Retex sur la configuration d’un serveur reverse proxy shibboleth, jouant le rôle de *Service Provider* au sein de la fédération éducation recherche.
Ce serveur disposera de son propre service de découverte.

Reverse proxy : Un **reverse proxy HTTP** est un **serveur intermédiaire** placé **devant un ou plusieurs serveurs web** pour **recevoir les requêtes des clients et les transmettre aux serveurs internes**, de façon **transparente pour l’utilisateur**.

Shibboleth : **Shibboleth** est une **solution d’authentification fédérée** qui permet à un utilisateur de se connecter à des services web **sans créer de compte local**, en utilisant l’identité fournie par son **organisation d’origine**.

Service Provider : Un **SP (Service Provider)** est un **service ou une application web** qui **délègue l’authentification des utilisateurs** à un système externe de confiance, appelé **IdP (Identity Provider)**.

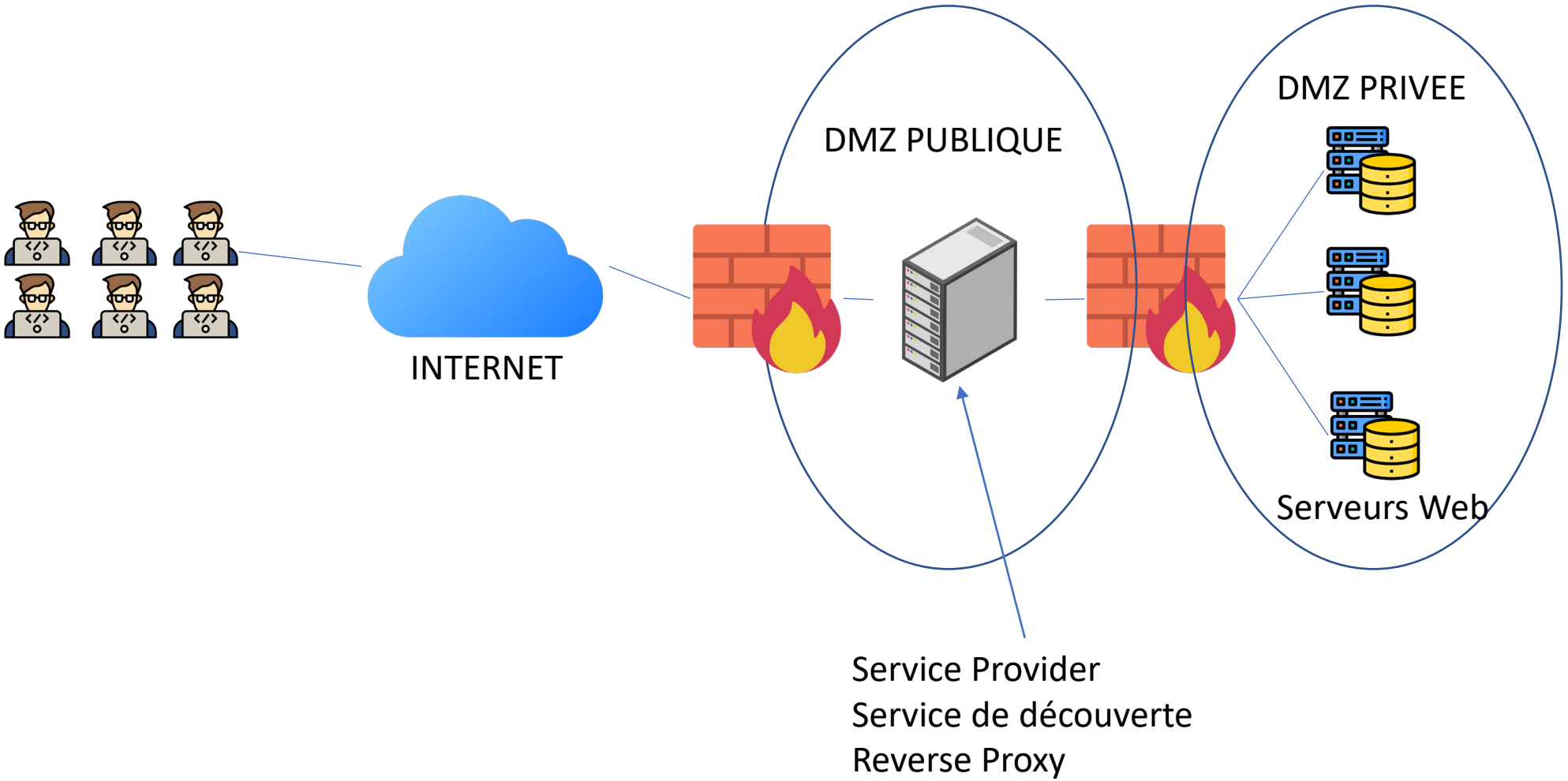
Fédération éducation recherche : La Fédération Éducation-Recherche est une infrastructure technique nationale visant à répondre aux besoins de fédération d'identité du monde de l'enseignement supérieur et recherche français.

Service de découverte : Une brique logicielle supplémentaire aussi appelée **(Discovery Service ou encore WAYF)** qui permet lors de la connexion d'un utilisateur de l'aiguiller vers le fournisseur d'identités de son établissement.
Exemple : https://discovery.renater.fr/renater/

Pourquoi ?

- Moins de gestion des comptes utilisateurs (on s’appuie sur l’idp de l’entité)
- Plus de problématique de gestion et de stockage des mots de passe
- Gagner en sécurité : ne plus afficher la mire de login de l’appli sur Internet
- Faciliter l’accessibilité aux utilisateurs des autres établissements

Architecture cible



Plan

1 – Définition du plan d’adressage
2 - Configuration du rôle Service Provider
    - 2a) la brique Apache
    - 2b) La brique shibboleth
3 - Branchement sur la fédération de test
4 - Configuration du service de découverte
5 – Configuration du rôle de reverse-proxy
6 – Illustration avec https://mon-appli.plbs.fr
7 – Illustration avec GLPI

1- Définition du plan d'adressage

Notre reverse proxy / service provider

- sp.plbs.fr en ip publique accessible depuis internet et connu de la FER

Les noms d'hôte de nos applications visibles par les clients (Frontend) :

- mon-appli.plbs.fr
- glpi.plbs.fr

=> en ip publiques accessibles depuis internet

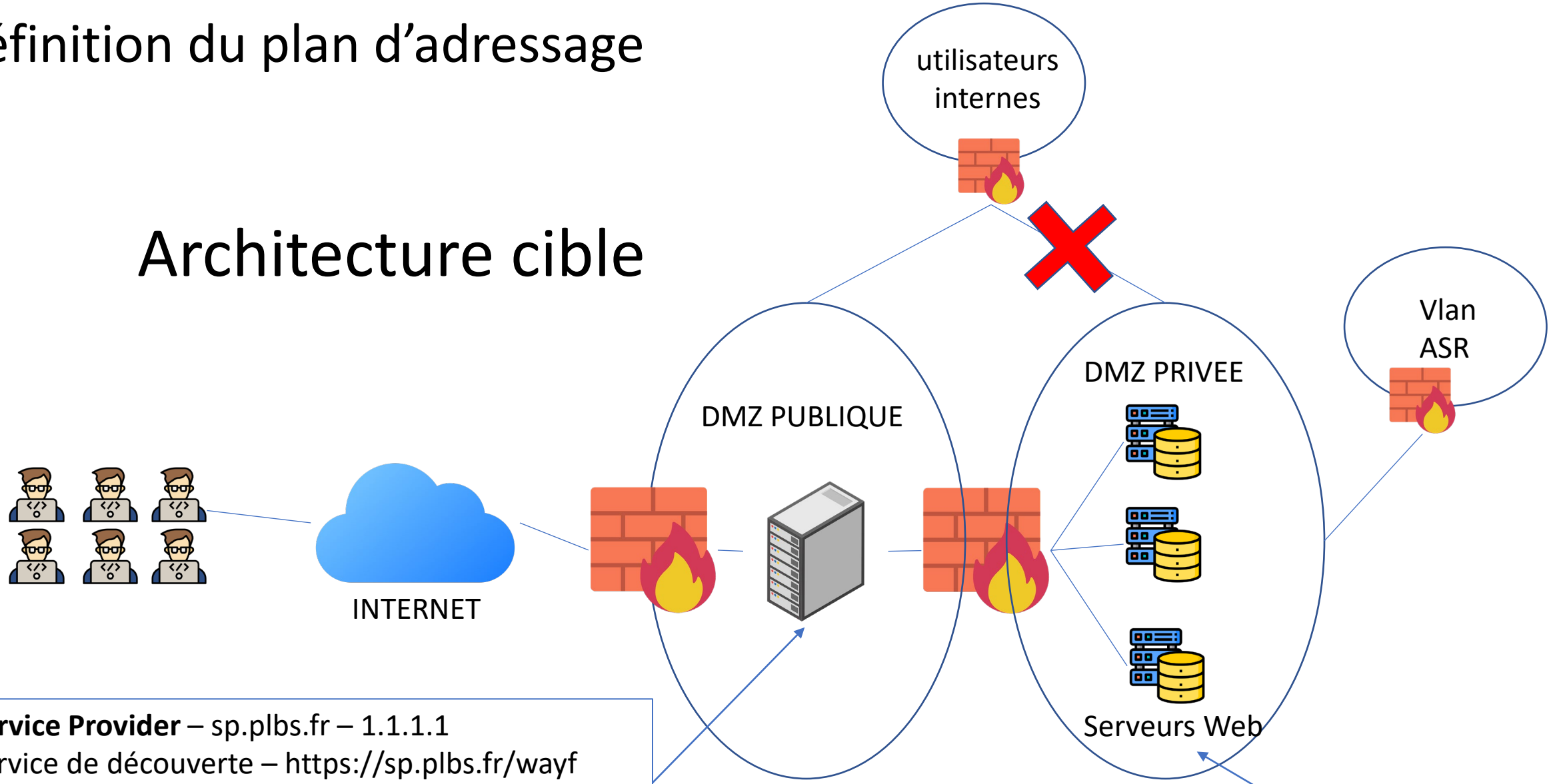
Les noms d'hôtes « rééls » de nos applications (Backend)

- int-mon-appli.plbs.fr
- int-glpi.plbs.fr

=> en ip privées accessibles uniquement depuis le reverse proxy (et le vlan d'administration ASR)

1- Définition du plan d'adressage

Architecture cible



Service Provider – sp.plbs.fr – 1.1.1.1
Service de découverte – https://sp.plbs.fr/wayf
vhost https://glpi.plbs.fr – 1.1.1.2
vhost https://mon-appli.plbs.fr – 1.1.1.3

http[s]://int-glpi.plbs.fr – 10.0.0.20
http[s]://int-mon-appli.plbs.fr – 10.0.0.30

2a - Configuration du rôle Service Provider : la brique Apache

```
@sp:/tmp # sudo apt install apache2 libapache2-mod-shib
@sp:/tmp # a2enmod ssl
@sp:/tmp # a2ensite default-ssl
```

Le module *shibd* est automatiquement activé à l'installation de *libapache2-mod-shib*.
Le fichier **/etc/apache2/conf-enabled/shib.conf** est crée

```
# Ensures handler will be accessible.
<Location /Shibboleth.sso>
  AuthType None
  Require all granted
</Location>

# Used for example style sheet in error templates.
<IfModule mod_alias.c>
  <Location /shibboleth-sp>
    AuthType None
    Require all granted
  </Location>
  Alias /shibboleth-sp/main.css /usr/share/shibboleth/main.css
</IfModule>
```

2a - Configuration du rôle Service Provider : la brique Apache

 # /etc/apache2/conf-enabled/default-ssl.conf

```
<VirtualHost 1.1.1.1:443>
        ServerName sp.plbs.fr
        SSLEngine on
        SSLCertificateFile "/usr/local/etc/apache24/ssl.crt/sp.plbs.fr.pem"
        SSLCertificateKeyFile "/usr/local/etc/apache24/ssl.key/sp.plbs.fr.key"

        ErrorLog "/var/log/httpd-error.log"
        TransferLog "/var/log/httpd-access.log«

    <Location /Shibboleth.sso>
        AuthType None          → pas d'authentification
        Require all granted
        SetHandler shib        → envoie la requête HTTP directement au module shibboleth
    </Location>

</VirtualHost>
```

2b - Configuration du rôle Service Provider : la brique Shibboleth

Editer : **/etc/shibboleth/Shibboleth2.xml**

```
<!-- The ApplicationDefaults element is where most of Shibboleth's SAML bits are defined. -->
    <ApplicationDefaults entityID="https://sp.plbs.fr"
        REMOTE_USER="eppn mail uid"
cipherSuites="DEFAULT:!EXP:!LOW:!aNULL:!eNULL:!DES:!IDEA:!SEED:!RC4:!3DES:!kRSA:!SSLv2:!SSLv3:!TLSv1:!TLSv1.
1">


<!--Configures SSO for a default IdP. To properly allow for >1 IdP, remove
    entityID property and adjust discoveryURL to point to discovery service.
    You can also override entityID on /Login query string, or in RequestMap/htaccess.-->

    <SSO entityID="https://test-idp.federation.renater.fr/idp/shibboleth">SAML2</SSO>

<!-- Session diagnostic service. -->
     <Handler type="Session" Location="/Session" showAttributeValues="true"/>
```

2b - Configuration du rôle Service Provider : la brique Shibboleth

```
<!-- Example of remotely supplied batch of signed metadata. -->
        <MetadataProvider type="XML" validate="true"
                    url="https://pub.federation.renater.fr/metadata/test/all.xml"
              backingFilePath="all-renater-test-metadata.xml" maxRefreshDelay="7200">
            <MetadataFilter type="Signature" certificate="renater-metadata-signing-cert-2016.pem" verifyBackup="false"/>
        </MetadataProvider>
```

```
root@sp:/tmp # curl https://pub.federation.renater.fr/metadata/certs/renater-metadata-signing-cert-2016.pem -O
root@sp:/tmp # mv renater-metadata-signing-cert-2016.pem /etc/shibboleth/
root@sp:/tmp # service shibboleth-sp start

root@sp:/var/cache/shibboleth # ll
total 36496
-rw-r--r--  1 shibd shibd 9303054 Feb 26 09:58 all-renater-test-metadata.xml
-rw-r--r--  1 shibd shibd      37 Feb 26 09:58 all-renater-test-metadata.xml.tag
```

2b - Configuration du rôle Service Provider : la brique Shibboleth

```
<!-- Simple file-based resolvers for separate signing/encryption keys. -->
        <CredentialResolver type="File" use="signing"
            key="sp-signing-key.pem" certificate="sp-signing-cert.pem"/>
        <CredentialResolver type="File" use="encryption"
            key="sp-encrypt-key.pem" certificate="sp-encrypt-cert.pem"/>
```

```
@sp:/tmp # sudo shib-keygen -n sp-encrypt
@sp:/tmp # sudo shib-keygen -n sp-signing


@sp:/tmp # ll /etc/shibboleth/*.pem
-rw-------  1 shibd shibd 1090 Nov 29  2023 /usr/local/etc/shibboleth/renater-metadata-signing-cert-2016.pem
-rw-------  1 shibd wheel 1428 Aug 18  2025 /usr/local/etc/shibboleth/sp-encrypt-cert.pem
-rw-------  1 shibd shibd 2484 Aug 18  2025 /usr/local/etc/shibboleth/sp-encrypt-key.pem
-rw-------  1 shibd shibd 1428 Aug 18  2025 /usr/local/etc/shibboleth/sp-signing-cert.pem
-rw-------  1 shibd shibd 2484 Aug 18  2025 /usr/local/etc/shibboleth/sp-signing-key.pem
```

2 - Configuration du rôle Service Provider : On teste !

```
@sp:/tmp # sudo systemctl restart shibd
@sp:/tmp # sudo systemctl restart apache2

@sp:/tmp # curl https://sp.plbs.fr/Shibboleth.sso/Session
<html><head><title>Session Summary</title></head><body><pre>
A valid session was not found.</pre></body></html>


@sp:/tmp # curl https://sp.plbs.fr/Shibboleth.sso/Metadata
```

3 - Branchement sur la FER

https://registry.federation.renater.fr/

3 - Branchement sur la FER

Ajout d'un fournisseur de service SAML

Présentation | Responsables | Contacts | Fédérations | Données utilisateur | Informations techniques | Conformité | Soumission

Les informations de cet onglet sont destinées à plusieurs audiences:

- les responsables de fédération, afin de vérifier que cette entité correspond aux conditions d'usage de cette fédération, au moment de la demande d'enregistrement
- les responsables de fournisseurs d'identité, afin qu'ils vérifient si ce fournisseur de service correspond aux conditions d'usage de leur organisme, et autorisent l'accès à leurs utilisateurs
- les utilisateurs finaux, afin de consentir à la transmission d'information à caractère personnel vers ce fournisseur de service, au moment de l'accès

En conséquence:

- les informations doivent être compréhensibles pour l'audience visée (c'est-à-dire en anglais pour une fédération internationale comme eduGAIN)
- Les URLs doivent être accessible pour l'audience visée (c'est-à-dire depuis internet, pour une fédération publique comme la Fédération Education/Recherche)

Nom

Le nom doit permettre aux utilisateurs d'identifier ce fournisseur de service.
Cette information est utilisée par les fournisseurs d'identité pour indiquer aux utilisateurs quel service demande à accéder à leurs données personnelles.

NOM (EN FRANÇAIS): *
service provider de test plbs

NOM (EN ANGLAIS):
My service

Logo

Le logo peut utiliser n'importe quel format, et n'importe quelles dimensions. Ces dimensions seront automatiquement calculées si le logo est accessible, autrement elles doivent être saisies manuellement.
Cette information est utilisée par les fournisseurs d'identité pour indiquer aux utilisateurs quel service demande à accéder à leurs données personnelles.

URL:
https://sp.domain.tld/logo.png
Saisissez l'URL de votre logo et validez avec la touche Entrée

LARGEUR: *

HAUTEUR: *

Description

La description doit permettre à un utilisateur de comprendre la finalité de ce service, et s'il est autorisé à y accéder: toute restriction d'audience, par rapport à l'audience de la fédération cible, doit être explicitement mentionnée.
Cette information est utilisée par les fournisseurs d'identité pour indiquer aux utilisateurs quel service demande à accéder à leurs données personnelles.

DESCRIPTION (EN FRANÇAIS): *
Test de fournisseur de service pour PLBS

DESCRIPTION (EN ANGLAIS):

3 - Branchement sur la FER

Page d'information

Cette page fournit des informations génériques sur ce fournisseur de service, telle que sa page d'accueil.

Cette information est utilisée par les fournisseurs d'identité pour indiquer aux utilisateurs quel service demande à accéder à leurs données personnelles.

URL: *

https://sp .plbs.fr

Catégorisation

Ces informations sont utilisées pour classifier le fournisseur de service.

Public du service:

- SERVICE À PORTÉE NATIONALE
- SERVICE COMMERCIAL
- COMMUNAUTÉ NATIONALE (TYPE UNT) OU INTERNATIONALE
- RESSOURCE LOCALE (UNR, PRES, DÉLÉGATION RÉGIONALE)

Type du service:

- ENSEIGNEMENT À DISTANCE
- OUTILS COLLABORATIFS
- DOCUMENTATION ÉLECTRONIQUE
- DISTRIBUTION DE LOGICIELS
- APPLICATION MÉTIER
- ACCÈS WI-FI
- SITE WEB INSTITUTIONNEL
- RESSOURCE EN PRÉ-PRODUCTION

Poursuivre

3 - Branchement sur la FER

Ajout d'un fournisseur de service SAML

Présentation | **Responsables** | Contacts | Fédérations | Données utilisateur | Informations techniques | Conformité | Soumission

Les informations de cet onglet correspondent aux personnes et à l'organisme en charge de cette entité SAML.

Responsables

Ces personnes sont autorisées à gérer cet objet sur le guichet.

⚠ Les utilisateurs sont identifiés par leur attribut eduPersonPrincipalName, une fois connus du guichet. Leur adresse email n'est utilisée que comme un identifiant temporaire, jusqu'à leur première connexion, et ne sera publiée nulle part.

LANGUE: *

français

Cette information est utilisée uniquement pour les notifications envoyées par le guichet.

RESPONSABLES: *

	ADRESSE EMAIL*	NOM	EDUPERSONPRINCIPALNAME
🗑	jeremy.maton@univ-lille.fr	MATON Jeremy	
🗑	karl.oulmi@cnrs.fr	OULMI Karl	

Rattachement à un organisme

L'organisme de rattachement porte la responsabilité légale de cette entité SAML, et il est obligatoire pour l'enregistrement dans la plupart des fédérations de production. Tous les responsables de cet organisme sont aussi responsables de cette entité, en plus de ceux déclarés plus haut.

SÉLECTION DE L'ORGANISME:

CNRS - Délégation régionale Hauts de France

Poursuivre

3 - Branchement sur la FER

Ajout d'un fournisseur de service SAML

Présentation | Responsables | Contacts | Fédérations | Données utilisateur | Informations techniques | Conformité | Soumission

Les informations de cet onglet correspondent à des points de contact publics pour cette entité SAML. Elle sont publiées dans les métadonnées, et sont destinées à être utilisées par les autres participants de la fédération. En conséquence:

- Les adresses email doivent être génériques, persistantes, utilisables par l'audience visée, et suffisament réactive

Contact technique

Point de contact pour les problèmes techniques.

NOM: Sinbios Team

ADRESSE EMAIL: * sinbios@plbs.fr

Contact sécurité

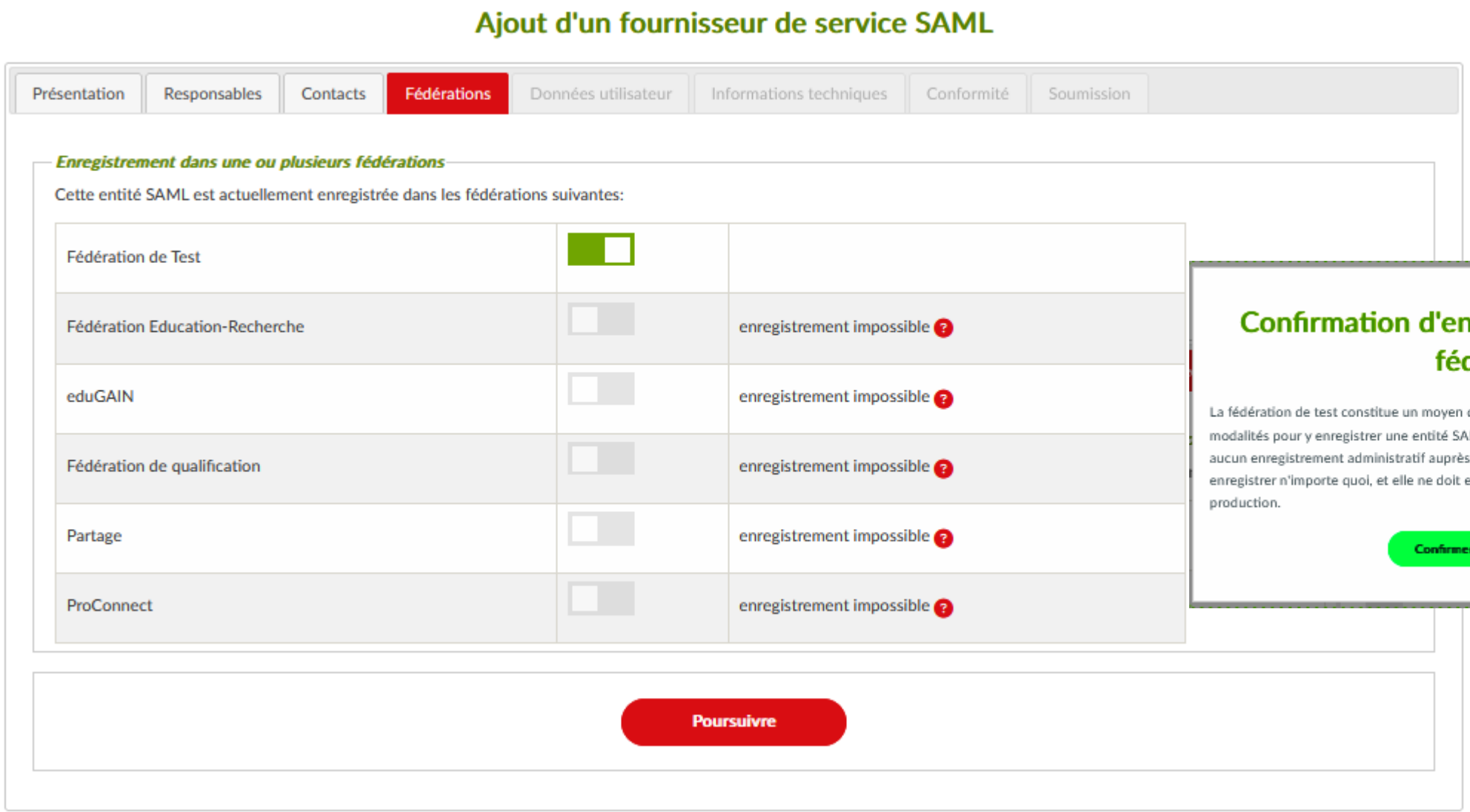
Point de contact pour les problèmes de sécurité. Ceci est nécessaire uniquement en cas d'utilisation d'un processus de traitement différent de celui des problèmes techniques, ou pour la conformité SIRTFI.

NOM:

ADRESSE EMAIL:

Poursuivre

3 - Branchement sur la FER



3 - Branchement sur la FER

SAML service provider https://sp .plbs.fr update

Presentation | Managers | Contacts | Federations | **User data** | Technical information | Compliance | Submission

Information provided on this tab is intended for multiple audiences:

- federation managers, in order to check if this entity meet their federation term of use, at registration request time
- identity provider managers, in order to check if this service provider meet their organization term of use, and allow attribute transfer

It is therefore necessary to provide adequate purpose (identification, autorisation, contact, display, etc.) and mandatory character for each request, so as to evaluate processing fairness.

Requested data

⚠ This page shows all attributes known from the registry, but there is unfortunaly no way to identify which are actually available, given the lack of a generic signalisation mechanism for an identity provider to advertise which attributes he is able and willing to transmit. For identification, we advise to rely on our preconisations. For other purposes, we advise to rely on standardized attribute sets, such as Research and Scolarship specification, or usage statistics for target federations.

NAME*	PURPOSE *	MANDATORY *
cn (commonName)	○ IDENTIFICATION ○ AUTHORIZATION ◉ OTHER	☑
displayName	○ IDENTIFICATION ○ AUTHORIZATION ◉ OTHER	☑
eduPersonPrimaryAffiliation	○ IDENTIFICATION ○ AUTHORIZATION ◉ OTHER	☐
eduPersonPrincipalName	◉ IDENTIFICATION ○ AUTHORIZATION ○ OTHER	☑
givenName (gn)	○ IDENTIFICATION ○ AUTHORIZATION ◉ OTHER	☑

3 - Branchement sur la FER

Aparté sur la diffusion des attributs

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

Les attributs diffusés dépendent de l’idp
Ex : avec l’attribut l’EPPN.

3 - Branchement sur la FER

Parameters

IDENTIFIER (ENTITY ID): *

https://sp .plbs.fr

The identifier of your SAML entity within the federation. The naming convention to use are defined in the federation technical framework.

Endpoints

ASSERTION CONSUMER SERVICE ENDPOINTS: *

These URLs are access point from the IdP to the SP; one endpoint for each protocol/profile should be declared. You may define more than one endpoint URL for each profile if your federated service may be accessed from different hosts. Associated index is an associated unique integer so that it can be referenced in a protocol message.

	BINDING*	URL*	INDEX*
🗑	HTTP Post (SAML 2)	https://sp .plbs.fr/Shibboleth.sso/SAML2/POST	1
🗑	ECP	https://sp .plbs.fr/Shibboleth.sso/SAML2/ECP	4
🗑	HTTP Post (SAML 2)	https://mon-appli.plbs.fr/Shibboleth.sso/SAML2/POST NON-BLOCKING WARNING: UNKNOWN SERVER NAME	2
🗑	ECP	https://mon-appli.plbs.fr/Shibboleth.sso/SAML2/ECP NON-BLOCKING WARNING: UNKNOWN SERVER NAME	5

3 - Branchement sur la FER

Certificates

Those certificates are used to secure exchanges between your SAML entity and other federation entities.

SIGNATURE CERTIFICATES:

A signature certificate is used to send authenticated messages to other entities. Such a certificate is not needed for a service provider, excepted for single logout (SLO) support. At most two may be present at once, for rollover purpose.

⚠ Adding or replacing a certificate for an already existing entity is a delicate operation•••

	SUBJECT	EMITTED BY	SERIAL NUMBER	EXPIRATION DATE	KEY LENGTH
	CN=sp	CN=sp	1B:56:36:92:B1:11:7F:9C:D5:€	24/02/2036	3072

ENCRYPTION CERTIFICATE:*

An encryption certificate is used to receive encrypted messages from other entities. Such a certificate is mandatory for a service provider. Only one may be present at once.

⚠ Adding or replacing a certificate for an already existing entity is a delicate operation•••

	SUBJECT	EMITTED BY	SERIAL NUMBER	EXPIRATION DATE	KEY LENGTH
	CN=sp	CN=sp	7A:4B:F9:E6:9B:D9:B7:8F:E3:5	24/02/2036	3072

Continue

3 - Branchement sur la FER

SAML service provider https://sp .plbs.fr update

Presentation | Managers | Contacts | Federations | User data | Technical information | Compliance | Submission

History

Date	Type	Author	Message	Notable changes
26/02/2026	Creation	MATON Jeremy		• Registration in federation *Test federation*
27/02/2026	Update	OULMI Karl	Mise à jour ext-appli	

Update summary: *

This information makes tracking changes easier, as well as validation process.

Submit

3 - Branchement sur la FER

30 minutes

[Guichet de la fédération] Enregistrement d'une entité SAML dans une fédération

Reply | Reply All | Forward | ...

N noreply@renater.fr
To OULMI Karl; jeremy.maton@univ-lille.fr
Thu 2/26/2026 2:57 PM

L'entité SAML https://sp .plbs.fr vient d'être enregistrée dans la fédération Fédération de Test.

Étape suivante

Les informations concernant cette entité vont être incluses dans les métadonnées de cette fédération, de façon à la faire connaitre aux autres entités, mais il faut également la configurer pour charger ces mêmes métadonnées afin que la réciproque soit vraie, et que l'ensemble fonctionne. Ces métadonnées sont disponibles de différentes façons:

- sous forme de fichiers: https://pub.federation.renater.fr/metadata/test
- via le protocole MDQ: https://mdq.federation.renater.fr/test

Pour plus de détails, vous pouvez consulter cette documentation.

Ce message a été généré par le guichet de la fédération d'identité.

3 - Branchement sur la FER : On teste !

https://sp.plbs.fr/Shibboleth.sso/Login

l'idP de test propose plusieurs comptes de test :

- etudiant1 (mot de passe : etudiant1) : profil étudiant en L3 d'histoire,
- lecteur1 (mot de passe : lecteur1) : profil lecteur autorisé (cf bibliothèque universitaire),
- enseignant1 (mot de passe : enseignant1) : profil d'un enseignant
- personnel1 (mot de passe : personnel1) : profil d'un personnel

3 - Branchement sur la FER : On teste !

https://sp.plbs.fr/Shibboleth.sso/Session

Miscellaneous
Session Expiration (barring inactivity): 479 minute(s)
Client Address:
SSO Protocol: urn:oasis:names:tc:SAML:2.0:protocol
Identity Provider: https://test-idp.federation.renater.fr/idp/shibboleth
Authentication Time: 2026-02-27T15:21:04.207Z
Authentication Context Class: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Authentication Context Decl: (none)

Attributes
cn: Dupont Jean
displayName: Jean Dupont
eppn: etudiant1@test-renater.fr
givenName: Jean
mail: jean.dupont@formation.renater.fr
o: formation.renater.fr
ou: maths
sn: Dupont
uid: etudiant1

3 - Branchement sur la FER : On teste !

https://sp.plbs.fr/Shibboleth.sso/Logout

Service d'authentification de test du GIP RENATER

Vous avez été déconnecté des services suivants:

Service Provider PLBS

L'opération de déconnexion est terminée, et aucun autre service ne semble avoir été accédé au cours de cette session.

Pour des raisons de sécurité, veuillez vous déconnecter et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.

Mot de passe oublié?

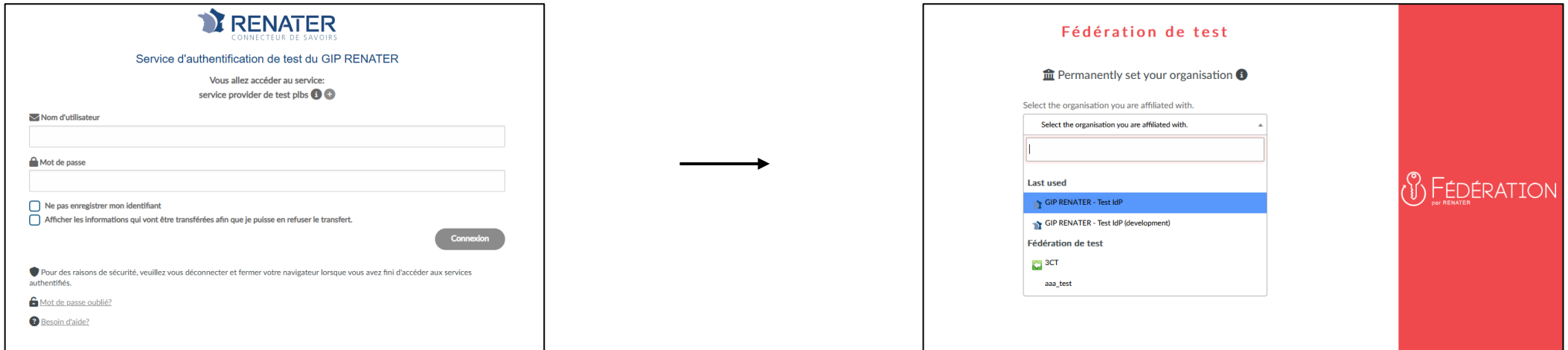
Besoin d'aide?

4 – Configuration du service de découverte

Configuration Shibboleth : ***/etc/shibboleth/Shibboleth2.xml***

```
<!--Configures SSO for a default IdP. To properly allow for >1 IdP, remove
    entityID property and adjust discoveryURL to point to discovery service.
    You can also override entityID on /Login query string, or in RequestMap/htaccess.-->

    <!--<SSO entityID="https://test-idp.federation.renater.fr/idp/shibboleth">SAML2</SSO>-->

    <SSO discoveryProtocol="SAMLDS" discoveryURL="https://discovery.renater.fr/test">SAML2</SSO>
```

https://sp.plbs.fr/Shibboleth.sso/Login



4 – Configuration du service de découverte

Switch (~Renater Suisse) met à disposition sur https://gitlab.switch.ch/aai/SWITCHwayf un service de découverte que l'on peut autohéberger.

```
@sp:/tmp # sudo apt install php-xml php8.3-cli php8.3 libapache2-mod-php8.3
@sp:/tmp # sudo a2enmod enable php8.3
@sp:/tmp # mkdir -p /var/www/html/wayf
@sp:/tmp # curl https://gitlab.switch.ch/aai/SWITCHwayf/-/archive/master/SWITCHwayf-master.tar.gz -O
@sp:/tmp # tar xvfz SWITCHwayf-master.tar.gz
@sp:/tmp # mv SWITCHwayf-master/* /var/www/html/wayf/

@sp:/var/www/html/wayf/ # php bin/update-metadata.php --metadata-file /var/cache/shibboleth/all-renater-test-metadata.xml --metadata-idp-file etc/IDProvider.metadata.php --metadata-sp-file etc/SProvider.metadata.php --verbose
```

Décommenter la ligne ***$auditLogFormat = '[%date %time] %ip %type %selection %idp %return %sp';*** dans *etc/config.php*

4 – Configuration du service de découverte

Editer : **/etc/apache2/sites-enabled/default-ssl.conf**

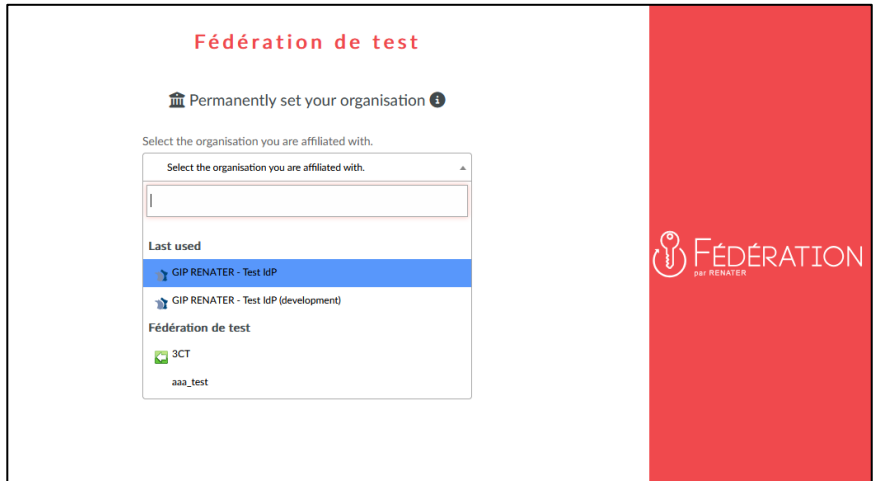
```
<VirtualHost 1.1.1.1:443>
        ServerName sp.plbs.fr
        SSLEngine on
        SSLCertificateFile "/usr/local/etc/apache24/ssl.crt/sp.plbs.fr.pem"
        SSLCertificateKeyFile "/usr/local/etc/apache24/ssl.key/sp.plbs.fr.key"

        ErrorLog "/var/log/httpd-error.log"
        TransferLog "/var/log/httpd-access.log«

    <Location /Shibboleth.sso>
           AuthType None
            Require all granted
          SetHandler shib
    </Location>

    ## Configuration du WAYF
    Alias /wayf /var/html/wayf/www
    <Directory /var/html/wayf/www>
        AllowOverride None
        Require all granted
    </Directory>
</VirtualHost>
```

4 – Configuration du service de découverte

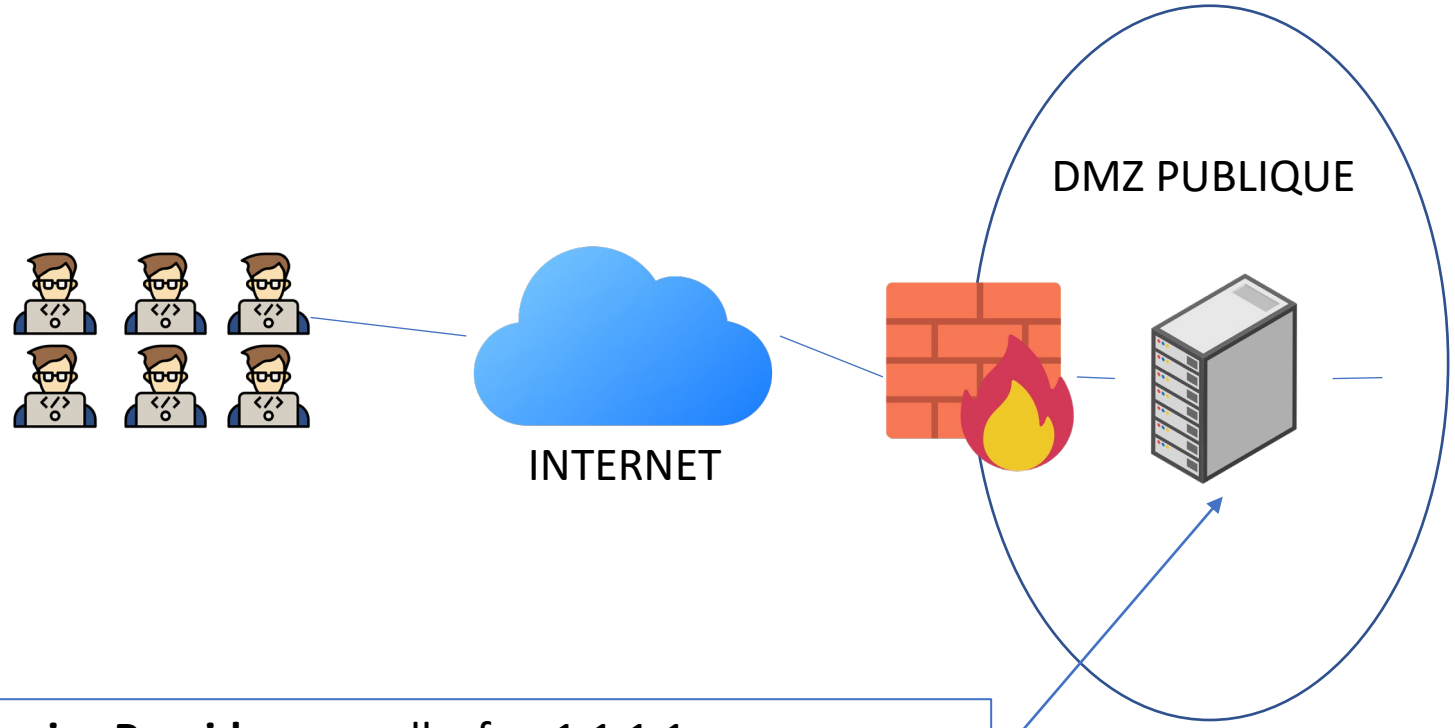
Editer : **/etc/shibboleth/Shibboleth2.xml**

```
<!--Configures SSO for a default IdP. To properly allow for >1 IdP, remove
    entityID property and adjust discoveryURL to point to discovery service.
    You can also override entityID on /Login query string, or in RequestMap/htaccess.-->

    <!--<SSO entityID="https://test-idp.federation.renater.fr/idp/shibboleth">SAML2</SSO>-->
    <!--<SSO discoveryProtocol="SAMLDS" discoveryURL="https://discovery.renater.fr/test">SAML2</SSO>-->

    <SSO discoveryProtocol="SAMLDS" discoveryURL="https://sp.plbs.fr/wayf">SAML2</SSO>
```

https://sp.plbs.fr/Shibboleth.sso/Login



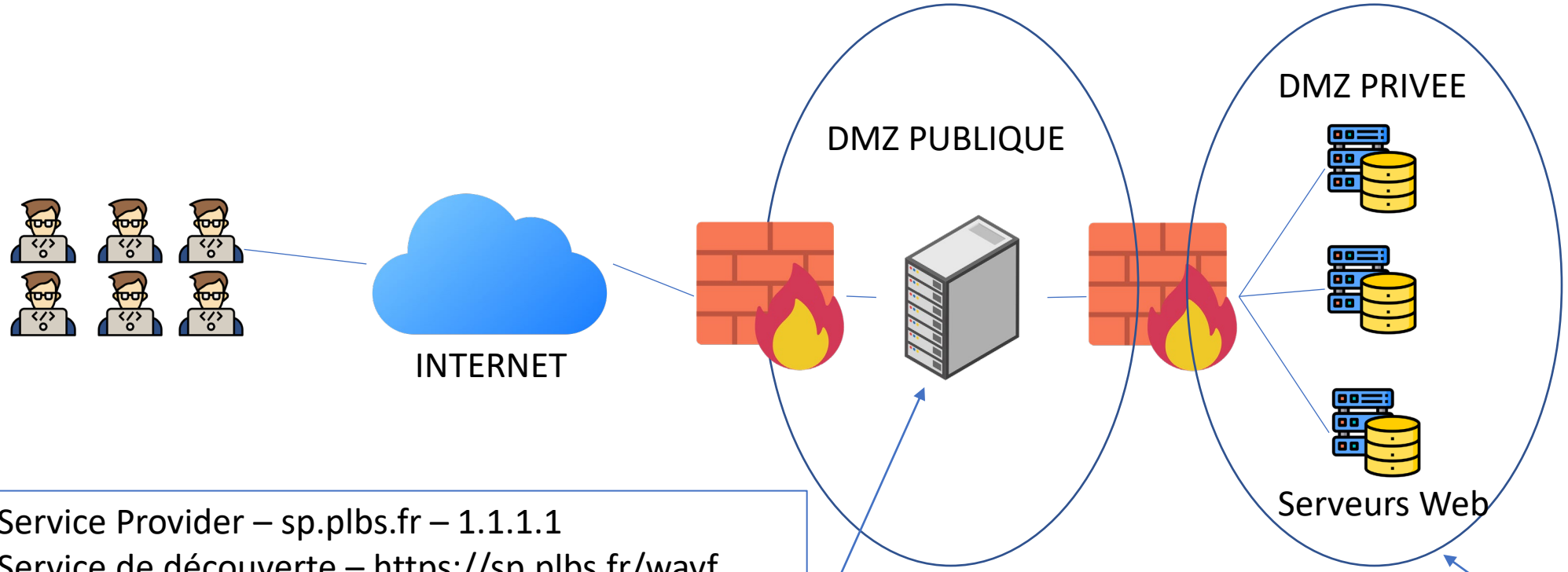
5 – Configuration du reverse proxy



Service Provider – sp.plbs.fr – 1.1.1.1
Service de découverte – https://sp.plbs.fr/wayf

5 – Configuration du reverse proxy

- Créer des VIP sur le serveur reverse proxy
- Créer des vhost Apache en écoute sur ces VIP
- Activer la fonction proxy sur Apache
- Activer l'authentification shibboleth sur ce vhost



Service Provider – sp.plbs.fr – 1.1.1.1
Service de découverte – https://sp.plbs.fr/wayf
vhost https://glpi.plbs.fr – 1.1.1.2
vhost https://mon-appli.plbs.fr – 1.1.1.3

http[s]://int-glpi.plbs.fr – 10.0.0.20
http[s]://int-mon-appli.plbs.fr – 10.0.0.30

5 – Configuration du reverse proxy

- Editer le fichier ***/etc/netplan/00-installer-config.yaml***

```
network:
  ethernets:
    ens192:
      addresses:
      - 1.1.1.1/24 -------→ sp.plbs.fr
      - 1.1.1.2/24 -------→ glpi.plbs.fr
      - 1.1.1.3/24 -------→ mon-appli.plbs.fr
      nameservers:
        addresses:
        …
        …
```

Tester et appliquer la configuration netplan si pas d'erreur

```
@sp:/tmp # sudo netplan try
@sp:/tmp # sudo netplan apply
@sp:/tmp # sudo a2enmod proxy
@sp:/tmp # sudo a2enmod rewrite
@sp:/tmp # sudo a2enmod headers
```

5 – Configuration du reverse proxy

Editer : **/etc/apache2/sites-enabled/default-ssl.conf**

```
<VirtualHost 1.1.1.3:443>
    ServerName mon-appli.plbs.fr
    SSLEngine on
    SSLProxyCACertificateFile "/etc/ssl/certs/HARICA-TLS-Root-2021-RSA.pem"
    SSLCertificateFile "/etc/ssl/certs/mon-appli.plbs.fr.pem"
    SSLCertificateKeyFile "/etc/ssl/private/mon-appli.plbs.fr.key"
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"

    ProxyPreserveHost On → on conserve l'host « mon-appli.plbs.fr » pendant toutes les communications http

    <Location />
        AuthType shibboleth                          → active le module shibbolteh
        ShibRequestSetting requireSession On         → force l'existence d'une session Shibboleth valide
        Require valid-user
        ShibUseHeaders On                            → récupérer les headers shibboleth

        ProxyPass  http://int-appli.plbs.fr/
        ProxyPassReverse  http://int-appli.plbs.fr/        → Masque le nom d'hôte interne au client
    </Location>
```

5 – Configuration du reverse proxy

Editer : **/etc/apache2/sites-enabled/default-ssl.conf** (suite)

Toujours dans <VirtualHost 1.1.1.3:443>

```
    <Location /Shibboleth.sso>
        SetHandler shib          → la requête est traitée par le module shib
        AuthType Non             → aucune authentification nécessaire
        Require all granted      → accès autorisé à tout le monde
    </Location>
</VirtualHost>
```

5 – Configuration du reverse proxy

```
<VirtualHost 1.1.1.3:443>
    ServerName mon-appli.plbs.fr
    SSLEngine on
    SSLProxyEngine On
    SSLProxyCACertificateFile "/etc/ssl/certs/HARICA-TLS-Root-2021-RSA.pem"
    SSLCertificateFile "/etc/ssl/certs/mon-appli.plbs.fr.pem"
    SSLCertificateKeyFile "/etc/ssl/private/mon-appli.plbs.fr.key"
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"

    ProxyPreserveHost Off          → on conserve le nom d'host « mon-appli.plbs.fr » pendant toutes les
                                   → communications http

    <Location />
        AuthType shibboleth
        ShibRequestSetting requireSession On
         Require valid-user
        ShibUseHeaders On

        ProxyPass  https://int-appli.plbs.fr/
        ProxyPassReverse  https://int-appli.plbs.fr/
    </Location>
    …
    …
</VirtualHost>
```

6 – Illustration avec mon-appli

```
# vhost sur serveurs internes

<VirtualHost 10.0.0.30:80>
    DocumentRoot "/var/www/html/mon-appli/"
    ServerName int-appli.plbs.fr
</VirtualHost>


# appli.php sur mon serveur int-appli.plbs.fr

<?php echo '<h1>Bienvenue sur mon Appli '.$_SERVER['HTTP_DISPLAYNAME'].'</h1>';
echo '<p><strong>Voici tout ce que je sais sur vous : </strong></p>';
echo '<table>';
foreach ($_SERVER as $key => $value) {
    $fkey='_'.$key;
    echo '<tr><td>'.$key.'</td><td>'.$value.'</td></tr>';
}
echo '</table>';
<a href="/Shibboleth.sso/Logout">[Fermer votre session Shibboleth]</a></p>
?>
```

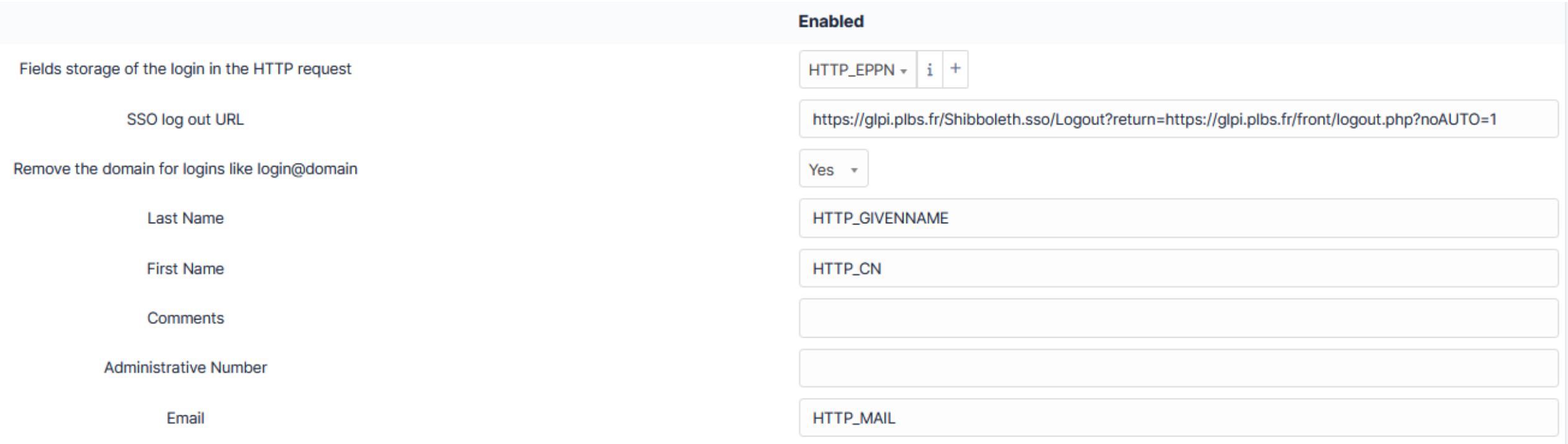
Bienvenue sur mon Appli Jean Dupont

Voici tout ce que je sais sur vous :

HTTP_SHIB_SESSION_ID	_fe56d7aabb83a6935c650856f11a52a2	
HTTP_SHIB_SESSION_INDEX	_4197007075445ada49a9902fba9582b6	
HTTP_SHIB_SESSION_EXPIRES	1772509599	
HTTP_SHIB_SESSION_INACTIVITY	1772484772	
HTTP_SHIB_IDENTITY_PROVIDER	https://test-idp.federation.renater.fr/idp/shibboleth	
HTTP_SHIB_AUTHENTICATION_METHOD	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport	
HTTP_SHIB_AUTHENTICATION_INSTANT	2026-03-02T19:46:37.926Z	
HTTP_SHIB_AUTHNCONTEXT_CLASS	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport	
HTTP_SHIB_HANDLER	https://mon-appli.plbs.fr/Shibboleth.sso	
HTTP_SUBJECT_ID		
HTTP_PAIRWISE_ID		
HTTP_EPPN	**etudiant1@test-renater.fr**	**-> $_SERVER['HTTP_EPPN']**
HTTP_AFFILIATION		
HTTP_ENTITLEMENT		
HTTP_PERSISTENT_ID		
HTTP_CN	**Dupont Jean**	**-> $_SERVER['HTTP_CN']**
HTTP_SN	**Dupont**	
HTTP_GIVENNAME	**Jean**	
HTTP_DISPLAYNAME	**Jean Dupont**	
HTTP_UID	**etudiant1**	
HTTP_MAIL	**jean.dupont@formation.renater.fr**	**-> $_SERVER['HTTP_MAIL']**
HTTP_TELEPHONENUMBER		
HTTP_FACSIMILETELEPHONENUMBER		
HTTP_POSTOFFICEBOX		
HTTP_POSTALCODE		
HTTP_O	**formation.renater.fr**	
HTTP_OU	**maths**	

6 – Illustration avec GLPI

Menu : *Other authentication sent in HTTP request*



Vigilance sur la gestion des sessions SAML vs GLPI !

Merci pour votre attention !