OSUG

Observatoire des
Sciences de l'Univers
de Grenoble

Identity Provider et Service Provider pour l'OSUG?

Eric Drevet, Bernard Boutherin

OSUG

Authentification versus droits ou rôles

- Les outils fournis par les fédérations d'identité ont pour but de vérifier l'identité – *authentifier* - la personne.
  ⇒Une fois cette personne authentifiée ils vont retourner des attributs sur cette personne dont son mail
  ⇒C'est magali.petestreussie@univ-grenoble-alpes.fr qui veut utiliser le service
- C'est l'application qui doit gérer les droits – *le rôle* - de la personne en fonction des attributs reçus
  => magali.petestreussie@univ-grenoble-alpes.fr a le droit ou n'a pas le droit de se connecter à mon application

OSUG

SAML protocole standardisé

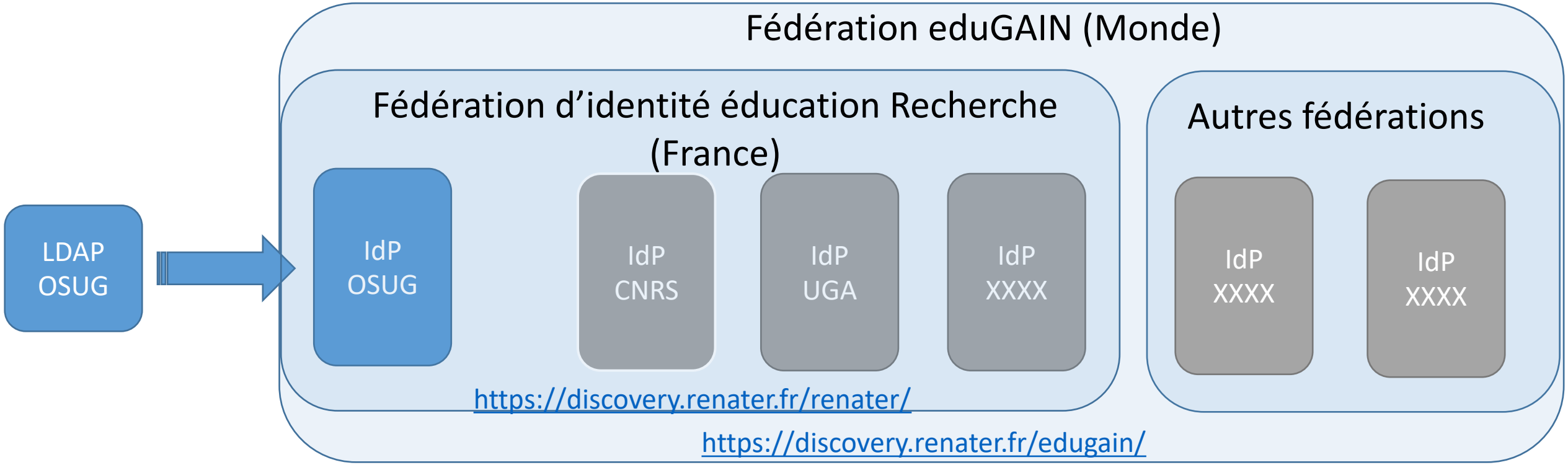
- OASIS : consortium de standardisation
- SAML est normalisé par l'OASIS
- SAML permet l'échange sécurisé d'informations d'identité dans un format XML où certaines parties peuvent être chiffrées par l'expéditeur ou par le destinataire.
- SAML définit trois briques de base
  - *L'Identity Provider* (Idp) qui authentifie l'utilisateur et récupère les attributs associés à son identité.
  - Le *Service Provider* (SP) qui protège l'accès à l'application sans authentification et redirige l'utilisateur vers son IdP
  - Dans le cadre d'une fédération le *Discovery Service* (DS) qui permet à l'utilisateur de choisir son IdP dans une liste.

OSUG

Shibboleth

- Pourquoi ce nom imprononçable ?
- Shibboleth est l'implémentation opensource du protocole SAML

Fédérations d'identité en France et dans le monde



Liste des IdP : https://services.renater.fr/federation/introduction/la-federation-education-recherche/fer-idps

OSUG

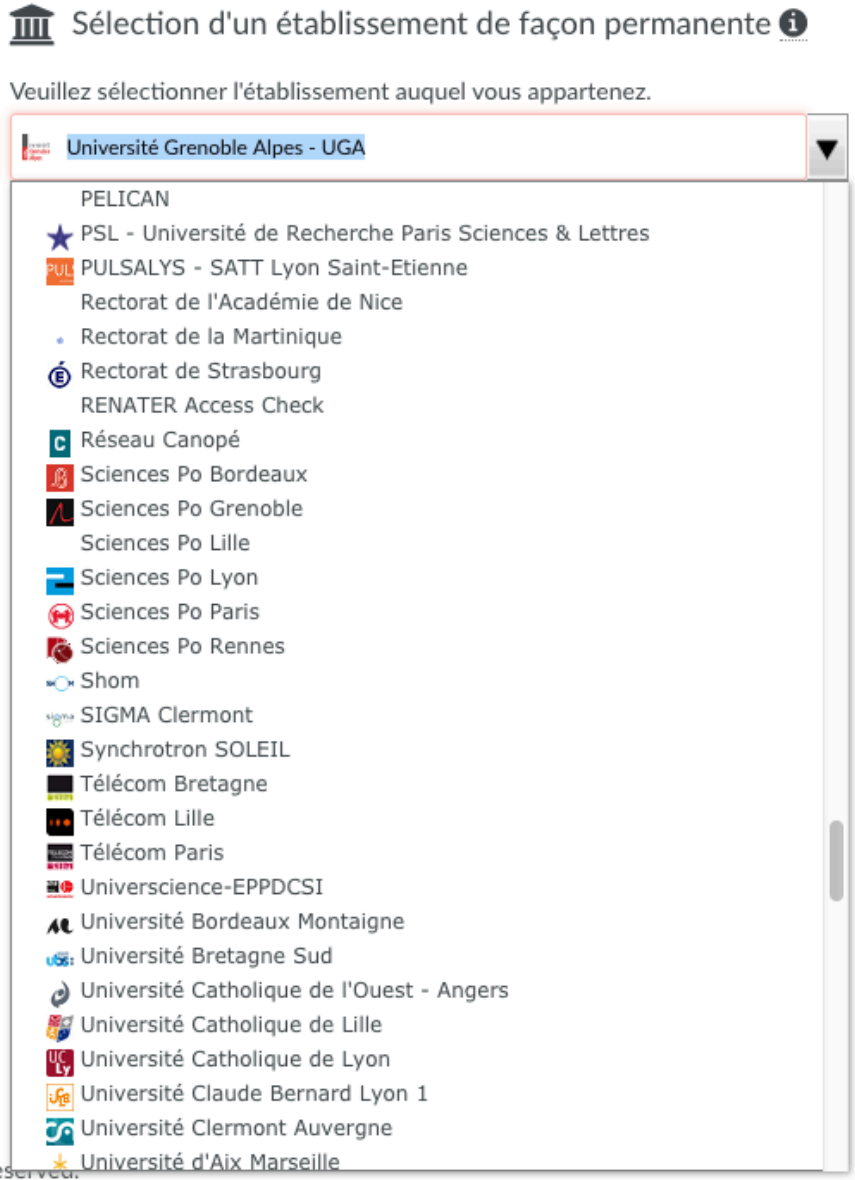
Discovery Service Fédération éducation-Recherche

Fédération Éducation - Recherche

- WAYF Where Are You From?

Choisir un IdP

- https://discovery.renater.fr/renater/



Discovery Service Fédération EduGAIN

Fédération eduGAIN

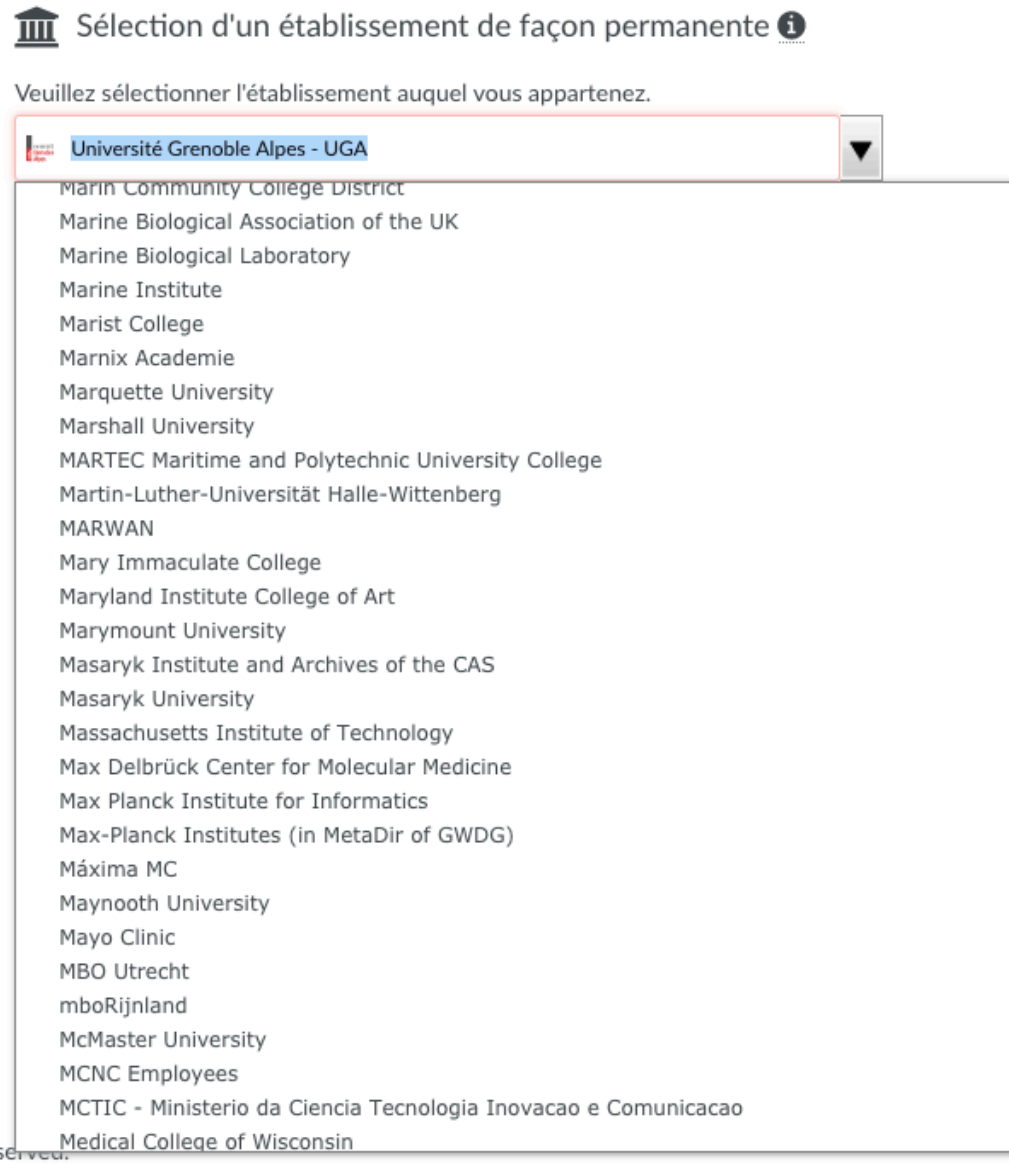
- eduGAIN

Education Global Authentication Infrastructure

Interconnecte des fédérations d'identité.

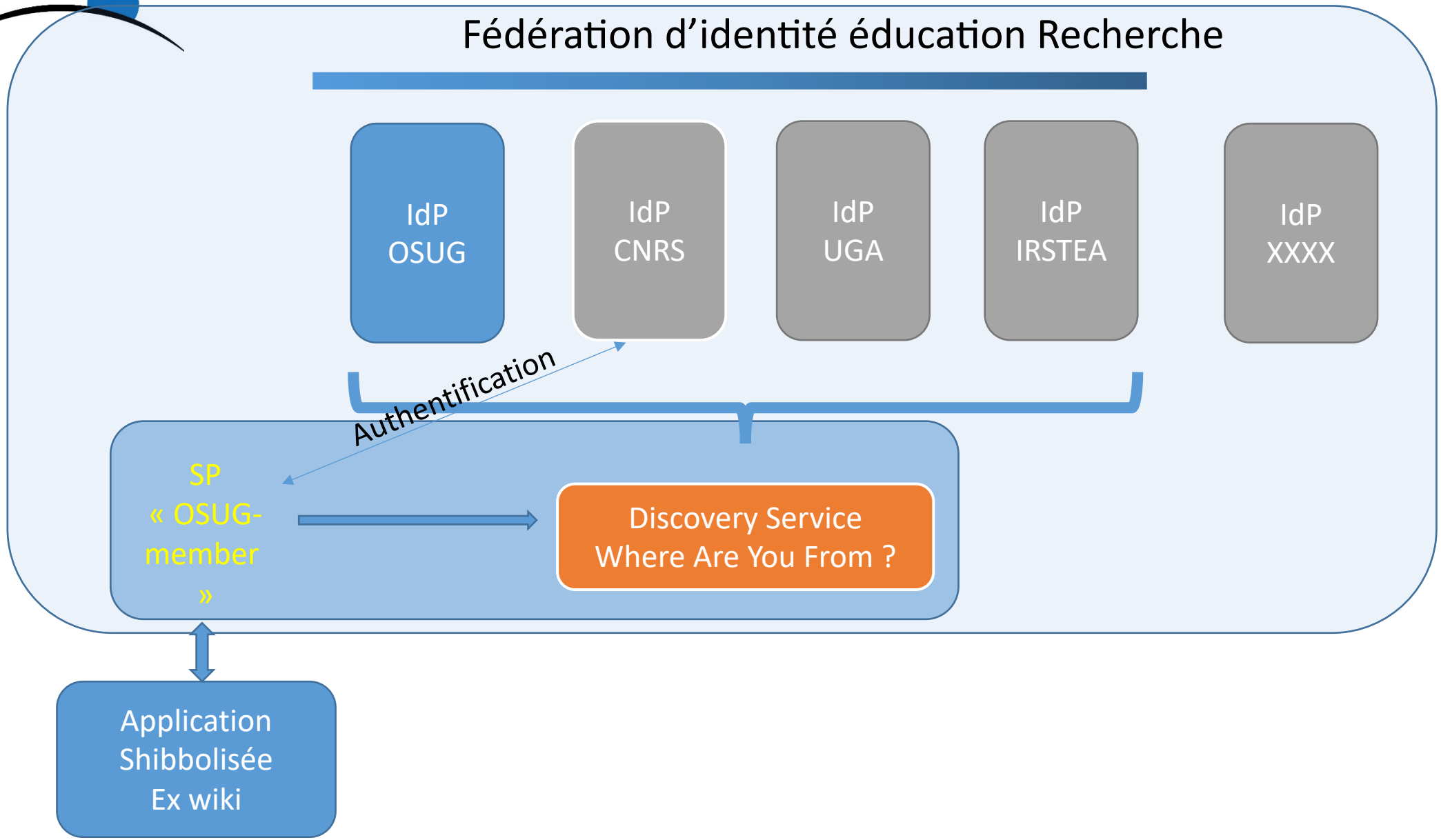
Au départ (2004-2009) un projet Européen!
Depuis 2012 projet de portée mondiale.

- https://discovery.renater.fr/edugain/



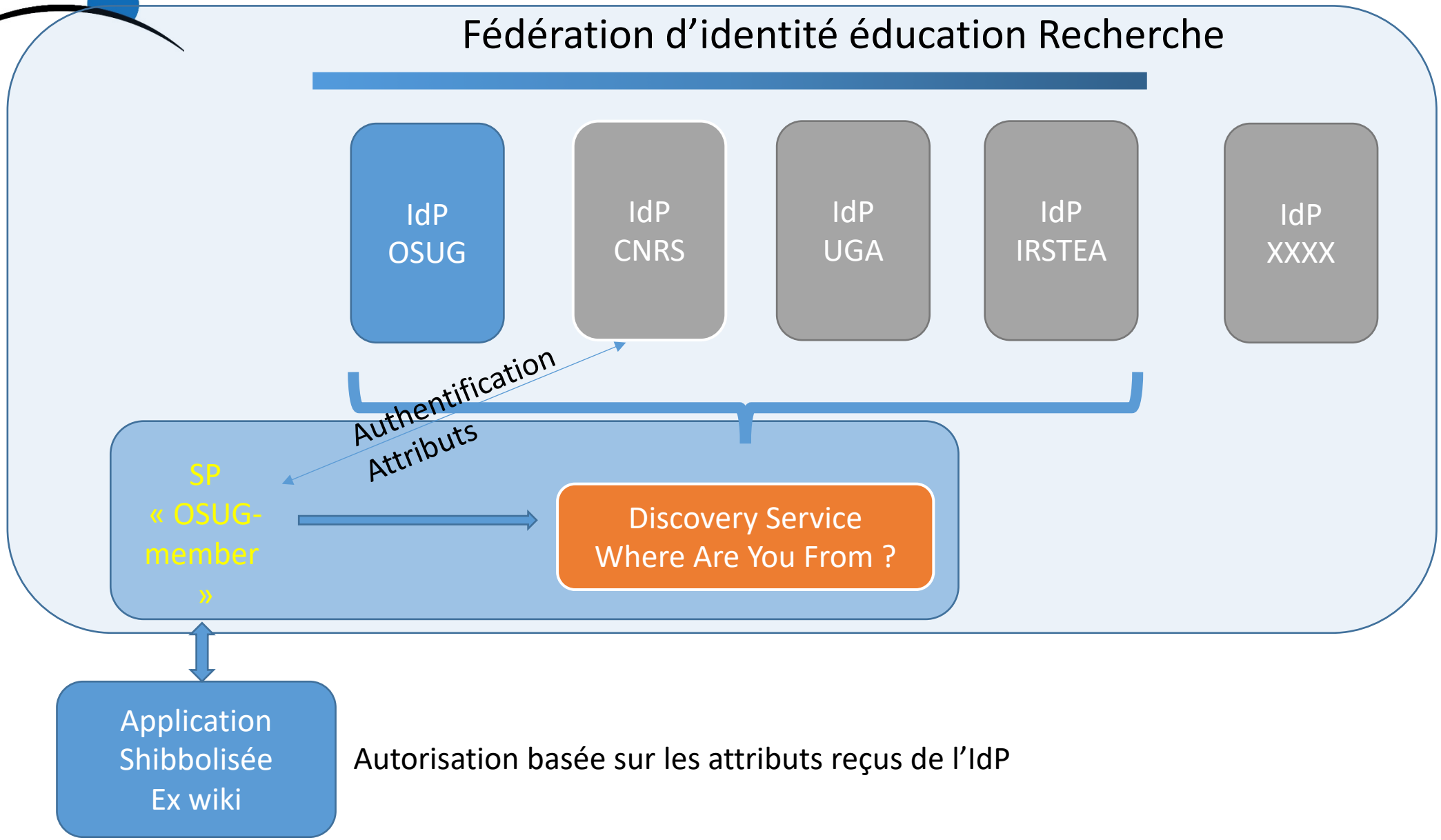
OSUG

Le rôle du Service Provider SP



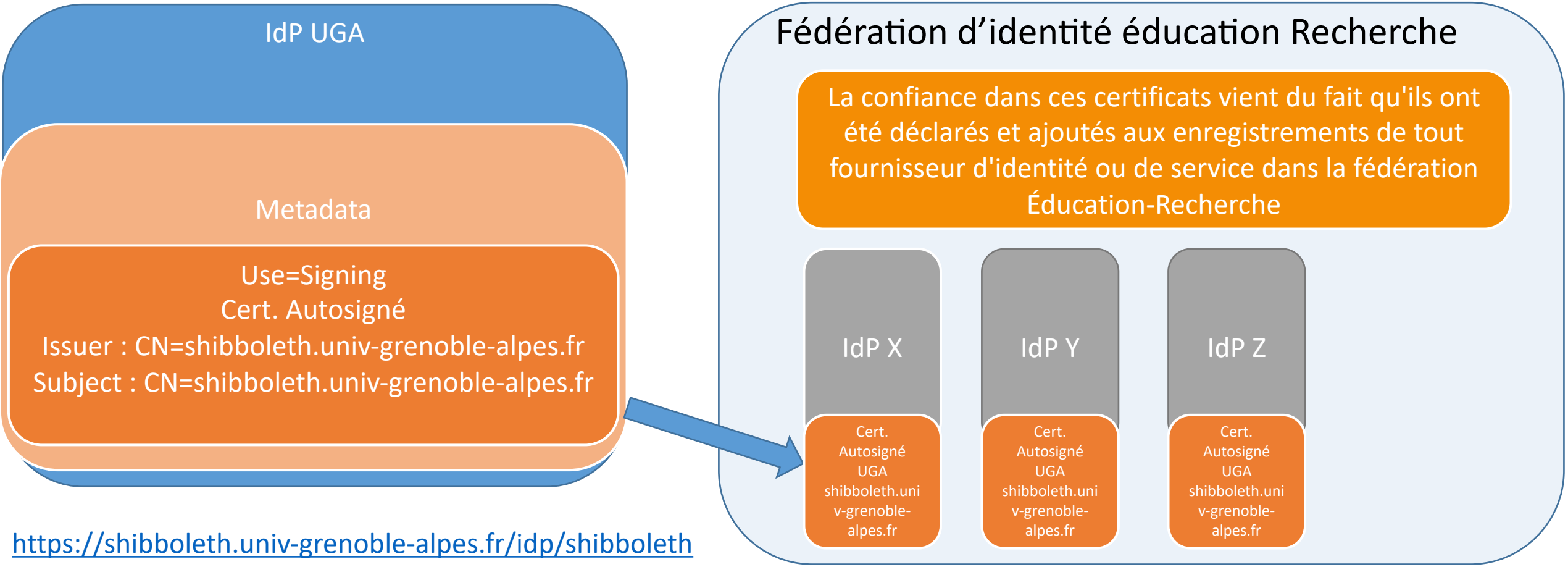
OSUG

Le rôle du Service Provider SP



Autorisation basée sur les attributs reçus de l'IdP

La confiance dans la fédération



https://shibboleth.univ-grenoble-alpes.fr/idp/shibboleth

https://services.renater.fr/federation/documentation/guides-installation/idp3.4/chap01#federation_d_identite_et_certificats

OSUG

Attributs retournés par un IdP

- A droite les attributs fournis par l'IdP UGA
- Autorisation
  - en fonction des attributs
  - Ou en fonction d'une liste de mails (qui est un attribut en fait)
  - Ou en fonction des IdP interrogés

Le Service Provider de Renater ci-dessous liste les attributs et variables retournés par l'IdP :

https://test-sp.federation.renater.fr/

Attribut (a↓z)	Valeur
mail	Bernard.Boutherin@univ-grenoble-alpes.fr
eduPersonPrincipalName	boutherb@univ-grenoble-alpes.fr
displayName	Bernard Boutherin
givenName	Bernard
sn	Boutherin
cn	boutherin bernard
supannEtablissement	{UAI}0383493R
eduPersonAffiliation	researcher;member;faculty
uid	boutherb
eduPersonPrimaryAffiliation	faculty
eduPersonScopedAffiliation	researcher@univ-grenoble-alpes.fr;faculty@univ-grenoble-alpes.fr;member@univ-grenoble-alpes.fr
eduPersonTargetedID	https://shibboleth.univ-grenoble-alpes.fr/idp/shibboleth!https://test-sp.federation.renater.fr!KvlHb9V26LJhUr7t9Ig/qBB9GOt
supannEmpId	83830
supannCivilite	M.
telephoneNumber	0456520883
postalAddress	UMS OSUG$bureau 115$OSUG D$CAMPUS
supannRoleGenerique	{PEC}accompagnateur
supannEtuSecteurDisciplinaire	{INCONNU}
supannListeRouge	FALSE
schacHomeOrganization	univ-grenoble-alpes.fr
schacHomeOrganizationType	urn:schac:homeOrganizationType:int:university

OSUG

Attributs
retournés par les IdP UGA et CNRS

Attribut (a↓z)	Valeur
mail	Bernard.Boutherin@univ-grenoble-alpes.fr
eduPersonPrincipalName	boutherb@univ-grenoble-alpes.fr
displayName	Bernard Boutherin
givenName	Bernard
sn	Boutherin
cn	boutherin bernard
supannEtablissement	{UAI}0383493R
eduPersonAffiliation	researcher;member;faculty
uid	boutherb
eduPersonPrimaryAffiliation	faculty
eduPersonScopedAffiliation	researcher@univ-grenoble-alpes.fr;faculty@univ-grenoble-alpes.fr;member@univ-grenoble-alpes.fr
eduPersonTargetedID	https://shibboleth.univ-grenoble-alpes.fr/idp/shibboleth!https://test-sp.federation.renater.fr!KvHb9V26LJhUr7t9Ig/qBB9GOtY=
supannEmpId	83830
supannCivilite	M.
telephoneNumber	0456520883
postalAddress	UMS OSUG$bureau 115$OSUG D$CAMPUS
supannRoleGenerique	{PEC}accompagnateur
supannEtuSecteurDisciplinaire	{INCONNU}
supannListeRouge	FALSE
schacHomeOrganization	univ-grenoble-alpes.fr
schacHomeOrganizationType	urn:schac:homeOrganizationType:int:university

Attribut (a↓z)	Valeur
mail	Ulrick.medda@meteo.fr
eduPersonPrincipalName	ulrick.medda@cnrs.fr
displayName	MEDDA Ulrick
givenName	Ulrick
sn	MEDDA
cn	MEDDA Ulrick
supannEtablissement	{METEO-FRANCE}UMR3589
eduPersonAffiliation	employee
uid	ulrick.medda
eduPersonScopedAffiliation	employee@cnrs.fr
eduPersonTargetedID	https://janus.cnrs.fr/idp!https://test-sp.federat /idp!https://test-sp.federation.renater.fr!AK5H
o	METEO-FRANCE
ou	UMR3589
eduOrgLegalName	Centre National de la Recherche Scientifique

OSUG

Attributs retournés par les IdP INRAE et IRSTEA

Attribute (a↓z)	Value
mail	eric.maldonado@inrae.fr
eduPersonPrincipalName	emaldonado@inra.fr
givenName	Eric
sn	Maldonado
cn	Eric Maldonado
eduPersonAffiliation	member;employee
uid	emaldonado
eduPersonScopedAffiliation	employee@inra.fr;member@inra.fr
eduPersonTargetedID	https://idp-preprod.inra.fr/idp/shibboleth!htt sp.federation.renater.fr!w1HtpBYM2ngdQI
telephoneNumber	+33 4 76 76 28 15
eduPersonPrimaryOrgUnitDN	01
eduPersonOrgUnitDN	1306
schacHomeOrganization	inra.fr
schacHomeOrganizationType	urn:schac:homeOrganizationType:int:publ institution

Attribute (a↓z)	Value
mail	eric.maldonado@irstea.fr
eduPersonPrincipalName	eric.maldonado@irstea.fr
displayName	Eric Maldonado
givenName	Eric
sn	Maldonado
cn	Maldonado Eric
supannEtablissement	{SIRET}180 070 013 0014 9
eduPersonAffiliation	member;employee
uid	eric.maldonado
eduPersonScopedAffiliation	member@irstea.fr;employee@irstea.fr
eduPersonTargetedID	https://idp.irstea.fr/idp/shibboleth!https://te sp.federation.renater.fr!0XO0xgB8CWH5
schacHomeOrganization	irstea.fr
schacHomeOrganizationType	urn:schac:homeOrganizationType:int:res

OSUG

Variables retournées par le Service Provider

- Pointeur sur l'IdP
- Heure d'authentification
- Identifiant de session
  - Évite de ré-authentifier la personne dans la suite

Variable (a↓z)	Valeur
Shib-Application-ID	default
Shib-Session-ID	_04e374b312894e409b74a54fdc4e93b7
Shib-Identity-Provider	https://shibboleth.univ-grenoble-alpes.fr/idp/shibboleth
Shib-Authentication-Instant	2020-02-10T15:24:07.016Z
Shib-Authentication-Method	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-AuthnContext-Class	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-Handler	https://test-sp.federation.renater.fr/Shibboleth.sso

OSUG

En pratique…

1 – Démo

- Application de blog en PhP avec authentification simple MDP dans l'application https://auth.osug.fr/myBlogBasic user1 pwd1
- Application shibbolisée https://auth.osug.fr/myBlogA1 avec authentification obligatoire; on ne peut plus utiliser les comptes locaux

Essayer de s'authentifier avec IdP UGA, et "IdP test auth.osug.fr »

On gère les autorisations dans le fichier Users basé sur l'attribut EPPN EduPersonPrincipalName

- Application Shibbolisée et et possibilité de login normal https://auth.osug.fr/myBlogA2

Possible aussi de créer une IdP pour les logins particuliers

OSUG

En pratique

2 - Fichiers de conf

/etc/apache2/sites-enabled/000-default-ssl.conf

/etc/shibboleth/shibbolet2.xml plusieurs types de Discovery Service ou IdP direct

« systemctl reload shibd » après modification

/etc/switchwayf/etc/IDprovider.conf configuration du DS

Attention le CNRS n'est pas dans la fédération de test

=> Comparer les fichiers de configuration

/var/www/html/appl1

Blog.class.php

shiblogin

/var/www/html/basic/

Blog.class.php