AGENCE
DU NUMÉRIQUE
EN SANTÉ

PRO Santé Connect

Mode opératoire technique pour un Fournisseur de Service

Statut : En cours | *Classification : Restreinte* | *Version : v5.4*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Documents de référence

Historique du document

Version	Rédigé par		Vérifié par		Validé par	
1.0	A.LOCQUET Leader Technique IN	Le 22/11/2018	P.KYCIA Chef de projet IN	Le 23/11/2018	J.METZGER Directeur de projet ASIP	Le JJ/MM/AA
	Motif et nature de la modification : **Création du document**					
2.0	J.METZGER Directeur de projet ASIP	23/11/2018	J.METZGER Directeur de projet ASIP	23/11/2018	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification : Modification de forme ; Ajout de la sécurisation du flux					
3.0	A.LOCQUET Leader Technique IN	29/11/2018	P.KYCIA Chef de projet IN	29/11/2018	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification : Prise en compte de « Volet Transport synchrone pour applications mobiles CI-SIS »					
4.0	A.LOCQUET Leader Technique IN	06/12/2018	P.KYCIA Chef de projet IN	06/12/2018	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification : Mise à jour des url du bac à sable					
4.1	J.METZGER Directeur de projet ASIP	11/01/2019	J.METZGER Directeur de projet ASIP	11/01/2019	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification : Ajout de descriptions à date					
4.2	J.METZGER Directeur de projet ASIP	14/01/2019	J.METZGER Directeur de projet ASIP	14/01/2019	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification : Corrections					
4.3	J.METZGER Directeur de projet ASIP	21/01/2019	J.METZGER Directeur de projet ASIP	21/01/2019	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification : Précisions générales					
4.4	J.F.PARGUET	25/01/2019	J.F.PARGUET	25/01/2019	J.F.PARGUET	
	Motif et nature de la modification : Précisions et validation					
4.5	J.METZGER	28/01/2019	J.METZGER	28/01/2019	J.METZGER	

	Directeur de projet ASIP		Directeur de projet ASIP		Directeur de projet ASIP	
	Motif et nature de la modification : Précisions générales					
4.6	J.METZGER Directeur de projet ASIP	29/01/2019	J.METZGER Directeur de projet ASIP	29/01/2019	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification : Précisions générales					
4.7	J.METZGER Directeur de projet ASIP	11/02/2019	J.METZGER Directeur de projet ASIP	11/02/2019	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification : Erratums sur les champs du Authorization Endpoint.					
4.8	J.METZGER Directeur de projet ASIP	19/02/2019	J.METZGER Directeur de projet ASIP	19/02/2019	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification : Erratums sur les scopes					
4.9	J.METZGER Directeur de projet ASIP	12/03/2019	J.METZGER Directeur de projet ASIP	12/03/2019	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification : Mise à jour des visuels ; Ajout du périmètre de compatibilité de l'application téléphone					
5.0	J.METZGER Directeur de projet ASIP	12/06/2019	J.METZGER Directeur de projet ASIP	12/06/2019	J.METZGER Directeur de projet ASIP	
	Motif et nature de la modification :					
5.1	C.SOPHIE AMOA OIDC	15/10/2019	J.METZGER Directeur de projet ASIP	15/10/2019	J.METZGER Directeur de projet ASIP	15/10/2019
	Motif et nature de la modification : Ajout de « Gestion des sessions » ; Ajout de « Refresh Token endpoint » ; Ajout de « Module Apache OIDC »					
5.2	C.SOPHIE AMOA OIDC	11/02/2020	L.Ragain Expert	11/02/2020	J.METZGER Directeur de projet ASIP	11/02/2020
	Motif et nature de la modification : Ajout de schémas temps de session ; Modification des URLs de configuration					
5.3	C.SOPHIE AMOA OIDC	20/02/2020	L.Ragain Expert	25/02/2020	J.METZGER Directeur de projet ASIP	28/02/2020
	Motif et nature de la modification : Durée de validité des tokens BAS ; JSON de retour du UserInfo BAS					
5.4	C.SOPHIE AMOA OIDC	23/06/2020	L.Ragain Expert	24/06/2020	J.METZGER Directeur de projet ASIP	24/06/2020

	Motif et nature de la modification : Modification de forme ; Modification de l'URL de configuration BAS et PROD, modification scope					
	Motif et nature de la modification :					
	Motif et nature de la modification :					

SOMMAIRE

TABLE DES FIGURES

TABLE DES TABLEAUX

1. OBJET DU DOCUMENT

Le présent document rappelle les principes généraux et le positionnement du service PRO-Santé-Connect puis décrit les prérequis et interfaces nécessaires à l'intégration d'un nouveau fournisseur de service (FS) au fournisseur d'identité PRO Santé Connect.

Dans cette version du document, les URLs des endpoints ne sont pas celles de l'environnement cible. Le document sera mis à jour quand elles seront définies et validées.

Les URLs des endpoints correspondent à l'environnement dit « Bac à Sable » destiné aux industriels désirant vérifier l'intégration de PRO Santé Connect.

2. PRESENTATION

2.1. PRO Santé Connect

2.1.1. Général

Pro Santé Connect a pour objectifs de libérer les fournisseurs de service des contraintes techniques de l'authentification en fournissant un service d'authentification à l'état de l'art, conforme aux standards internationaux. Le service supporte différents dispositifs d'authentification (CPS, smartphone, OTP SMS, …) afin de s'adapter aux différentes modalités métier des utilisateurs mais aussi afin de permettre l'évolution des dispositifs d'authentification sans impact sur les fournisseurs de service.

PRO Santé Connect est un service d'authentification délégué au sens du référentiel d'authentification de la PGSSI-S

PRO Santé Connect regroupe un Fournisseur d'Identité (PRO Santé Connect) et un système d'authentification sur smartphone (e-CPS). Il libère les services utilisateurs des contraintes de l'authentification et de sa maintenance sécuritaire tout en garantissant à la fois la conformité réglementaire de celle-ci (PGSSI-S) et au volet transport pour les applications mobiles du CI-SIS.

PRO Santé Connect met en œuvre une technologie identique à celle de FranceConnect tout en propageant les identifiants et les professions / rôles / situations d'exercice des référentiels sectoriels. PRO Santé Connect est un fournisseur d'identité (FI) selon la norme OpenID Connect (OIDC), surcouche du protocole OAuth2.0. Un certain nombre de endpoints REST sont mis à disposition pour effectuer une authentification en suivant cette norme. Ces endpoints sont décrits dans la suite de ce document.

A ce jour, PRO Santé Connect permet de s'authentifier avec sa CPS ou avec son seul smartphone afin d'accéder à des applications où qu'elles soient (ex. installées sur un smartphone, sur un poste de travail fixe ou en mode SAS). Ce service est opérationnel pour l'ensemble des porteurs de carte CPx (CPS RPPS, CPS ADELI, CPF, CPE libérale, CPE structure, …).

PRO Santé Connect admet un ensemble évolutif de dispositifs d'authentification :

- CPS,
- e-CPS Application (téléphone),
- OTP SMS, TOTP, …
- …

Le Fournisseur de Service contractualise avec l'ASIP Santé pour utiliser PRO Santé Connect. Ses utilisateurs peuvent ensuite bénéficier de l'ensemble des dispositifs d'authentification reconnus (dont la e-CPS) pour accéder à ses services en ligne.

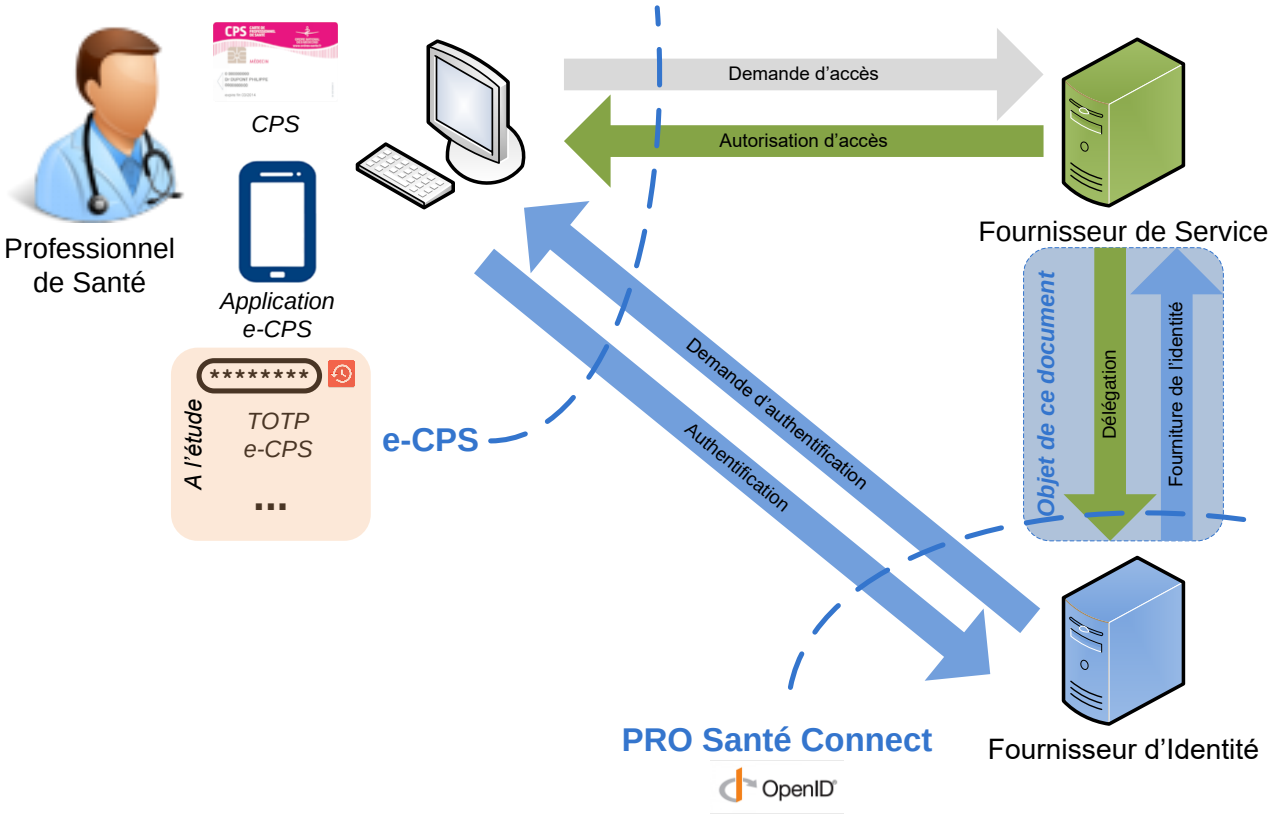


Figure 1 : Cinématique OIDC

Il existe plusieurs clients pour pouvoir intégrer plus facilement un FI comme PRO Santé Connect disponible sur https://openid.net/developers/certified/.

Des informations plus précises sont accessibles sur https://openid.net/connect.

2.1.2. Apports

La complexité liée à la gestion de l'authentification est déportée vers PRO Santé Connect ce qui simplifie de beaucoup et diminue les coûts de mise en œuvre des téléservices et des applications métier :

- L'intégration de PRO Santé Connect est relativement simple car la technologie utilisée (OpenID Connect) est un standard largement diffusé pour le grand public (France Connect, Google, Microsoft, …) et maintenu par la Fondation OpenID qui fournit la documentation ainsi que des ressources d'intégration certifiées (librairies, code exemple, …).
- Les promoteurs de téléservices et les éditeurs peuvent concentrer leurs efforts et leurs investissements sur les aspects métier du domaine de la santé.
- L'ergonomie d'utilisation est améliorée par l'homogénéisation des accès aux téléservices. L'expérience utilisateur à travers e-CPS sera la même pour la phase de connexion quel que soit le téléservice adressé.
- La conformité réglementaire relative à l'accès aux données de santé au travers des téléservices est portée par PRO Santé Connect qui assure la cohérence avec la PGSSI-S. Les évolutions associées sont prises en charge au niveau de PRO Santé Connect qui permet notamment l'intégration de nouveaux moyens d'authentification sans impact technique sur les téléservices.
- La sécurité des implémentations relative à l'authentification est homogénéisée avec un niveau d'exigence élevé (certification CSPN, maintenance sécuritaire continue), ce qui permet de supprimer les disparités actuellement constatées.

- La démarche PRO Santé Connect contribue à favoriser l'interopérabilité concernant la gestion des identités et le contrôle d'accès. La conformité vis-à-vis du CI-SIS sur ces sujets sera assurée au niveau de PRO Santé Connect.
- Le lien avec l'identité sectorielle (identification nationale des professionnels de santé) est natif, quel que soit le moyen d'authentification d'e-CPS mis en œuvre, il n'y a pas d'enrôlement spécifique à effectuer par chaque promoteur de téléservice.

PRO Santé Connect bénéficie d'un engagement de service en haute disponibilité avec mise en place d'un système de redondance. Des plans de continuité d'activité et de reprise d'activité à forts niveaux d'exigences sont définis. L'hébergement est assuré par un Organisme d'Importance Vitale qui est en mesure d'apporter les réponses à cette contrainte aussi bien en ce qui concerne l'architecture technique qu'au niveau organisationnel.

FranceConnect et PRO Santé Connect s'appuient sur la même technologie (OpenID Connect) mais les traits d'identité véhiculés par FranceConnect (citoyen ou professionnel) sont différents de ceux permettant d'assurer l'interopérabilité des systèmes d'information du secteur santé (identifiant professionnel national, profession, activités d'exercice, …).

2.1.3. Standards utilisés

PRO Santé Connect se base sur les standards suivants :

- HTTP 1.1 RFC 7230 – 7235 de l'IETF
- TLS 1.2 (ou supérieur) RFC 5246 de l'IETF
- JSON RFC 7159 de l'IETF
- OpenID Connect 1.0 (OIDC 1.0) de l'OIDF (OpenID Foundation)
- OAuth 2.0 RFC 6749 et RFC 6750 de l'IETF
- JWT (JSON Web Token) RFC 7519, JWS RFC 7515, JWE RFC 7516, JWA RFC 7518 de l'IETF

Les standards suivants ne sont pas appliqués :

- FHIR STU3 Security labels d'HL7
- HEART Profile for OAuth 2.0, HEART Profile for OpenID Connect 1.0 de l'OIDF

L'entête HTTP Category n'est pas utilisé au sein de PRO santé Connect (voir ci-dessus : standards non appliqués).

Les échanges applicatifs de données structurées se font uniquement au format JSON.

Les jetons (identification et information) ont bien un chiffrement asymétrique avec une clé RSA 2048. L'algorithme de chiffrement est du RSA SHA-256.

2.1.4. Environnement d'intégration

PRO Santé Connect propose un environnement totalement dédié à l'intégration. Il permet de vérifier le bon fonctionnement d'une intégration de PRO Santé Connect à l'aide de CPS de TEST.

> ***Cet environnement « Bac à Sable » a pour objectif de préparer l'intégration de PRO Santé Connect, i.e. vis-à-vis du standard OpenID, au sein d'une solution. Il n'est pas garanti que les informations d'identification de l'utilisateur fournies suite à l'authentification correspondent en tout point à celles décrites dans ce document. Seul l'identifiant national peut être considéré comme une base fonctionnelle stable représentative du comportement de l'environnement de production.***

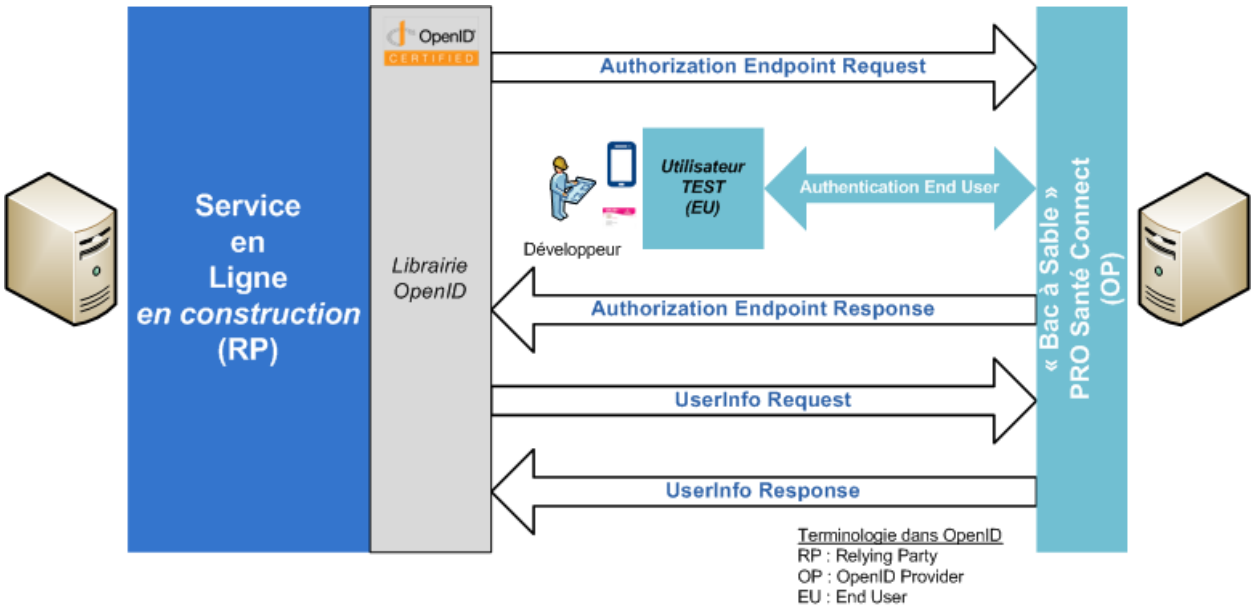


Figure 2 : Cinématique sur le Bac à sable

2.1.5. Gestion des sessions

Les sessions sont de deux types : gérées par le FS, ou gérées par le FI.

2.1.5.1. Session gérée par le FS

Elle permet de stocker les tokens d'un utilisateur connecté sur ce FS.

Le FS se doit de maîtriser sa session avec un utilisateur, i.e. notamment conserver l'access_token & le refresh_token correspondants et les rafraichir régulièrement au cours de sa session.

Les contraintes temporelles que nous imposons sont les suivantes :

La durée de validité des tokens est de **2 minutes** avant rafraichissement	**Access Token**

De plus, nous conseillons :

Après **4 minutes** d'inactivité de l'utilisateur, de stopper le rafraichissement des tokens	**FS Session idle**
Après **15 minutes**, la session gérée par le FS expire	**FS Session max**

2.1.5.2. Session gérée par le FI

Elle permet de conserver l'état connecté d'un utilisateur sur le FI.

Tant que un FS rafraichit ses tokens pour un utilisateur, ce dernier conserve sa session auprès du FI. Sa session auprès du FI expire lorsqu'après un certain temps, plus aucun FS ne rafraichit ses tokens pour cet utilisateur, i.e. l'utilisateur est inactif suffisamment longtemps pour perdre toutes ses sessions FS et donc ensuite perdre sa session FI.

Les contraintes temporelles que nous imposons sont les suivantes :

Après **15 minutes** d'inactivité, la session gérée par le FI expire	**FI Session idle**
Après **4 heures**, la session FI expire	**FI Session max**

Ces valeurs sont en cours de définition dans le cadre de l'expérimentation

Sur le bac à sable, les valeurs sont les suivantes :
- Access token : 5 minutes
- Refresh token : 30 minutes
Il n'y a pas de FI session max ni de FI session idle

2.1.5.3. Cinématiques de gestion de sessions

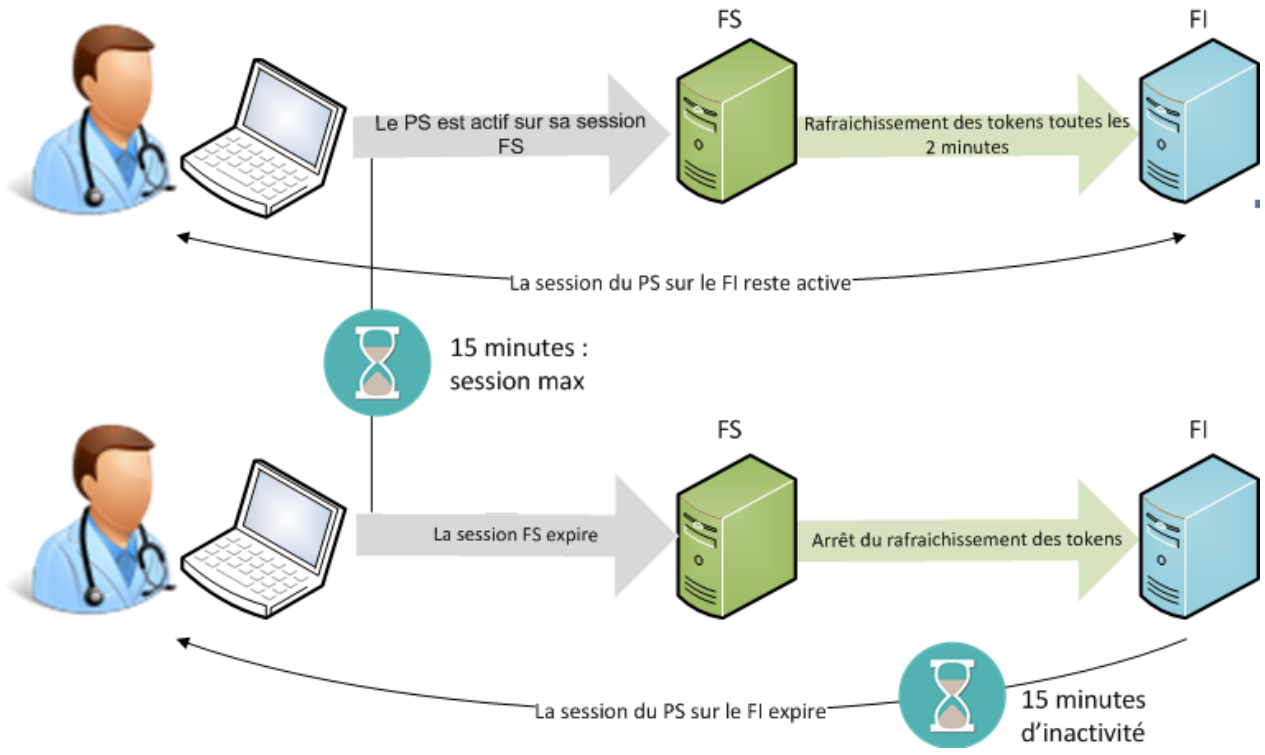


Figure 3 : Expiration de la session FS (FS session max)

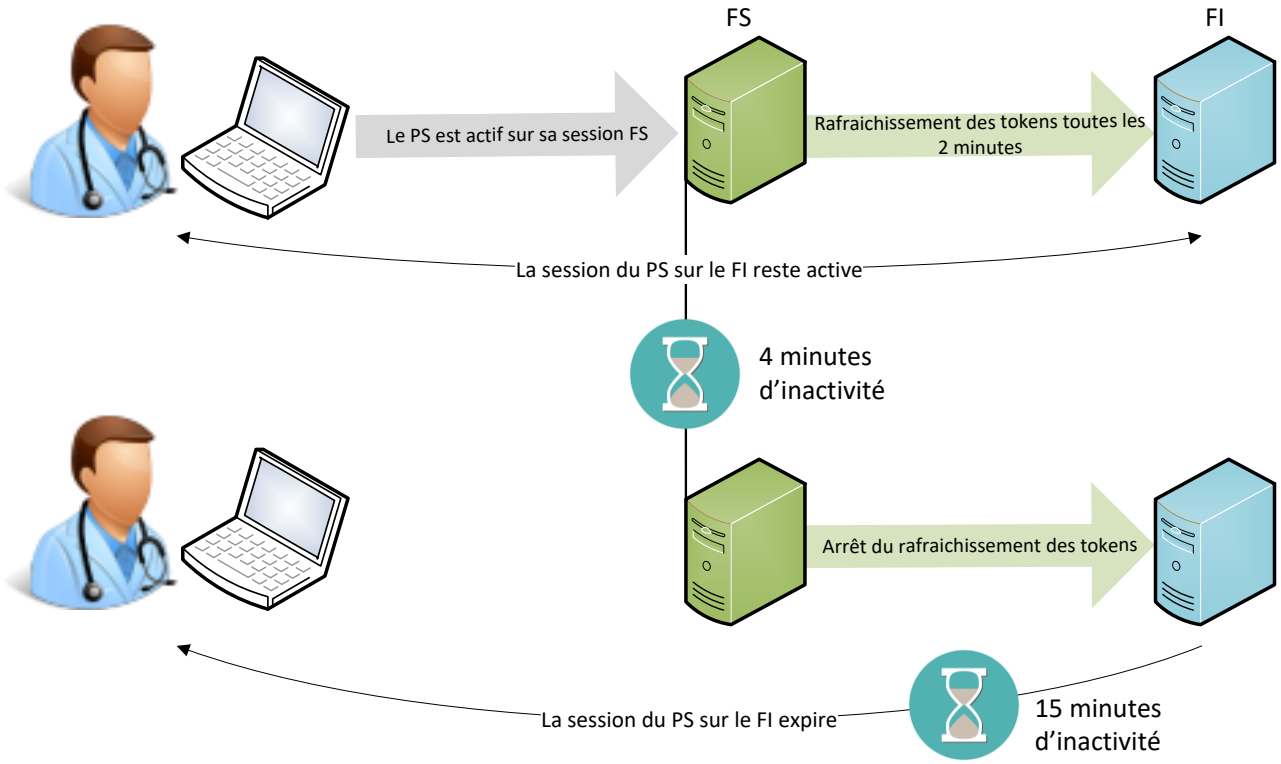


Figure 4 : Inactivité de la session FS (FS session idle)

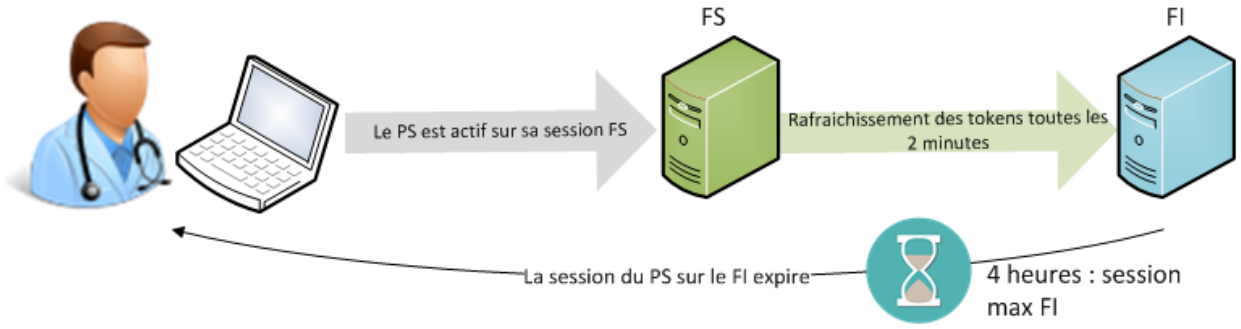


Figure 5 : Expiration de la session FI (FI session max)

2.2. e-CPS

2.2.1. Général

La e-CPS est l'évolution de la CPS vers sa dématérialisation. Nous capitalisons sur la marque CPS tout en proposant de nouveaux services et usages :

- La e-CPS et la CPS sont des dispositifs d'authentification reconnus par le FI « PRO Santé Connect »,
- Le FI « PRO Santé Connect » permet la continuité et l'évolution des dispositifs d'authentification de l'écosystème (Espace national de confiance santé social).

Figure 6 : Présentation de la e-CPS

2.2.2. Utilisation

2.2.2.1. Découverte du service par l'utilisateur

Dans un premier temps, le professionnel de Santé doit réaliser une activation de sa e-CPS :

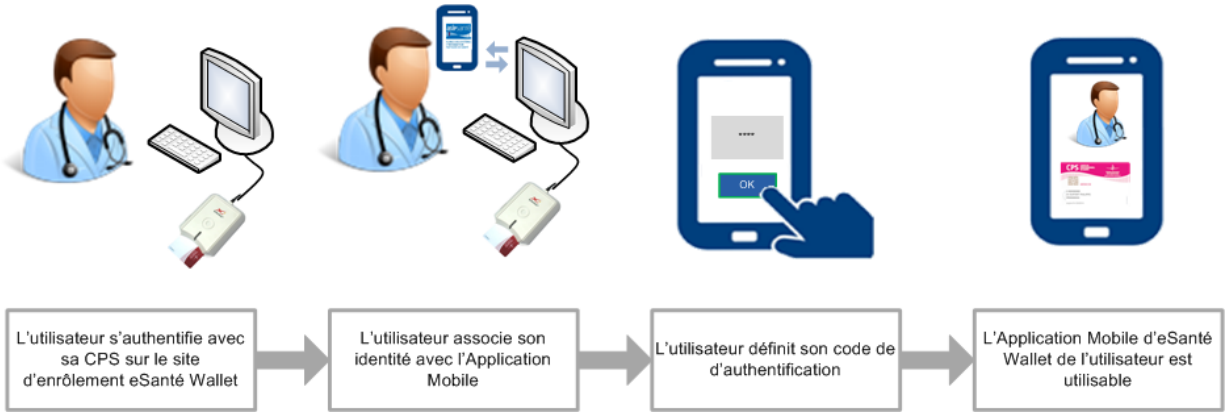


Figure 7 : Activation de la e-CPS

Ensuite, il peut s'authentifier pour accéder à un service en ligne :

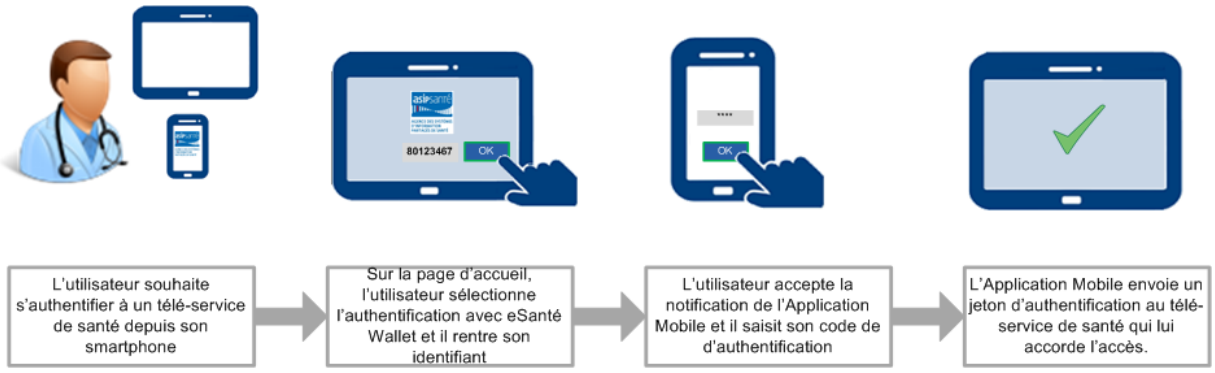


Figure 8 : Authentification de l'utilisateur

2.2.2.2. Authentification à un Fournisseur de Service

Avec e-CPS, PRO Santé Connect permet au Professionnel de Santé :

- soit de s'authentifier sur un appareil mobile type smartphone ou tablette :

Figure 9 : Authentification sur mobile

- soit de s'authentifier sur un poste de travail sans usage de la CPS :

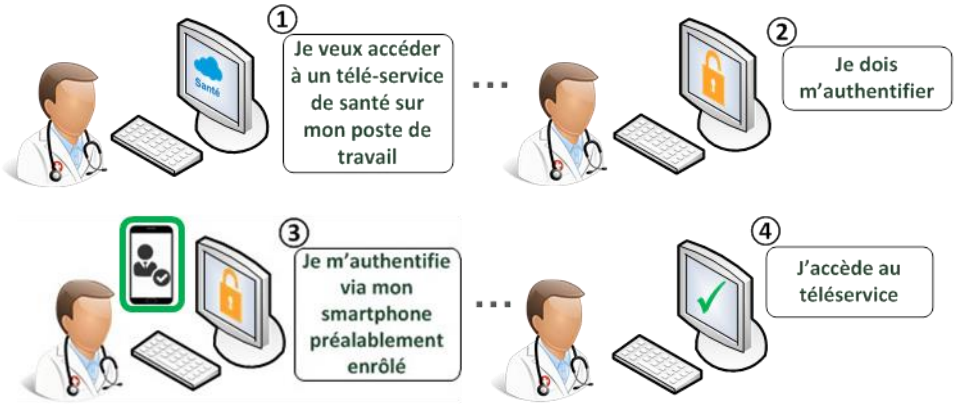


Figure 10 : Authentification par e-CPS

2.2.3. Quelques écrans

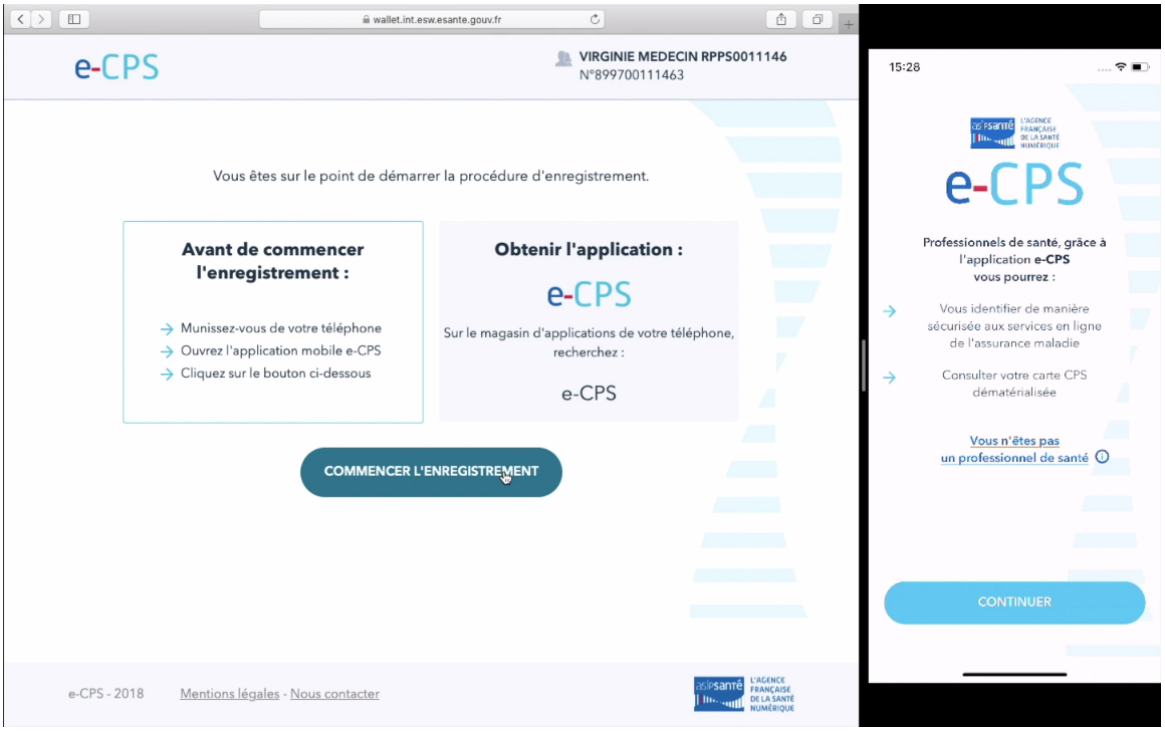


Figure 11 : Début du processus d'activation

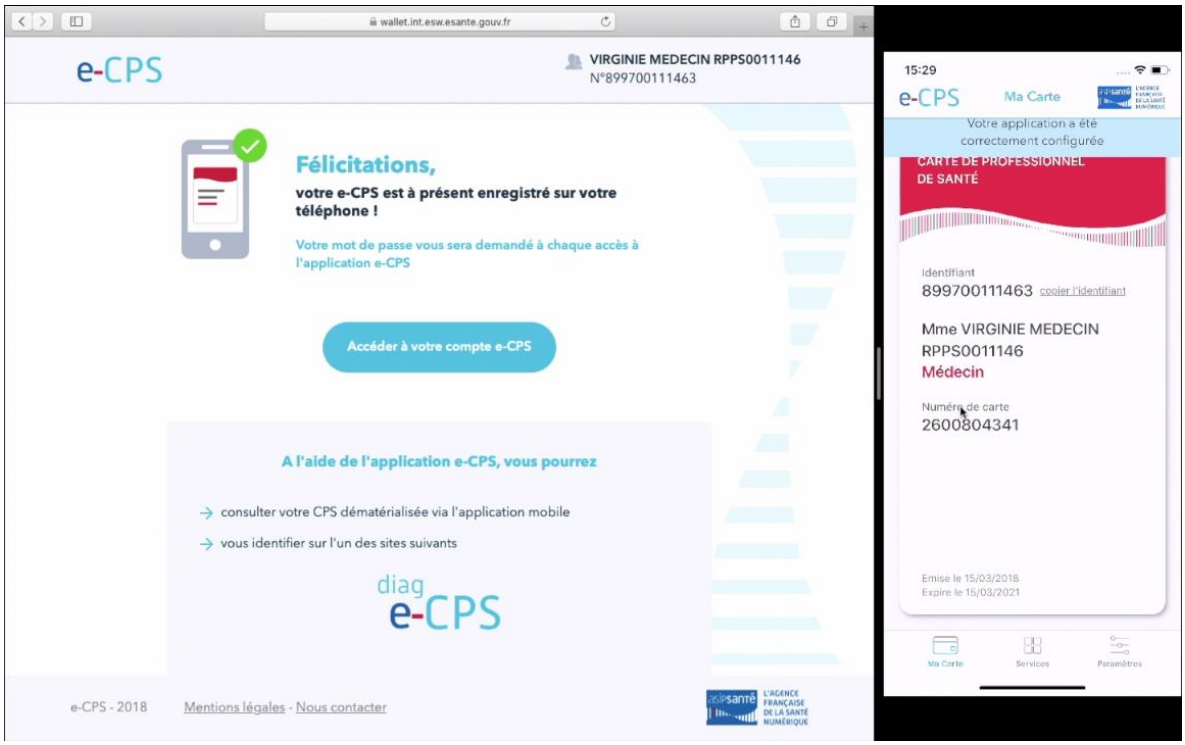


Figure 12 : Fin du processus d'activation

Figure 13 : Expiration de la CPS

Figure 14 : La CPS a expiré

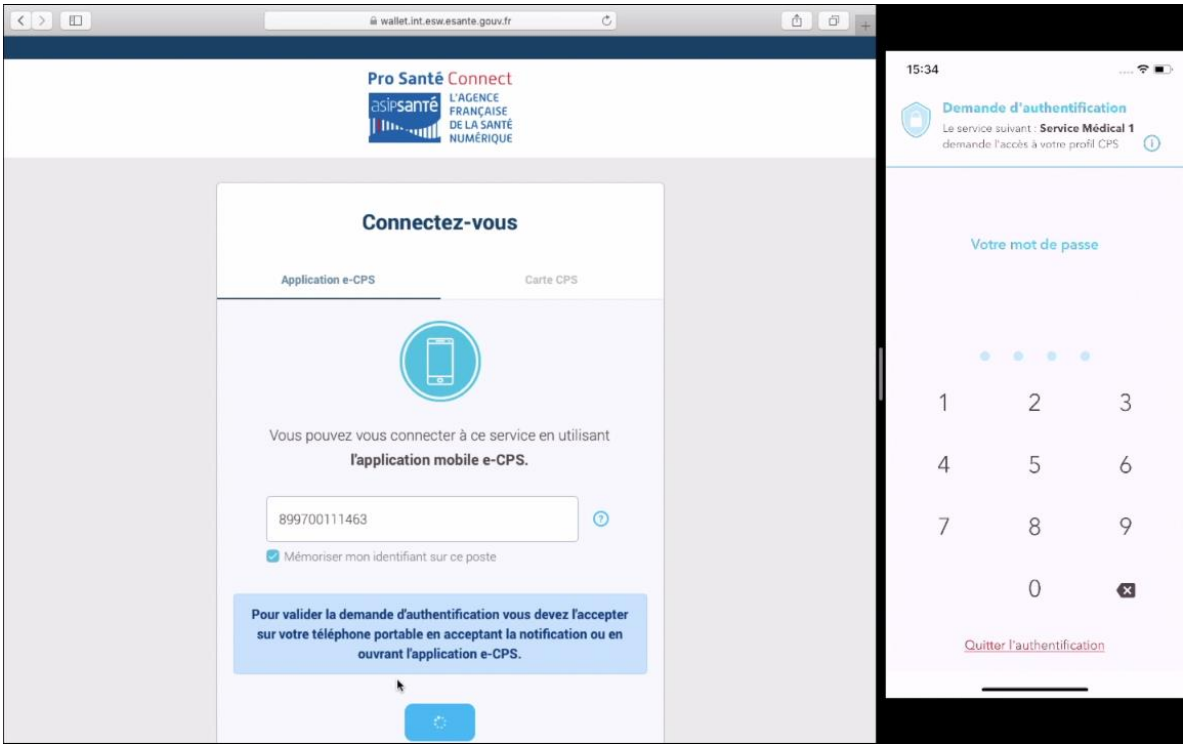


Figure 15 : Connexion par e-CPS

2.2.4. Compatibilité

Tableau 1 : Compatibilité de l'application

Système d'exploitation	Compatibilité	Appareils
Android 5.0	Non	
Android 6.0	Oui	
Android 7.0	Oui	Wiko Tommy2 plus, Moto G(5S), OnePlus 5T
Android 8.0	Oui	SONY Xperia H8324, Google Pixel, Huwaei P20, HTC U11, SAMSUNG A3, SAMSUNG S9, Samsung Galaxy S8, LENOVO Tab4 10
Android 9.0	Oui	Huawei P20
Android 10	Oui	
iOS 10	Non	
iOS 11	Oui	iPhone 7, iPhone 7s, iPhone 8, iPhone XS
iOS 12	Oui	iPhone XS
iOS 13	Oui	

Les tablettes ne sont pas supportées par l'application e-CPS. Cependant l'application peut être fonctionnelle.

3. REFERENCEMENT D'UN FS

Chaque nouveau fournisseur de service (FS) doit être référencé dans le FI PRO Santé Connect, pour ensuite profiter du service d'authentification. Il lui sera ensuite fourni les informations nécessaires pour accéder aux endpoints OIDC.

3.1. Prérequis pour référencer un FS auprès de PRO Santé Connect

Les informations suivantes sont à fournir par chaque FS pour permettre son enregistrement dans PRO Santé Connect :

Tableau 2 : Information pour enregistrement dans PSC

Nom du service	libellé représentant le nom du FS qui sera affiché dans l'application mobile e-CPS
Url de callback	URL vers laquelle l'utilisateur est retourné après une authentification réussie
Logo	visuel du FS pour être référencé dans l'application mobile e-CPS (image au format PNG en LxH)

En retour, PRO Santé Connect fournira les éléments nécessaires pour chaque client OIDC :

Tableau 3 : Eléments propres à chaque client OIDC

clientId	Identifiant calculé sur la base du nom du service
clientSecret	secret aléatoire

3.2. Prérequis pour tester un FS auprès de PRO Santé Connect

Pour valider l'intégration complète d'un FS, il est nécessaire d'avoir :

- Une CPS de TEST
- Pour l'authentification par smartphone :
  - Un téléphone (uniquement pour valider l'authentification par smartphone) disposant de l'application mobile e-CPS Bac à Sable :
    - Android (version >= 6.0)
  - Une connexion à internet depuis le téléphone :
    - 4G
    - ou WIFI

4. DESCRIPTION DES ENDPOINTS

4.1. Préalable

4.1.1. Lien FS/FI

Le Fournisseur de Service et le Fournisseur d'identité doivent communiquer via une connexion sécurisée.

Les paramètres de sécurité de la protection des flux entre le FS et le FI suivent les préconisations de l'ANSSI : **TLS1.2**.

4.1.2. Scopes

PRO Santé Connect propose un ensemble d'informations du secteur Santé Social lié à l'utilisateur identifié :

1. les traits de son identité professionnelle,
2. les informations liées au contexte de son accès courant au service en ligne, i.e. les informations nécessaires et suffisantes à la construction d'une assertion VIHF.
3. les informations complètes de l'ensemble de ses exercices professionnels.

Afin de simplifier son usage par un fournisseur de service, PRO Santé Connect offre deux scopes au sens OpenID :

Tableau 4 : Détails des scopes

Scope	Par défaut	VIHF
les traits de son identité professionnelle	Présent	Présent
les informations liées au contexte de son accès courant au service en ligne, i.e. les informations nécessaires et suffisantes à la construction d'une assertion VIHF	Non présent	Présent
les informations complètes de l'ensemble de ses exercices professionnels	Présent	*En cours de rédaction*
Signature des jetons	*En cours de rédaction*	Présent

Dans le scope par défaut, les informations liées au contexte seront présentes mais non déterminante : elles contiendront les informations de la 1ière activité professionnelle.

Cependant, dans la majorité des cas, les données professionnelles sont limitées à une seule et unique activité professionnelle.

Dans le cadre de la première phase d'expérimentation de PRO Santé Connect, seul le scope par défaut sera disponible et est décrit dans la suite de ce document

Le scope VIHF sera disponible ultérieurement. La documentation sera modifiée en conséquence.

4.2. Rappel

Les endpoints mis à disposition par PRO Santé Connect sont les endpoints FI OIDC. Ils sont décrits dans la configuration OIDC de la plateforme :

Tableau 5 : URLs de configuration PRO Santé Connect

Paramètre	Valeur
URL Bac à Sable	https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/.well-known/wallet-openid-configuration
URL	https://auth.esw.esante.gouv.fr/auth/realms/esante-wallet/.well-known/wallet-openid-configuration

Ce JSON de description des endpoints est standard et peut être utilisé directement par les clients OIDC :


```
{
   "issuer":"https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet",
   "authorization_endpoint":"https://wallet.bas.esw.esante.gouv.fr/auth",
   "token_endpoint":"https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/token",
   "token_introspection_endpoint":"https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-
connect/token/introspect",
   "userinfo_endpoint":"https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/userinfo",
   "end_session_endpoint":"https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/logout",
   "jwks_uri":"https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/certs",
   "check_session_iframe":"https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/login-status-
iframe.html",
   "grant_types_supported":[
      "authorization_code",
      "implicit",
      "refresh_token",
      "password",
      "client_credentials"
   ],
   "response_types_supported":[
      "code",
      "none",
      "id_token",
      "token",
      "id_token token",
      "code id_token",
      "code token",
      "code id_token token"
   ],
   "subject_types_supported":[
      "public",
      "pairwise"
   ],
   "id_token_signing_alg_values_supported":[
      "RS256"
   ],
   "userinfo_signing_alg_values_supported":[
      "RS256"
   ],
   "request_object_signing_alg_values_supported":[
      "none",
```

```
        "RS256"
    ],
    "response_modes_supported":[
        "query",
        "fragment",
        "form_post"
    ],
    "registration_endpoint":"https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/clients-registrations/openid-connect",
    "token_endpoint_auth_methods_supported":[
        "private_key_jwt",
        "client_secret_basic",
        "client_secret_post",
        "client_secret_jwt"
    ],
    "token_endpoint_auth_signing_alg_values_supported":[
        "RS256"
    ],
    "claims_supported":[      ], // en cours de rédaction
    "claim_types_supported":[
        "normal"
    ],
    "claims_parameter_supported":false,
    "scopes_supported":[      ], // en cours de rédaction
    "request_parameter_supported":true,
    "request_uri_parameter_supported":true,
    "code_challenge_methods_supported":[
        "plain",
        "S256"
    ],
    "tls_client_certificate_bound_access_tokens":true
}
```


Le fonctionnement nominal d'une authentification et de la récupération des informations d'un utilisateur passe par 3 endpoints :

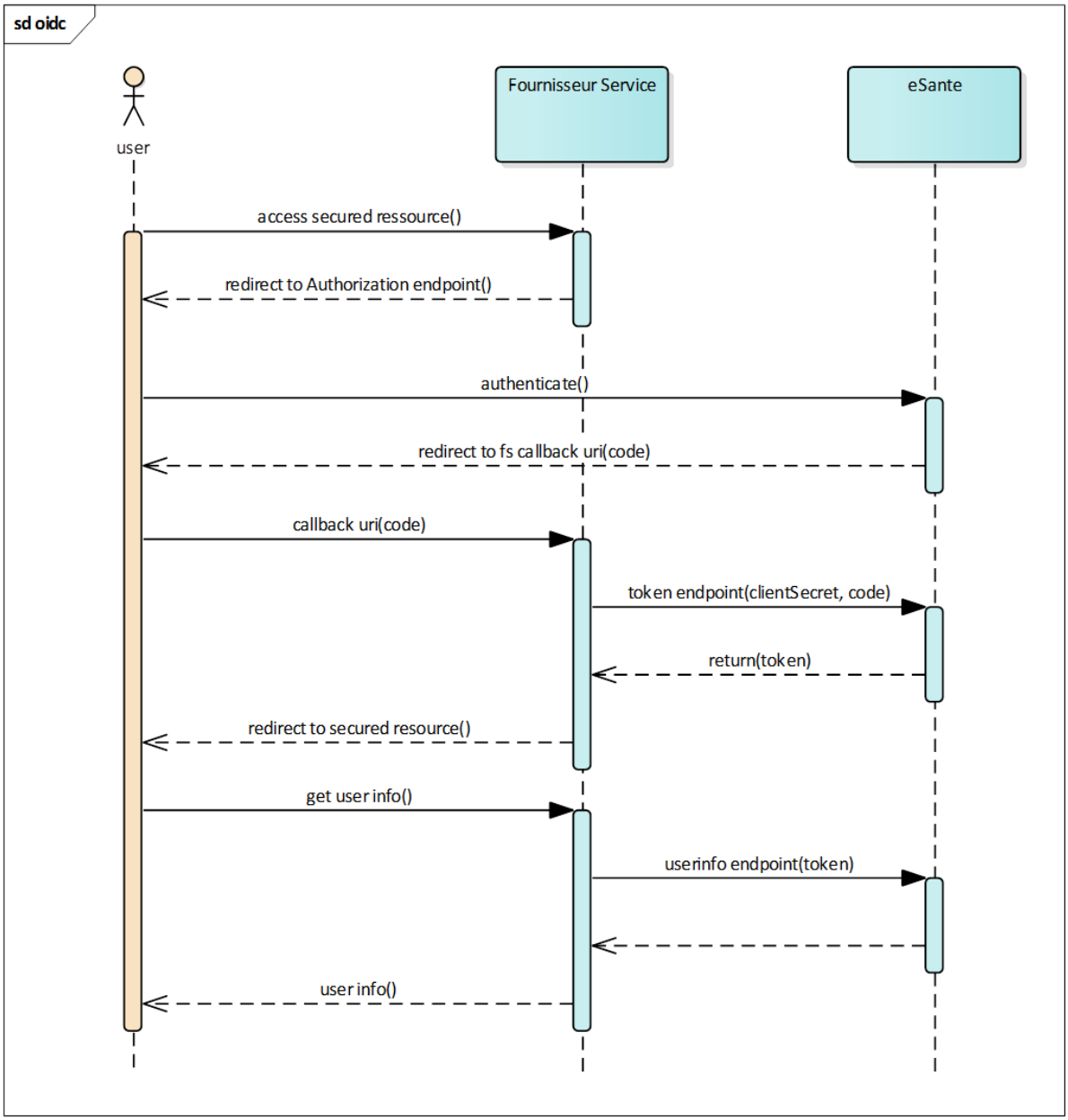


Figure 16 : Cinématique nominale

4.3. Authorization Endpoint

URL vers laquelle l'utilisateur doit être redirigé par le FS, lorsqu'il doit être authentifié.

Tableau 6 : URL de l'authorization endpoint

Paramètre	Valeur
URL Bac à Sable	https://wallet.bas.esw.esante.gouv.fr/auth
URL	https://wallet.esw.esante.gouv.fr/auth
Méthode	GET

Tableau 7 : Paramètres de query

Paramètre	Valeur
response_type	'code'
client_id	${client id}
redirect_uri	${callback uri}
scope	scopes séparés par des espaces. Permet de définir les informations de l'utilisateur que le FS souhaite récupérer. La liste des scopes est en cours de définition. Le scope « openid » est obligatoire. **Le scope doit prendre la valeur « openid scope_all »**
state	valeur générée aléatoirement par le FS, renvoyée telle quelle dans l'url de callback pour être vérifiée par le FS. Il permet de se prémunir contre les attaques CSRF.
nonce	valeur générée aléatoirement par le FS, recopié dans le token d'authentification pour être vérifié par le FS. Il permet de se prémunir contre les attaques de rejeu.
acr_values	**Ce champ est nécessaire et doit prendre la valeur « eidas2 »**

Réponse : une fois l'authentification terminée, le FI redirige l'utilisateur vers la callback uri avec en query params :

Tableau 8 : Paramètres de query

Paramètre	Valeur
code	Code d'autorisation : code à usage unique permettant d'appeler le service / token
state	Valeur envoyée par le FS.

4.4. Token Endpoint

Appel REST permettant de récupérer les tokens d'authentification à partir du code passé en query_param de l'uri de callback.

Tableau 9 : URL du token endpoint

Paramètre	Valeur
URL Bac à Sable	https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/token
URL	https://auth.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/token
Méthode	POST

Body (application/x-www-form-urlencoded) :

Paramètre	Valeur
grant_type	'authorization_code'
redirect_uri	${callback uri}
client_id	${client id}
client_secret	${client secret}
code	code récupéré en query param dans l'uri de callback

Réponse (JSON) :

```
{
    'access_token': ${access_token},
    'token_type': 'Bearer',
    'refresh_token': ${refresh_token},
    'expires_in': ${expiration},
    'id_token': ${id_token}
}
```

Avec ${id_token} :

Paramètre	Valeur
sub	Identifiant de l'utilisateur final, du sujet authentifié.
iss	Identité de l'émetteur du jeton. URL de l'endpoint de jetons du serveur d'identification.
aud	Ce champ contient la liste des identifiants des systèmes cibles pour lesquels le jeton a été fourni. La liste doit contenir au moins une entrée. Il doit compter parmi ses valeurs la valeur du champ OAuth 2.0 client_id du système cible.
exp	Date et heure exprimées en temps universel coordonné (UTC) de fin de validité du jeton.
iat	Date et heure exprimées en temps universel coordonné (UTC) de création du jeton.
jti	Identifiant unique du jeton permettant de révoquer le jeton et empêcher le rejeu.
nonce	Chaine de caractère associant la session du système cible à l'ID token. Contient la valeur du nonce de la requête d'authentification du système cible. Le « nonce » est nécessaire afin d'éviter les attaques par rejeu.

```
{
    'sub': ${sub},
    ... : ...
}
```

Dans le scope VIHF, la signature du jeton suit les préconisations suivantes :

- chiffrement asymétrique,
- clé RSA 2048 au minimum,

4.5. UserInfo Endpoint

Endpoint permettant de récupérer les informations de l'utilisateur.

Paramètre	Valeur
URL bac à Sable	https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/userinfo
URL	https://auth.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/userinfo
Méthode	GET
Header HTTP	Authorization = 'Bearer ${access_token}'

Réponse (JSON) de la Production :

Dans le scope VIHF, la signature du jeton suit les préconisations suivantes :

- chiffrement asymétrique,

- clé RSA 2048 au minimum.

Les paramètres ci-dessous sont intégrés au fur et à mesure.

De plus, ces paramètres peuvent être amenés à évoluer pour s'adapter au mieux aux besoins de l'expérimentation.

La documentation sera mise à jour en conséquence.

Paramètre	Valeur
family_name	Nom d'exercice
given_name	Prénom de l'utilisateur
sub	Identifiant de l'utilisateur final, du sujet authentifié.
iss	Identité de l'émetteur du jeton. URL de l'endpoint d'informations utilisateur du serveur d'identification.
aud	Ce champ contient la liste des identifiants des systèmes cibles pour lesquels le jeton a été délivré. La liste doit contenir au moins une entrée. Doit contenir parmi ses valeurs le champ OAuth 2.0 client_id du système cible.

Paramètre	Valeur
SubjectNameID	**Ce champ contient le PS-IdNat**
SubjectRefPro	List des données du Référentiel Professionnel du PS identifié PS-IdNat.
UITVersion	Version du jeton utilisée. « 1.0 »
Palier_Authentification	« APPPRIP3^1.2.250.1.213.1.5.1.1.1 » pour le palier 3 de l'authentification privée des acteurs sanitaires, médico-sociaux et sociaux personnes physiques. « APPPRIP2^1.2.250.1.213.1.5.1.1.1 » pour le palier 2 de l'authentification privée des acteurs sanitaires, médico-sociaux et sociaux personnes physiques. « APPPRIP1^1.2.250.1.213.1.5.1.1.1 » pour le palier 1 de l'authentification privée des acteurs sanitaires, médico-sociaux et sociaux personnes physiques.
PSI_Locale	1.2.250.1.213.1.3.1.1
SubjectRole	Dans le cadre du scope VIHF, contient le « [Code SubjectRole]^1.2.250.1.213.1.1.5.5» avec Code SubjectRole de la ligne sélectionnée par le PS parmi les données de SubjectRefPro. Sinon, contient la valeur correspondante d'une ligne des données de SubjectRefPro.
Secteur_Activite	Dans le cadre du scope VIHF, contient le « [Code Secteur_Activite]^1.2.250.1.71.4.2.4» avec Code Secteur_Activite de la ligne sélectionnée par le PS parmi les données de SubjectRefPro. Sinon, contient la valeur correspondante d'une ligne des données de SubjectRefPro.
SubjectOrganization	Dans le cadre du scope VIHF, contient le nom ou description de la personne morale, structure d'exercice de la ligne sélectionnée par le PS parmi les données de SubjectRefPro. Sinon, contient la valeur correspondante d'une ligne des données de SubjectRefPro.
SubjectOrganizationID	Dans le cadre du scope VIHF, contient l'identifiant de la personne morale, structure d'exercice de la ligne sélectionnée par le PS parmi les données de SubjectRefPro. Sinon, contient la valeur correspondante d'une ligne des données de SubjectRefPro.
Acces_Regulation_Medicale	Dans le cadre du scope VIHF, VRAI si accès pour régulation médicale (exemple : Urgentiste), Sinon FAUX par défaut.
Mode_Acces_Raison	Dans le cadre du scope VIHF, si Acces_Regulation_Medicale est VRAI, contient un commentaire, Sinon « » par défaut.

4.6. Refresh token endpoint

Appel rest permettant de renouveler les tokens d'identification lorsque le token d'accès est expiré et que le client souhaite le renouveler.

Paramètre	Valeur
URL Bac à Sable	https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/token
URL	https://auth.esw.esante.gouv.fr/auth/realms/esante-wallet/protocol/openid-connect/token
Méthode	POST

Body :

Paramètre	Valeur
grant_type	'refresh_token'
redirect_uri	${callback uri}
client_id	${client id}
client_secret	${client secret}
refresh_token	${refresh_token}

Réponse (JSON) : si le scope du token initial incluait '*openid*', alors un nouveau token ID sera également dans la réponse reçue.

```
{
    'access_token': ${access_token},
    'token_type': 'Bearer',
    'expires_in': ${expiration},
    'id_token': ${id_token}
}
```

Avec ${id_token} :

Paramètre	Valeur
sub	Identifiant de l'utilisateur final, du sujet authentifié.
iss	Identité de l'émetteur du jeton. URL de l'endpoint de jetons du serveur d'identification.

Paramètre	Valeur
aud	Ce champ contient la liste des identifiants des systèmes cibles pour lesquels le jeton a été fourni. La liste doit contenir au moins une entrée. Il doit compter parmi ses valeurs la valeur du champ OAuth 2.0 client_id du système cible.
exp	Date et heure exprimées en temps universel coordonné (UTC) de fin de validité du jeton.
iat	Date et heure exprimées en temps universel coordonné (UTC) de création du jeton.
jti	Identifiant unique du jeton permettant de révoquer le jeton et empêcher le rejeu.
nonce	Chaine de caractère associant la session du système cible à l'ID token. Contient la valeur du nonce de la requête d'authentification du système cible. Le « nonce » est nécessaire afin d'éviter les attaques par rejeu.

5. GLOSSAIRE

Acronyme	Message
FI	Fournisseur d'Identité
FS	Fournisseur de Service
OIDC	OpenID Connect
REST	REpresentational State Transfer

Annexe A : TESTER UN FS SUR LE BAC A SABLE

Afin de tester un FS sur le Bac à Sable de PRO Santé Connect, il est nécessaire de réaliser les étapes suivantes :

1. Souscrire au contrat éditeur vous liant à l'ANS.
2. Disposer de CPS de TEST.
3. Soumettre à l'ANS la demande de raccordement au Bac à Sable, contenant les informations suivantes :
   - Un contact interne à l'entreprise responsable de cette procédure,
   - La dénomination du service,
   - Une rapide description du service,
   - L'URL de redirection du service.
4. En réponse, l'ANS fournit :
   a. un ClientID unique pour le FS et le secret associé.
5. Choisir une solution OpenID Connect qui correspond à l'architecture du FS :
   - Module DRUPAL OpenID Connect,
   - Module Apache,
   - ….
6. Intégrer la solution précédente au FS en suivant les documentations officielles de la solution choisie.
7. Tester la connexion sur votre FS :
   a. En utilisant directement une de vos CPS de TEST,
   b. En téléchargeant l'application mobile et en l'activant à l'aide d'une de vos CPS de TEST.

> ***L'application mobile du Bac à Sable « e-CPS Bac à Sable » n'est disponible que sous Android.***

Annexe B : tester un FS utilisateur de jeton VIHF sur le Bac à sable

Dans le cadre de la première phase d'expérimentation de PRO Santé Connect, seul le scope par défaut sera disponible et est décrit dans ce document

Le scope VIHF sera disponible ultérieurement. La documentation sera modifiée en conséquence.

Annexe C : référencer un FS

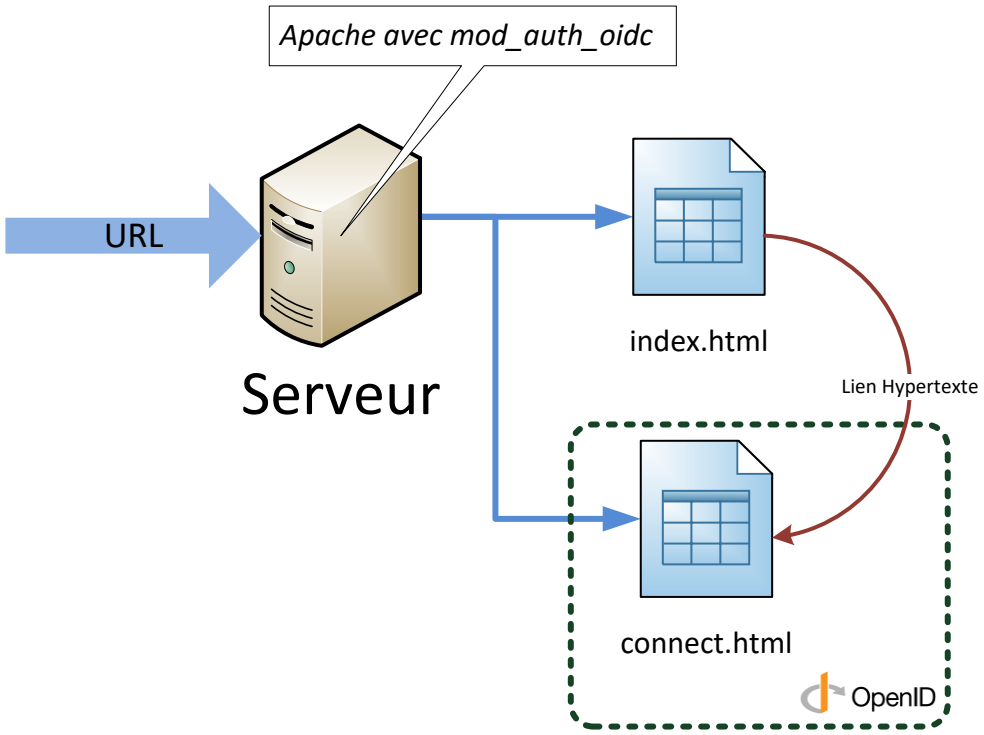
Cette annexe est en cours de définition.

Annexe D : référencer un FS utilisateur de jeton VIHF

Dans le cadre de la première phase d'expérimentation de PRO Santé Connect, seul le scope par défaut sera disponible et est décrit ce document

Le scope VIHF sera disponible ultérieurement. La documentation sera modifiée en conséquence.

Annexe E : Module Apache OIDC



En plus d'un serveur Apache correctement configuré, le module mod_auth_oidc est utilisé dans cet exemple. De plus, le serveur est accessible en HTTPS, i.e. port 443, sur une URL. Il admet une page d'accueil sur laquelle un bouton renvoi vers la page `connect.html`. La configuration ressemble alors à ceci ; *seule la configuration essentielle au standard OpenID est détaillée* :

```
LoadModule auth_openidc_module modules/mod_auth_openidc.so

<VirtualHost *:443>

    ServerName ${HOSTIP}

    DocumentRoot /var/www/html

    # Autres configuration, par exemple mod_ssl, mod_rewrite, …
    # this is required by mod_auth_openidc
    OIDCCryptoPassphrase ${PASSPHRASE}
    OIDCProviderMetadataURL
https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet/.well-
known/wallet-openid-configuration
    OIDCClientID ${CLIENT_ID}
    OIDCClientSecret ${CLIENT_SECRET}
```

```
    OIDCRedirectURI http://${HOSTIP}/${CLIENT_APP_NAME}/redirect_uri


    # maps the prefered_username claim to the REMOTE_USER environment
variable
    OIDCRemoteUserClaim preferred_username
    # Autres configuration, par exemple mod_ssl, mod_rewrite, …


    <Location /${CLIENT_APP_NAME}/>
        AuthType openid-connect
        Require valid-user
    </Location>


    # Example of a file protected by OpenID valid user
    <Location /connect.html>
        AuthType openid-connect
        Require valid-user
    </Location>


    # Autres configuration, par exemple Location, …
    OIDCProviderAuthorizationEndpoint https://wallet.bas.esw.esante.gouv.fr/auth


</VirtualHost>
```

Le tableau ci-dessous détaille les paramètres utilisés dans l'exemple ci-dessus :

LoadModule	mod_nom-module.so Modules apache chargés ; autant de LoadModule que de modules à charger
ServerName	URL
ServerAdmin	L'adresse électronique que le serveur inclut dans les messages d'erreur envoyés au client
DocumentRoot	Racine principale
OIDCCryptoPassphrase	Un mot de passe définit aléatoirement
OIDCProviderMetadataURL	L'url du bac à sable
OIDCClientID	L'ID client fourni
OIDCClientSecret	Le secret client fourni
OIDCRedirectURI	L'URI de redirection de l'application
OIDCRemoteUserClaim	Le nom d'utilisateur
Location /${CLIENT_APP_NAME}	Location permettant les échanges OpenID entre le module

	mod_auth_oidc et PRO Santé Connect