La fédération à l'échelle internationale avec eduGAIN

Journée fédération 2013

Olivier Salaün (RENATER)

RENATER
CONNECTEUR DE SAVOIRS

SAML, tout le monde s'y est mis

- Chronologie :
  - 2005 : fédérations Suisse et USA
  - 2006 : fédération du CRU
- Les fédérations education-recherche
  - 33 fédérations (au moins)
  - en Europe et ailleurs
- Utilisation généralisée de SAML2

https://refeds.org/resources_list.html

RENATER
CONNECTEUR DE SAVOIRS

Pourquoi une inter-fédération ?

- exemple 1 : diplôme transnational
  - formation co-organisée par des universités de plusieurs pays
    - leurs IdPs sont inscrits dans des fédérations nationales différentes
  - des ressources pédagogiques accessibles depuis plusieurs IdP
- solutions
  - gestion de relations bilatérales
  - inscription des SP dans chaque fédération

RENATER
CONNECTEUR DE SAVOIRS

Pourquoi une inter-fédération ?

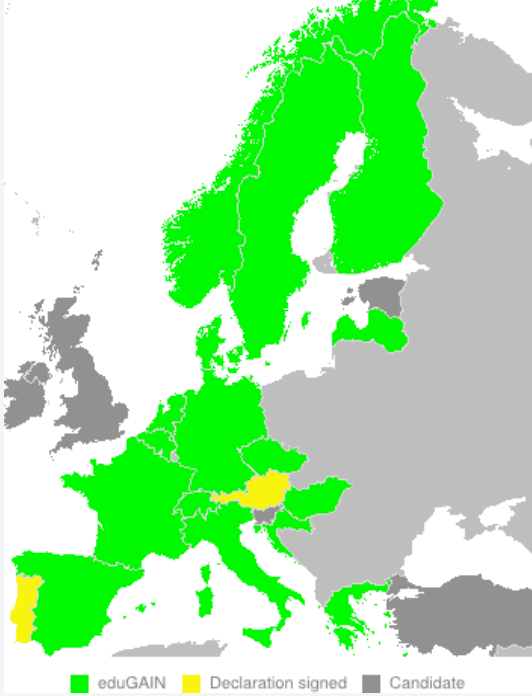
- exemple 2 : une communauté internationale de chercheurs
  - besoin de partage de ressources, d'outils collaboratifs
    - => authentification et droits d'accès
  - concerne quelques individus dans chaque organisme, dans des pays différents
- Solutions
  - inscription des SPs dans chaque fédération hors de portée
  - gestion des identités autonome

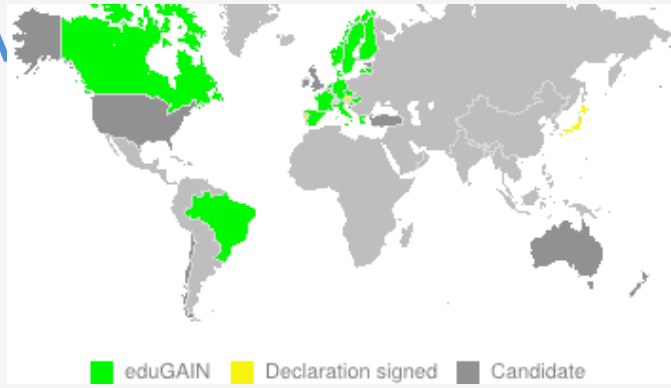
RENATER
CONNECTEUR DE SAVOIRS

eduGAIN c'est quoi ?

- une interconnexion de fédérations
  - plus compliqué à réaliser que pour eduroam
- périmètre initialement UE
  - finalement plus large (Brésil, Canada, Japon, Australie, Chili, Nouvelle Zélande, Turquie, USA

http://edugain.org/





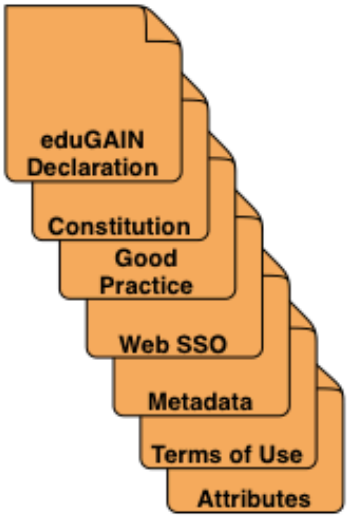
RENATER
CONNECTEUR DE SAVOIRS

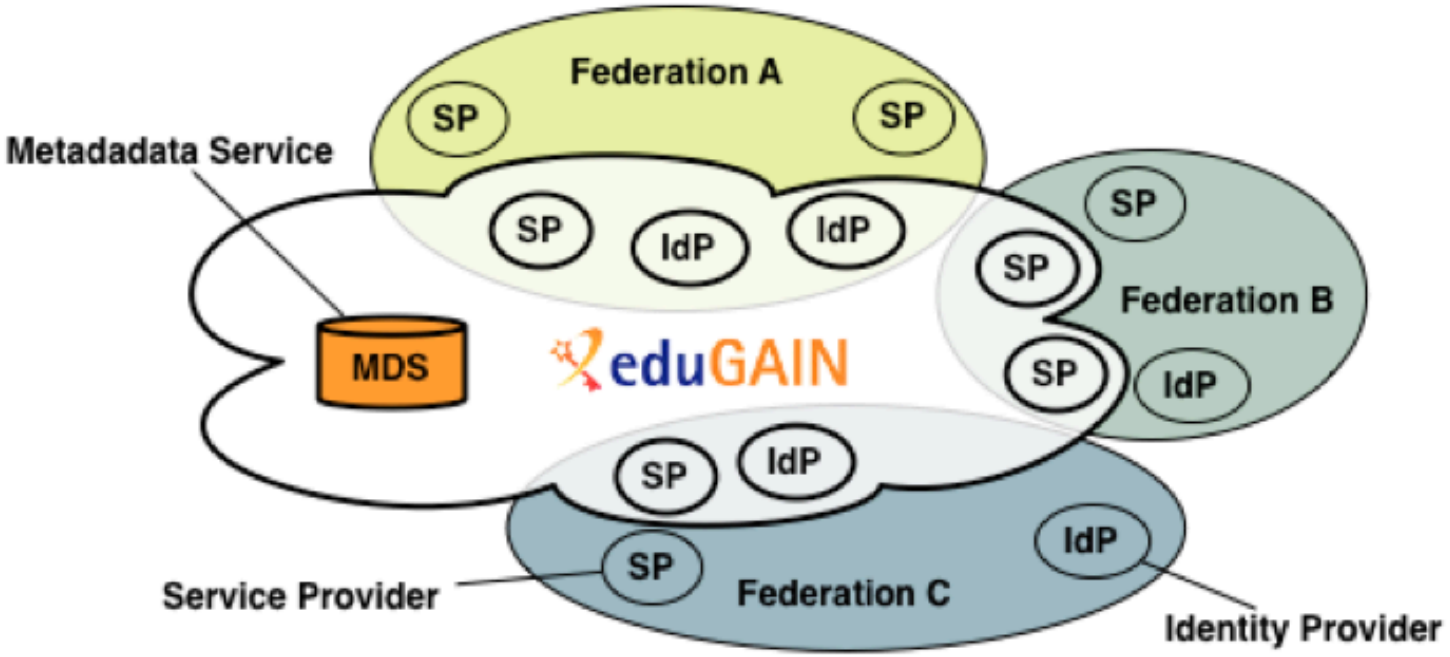
Qui gère eduGAIN ?

- GEANT : l'opérateur du réseau européen education-recherche
- ne fournit pas que des tuyaux
  - eduGAIN, eduROAM, eduPKI, eduCONF
  - à venir : Cloud Services
- projet GN3+
  - avril 2013 => avril 2015
  - inclut la poursuite de eduGAIN

http://www.geant.net

eduGAIN et RENATER





- RENATER a signé la déclaration eduGAIN
- Chaque SP et IdP français **choisit** de participer à eduGAIN
- Les méta-données des entités SAML participantes sont :
  1. transmises par RENATER
  2. agrégées par GEANT
  3. republiées par RENATER

RENATER
CONNECTEUR DE SAVOIRS

eduGAIN si vous gérez un SP

1. configurer le logiciel SP
2. adapter la gestion des attributs utilisateurs
3. adapter le discovery service
4. demander l'inscription du SP dans eduGAIN

RENATER
CONNECTEUR DE SAVOIRS

eduGAIN si vous gérez un IdP

1. configurer le logiciel IdP
2. enrichir les attributs utilisateurs
3. demander l'inscription de l'IdP dans eduGAIN

RENATER
CONNECTEUR DE SAVOIRS

Configuration des logiciels SP et IdP

- chargement des méta-données eduGAIN
  - deux fichiers de méta-données
    - idps-edugain-metadata.xml
    - sps-edugain-metadata.xml
  - publiés par RENATER
- Vérification de la signature des MD
  - un nouveau certificat
- Documentation à venir...

RENATER
CONNECTEUR DE SAVOIRS

Format des méta-données eduGAIN

- Référence
  - http://www.geant.net/service/edugain/resources
- élément RegistrationInfo
  - organisme ayant enregistré l'entité SAML
- élément RequestedAttribute
  - concerne les SP
  - informations sur les attributs utilisateurs demandés
- élément UIInfo
  - intitulé et description en Français et en Anglais
  - autres informations optionnelles :
    - Keywords, Logo, PrivacyStatementURL, IPHint, DomainHint, GeolocationHint

https://federation.renater.fr/edugain/edugain-metadata.xml

RENATER
CONNECTEUR DE SAVOIRS

eduGAIN et attributs utilisateurs

- Référence : eduGAIN attribute profile
  - http://www.geant.net/service/edugain/resources/
- Attributs recommandés :
  - displayName,
  - cn,
  - mail,
  - eduPersonAffiliation,
  - eduPersonScopedAffiliation,
  - eduPersonPrincipalName,
  - eduPersonTargetedID,
  - schacHomeOrganization,
  - schacOrganizationType

RENATER
CONNECTEUR DE SAVOIRS

eduGAIN et attributs utilisateurs

- contraintes sur eduPerson(Scoped) Affiliation :
  - valeurs utilisables : member, faculty, student, alum, affiliate, library-walk-in
  - valeurs à éviter : employee, staff
- identification de l'organisme :
  - schacHomeOrganization
    - exemple : univ-orleans.fr
  - schacHomeOrganizationType
    - exemple : urn:mace:terena.org:schac:homeOrganizationType:eu:higherEducationalInstitution

RENATER
CONNECTEUR DE SAVOIRS

Attributs / configuration IdP

- Ajouter de nouveaux attributs
  - attribute-resolver.xml et attribute-filter.xml
- Filtrer certaines valeurs d'attributs
  - regex au niveau AttributeFilterPolicy
- Filtres automatiques
  - pas d'équivalent des filtres automatiques fournis par RENATER
  - mais nouvelle fonctionnalité prometteuse dans IdP Shibboleth 2.4.0
    - IdPFilterRequirementAttributeInMetadata

RENATER
CONNECTEUR DE SAVOIRS

Attributs / configuration SP

- Ajouter de nouveaux attributs
  - attribute-policy.xml et attribute-map.xml
- Adapter les contrôles d'accès à la nouvelle population :
  - dans la configuration Apache
  - dans les applications
- Conformité au Code Of Conduct eduGAIN ?

RENATER
CONNECTEUR DE SAVOIRS

Data Protection Code Of Conduct (travail en cours)

- Objectif :
  - It is expected that Home Organisations are more willing to release attributes to Service Providers who manifest conformance to the Data protection Code of Conduct
- Principes
  - publication d'une Privacy Policy (en Anglais au moins)
    - entité légale
    - finalité des traitements
    - catégorie des attributs
    - destinataire des données
    - droit accès/rectification des données ?
  - demande d'attributs minimale
  - pas d'utilisation des données pour d'autres traitements
  - pas de traitements secondaires des données
  - sécurisation des données

https://refeds.terena.org/index.php/CocPilotReport

RENATER
CONNECTEUR DE SAVOIRS

eduGAIN et service de découverte

- le SP doit utiliser un DS/WAYF adapté
  - consommant les méta-données eduGAIN
- une instance proposée par RENATER
  - https://discovery.renater.fr/edugain
  - mode embedded
- autre implémentation intéressante
  - http://discojuice.org/
  - bien adapté à l'échelle eduGAIN
  - mais en mode SaaS

Inscrire un SP/IdP dans eduGAIN

RENATER
CONNECTEUR DE SAVOIRS

Maturité de eduGAIN ?

- Prémices du projet fin 2005
  - architecture actuelle adoptée en 2010
- Des chiffres
  - 18 fédérations raccordées
  - 63 IdP
  - 52 SP
- Montée en puissance
  - proposer plus de services
  - couvrir plus d'IdPs
  - => l'oeuf et la poule

RENATER
CONNECTEUR DE SAVOIRS

Une killer application ?

- Editeurs de documentation électronique
  - pourraient participer via une fédération nationale
  - JISC (UK) serait le point d'entrée le plus naturel
    - mais problème de charge/support
    - modèle économique ?
- Donc ça n'est pas la killer application

RENATER
CONNECTEUR DE SAVOIRS

En bref...

- Vous pouvez (presque) vous lancer
  - modulo documentation et nouveau guichet
  - ouverture début juin 2013
- Questions ou cas d'usage ?
  - Contactez-nous