



PRO Santé Connect JNI 2019

Joachim Metzger

Chef de projet Pro Santé Connect / e-CPS

Sommaire

Chapitre 1 : Pré-étude

Chapitre 2 : Etape 1 – Expérimentation sur le Bac à Sable

Chapitre 3 : Etape 2 – Mise en Production

Chapitre 4 : Exemples



Pré-étude

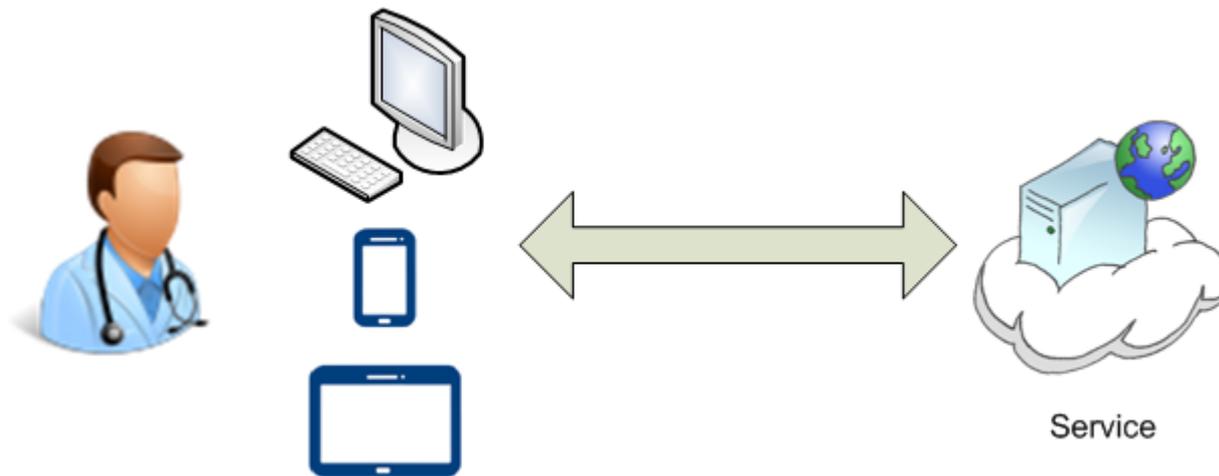


PRO Santé Connect s'appuie sur le standard OpenID. La fondation OpenID (<https://openid.net/>) offre de l'aide à l'implémentation de son standard (<https://openid.net/developers/libraries/>).

Il est indispensable de prendre connaissance de ce standard en début de toute étude technique.

Pré-étude : Vue générale d'un service

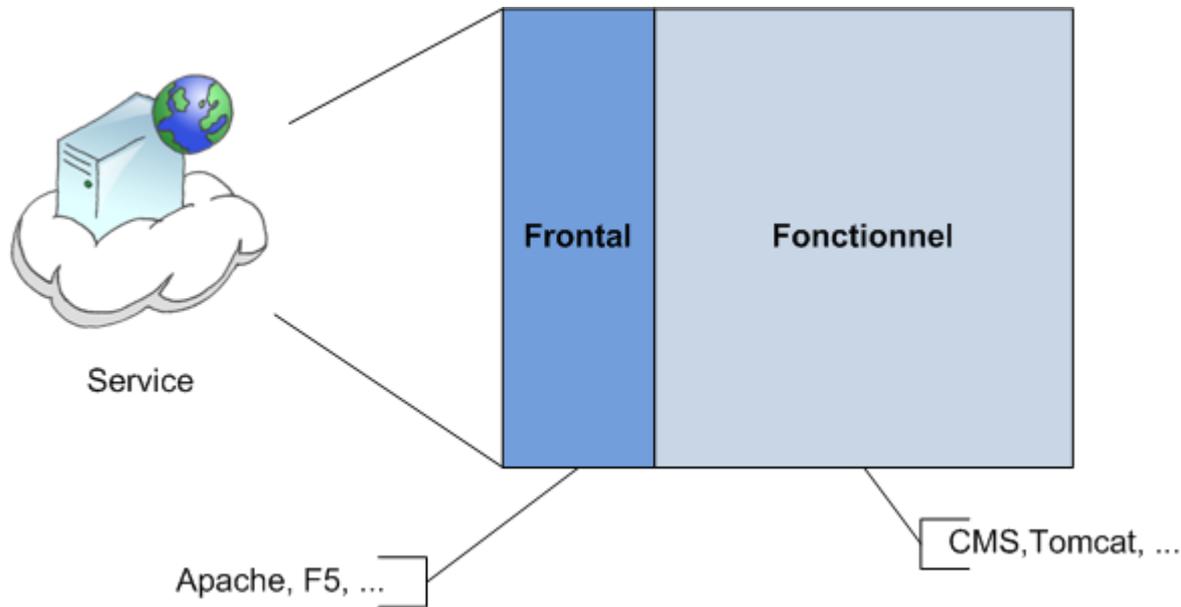
Cet atelier se focalisera sur le cas d'un service en ligne, i.e. accessible depuis un navigateur quelconque.



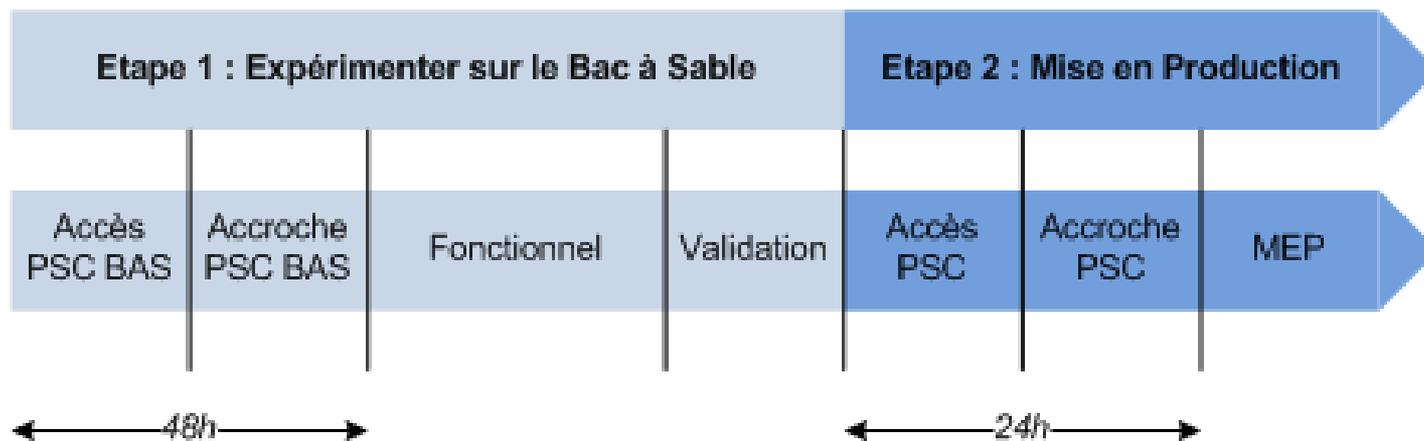
Pré-étude : Architecture générale

D'un point de vue purement général, nous pouvons découper n'importe quel service accessible en ligne en 2 parties :

- Le frontal, qui gère la connexion et les échanges avec le navigateur de l'utilisateur,
- Le fonctionnel, qui gère l'applicatif métier.



Le planning est construit en 2 grandes étapes :





Etape 1



Etape 1 : Expérimenter PRO Santé Connect

L'ASIP Santé met à disposition un environnement Bac à Sable permettant à tout industriel de préparer sa solution à PRO santé Connect.

Cet environnement permet d'utiliser :

- **Des CPS de TEST,**
- **Une application e-CPS BAS sur le Play Store Google**



Un accès au site Intégrateurs est nécessaire pour pouvoir débiter cette étape. L'ASIP Santé peut alors vous assister dans vos démarches techniques.

Etape 1.1 : Demander l'accès au Bac à Sable

En préalable d'une demande d'accès au Bac à Sable, il est nécessaire :

- **de construire préalablement un environnement de développement.**
- **d'ouvrir les flux de cet environnement vers l'extérieur.**
- **d'intégrer et de configurer la librairie OpenID adéquate à votre architecture technique, par exemple :**
 - **Mod_auth_oidc pour Apache,**
 - **Module OpenID Connect sous WordPress,**
 - **Module OpenID Connect sous Drupal.**

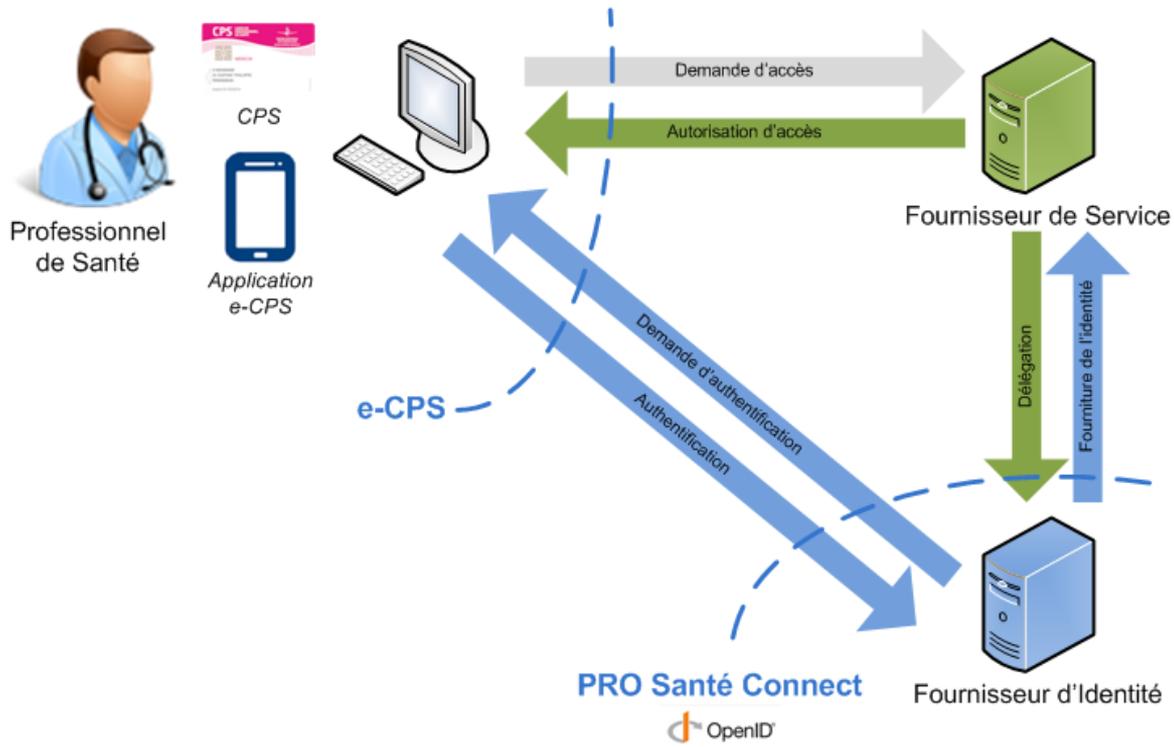
La configuration technique d'OpenID vous fournira alors une URL de redirection qui sera la base technique de votre demande d'accès.

Vous pouvez alors remplir notre formulaire de demande sur <https://integrateurs-cps.asipsante.fr/formulaire/participer-experimentation>.

Etape 1.2 : Accrochage à PRO Santé Connect Bac à Sable

Rappel :

L'URL de redirection permet à PRO Santé Connect de redonner la main au Fournisseur de Service.



Etape 1.2 : Accrochage à PRO Santé Connect Bac à Sable

1. A partir de l'URL de redirection, l'ASIP Santé vous fournit un couple ClientID/Secret,
2. Vous pouvez alors finaliser la configuration grâce aux informations du Mode Opérateur mis à votre disposition

<https://integrateurs-cps.asipsante.fr/pages/prosanteconnect/mode-operatoire>).

Ce document décrit les paramètres (endpoints, scope, ...) OpenID à définir dans votre librairie OpenID.

3. Vous pouvez alors utiliser une CPS de TEST pour tester votre accrochage OpenID à PRO Santé Connect Bac à Sable. Cette étape dure environ 48h.



Etape 1.3 : Intégration des informations à votre fonctionnel

L'hétérogénéité des architectures techniques qui ont intégré PRO Santé Connect, nous permet d'avoir le retour suivant :

- **Les informations du jeton OpenID sont aisément récupérables dans la partie fonctionnelle depuis la partie frontal.**
- **La tâche d'intégration au fonctionnel :**
 - **est totalement dépendante de votre gestion actuelle de l'authentification des utilisateurs dans tous les cas,**
 - **est d'environ 2 mois, validation incluse, si vos comptes utilisateurs s'appuient déjà sur le numéro RPPS de vos utilisateurs.**

PRO Santé Connect supporte actuellement l'authentification par :

- **CPS**
- **et e-CPS**

Par conséquent, l'usage de la CPS est suffisant pour valider techniquement le bon fonctionnement. En effet, quelque soit le moyen d'authentification, PRO Santé Connect renvoie un jeton équivalent.

L'application e-CPS est cependant utile dans le cadre d'une validation ergonomique.



Etape 2



Etape 2 : Mise en Production

La Mise en Production de votre service intégrant PRO Santé Connect se déroule de la même manière que pour l'accès au Bac à Sable.

Une fois en Production, les utilisateurs de votre service pourront se connecter :

- soit grâce à leur CPS,
- soit grâce à leur e-CPS qu'ils auront préalablement activée
- (L'application e-CPS est disponible sur le Google Play et l'App Store).



Aucune demande d'accès à la production ne sera acceptée sans expérimentation préalable avec l'environnement Bac à Sable.

Etape 2.1 : Postuler à PRO Santé Connect

De manière similaire, il est indispensable d'avoir une URL de redirection lors que vous postulez à PRO Santé Connect.

Vous pouvez alors remplir le formulaire afin de Postuler à PRO Santé Connect (*en cours de rédaction, prévu pour décembre 2019*).

Etape 2.2 : Accrochage à PRO Santé Connect

1. A partir de l'URL de redirection, l'ASIP Santé vous fournit un nouveau couple ClientID/Secret,
2. Vous pouvez alors finaliser la configuration grâce aux informations du Mode Opérateur mis à votre disposition

<https://integrateurs-cps.asipsante.fr/pages/prosanteconnect/mode-operatoire>).

Quelques paramètres sont à modifier, notamment les endpoints.

3. Vous pouvez alors tester votre accrochage OpenID à PRO Santé Connect. Cette étape dure environ 24h.



Rappel : les CPS de TEST ne sont pas acceptées; il est donc nécessaire de valider à l'aide d'un utilisateur final.

Etape 2.3 : Mise en Production

La Mise en Production de votre service intégrant PRO Santé Connect est entièrement laissée à votre discrétion.



Exemples



Exemples

Afin de vous présenter la facilité de la phase d'accrochage à PRO Santé Connect, voici 2 exemples basés sur :

1. une maquette d'un service de l'assurance maladie :

- 2 pages Web HTML/PHP,
- Apache.

2. un démonstrateur utilisé lors de notre présentation du 6 septembre 2019 :

- Wordpress,
- Apache.

Dans les 2 exemples, l'hébergement est sous un simple VPS d'OVH tournant sous CentOS 7.

Exemple 1 : Apache/mod_auth_oidc

PROFESSIONNELS DE SANTÉ

CONNECTEZ-VOUS !



Renseignez les champs suivants :

N° d'Assurance Maladie

Mot de passe

[Mot de passe oublié](#)

SE CONNECTER

SE CONNECTER par e-CPS

Maladie

INFOS PATIENT

VIRGINIE MEDECIN RPPS0021354 

IDENTIFIEZ VOTRE PATIENT(E)



Entrez son n° de Sécurité Sociale (13 caractères)

Exemple 1 : Apache/mod_auth_oidc

```
<VirtualHost *:80>
    ServerName amelipro-infopatient.integrateurs-cps.asipsante.fr

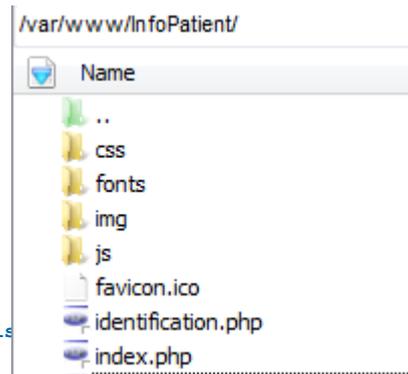
    # OpenID
    #OIDCProviderMetadataURL https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/.well-known/openid-configuration

    OIDCProviderIssuer https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet
    OIDCProviderAuthorizationEndpoint https://wallet.bas.esw.esante.gouv.fr/auth
    OIDCProviderTokenEndpoint https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/token
    OIDCProviderUserInfoEndpoint https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/userinfo
    OIDCProviderJwksUri https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/certs
    OIDCClientID infopatient-demo
    OIDCClientSecret *****
    OIDCAuthRequestParams acr_values=eidas2

    OIDCRedirectURI http://amelipro-infopatient.integrateurs-cps.asipsante.fr/access/openidc
    OIDCCryptoPassphrase 0123456789
    OIDCScope "openid scope_1 scope_2"
    OIDCSSLValidateServer Off
    OIDCRemoteUserClaim preferred_username
    OIDCPassIDTokenAs claims
    #OIDCPassUserInfoAs claims
    OIDCPassClaimsAs environment

    # Time to live in seconds for state parameter i.e. the interval in which the authorization request
    # and the corresponding response need to be processed. When not defined the default of 300 seconds is
    OIDCStateTimeout 1800

    # Interval in seconds after which the session will be invalidated when no interaction has occurred.
    # When not defined, the default is 300 seconds.
    OIDCSessionInactivityTimeout 1800
```



Exemple 1 : Apache/mod_auth_oidc

```
DocumentRoot /var/www/InfoPatient

<Directory /var/www/InfoPatient>
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>

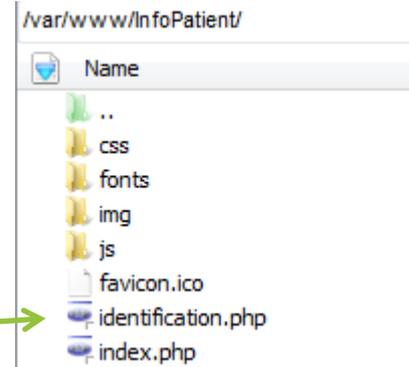
# Redirect URL
<Location /access/openidc>
    AuthType openid-connect
    Require valid-user
</Location>

# identification
<Location /identification.php>
    AuthType openid-connect
    Require valid-user
</Location>

<Location /info-patient.php>
    AuthType openid-connect
    Require valid-user
</Location>

# Log parameters
LogLevel warn
CustomLog logs/amelipro-infopatient.integrateurs-cps.asipsante.fr.log combined
ErrorLog logs/amelipro-infopatient.integrateurs-cps.asipsante.fr.log

</VirtualHost>
```



Exemple 1 : Apache/mod_auth_oidc

PROFESSIONNELS DE SANTÉ

CONNECTEZ-VOUS !

Renseignez les champs suivants :

N° d'Assurance Maladie

Mot de passe

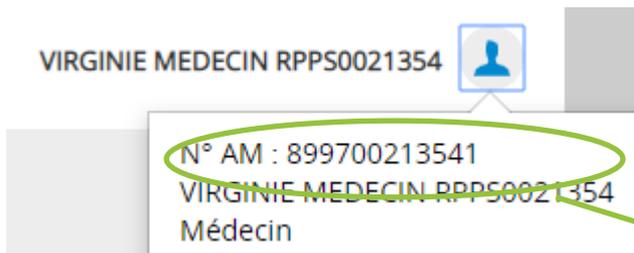
Mot de passe oublié

SE CONNECTER

SE CONNECTER par e-CPS

```
<a href="identification.php" >  
  <button type="button" class="btn-connexion  
  no-margin">  
    SE CONNECTER  
  </button>  
</a>
```

Exemple 1 : Apache/mod_auth_oidc



```
<?php
```

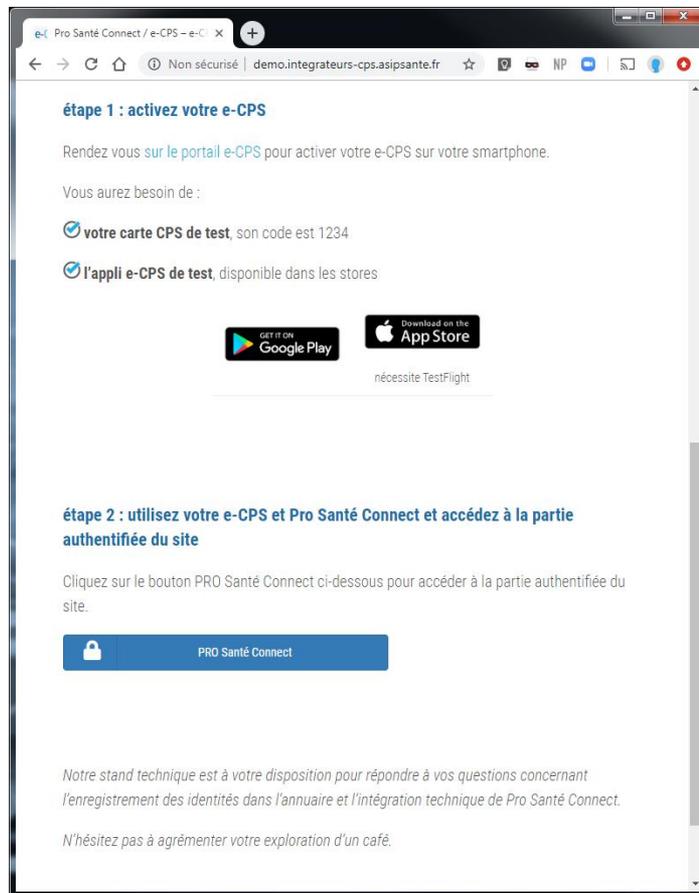
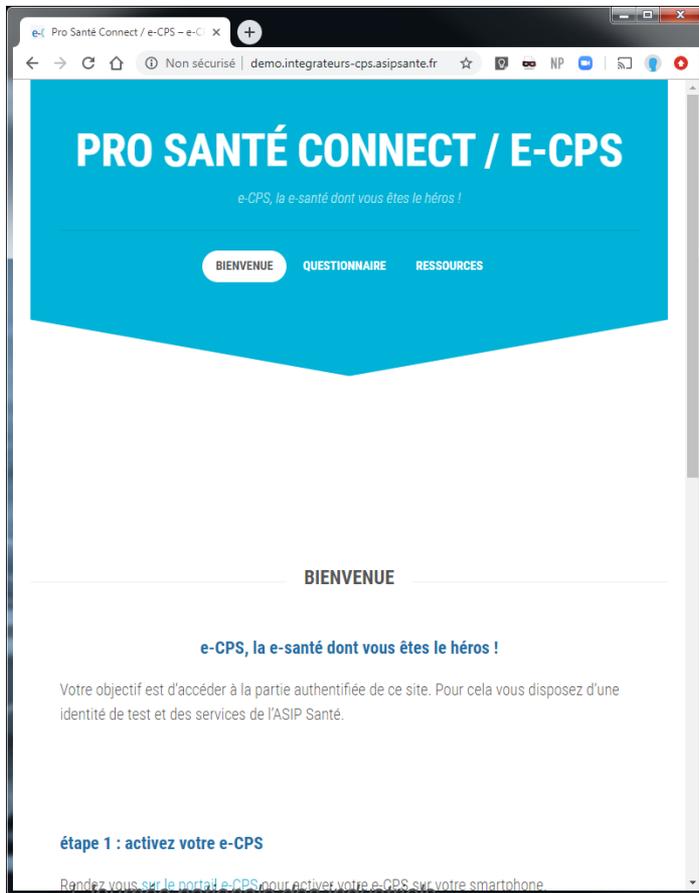
```
$identifiant =  
$_SERVER['OIDC_CLAIM_identifiant'];
```

```
?>
```

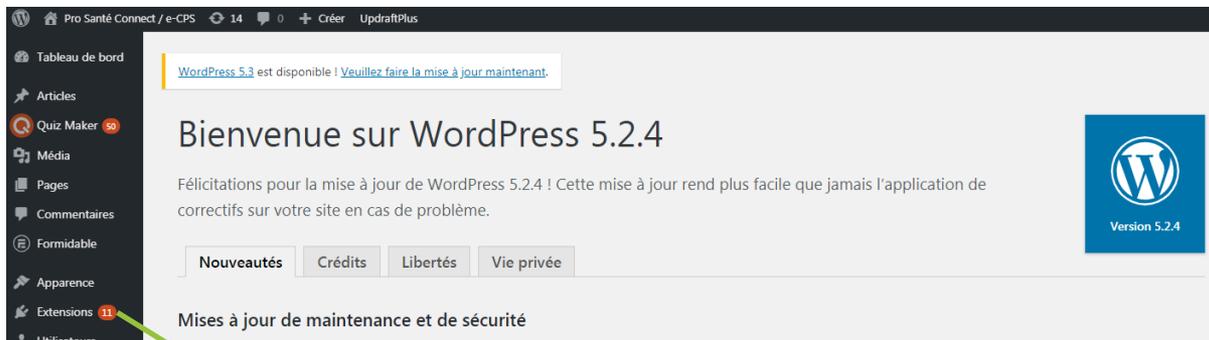
```
...
```

```
N° AM : <?php echo $identifiant; ?>
```

Exemple 2 : WordPress/Module OpenID Connect

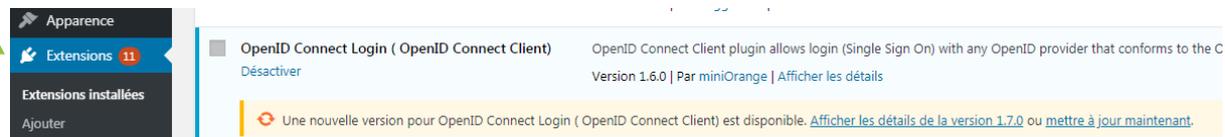


Exemple 2 : WordPress/Module OpenID Connect



Le choix de ce module est arbitraire. Il est reconnu comme très bien intégré et gratuit pour un Fournisseur d'Identité.

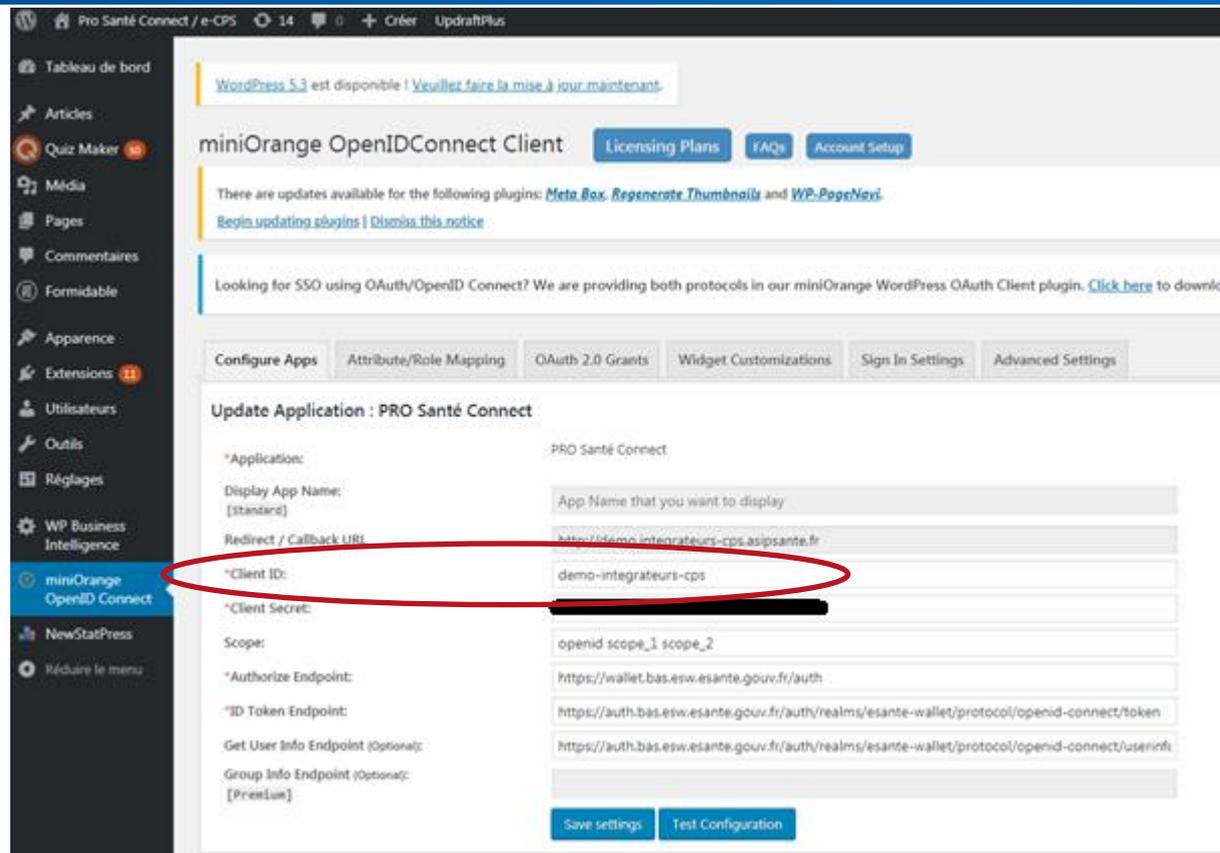
Il en existe beaucoup d'autres.



Exemple 2 : WordPress/Module OpenID Connect

La configuration du module est simple :

Il suffit de le paramétrer avec les informations du mode opératoire (ici avec PRO Santé Connect Bac à Sable).



The screenshot shows the WordPress admin dashboard with the miniOrange OpenID Connect Client plugin configuration page. The left sidebar contains various dashboard widgets, and the main content area displays the configuration for the 'PRO Santé Connect' application. The 'Client ID' field is highlighted with a red circle.

WordPress 5.3 est disponible ! Veuillez faire la mise à jour maintenant.

miniOrange OpenIDConnect Client [Licensing Plans](#) [FAQs](#) [Account Setup](#)

There are updates available for the following plugins: [Meta Box](#), [Regenerate Thumbnails](#) and [WP-PageNavi](#).
[Begin updating plugins](#) | [Dismiss this notice](#)

Looking for SSO using OAuth/OpenID Connect? We are providing both protocols in our miniOrange WordPress OAuth Client plugin. [Click here](#) to download.

Configure Apps Attribute/Role Mapping OAuth 2.0 Grants Widget Customizations Sign In Settings Advanced Settings

Update Application : PRO Santé Connect

*Application: PRO Santé Connect

Display App Name: [standard] App Name that you want to display

Redirect / Callback URL: https://demo.integrateurs-cps.asipsante.fr

*Client ID: demo-integrateurs-cps

*Client Secret: [REDACTED]

Scope: openid scope_1 scope_2

*Authorize Endpoint: https://wallet.bas.esw.esante.gouv.fr/auth

*ID Token Endpoint: https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/token

Get User Info Endpoint (Optional): https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/userinfo

Group Info Endpoint (Optional): [Premium]

[Save settings](#) [Test Configuration](#)

Exemple 2 : WordPress/Module OpenID Connect

The screenshot shows the WordPress admin interface. The left sidebar contains various menu items: Tableau de bord, Articles, Quiz Maker (50), Média, Pages (highlighted), Toutes les pages, Ajouter, Commentaires, Formidable, Apparence, Extensions (11), Utilisateurs, Outils, and Réglages. The main content area displays the configuration for the 'PRO Santé Connect' widget. The title is 'étape 2 : utilisez votre e-CPS et Pro Santé Connect et accédez à la partie authentifiée du site'. Below the title is a text area containing the instruction: 'Cliquez sur le bouton PRO Santé Connect ci-dessous pour accéder à la partie authentifiée du site.' At the bottom, there is a shortcode field with the value: `[do_widget id=mo_openidconnect_widget-4]`.

The screenshot shows the 'PRO Santé Connect' widget on a mobile device. The page title is 'Pro Santé Connect / e-CPS - e-CPS'. The content is divided into two steps:

- étape 1 : activez votre e-CPS**
Rendez vous sur le portail e-CPS pour activer votre e-CPS sur votre smartphone.
Vous aurez besoin de :
 - ✓ votre carte CPS de test, son code est 1234
 - ✓ l'appli e-CPS de test, disponible dans les storesBelow this are buttons for 'GET IT ON Google Play' and 'Download on the App Store', with a note 'nécessite TestFlight'.
- étape 2 : utilisez votre e-CPS et Pro Santé Connect et accédez à la partie authentifiée du site**
Cliquez sur le bouton PRO Santé Connect ci-dessous pour accéder à la partie authentifiée du site.
Below this is a blue button with a lock icon and the text 'PRO Santé Connect'. A green arrow points from the shortcode field in the previous screenshot to this button.

At the bottom, there is a footer with the text: 'Notre stand technique est à votre disposition pour répondre à vos questions concernant l'enregistrement des identités dans l'annuaire et l'intégration technique de Pro Santé Connect. N'hésitez pas à agrémenter votre exploration d'un café.'

Pour toute question sur cette présentation, vous pouvez contacter :



prosanteconnect.editeurs@asipsante.fr

Pour retrouver le guide, flashez ce QR code :





esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'ASIP Santé et s'informer sur l'actualité de la e-santé.

 @esante_gouv_fr

 [linkedin.com/company/asip-sante](https://www.linkedin.com/company/asip-sante)