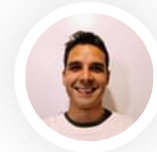
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

PRO SANTÉ CONNECT
Un service du ministère chargé de la Santé

Pro Santé Connect

27/03/2024

Se raccorder à Pro Santé Connect en CIBA



AGENCE DU NUMÉRIQUE EN SANTÉ

Sommaire

1. Présentation générale de Pro Santé Connect
2. Concepts généraux d’OpenID Connect
3. Mise en place d’un flux CIBA dans le cadre de Pro Santé Connect
4. Questions / réponses

AGENCE DU NUMÉRIQUE EN SANTÉ

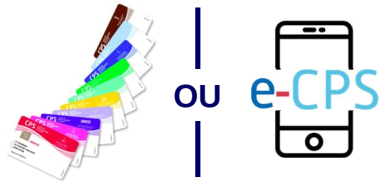
Présentation générale de Pro Santé Connect

Pro Santé Connect : Le fournisseur d'identité de l'ANS pour les Professionnels de Santé

Pro Santé Connect permet une **délégation de l'authentification compatible avec une CPS ou une e-CPS**

Pro Santé Connect **s'appuie sur l'Annuaire National de référence** pour renvoyer les informations, relatives au PS voulant se connecter à un service, au Fournisseur de Service concerné

2 options



1 option

Un des enjeux de Pro Santé Connect est de mettre à disposition des **MIE adaptés aux usages du terrain**

FIDO2
2024

Biométrie
A l'étude

Sans contact
A l'étude

Fournisseur d'identité Pro Santé Connect

Pro Santé Connect réalise l'authentification pour votre service

- Utilisation des différents moyens d'authentification, sans avoir à les développer
- Données d'identification issues de l'annuaire national de référence
- Jeton standard, protocole OpenID. L'Agence fait partie de la communauté OpenID
- Solution d'authentification forte en mobilité
- Disponible sur API.gouv

Authentification forte
validée par l'ANS

Pro Santé Connect : Parcours de raccordement

Prérequis

Juridique

- Personne morale immatriculée dans l'Union Européenne
- Service proposé en langue française et offrant des fonctionnalités nécessitant une identification électronique
- Utilisateurs finaux intervenants dans les secteurs sanitaire, médico-social et social

Technique

- Gestion d'habilitation
- Standard OpenID
- Mise en place d'un serveur intermédiaire (CIBA)

Etape 1

1 sem.

Demander un accès sur API.gouv.fr

- Se rendre sur la **page Pro Santé Connect** du site API.gouv[(1)]
- Remplir une **demande d'accès à l'API Pro Santé Connect**
- **Créer son compte sur iSC afin de pouvoir accéder à son Espace Authentifié**

Etape 2

2 sem.

Commander un certificat de test et raccorder son service au Bac à Sable (BAS)

- **Demander un raccordement au BAS** via la rubrique « Gérer votre service » du Portail Industriel
- Réaliser des **tests d'accrochage** à l'aide de :
  - Une CPx de test commandable via le formulaire F414 de l'ANS ;
  - Une e-CPS de test activable avec une CPx de test ou une identité de test[(2)]
- **Commander un certificat de test** sur la PFCNG (nécessite une carte de test habilitée, un lecteur PC/SC et votre client_id)

Etape 3

2 sem.

Commander un certificat de production et raccorder son service à la production

- **Respecter le référentiel** des exigences de Pro Santé Connect
- **Demander un raccordement à la production** via la rubrique « Gérer votre service » du Portail Industriels
- **Commander un certificat de production** sur la PFCNG (nécessite une carte de prod habilitée, un lecteur PC/SC et votre client_id)

(1) API.gouv est un site permettant de rechercher les API du service public

(2) Le service web EDIT permet de créer des identités de test

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Concepts généraux d’OpenID Connect

Introduction à OpenID Connect

Définition	OpenID Connect (OIDC) est un protocole d'authentification standard sur Internet qui permet aux clients d'obtenir des informations d'identité des utilisateurs finaux.
Origine et standard	Fondamentalement, OIDC est une couche d'identité simple construite au-dessus du protocole OAuth 2.0. C'est un standard ouvert qui a été développé par la Fondation OpenID.
Fonctionnalités	Comparé à OAuth, OIDC fournit des fonctionnalités d'authentification supplémentaires. Pendant que OAuth 2.0 se concentre sur l'autorisation d'accès, OIDC y ajoute l'authentification et l'identification de l'utilisateur.
Flux d'authentification	OIDC définit plusieurs "flux" ou "grant types" pour divers scénarios d'utilisation, tels que les applications web, mobiles, de bureau ou même les API de backend à backend.
JWT	OIDC introduit le concept d'ID Tokens, qui sont des JSON Web Tokens (JWT), fournissant un moyen sécurisé et standardisé pour représenter les revendications (claims) à propos d'une entité (généralement un utilisateur).
Avantages	OIDC favorise une authentification et une autorisation sécurisées, standardisées et simplifiées à travers les services et les applications.

Intégration d’un flux en lien avec vos cas d’usage : Code Flow ou CIBA

Code Flow

- Désigne un **flux standard OpenID de redirection** vers un fournisseur d’identité (dans notre cas Pro Santé Connect) et de renvoie de jeton d’accès
- Est considéré comme **l’un des flux les plus sécurisé de OpenID Connect** vu qu’il ne renvoie pas de jetons d’accès à l’utilisateur
- Est adapté aux **clients web**
- Est **rapide d’implémentation**

CIBA

- Désigne un **flux standard OpenID découplé** permettant d’avoir une authentification initiée dans un appareil et finalisée dans un autre
- **Améliore l’expérience utilisateur** et permet de nombreux usages
- Est adapté aux **clients lourds** et aux **applications mobiles**
- Nécessite la mise en place d’un **serveur intermédiaire**

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Mise en place d’un flux CIBA dans le cadre de Pro Santé Connect

Raccordement technique à Pro Santé Connect

Pré requis

- Prendre connaissance du standard OpenID sur lequel s'appuie PSC
- Disposer d'un environnement de développement
- Ouvrir les flux vers l'extérieur
- Intégrer et configurer la librairie OpenID adéquate à votre architecture technique
- Avoir déployé un serveur intermédiaire (CIBA)
- Disposer d'un client_id et client_secret
- Avoir commandé un certificat mTLS contenant le client_id

Etape 1

- Finaliser la configuration grâce aux informations de la documentation technique
  - Indiquer les endpoints associés aux requêtes
  - Définir les scopes à utiliser
  - Gérer la déconnexion à votre service
- Configurer les échanges mTLS entre le serveur intermédiaire et le serveur Pro Santé Connect

Etape 2

- Réaliser un test d'accrochage à l'aide d'un MIE de test (e-CPS de test, CPS de test)

Etape 3

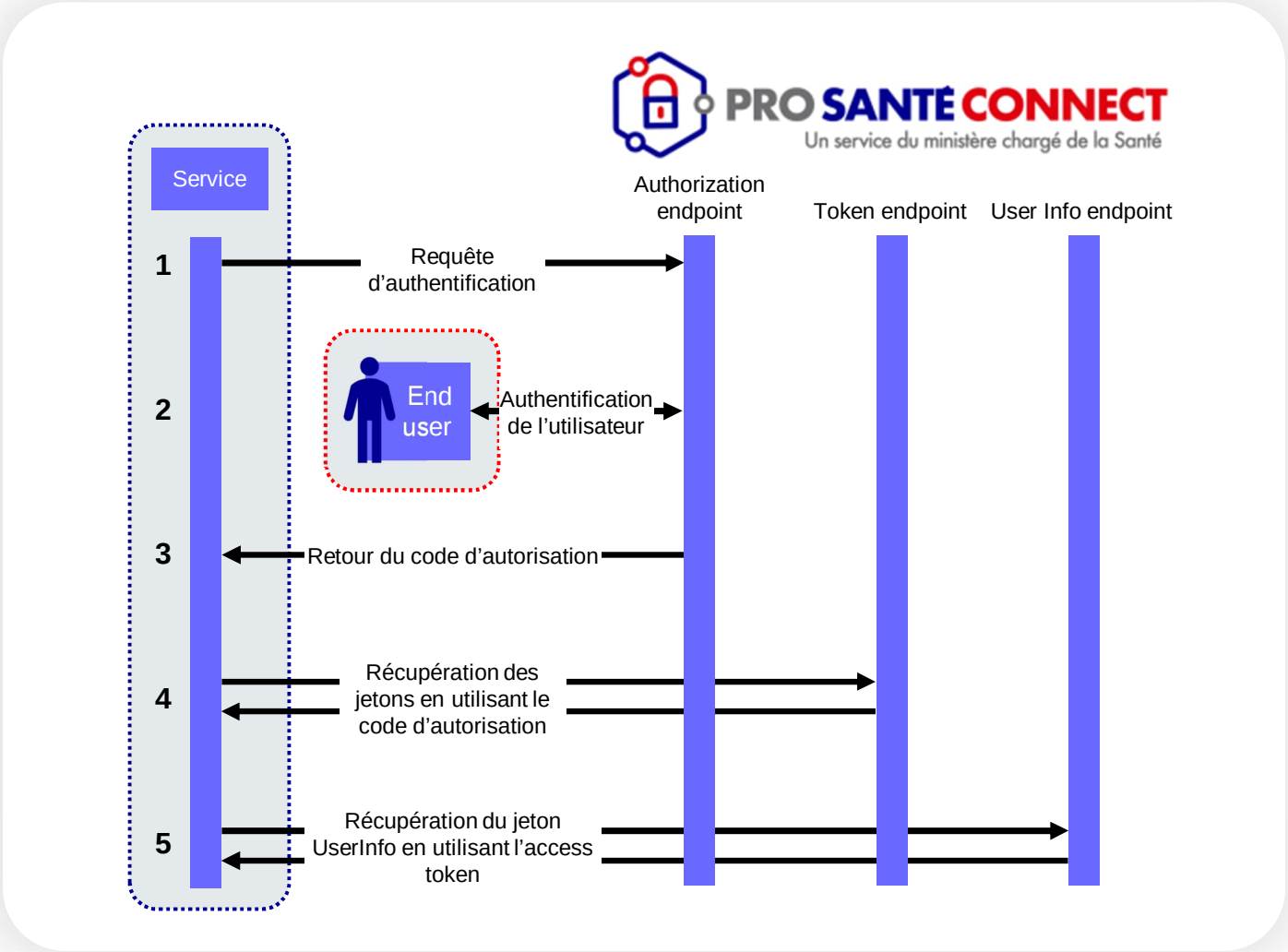
- Intégrer les informations récupérées depuis Pro Santé Connect dans votre back-office afin de gérer les habilitations d'accès à vos services

La communication entre votre serveur intermédiaire et le client lourd est de votre ressort

(1) API.gouv est un site permettant de rechercher les API du service public

(2) Le service web EDIT permet de créer des identités de test

Présentation simplifiée du flux authorization code flow (OIDC « traditionnel »)

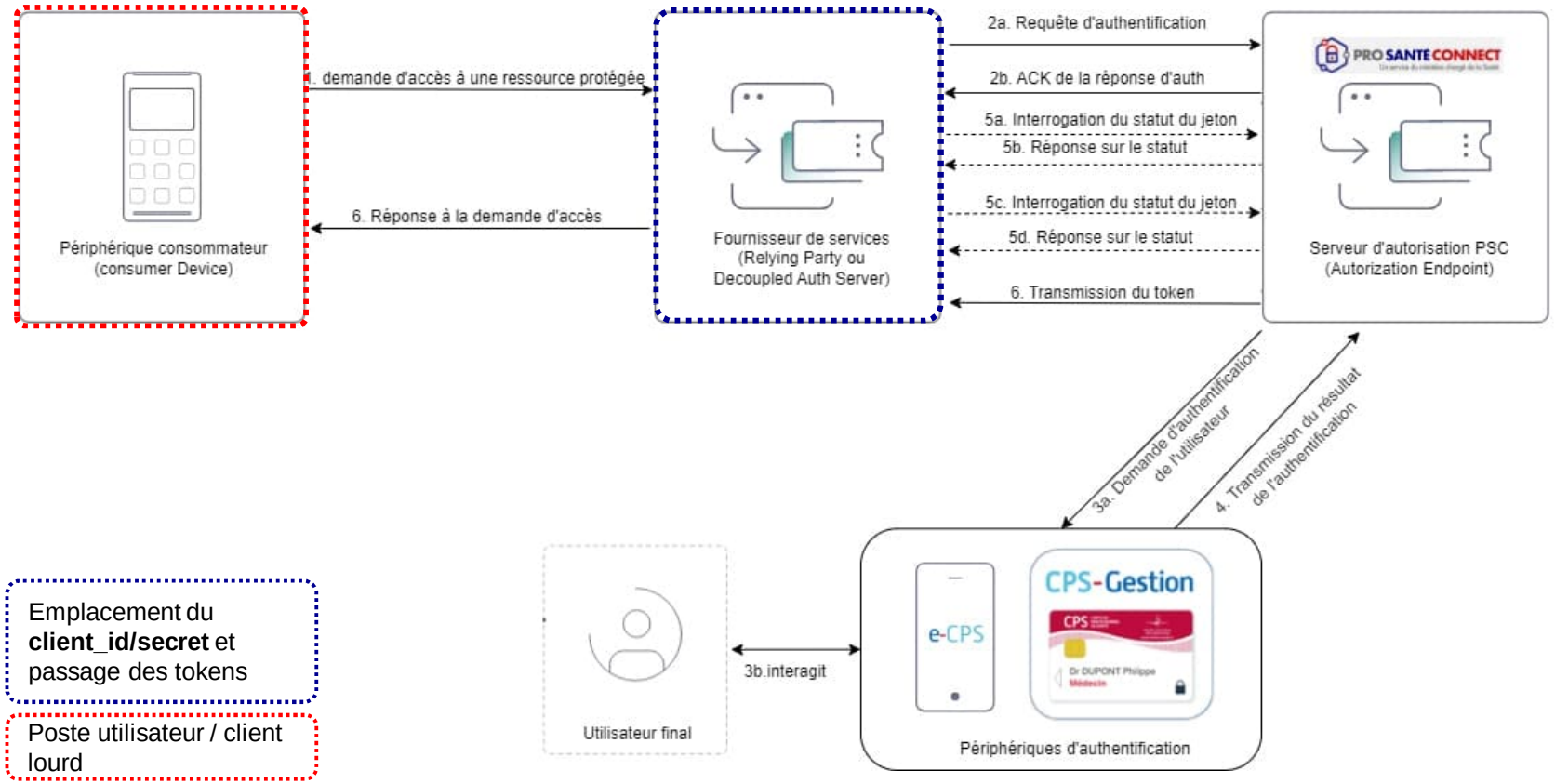


Emplacement du **client_id/secret** et passage des tokens

Poste utilisateur / navigateur web

Présentation du processus CIBA

Schéma du processus d'authentification CIBA



Importance du serveur intermédiaire

Mutualiser le développement afin de simplifier l'intégration de Pro Santé Connect dans plusieurs produits

Regrouper en un seul endroit toutes les configurations sensibles

Proposer une application client mobile dans le respect du référentiel PSC

Proposer un client lourd dans le respect du référentiel PSC

Connexion par carte CPx via CPS-Gestion – Démonstration à travers un logiciel métier

CPS-Gestion

Permet de vous authentifier par carte CPx via un flux CIBA

Disponible sur le Windows Store depuis le 13 mars 2024

Version MacOS à venir

Le MIE est à spécifier au moment où le service fait sa demande d'authentification

L'outil gère à la fois les carte CPx de test et de production et adresse l'environnement correspondant au type de carte insérée

Raccordement fonctionnel : Gestion des habilitations au sein de vos applicatifs

Pro Santé Connect renvoie **les informations relatives à l'utilisateur** souhaitant se connecter à votre service **en fonction de ce que vous lui demandez**

Les informations comprises dans le jeton permettent de **faciliter la gestion des habilitations** de vos utilisateurs en vous permettant de vous baser sur **différents niveaux d'information** afin **d'affiner les différents niveaux d'accès** :

Un PS en particulier
(gestion de compte classique)

Les PS d'une même structure
(donner accès à une base documentaire commune)

Les PS d'une même profession
(applicatif réservé pour une catégorie de PS)

Il est possible d'utiliser des « Scopes » permettant de cibler seulement les informations utiles afin d'alléger le jeton renvoyé

Présentation des bonnes pratiques

Lors des tests, bien pointer vers les endpoints de l'environnement BAS

Ne jamais transmettre votre ClientSecret lors de vos demandes de support

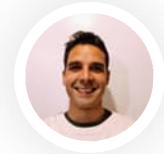
Pour tester une connexion Pro Santé Connect, il est possible d'utiliser :
- **une carte de test**
- **un mobile Android**
- **un émulateur Android**

Différences entre CodeFlow et CIBA

CodeFlow
- **Nom du service**
- **Redirect uri**

CIBA
- **Nom du service**

Les connexions par cartes passent par l'application CPS-gestion disponible sur le store Windows
(à venir sur macOS)



Ressources utiles

1. Portail Industriels pour PSC : https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect
2. Lien vers la doc technique : https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/documentation-technique
3. Lien vers la doc technique CIBA : https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/ciba
4. Collection Postman Pro Santé Connect : https://www.postman.com/red-rocket-401896/workspace/ans-prosanteconnect/overview
5. Page de nos webinaires : https://industriels.esante.gouv.fr/videos?f%5B0%5D=produits_services%3A530
6. Lien vers OpenID : https://openid.net/developers/how-connect-works/

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Questions / réponses

Réponses aux questions du webinaire 1/2

- **Quel jeton est-il interdit de stocker sur le poste client ?**

Le client_secret ne doit jamais être présent sur le poste client, il doit impérativement être stocké sur le serveur intermédiaire. Nous recommandons, dans la mesure du possible, de conserver également le client_id et les jetons d'accès (access_token, id_token, et refresh_token) sur le serveur intermédiaire.

- **Dans CPS-Gestion, l'authentification par CPS (au lieu de e-CPS) a-t-elle fait l'objet d'un aménagement d'API ?**

Si le raccordement à Pro Santé Connect a déjà été réalisé en flux CIBA dans un service, il fonctionnera en e-CPS par défaut. Pour ajouter la possibilité à l'utilisateur de s'authentifier à l'aide de sa CPx, il faut ajouter un paramètre optionnel « channel » (documenté dans la documentation technique) pour spécifier le type de MIE à utiliser.

- **Pour l'installation d'un serveur intermédiaire y-a-t-il une documentation à suivre ?**

Pas de documentation ANS, l'implémentation d'un serveur intermédiaire est du ressort du fournisseur de service, il peut donc l'implémenter de la manière qu'il le souhaite.

- **Comment commander un certificat mTLS ?**

Vous pouvez commander un certificat mTLS via la PFCNG. La procédure est détaillée au chapitre Authentification mTLS de la documentation technique.

- **Peut-on utiliser des certificats utilisés pour le DMP pour faire du mTLS sur Pro Santé Connect**

Pour Pro Santé Connect il faut que le certificat contienne le client_id dans le champ "CN" du certificat. Sur la plateforme de commande de certificats logiciels, le client_id doit être renseigné dans le champ "service applicatif". C'est ce dernier qui alimentera le champ "CN" du certificat. Il faut donc un certificat spécifique à Pro Santé Connect.

Questions et réponses du webinaire 2/2

- **Est-il prévu de mettre à disposition une librairie open source permettant d'implémenter CIBA dans des services ? Si oui en quel langage ?**

L'équipe Pro Santé Connect étudie la possibilité de mettre cela en place, aucune date de mise à disposition ni de langage utilisé ne peut être annoncée à ce stade.

- **Les certificats mTLS deviennent obligatoires en CodeFlow et en CIBA ? Si oui y-a-t-il une date d'échéance ?**

Les certificats mTLS deviennent en effet obligatoires en CodeFlow et en CIBA :

- Avant juin 2024 :
  - En BAS – facultatif (n'hésitez pas à tester leurs déploiements sur vos environnements de test afin de vous familiariser avec le process)
  - En production – non disponible
- Après juin 2024 :
  - En BAS – obligatoire
  - En production – facultatif (passera en obligatoire dans un délai de 6 mois à compter de juin 2024)

- **Dans le cas d'un flux CIBA pour une application mobile, l'authentification se fait forcément en e-CPS ?**

Non pas forcément, il est possible d'utiliser CPS-Gestion et la carte CPx sur un poste Windows, ou macOS (à venir). Mais en usage full mobile, l'utilisateur aura accès uniquement à sa e-CPS.

AGENCE
DU NUMÉRIQUE
EN SANTÉ

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante