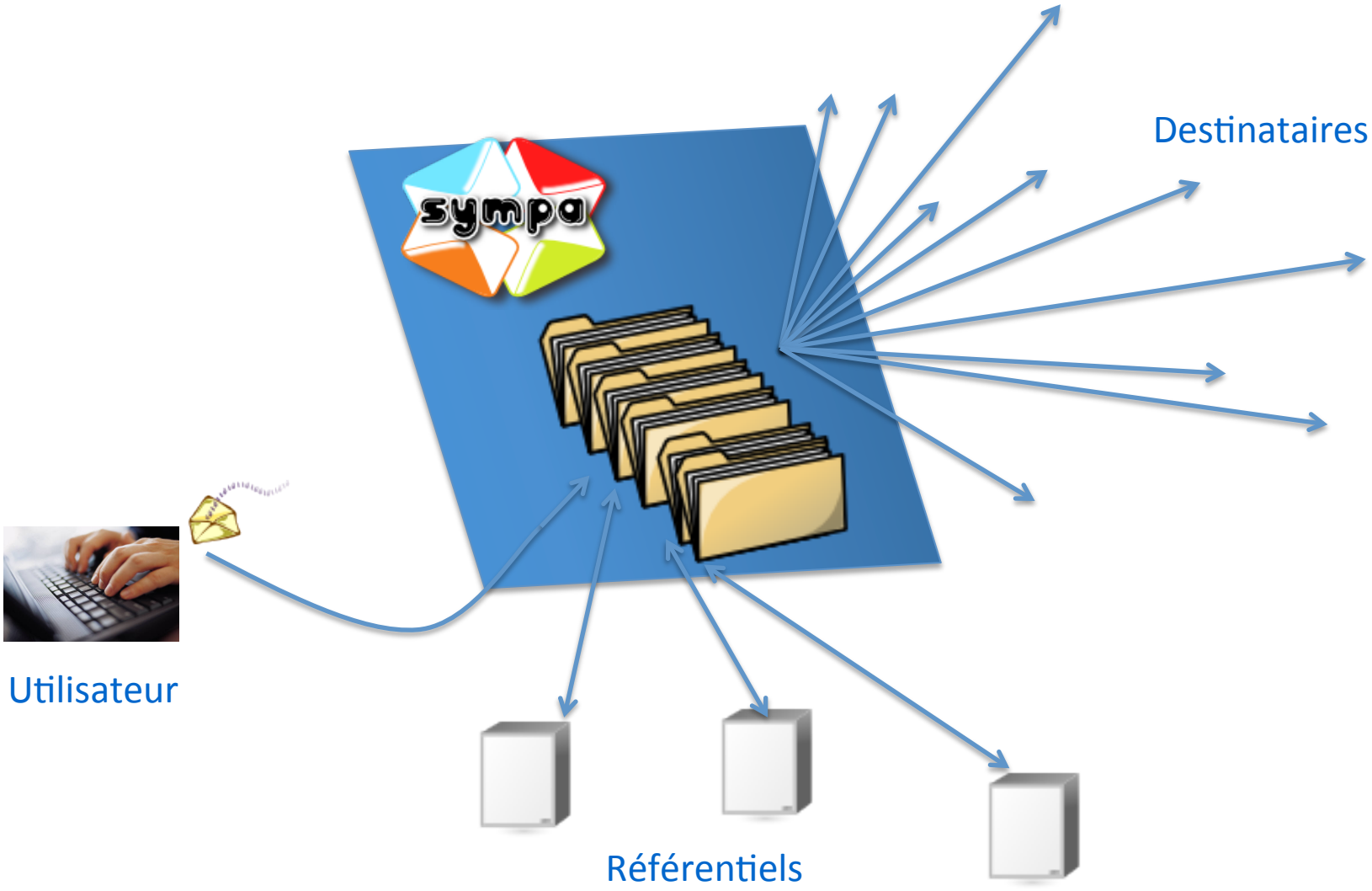
La fédération d'identités



Plusieurs solutions

HEXAA	http://www.hexaa.eu
PERUN	http://perun.cesnet.cz
OpenConext	https://www.openconext.org/
Unity	http://unity-idm.eu/
Switch GMT	http://unity-idm.eu/
GaKuNim mAP	https://map.gakunin.nii.ac.jp/map/
Grouper	http://www.internet2.edu/products-services/trust-identity-middleware/grouper/
Comanage	http://www.internet2.edu/products-services/trust-identity-middleware/comanage/
REMS	www.csc.fi/rems
Openstack VO	http://sec.cs.kent.ac.uk/CLASSe/index.html
Sympa	https://services.renater.fr/groupware/index

Sympa



SYMPA a du succès

- 90% des serveurs de listes utilisés dans l'environnement Education-Recherche en France
- Utilisé par différents ministères (défense, éducation, affaires étrangères …)
- Choisi par des opérateurs ou des grands groupes
- Mais aussi la NASA, l'UNESCO …
- Les utilisateurs sont majoritairement hors nos frontières (traduit en 12 langues)

SYMPA est robuste

- Une liste compte 1 600 000 membres
- Un serveur gère 32 000 listes
- Un serveur supporte 30 000 virtual hosts
- Un server compte plus de 3 000 000 de membres de listes

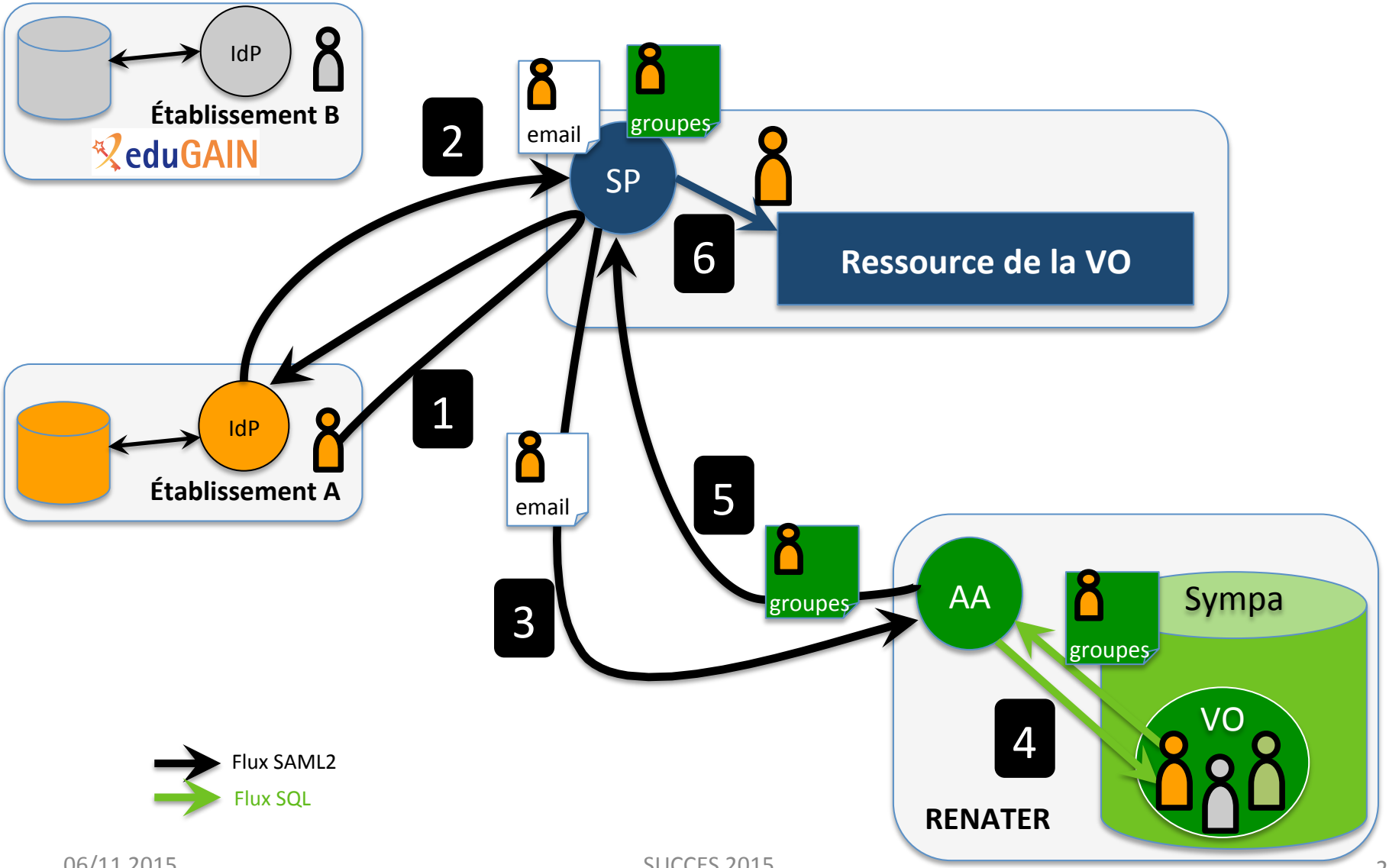
SYMPA est ouvert

- Alimentation automatique depuis des sources externes (SQL, Ldap, SMTP, flat files, Sympa…)
- Support des protocoles SOAP et VOOT pour intéragir avec d'autres applications

Sympa est notre solution

- Sympa est déjà très largement déployé dans notre communauté
- Sympa gère déjà des groupes et des autorisations pour ses propres besoins (wiki, porte documents, Foodle…)
- Sympa s'interface avec une grande variété de sources de données
- Sympa sait répondre à des APIs de requête d'appartenance à un groupe
- Sympa n'est pas intrusif pour les services déployés

Le workflow du service



Cinématique d'accès

1. Un utilisateur non authentifié souhaite accéder à un service ou a des ressources en ligne
2. Il est redirigé vers le fournisseur d'identités de son établissement qui l'authentifie et transfère les attributs le caractérisant à la ressource
3. La ressource fait une demande d'attributs complémentaire auprès du service d'autorisation. Un identifiant unique de l'utilisateur est échangé
4. L'autorité d'attributs du service d'autorisation enrichit les attributs propagés
5. L'autorité d'attributs renvoie l'assertion d'authentification enrichie (contenant les groupes d'appartenance de l'utilisateur) à la ressource accédée. La ressource peut ainsi vérifier que l'utilisateur appartient à un groupe autorisé
6. L'utilisateur accède à la ressource.

FileSender Premium

- RENATER propose un nouveau service **FileSender Premium** (très gros fichiers)
  - Le contrôle d'accès est réalisé par le service d'autorisation pour les VOs.
    - Chaque établissement souscripteur du service, alimente sa propre liste via l'interface web dans Sympa (Universalistes)
    - Une metaliste regroupe les différentes listes et est le support d'autorisation du service

Quelques ressources

- Une démo est accessible pour tester le service :

  https://groupes-aa.renater.fr/validation

- La documentation du service est ici :

  https://services.renater.fr/groupware/autorisation/index

Quelques ressources complémentaires

- AARC
  - https://aarc-project.eu
  - https://docs.google.com/forms/d/1xHaCINRaizjWfY6K-4-1O9z81NAyBsmxtJNSNGXSICU/viewform
- TANDEM
  - http://www.tandem-wacren.eu
- MAGIC
  - http://magic-project.eu/
- GN4
  - http://www.geant.org

RENATER
CONNECTEUR DE SAVOIRS

MERCI