

26M12 ANNEXE N°2 au CCP

CONFIGURATION TECHNIQUE POUR LES IMPLANTATIONS DE L'UNIVERSITÉ PARIS 1 PANTHÉON-SORBONNE

L'université Paris 1 Panthéon-Sorbonne est répartie sur 30 sites à Paris et proche banlieue. Les principaux sites sont raccordés au réseau de collecte RAP (Réseau Académique Parisien). L'accès vers l'extérieur se fait par la traduction d'adresses IP (NAT) ou par proxy.

De nouvelles implantations de l'université sont possibles durant la durée de ce marché. En effet, certains services de l'université Paris 1 déménagent, de nouveaux bâtiments vont être occupés par des services de l'université Paris 1.

1. Les adresses IP

L'université Paris 1 utilise des adresses IP v4 et IP v6. Le fournisseur doit pouvoir gérer un adressage en IP v6. Pendant la période de transition IP v4 / IP v6, des machines pourront avoir un double adressage.

1.1. Liste des adresses IP v4

193.55.96-103.0 à 255
193.55.107.0 à 255
194.214.25-36.0 à 255
194.214.199.137
194.214.199.160

1.2. Préfixes IP v6 (pour l'ensemble de l'université)

2001:660:3305/48
2001:660:3311/48

2. Proxies des bibliothèques de Paris 1

2.1. Proxies SCD et bibliothèques associées

Reverse proxy EZproxy avec authentification SSO :
ezpaarse.univ-paris1.fr
Adresse IP v4 : 193.55.96.20
Adresse IP v6 : 2001:660:3305::20

2.2. Proxies BIU Cujas

Proxy pour les postes publics de la salle de lecture :
193.55.98.192
193.55.98.92
193.55.98.4
Reverse proxy : bcujas-ezp.univ-paris1.fr, 193.55.98.12

2.3. Proxies BIU Sorbonne

Reverse proxy (EZproxy) : janus.bis-sorbonne.fr, IPv4 ; 193.55.97.20 ; IPv6 :
2001:660:3311:4000::20

3. Authentification

Lorsque l'accès aux périodiques électroniques nécessite une authentification (accès distant et cas de certaines ressources en accès sur place), celle-ci s'appuie sur la base utilisateurs de l'université (cas du SCD et des bibliothèques intégrées et associées) ou celle de la bibliothèque (cas des bibliothèques inter-universitaires Cujas et Sorbonne). A cet effet deux mécanismes sont proposés :

- Intégration native par les soins de l'éditeur de la ressource électronique concernée dans la fédération d'identités Education-Recherche, en tant que « Service Provider » (SP). Dans ce mode de fonctionnement, le contrôle d'accès (vérification que la personne authentifiée dispose bien d'un profil l'autorisant à accéder à la ressource) est du ressort de l'éditeur.
- Accès à la ressource électronique au travers d'un reverse-proxy authentifiant de type « EZProxy » ou analogue, déployé par l'université ou la bibliothèque concernée. Dans ce mode, le contrôle d'accès est du ressort de l'université ou de la bibliothèque ayant déployé le reverse-proxy, le contrôle au niveau éditeur se limitant alors à une simple autorisation d'adresse IP.

Ces mécanismes devront permettre d'accéder aux ressources électroniques depuis des postes extérieurs à l'université, dans le respect des droits définis par chaque éditeur sur ses ressources en ligne.

Références :

- Fédération Education-Recherche : <https://services.renater.fr/federation/index>
- SUPANN : <https://services.renater.fr/documentation/supann/index>
- Internet2 eduPerson : <https://www.internet2.edu/products-services/trust-identity-middleware/eduperson-eduorg/>

3.1. SCD

Au SCD, l'accès aux ressources électroniques fait depuis 2020 par le portail documentaire EDS. L'accès aux bases utilise les procédés Z 39.50, passerelle XML, API ou requête HTTP. Dans le cas des bouquets de périodiques, l'open-url doit être possible. L'accès distant aux bases et aux bouquets de périodiques se fera également via le portail, par le biais d'un reverse-proxy EZProxy ou la fédération Education-Recherche pour les bases supportant nativement ce mode d'accès.

Le reverse-proxy est configuré pour proposer deux modes de fonctionnement en fonction de la localisation du poste de travail du lecteur et des termes du contrat de licence :

- Pour les postes internes aux locaux du SCD, lorsque la licence éditeur le permet, l'accès se fait sans authentification personnelle. L'autorisation s'effectue dans ce cas sur le reverse-proxy par contrôle d'adresse IP du poste de travail.
- Dans les autres cas (en particulier l'accès distant), l'utilisateur est authentifié et un contrôle d'accès basé sur son profil est appliqué. Ces opérations sont effectuées en interne par le reverse-proxy en s'appuyant sur les mécanismes de la fédération Education-Recherche, de la même manière que sur une base de données nativement intégrée à la fédération. Le fournisseur d'identités (IDP) utilisé est celui de l'université Paris 1 Panthéon-Sorbonne, qui s'appuie sur l'annuaire LDAP et l'authentification Web SSO (Single-Sign-On) de l'université.

Le fournisseur d'identités (IDP) de l'université Paris 1 cesse de présenter la valeur « common-lib-terms » de l'attribut eduPersonEntitlement lorsque l'utilisateur ne dispose plus d'un profil éligible à l'accès distant aux bases documentaires, ce qui permet de révoquer les accès aussi bien via le reverse-proxy que nativement via la fédération d'identités.

3.2. BIU Cujas

La bibliothèque interuniversitaire Cujas, donne accès sur les postes publics de la salle de lecture à l'ensemble de ses lecteurs inscrits, selon les conditions négociées avec les éditeurs dans le cadre des licences. Elle donne également accès sur les postes professionnels à ses personnels. Elle propose un accès distant aux lecteurs usagers autorisés (lecteurs de l'université Paris 1, lecteurs de l'Université Paris 2, personnels de la bibliothèque, selon les conditions de la licence).

L'accès dans les locaux, sur les postes publics mis à disposition par la bibliothèque, passe par un proxy. Le verrouillage du poste de consultation se fait en mode kiosk.

L'accès distant passe par un reverse proxy (EZProxy) s'appuyant sur le module PDS (Patron Directory Service) dédié à la gestion des authentifications des usagers ainsi que du SSO (Single Sign On). Ce module s'appuie sur la base des lecteurs inscrits à la bibliothèque gérée dans le SIGB Alma.

L'authentification par l'intermédiaire de la fédération d'identité Education-Recherche peut aussi être proposée, mais à titre marginal.

La BIU Cujas maintient le principe que différents modes d'authentification doivent être possibles.

Prérequis et compatibilité :

cf <http://www.oclc.org/support/services/ezproxy/documentation.en.html>

Compatibilité OpenURL

3.3. Bibliothèque de la Sorbonne

La bibliothèque interuniversitaire de la Sorbonne, selon les conditions négociées avec les éditeurs dans le cadre des licences, donne accès aux ressources en ligne, sur ses postes, à l'ensemble de ses lecteurs inscrits et à ses professionnels. L'accès depuis les locaux de la bibliothèque sur les postes mis à disposition des lecteurs, passe par un proxy web dont l'adresse IP est déclarée aux éditeurs. Quant aux postes des professionnels de la bibliothèque, l'accès se fait directement après reconnaissance des adresses IP sur les serveurs des éditeurs. La bibliothèque propose aussi à ses lecteurs inscrits un accès distant grâce au reverse proxy EZproxy. Les lecteurs s'authentifient grâce à un protocole d'authentification unique (SSO Single Sign-On) qui s'appuie sur l'annuaire LDAP de l'université Paris 1 Panthéon-Sorbonne, lequel contient l'ensemble des lecteurs inscrits à la bibliothèque : dès que la date d'inscription d'un lecteur n'est plus valide, le système lui interdit d'accéder à distance aux ressources en ligne non libres.

4. Les protocoles

Les protocoles d'échange utilisés sont des standards basés sur TCP/IP, en version 4 (IP v4) et 6 (IP v6).

La fédération d'identités fait appel au standard SAML (Security assertion markup language) version 2, à la technologie Shibboleth qui fait office d'implémentation de référence, aux protocoles HTTP et HTTPS, et aux définitions d'attributs des recommandations SUPANN et Internet2 eduPerson.

5. L'environnement machine

Les postes de travail de l'université sont sous différents systèmes d'exploitation : Linux, Mac OS X, Windows. Toutes les versions peuvent coexister.