

CAMPUS CONDORCET Paris–Aubervilliers
Cité des humanités et des sciences sociales

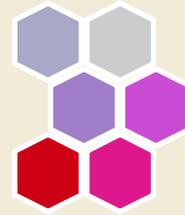
Référentiel d'Identités du Campus Condorcet (POC RICCO)

ANF Données de la recherche 2017 – Nancy

Gautier Auburtin - Chargé d'urbanisation numérique
Correspondant Informatique et libertés



Plan de l'intervention



Présentation rapide du Campus Condorcet

- Fondateurs et partenaires institutionnels
- Structures de recherche et populations concernées
- Services offerts par le Campus pour les données de la recherche

Gestion des identités sur le Campus

- Objectifs d'un référentiel / Vie de Campus
- Scénarios motivant une preuve de concept (POC)
- Standards de gestion des identités dans l'ESR
- Protection des données personnelles (CNIL / CIL)
- Gouvernance en lien avec les établissements fondateurs
- Choix d'un modèle orienté utilisateur

Élargissement aux identifiants de la recherche

- Implémentation possible d'ORCID
- Autres Perspectives (OpenID, FranceConnect)

Présentation du Campus Condorcet



L'ÉCOLE
DES HAUTES
ÉTUDES EN
SCIENCES SOCIALES



École
nationale
des
chartes



École Pratique
des Hautes Études

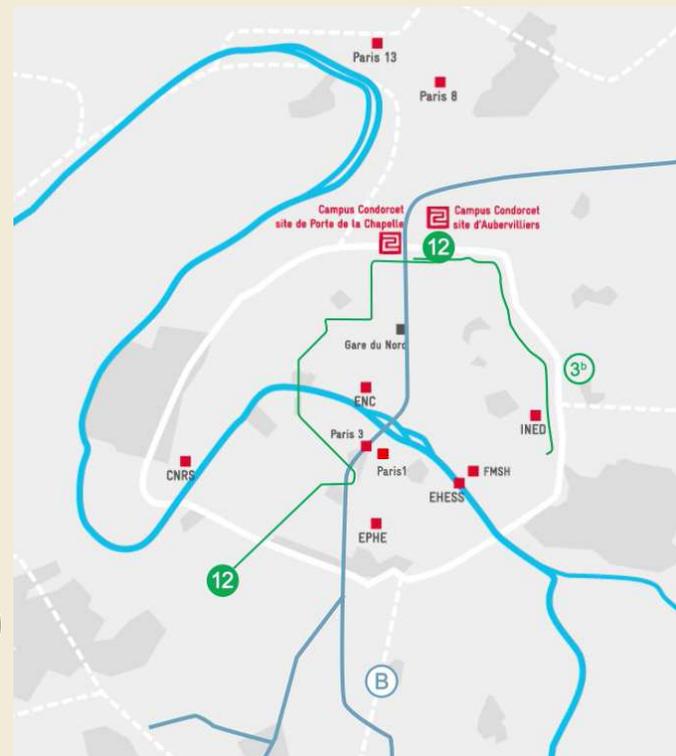


fondation
maison des
sciences
de l'homme

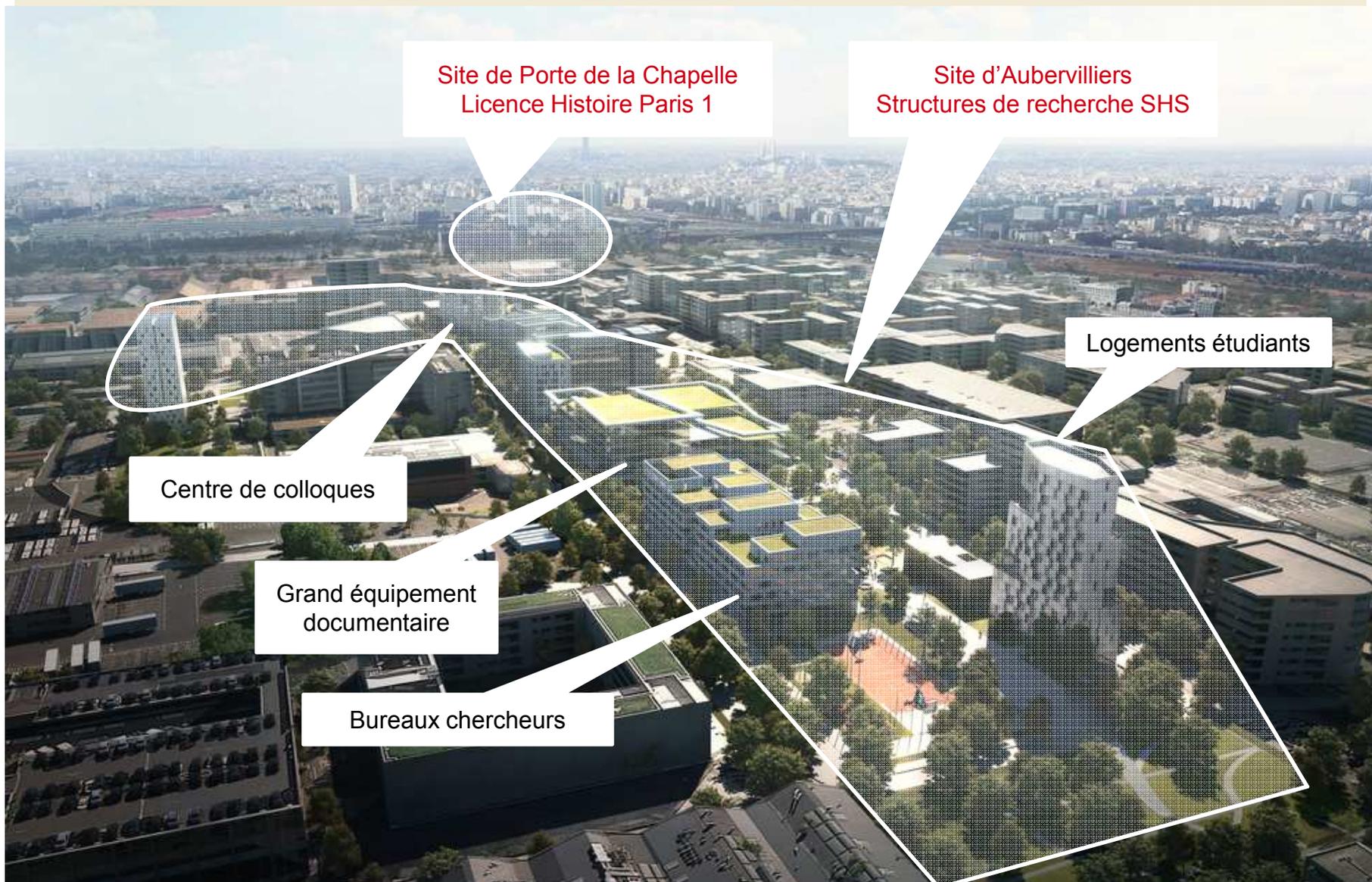
10 fondateurs unis pour un projet commun



- En 2019, 6 000 usagers (potentiel 15 000)
- 10 établissements fondateurs :
CNRS, EHESS, ENC, EPHE, FMSH, INED, Paris 1, Paris 3, Paris 8, Paris 13
- 60 unités de recherche (10 sous multiples tutelles)
- 50 centres documentaires rassemblés dans le GED
- 2 Sites : Aubervilliers & Porte de la Chapelle
(Licences Histoire Paris 1)



Perspective Nord-Sud du Campus



Organisation fonctionnelle du Campus

Plan de masse du site d'Aubervilliers

- 2 résidences étudiantes
- 3 bâtiments dédiés (EHESS, EPCC, INED)
- 1 grande bibliothèque (GED)
- 2 bâtiments de bureaux mutualisés
- 6 « équipements » mutualisés
- 1 programme principal en PPP
- 3 programmes en MOP (région IDF, EPCC)



10 fondateurs unis pour un projet commun



Profils d'usagers sur le Campus

6 000 usagers (potentiel 15 000)

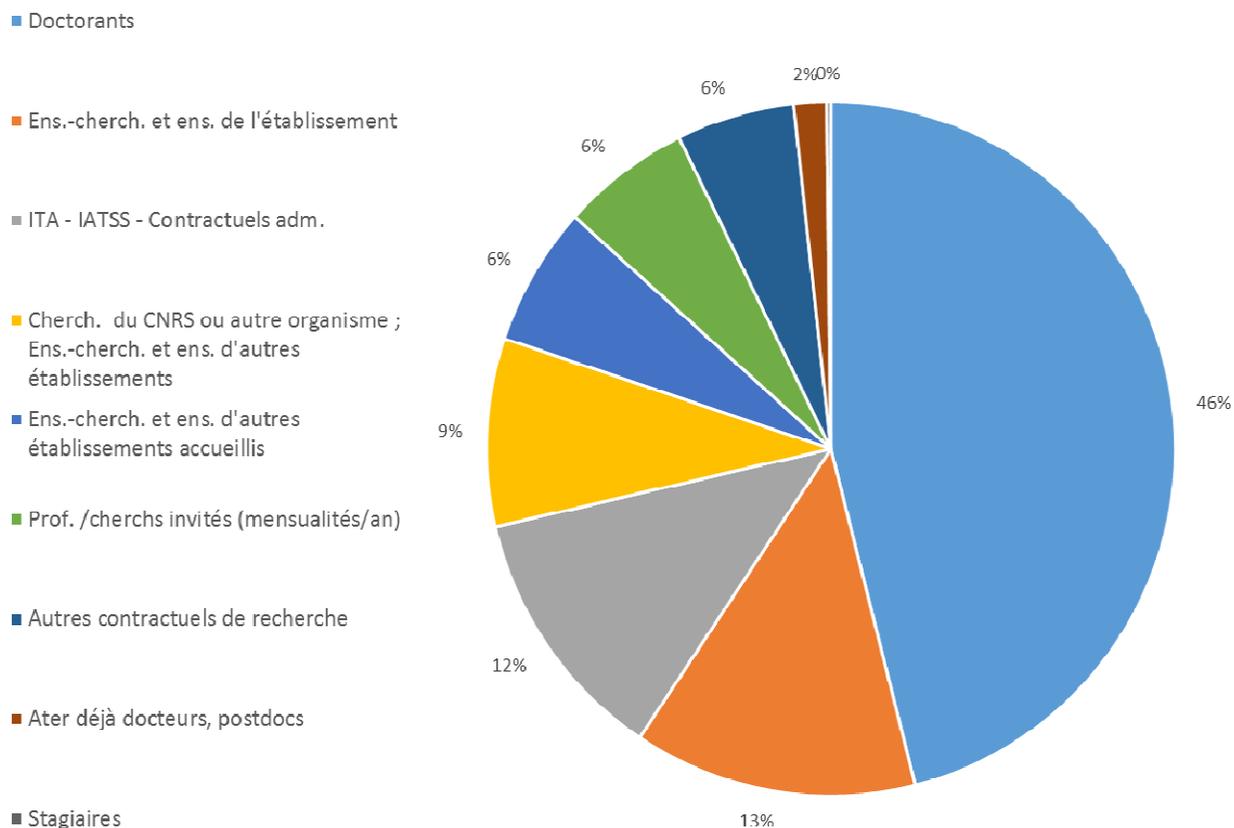
Profils

[projection 2013]

- 46 % Doctorants
- 13 % Docteurs
- 15 % Chercheurs
- 6% Profs. invités

- 12% ITA
- 6% Contractuels

Population par catégorie d'usagers



Services potentiels pour les données

Grand équipement documentaire

- 50 centres documentaires
- Bibliothèques FMSH & INED
- Archives scientifiques UMR
- 1 Mn de documents (80% LA)
- Délégitaire Collex Persée

Hôtel à projets

- Accueil de projets
- Salle serveur et équipements
- Equipe pluri-compétences

Structures installées en tout ou partie

- Huma-Num (CNRS)
- CLAMOR (CNRS)
- IRHT (CNRS)
- PRODIG (Paris 1)
-

Projets soutenus

- Biblissima (Equipex, 2011-2018)
- Labex (Arts-H2H) ; appels à projets Campus Condorcet



Grand équipement documentaire (E. de Prozamparc)



Objectifs du référentiel d'identités Campus

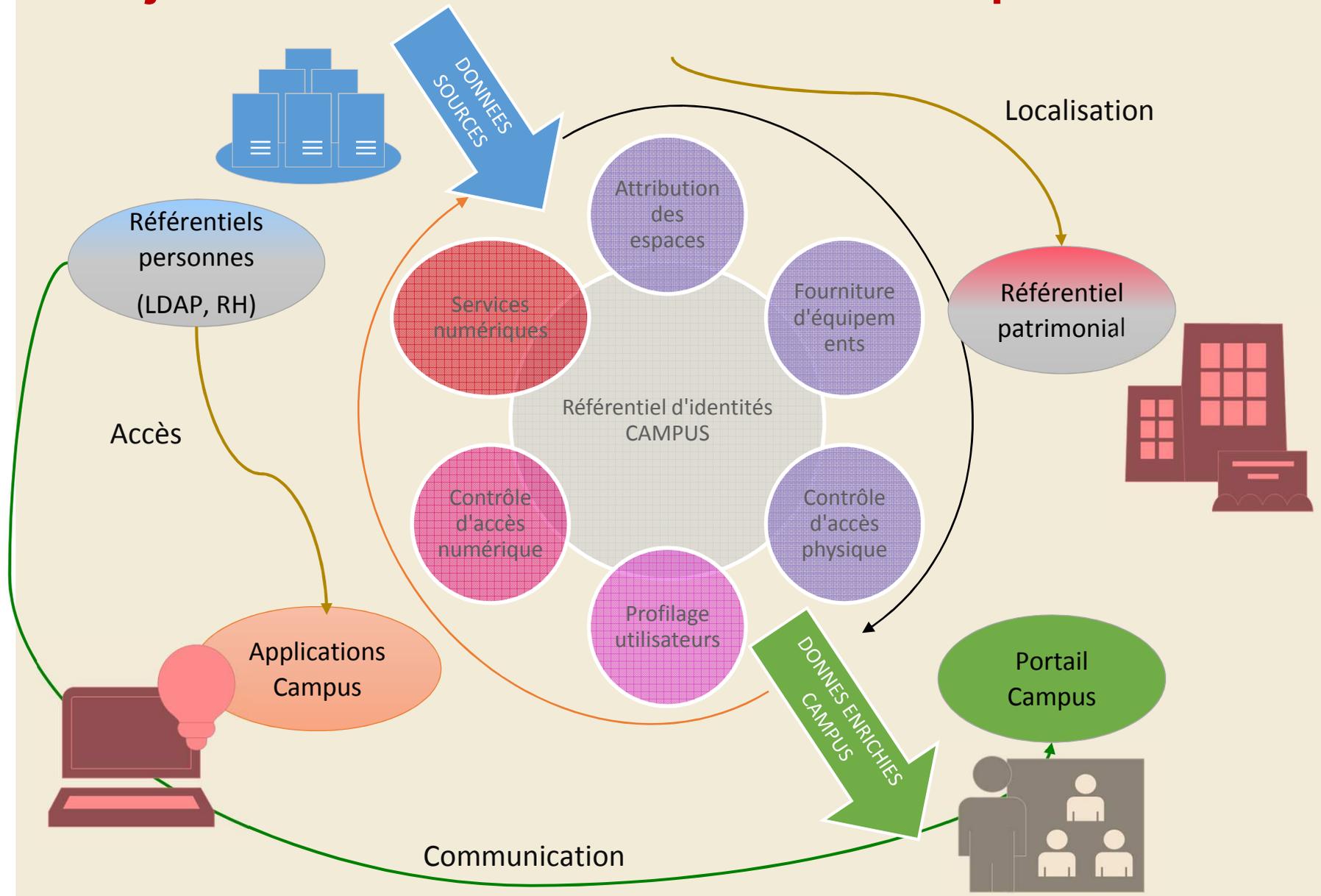
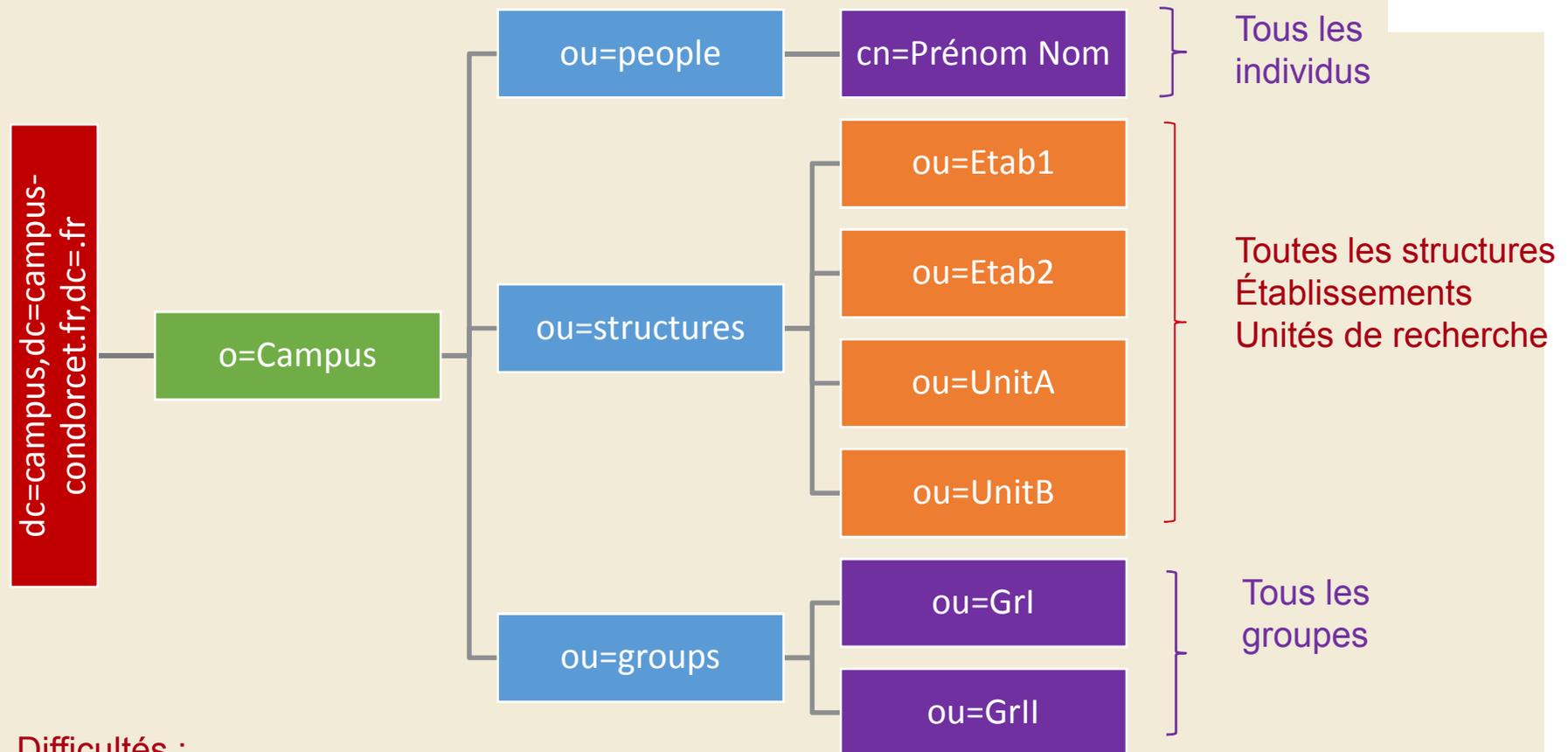


Schéma type d'un annuaire LDAP



Difficultés :

- La structure LDAP remet à plat la structure organisationnelle (individus, structures et groupes)
- Seules les valeurs des attributs permettent d'organiser entre eux les objets
supannEtablissement : {UAI}0753742K
supannRoleEntite = [role=STAGIAIRE][type=pôle][code=communication]
- Ces valeurs sont fondées sur des schémas et des nomenclatures différemment appliquées

De quelles données a-t-on besoin ?

Valeurs utiles	Attribut	Format/ qualité
Identifiant	eduPersonPrincipalName	pnom@domaine.fr prenom.nom@domaine.fr
Nom	surname	Dépend du SI RH Modifiable par l'individu ?
Prénom	givenName	Dépend du SI RH Modifiable par l'individu ?
Courriel	mail	<u>prenom.nom@domaine.fr</u>
Statut principal	eduPersonPrimaryAffiliation	researcher
Statuts	eduPersonAffiliation	student, faculty, employee, affiliate, alum, researcher, retired, emeritus, member, staff, teacher et registered_reader
Établissement	supannEtablissement	Code Etablissement UAI / SIRET (CNRS)
Affectation principale	supannEntiteAffectationPrincipale	Code Unité Code Local / Code RNSR
Affectations	supannEntiteAffectation	Code Unité Code Local / Code RNSR
Corps	supannEmpCorps	Nomenclature NCORPS (MENESR, Base Centrale des Nomenclatures)
Liste rouge	supannListeRouge	Souhaite ou non être présent dans l'annuaire

Autres attributs à considérer

Valeurs utiles	Attribut	Format/ qualité
Identifiant stable	eEduPersonUniqueId	124556@domaine.fr Opaque Nécessaire pour EDUGAIN
Affiliation	eduPersonScopedAffiliation	faculty@domaine.fr profil.domaine.fr Nécessaire pour EDUGAIN
Organisation	schacHomeOrganization*	domaine.fr profil.domaine.fr Nécessaire pour EDUGAIN
Type d'Organisation	schacHomeOrganizationType*	urn:schac:homeOrganizationType:eu:higherEducationalInstitution Nécessaire pour EDUGAIN
Identifiant ORCID	eduPersonOrcid	http://orcid.org/0000-0002-1825-0097
Données privées	schacMotherTongue* schacGender schacDateOfBirth schacYearOfBirth schacPlaceOfBirth schacCountryOfCitizenship schacPersonalTitle	Rarement disponibles dans les annuaires LDAP Gestion par l'utilisateur ?

*SCHAC : SCHEMA for Academia : v:1.5.0--2015 (TERENA / GEANT / EDUGAIN)

Fédération d'identité, à quoi ça sert ?

Architecture technique et organisationnelle pour l'accès à des services numériques



Shibboleth



- Niveaux de confiance entre :
 - Fournisseurs d'identités (Identity Provider, IDP)
 - Fournisseurs de services (Service Provider, SP)
 - Fournisseurs de données (Data Provider, DP) pour France Connect
- Protocole d'appui :
 - Schémas de métadonnées
 - Authentification sécurisé en mode Web
 - SAML (Security assertion markup language) pour l'ESR
 - OAuth 2.0 pour l'État et le grand public (FranceConnect, Google)
 - Différentes implémentations (Shibboleth, OpenIdConnect)

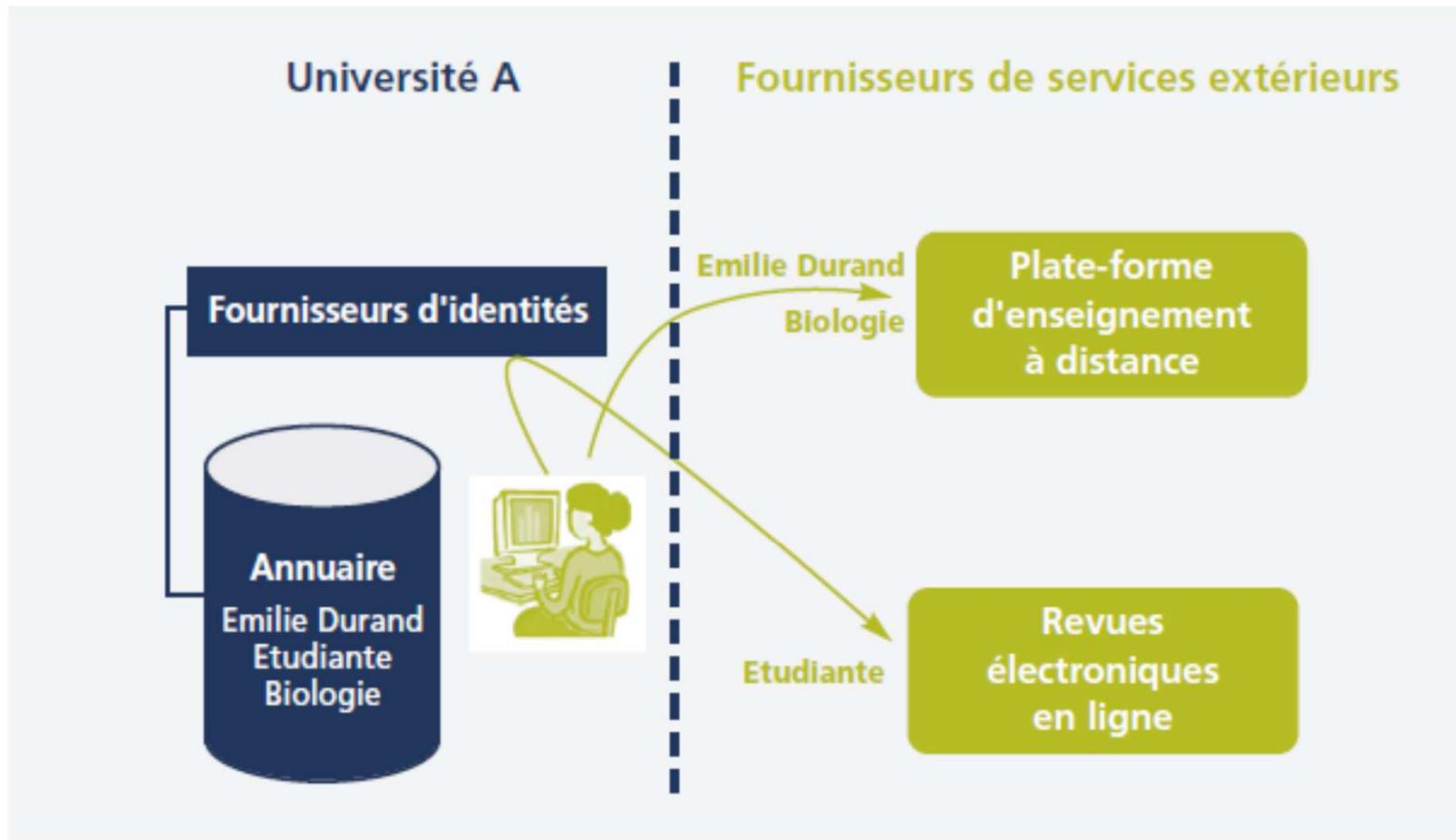
Fédérations

- Nationales :
Éducation Recherche France (Renater), État (FranceConnect), SWITCH AAI (Suisse), etc.
- Transnationales :
EDUGAIN (44 membres NREN)
- Locales :
Campus Condorcet, autres...
- Centralisées ou distribuées
(FranceConnect vs Renater)



Modalités d'accès à une ressource électronique

Schéma de fonctionnement de la fédération d'identités

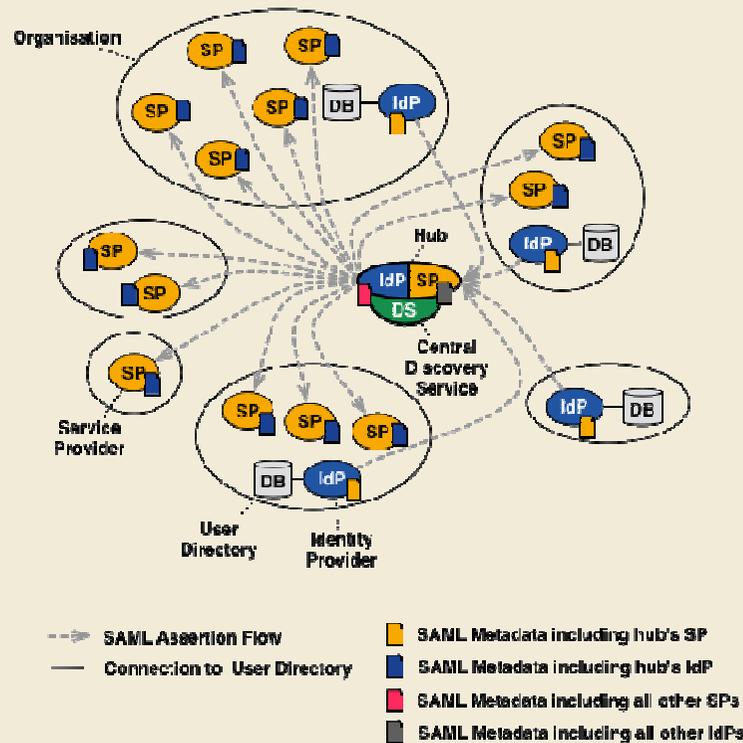


Modèles de fédérations

Hub and Spoke

Hub-and-Spoke Federation with Distributed Login

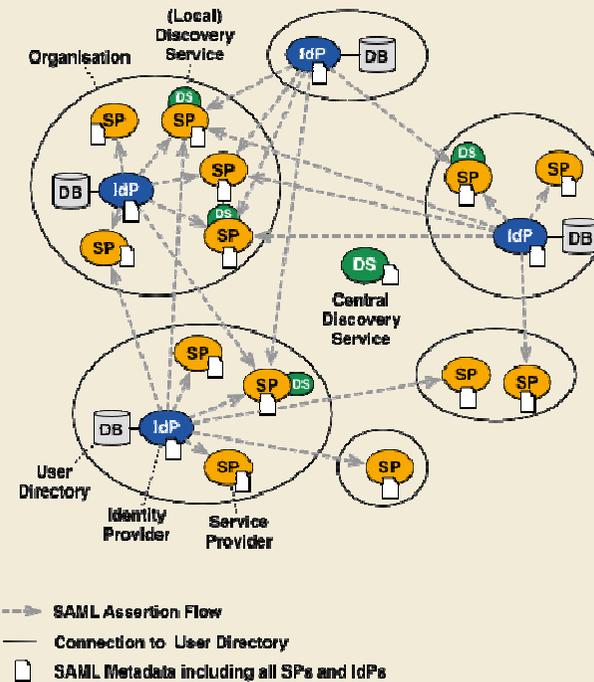
~15% of all NREN Federations (June 2013)
SURFconext, WAYF.dk, SIF, TAAT, Confia



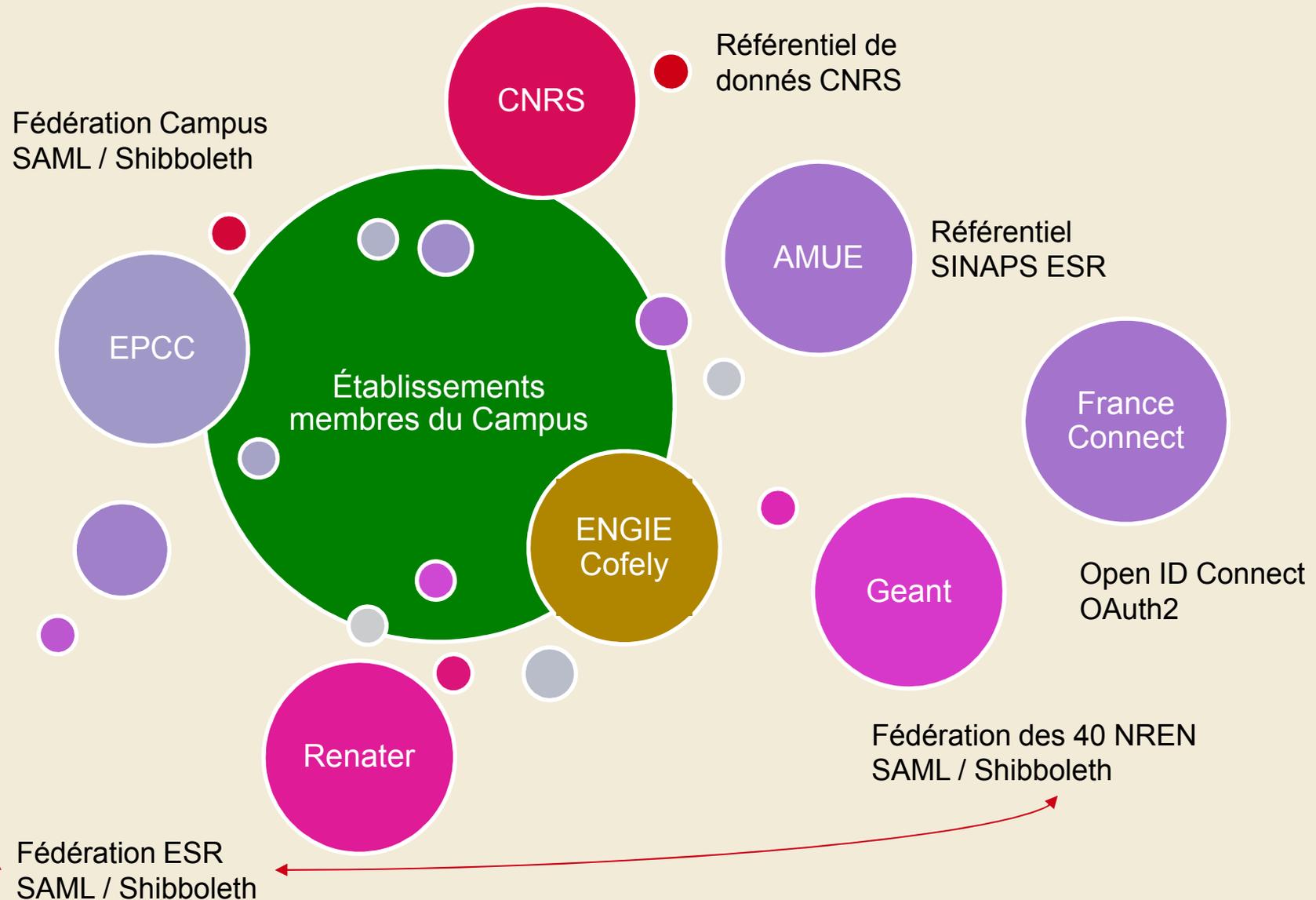
Mesh (point à point)

Full Mesh Federation

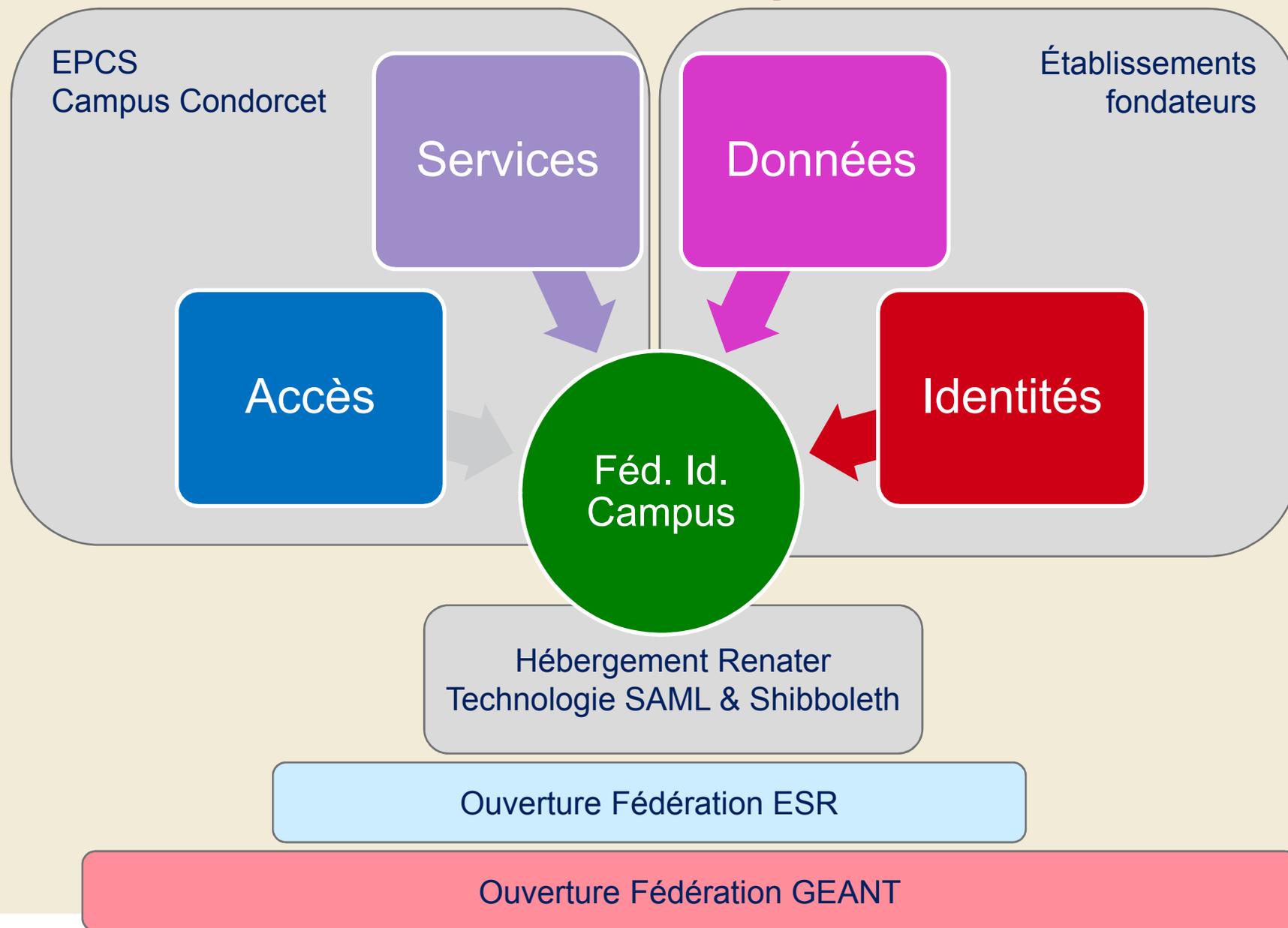
~80% of all NREN Federations (June 2013)
E.g InCommon, UKAMF, SWITCHaai, SWAMID, HAKA, AAF



Gestion des identités sur le Campus



Fédération d'identités du Campus Condorcet



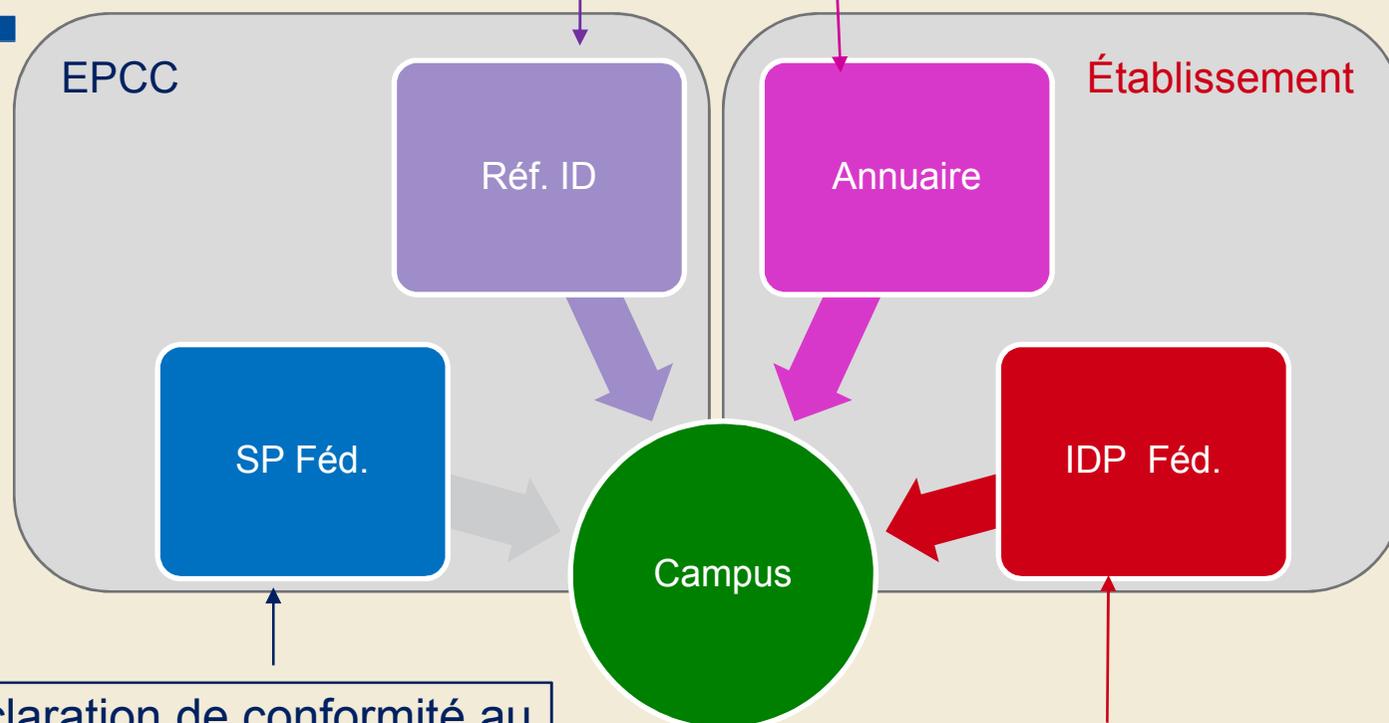
Formalités à accomplir / transferts de données

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS



Inscription au registre

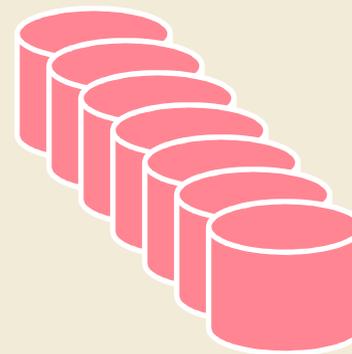
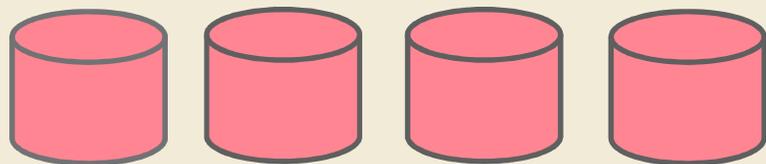
- Information préalable des personnes
- Mise à jour déclaration (ou registre) (destinataires, données transmises)



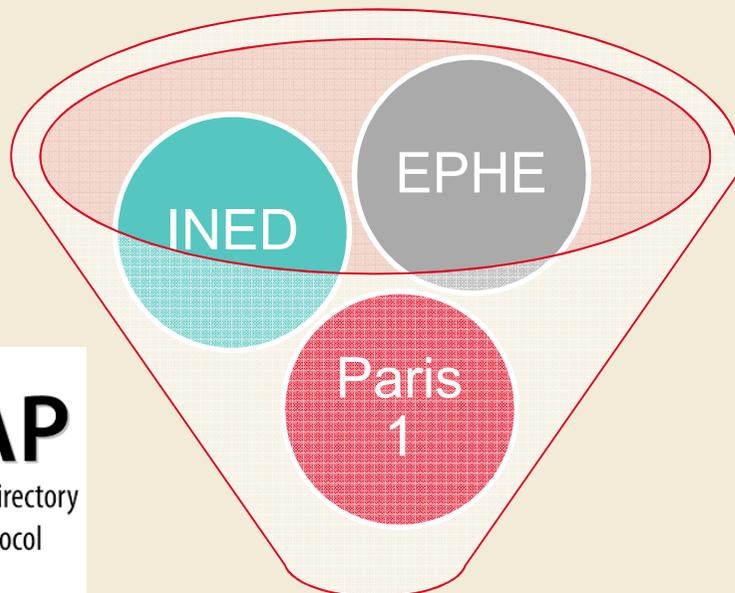
Déclaration de conformité au
RU Télé services (comptes
invités)

Mise à jour déclaration (ou registre) de
la gestion des étudiants et de l'annuaire
(destinataires, données transmises)

Modèle d'approvisionnement « classique »



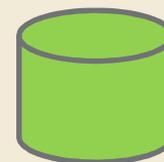
Comment informer les personnes?



LDAP
Lightweight Directory
Access Protocol



**CAMPUS @
CONDORCET**
Paris-Aubervilliers



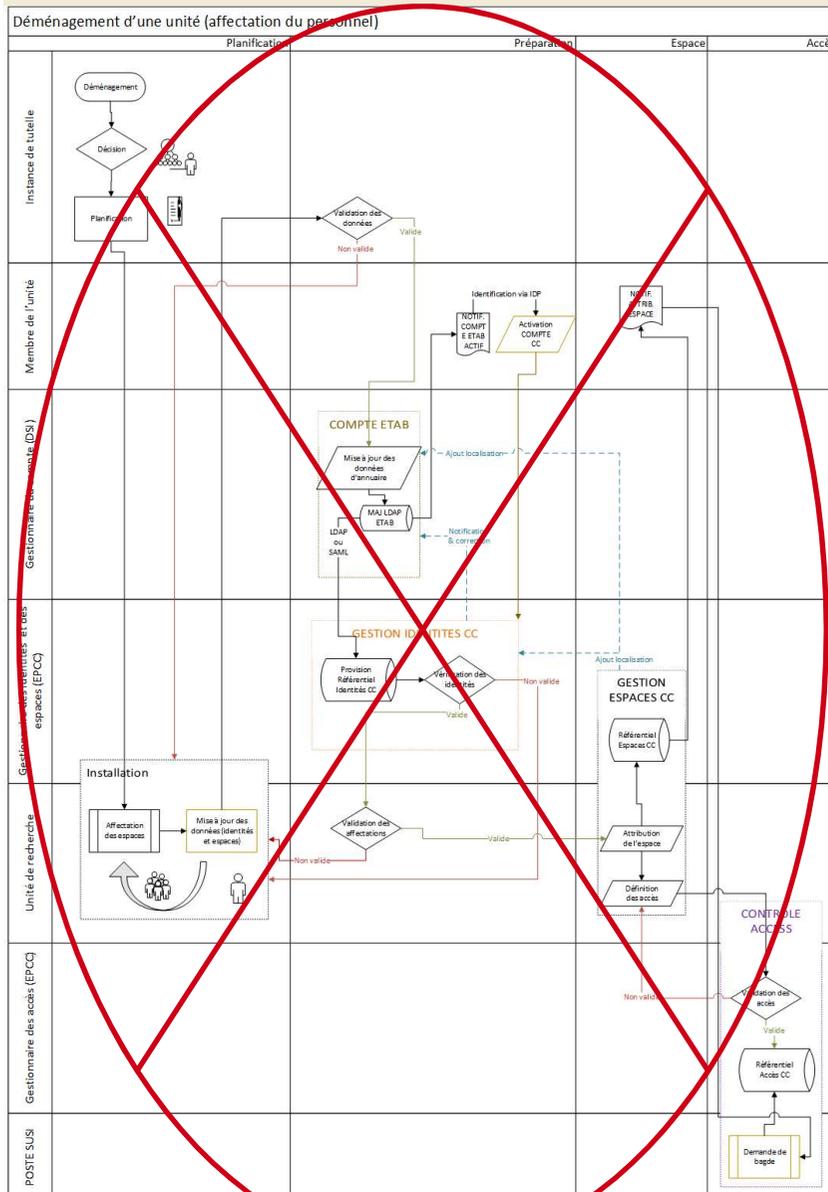
Comment synchroniser les données ?

Obstacles au transfert de données



- L'autorisation de transfert n'est accordée que sur la base de **finalités spécifiques** (une par traitement) et **détaillées** (de sorte à garantir la **proportionnalité** des données transmises aux finalités du traitement)
- Accès non justifié aux données du référentiel CNRS (Web Services)
- Difficulté pour **concilier le respect des formalités** à accomplir eu égard aux données personnelles **avec les finalités et le rythme imposé** par le POC
- Un scénario alternatif a été proposé aux CIIs :
 - **S'appuyer sur la fédération d'identités pour, dans le cadre d'un processus d'invitation, soumettre ce transfert de données à l'approbation de l'utilisateur.**
 - **L'utilisateur est actif dans le traitement de données et y donne son accord**

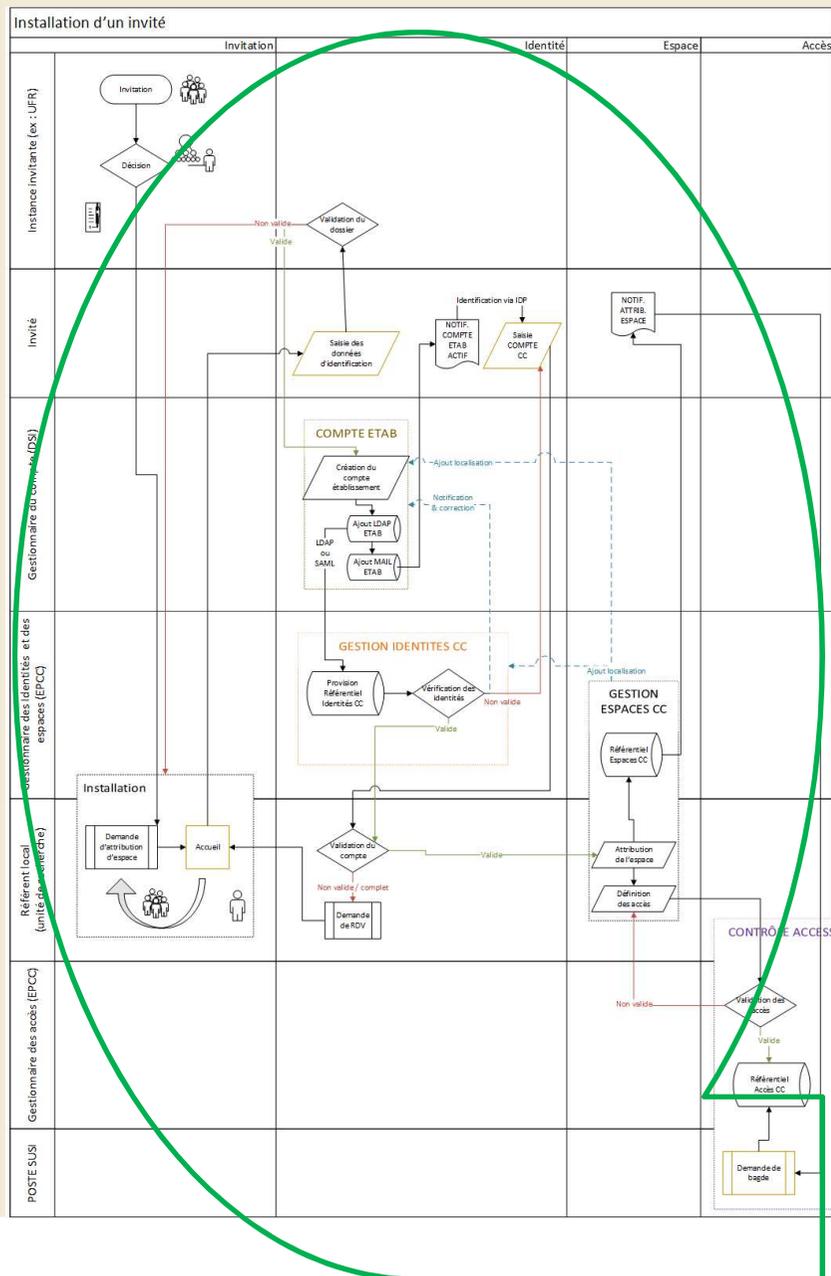
Processus de déménagement d'une unité



- Complexité des flux d'import de données disproportionnée / volume d'identités
- Absence de mécanisme de synchronisation de données

→ Abandon pour le POC (envisageable ultérieurement pour un établissement complet)

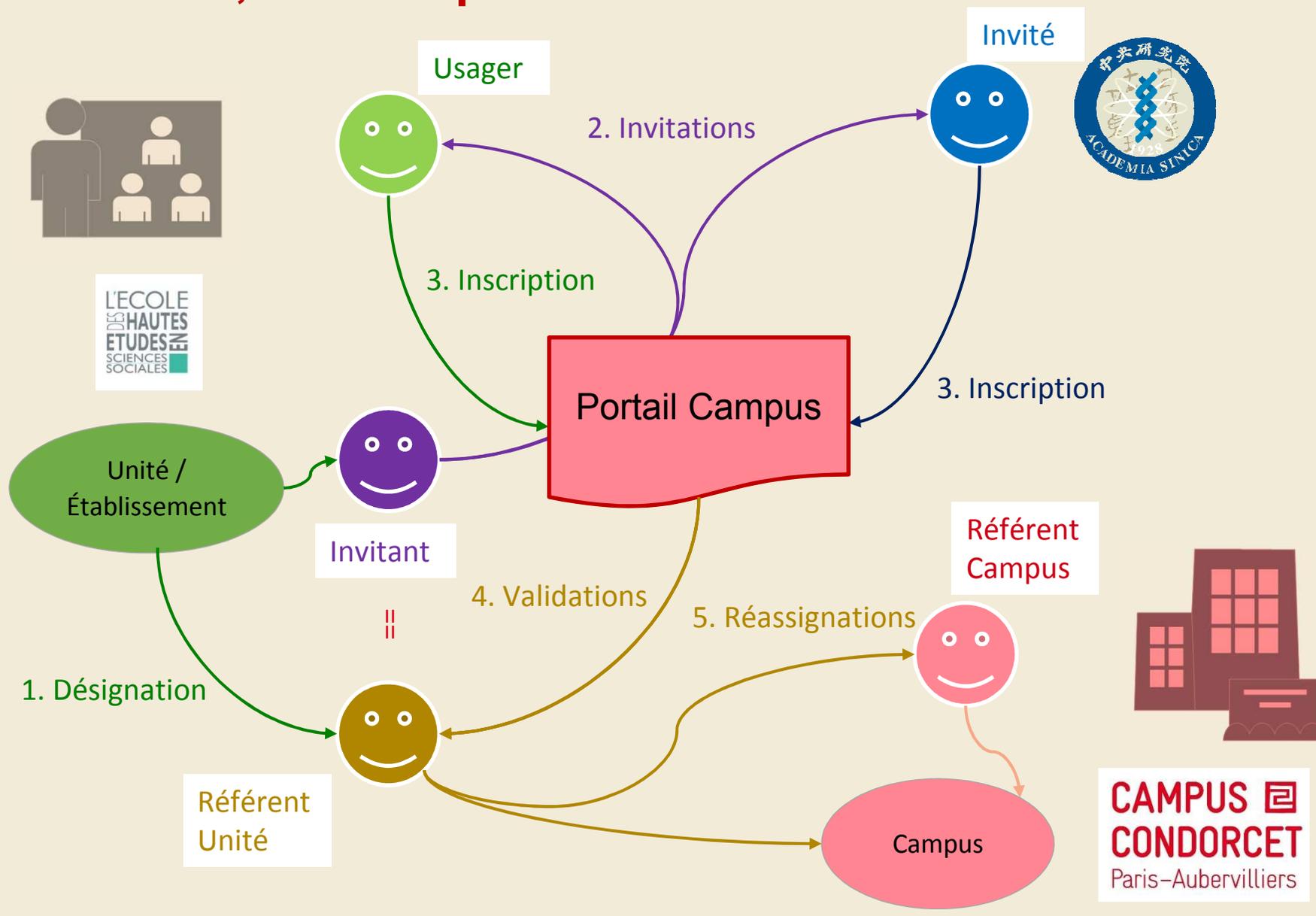
Processus d'installation d'un chercheur invité



Étape 1 : Prototype de mise au point du processus

→ Proposition : élargir à tous les établissements membres

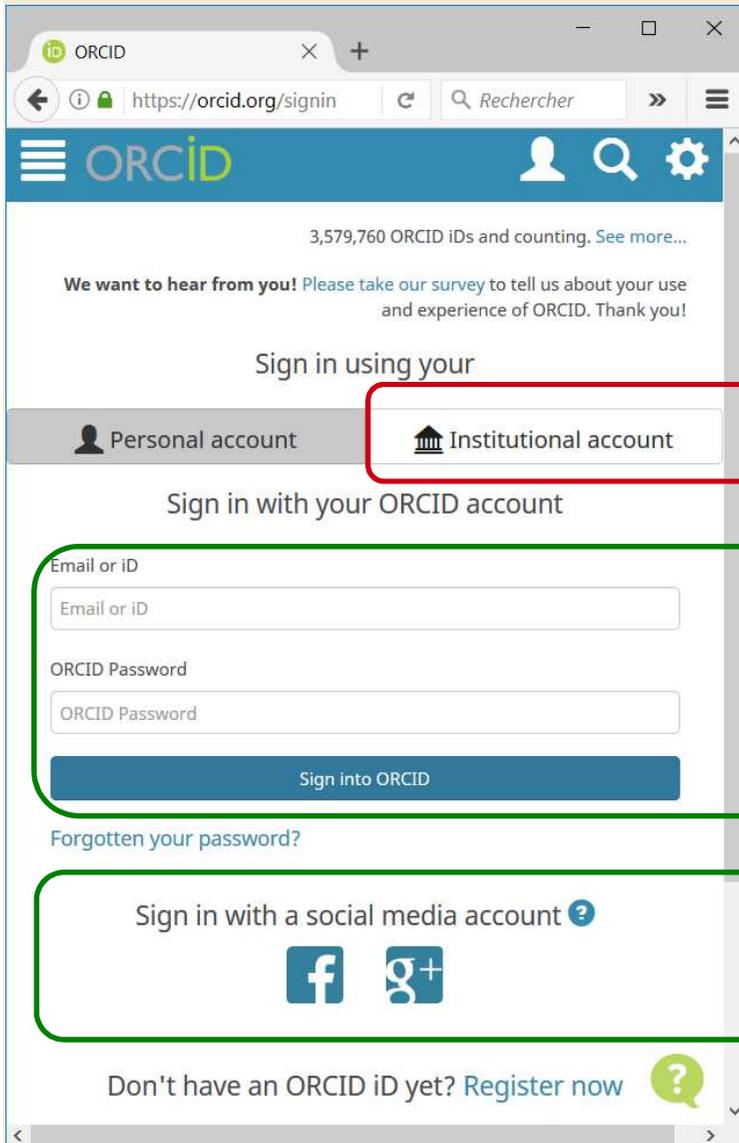
Acteurs, rôles et processus fonctionnels



Élargissement aux données de la recherche

LES IDENTIFIANTS ORCID

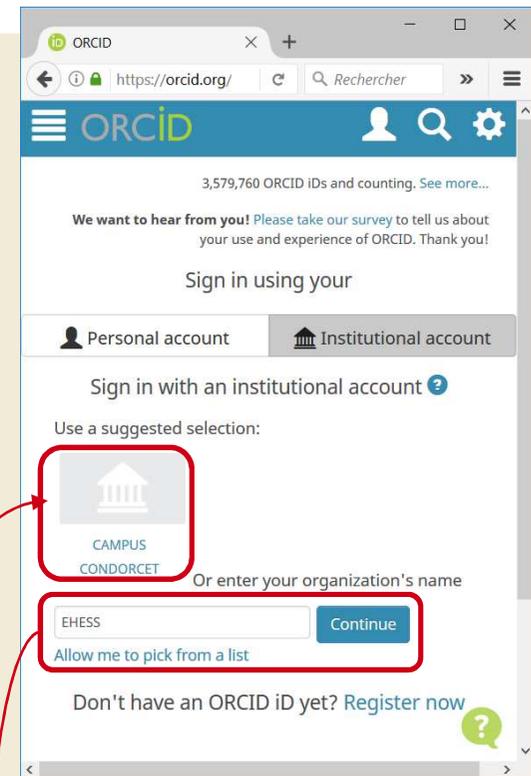
Identification sur ORCID



Compte d'affiliation institutionnel

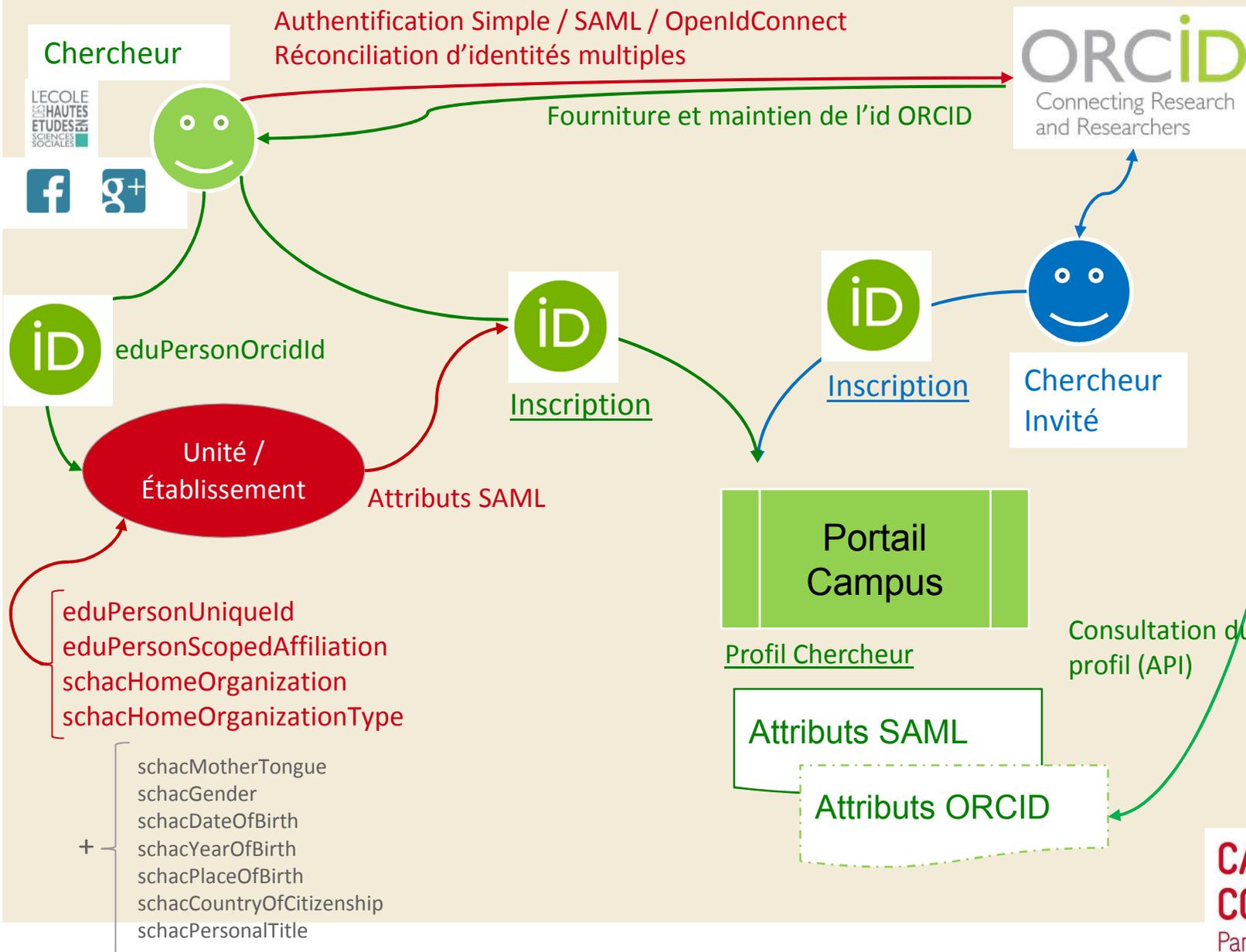
Compte local ORCID

Compte lié à une identité sociale

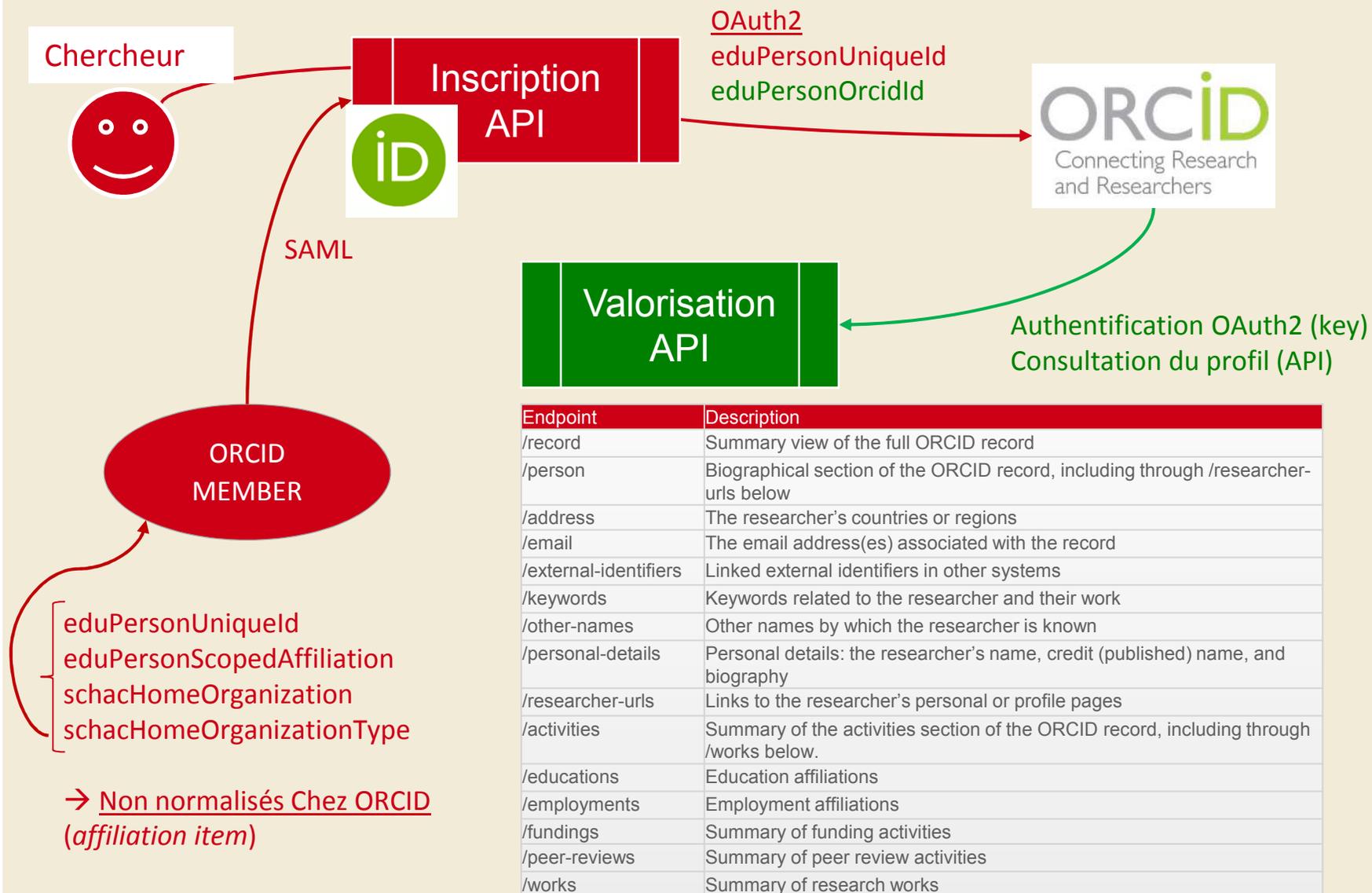


Hypothèse d'intégration d'ORCID / Portail

Profil public ou
Tiers de confiance



Modèle d'intégration ORCID / SI identités*



* <https://members.orcid.org/api/workflow/RIM-systems>

Autorisations d'accès au profil ORCID

Alternate sign in accounts

You can sign into ORCID using the personal and institutional accounts you have linked to your ORCID record.

[Find out more](#)

Alternate sign in ID	Identity provider	Access granted	
116f91...@campus-condorcet.fr	CAMPUS CONDORCET	2017-06-26	🗑️
116f91...@ehess.fr	EHESS	2017-06-26	🗑️
116f91...@gmail.com	Google	2017-06-26	🗑️

The screenshot shows the ORCID account settings page. A red box highlights the 'By default, who should be able to see information added to your ORCID Record?' section, which contains three radio button options: 'Public' (selected), 'Authenticated users', and 'Only me'. A green box highlights the 'Trusted organizations' section, which includes a description and a 'Find out more' link. Another green box highlights the 'Trusted individuals' section, which also includes a description and a 'Find out more' link. A green arrow points from the 'Niveau d'accès par défaut' label to the red box. Two green arrows point from the 'Tiers de confiance institutionnels' and 'Tiers de confiance Individuels' labels to the green boxes respectively. The browser's address bar shows 'https://orcid.org/account' and the search bar contains 'Rechercher'.

Account settings

- Email and contact preferences [Edit](#)
- Language display preferences [Edit](#)
- ORCID inbox notifications [Edit](#)
- Password [Edit](#)
- Privacy preferences [Hide](#)

By default, who should be able to see information added to your ORCID Record?

Public Authenticated users Only me

- Security question [Edit](#)
- Deactivate account [Deactivate this ORCID record...](#)
- Remove duplicate record [Remove duplicate record](#)

Trusted organizations

You can allow permission for your ORCID Record to be updated by a trusted organization. [Find out more](#)

Trusted individuals

You can grant permission to another ORCID user to update your ORCID record on your behalf. [Find out more](#)

Trusted individual	ORCID iD	Access granted
--------------------	----------	----------------

Niveau d'accès par défaut

Tiers de confiance institutionnels

Tiers de confiance Individuels

ORCID et la gestion des identités et des données

Repose sur un modèle de gestion d'identités « User centric »

- Ex : OpenId / FranceConnect / SwitchEduId
- Maîtrise de ses données par l'utilisateur
- Apport de données complémentaires par l'institution (Idem POC Campus)



Mais ORCID :

- Ne repose pas sur un modèle de données très standardisé
- Réalise des transferts massifs de données hors UE
 - Données personnelles (cf. Safe Harbour / Privacy Shield)
 - Patrimoine scientifique

→ Tout transfert de données du SI de l'affiliation vers ORCID doit reposer sur :

- Une étude préalable avec le Cil de l'établissement
- La consultation du fonctionnaire de Défense
- Le consentement exprès et éclairé de l'utilisateur

Preuve de concept, et ensuite ?

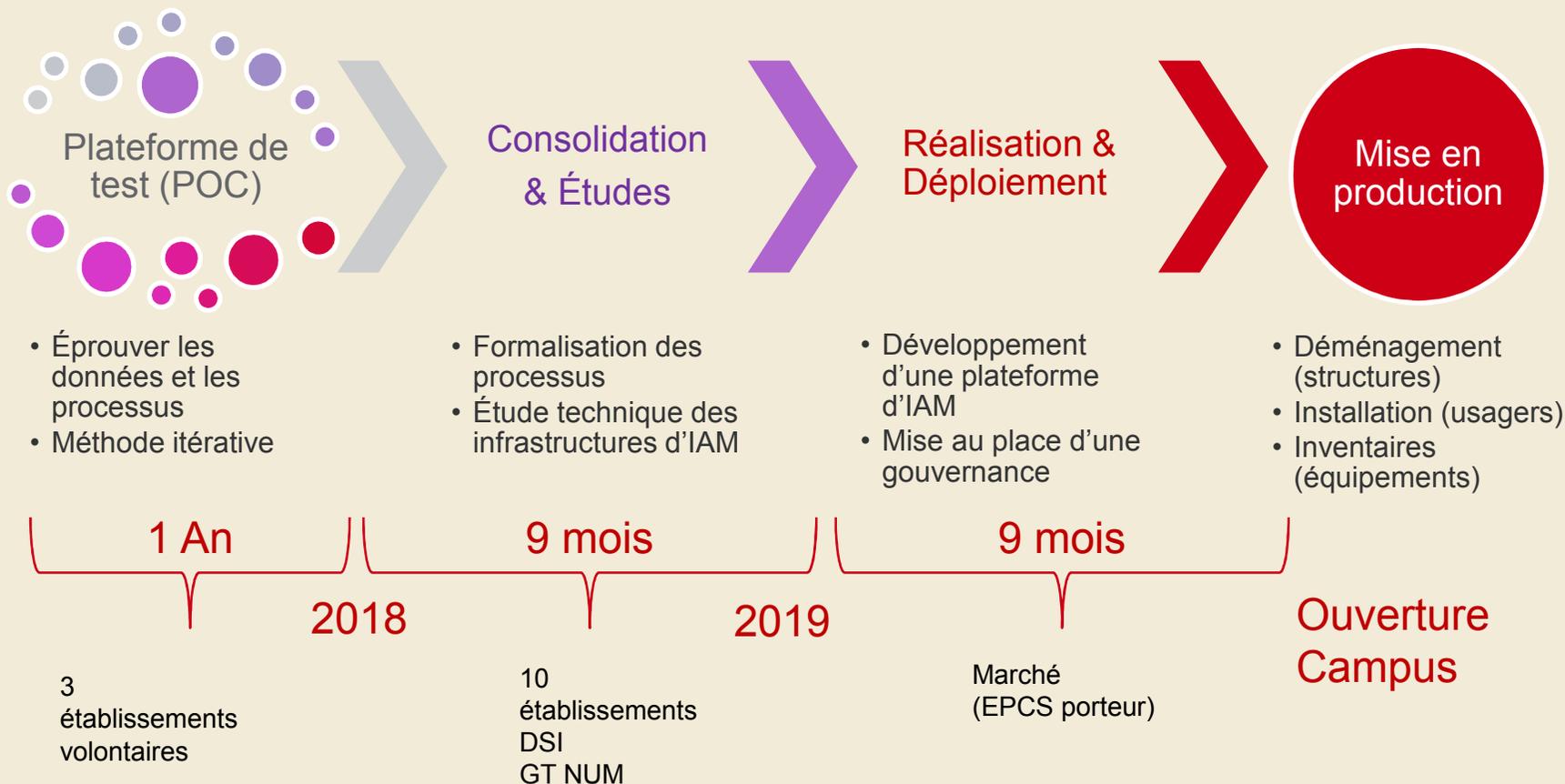


Schéma fonctionnel du processus d'inscription

Gestion des comptes invités

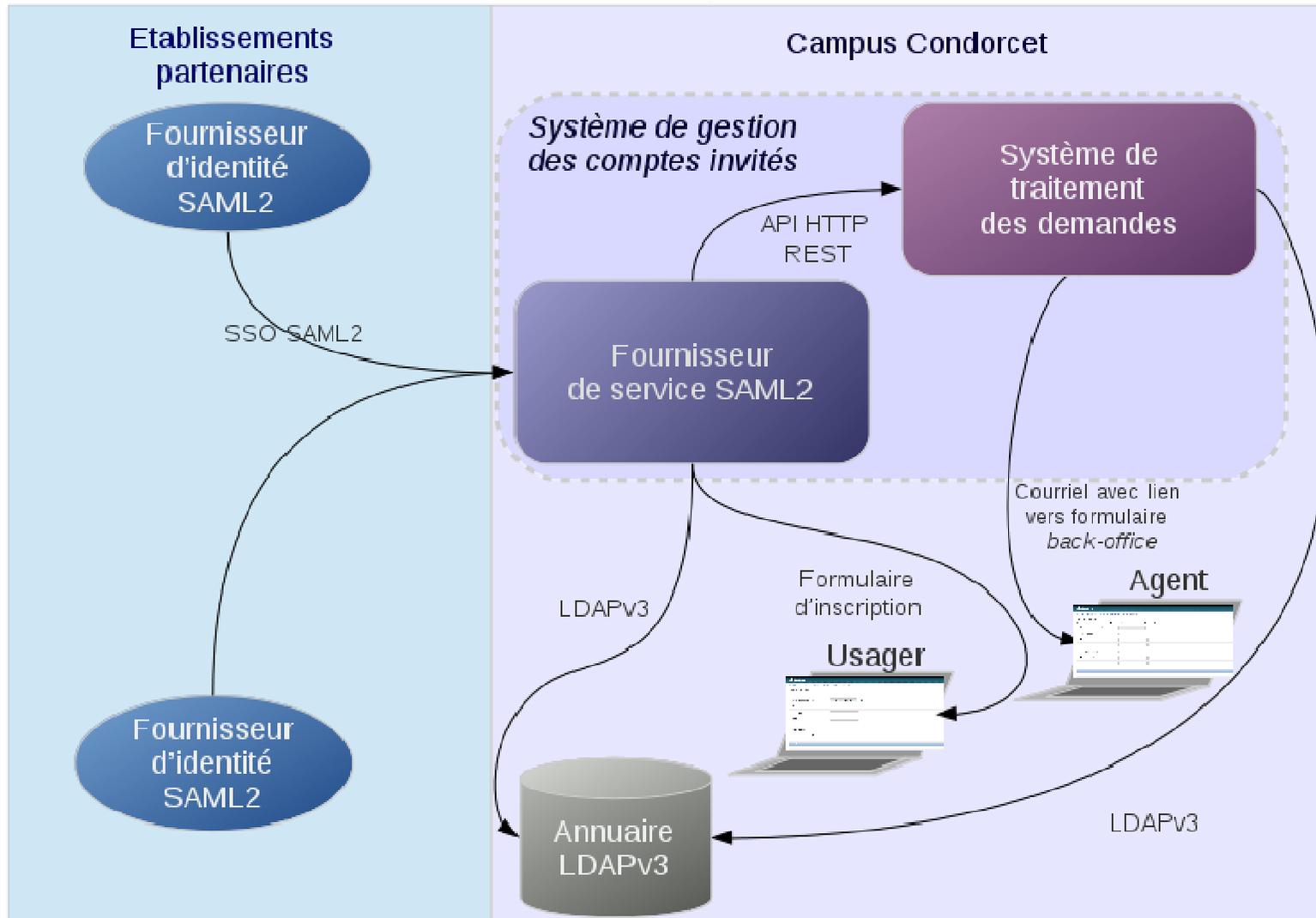
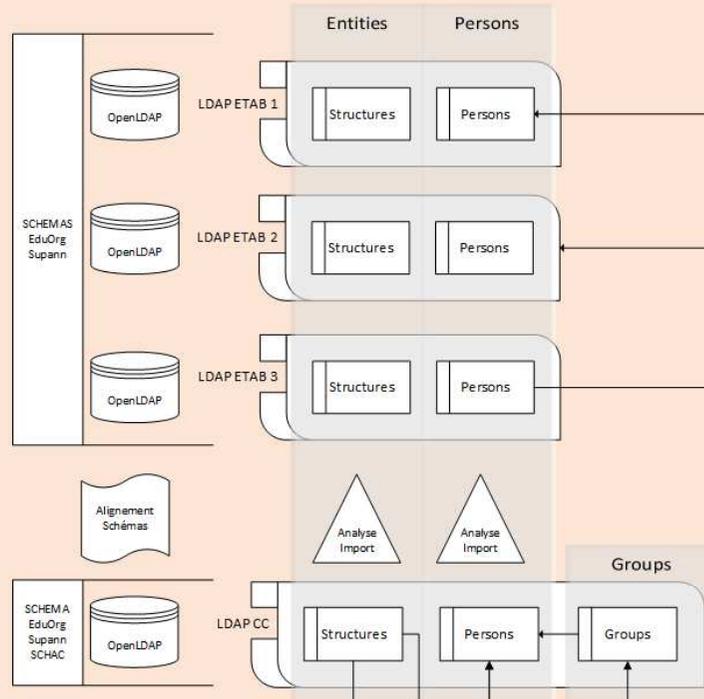
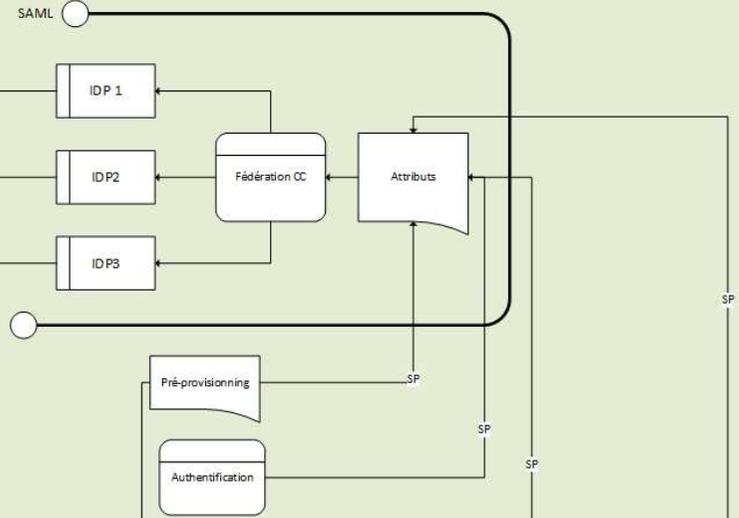


Schéma technique du référentiel d'identités Campus

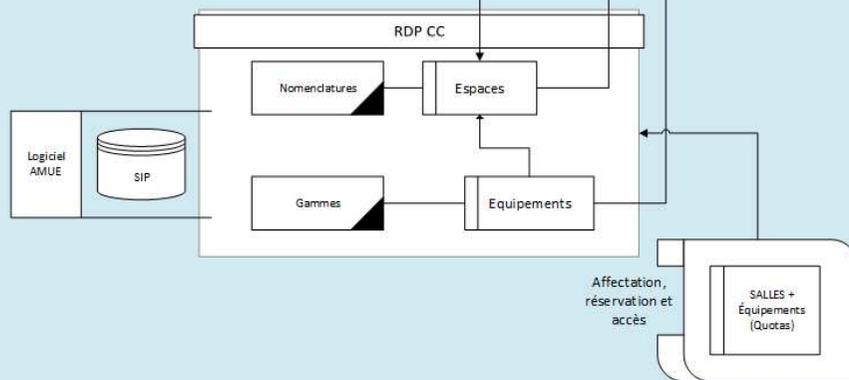
A. MODELE DE DONNEES



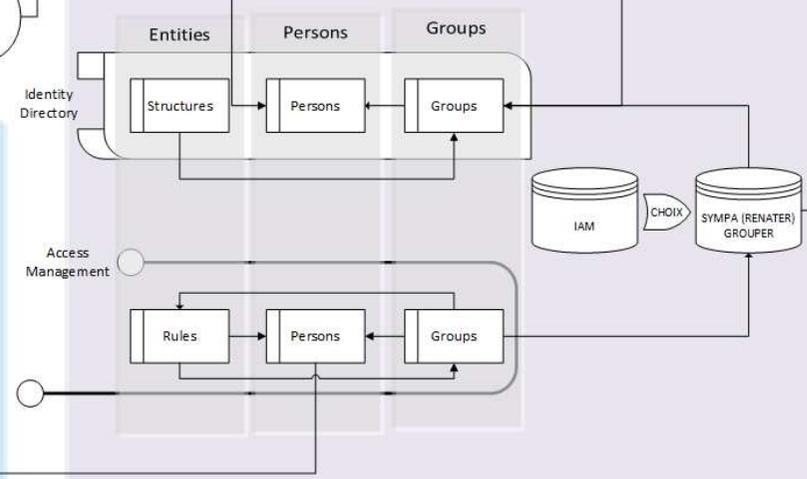
B. PROVISIONNEMENT



B. AFFECTATIONS DES ESPACES



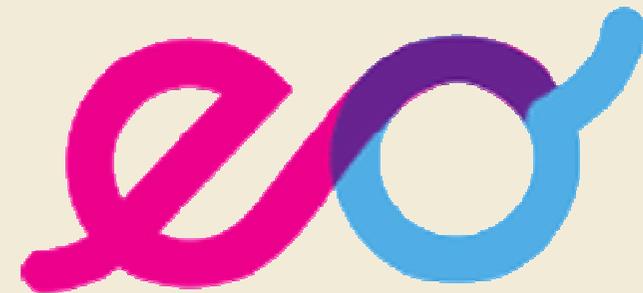
Gestion des identités et des accès



CAMPUS 
CONDORCET
Paris-Aubervilliers

<http://sp-condorcet.dev.entrouvert.org/>

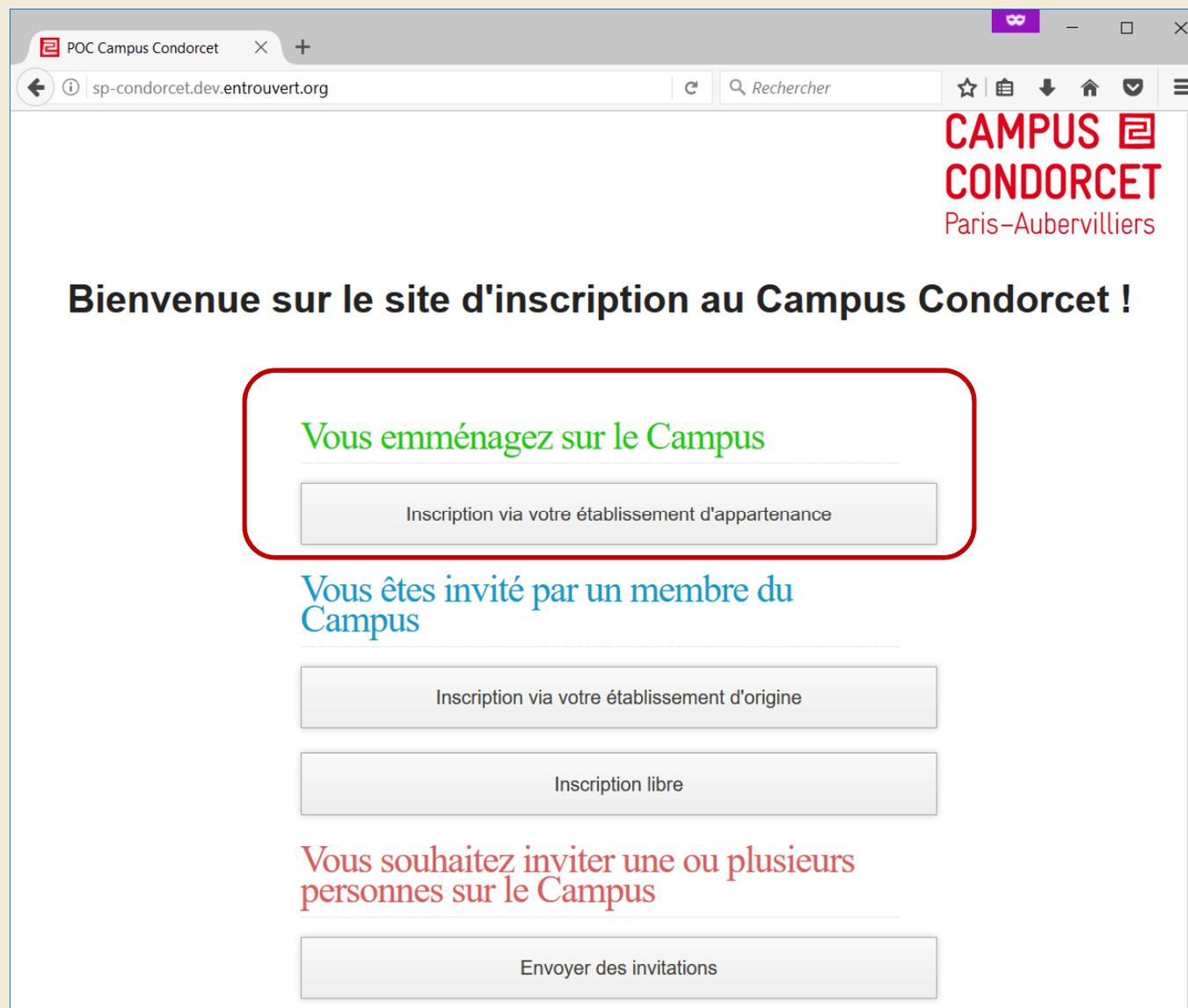
PROTOTYPE



entrouvert

INSCRIPTIONS

Inscription pour l'emménagement d'un usager



POC Campus Condorcet

sp-condorcet.dev.entrouvert.org

Rechercher

CAMPUS
CONDORCET
Paris-Aubervilliers

Bienvenue sur le site d'inscription au Campus Condorcet !

Vous emménagez sur le Campus

Inscription via votre établissement d'appartenance

Vous êtes invité par un membre du Campus

Inscription via votre établissement d'origine

Inscription libre

Vous souhaitez inviter une ou plusieurs personnes sur le Campus

Envoyer des invitations

Inscription pour l'emménagement d'un usager

Pour accéder au service Partages Campus Condorcet sélectionnez ou cherchez l'établissement auquel vous appartenez.

Veillez entrer le nom de votre établissement...

Veillez entrer le nom de votre établissement...

- CAMPUS CONDORCET
- CNRS
- Ecole Nationale des Chartes production
- EHESS**
- EPHE - Ecole Pratique des Hautes Etudes
- FMSH Fondation Maison des Sciences de l'Homme
- INED - Institut National d'Etudes Démographiques
- Université de Paris 3 - Sorbonne Nouvelle
- Université de Paris 8 - Vincennes
- Université Paris 1 Panthéon-Sorbonne
- Université Paris 13

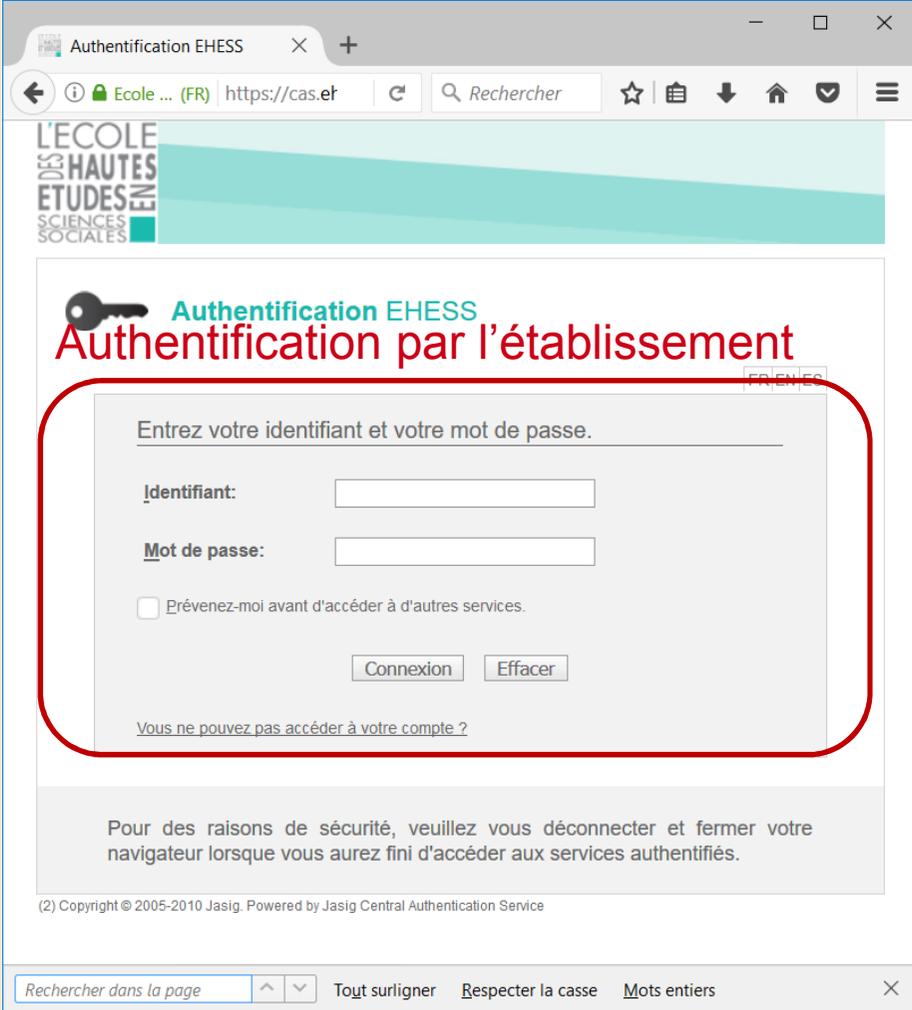
Connexion

Connexion en cours.

Connexion

Fédération Campus Condorcet (11 membres)

Inscription pour l'emménagement d'un usager



The screenshot shows a web browser window titled 'Authentication EHESS' with the URL 'https://cas.eh'. The page header includes the logo for 'L'ÉCOLE DES HAUTES ÉTUDES SCIENCES SOCIALES'. The main content area is titled 'Authentification EHESS' and 'Authentification par l'établissement'. A red rounded rectangle highlights the login form, which contains the following elements:

- Text: 'Entrez votre identifiant et votre mot de passe.'
- Label: 'Identifiant:' followed by a text input field.
- Label: 'Mot de passe:' followed by a text input field.
- Checkbox: 'Prévenez-moi avant d'accéder à d'autres services.'
- Buttons: 'Connexion' and 'Effacer'.
- Link: 'Vous ne pouvez pas accéder à votre compte ?'

Below the form, there is a security notice: 'Pour des raisons de sécurité, veuillez vous déconnecter et fermer votre navigateur lorsque vous aurez fini d'accéder aux services authentifiés.' At the bottom, there is a footer: '(2) Copyright © 2005-2010 Jasig. Powered by Jasig Central Authentication Service' and a search bar with options: 'Rechercher dans la page', 'Tout surligner', 'Respecter la casse', and 'Mots entiers'.

Si la personne change d'établissement

- Elle ne peut plus se connecter

Nous appliquons la politique des établissements

Inscription pour l'emménagement d'un usager

Vous souhaitez accéder à:
AAI Viewer Interfederation Test de switch.ch

Description du service:
This service is used to test the interederation readiness of SWITCHaaI Identity Providers.

[Informations supplémentaires concernant le service](#)

Informations transmises au service	
commonName	Auburtin Gautier
displayName	Gautier Auburtin
eduPersonAffiliation	member staff
eduPersonPrincipalName	gautier.auburtin@campus-condorcet.fr
eduPersonScopedAffiliation	staff@campus-condorcet.fr member@campus-condorcet.fr
email	gautier.auburtin@campus-condorcet.fr

[Données privé du service](#)

LES informations listées vont être transmises au service si vous souhaitez continuer.

Acceptez-vous d'envoyer ses informations au service à chaque connexion?

Selectionnez la durée de votre consentement:

- Me demander lors de la prochaine connexion
 - J'accepte d'envoyer mes informations pour cette fois.
- Me demander à nouveau si les informations envoyées changent
 - J'accepte que les informations soient automatiquement envoyées à la prochaine connexion.
- Ne plus me demander
 - J'accepte que **toutes** les informations soient transmises à **tous** les services.

Votre choix peut être modifié à partir de la page de connexion en cochant la case **vérifier les informations envoyées au service.**

Collecte
de données personnelles

- Visualisation des données transmises
- Consentement de la personne
- Mise à jour des données dans la durée

Inscription pour l'emménagement d'un usager

Attributs fournis non modifiables

- Nom
- Prénom
- Courriel
- Statut principale
- Établissement
- Affectation principale

Attributs fournis mais modifiables

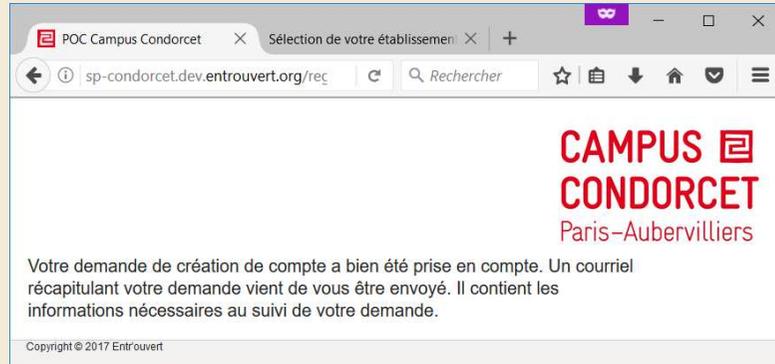
- Corps
- Liste rouge

Attributs normalisés

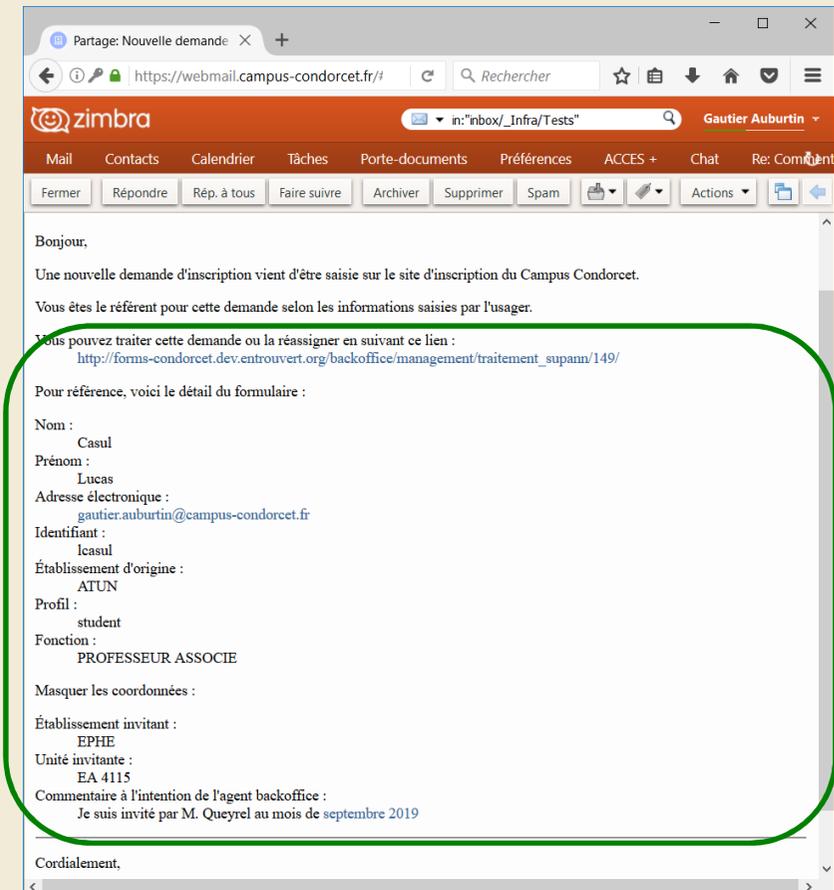
- EduPerson
- Supann

Valeurs fournies	Attributs SAML
Identifiant	eduPersonPrincipalName
Nom	surname
Prénom	givenName
Courriel	mail
Statut principal	eduPersonPrimaryAffiliation
Statuts	eduPersonAffiliation
Établissement	supannEtablissement
Affectation principale	supannEntiteAffectationPrincipale
Affectations	supannEntiteAffectation
Corps	supannEmpCorps
Liste rouge	supannListeRouge

Inscription pour l'emménagement d'un usager



Notification de l'utilisateur



Envoi pour validation au référent

Conditions

Si Structure → Réf. Structure

↙ Sinon → Réf. établissement

↙ Sinon → Réf. par défaut

→ Récapitulatif de la demande

→ Lien direct vers le formulaire

Inscription pour l'emménagement d'un usager

Backoffice de wcs - Inscription c X +
forms-condorcet.dev.entrouvert.org/back

Traitement Inscription des invités (par i référent_default déconnexion)

Résumé

Nom
Casul

Prénom
Lucas

Adresse électronique
gautier.auburtin@campus-condorcet.fr

Identifiant
lcasul

Établissement d'origine
ATUN

Profil
student

Fonction
PROFESSEUR ASSOCIE

Masquer les coordonnées

Établissement invitant
EPHE

Unité invitante
EA 4115

Commentaire à l'intention de l'agent backoffice
Je suis invité par M. Queyrel au mois de septembre 2019

Statut
Demande reçue

Informations générales

Le formulaire a été enregistré le 01/07/2017 13:26 avec le numéro 3-149.

Statut : Demande reçue

Backoffice de wcs - Inscription c X +
forms-condorcet.dev.entrouvert.org/back

Assignment Établissement 01/07/2017 13:26

Assignment Unité 01/07/2017 13:26

Demande reçue 01/07/2017 13:26

Informations générales

Le formulaire a été enregistré le 01/07/2017 13:26 avec le numéro 3-149.

Statut : Demande reçue

Commentaire

Bonjour, je confirme votre inscription au Campus. Votre bureau est le A1-001-124, dans le Bâtiment Recherche 1 qui longe le cours des humanités. Veuillez prendre possession de votre badge d'accès au PC sécurité dans le Bâtiment EPCC.

Cordialement

Ajouter le commentaire Vérifier et valider Réassigner

Validation

Réassignation

Vérifier, éditer si nécessaire, puis valider les données saisies par l'usager.

Vous serez ensuite invité à modifier l'établissement ou l'unité ce qui entraînera une réassignation de la demande.

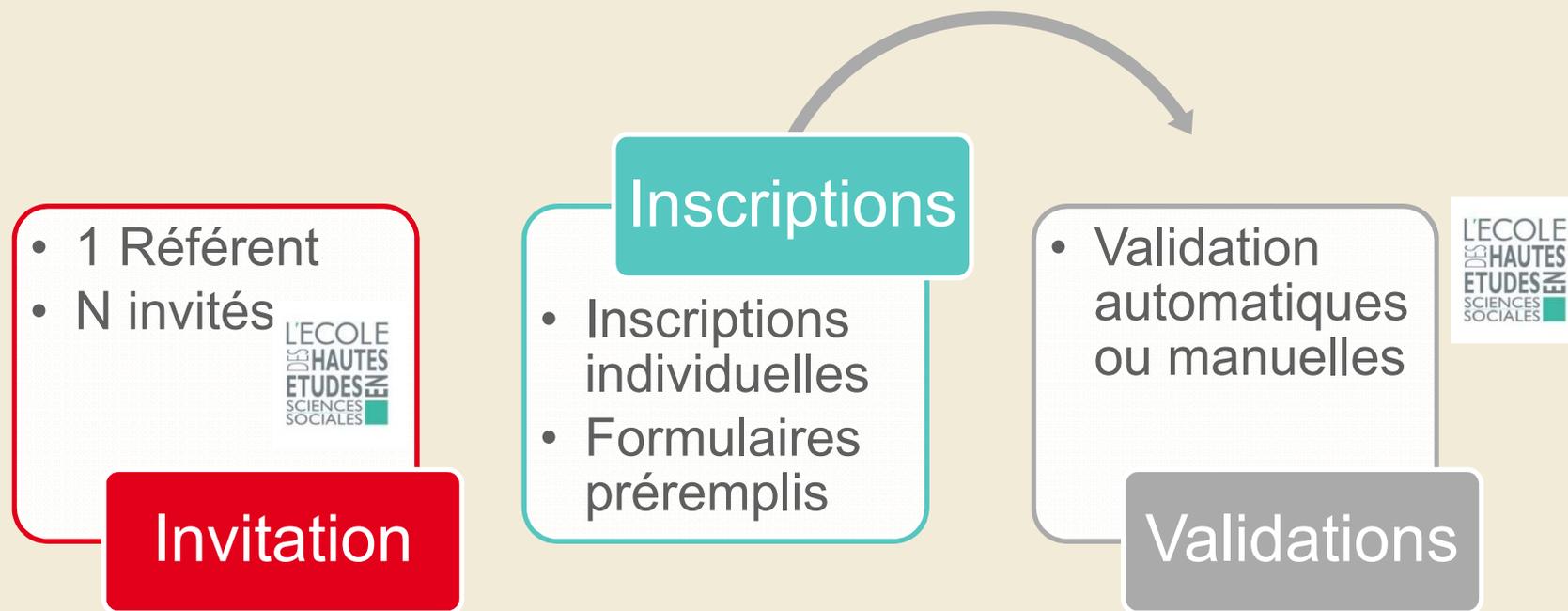
Retour au listing

Traitement de la demande

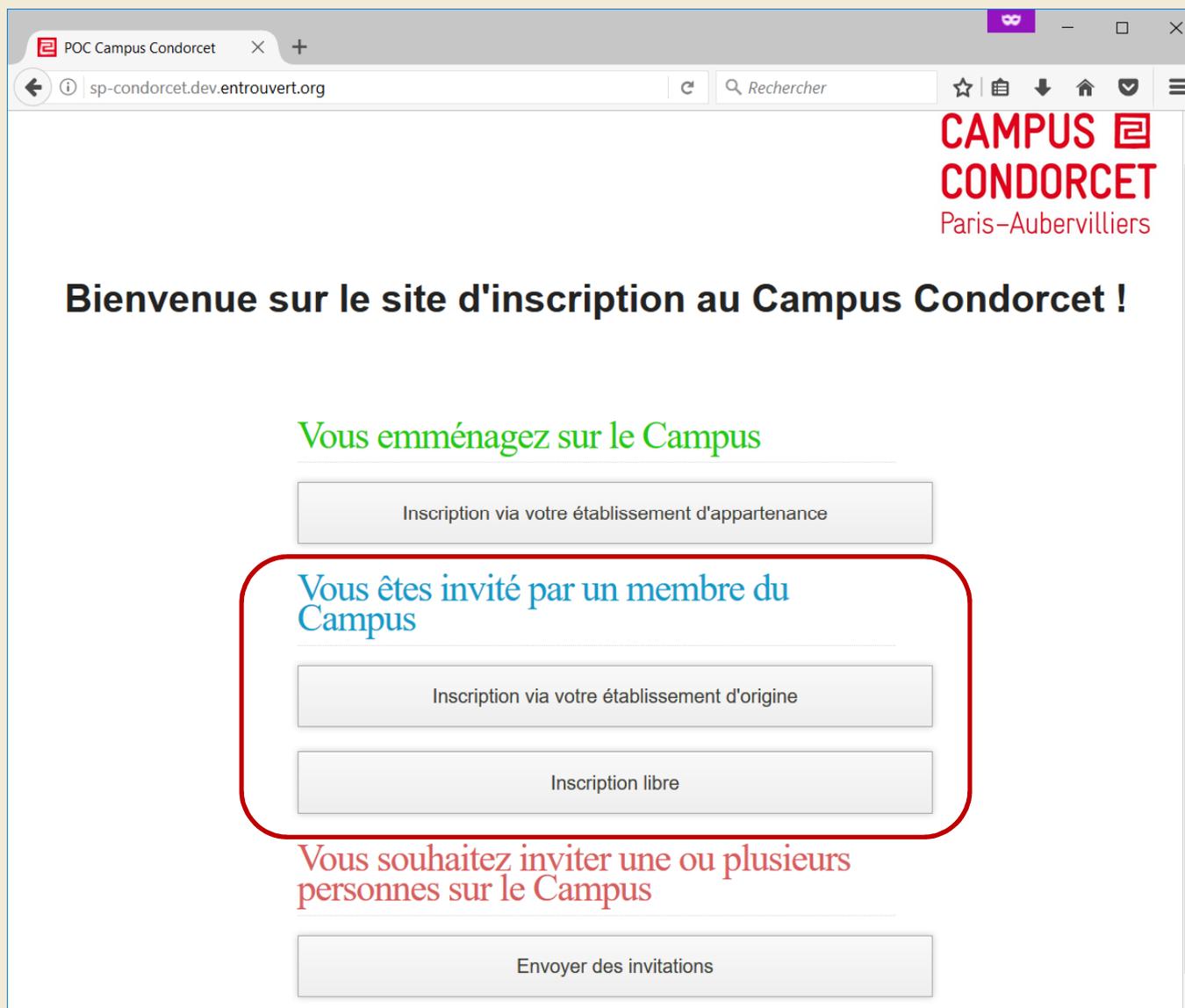
- Commentaire
- Informations complètes → Validation
- Sinon :
 - ↳ Réassignation vers un autre référent

INVITATIONS

Modèle d'invitation proposé



Invitation d'une ou plusieurs personnes



The screenshot shows a web browser window with the URL `sp-condorcet.dev.entrouvert.org`. The page header includes the logo for **CAMPUS CONDORCET Paris-Aubervilliers**. The main heading reads **Bienvenue sur le site d'inscription au Campus Condorcet !**. Below this, there are three main sections:

- Vous emménagez sur le Campus** (in green text), with a button for "Inscription via votre établissement d'appartenance".
- Vous êtes invité par un membre du Campus** (in blue text), which is highlighted with a red rounded rectangle. It contains two buttons: "Inscription via votre établissement d'origine" and "Inscription libre".
- Vous souhaitez inviter une ou plusieurs personnes sur le Campus** (in red text), with a button for "Envoyer des invitations".

Inscription d'une personne invitée

POC Campus Condorcet

sp-condorcet.dev.entrou

Rechercher

Adresse(s) électronique(s) destinataire(s) de l'invitation : *

gautier.auburtin@gmail.com

Si plusieurs adresses, veuillez laisser un espace entre elles

Message d'invitation :

Bonjour,
Veuillez vous inscrire sur le site du Campus Condorcet

Votre identifiant RENATER : *

invitant1

Votre adresse électronique : *

gautier.auburtin@campus-condorcet.fr

Votre nom : *

invitant1

Votre prénom : *

invitant1

Votre établissement : *

ATUN

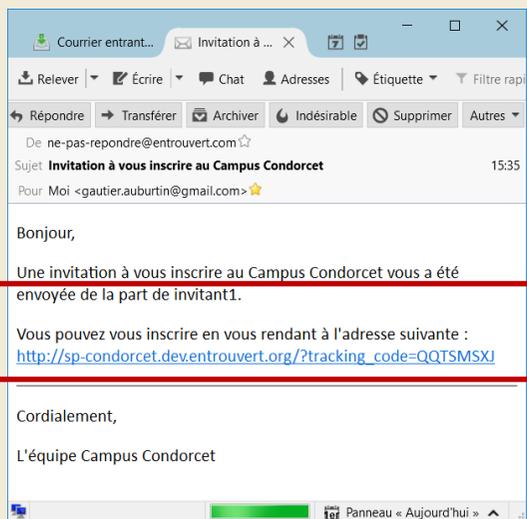
Envoi d'une invitation

- Adresses des invités
- Message libre

Information de contexte

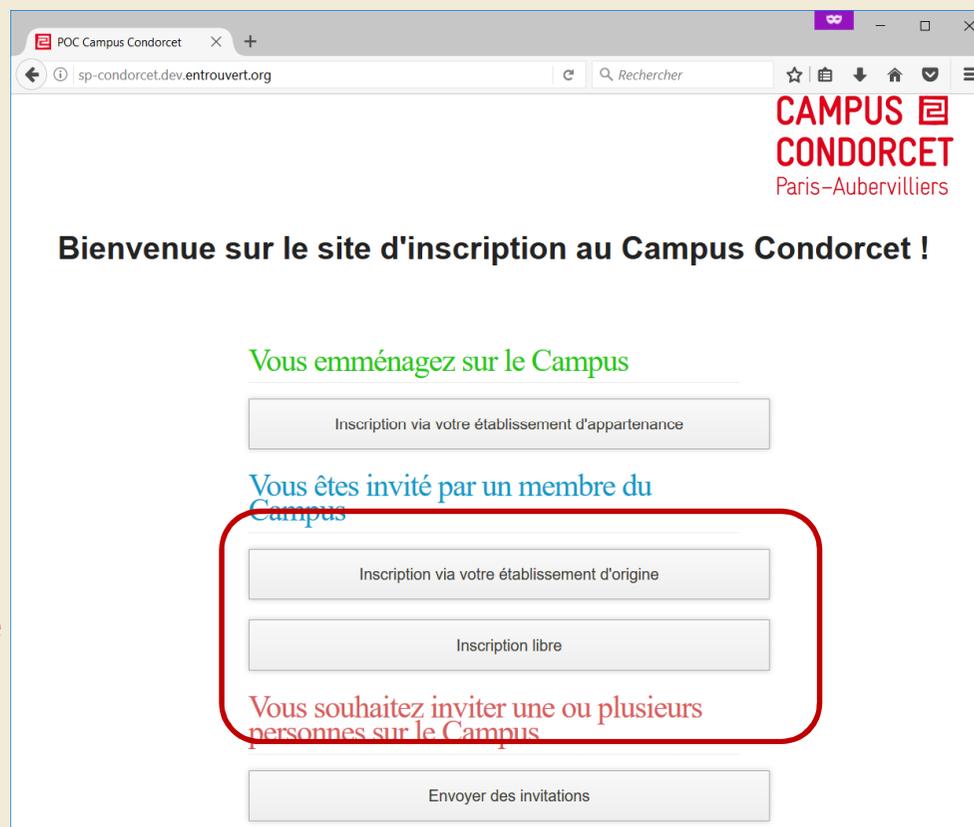
- L'affiliation de l'invitant détermine la structure invitante
- Le processus est automatisé (validation optionnelle)

Inscription suite à une invitation

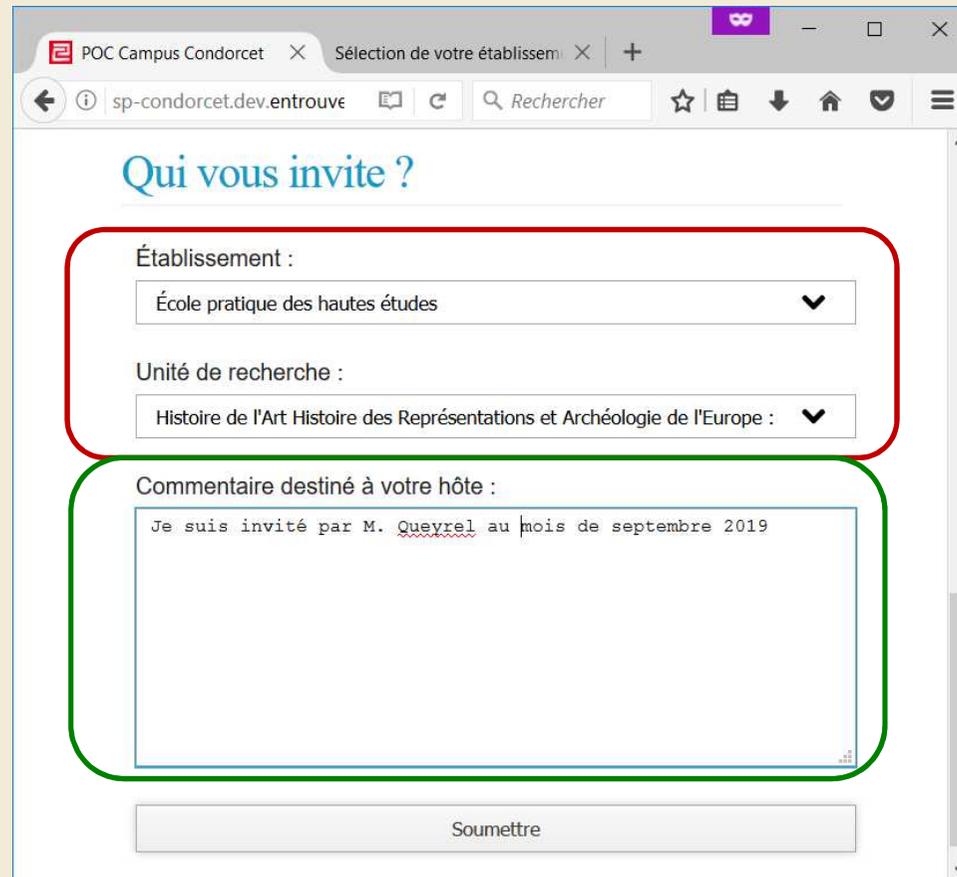


L'invité se connecte :

- Via son établissement d'origine
- attributs
- En saisie libre



Inscription suite à une invitation



The screenshot shows a web browser window with the URL 'sp-condorcet.dev.entrouve'. The page title is 'Qui vous invite ?'. There are two dropdown menus: 'Établissement : École pratique des hautes études' and 'Unité de recherche : Histoire de l'Art Histoire des Représentations et Archéologie de l'Europe :'. Below these is a text area for 'Commentaire destiné à votre hôte :' containing the text 'Je suis invité par M. Queyrel au mois de septembre 2019'. A 'Soumettre' button is at the bottom.

Structure invitante déjà renseignée

- Établissement
- Unité de recherche

→ Détermine la personne devant valider l'inscription (invitant / référent)

Message de contexte

→ Rend possible une réaffectation vers un autre référent