



Fédération d'identités | Exemple du CNOUS

Cas d'usage recueilli auprès du RSSI du CNOUS, M.PERROT

« La Fédération d'identités est devenue la norme d'authentification pour les nouvelles applications. »

PRÉSENTATION DE L'ÉTABLISSEMENT



« Le Centre National des Oeuvres Universitaires & Scolaires ([CNOUS](#)) pilote les 26 Crous régionaux, en particulier dans le domaine du numérique en mettant en place divers outils nationaux à destination de la vie étudiante et des agents du réseau des Crous. »

LE BESOIN

« Le CNOUS c'est 26 établissements et donc 26 annuaires à fédérer : la première brique a été la mise en place d'un [DS](#)¹, puis d'un IDP² par établissement afin de permettre l'usage d'outils nationaux [shibbolisés](#) dont l'authentification était basée sur les sésames des annuaires régionaux.

Certains de nos services sont destinés aux étudiants ou à certains agents des Ecoles ou Universités (assistantes sociales par exemple), donc l'enregistrement doit, dans ces cas là, être fait dans la Fédération Éducation-Recherche.

Certaines solutions comme le routeur du projet [European Student Card](#) a également nécessité l'usage de l'inter-fédération [Edugain](#), dont la [Fédération RENATER](#) fait partie.

Quelques exceptions sont présentes dans l'inter-fédération Edugain, mais la plupart de nos SPs³ sont enregistrés dans l'une de nos deux fédérations privées. La raison d'être de ces deux fédérations privées (et de leurs DS respectifs) est de permettre de répartir les SPs dans leurs trois principaux états (test, qualification, pre-prod/prod) afin de les cloisonner et les trier. »

LA MISE EN PLACE DE LA FÉDÉRATION⁴

« On a dans un premier temps déployé des modèles de serveurs pré-installés dans la plupart des Crous mais la charge de travail induite par la maintenance de ces nombreux serveurs nous a très rapidement conduit à mettre en place une "usine à IDP" où sont désormais concentrés 21 des 26 IDPs du réseau. La plupart des SPs utilisent les briques shibboleth mais il y a quelques exceptions basées sur du SimpleSAML. »

« Equipe RENATER présente, disponible et compétente, comme toujours. »

LES RÉSULTATS

« La Fédération est devenue la norme d'authentification des nouvelles applications. Nos anciennes applications ne sont pas encore toutes migrées par manque de temps, et parfois de compétences chez nos prestataires. Mais c'est tout de même environ 178 entités SAML, dont 29 IDPs, 3 DS et 2 fédérations privées qui ont été créés.

De plus nous avons un projet d'utilisation d'OpenID en complément ou en remplacement de SAML sur quelques rares SPs destinés aux étudiants. »

Quelques exemples de services iconiques déployés par le CNOUS dans ces fédérations :

- [MesservicesEtudiant](#)
- [Portail de la vie étudiante Screen \(Xibo mutualisé\)](#)
- [Portail CVEC](#)
- Et beaucoup d'autres encore...

¹ Discovery Service : permet à l'utilisateur de sélectionner manuellement son domaine parmi une liste.

² Identity Provider : fournisseur d'identité, s'occupe d'authentifier l'utilisateur ainsi que de récupérer des informations additionnelles associées à son identité.

³ Service Provider : fournisseur de service, protège l'accès aux applications. Il refuse tout accès sans authentification préalable et redirige l'utilisateur non authentifié vers son fournisseur d'identité.

⁴ [En savoir +](#)

EN SAVOIR +

LA FÉDÉRATION D'IDENTITÉS ÉDUCATION-RECHERCHE :



Plus de **350**
établissements membres
de la Fédération



Plus de **1300** services
dans la Fédération
Éducation-Recherche



Plus de **130K**
comptes gérés