Le portail intranet du Conseil Général du Nord

Mise en place de l'authentification SAML sur le CMS WordPress

Rapport de stage

Stage de 2ème année BTS S.I.O.

Référence : CD59_RapportStage_ERD_MiseEnPlaceSAML.doc
Révision : **1.0**
Etat : **PREL**
Date : 15/12/2023

Référence	Description (Nature et chapitres concernés)
	Tous

Circuit de validation

	Nom	Société	Date
Auteur :	Leclercq Fednail	CD59	15/12/23
Vérificateur :	Laidouni Mehdi	CD59	
Approbateur :			

Historique des révisions

Révision	Date	Modification (Nature et chapitres concernés)	Origine	Auteur
1.0	15/12/23	Création - Tous	CD59	Leclercq Fednail

Documents annexes

Sommaire

1 But, domaine d'application et responsabilités

1.1 Objectifs du document

Ce document a pour objectif décrire les activités réalisées pendant le stage : la mission principale confiée était de remplacer l'authentification par Windows sur deux sites qui ont été produit avec le système de gestion de contenu (C.M.S. pour content managment system) WordPress. Un second projet a été réalisé durant le stage : le prototype d'une application « répertoire d'élève » avec inscription en ligne.

1.2 Périmètre du document

Ce document précise le fonctionnement et le paramétrage du plugin (extension) WordPress utilisé pour mettre en œuvre l'authentification unique en SAML.

L'objectif de cette solution est de pouvoir simplifier l'accès à ces 2 sites Web, en permettant la reconnaissance automatique de l'utilisateur connecté.

Ce document reprend le contexte environnemental du stage, les concepts et définitions nécessaires à la compréhension du sujet ainsi que la description des opérations et du paramétrage de l'extension utilisé pour répondre à ce besoin.

Il comporte en outre une brève description du prototype de l'application « répertoire d'élèves » (TODO : à compléter par description rapide de l'application produite , sous PHP Symfony)

2 Contexte de l'établissement

2.1 Le conseil départemental du Nord

Depuis l'Assemblée constituante du 26 février 1790, la France est découpée en départements (83 à l'origine). On compte aujourd'hui 96 départements métropolitains et quatre départements d'outre-mer (Martinique, Guadeloupe, Guyane et La Réunion) pour un total de 100.

Ce découpage issu de la décentralisation a donné naissance à ce type de collectivités territoriales que sont les départements, au même titre que les communes et que les régions.

Le Nord est le département français comprenant les territoires les plus septentrionaux de la France. Lille en est la préfecture et la plus grande ville. L'Insee et la Poste lui attribuent le code 59. Avec 2 607 746 habitants en 2020, il est le département le plus peuplé du pays, porté par la métropole lilloise qui abrite presque la moitié de sa population

Médecin, ingénieur, gardien des espaces naturels sensibles, agent d'exploitation des routes, secrétaire, agent d'accueil, architecte, contrôleur de gestion, assistant social, médiateur culturel… Plus de 100 métiers sont exercés au Département du Nord.

Le Département du Nord **employait 8 241 agents départementaux au 1er décembre 2022 et 2600 assistants familiaux** accueillant au moins un enfant dans le cadre de la protection de l'enfance.

L'effectif départemental est constitué de 71% de femmes. Elles occupent principalement des fonctions d'encadrement de proximité et leur part progresse sur les fonctions d'encadrement supérieur.

2.2 La direction des systèmes d'information

Le parc informatique est composé de 12 000 postes répartis sur l'ensemble du territoire du Nord, lui-même découpé en 6 arrondissements. Un ensemble de 350 solutions et applications informatiques forme l'écosystème informatique. La direction est organisée en 5 pôles :

- Pôle Sécurité et Architecture
- PGP Pole Gestion patrimoine
- PPA à Pole pilotage et Appui
- PRU à Pole relation utilisateurs
- PSN à Pole Solutions Numériques

Le pôle Solutions Numériques comporte 3 services :

- Service Production et Intégration Application
- Service Ingénierie technique
- Service numérique *(anciennement nommé équipe ressource et développements avant la refonte du schéma directeur, révision de l'organigramme)*

Le stage a été réalisé au sein du service numérique.

2.3 L'équipe ressources et développements devenu Service Numérique

C'est un service composé de 10 personnes avec des profils et fonctions différentes : un responsable de service, 4 chefs de projet informatiques, 2 apprentis ingénieur, 2 concepteurs développeurs et un ingénieur en infographie.

Il est en charge de l'ensemble des sites internet institutionnels (*lenord.fr*), culturels (musée de Flandres par exemple) ou spécifiques (laboratoire départemental), du portail Intranet, de certains référentiels comme les annuaires (exemple annuaire d'entreprise) et sujets transverses (Gestion électronique des documents , archivage électronique) et divers outils de gestion ou d'interfaçage d'applications (Liaison entre la gestion de projets et la gestion financière).

Certains projets innovants sont également menés dans ce service : jeux en ligne pour sensibilisation de certains publics comme les collégiens, application tactile pour les musées.

2.4 Objectif principal : remplacer l'authentification par du SSO *sigle sign-on ou authenfication unique*

Plusieurs sites ont été réalisés sur le CMS WordPress au sein du service numérique. La mission confiée concerne 2 sites nommés La ressourcerie : une version agents et une version assistant familial.

Ces sites sont accessibles en interne et par internet. L'identification des utilisateurs était assurée par un extension par laquelle l'agent devait saisir son identifiant Windows et son mot de passe.

3 Les sites Ressourcerie sous WordPress

3.1 La norme imposée : SAML

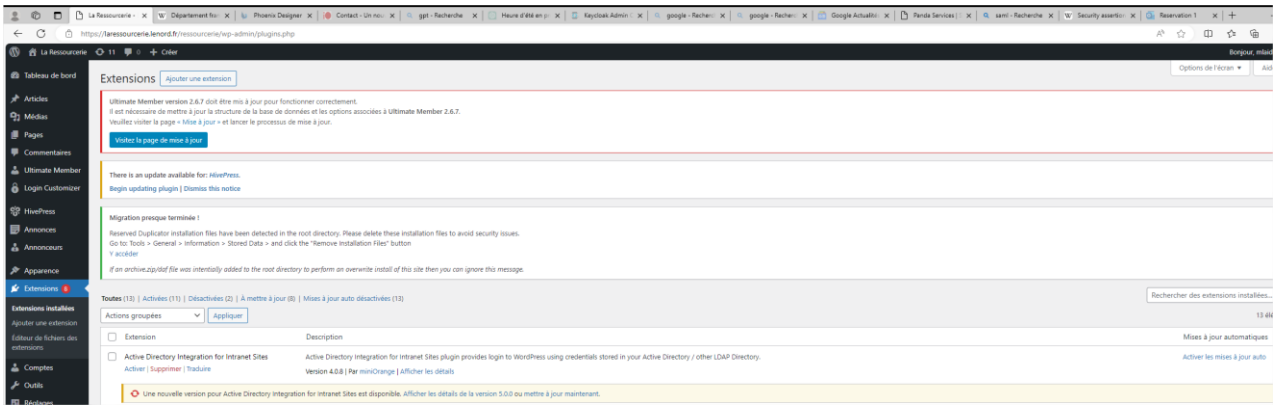
Security assertion markup language (SAML) est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité.

SAML propose l'authentification unique (en anglais single sign-on ou SSO) sur le web. De cette manière, un utilisateur peut naviguer sur plusieurs sites différents en ne s'authentifiant qu'une seule fois, sans pour autant que ces sites aient accès à des informations trop confidentielles.

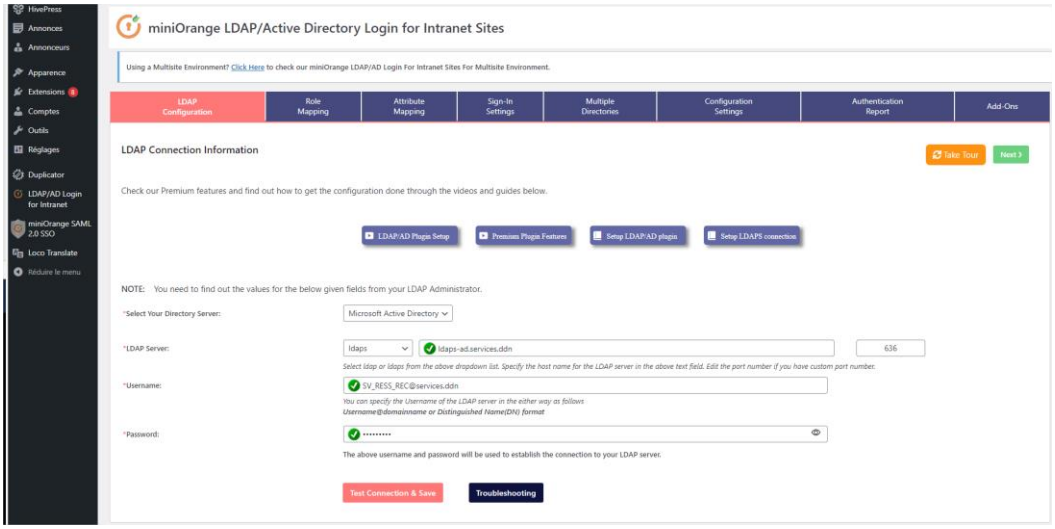
A la création de ces deux sites, une extension pour permettre l'authentification était existante : celle-ci ne convenait pas à la cible souhaitée car elle obligeait l'utilisateur à devoir saisir à nouveau ses identifiants Windows même si celui-ci était déjà connecté au réseau interne. Le service sécurité et architecture a imposé la mise en place de l'authentification unique SSO en utilisant le langage normé SAML.

3.2 Etude et choix de la solution

Back-office du CMS WordPress



La solution précédente était l'extension **Active Directory Intégration for Intranet Sites** configurée ainsi :



L'éditeur de cette extension (en anglais Plug-In) est Mini-Orange et propose une extension qui prend en charge l'authenfication SAML. Le choix de cet éditeur était préférable de par sa renommée et pour assurer les mises à jour régulières et la maintenance de l'extension SAMLw.

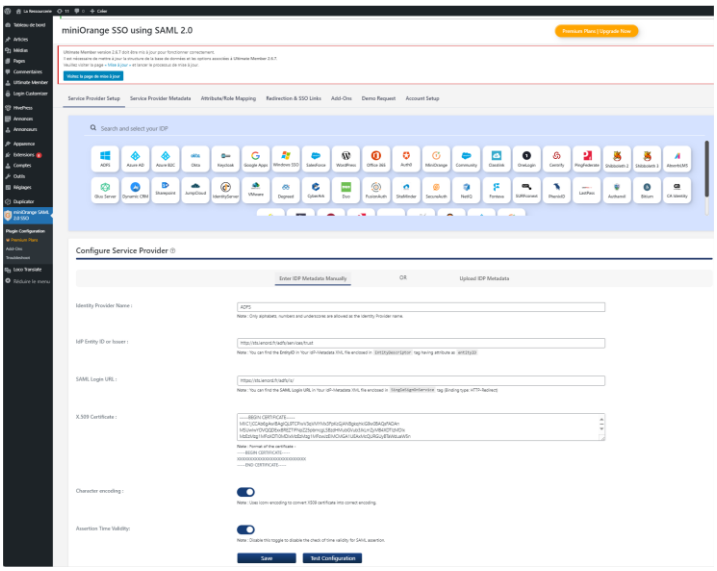
3.3 Mise en œuvre de la solution

3.3.1 Intégration du certificat d'authentification

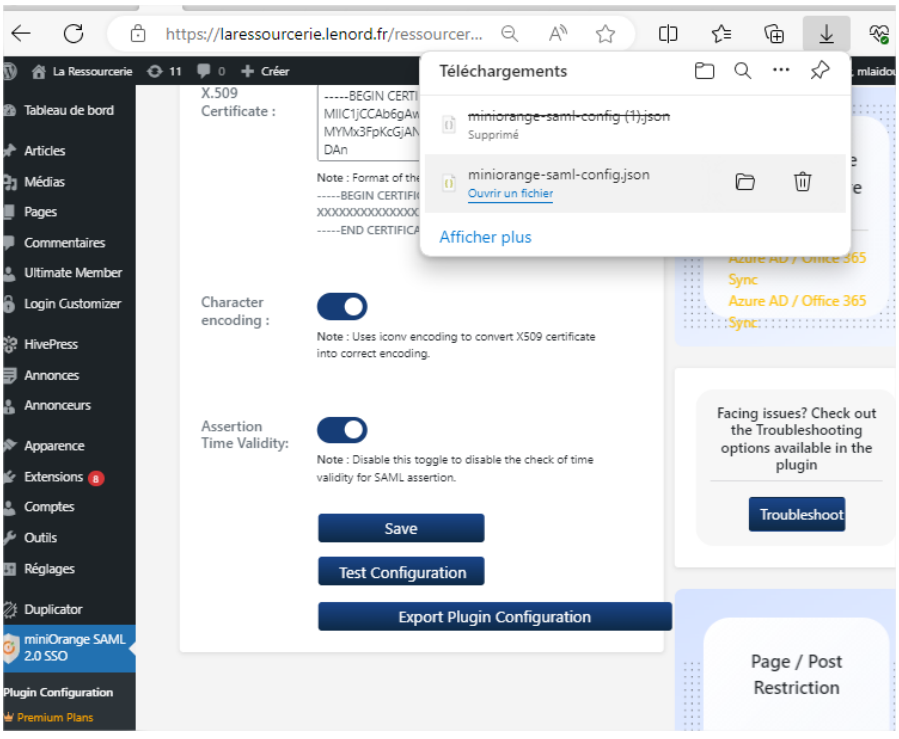
Le certificat d'authentification du Département du Nord nous a été fourni par le chef de projet en charge de l'annuaire d'authentification Windows Active Directory.

Les 3 données **Identity Provider Name , IdP Entity ID or Issuer et SAML Login URL** nous ont également été fournis par ce chef de projet.

Dans la configuration de l'extension miniOrange SSO using SAML 2.0, nous avons intégré ce certificat et les paramètres comme suivant :



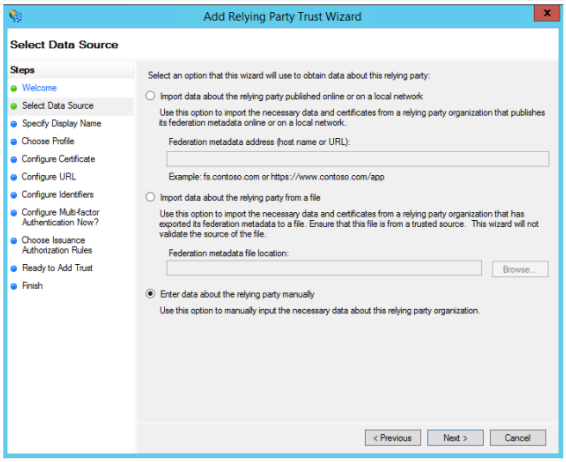
Une fois cette configuration prête, nous avons exporter le paramétrage pour faciliter la création de la liaison dans active directory par le fichier **miniorange-saml-config.json** obtenu par le bouton **Export Plugin Configuration**: (et avons transmis ce fichier au chef de projet Active Directory)



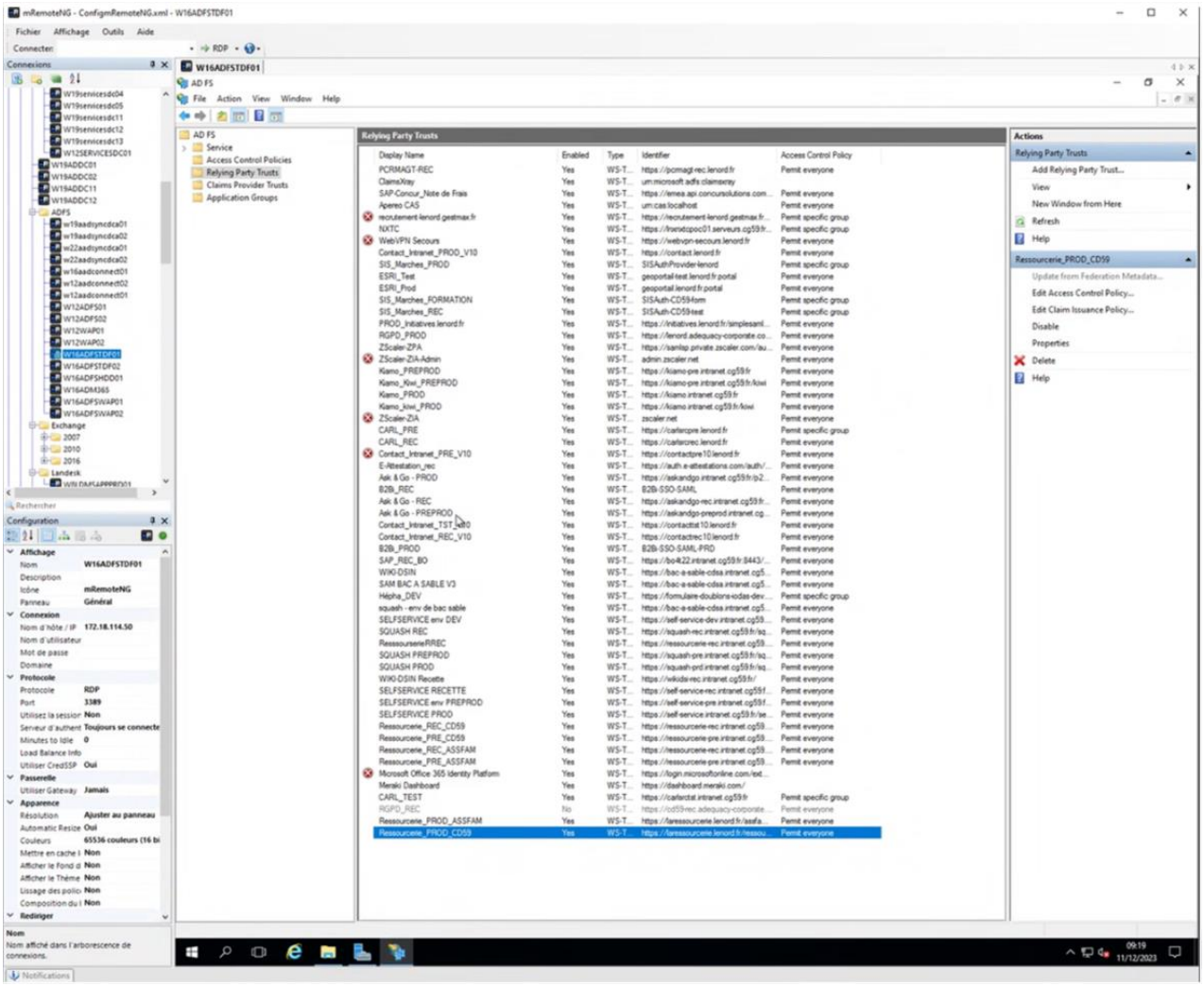
3.3.2 Paramétrage du contrôleur de domaine Active Directory

Le paramétrage de la connexion unique pour ces 2 sites a été réalisé selon une procédure par le chef de projet Active Directory décrite via ce lien :

[Configuration de la connexion unique en utilisant Active Directory avec ADFS et SAML – Aide Zendesk]



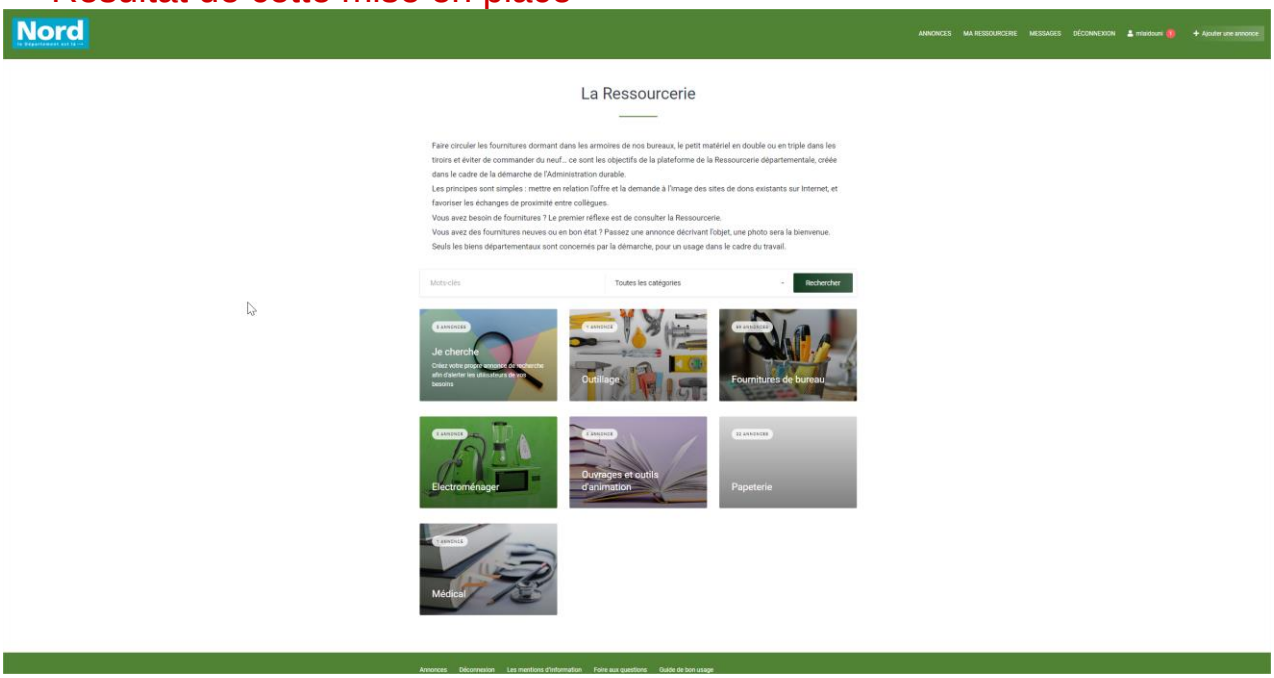
En suivant chacune des étapes, on obtient une chaine de connexion via Active Directory :



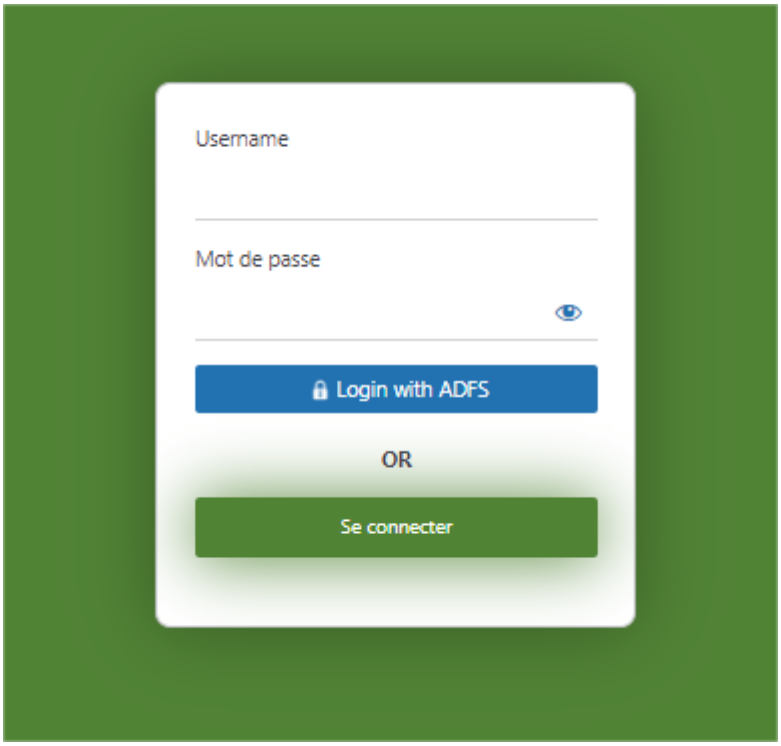
3.3.3 Activation de l'extension

Une fois la liaison créée dans AD, il a fallu activer l'extension par le lien **Activer** :

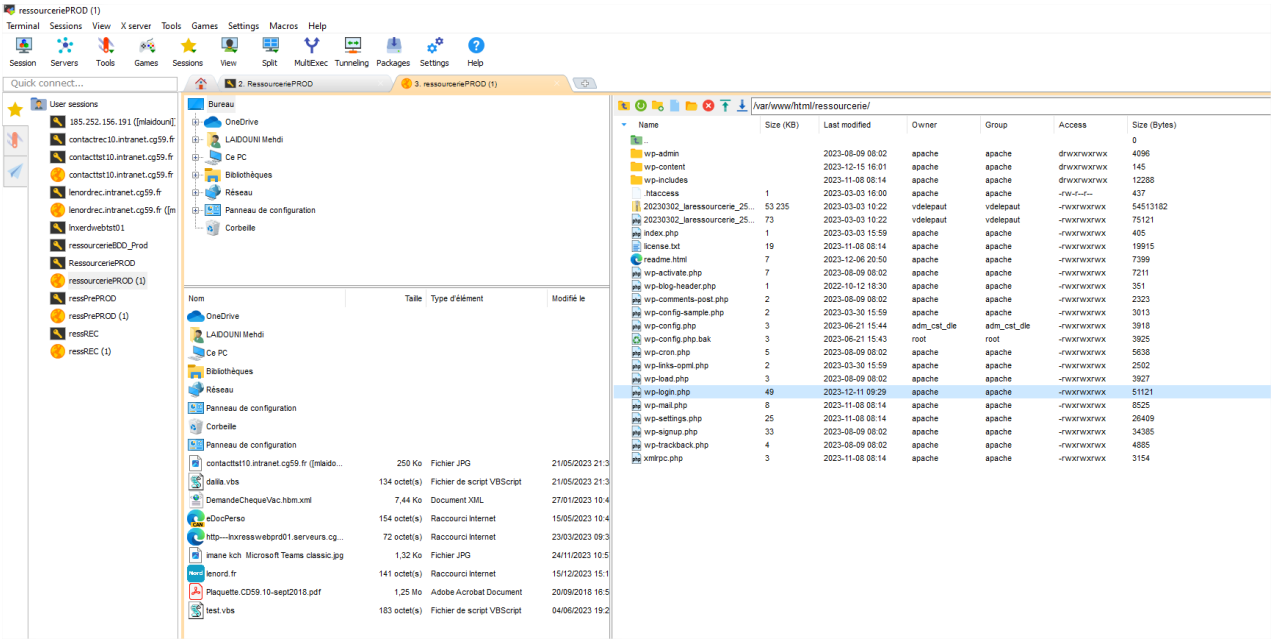
3.3.4 Résultat de cette mise en place



Fenêtre d'authentification unique :



Remarque : le clic sur Login with ADFS est inutile car nous avons ajouté un script automatique pour ce clic dans un fichier nommé wp-login.php :



Lignes ajoutées pour automatiser ce clic :

```
<script>
        document.getElementById("saml_user_login_input").value = "saml_user_login";
        document.getElementById("loginform").submit();
</script>
```

4 Réalisation annexe : application « Répertoire Elèves »

4.1 Framework PHP Symfony

Symfony est un Framework PHP open source largement utilisé pour le développement web. Il a une structure robuste et modulaire pour la création d'applications web évolutives et performantes. Voici un résumé des composants clés de Symfony :

Composer : Symfony utilise Composer, un gestionnaire de dépendances pour PHP, pour gérer les bibliothèques et les packages nécessaires au projet.

Composer simplifie le processus d'installation, de mise à jour et de gestion des dépendances, assurant ainsi un développement efficace et la gestion des versions.

Architecture MVC : Symfony suit le modèle de conception MVC (Modèle-Vue-Contrôleur), ce qui permet de séparer les préoccupations et d'organiser le code de manière structurée.

Le modèle représente les données et la logique métier, la vue gère l'affichage, et le contrôleur gère la logique de traitement des requêtes et des réponses.

Composants Symfony : Symfony est composé d'un ensemble de composants réutilisables (ClassLoader, HttpFoundation, Routing, etc.) qui peuvent être utilisés indépendamment ou combinés pour répondre aux besoins spécifiques du projet.

Bundles : Les bundles sont des extensions modulaires dans Symfony qui regroupent des fonctionnalités spécifiques. Ils permettent d'ajouter des fonctionnalités prêtes à l'emploi, comme l'authentification, la gestion des formulaires, etc.

Doctrine ORM : Symfony intègre Doctrine, un gestionnaire de base de données objet relationnel (ORM), facilitant ainsi la manipulation des données de la base de données à travers des objets PHP.

Twig : Symfony utilise le moteur de Template Twig pour gérer la couche de présentation. Twig offre une syntaxe claire et concise pour faciliter la création de vues.

Console Component : Le composant Console permet la création de commandes en ligne pour automatiser des tâches et effectuer des opérations en dehors de l'interface utilisateur.

Sécurité : Symfony propose des fonctionnalités de sécurité intégrées, telles que l'authentification, l'autorisation, et la protection contre les attaques CSRF (Cross-Site Request Forgery).

Symfony, avec l'aide de Composer, offre un environnement de développement flexible, modulaire et bien structuré, ce qui en fait un choix populaire pour la création d'applications web PHP modernes et évolutives.

4.2 Les outils environnements de développements : IDE

Wamp (apache, interpretateur PHP, MySQL avec site MyAdmin) PhpStorm et VisualCode.

4.3 Le prototype d'une application « répertoire d'élève »

Comme je l'ai mentionné plus haut j'avait pour projet annexe de créer un prototype d'une application de répertoire d'élève. L'objectif de cette application était de fournir une plateforme centralisée pour gérer les informations des élèves, y compris leurs coordonnées, leurs performances académiques, et leurs activités parascolaires.

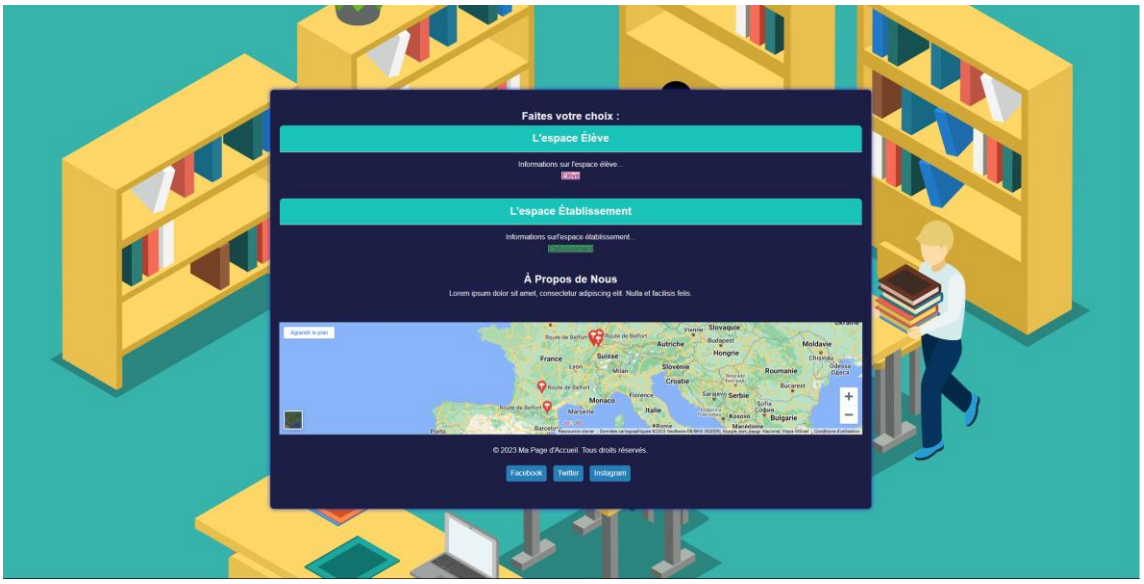
J'ai choisi d'utiliser le langage de programmation PHP et le Framework Web Symfony pour implémenter cette application. La base de données de l'application a été créée à l'aide de la commande

- ➔ **php bin/console doctrine:database:create**

4.4 4.4 Fonctionnalités clés de l'application

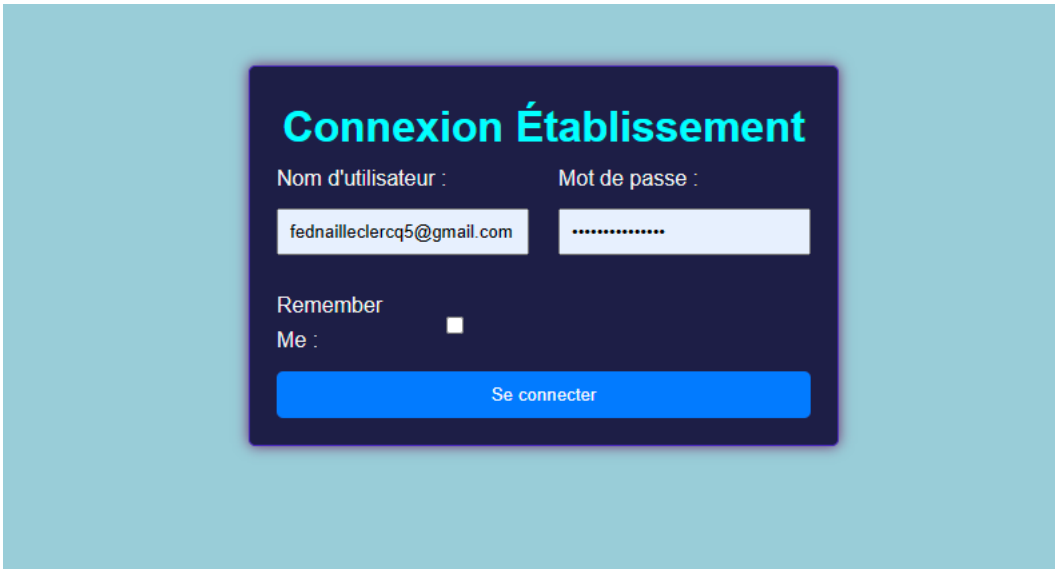
Dans le cadre du développement du prototype de l'application de répertoire d'élèves, plusieurs fonctionnalités clés ont été envisagées pour garantir une expérience utilisateur optimale. Ces fonctionnalités comprennent :

4.4.1 Gestion des profils d'élèves et établissement



L'application permettra aux établissements de créer, modifier et supprimer des profils d'élèves. Ce profil inclura des informations telles que le nom de l'élève, sa classe, ses résultats scolaires et d'autres détails pertinents.

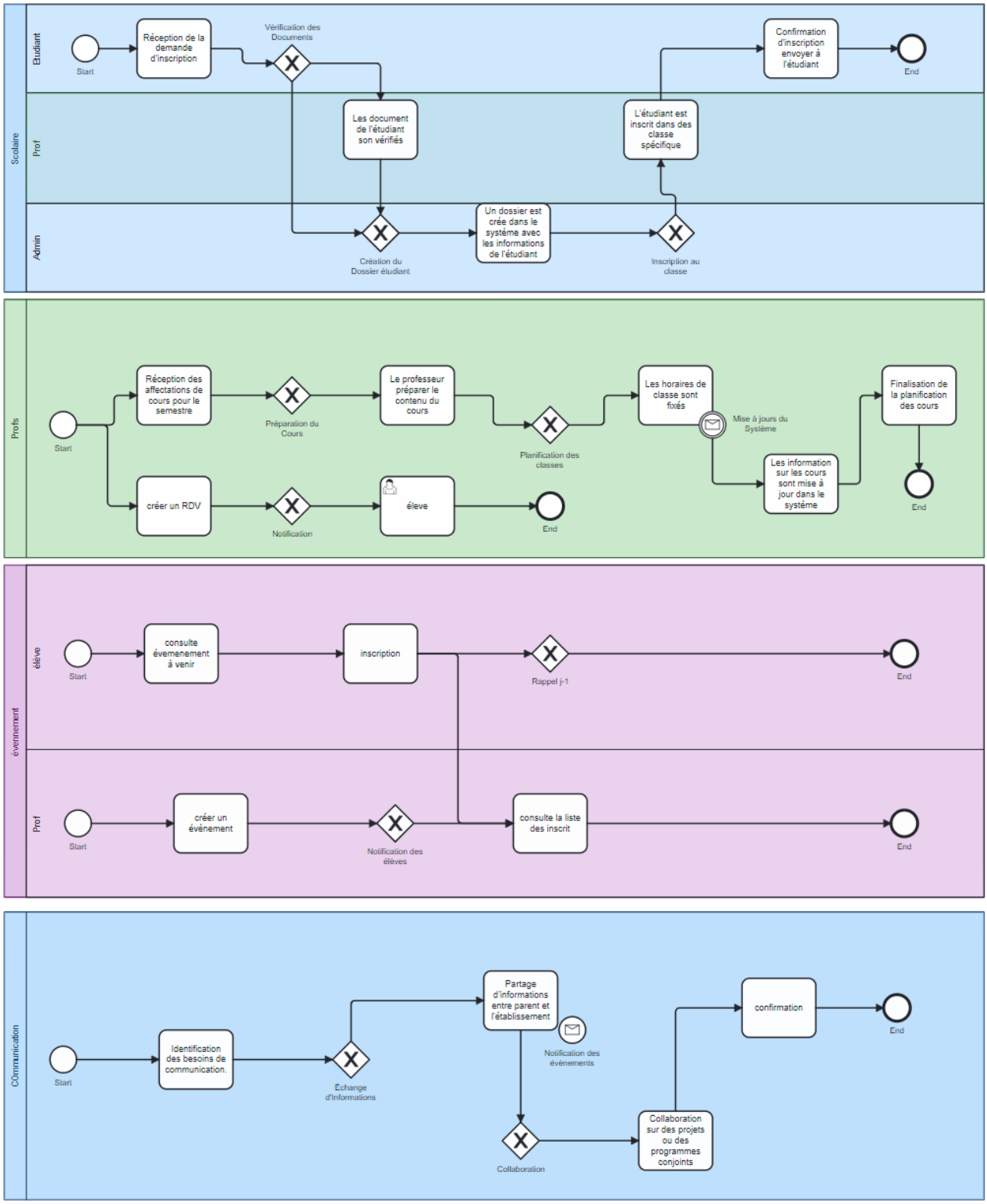
La page login pour accéder à l'espace établissement pour gérer les fonctionnalité clés d'un l'établissement tels que les informations des élèves, y compris leurs coordonnées, leurs performances académiques, et leurs activités parascolaires.



La page login pour accéder à l'espace où vous retrouverait le Tableau de bord qu'un élève aurait besoin tels qu'un calendrier des événements scolaires, une liste des devoirs à faire, une liste des notes, Une liste des absences, un lien vers la messagerie électronique de l'école, un lien vers le site Web de l'école, le Dashboard peut également inclure des informations plus spécifiques, telles que :

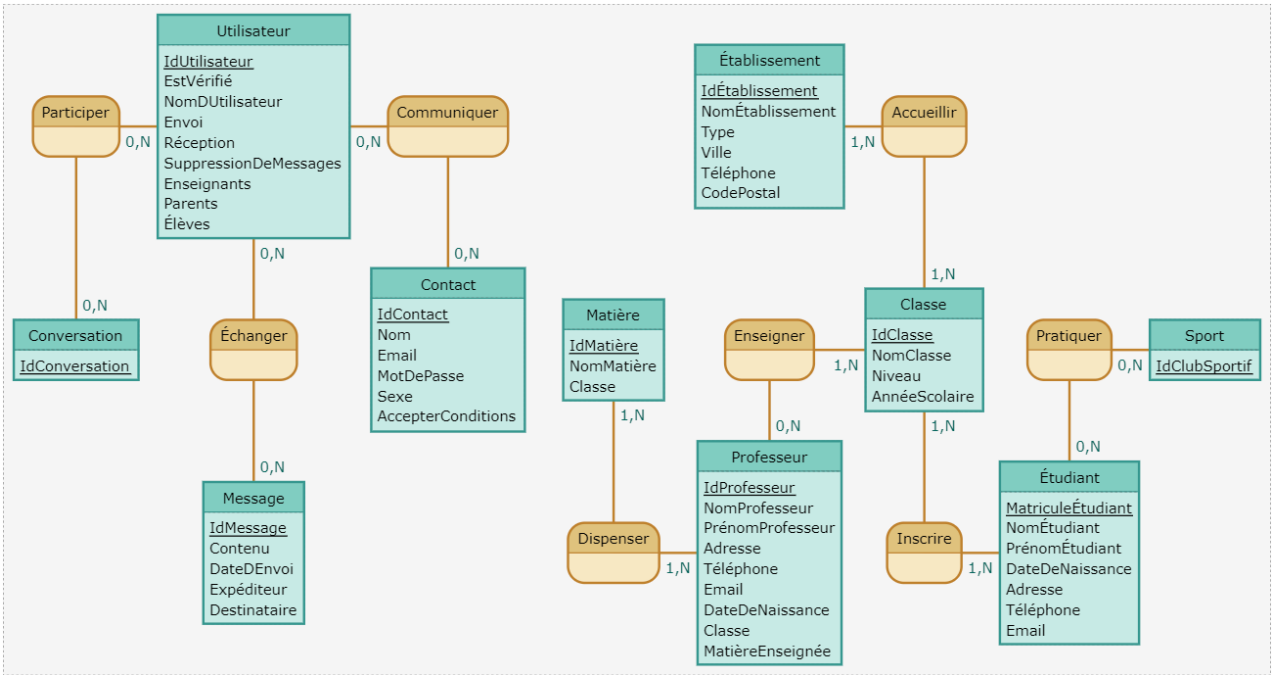
Les résultats des tests, les progrès dans les cours, les activités parascolaires auxquelles l'élève participe

4.4.2 Le Business Process Model (BPM)



4.4.3 LE MCV → MVC

Ce MCD résume la structure de chaque table de votre base de données. Elles suivent la structure relationnelle entre les différentes entités et les liens qui les unissent, typique d'un schéma de base de données. Ce modèle relationnel couvre divers aspects cruciaux tels que la gestion des classes, des étudiants, des professeurs, des établissements scolaires, ainsi que la communication et les activités extrascolaires.



Vue d'implémentation