AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

CI-SIS VOLET TRANSPORT

APIs PRO SANTE CONNECTEES

WEBINAIRE

28/04/2023

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Sommaire

- VOLET TRANSPORT DU CI-SIS – OBJECTIF ET PLANNING,
- HISTORIQUE CONCERNANT LA SECURISATION DES APIs DE ESANTE,
- MODALITES DE RACCORDEMENT D'UN FOURNISSEUR DE SERVICE A PRO SANTE CONNECT,
- APIs PRO SANTE CONNECTEES – STRATEGIE ET PRINCIPE DE SECURISATION,
- APIs PRO SANTE CONNECTEES – INTEGRATION DANS LES TELESERVICES DE LA CNAM.

VOLET TRANSPORT DU CI-SIS POUR LES APIs PRO SANTE CONNECTEES - OBJECTIFS

- **Ces APIs Pro santé Connectées doivent faciliter les usages et l'authentification sur les téléservices de esanté dans des architectures connectées.**

- **Ce volet contient en priorité une partie sur les APIs ProSanteConnectee (openid connect + OAUTH2).**

- **Ce volet s'appliquera de façon transverse aux services de esanté dont les services de l'Assurance Maladie (DMP, INSi, SPEi…).**

⇨ **Avoir un volet transport sur un CI-SIS commun CNAM/GIE SV et ANS.**

⇨ **Avoir une architecture standard pour les APIs avec un bon niveau de sécurité.**

Répondre à un objectif de la vague 2 du Ségur : généralisation de la consultation du DMP et ouverture des téléservices AMO à Pro Santé Connect.

VOLET TRANSPORT DU CI-SIS POUR LES APIs PRO SANTE CONNECTEES - OBJECTIFS

L'objectif de cette présentation est d'expliciter ce que l'on entend par :

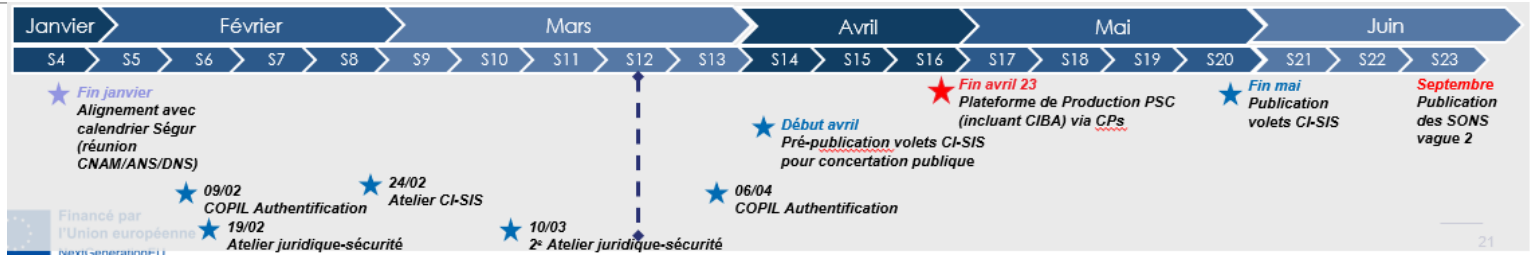
« Avoir une architecture standard pour les APIs avec un bon niveau de sécurité ».

Ci-dessous le fil conducteur des principes de sécurisation retenus :

- **Généraliser l'authentification forte de professionnels de santé sur les téléservices de esanté,**
- **Permettre cette authentification forte en mobilité,**
- **Centraliser l'authentification de professionnels de santé avec Pro Santé Connect,**
- **Renforcer le contrôle d'accès au niveau des APIs,**

…

VOLET TRANSPORT DU CI-SIS POUR LES APIs PRO SANTE CONNECTEES - PLANNING



- **Du 07/04 au 05/05 :**

Pour la partie APIs PSConnectées : Mise en concertation et organisation d'ateliers/webinaires avec des éditeurs,
⇒ https://participez.esante.gouv.fr/project/volet-transport-api-pro-sante-connectees/presentation/presentation

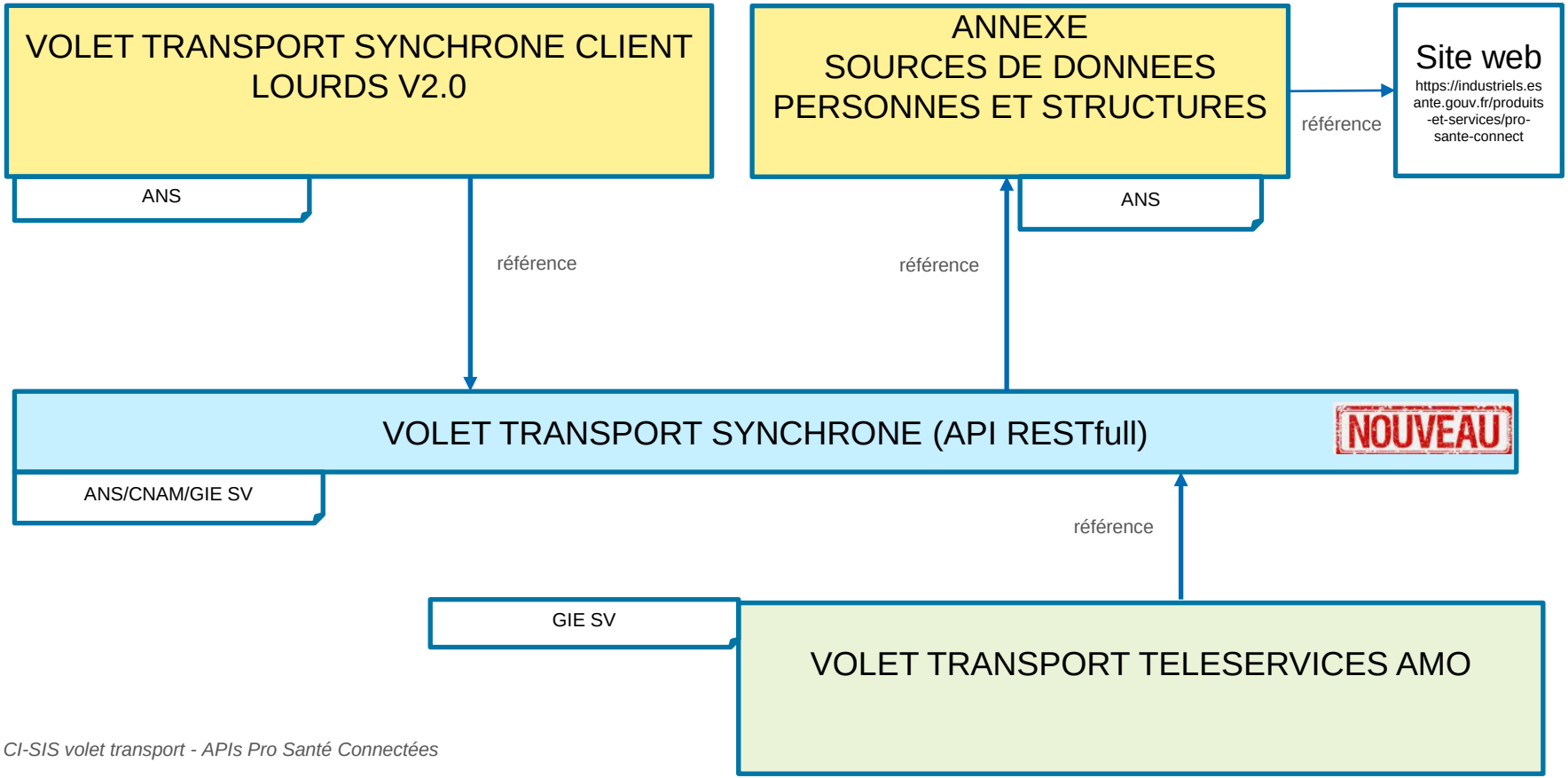
- **Du 07/04 au 30/05 :**

Ajout des cas d'usage concernant les APIs non Pro santé connectées : Authentification indirecte des structures entre autres.

- **Le 30/05 :**

date cible de publication des volets transport du CISIS (à confirmer).

ARCHITECTURE DOCUMENTAIRE DES VOLETS TRANSPORT DU CI-SIS



HISTORIQUE DES MODES DE SECURISATION DES APIs EXISTANTS

Authentification TLS réciproque directe par carte CPS

(Exemple API pour l'alimentation et la consultation du DMP par le PS)

- API SOAP invoquée par un PS, sécurisées de bout en bout par une authentification TLS réciproque par carte CPS depuis un logiciel PS.

Dans le cas du DMP, On fait confiance au PS en authentification directe.

- Les données métier du PS et de ses situations d'exercice sont extraites de la carte CPS.
- Le logiciel PS est homologué DMP compatible par le CNDA.

VOLET CI-SIS TRANSPORT SYNCHRONE CLIENT LOURDS V2.0

HISTORIQUE DES MODES DE SECURISATION DES APIs EXISTANTS

Authentification sans TLS réciproque directe par carte CPS

(Exemple API pour la consultation du service INSi ou du service ADRi/TLSi de la CNAM)

- API SOAP invoquée par un PS, avec la signature d'une assertion SAML via le certificat de signature de la carte CPS. Pas de TLS réciproque, simplement un TLS serveur.
- Les données métier du PS et de ses situations d'exercice sont extraites de la carte CPS.
- Le logiciel PS doit implémenter un service de signature à l'aide de la carte CPS.
- Le logiciel PS est homologué TLSi compatible par le CNDA.

VOLET TRANSPORT TELESERVICES AMO

PRO SANTE CONNECT & APIs PRO SANTE CONNECTEES

L'authentification du PS peut désormais être déléguée à PSC.

PSC fournit les données métiers du PS et ses situations d'exercice.

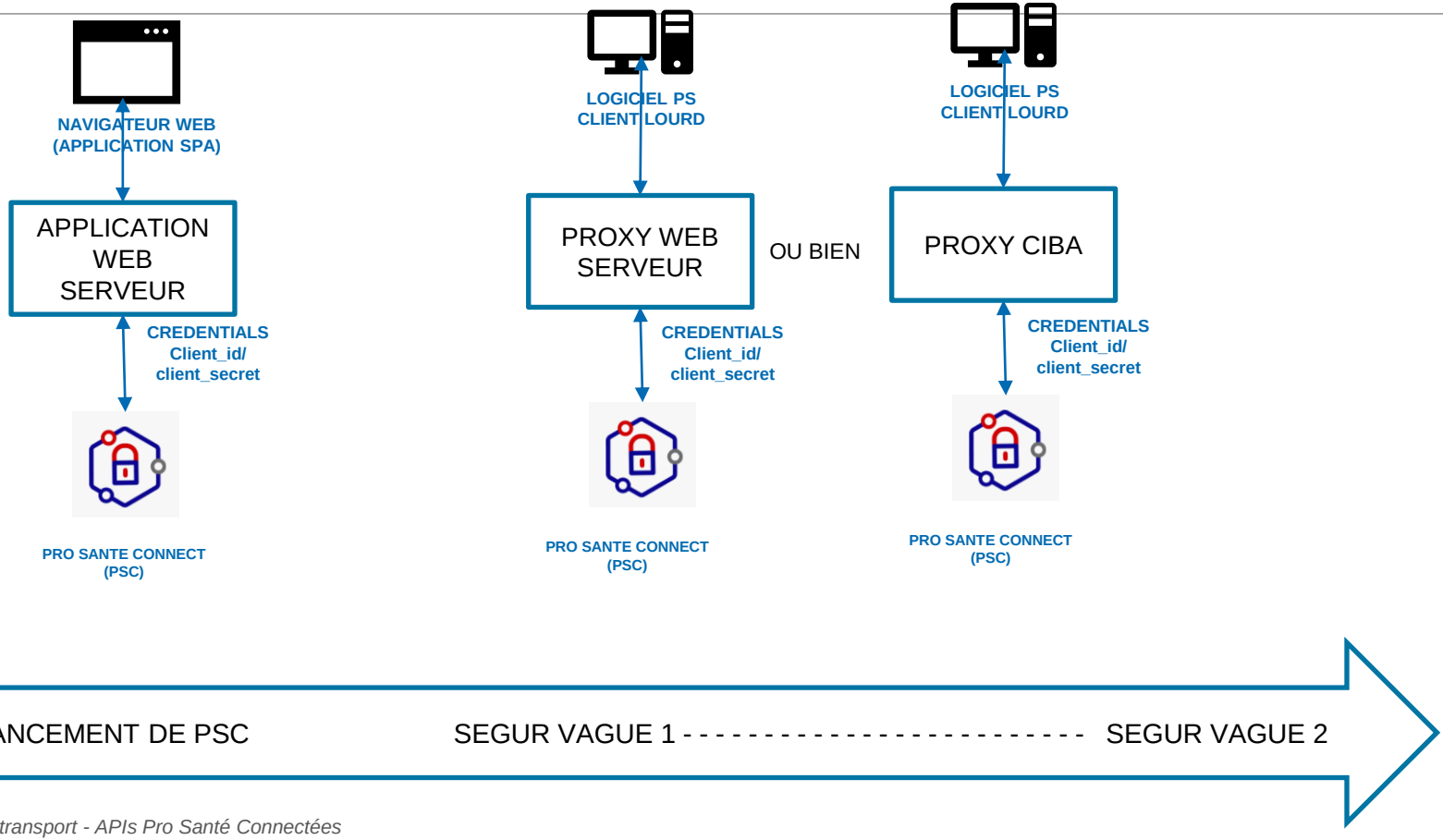
- Le logiciel PS n'a plus besoin d'implémenter de service de signature ou de TLS réciproque.
- Le PS peut se connecter à son logiciel PS en mobilité.

=> Changement de paradigme concernant l'authentification d'un PS sur un service cible (API) via son Logiciel PS.

=> La sécurisation n'est plus réalisée de bout en bout par une session TLS : Il s'agit d'authentifier l'utilisateur PS en véhiculant une preuve d'authentification du PS (access token PSC) jusqu'au service cible (API).

Comment sécurise-t-on la transaction de bout en bout ?

MODALITES DE RACCORDEMENT D'UN SERVICE A PRO SANTE CONNECT (PSC)



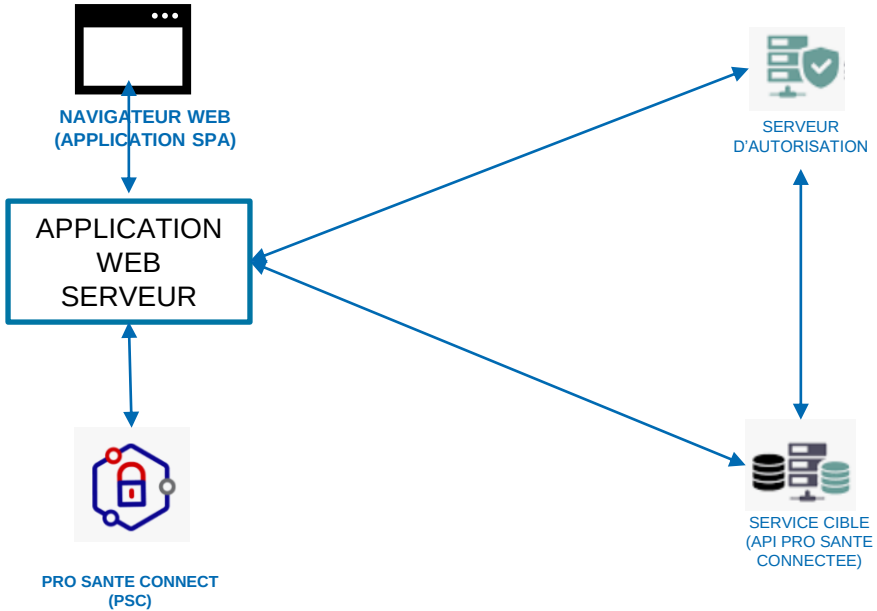
MODALITES DE RACCORDEMENT D'UN SERVICE A PRO SANTE CONNECT (PSC) – PRINCIPES DE SECURISATION

- Le serveur applicatif (web ou CIBA) du Fournisseur de Service s'authentifie sur PSC via les credentials client_id /client_secret (1 client_id et un certificat mTLS client en cible).
- Dans le cas d'un Logiciel PS client lourd, c'est le serveur applicatif (web ou CIBA) qui est le client confidentiel de PSC.
- L'access token PSC ne remonte pas sur l'instance de LPS client lourd ni sur le navigateur web.

⇒ Principe de séparation de credentials.

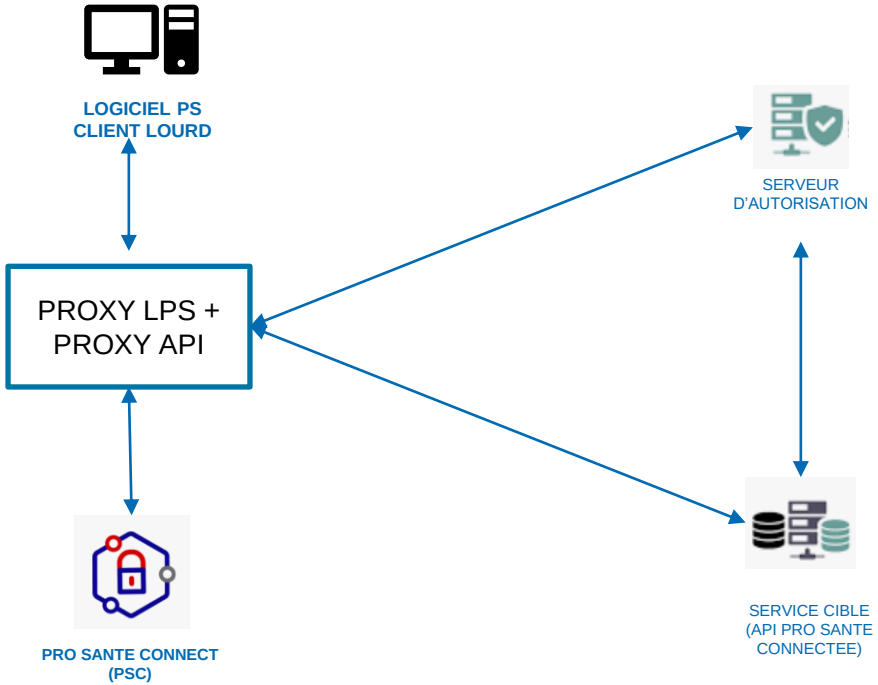
- L'access token PSC possède un attribut d'audience (azp) spécifique au fournisseur de service.

Cas d'une application web



Contrôle d'accès réalisé en entrée de l'API.

Cas d'un logiciel PS client lourd



Contrôle d'accès réalisé en entrée de l'API.

PROXY LPS
=
PROXY WEB SERVEUR
OU
PROXY CIBA

APIs PROSANTE CONNECTEES – AUTHENTIFICATION SUR L'API

- **Découplage des requêtes vers le service cible (API) et des requêtes vers PSC.**
  - L'access_token PSC est utilisé une seule fois pour initier l'authentification sur le service cible lors de l'échange de tokens : access_token PSC contre un access_token API.
  - **La durée de validité de l'access_token API est de 1h contre 2 minutes pour l'access_token PSC.**
  - Cela évite une sur sollicitation de PSC lors de l'envoi des requêtes vers le service cible (API).

- **Sécurisation :**
  - Gestion des credentials pour s'authentifier sur PSC et sur le serveur d'autorisation du service cible (API).
    1 client_id et un certificat TLS client par proxy LPS FS/API.
  - L'access_token PSC et l'access_token API ne remontent pas sur l'instance de LPS client lourd ni sur le navigateur.
  - Contrôle d'accès d'un Fournisseur de Service (proxy LPS FS/API) sur le service cible grâce aux scopes.
  - **Possibilité d'ajouter des claims métiers dans l'access_token API**

Le Fournisseur de l'API a la main sur l'enrôlement et sur le contrôle d'accès des services clients de l'API.

APIs PROSANTE CONNECTEES – AUTHENTIFICATION SUR L'API

Changement de paradigme par rapport aux APIs sécurisé par un TLS réciproque par carte CPS.

o ***Introduction de trois types de composants complémentaires pour assurer l'authentification du PS***

• Le composant Fournisseur d'identité ProSantéConnect (PSC) en charge de réaliser l'authentification effective des PS selon le standard OpenID Connect, via sa CPS ou sa e-CPS

• Le composant logique Proxy LPS FS qui assure l'interface entre les instances de logiciels LPS clients lourds des PS et PSC.

• Le composant logique Proxy LPS API qui assure l'interface entre les instances de logiciels LPS clients lourds des PS et un service cible

⇒ **Les LPS clients lourds ne font plus d'accès directs vers les différents services cibles.**

⇒ **Le proxy LPS PSC et le proxy LPS API sont regroupés dans la même brique technique sur un serveur unique.**

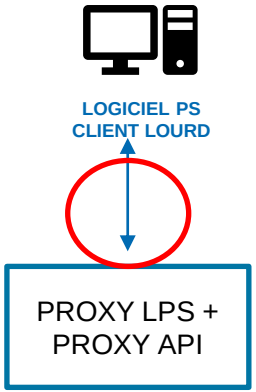
• Le composant Serveur d'Autorisation du Service cible, est en charge de gérer les sessions d'accès avec les PS ainsi que les autorisations d'accès du proxy LPS API au service cible.

=> Tous ces composants échangent via des API REST respectant le standard OpenId Connect et le standard OAUTH2.

APIs PROSANTE CONNECTEES – SECURISATION DE LA CONNEXION ENTRE L'INSTANCE DE LPS ET LE PROXY LPS FS/API

Les éditeurs sont libres d'implémenter leur solution de sécurisation du lien entre l'instance de LPS et le serveur proxy LPS FS/API.

Cette solution doit être conforme aux exigences du référentiel PSC et aux exigences de sécurité de la vague 2 du Ségur.



APIs PROSANTE CONNECTEES - INTEGRATION DANS LES SERVICES DE LA CNAM

Pour être compatible avec les plannings de la vague 2 du Ségur et pour minimiser les impacts sur les LPS déployés, Les équipes d'architectes de la CNAM ont décidé d'encapsuler les requêtes historiques (SOAP + SAML) dans les nouvelles requêtes REST/OAUTH2 des APIs pro santé connectées.

Cependant, la cible concernant les téléservices de la CNAM est la généralisation des APIs RESTfull et le décommissionnement des APIs SOAP/SAML.

Côté ANS :

Donc nous avons mis à jour le document historique ci-dessous :

- Volet Transport Client Lourd pour les services de santé (V2.0 -> v3.0) : https://esante.gouv.fr/volet-transport-synchrone-pour-client-lourd

⇨ **Nota bene : ce document est applicable aux services qui utilisent un VIHF et il est référencé dans le nouveau volet sur les APIs REST Pro Sante Connectées dans ce document.**

Côté GIE SV/CNAM :

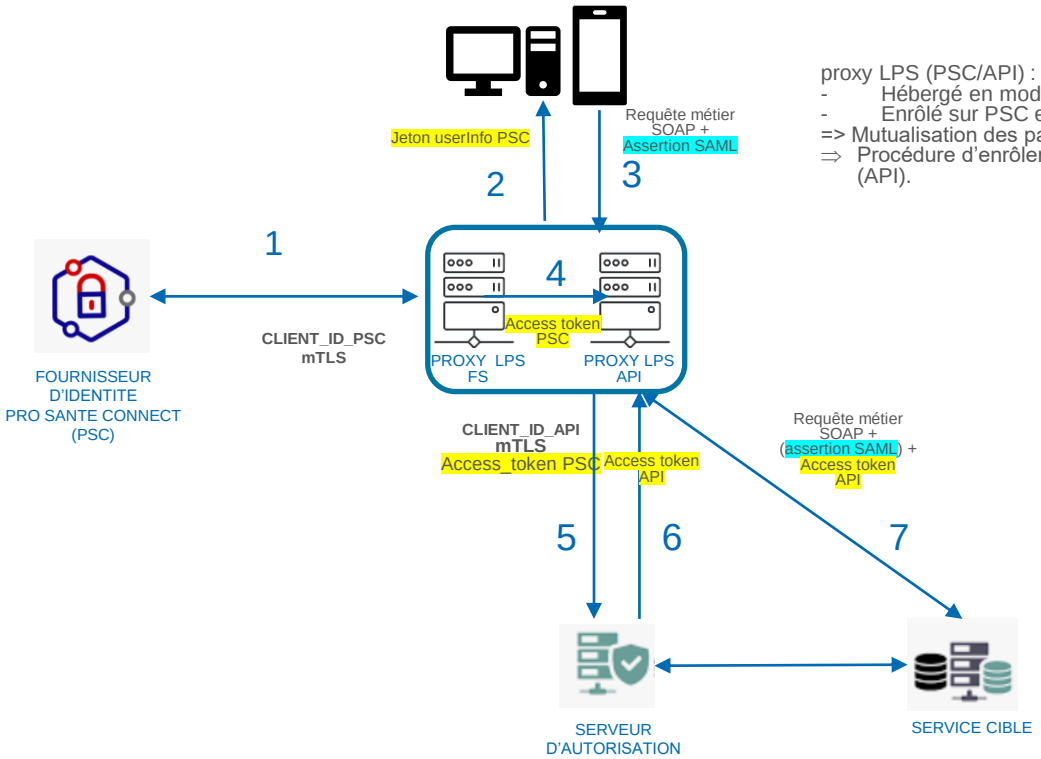
Donc les équipes du GIE SESAM VITALE devoir mettre à jour le document historique ci-dessous :

- Volet transport synchrone des téléservices (TLSi) AMO (Assurance Maladie Obligatoire).

https://industriels.sesam-vitale.fr/group/integrer-tlsi

⇒ **Le GIE SV référencera le nouveau volet les APIs REST ProSanteConnectées dans ce document.**

APIs PRO SANTE CONNECTEES – CINEMATIQUE D'AUTHENTIFICATION SUR UN TELESERVICE DE LA CNAM



proxy LPS (PSC/API) :
- Hébergé en mode SAAS côté éditeur,
- Enrôlé sur PSC et sur chaque API

=> Mutualisation des paramètres d'authentification (certificat mTLS client et clientID).

⇒ Procédure d'enrôlement à construire par chaque fournisseur de service cible (API).

APIs PROSANTE CONNECTEES – SEQUENCES D'AUTHENTIFICATION ET D'IDENTIFICATION SUR UN TELESERVICE DE LA CNAM

Séquence d'authentification et d'identification du PS sur son instance de LPS via pro santé connect (PSC).

- L'instance de LPS invoque le proxy LPS FS qui réalise un flux openid connect & mTLS sur PSC.

L'access token PSC reste sur le proxy LPS FS.

- Le proxy LPS FS peut demander le jeton userinfo PSC à PSC et le peut le transmettre à l'instance de LPS.

Les 2 blocs de séquences ci-dessous ne sont pas forcément synchrone avec la séquence d'authentification du PS sur PSC.

Génération de la requête SOAP et de l'assertion SAML (VIHF ou AMO) sur l'instance de LPS

(Lorsque le PS souhaite accéder au service cible (exemple DMP ou TLSi AMO)

- L'instance de LPS construit la requête SOAP et forge une assertion SAML non signée avec les données du jeton user info PSC.
- L'instance de LPS envoie la requête SOAP et l'assertion SAML au proxy LPS API.

Séquence d'authentification et d'autorisation du proxy LPS API sur le service cible

- Le proxy LPS API s'authentifie en mTLS sur le serveur d'autorisation du service cible et réalise un flux OAUTH2 token exchange : échange d'un access token PSC contre un access token API.
- Le proxy LPS API envoie la requête SOAP et l'assertion SAML et l'access token API au service cible.

APIs PROSANTE CONNECTEES – SEQUENCES D'AUTHENTIFICATION ET D'IDENTIFICATION SUR UN TELESERVICE DE LA CNAM

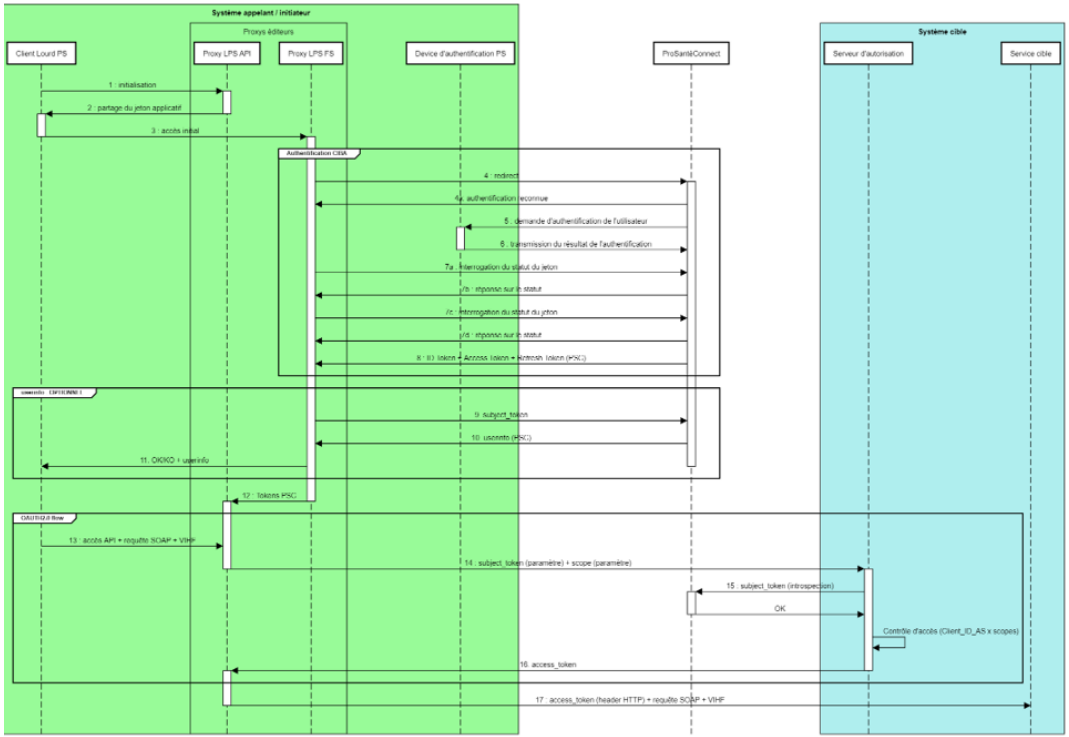


Figure 20 : intégration du requêtage par protocole SOAP dans le flow Oauth2.0

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

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