# Fédération Éducation-Recherche

## An overview of the French academic identity federation

Mehdi Hached – April 2014

# Plan

- A bit of History
- La Fédération Éducation – Recherche
- Today’s federation status and tools
- Inter-federations
  - How to interoperate?
  - Challenges
- The future

# A bit of History…
# The French HE landscape

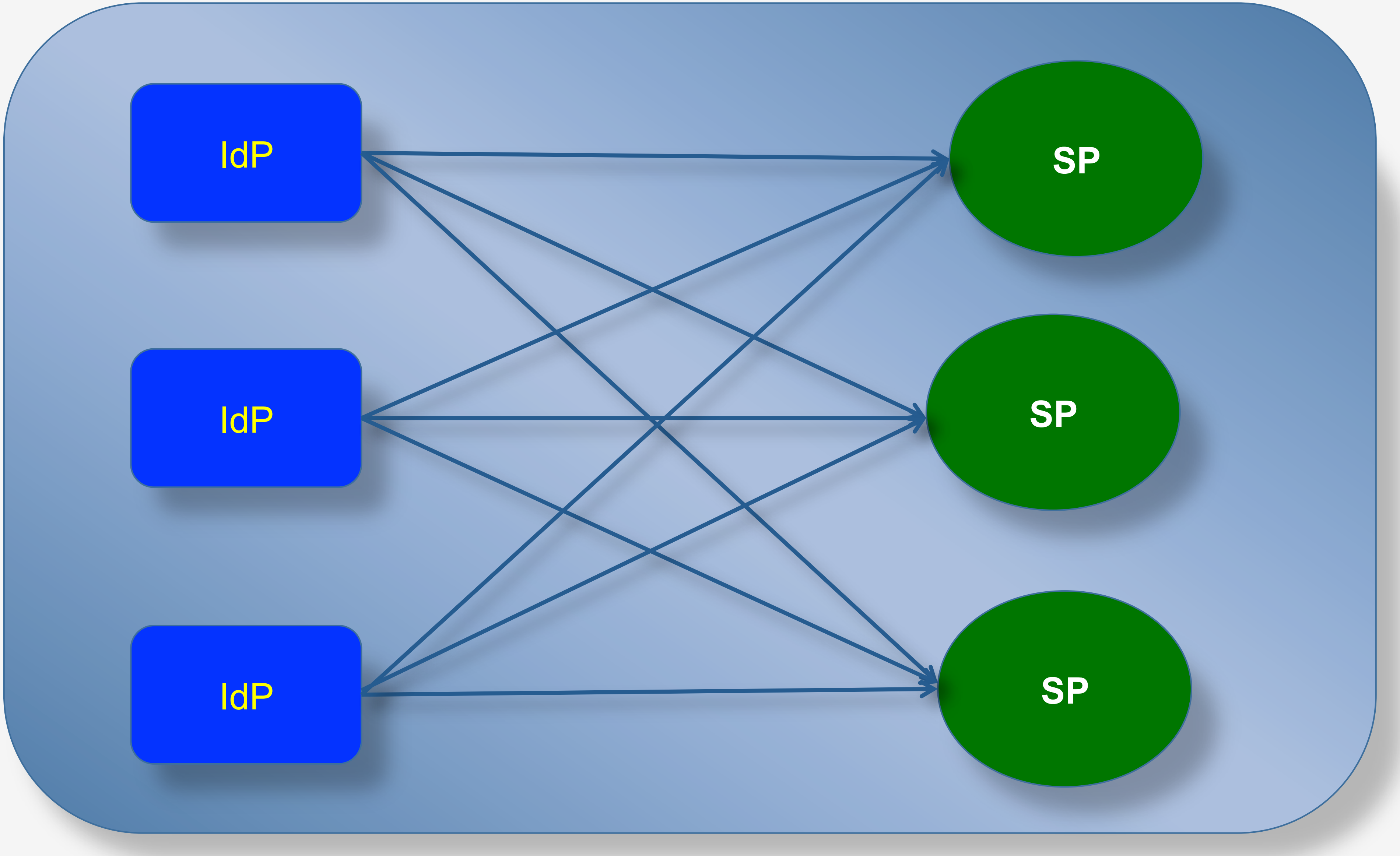
- From 2003 to 2005
  - – Massive usage of institutional portals
  - – regrouping most of universities online applications
  - – Using institutional Single Sign On (SSO) technology (Mostly SSO-CAS)
  - – Relying (mostly) on LDAP back-ends
  - – LDAP structured upon ***Supann*** repositories schema
    - *Supann* = French Higher Education superset of *eduPerson*
- Needs to open up for collaboration and to ease accesses to vendors online applications:
  - – Beyond institutional SSO = SAML identity federation

## Supann Definition of *eduPersonAffiliation*

**Student**
**Faculty**
**Staff**
**Employee**
**Member**
**Affiliate**
**Alum**
**library-walk-in**
**researcher** (SupAnn 2008)
**retired** (SupAnn 2008)
**emeritus** (SupAnn 2008)

# Fédération Éducation-Recherche

- Tests and pilot phase in 2006
- First production deployment in 2007
  - only Higher Education (HE) first
- Operation and maintenance by RENATER
  - Participation = Signed charters
- Type of federation = « Mesh »
- Figures:
  - 200 Identity providers (IdP)
    - 99% Shibboleth
  - 460+ service providers (SP)
    - 90% Shibboleth
    - 10% simpleSAMLphp,openSSO, Lasso library, ADFS…


IdP
IdP
IdP
SP
SP
SP

# Type of service providers

- E-Journals
- E-Learning
- Groupwares
- Shared « home-brewed » applications
- Extranets
- Wi-Fi connectivity (captive portals)
- …

RENATER
CONNECTEUR DE SAVOIRS

# What about e-journals?

- ***Couperin***: A consortium that intermediate the negociations with editors
  - CARE (?) in Italy
- Big investment in time and effort to make them join the federation
- But, e-journals are not the « killer apps »
  - Fine statistics are hard to obtain through SAML
  - Organizations need reliable statistics
- So, reverse proxies are still heavily used

# How did the federation grew?

- Collaboration
  - among regional HE organizations
  - among national HE organizations working on the same field
- Some HE Ministry's programs pushing the identity federation technology
- In 2008, the scope of the federation went larger
  - Research organizations joined the federation
- RENATER's own national web services
  - Certificates, groupware, forge, anti-spam…

# Helping HE organizations

- 3 to 4 free training sessions per year
  - IdP installation
  - SP installation and applications *domestication*
- Biennial « Federation's day »
  - Evolutions
  - News
  - Sharing community experiences
- Online documentation - A LOT !
  - Self-training materials
  - Data privacy guidance
  - Technical FAQ

# Marketing?

- Identity federation is a prolongation of the organization's web SSO already in-place
  - User's already used to SSO functionning
- Organizations run their own technical sofwares
  - They advertise about the external services available to staff/students/researchers
- RENATER announces new national or commercial services
- RENATER provides tools to lighten IdPs' managers workload

# Federation’s Tools

- Testbed federation and more:
  - Test IdP with different test accounts
  - Test SP
  - Test Discovery service
  - IdP validator to check some « standards » profiles
- IdP of last resort
- Remote attributes filters (Shibboleth IdP format) tuned by service provider or category:
  - National
  - Commercial
  - Local
  - Community…
- Federation as a service (new 2014)

# Inter-federations

- National (soon… maybe)
  - 1st degree federation
  - Ministry future federation (?)
- International (now)
  - eduGAIN

- Challenges that implies
  - Opt In / Opt Out
  - Attribute release scaling for international exchanges
  - Data Privacy concerns outside EU

# Scalability

- It is easy to add providers in metadata
- It is more challenging to make IdP well configured to release the right attributes
  - And sometime with the right value
- → Almost solved in the national scope with the remote attributes filters
  - But they are Shibboleth only
  - International inter-federation will need such tools
  - SAML 2 <AttributeConsumingService> metadata extension

# Data Privacy

- ***CNIL :*** French Data Privacy agency
- Work closely with them through ***supCIL***
  - HE Data privacy officers association
- Submitted to Data Privacy Law
  - As service providers
    - Purpose of use
    - Minimal disclosure
  - As Identity providers
    - User information and (possibly) consent

# Future

- Lack of monitoring and usage statistics
  - Test and implement a solution. Raptor ?
  - How about security policies of organizations regarding the probes ?
- IdP Hosting
  - For small organizations
  - Study the technical requirements
- Studies and guidances for strong authentication
  - what about the level of assurance (LoA)?
- Working on a LoA for the French federation
  - Including the data provisionning quality

RENATER
CONNECTEUR DE SAVOIRS

# Domande ?