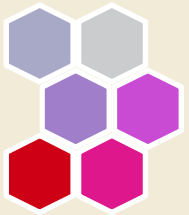
CAMPUS CONDORCET Paris–Aubervilliers
Cité des humanités et des sciences sociales

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

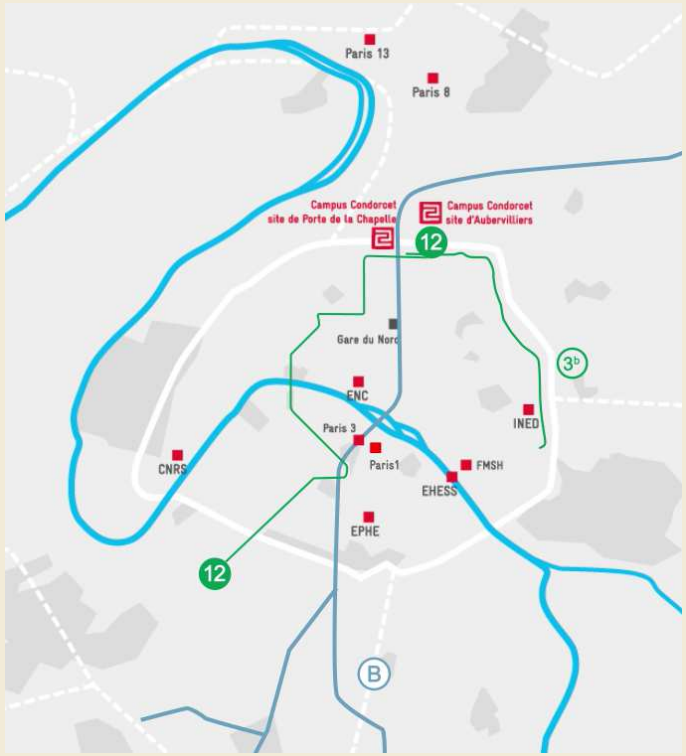
- Objectifs d'un référentiel / Vie de Campus
- Scénarios motivant une preuve de concept (POC)
- Standards de gestion des identités dans l'ESR
- Protection des données personnelles (CNIL / CIL)
- Gouvernance en lien avec les établissements fondateurs
- Choix d'un modèle orienté utilisateur

Élargissement aux identifiants de la recherche

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

Présentation du Campus Condorcet

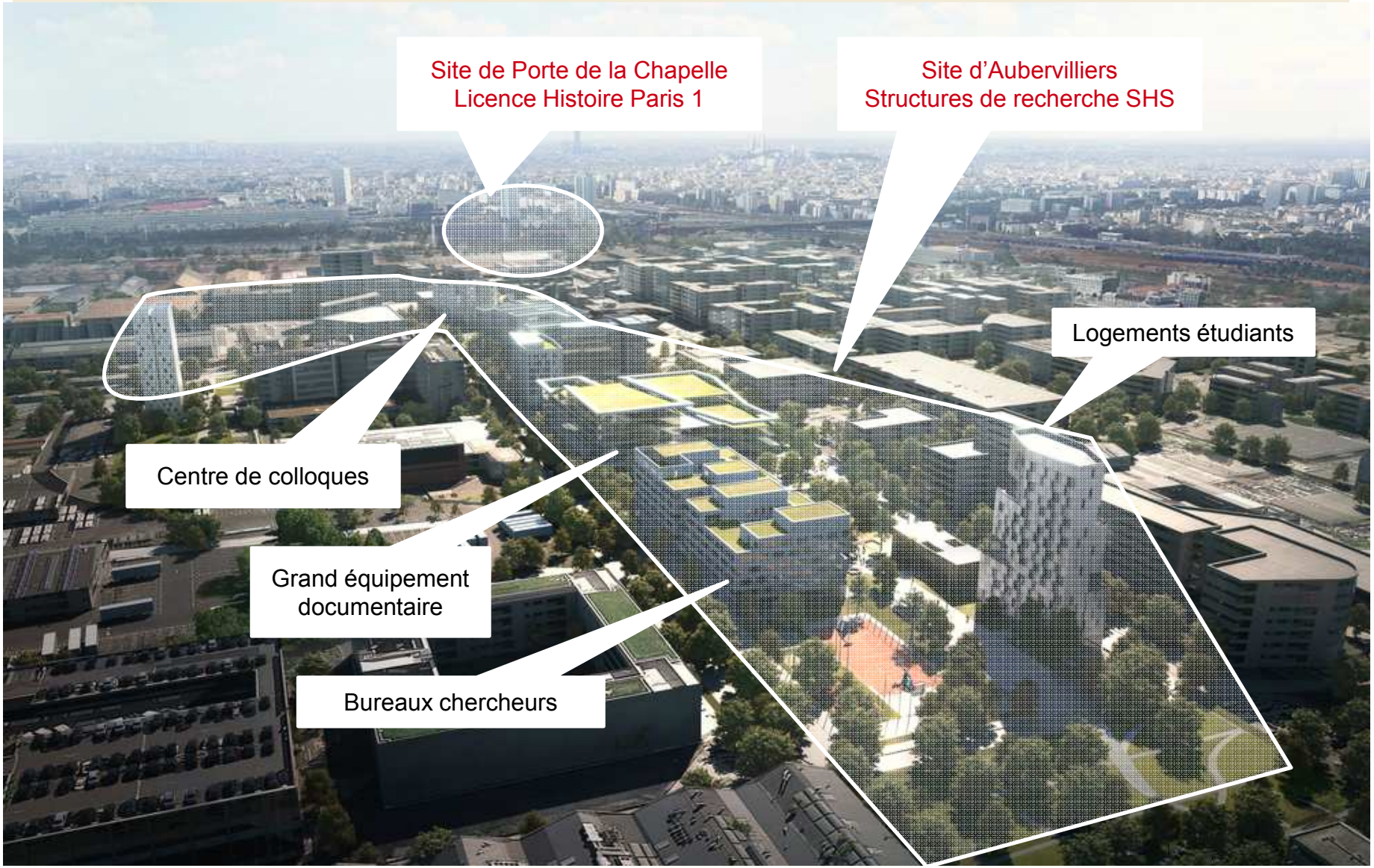
10 fondateurs unis pour un projet commun



- 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

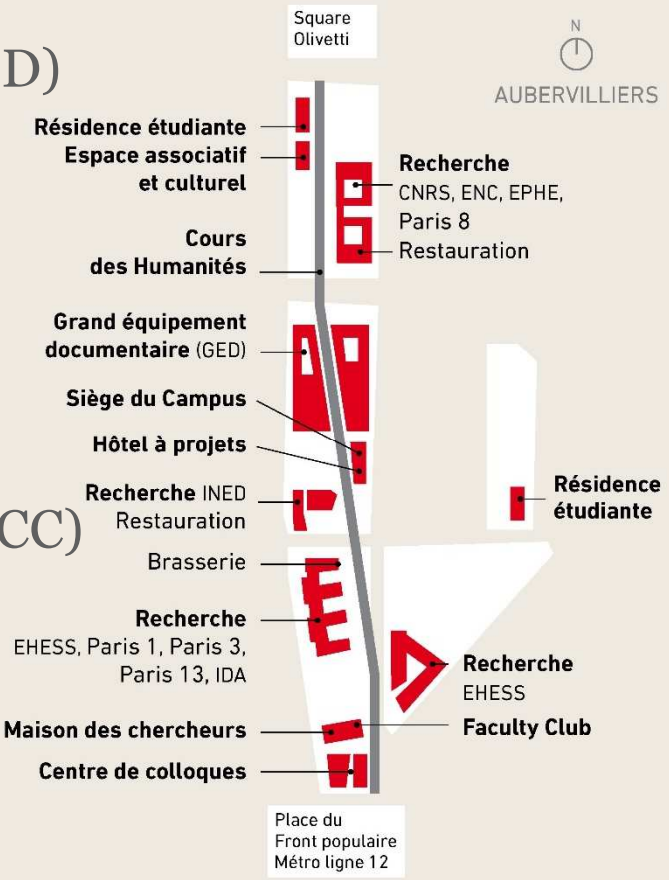


Organisation fonctionnelle du Campus

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

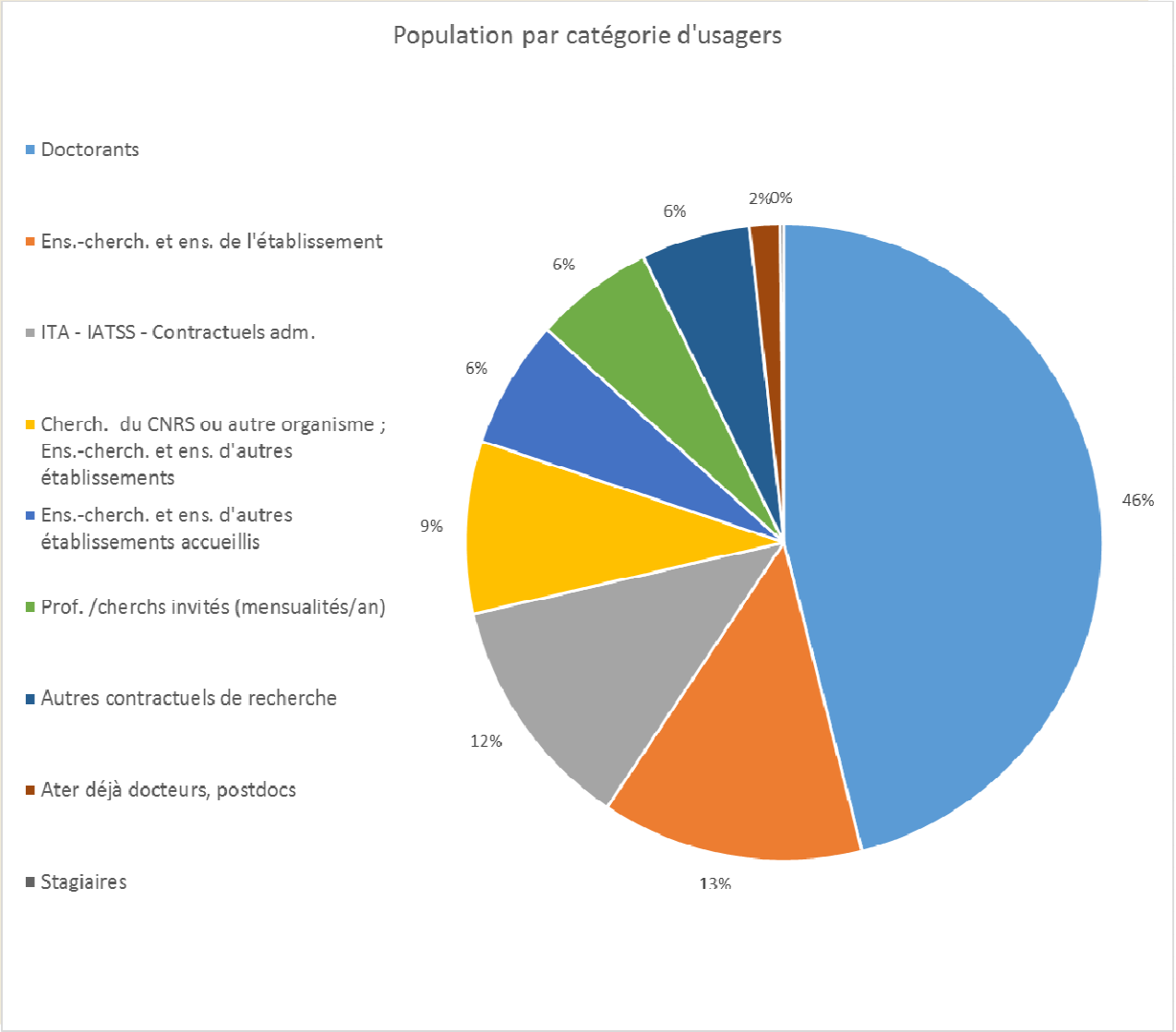
6 000 usagers (potentiel 15 000)

Profils

[projection 2013]

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

- 12% ITA
- 6% Contractuels



Services potentiels pour les données

Grand équipement documentaire

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

Grand équipement documentaire (E. de Prozamparc)

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)
- .....

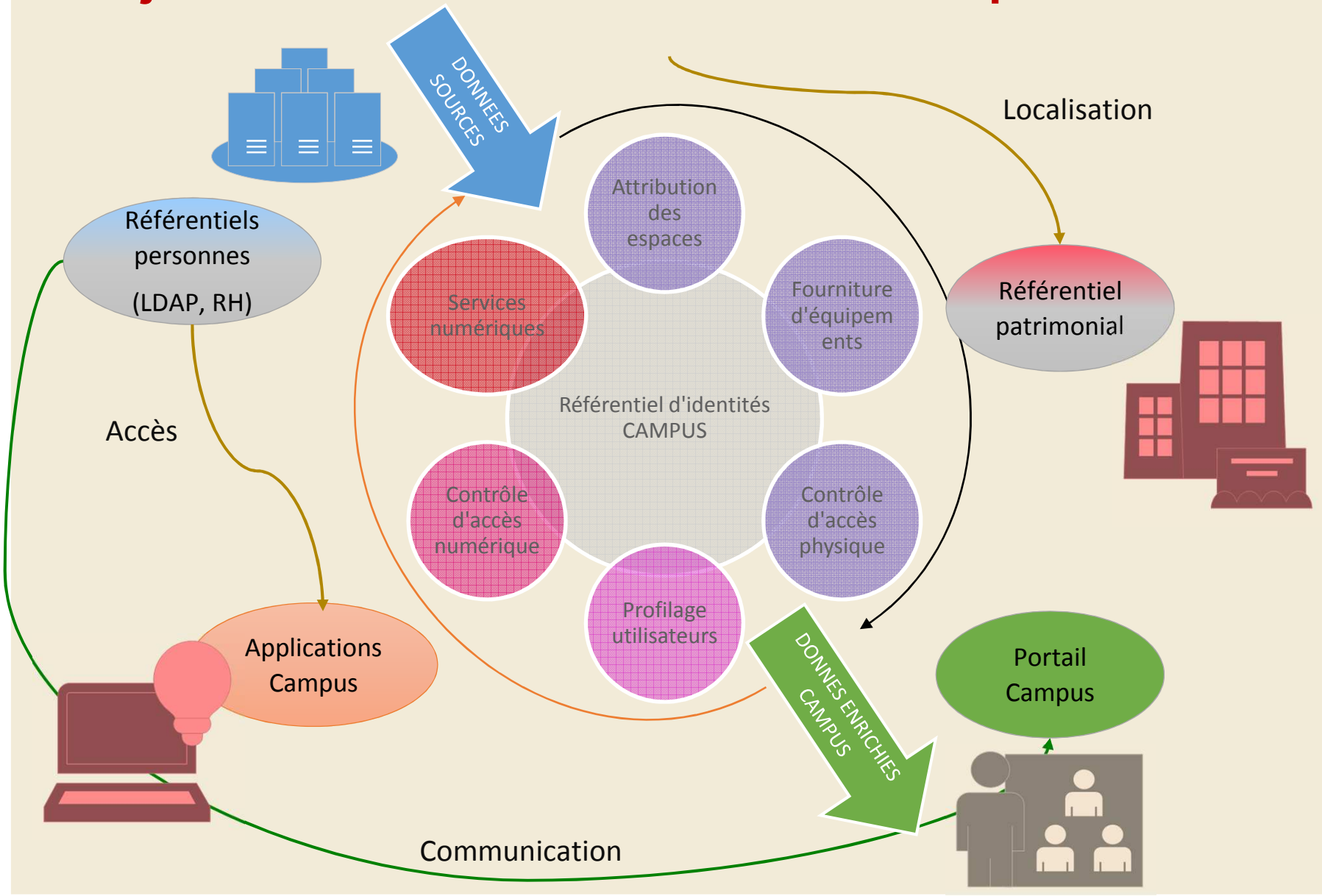
Huma-Num
la TGIR des humanités numériques

Projets soutenus

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

CAMPUS CONDORCET
Paris-Aubervilliers

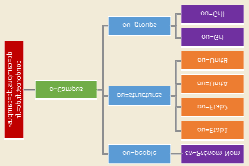
Objectifs du référentiel d'identités Campus



Scénarios pour une preuve de concept (POC)

Annuaire LDAP* multi-établissements ;

- Définition d'un modèle de données
- Recommandations d'alignement

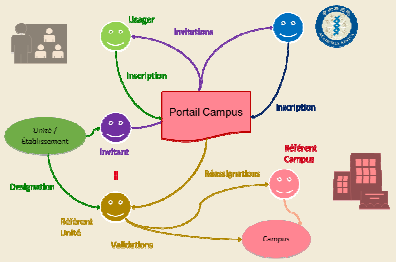


Processus d'approvisionnement automatique (déménagement)

- Import de données depuis les LDAP
- Synchronisation des données sur événements

Processus d'approvisionnement manuel (chercheur invité)

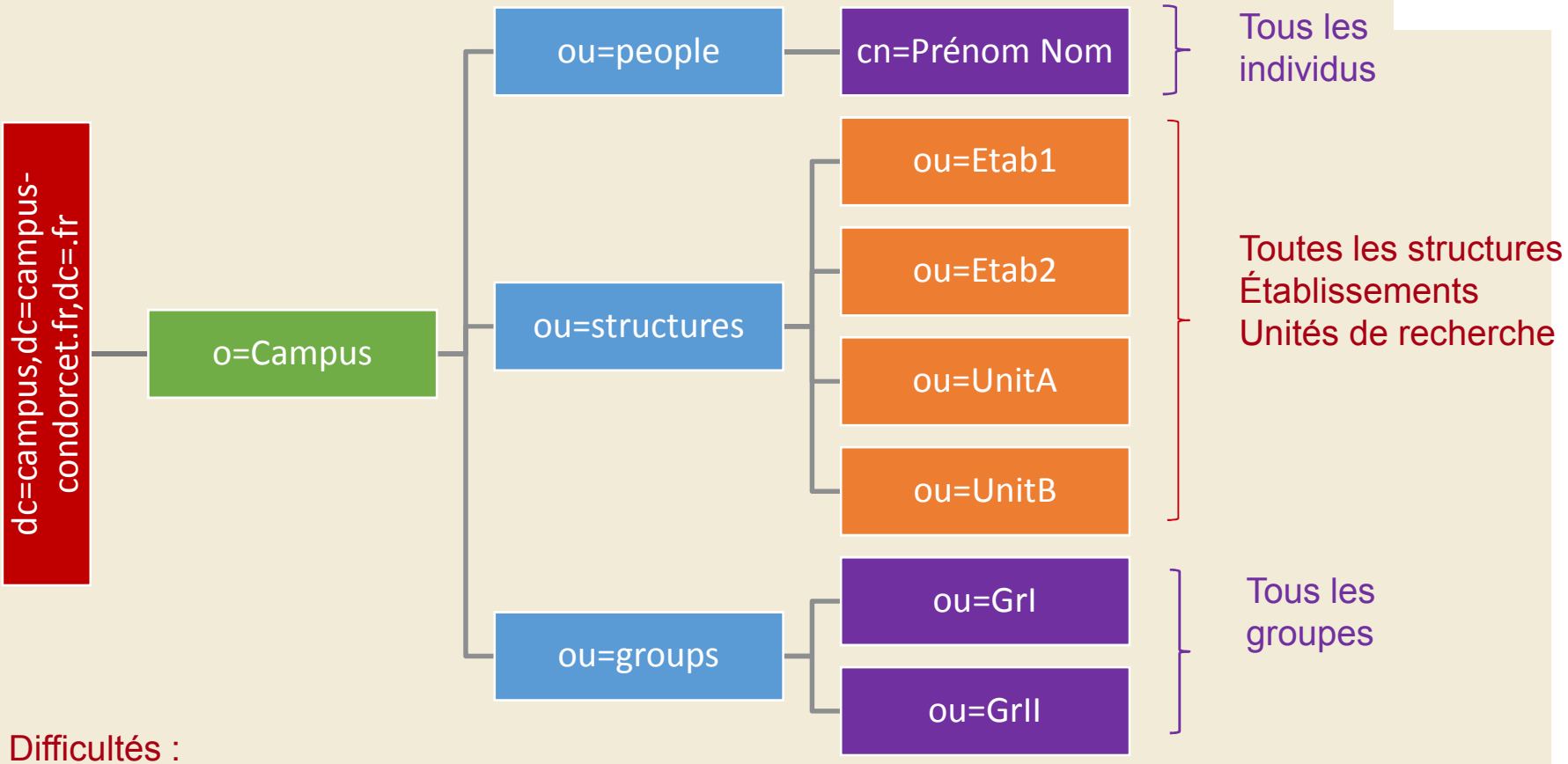
- Fédération d'identités (Renater / Campus Condorcet)
- Collecte d'attributs à la volée (SAML via IDP)
- Enrichissement des données par formulaire libre
- Workflow de validation (référents / structures)



*LDAP = LightWeight Directory Access Protocol (IETF / RFC)

Schéma type d'un annuaire LDAP

LDAP
Lightweight Directory Access Protocol



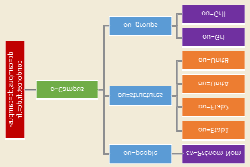
Difficultés :

- 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

Description LDAP d'un individu

Schémas d'attributs disponibles (classes)

- inetOrgPerson (IETF – RFC*)
- eduPerson (Internet 2)
- supannPerson (Renater)
- + Classes et attributs / Structures (organizationalUnit, supannEntite)



+ Nomenclatures applicables à eduPerson + supannPerson

Grande variabilité d'usage dans les établissements

- Codifications locales (structures, APOGEE)
- Complexité des données (attributs composites, Cf. profil étudiant)
- Extrême complexité des alignements / synchronisations (hors fusion type COMUE)

Pouvait-on espérer y arriver à 10 + 1 ? ;-)

* IETF – RFC = Internet Engineering Task Force - Request for Comments

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	prenom.nom@domaine.fr
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

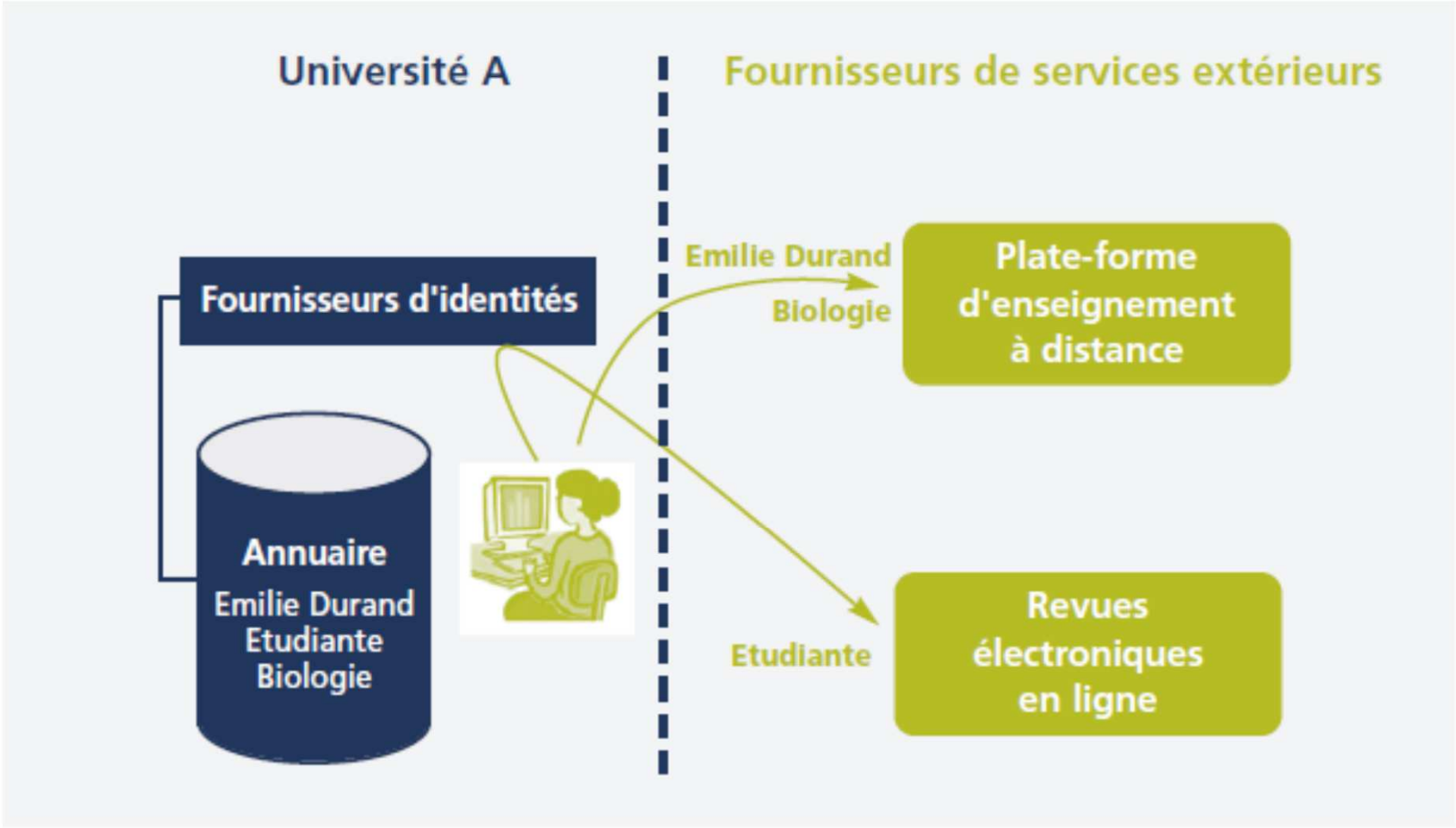
- Niveaux de confiance entre :
  - Fournisseurs d'identités (Identity Provider, IDP)
  - Fournisseurs de services (Service Provider, SP)
  - Fournisseurs de données (Data Provider, DP) pour France Connect
- Protocole d'appui :
  - Schémas de métadonnées
  - Authentification sécurisé en mode Web
  - SAML (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

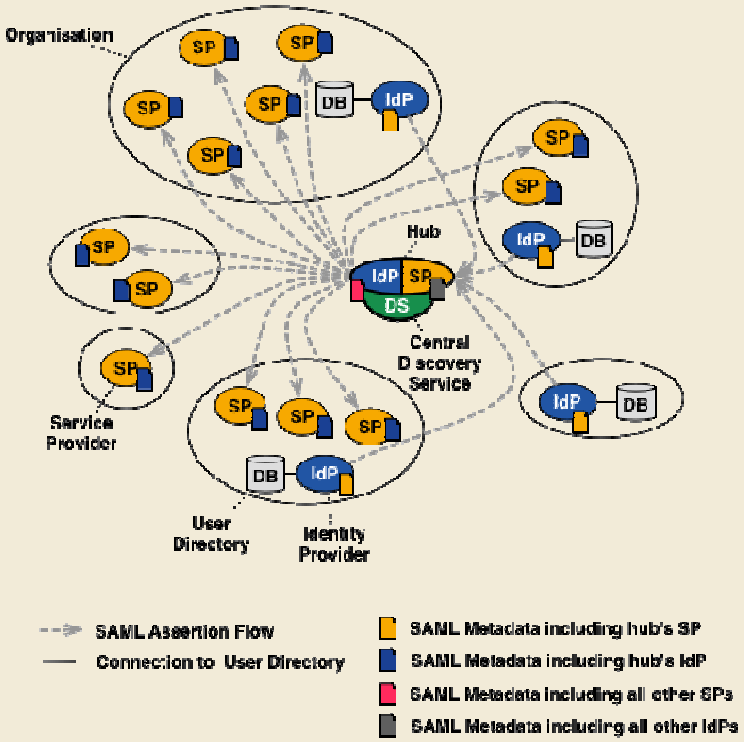


Modèles de fédérations

Hub and Spoke

Hub-and-Spoke Federation with Distributed Login

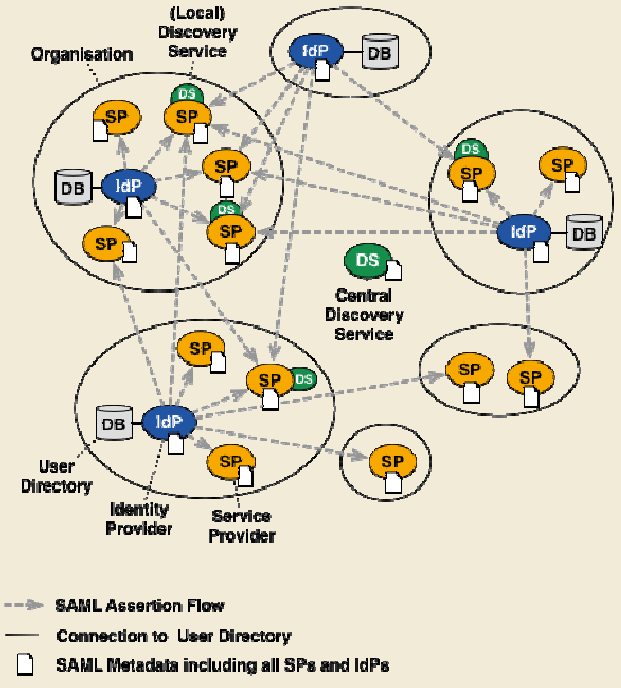
~15% of all NREN Federations (June 2013)
SURFconext, WAYF.dk, SIR, TAAT, Confia



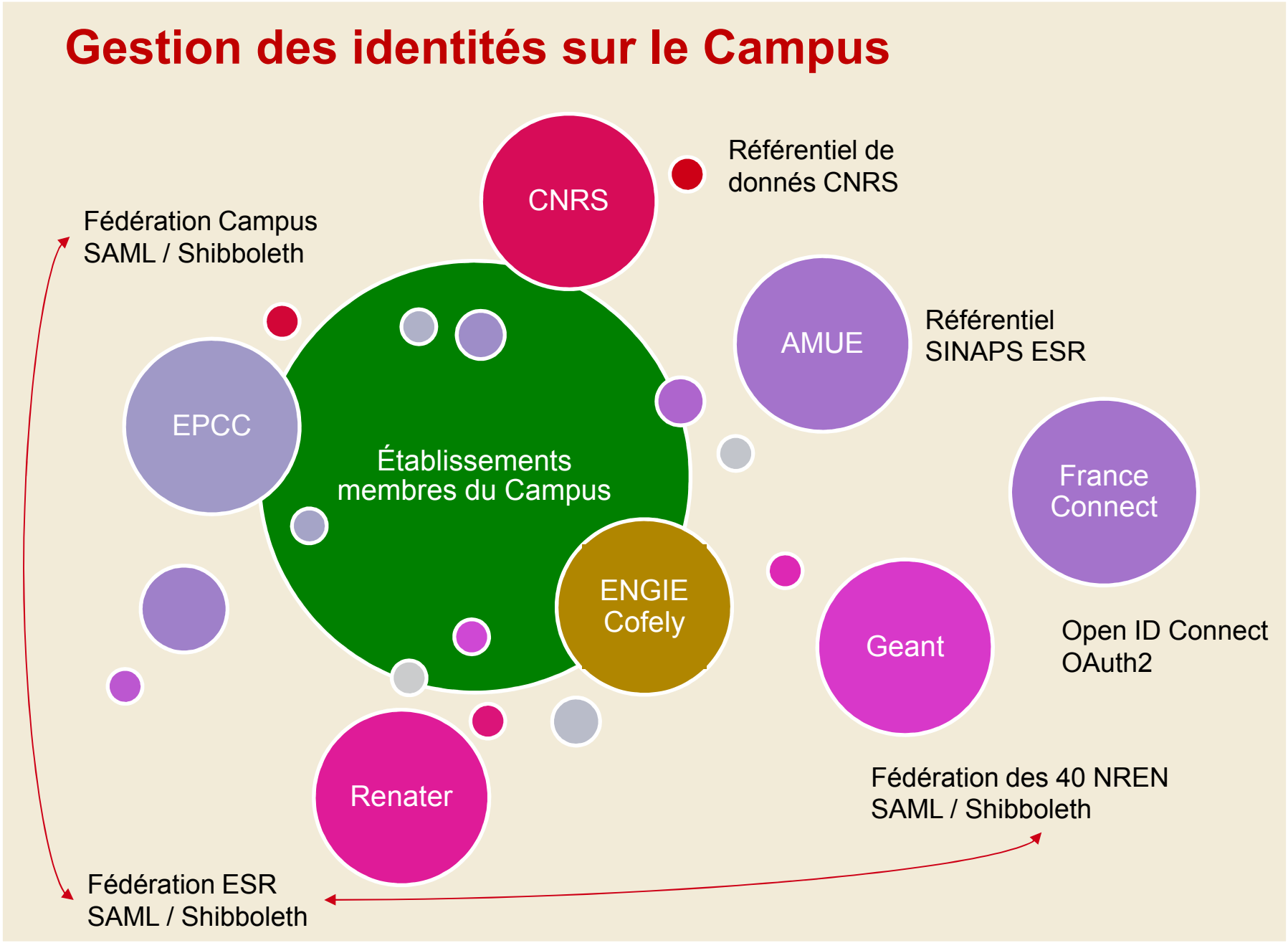
Mesh (point à point)

Full Mesh Federation

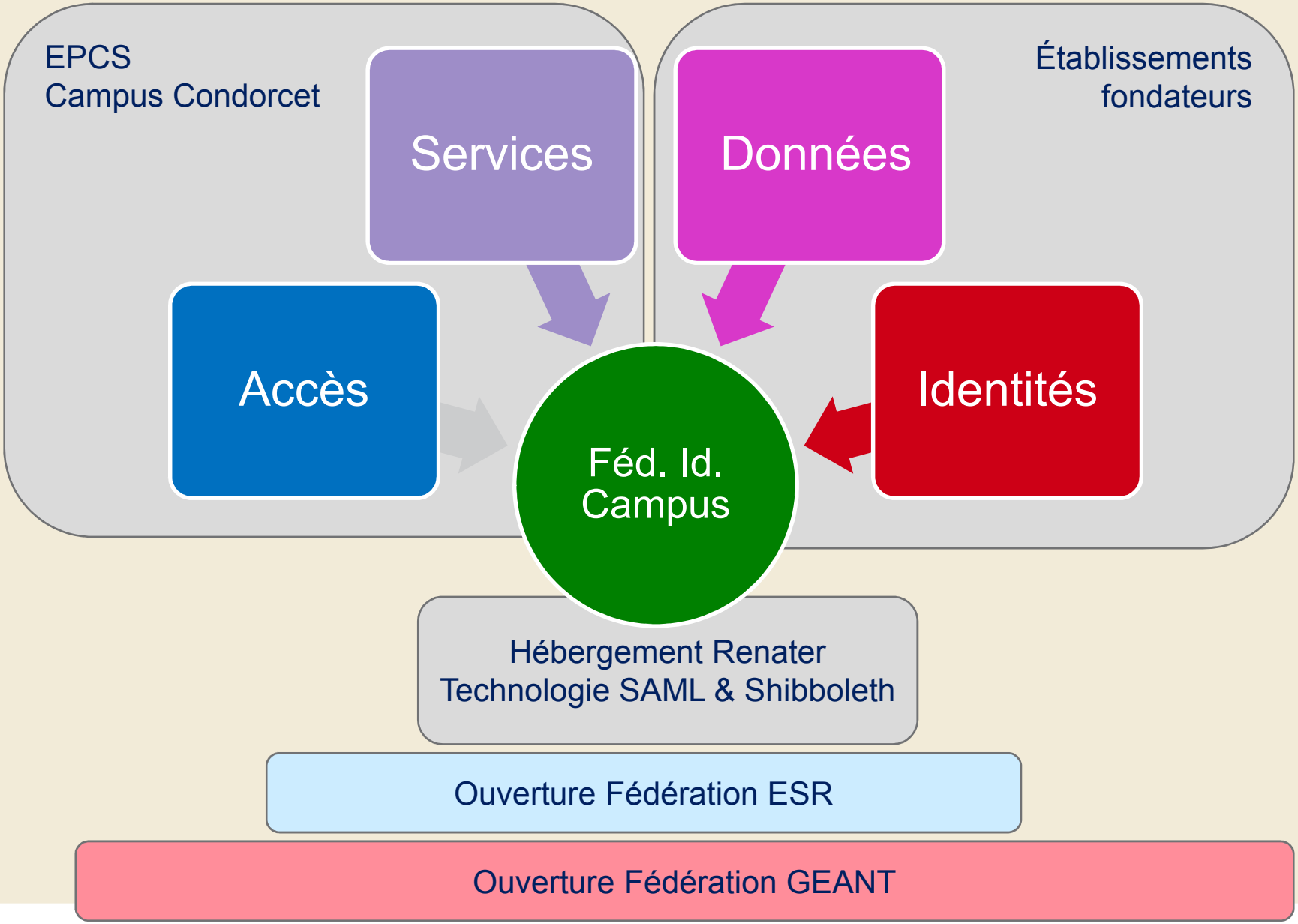
~80% of all NREN Federations (June 2013)
E.g InCommon, UKAMF, SWITCHaai, SWAMID, HAKA, AAF



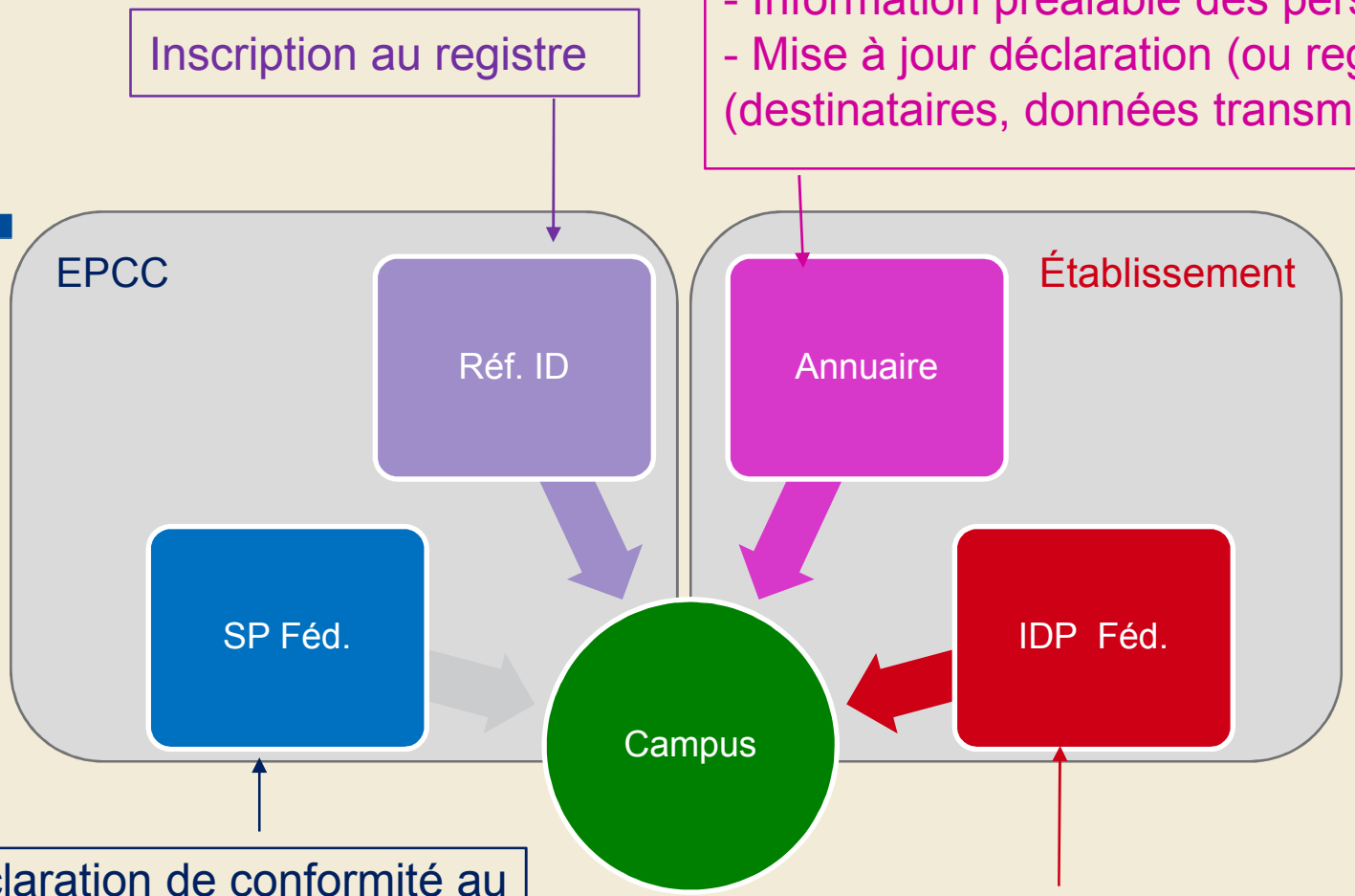
Gestion des identités sur le Campus



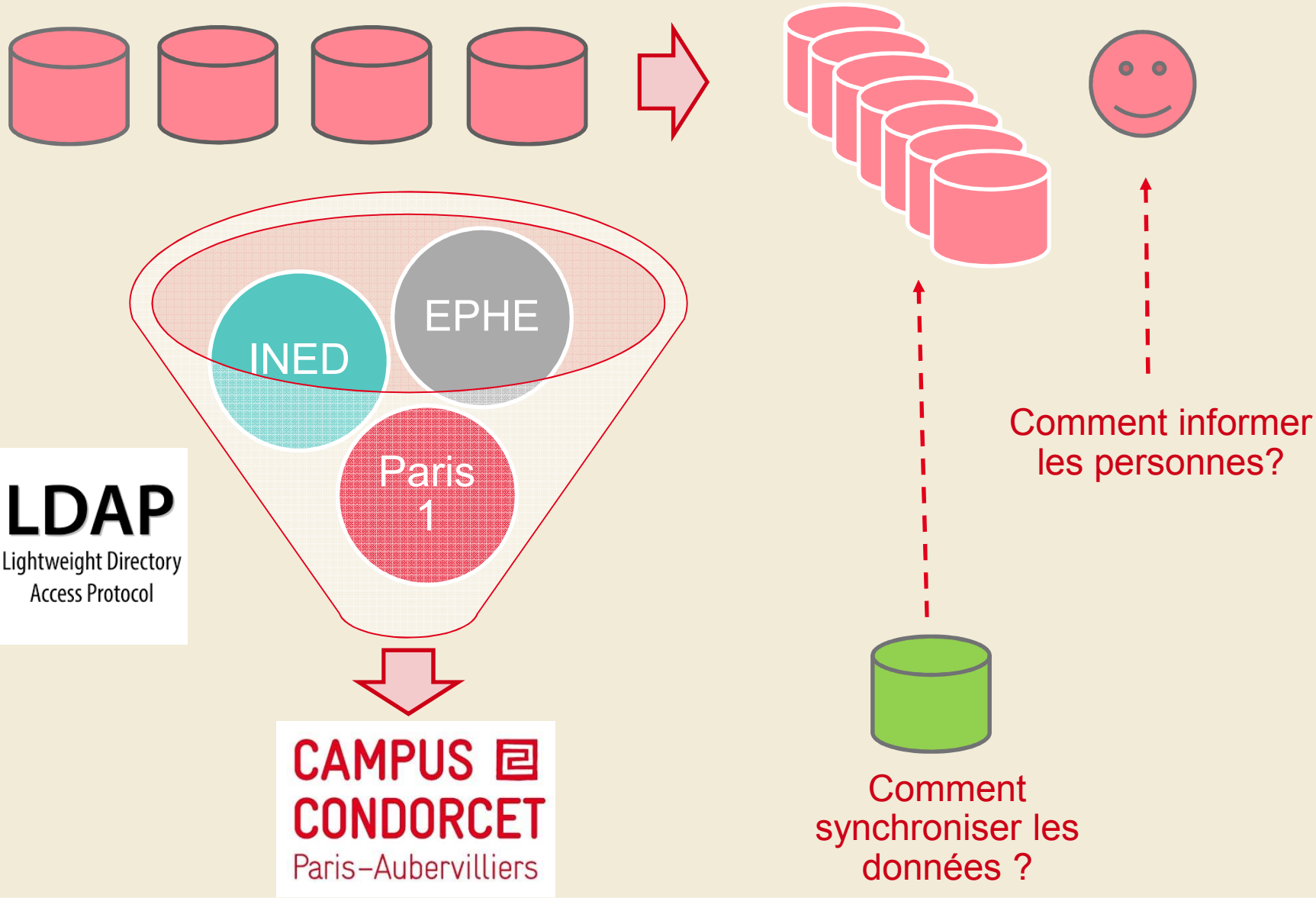
Fédération d'identités du Campus Condorcet



Formalités à accomplir / transferts de données



Modèle d'approvisionnement « classique »



Obstacles au transfert de données

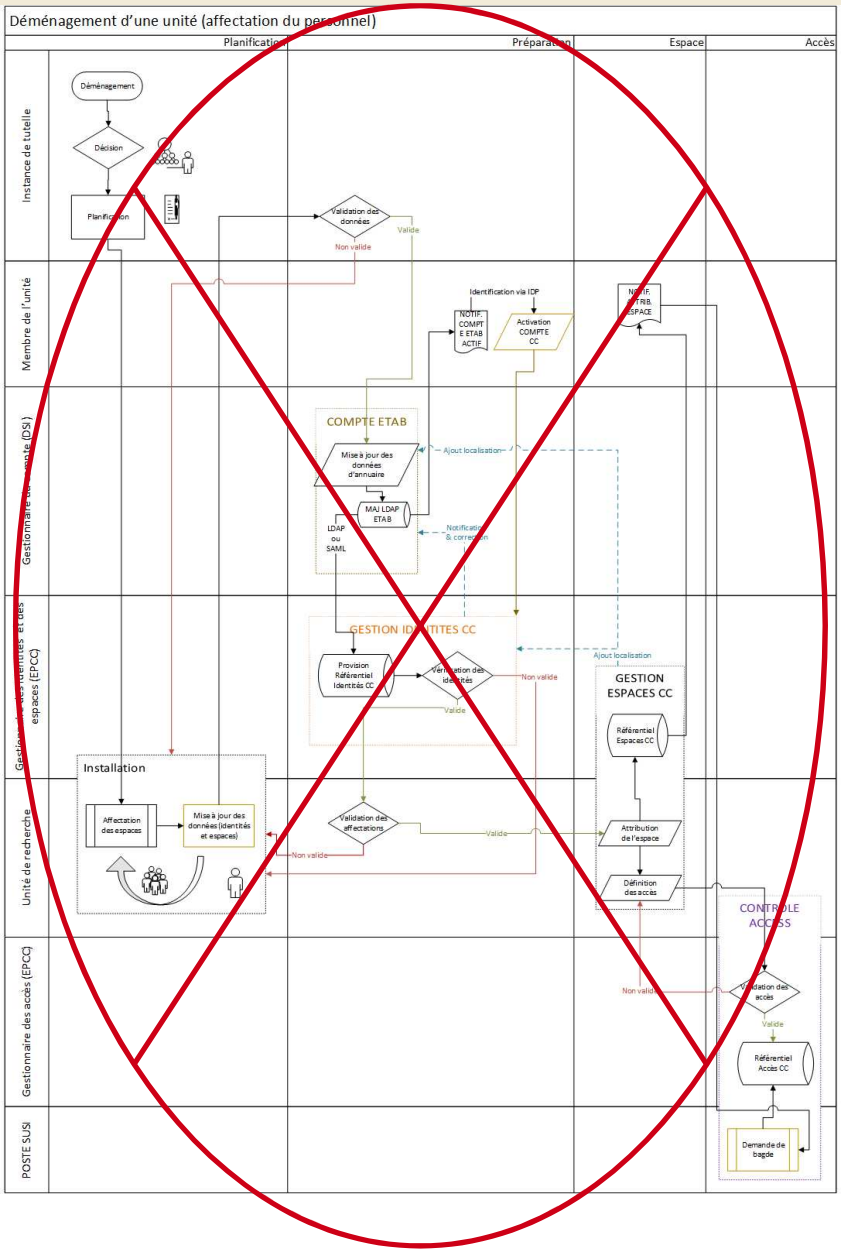
- L'autorisation de transfert n'est accordée que sur la base de finalités spécifiques (une par traitement) et détaillées (de sorte à garantir la proportionnalité des données transmises aux finalités du traitement)

→ 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 CIls :
  - 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

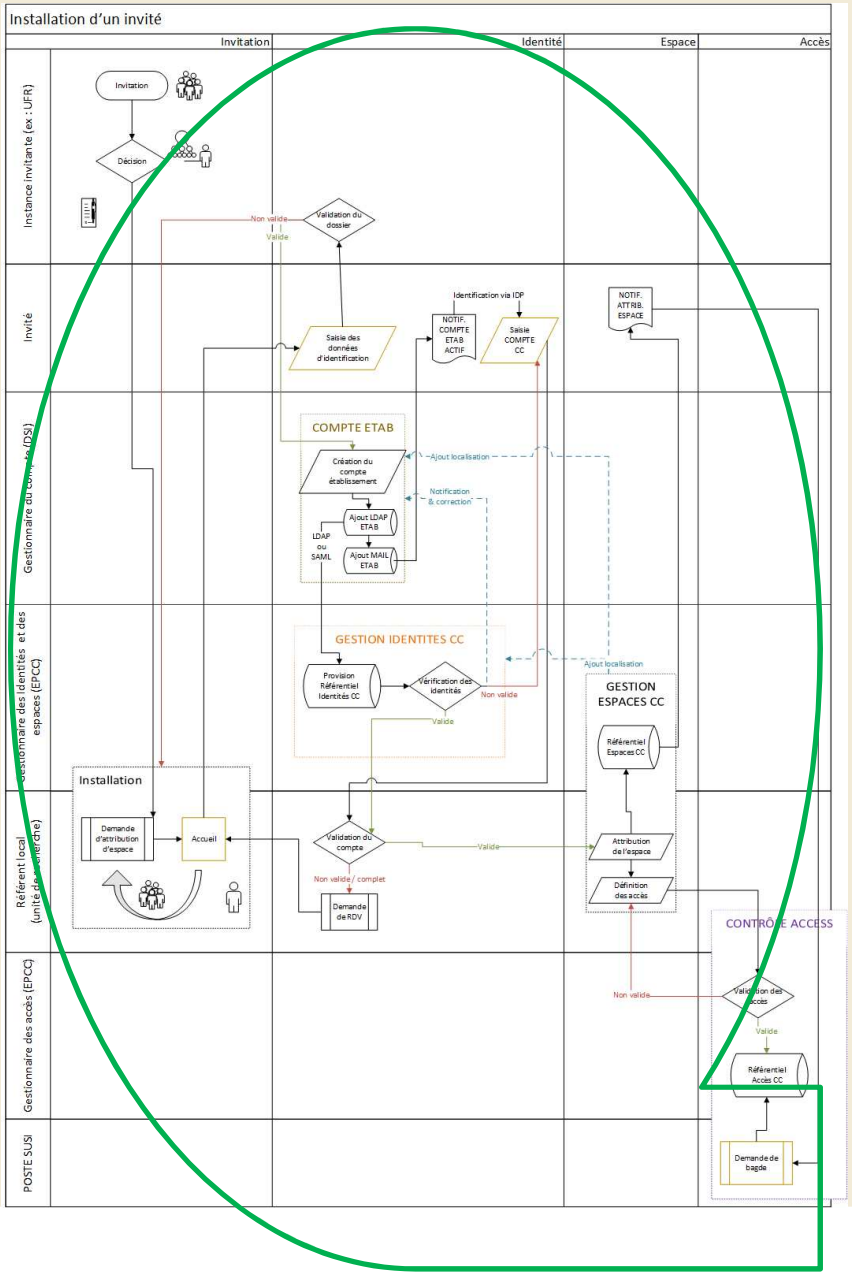
Processus de déménagement d'une unité



- 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

Usager

Invité

2. Invitations

3. Inscription

3. Inscription

Portail Campus

Unité / Établissement

Invitant

4. Validations

Référent Campus

5. Réassignations

1. Désignation

Référent Unité

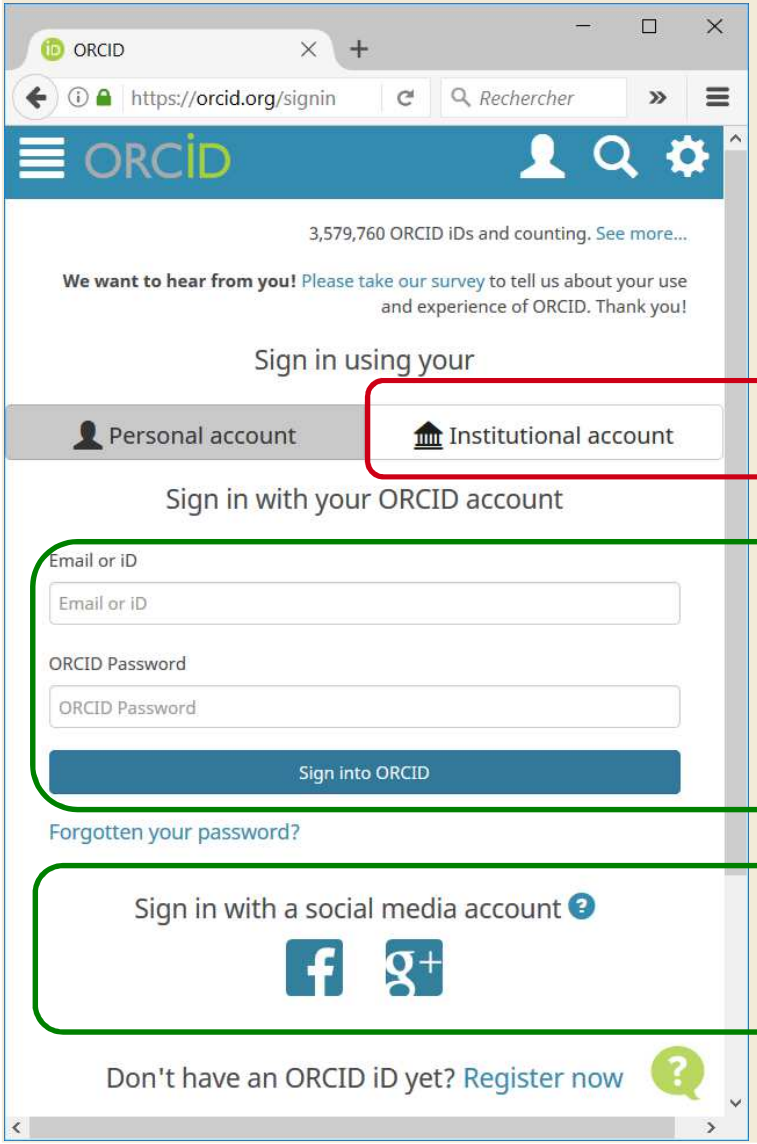
Campus

CAMPUS CONDORCET
Paris–Aubervilliers

Élargissement aux données de la recherche

LES IDENTIFIANTS ORCID

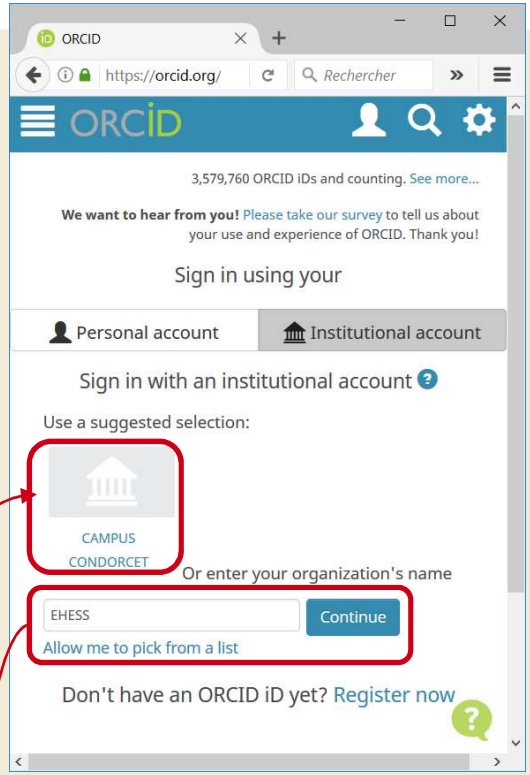
Identification sur ORCID



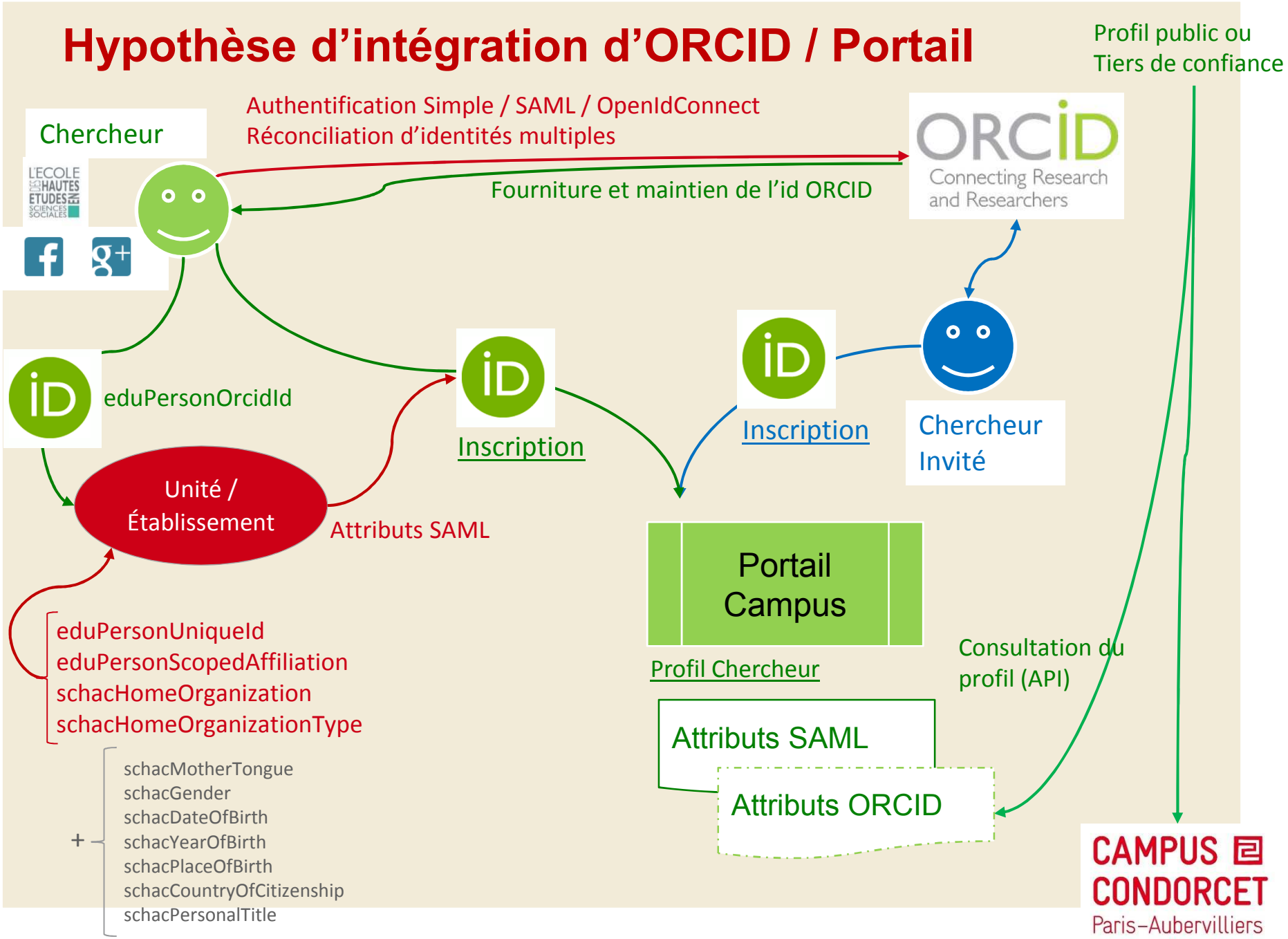
Compte d'affiliation institutionnel

Compte local ORCID

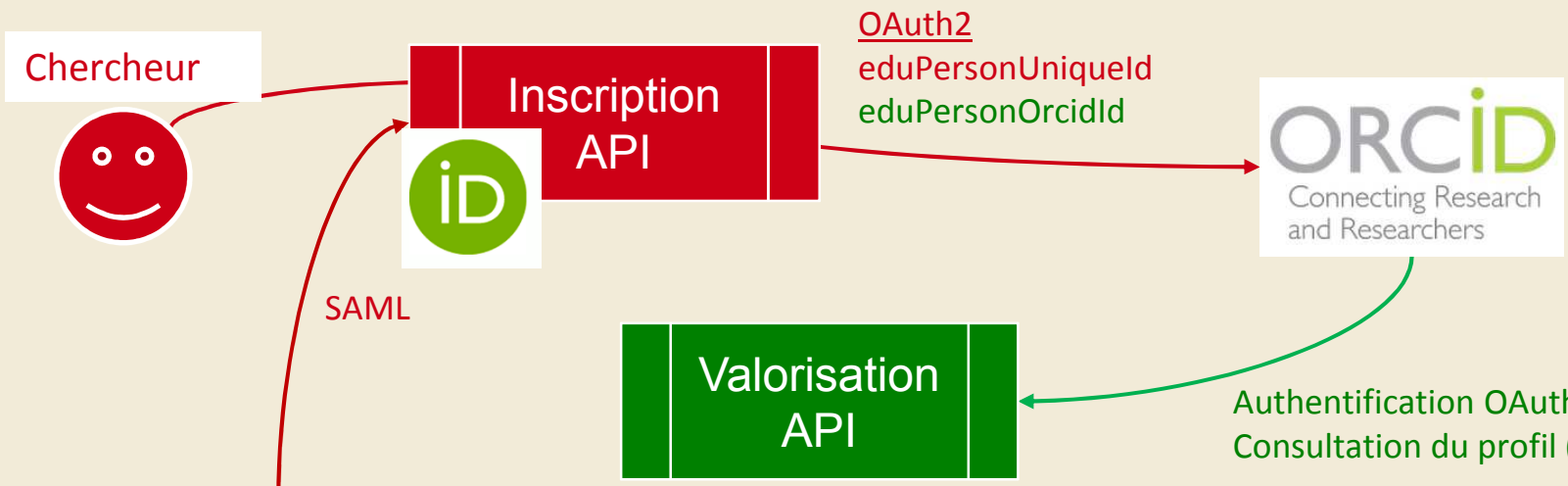
Compte lié à une identité sociale



Hypothèse d'intégration d'ORCID / Portail



Modèle d'intégration ORCID / SI identités*



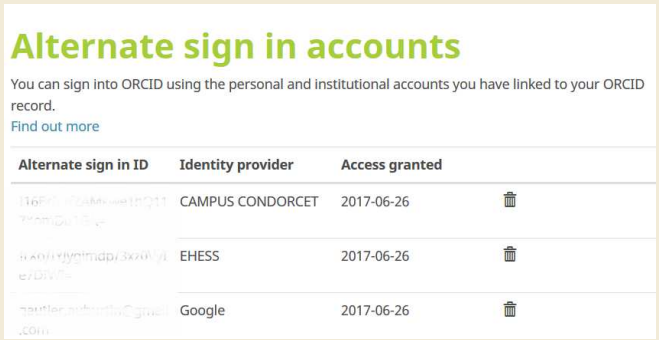
eduPersonUniqueId
eduPersonScopedAffiliation
schacHomeOrganization
schacHomeOrganizationType

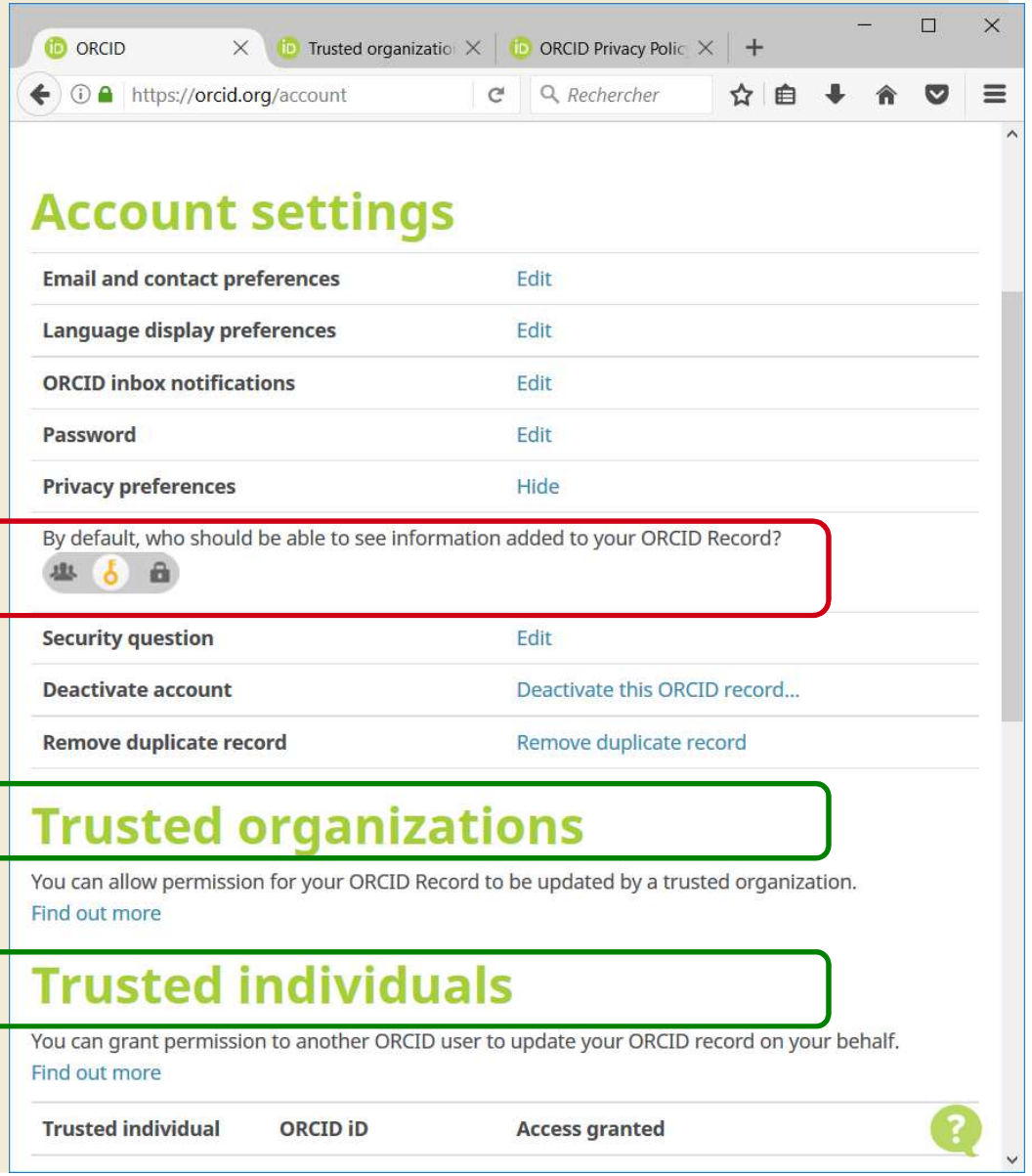
→ Non normalisés Chez ORCID (*affiliation item*)

Endpoint	Description
/record	Summary view of the full ORCID record
/person	Biographical section of the ORCID record, including through /researcher-urls below
/address	The researcher's countries or regions
/email	The email address(es) associated with the record
/external-identifiers	Linked external identifiers in other systems
/keywords	Keywords related to the researcher and their work
/other-names	Other names by which the researcher is known
/personal-details	Personal details: the researcher's name, credit (published) name, and biography
/researcher-urls	Links to the researcher's personal or profile pages
/activities	Summary of the activities section of the ORCID record, including through /works below.
/educations	Education affiliations
/employments	Employment affiliations
/fundings	Summary of funding activities
/peer-reviews	Summary of peer review activities
/works	Summary of research works

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

Autorisations d’accès au profil ORCID





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 Habour / Privacy Shield)
    - Patrimoine scientifique

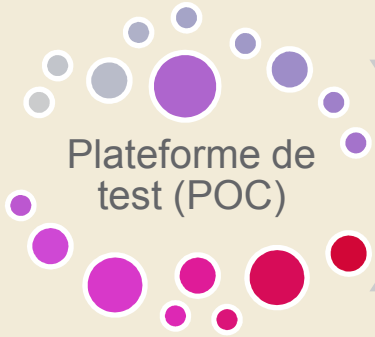
→ Tout transfert de données du SI de l'affiliation vers ORCID doit reposer sur :

→ 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 ?



Plateforme de test (POC)

Consolidation & Études

Réalisation & Déploiement

Mise en production

- Éprouver les données et les processus
- Méthode itérative

- Formalisation des processus
- Étude technique des infrastructures d'IAM

- Développement d'une plateforme d'IAM
- Mise au place d'une gouvernance

- Déménagement (structures)
- Installation (usagers)
- Inventaires (équipements)

1 An — 9 mois — 9 mois

2018 — 2019 — Ouverture Campus

3 établissements volontaires

10 établissements DSI GT NUM

Marché (EPCS porteur)

École Pratique des Hautes Étude

UNIVERSITÉ PARIS 1 PANTHÉON SORBONNE

ined INSTITUT NATIONAL D'ÉTUDES DÉMOGRAPHIQUES

Schéma fonctionnel du processus d'inscription

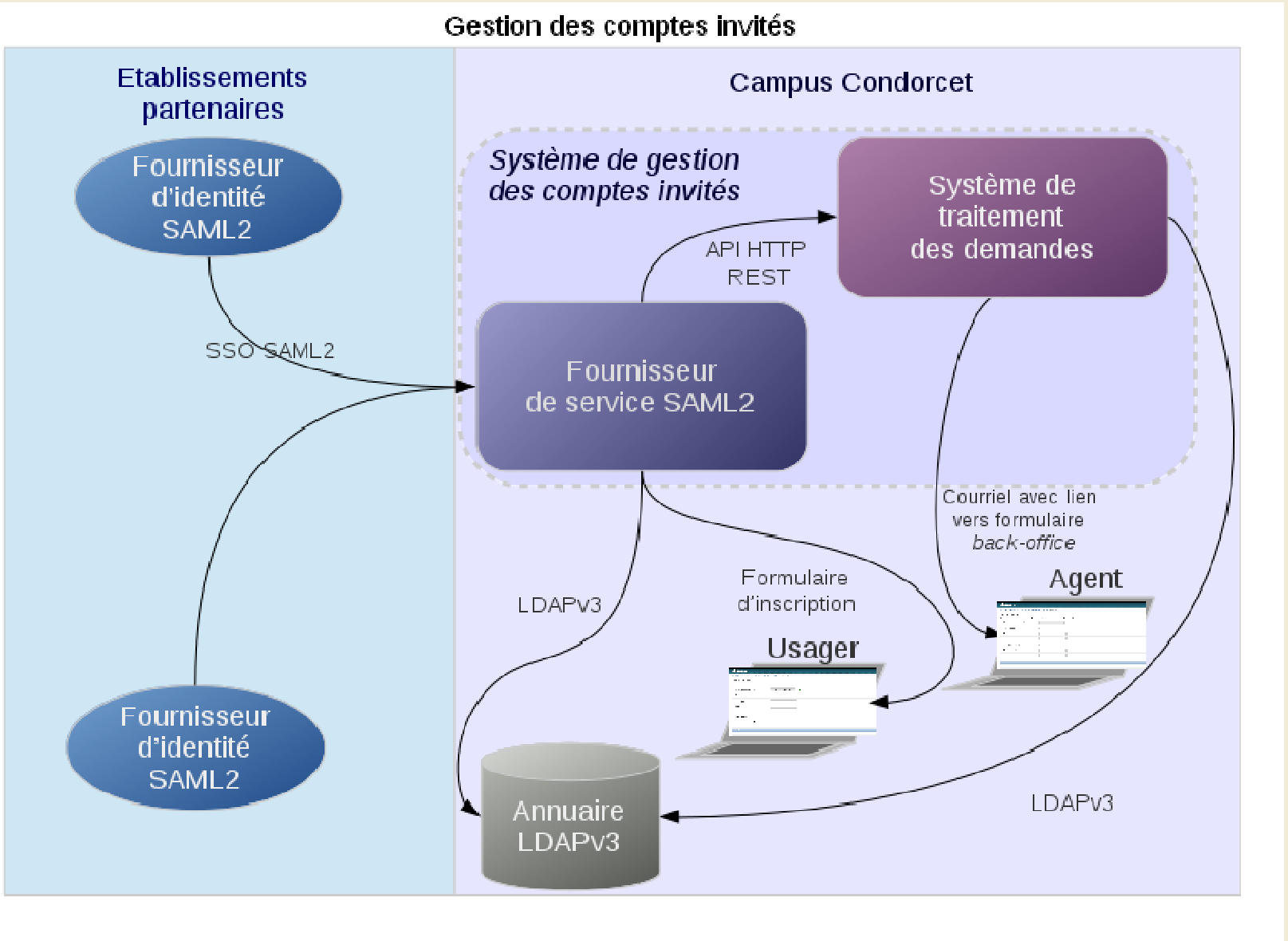
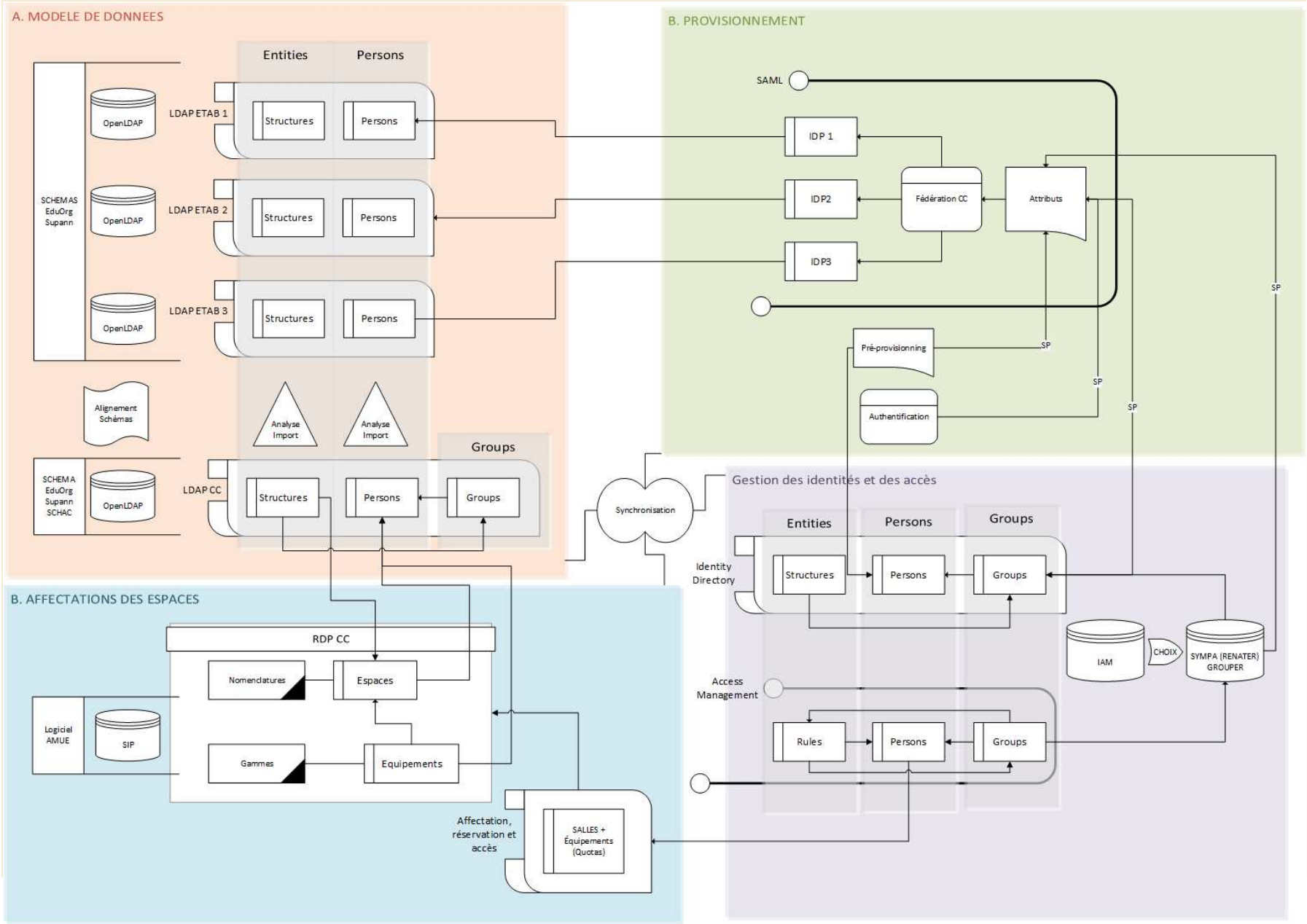


Schéma technique du référentiel d'identités Campus



CAMPUS CONDORCET
Paris–Aubervilliers

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

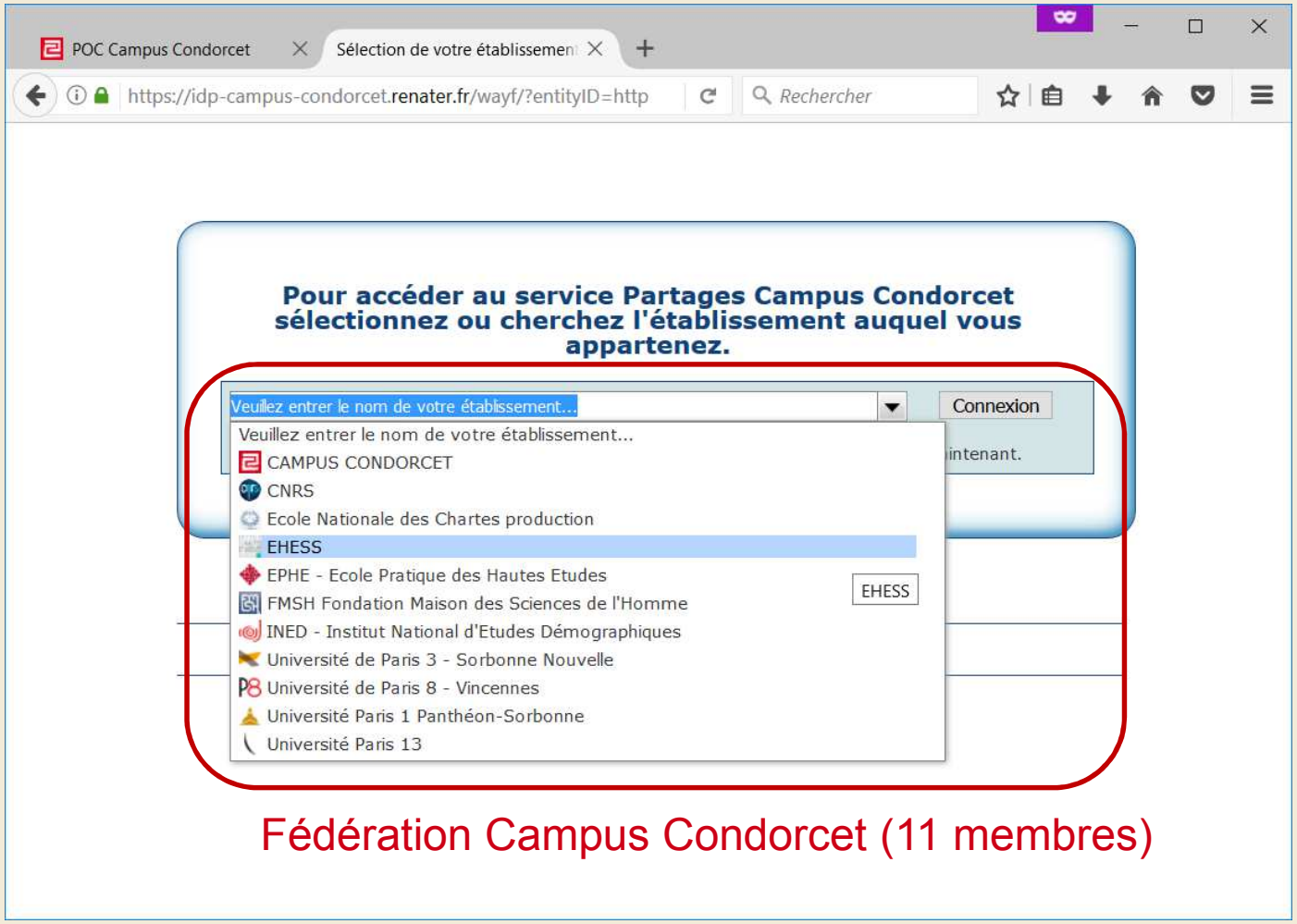
PROTOTYPE

entr'ouvert

INSCRIPTIONS

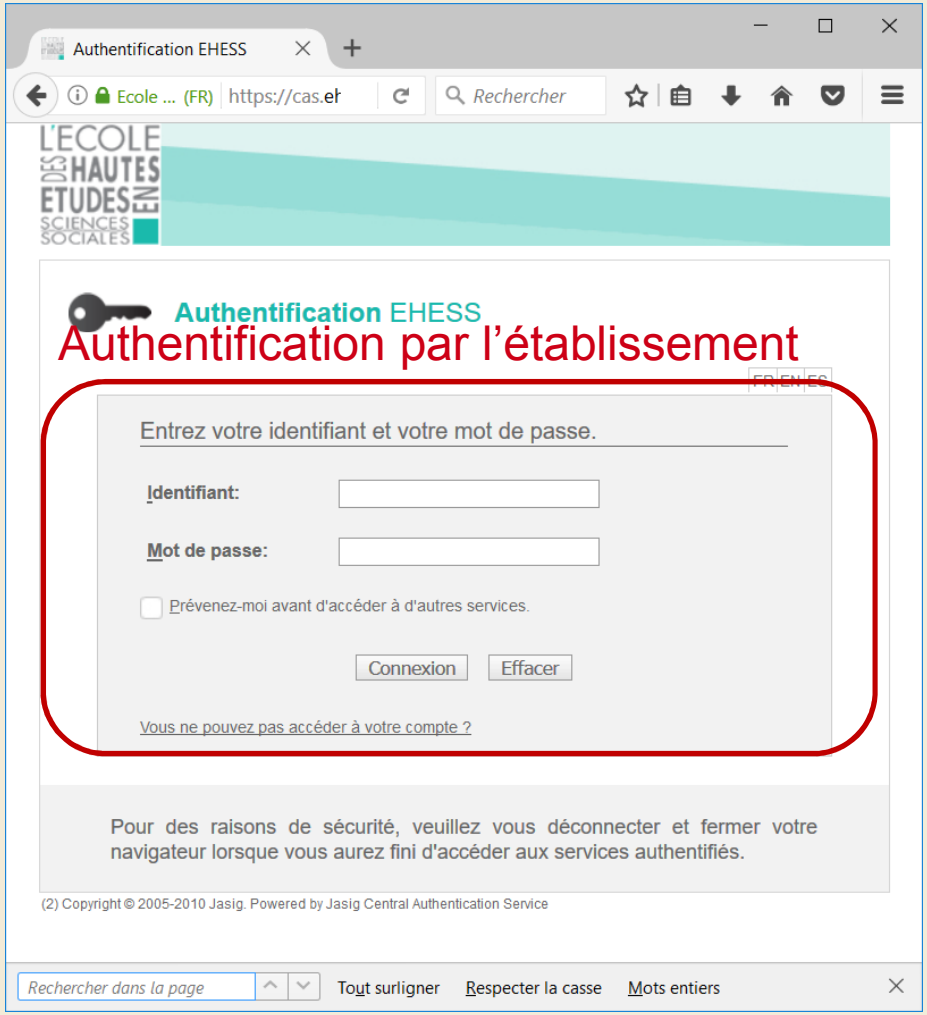
Inscription pour l'emménagement d'un usager

Inscription pour l'emménagement d'un usager



Fédération Campus Condorcet (11 membres)

Inscription pour l'emménagement d'un usager

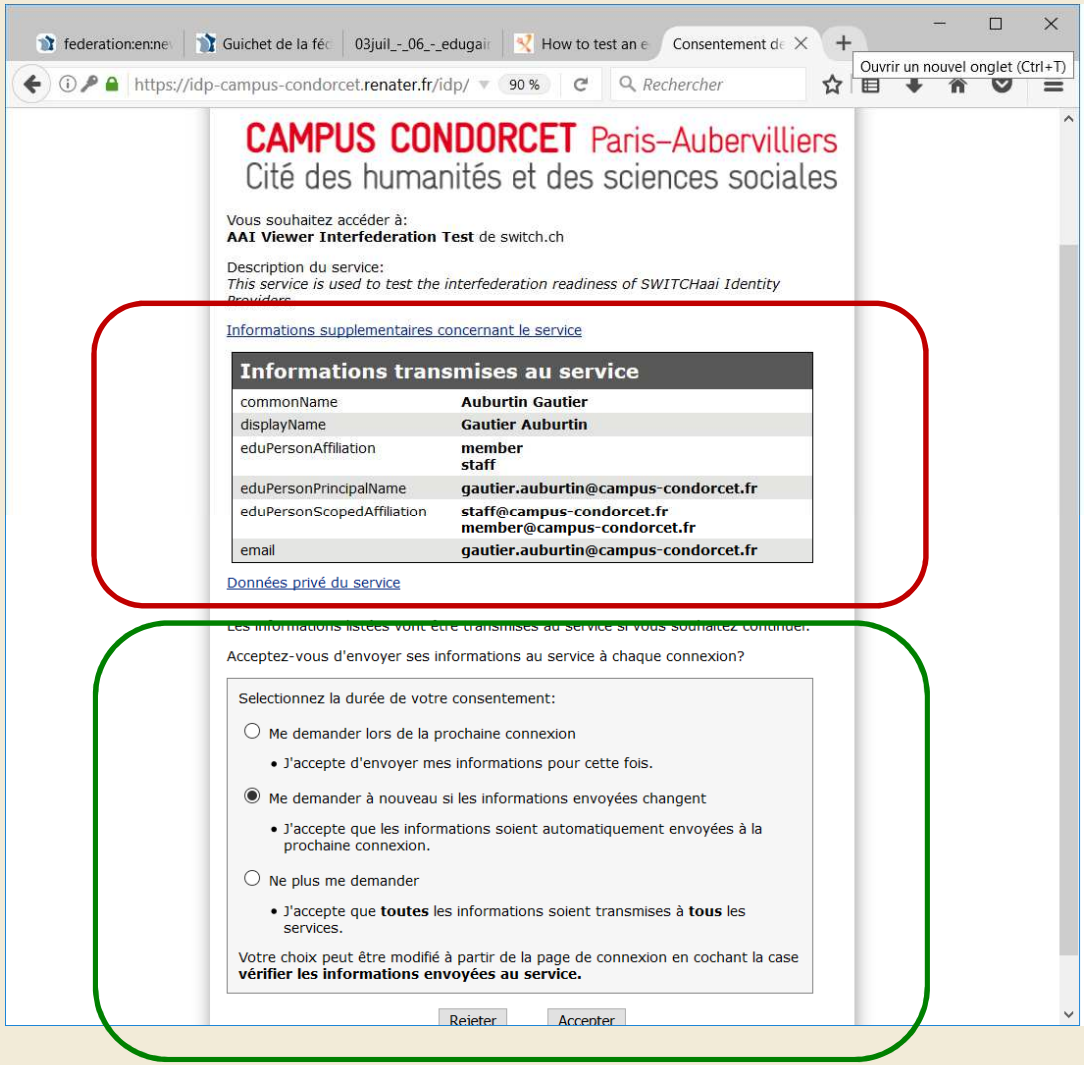


Si la personne change d'établissement

- Elle ne peut plus se connecter

Nous appliquons la politique des établissements

Inscription pour l'emménagement d'un usager

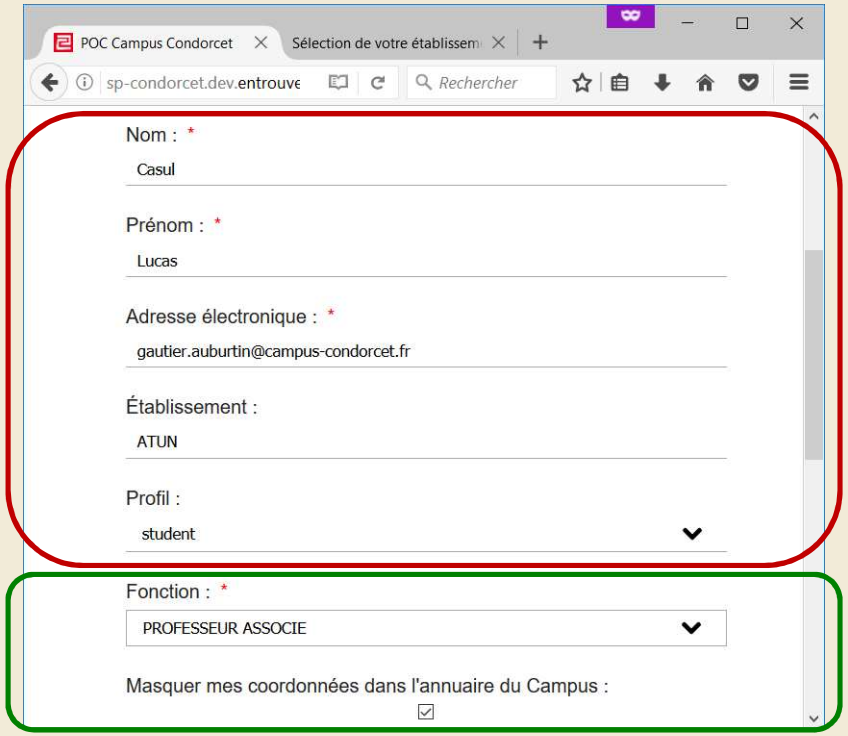


Collecte
de données personnelles

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Inscription pour l'emménagement d'un usager



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

Attributs fournis non modifiables

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

Attributs fournis mais modifiables

- Corps
- Liste rouge

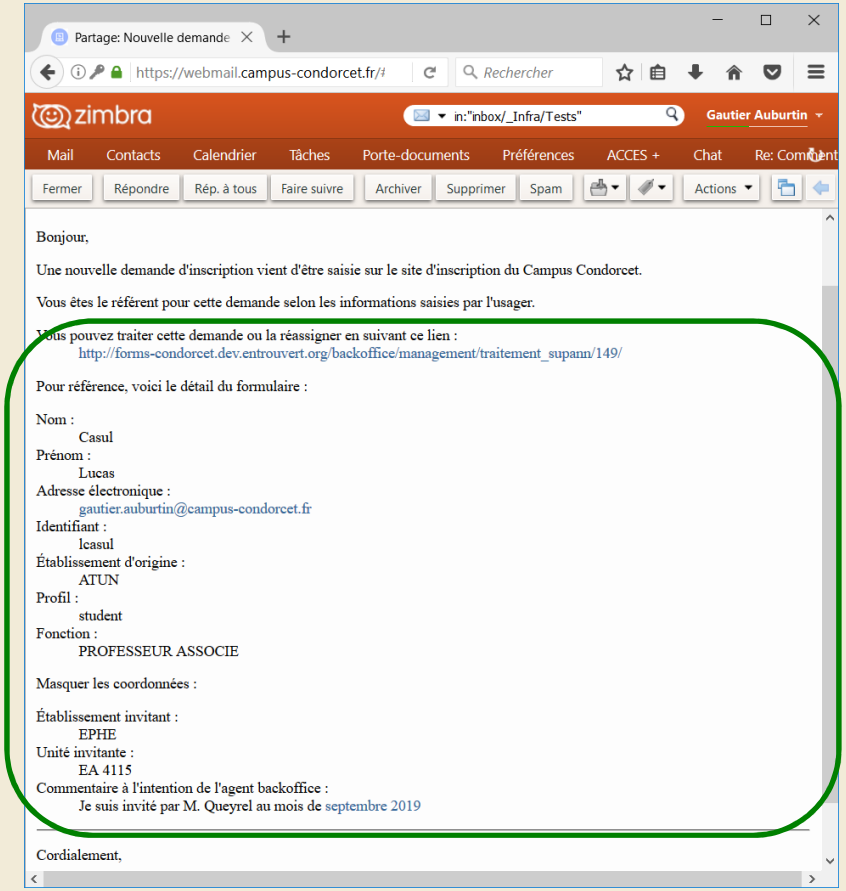
Attributs normalisés

- EduPerson
- Supann

RENATER
CONNECTEUR DE SAVOIRS

Inscription pour l'emménagement d'un usager

Notification de l'usager



Envoi pour validation au référent

<u>Conditions</u>

Si Structure → Réf. Structure

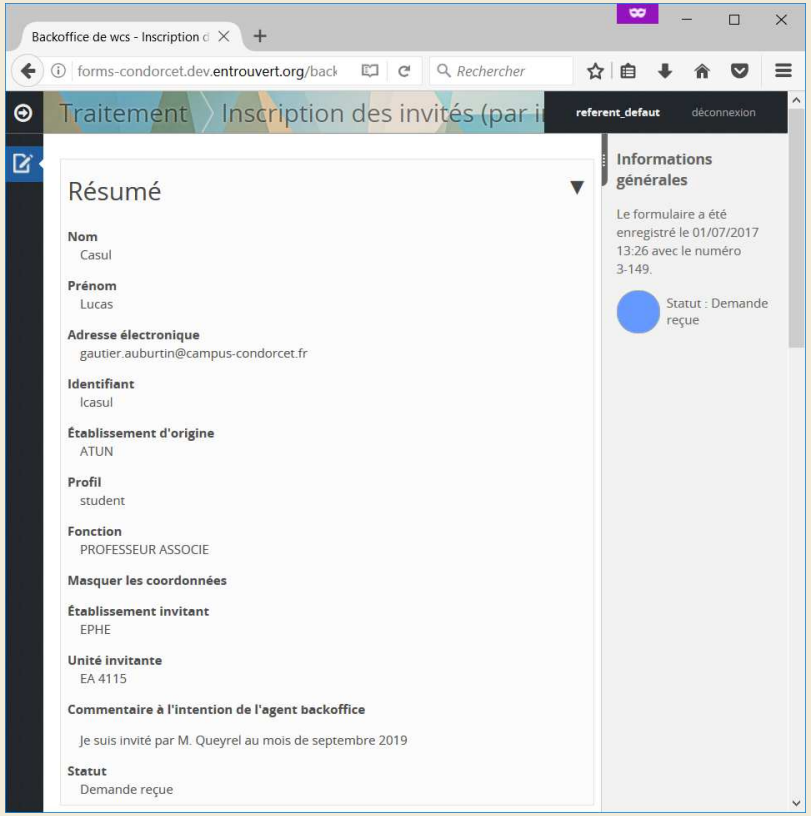
↳ Sinon → Réf. établissement

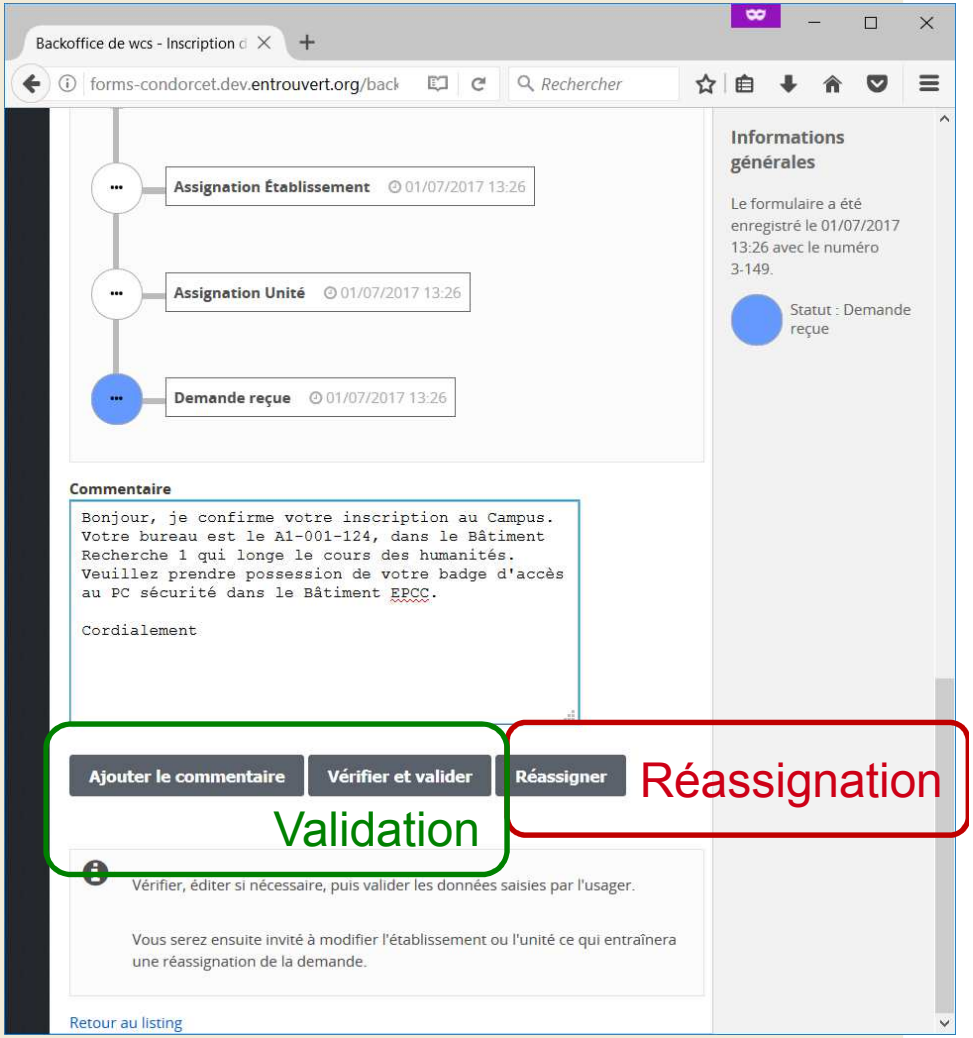
↳ Sinon → Réf. par défaut

→ Récapitulatif de la demande

→ Lien direct vers le formulaire

Inscription pour l'emménagement d'un usager





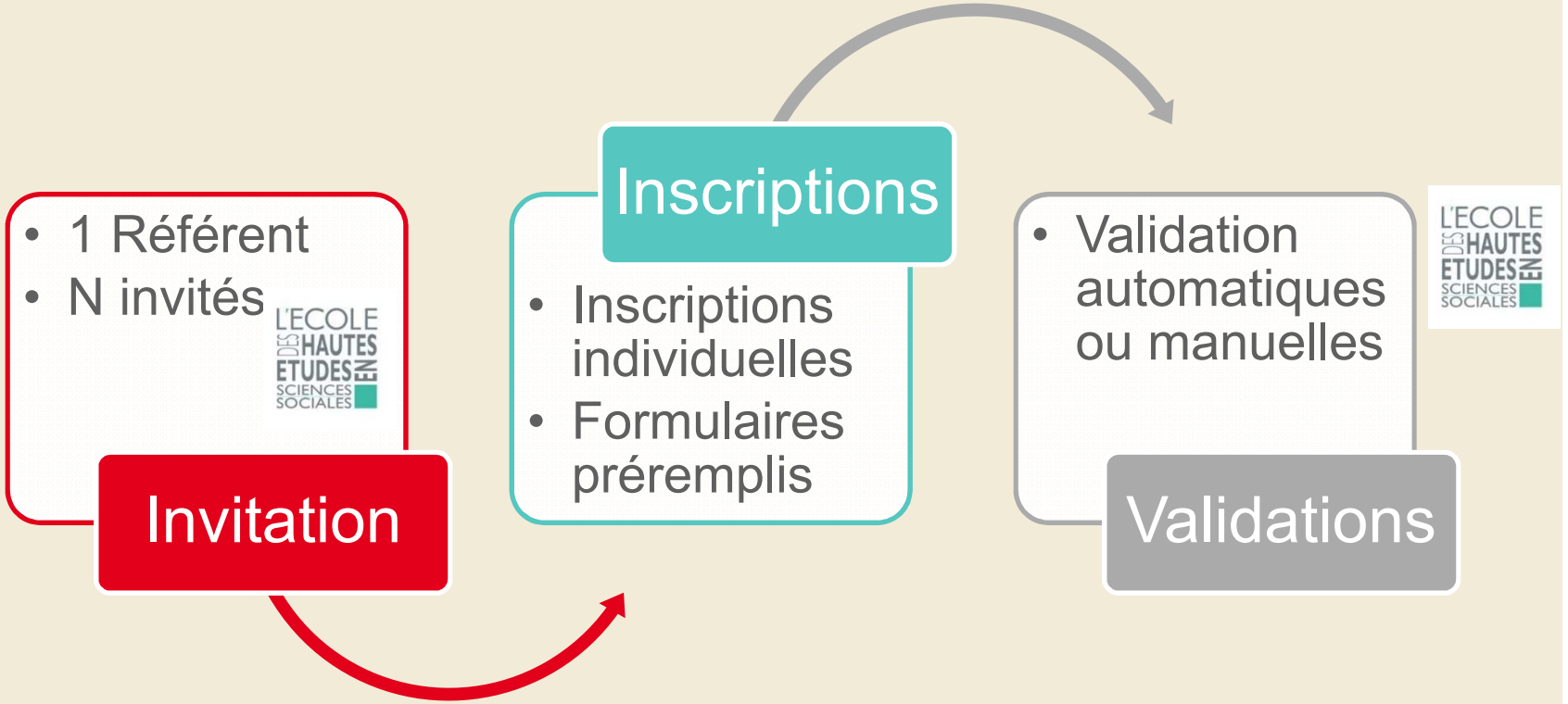
Traitement de la demande

- Commentaire
- Informations complètes → Validation
- Sinon :

  ↳ Réassignation vers un autre référent

INVITATIONS

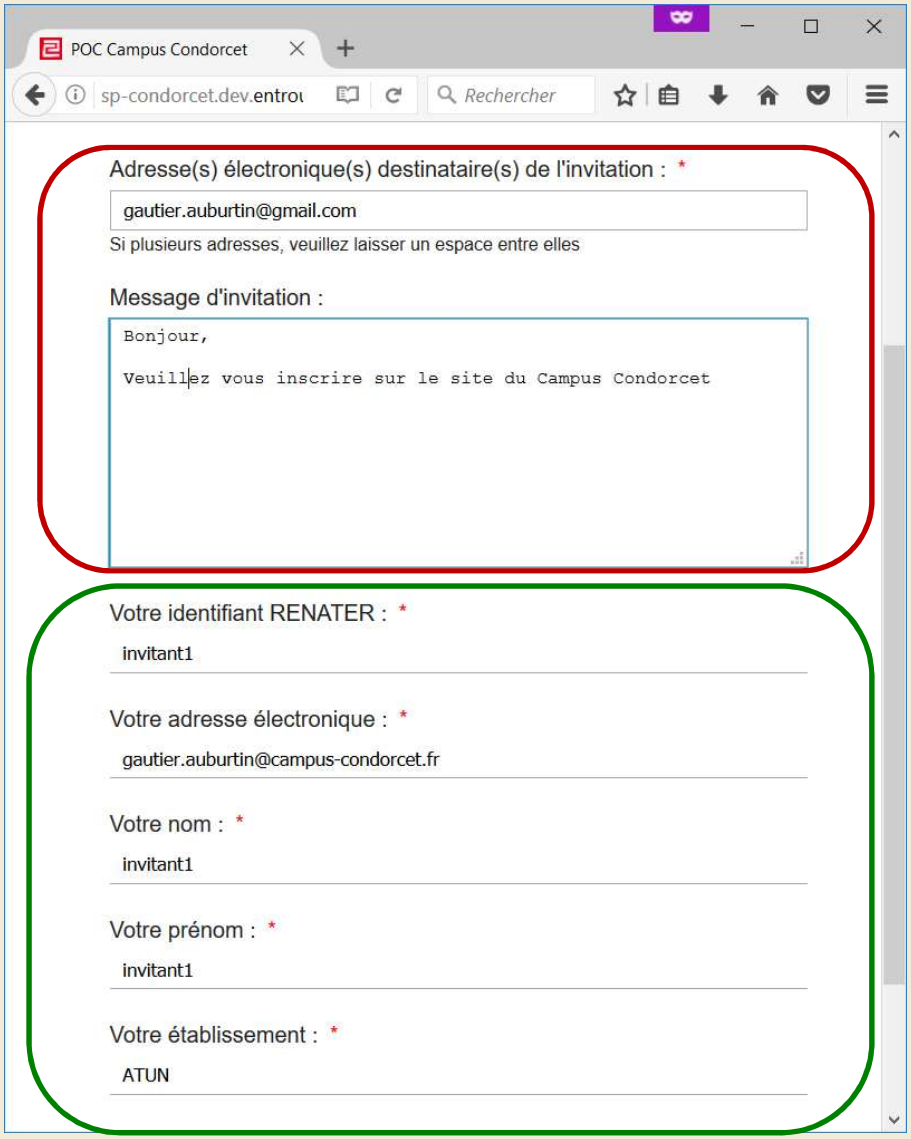
Modèle d'invitation proposé



CAMPUS CONDORCET
Paris–Aubervilliers

Invitation d’une ou plusieurs personnes

Inscription d'une personne invitée



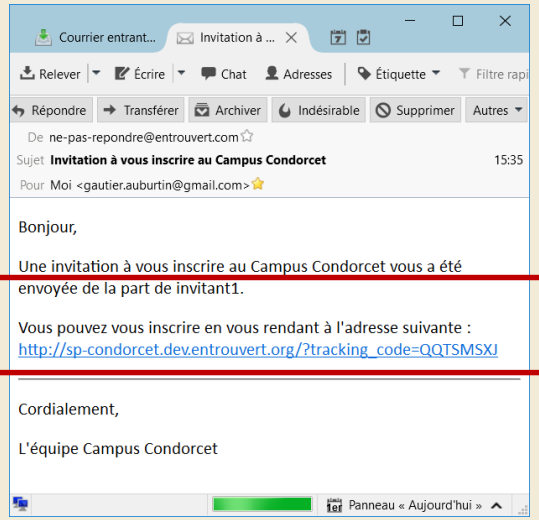
Envoi d'une invitation

- Adresses des invités
- Message libre

Information de contexte

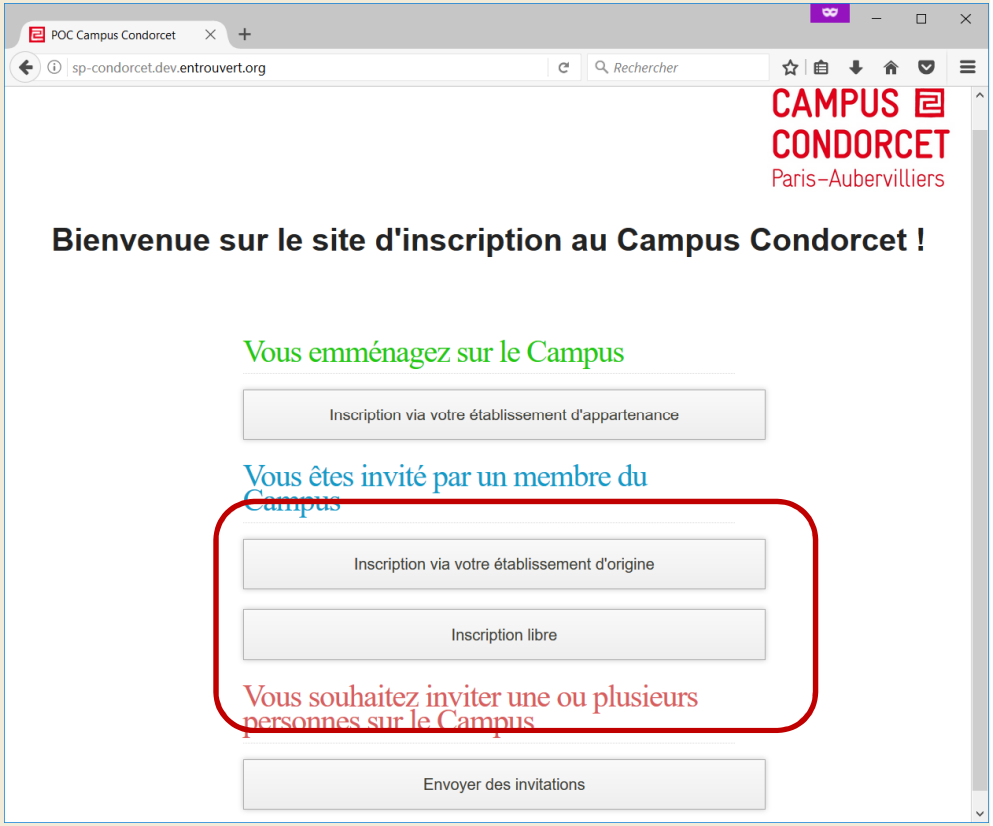
- L'affiliation de l'invitant détermine la structure invitante
- Le processus est automatisé (validation optionnelle)

Inscription suite à une invitation

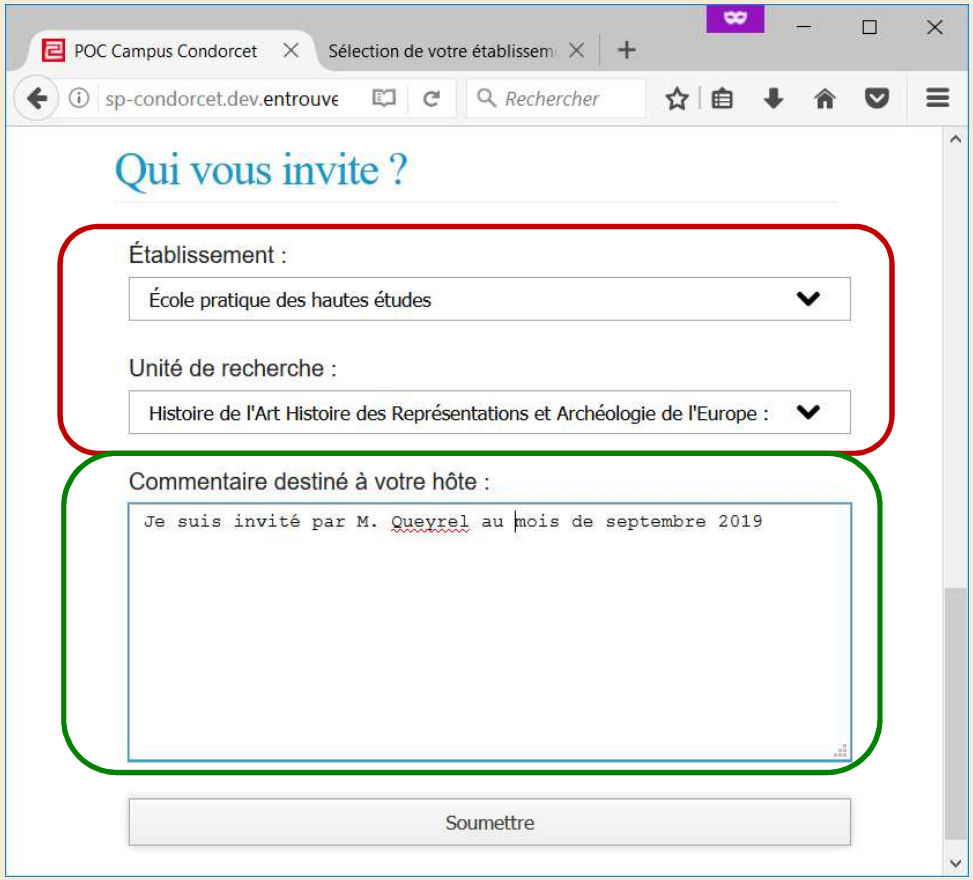


L'invité se connecte :

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



Inscription suite à une invitation



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