

International authentication with eduGAIN ou comment fédérer les identités au niveau international

Lukas Hämmerle, GÉANT/SWITCH

Olivier Salaün, GÉANT/RENATER

JRES 2013

13. December 2013

Presentation Overview

- History of identity federation and eduGAIN
- How Interfederation and eduGAIN works
- Facts and Figures
- How to join eduGAIN in France

The Situation on Campus: Lots of Applications



- More and more applications for students and researchers
- Many applications require authentication and authorization

The Problem: Lots of Applications -> Lots of Passwords



- One password for each application does not scale
- Tons of passwords to manage for users and service operators
- Varying degree of password security
- Increased helpdesk work due to lost passwords
- Collaborative usage of application is difficult

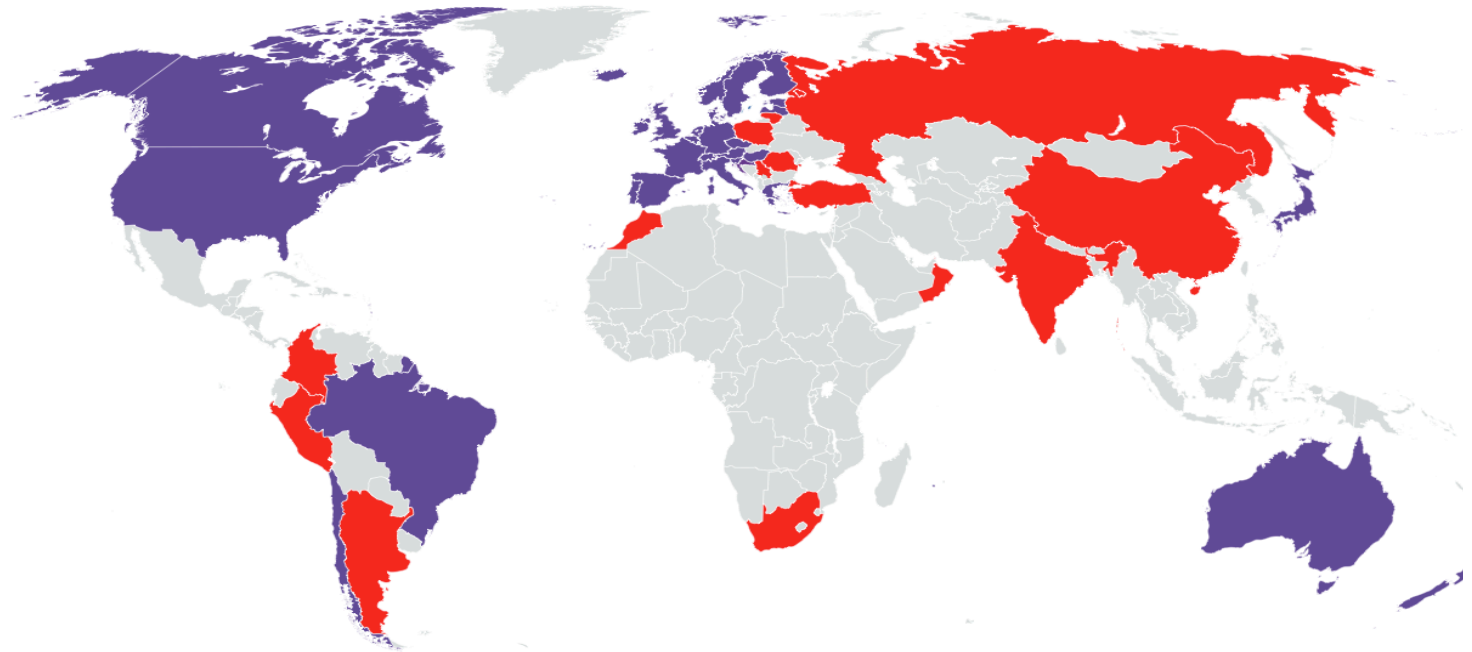
The Solution: Federated Identity Management

- Create an (identity) federation:
 - Multiple organisations/services agree on common technical and legal standards => **trust**
 - Deploy Identity and Service Providers
 - Mutually trust each other's identity assertions
 - Collaborate, e.g. common e-learning platform
- One login name and password for users
- Password entered only on login page of home organisation
- First Academic Identity Federations started in 2005
- Many countries have national academic identity federations today!

Federation



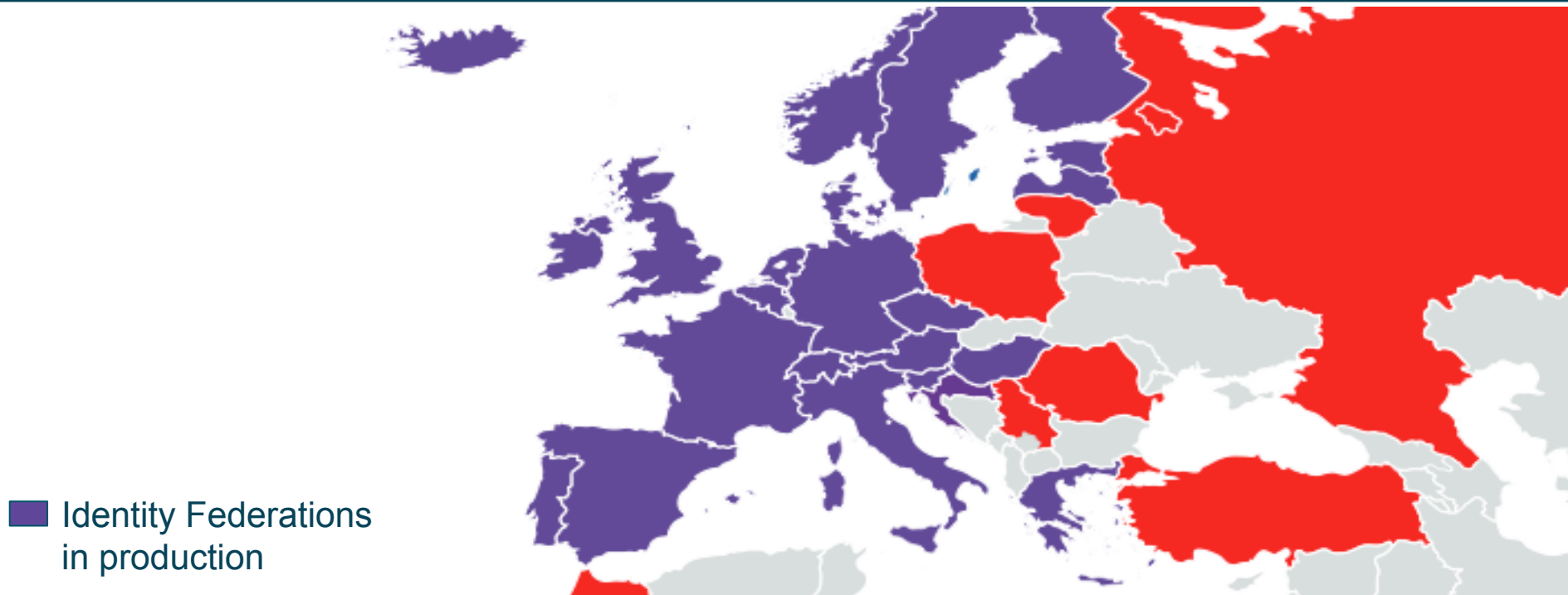
National Identity Federations World Wide



- 30 Identity Federations in production
- 12 Identity Federations in pilot

last update 14. October 2013, www.refeds.org

National Identity Federations in Europe



■ Identity Federations
in production

■ Identity Federations
in pilot



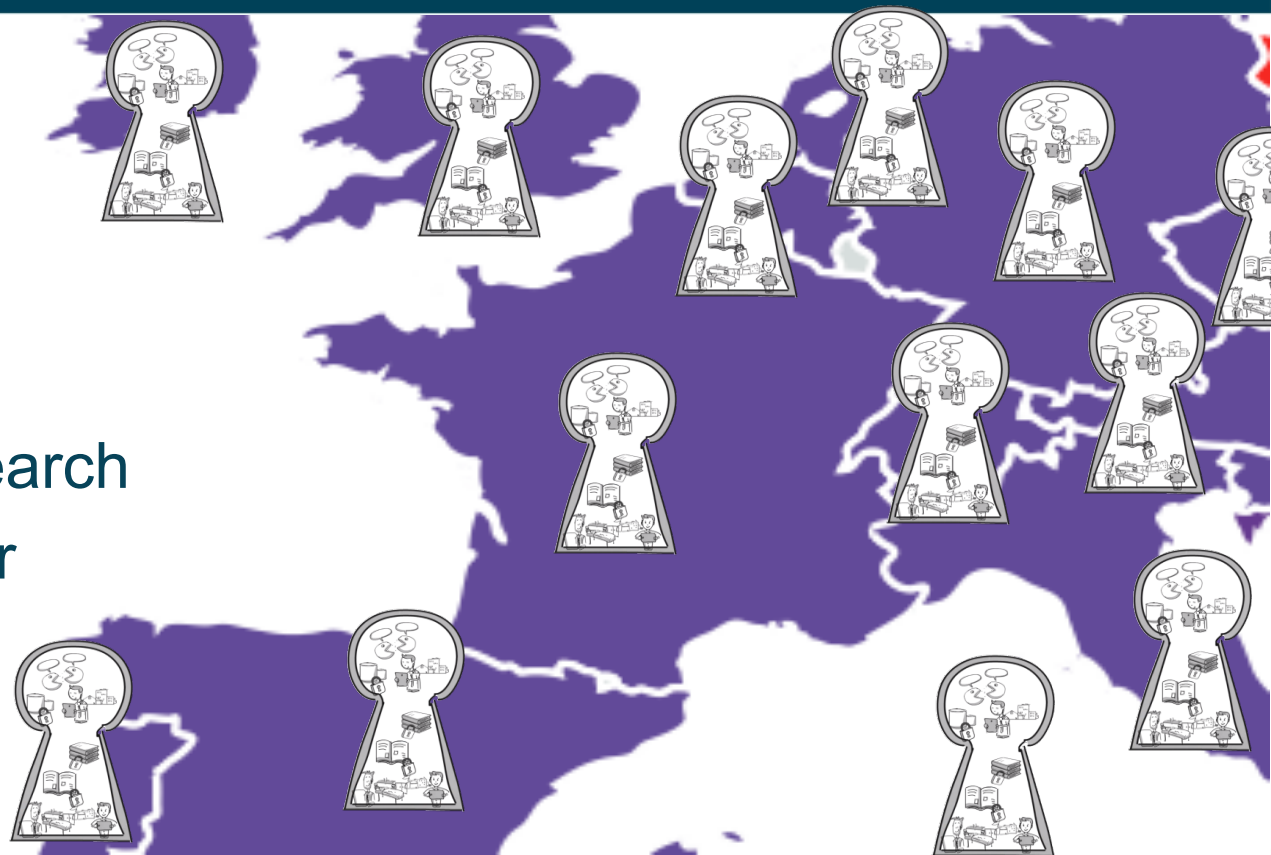
REFEDS

last update: 14. October 2013, www.refeds.org

National Federations Are Limited by Country Borders

All Federations:

- Support SAML2
- education & research
- Use same/similar user attributes




Options to Offer a Service to Users in Multiple Countries

- **Option A:**
Provide each user a login name/ password. User management effort.
- **Option B:**
Make service join multiple federations. Complicated, lots of paperwork and different requirements
- **Option C?**



Atlases - PATHOLOGY IMAGES
Collection of **high resolution** histological images

Lang:   Registered users: 34798

Hypertext atlas of Dermatopathology version 10.97, March 2013

Hypertext Atlas of Dermatopathology contains thousands of clinical and histological images of skin diseases. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Fetal Pathology version 2.23, March 2013


Hypertext Atlas of Fetal Pathology contains clinical and histological images of various form of developmental anomalies. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Neonatal Pathology version 1.12, March 2013


Hypertext Atlas of Neonatal Pathology contains clinical and histological images of various forms of neonatal pathology. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Bone Marrow Pathology version 1.11, March 2013

Hypertext Atlas of Bone Marrow Pathology Pathology contains clinical and histological images of various forms of bone marrow diseases. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

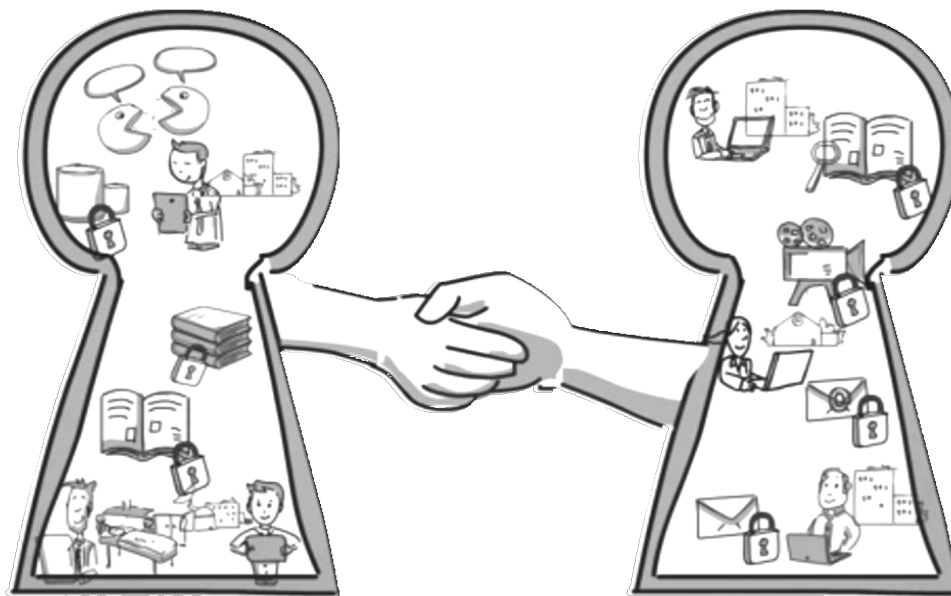
Hypertext atlas of Rare Lymphomas version 0.84, March 2013

Hypertext Atlas of Rare Lymphomas contains clinical and histological images of some rare hematologic/lymphatic malignancies of children. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

In order to have an access to the **high resolution** images you have to **LOGIN** below:
If you have an account in one of the following **identity federation**, click on the logo.

-  **eduID.cz**
-  **Log ind med WAYF** 
-  **SIR** 
-  **SWITCHaai**
-  **DFN** 
-  **AA @EduHr** 
-  **ide garr** 
-  **GakuNin** 
-  **Riquator** 

Service: Atlas, Federations joined: 19, URL: atlases.muni.cz

Option C, the Next Step: Interconnect National Federations



Provide legal and technical frameworks to make national Federations interoperate = interfederate

Interfederation Use Cases



Researchers

Often work together in international research projects, which operate many web-based services that need authentication. Services are in different countries/federations. Thanks to Interfederation researchers can use their institution's account.



Lecturers

Can start e-learning collaborations across country borders. Create (costly) e-learning content collaboratively or easier "sell" it to other universities abroad.



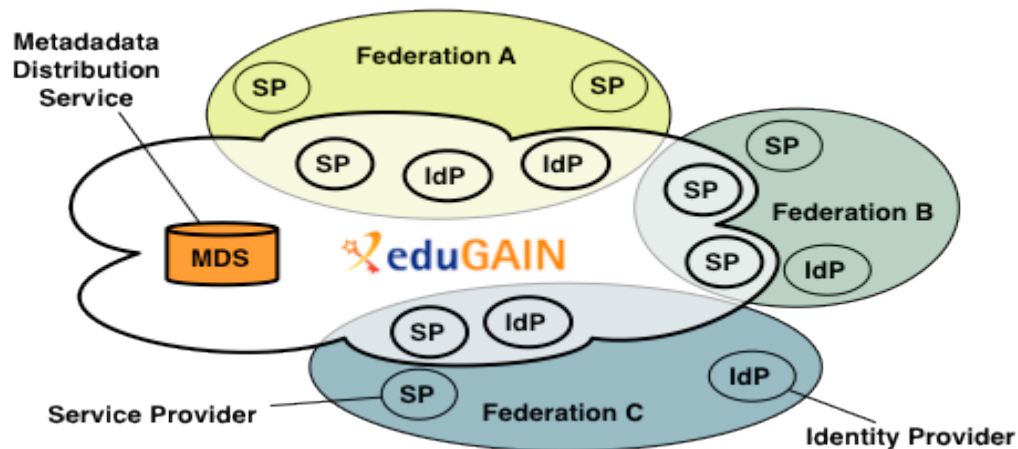
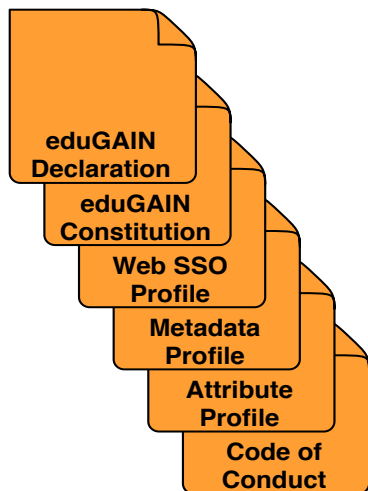
Content Publishers

Companies like Elsevier/Thomson Reuters/etc. already joined multiple identity federations. Cumbersome for them and for federation operators. Thanks to Interfederation: Join one, be connected to many!

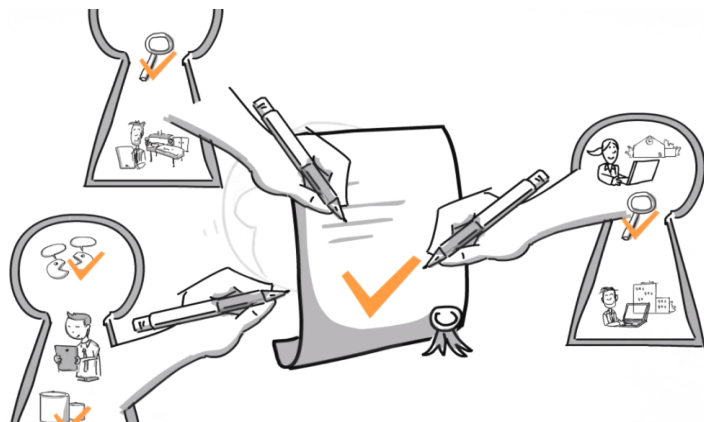


- Global **A**uthentication **I**nfrastructure for **e**ducation
- An interfederation service *primarily* for Research & Education
Connects existing SAML-based academic identity federations
- SAML2-based
Currently mostly web-based services but non-web services would be supported too (e.g. via SAML ECP)
- Developed and funded by European GÉANT projects (www.geant.net)
but open also to non-European federations
- Web site: www.eduGAIN.org

eduGAIN: What Is it and How Does it Work?



- eduGAIN provides policy framework and standards to build trust
- SPs and IdPs of participating federations should opt-in for eduGAIN
- MDS fetches, aggregates and republishes metadata



- eduGAIN Declaration (3 pages)
 - Signed by each eduGAIN Member Federation
 - Contains 13 rules that federations promise to obey
- eduGAIN Constitution (10 pages)
- Profiles for SAML, Metadata, Attributes, ...
- GEANT Data Protection Code of Conduct
 - Declaration of Service Providers to "behave well" with user data
 - Applicable in EU/EEA or similar

eduGAIN: Who is Behind it and How Is it Governed?



Current Governing Structure

- **eduGAIN Steering Group (eSG)**

Each member federation has one representative. Votes on which new federations are accepted or policy changes.

- **eduGAIN Executive Committee (eEC)**

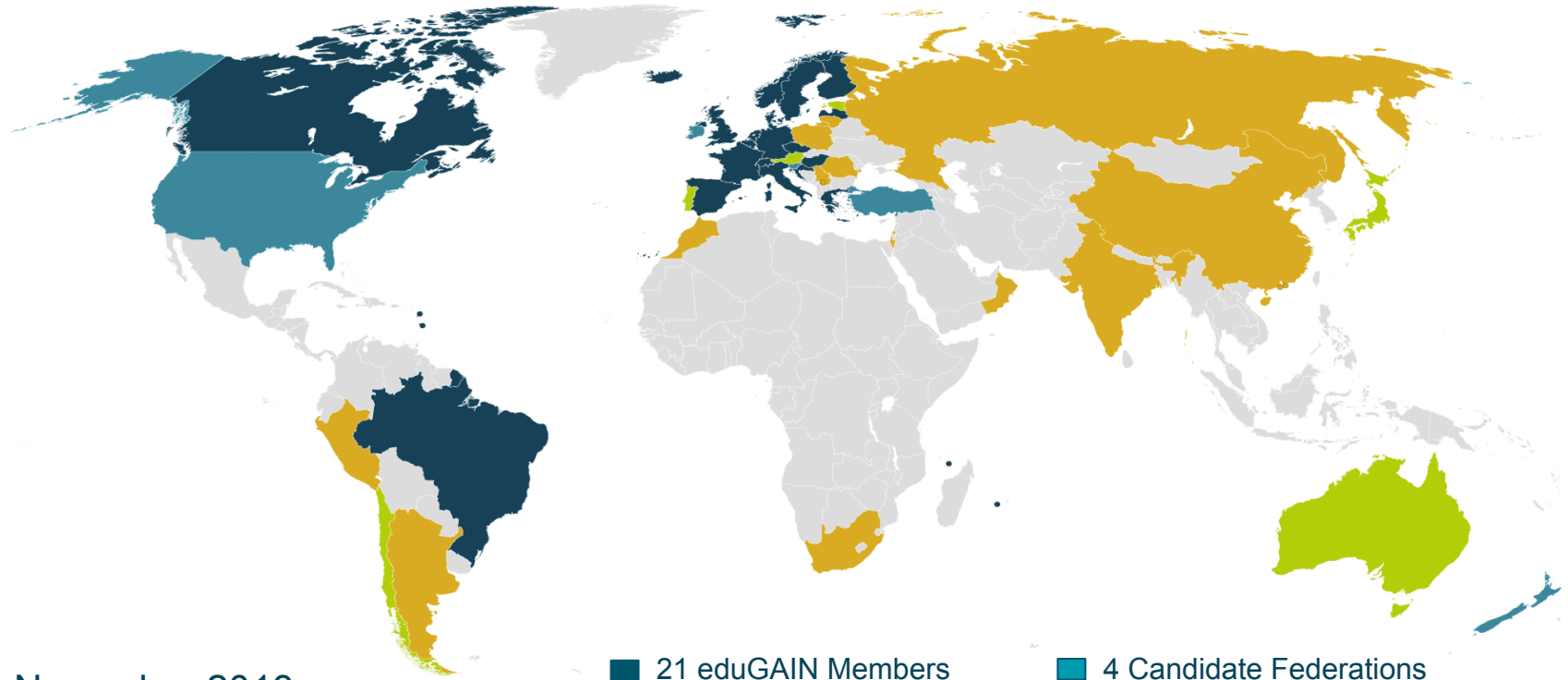
Approves changes to the constitution and has veto right. Currently nominated by GEANT Executive Committee but might change.

Other Key Persons

- Operational Team (Tomasz Wolniewicz, UMK, PL)
- Policy & Code of Conduct (Mikael Linden, CSC, FI)
- Emerging Federations (Brook Schofield/Nadia Sluer, TERENA, NL)
- FaaS (Marina Vermezovic, AMRES, RS/Valter Nordh, SWAMID, SE)
- Engaging User Communities (Lukas Hämmerle/Ann Harding, SWITCH, CH)

- **April 2011:** Official start of eduGAIN
- **Nov 2013: 21 Federations** are members (50%) , 5 joining
- **Entities: 147 IdPs, 71 SPs**
One IdP can represent for dozens of organisations and services depending on federation architecture => actual numbers are higher
- **Whole (academic) SAML landscape:**
42 Federations, 2424 IdPs, 4772 SPs (gathered from metadata)
Not all of them need to be interfederated, e.g. many internal SPs

eduGAIN & Federation Status



November 2013

21 eduGAIN Members
5 Joining eduGAIN

4 Candidate Federations
12 Other Federations

● **Chicken and Egg Problem**

- Many Federations joined eduGAIN but number of entities of these federations that opted-in for eduGAIN increases slowly
- More Identity Providers => more Services => more Identity Providers
- No global killer application. Critical mass has to be reached yet!
- Important that initially universities and Research organisations opt-in

● **Attribute Release**

- Manually deciding which attributes are released for which service does not scale
- Automatic release based on standard release rules managed by the federation or based on service's (entity) category
- eduGAIN recommends to support: display name, affiliation, TargetedID, PrincipalName, home organisation and type

Recommendations

Organisations participating in international projects:

- Enable your Identity Provider for Interfederation/eduGAIN!
 - Large research projects often have only very few researchers from one individual organisation. But one individual organisation often has many researchers in different research projects that could benefit from federated international authentication via eduGAIN!
 - RENATER provides instructions for the Federation Education – Recherche (FER) with the necessary steps to opt-in
- Configure automatic (rule-based) attribute release for services which support the GÉANT Data Protection Code of Conduct (CoC)

How to join eduGAIN in France

- RENATER est le guichet national pour eduGAIN
 - RENATER a signé la déclaration eduGAIN
 - RENATER gère l'inscription dans eduGAIN pour la France
 - RENATER publie les méta-données eduGAIN

Inscrire un IdP/SP dans eduGAIN

1. Configurer le logiciel (SP ou IdP)
2. Si vous gérez un SP :
 - a. *Adapter la gestion des attributs utilisateurs*
 - b. *Adapter le discovery service*
3. Si vous gérez un IdP :
 - a. *Enrichir les attributs utilisateurs*
4. Demander l'inscription auprès de RENATER (guichet de la fédération)
5. Tester la configuration

Configuration des logiciels SP et IdP

- Chargement des méta-données eduGAIN
 - en plus des méta-données de la fédération Education-Recherche
 - deux fichiers de méta-données
 - *idps-edugain-metadata.xml*
 - *sps-edugain-metadata.xml*
 - publiés par RENATER
 - <https://federation.renater.fr/edugain/>
- Documentation
 - <https://services.renater.fr/federation/docs/fiches/edugain>

Format des méta-données eduGAIN

- Référence
 - <http://www.geant.net/service/edugain/resources>
- Élément RegistrationInfo
 - Organismes ayant enregistré l'entité SAML
- Élément RequestedAttribute
 - associé à un 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*

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 (*)
- (*) attributs non prévus dans SupAnn 2009

eduGAIN et attributs utilisateurs

- Contraintes sur eduPerson(Scoped)Affiliation :
 - valeurs utilisables : member, faculty, student, alum, affiliate, library-walk-in
 - valeurs ambiguës au niveau international : employee, staff
- Identification de l'organisme :
 - schacHomeOrganization
 - *exemple : univ-orleans.fr*
 - schacHomeOrganizationType
 - *exemple :*
urn:mace:terena.org:schac:homeOrganizationType:eu:higherEducationalInstitution

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 dans IdP Shibboleth 2.4.0

```
<AttributeFilterPolicy id="releaseThoseAttributesToAll">
  <PolicyRequirementRule xsi:type="basic:ANY"/>
  <AttributeRule attributeID="displayName">
    <PermitValueRule xsi:type="saml:AttributeInMetadata" onlyIfRequired="false"/>
  </AttributeRule>
  <AttributeRule attributeID="email">
    <PermitValueRule xsi:type="saml:AttributeInMetadata" onlyIfRequired="false"/>
  </AttributeRule>
</AttributeFilterPolicy>
```

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 ?

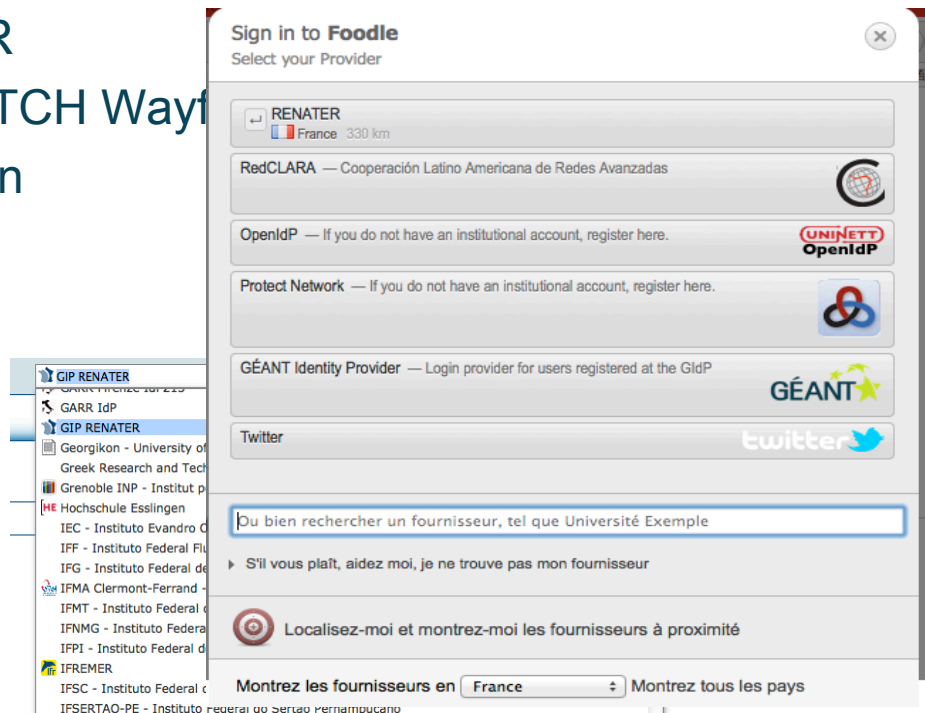
Data Protection Code Of Conduct

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



- Objectif : engagement des SP concernant le traitement des données à caractère personnel
- Principe
 - 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 autres traitements
 - pas de traitements secondaires des données
 - sécurisation des données
- Version du document pour les pays hors UE en préparation

- Le SP doit utiliser un DS/WAYF adapté à eduGAIN
- Une instance proposée par RENATER
 - utilise la nouvelle version de SWITCH Wayf
 - <https://discovery.renater.fr/edugain>
 - *mode embedded*
 - *search as you type*
 - *affichage des logos*
- Autre implémentation intéressante
 - <http://discojuice.org/>
 - bien adapté à l'échelle eduGAIN



Sign in to **Foodle**
Select your Provider

- RENATER
France 330 km
- RedCLARA — Cooperación Latino Americana de Redes Avanzadas
- OpenIdP — If you do not have an institutional account, register here. **UNI-NETT OpenIdP**
- Protect Network — If you do not have an institutional account, register here.
- GÉANT Identity Provider — Login provider for users registered at the GidP **GÉANT**
- Twitter **twitter**

🔍 Du bien rechercher un fournisseur, tel que Université Exemple

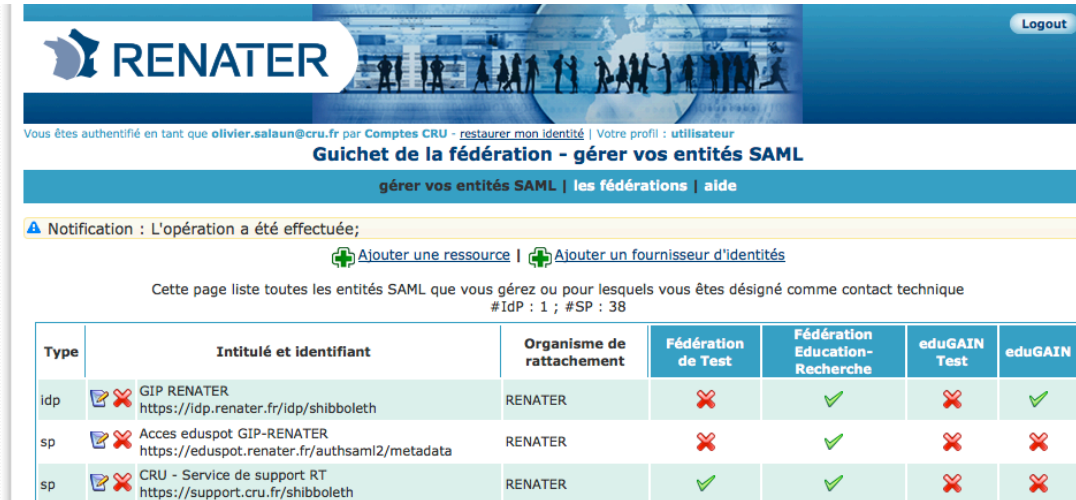
▶ S'il vous plaît, aidez moi, je ne trouve pas mon fournisseur

🎯 Localisez-moi et montrez-moi les fournisseurs à proximité

Montrez les fournisseurs en **France** Montrez tous les pays

Inscription via le guichet de la fédération

- Aujourd'hui
 - Contactez-nous
- Février 2014
 - via le guichet de la fédération



RENATER Logout

Vous êtes authentifié en tant que olivier.salaun@cru.fr par Comptes CRU - restaurer mon identité | Votre profil : utilisateur

Guichet de la fédération - gérer vos entités SAML

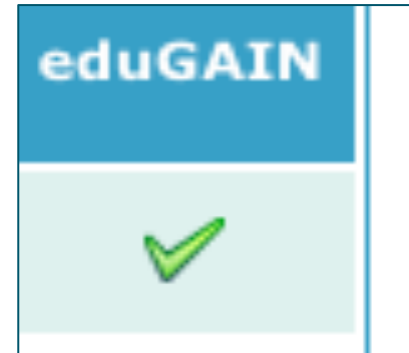
[gérer vos entités SAML](#) | [les fédérations](#) | [aide](#)

▲ Notification : L'opération a été effectuée;

[Ajouter une ressource](#) | [Ajouter un fournisseur d'identités](#)

Cette page liste toutes les entités SAML que vous gérez ou pour lesquels vous êtes désigné comme contact technique
#IdP : 1 ; #SP : 38

Type	Intitulé et identifiant	Organisme de rattachement	Fédération de Test	Fédération Education-Recherche	eduGAIN Test	eduGAIN
idp	GIP RENATER https://idp.renater.fr/idp/shibboleth	RENATER				
sp	Accès eduspot GIP-RENATER https://eduspot.renater.fr/authsaml2/metadata	RENATER				
sp	CRU - Service de support RT https://support.cru.fr/shibboleth	RENATER				



Conclusion

- eduGAIN est adapté pour les communautés internationales
 - mais population dispersée à votre échelle
- Inscrivez vos IdP dans eduGAIN, par anticipation
 - pour qu'eduGAIN devienne un service de base
- Une démo sur le stand RENATER
- Les projets GEANT
 - vous pouvez participer
- Des questions ?