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!
Example SWITCHaai Federation (Switzerland)

Number of Federation-enabled accounts

98% coverage in higher education

Number of Organizations

Number of Resources/Services
National Identity Federations World Wide

30 Identity Federations in production
12 Identity Federations in pilot

National Identity Federations in Europe

Identity Federations in production

Identity Federations in pilot

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?**

**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!
Interfederation with eduGAIN

- **Global Authentication INfrastructure for education**

- 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](http://www.geant.net)) but open also to non-European federations

- Web site: [www.eduGAIN.org](http://www.eduGAIN.org)
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: Legal Trust and Profiles

- 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)
eduGAIN: Some Statistics

- **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
eduGAIN: Current Difficulties and Problems

- **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

- Elément RegistrationInfo
  - Organismes ayant enregistré l'entité SAML

- Elément RequestedAttribute
  - associé à un SP
  - informations sur les attributs utilisateurs demandés

- Elément UIInfo
  - intitulé et description en Français et en Anglais
  - autres informations optionnelles :
    - Keywords, Logo, PrivacyStatementURL, IPHint, DomainHint, GeolocationHint
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

```xml
<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>
```
• 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 ?
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
• Autre implémentation intéressante
  – http://discojuice.org/
• bien adapté à l’échelle eduGAIN
Inscription via le guichet de la fédération

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