

Webinaire ANS

Comment intégrer l'API LPS dans les LPS/DUI ?

19/01/2024





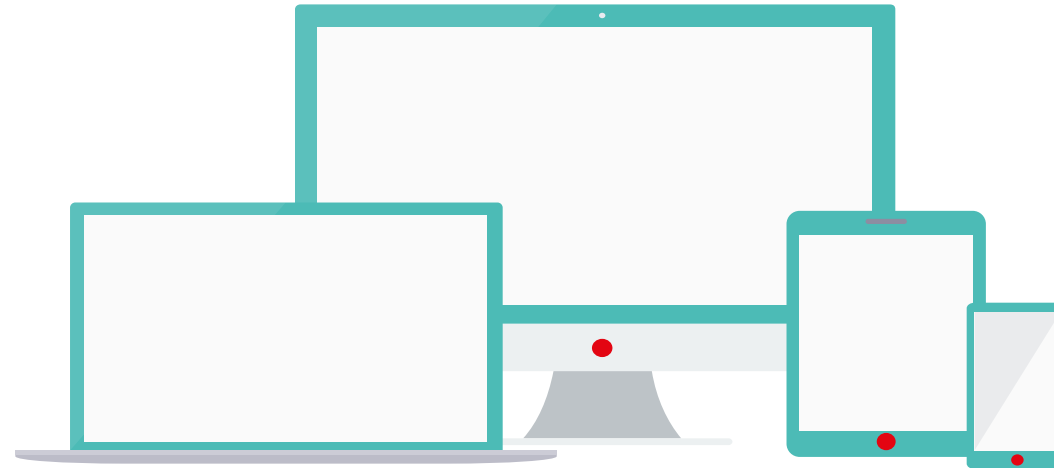
Edouard BRIS - ANS
**Responsable de l'équipe
« Echanges »**



Mike GUEYE - ANS
**Responsable du projet Espace
de Confiance MSSanté**



- Le webinaire est enregistré et sera disponible sur le site esante.gouv.fr



- Les questions sont à poser via la fenêtre « Q / R »
- Nous prendrons des questions à l'issue de chaque partie
- Merci de lever la main pour prendre la parole (le micro sera activé par les intervenants)

Introduction

Contexte / rappels :

- ▶ Le lancement de l'API LPS a officiellement été **annoncé le 14 décembre 2023** (communication par email aux contacts éditeurs référencés Ségur vague 1, en annexe)
- ▶ Désormais **tous les Opérateurs référencés Ségur** proposent l'interface API LPS (<https://esante.gouv.fr/segur/solutions-referencées>)
- ▶ L'API LPS est décrite dans :
 - Le Référentiel #1 Opérateurs MSSanté v1.5 **publié le 22/04/2022** (co-construction industriels T4 2021- T1 2022)
 - Le Référentiel #2 Clients de messagerie MSSanté v1.0 **publié le 31/01/2023**

Rq : [version mineure corrective 1.0.1 publiée le 18/01/24](#) pour adapter la méthode d'autoconfiguration

- ▶ La conformité avec l'API LPS sera exigée pour la majorité des couloirs **Ségur vague 2**

Objectif du webinaire :

- ▶ Permettre aux éditeurs de LPS/DUI d'intégrer l'API LPS dans leurs logiciels, sans attendre le référencement Ségur vague 2

Rappel : Afin de gérer la transition depuis les anciennes interfaces MSSanté utilisées par les LPS/DUI, merci de répondre au [questionnaire](#) avant le 24/01/24 (14 éditeurs ont répondu à date)

SOMMAIRE

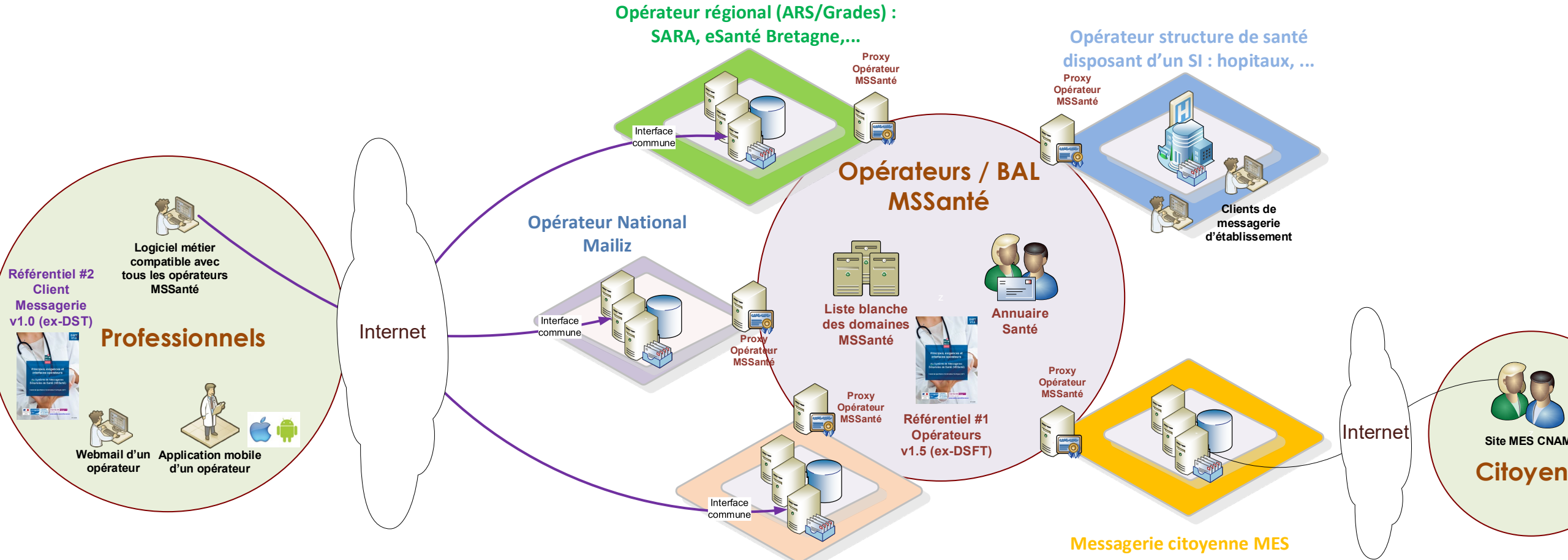
- I. Pourquoi l'API LPS ?
 - Rappel des enjeux
 - Point sur état de sa mise en oeuvre

- II. L'API LPS, c'est quoi ?
 - Grands principes
 - Doctrine d'utilisation

- III. L'API LPS, quelles modalités d'authentification ?
 - BAL PER/ORG : PSC
 - BAL APP : certificat AUTL_CLI

- IV. L'API LPS, quel accompagnement ?
 - Outils tests
 - Ressources et support

I Pourquoi l'API LPS ?



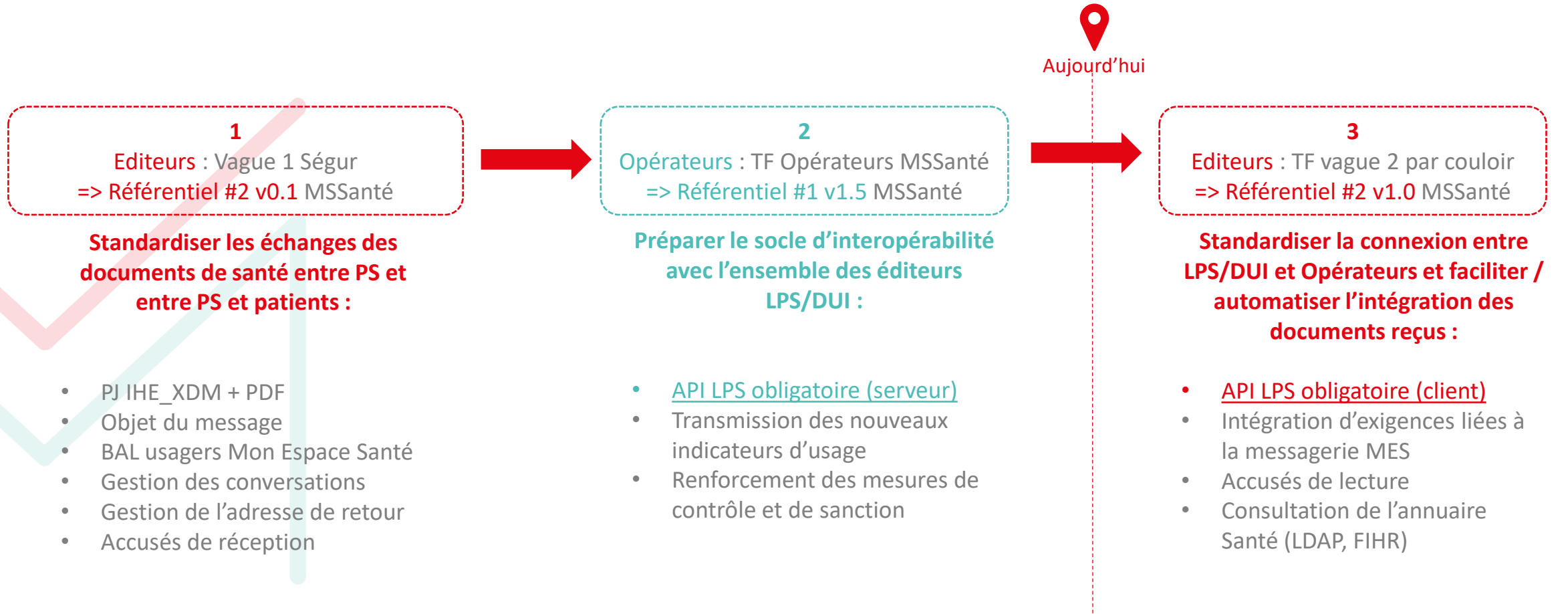
Constats

- La diversité des solutions d'interfaçage proposées par les Opérateurs aux LPS :
- rend les **déploiements complexes** voire impossible pour les éditeurs
 - empêche de **garantir un niveau de sécurité commun** lors du transport des messages,
 - empêche de **proposer des fonctionnalités de messagerie communes** à l'ensemble des professionnels (ex : accusés de lecture ...)

Objectifs

- **Permettre aux éditeurs de LPS/DUI** de s'accrocher avec n'importe quel Opérateur
- **Permettre aux professionnels** de changer :
 - d'Opérateur en conservant son logiciel professionnel
 - de logiciel professionnel sans changer d'Opérateur
- **Ne pas perturber** les intégrations qui fonctionnent en structure

3 grandes étapes pour MSSanté en lien avec le Ségur



Remarque

Concernant les exigences MSSanté présentes dans les REM du Ségur vague 2, toujours se reporter au Ref#2 MSSanté pour disposer du contexte de l'exigence, ainsi que des exemples...

Exigences générales

Exigences applicables à tous les types de BAL :

- exigences API LPS communes aux 3 types de BAL
- exigences indicateurs (présence INS qualifié, type de CDA, id LPS)
- autres exigences : MES, traces, encodage
- + exigences vague 1 adaptées aux évolutions vague 2

Exigences spécifiques BAL PER & ORG

- exigences MIE PSC
- exigences dites « expérience utilisateurs » pour les LPS proposant une IHM aux PS

ou
/
et

Exigences spécifiques BAL APP

- exigence MIE certificat ORG_AUTH_CLI



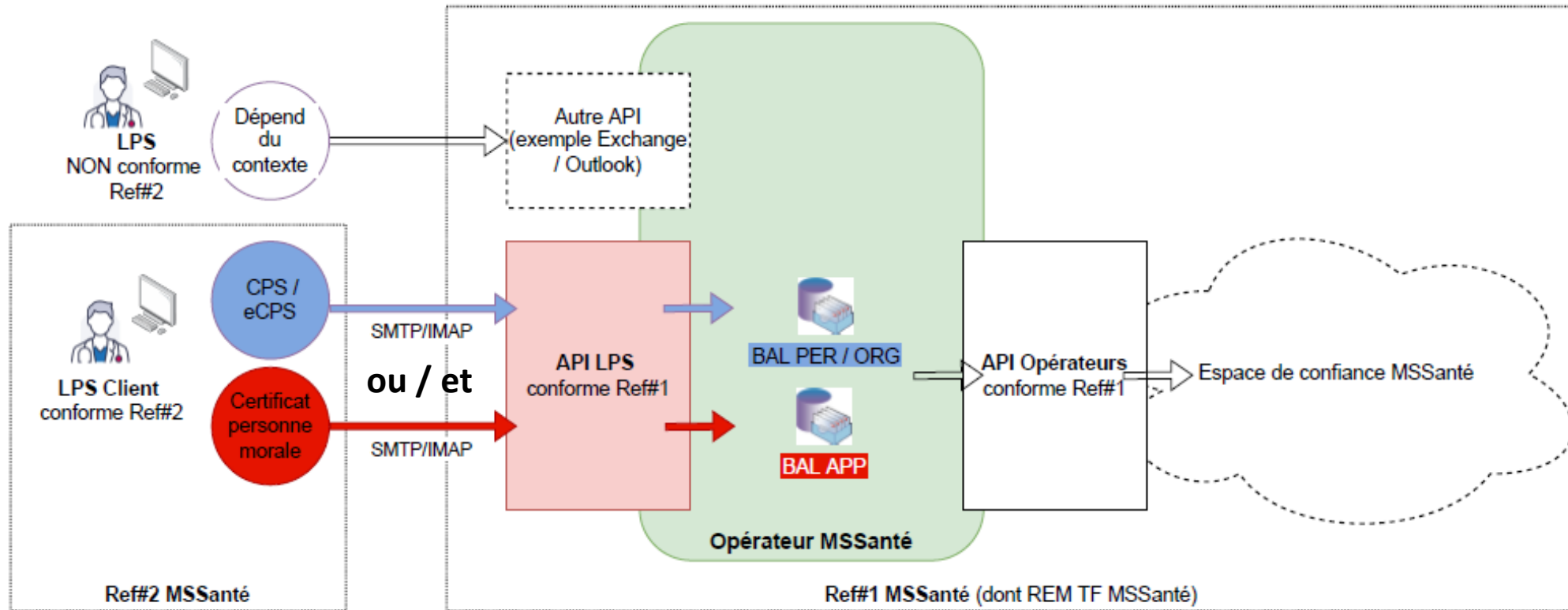
Questions / réponses



II L'API LPS, c'est quoi ?

- Grands principes
- Doctrine d'utilisation

API LPS – Grands principes



Caractéristiques principales

- Obligation d'utiliser les protocoles standards de messagerie (IMAP 4 + SMTP avec StartTLS) + TLS 1.2 minimum
- PSC obligatoire pour l'authentification des personnes physiques : CPS ou eCPS
- Certificat logiciel IGC Santé (ORG AUTH_CLI) obligatoire pour authentifier les personnes morales sur les BAL envoyant des messages automatiquement

Rappels :

- Conçue pour répondre en premier lieu aux éditeurs de LPS **en exercice libéral**
- **En structure** (CH...) les besoins d'interopérabilité des DPI/PFI avec plusieurs Opérateurs sont moindres
- **En structure** (CH...) l'usage de la CPS ou de la eCPS n'est pas généralisée comme moyen d'authentification

Position ANS/DNS :

Le Ref#1 Opérateurs depuis la version 1.5 :

- impose aux Opérateurs de proposer l'API LPS
- mais **n'impose pas de basculer tous les usages sur l'API LPS**. Exemple : Outlook/Exchange, ...

Coté éditeurs de LPS l'implémentation de l'API LPS dépend de chaque couloir :

- API LPS BAL PER/ORG (PSC) : imposée dans les REM **MDV et RIS**
- API LPS BAL APP (auth_cli) : imposée dans les REM **PFI et RIS**

Modalités de transition pour les LPS utilisant d'autres API :

Comme pour les Opérateurs, les LPS doivent **conserver les anciennes interfaces Opérateurs** le temps de la bascule de l'ensemble des PS. Exemple : Mailiz maintient les interfaces DST en parallèle de l'API LPS le temps de la transition



RE_LPS_0200

Le système PEUT proposer, en complément de l'API LPS, des interfaces avec des LPS qui lui seraient spécifiques afin de s'adapter à des contraintes d'un client particulier qui ne pourrait utiliser l'API LPS commune MSSanté. Dans ce cas, l'Opérateur a la responsabilité de s'assurer que les modalités d'authentification employées sont conformes avec le référentiel d'identification électronique de la PGSSI-S.



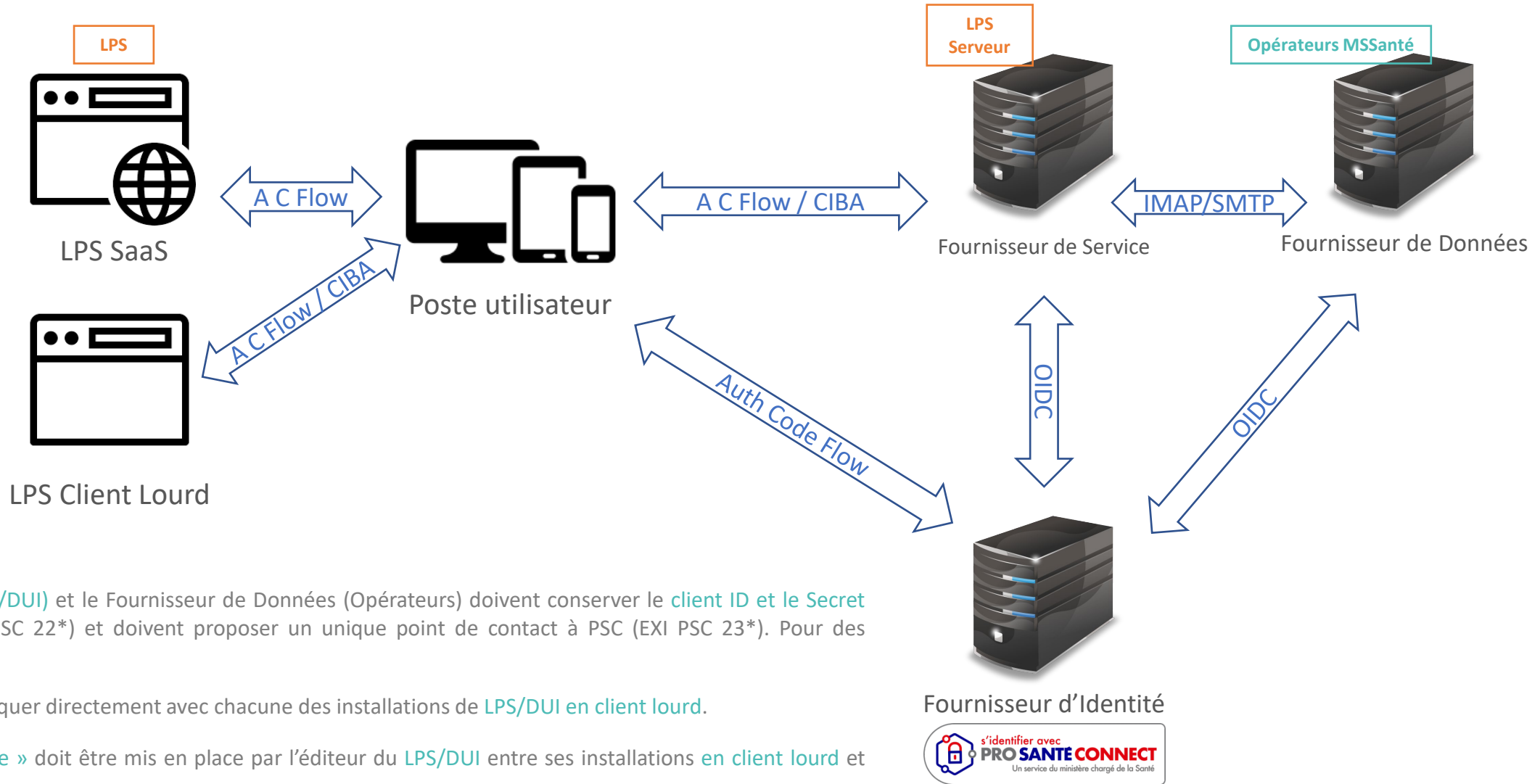
Questions / réponses

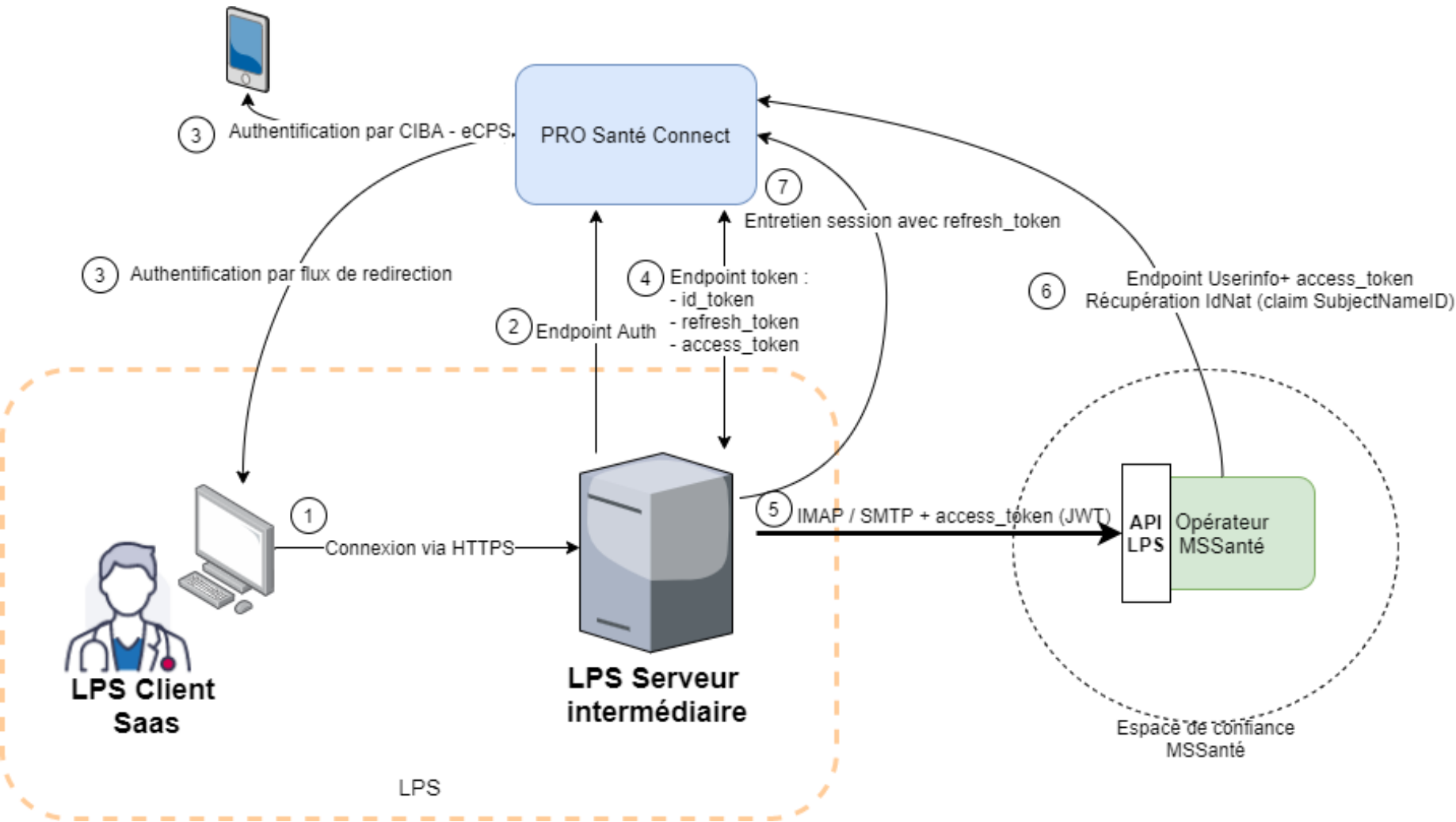


III L'API LPS, modalités d'authentification

- BAL PER/ORG : PSC
- BAL APP : certificat AUTL_CLI

PSC : Modalités d'utilisation via une API

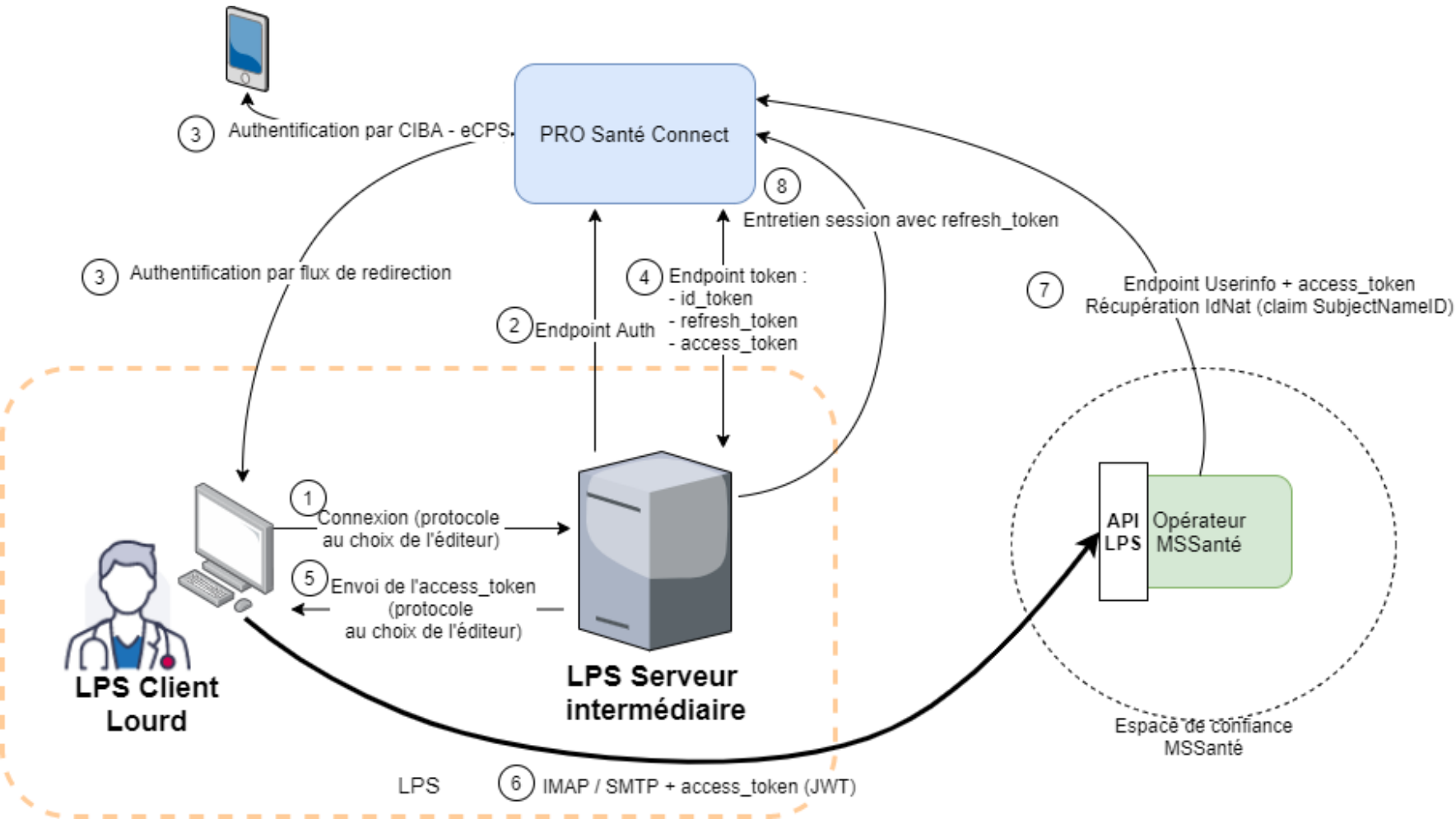




Spécificités

Rappel : La démarche de raccordement du Serveur Intermédiaire à PSC doit être menée par l'éditeur LPS/DUI

- L'access_token doit être transmis à l'Opérateur via les requêtes IMAP ou SMTP



Spécificités

L'access Token est récupéré par le LPS Serveur Intermédiaire, puis transmis au LPS client lourd

Étape 5 :

- Pour des raisons de sécurité, l'Access Token PSC au format JWT ne doit pas être stocké de façon permanente sur le poste de travail du professionnel. Il doit être mémorisé de façon temporaire, pour une durée correspondant à sa durée de vie.
- Le moyen de mémorisation de l'Access Token PSC doit être protégé des accès et attaques externes. Le niveau de sécurisation utilisé pour la mémorisation temporaire doit être éprouvé.

Objectif :

Transmettre l'`access_token` à l'Opérateur via IMAP ou SMTP

Modalité :

- Mécanisme SASL d'authentification OAuth 2.0 avec l'implémentation **XOAUTH2**
- Structure de la chaine d'authentification XOAUTH2 :

```
base64("user=" {User} "^Aauth=Bearer " {Access Token PSC} "^A^A")
```

Avec :

User : adresse email de la BAL à utiliser

^A : le caractère contrôle+A (\001)

Gestion des erreurs d'authentification par le LPS/DUI :

Le LPS doit gérer les **codes d'erreur** d'authentification (IMAP : RFC 5530, SMTP : RFC 4954) transmis par l'Opérateur

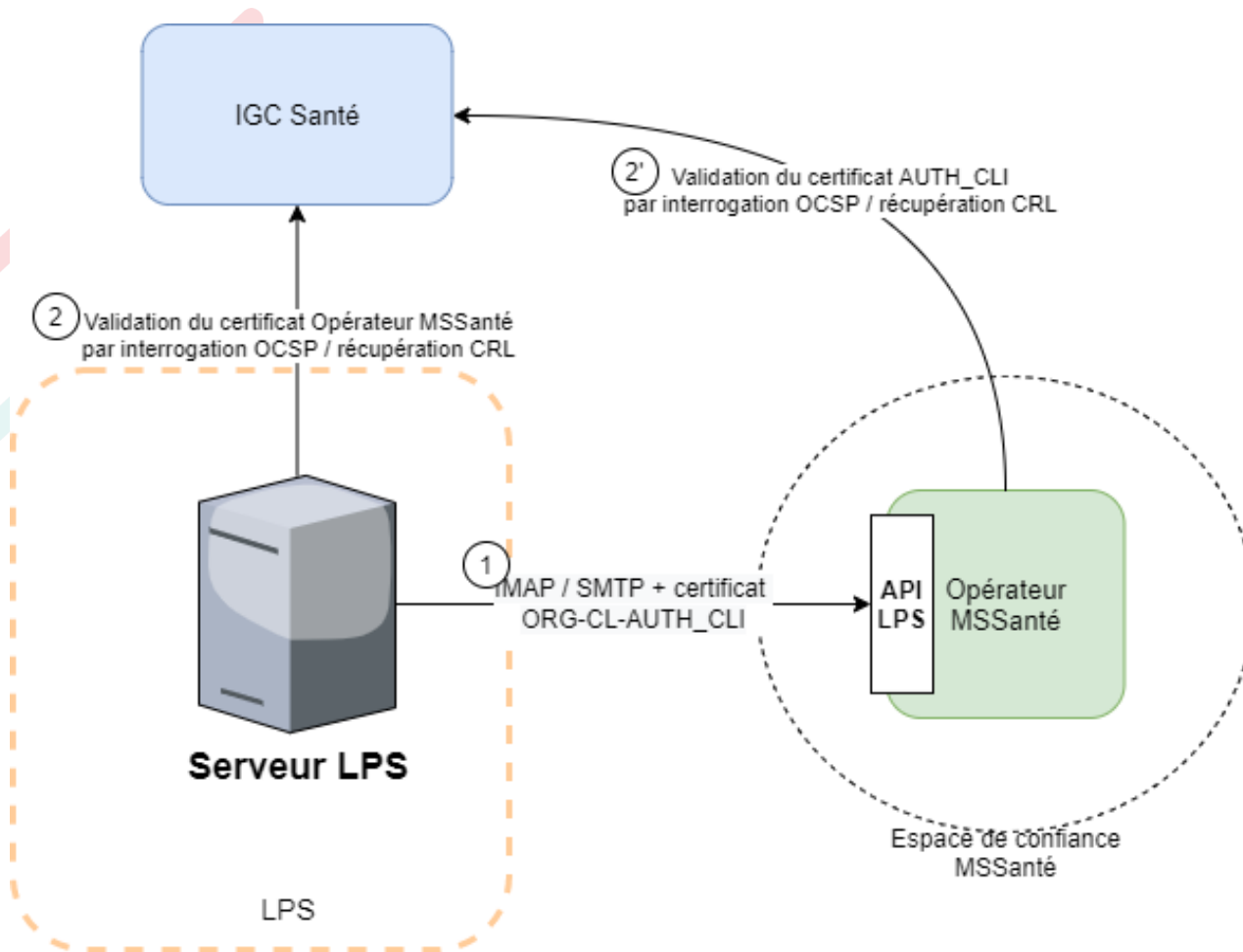
Objectifs :

- Maintenir la session utilisateur, sans redemander une identification électronique au professionnel
- Fermer les sessions IMAP/SMTP lors de la déconnexion PSC
- Suite à la détection d'une fin de session IMAP ou SMTP déclenchée par l'Opérateur MSSanté, lorsque l'authentification PSC est toujours valide, le LPS pouvoir **réouvrir automatiquement une session IMAP ou SMTP** (i.e. sans intervention du PS)

Modalités :

- Le LPS serveur intermédiaire doit renouveler le Refresh Token, avant son expiration
- Le LPS doit détecter la déconnexion PSC pour fermer les sessions IMAP/SMTP avec l'Opérateur
- Cas client lourd : si le Refresh Token devient invalide, le LPS serveur intermédiaire doit demander au LPS de mettre fin à la session utilisateur

BAL APP: Cinématique d'authentification



Spécificités

- Détenir un certificat logiciel ORG AUTH_CLI de l'IGC Santé rattaché à la structure qui détient la BAL
- Un même certificat peut être utilisé par plusieurs BAL de la structure, voire pour accéder à différents plusieurs services esante

Etape 1 :

- Monter la session TLS avec STARTTLS en présentant le certificat ORG AUTH_CLI
- Transmettre l'adresse de la BAL dans le login de la méthode d'authentification PLAIN

Structure du DN du certificat :

CN=<libre>

OU=<IdNatStruc>

O=<NomStruc>

ST=<département> (XX)

C=FR

Objectif :

Simplifier la configuration des BAL dans les LPS en exposant les FQDN des interfaces IMAP/SMTP des opérateurs

Modalités :

- Mécanisme standard basé sur la **déclaration DNS du domaine de l'adresse de la BAL**
 - Le LPS peut récupérer via DNS les FQDN des serveurs SMTP et IMAP de l'opérateur (interface BAL PER/ORG et APP)
1. Interroger le DNS du domaine de la BAL pour récupérer les **attributs _submission._tcp & _imap._tcp de type SRV**, afin d'obtenir les points d'entrée (hostname + port) SMTP et IMAP,
 2. Suivant le type de BAL à configurer, les points d'entrée à utiliser sont spécifiés en fonction de la **priorité de l'attribut** : 10 (PER/ORG) ou 20 (APP)

```
_submission._tcp SRV 10 1 587 [FQDN front smtp psc de l'opérateur]  
_submission._tcp SRV 20 1 587 [FQDN front smtp authcli de l'opérateur]  
_imap._tcp SRV 10 1 143 [FQDN front imap psc de l'opérateur]  
_imap._tcp SRV 20 1 143 [FQDN front imap authcli de l'opérateur]
```



Questions / réponses



IV L'API LPS, quel accompagnement ?

- Outils tests
- Ressources et support

OBJECTIFS

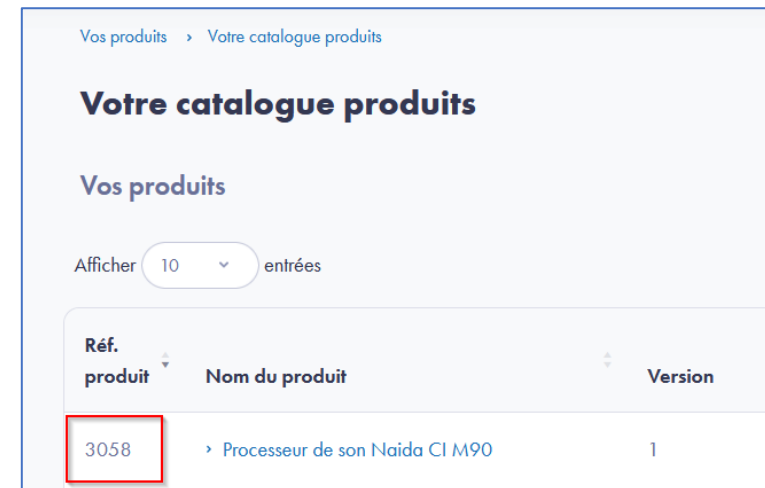
- Mettre à disposition un environnement de test/recette pour la mise en œuvre de l'API LPS
- Permettre aux solutions de messagerie de vérifier leur conformité à certaines exigences du Ref #2
- Confirmer la bonne mise en œuvre de l'interface API LPS avant accrochage avec des Opérateurs en production
- Produire un CR de test attestant de la conformité de la solution aux exigences du Ref #2 (*utilisé pour le référencement Ségur vague 2*)

FONCTIONALITES

- Simuler un Opérateur « de référence avec l'API LPS » (*isolé de l'Espace de Confiance de test pour l'instant*)
- Proposer 2 BAL de test (PER/ORG & APP) accessibles à travers l'API LPS (*PSC et certificat AUTH_CLI*) et un webmail
- Un même compte utilisateur permet de tester plusieurs logiciels d'un même éditeur

PREREQUIS

- Un compte ouvert sur « Industriel Santé Connect » pour accéder à MOTCO2 (*isconnect.esante.gouv.fr/enrollement/user/start?*)
- Avoir déclaré la(les) solution(s) qui fera(ont) l'objet des tests sur la plateforme « Convergence » afin d'obtenir un NIL (*convergence.esante.gouv.fr*)
- Être en possession d'identité de test (*identifiant national*):
 - À travers une CPx de test (*identité personne physique ou certificat AUTH_CLI*)
 - À travers EDIT sur l'environnement « bac à sable » de PSC qui permet la création d'une identité de test (*identité personne physique non reliée à l'annuaire partenaire*)



Vos produits > Votre catalogue produits

Votre catalogue produits

Vos produits

Afficher 10 entrées

Réf. produit	Nom du produit	Version
3058	> Processeur de son Naida CI M90	1

Plateforme Convergence

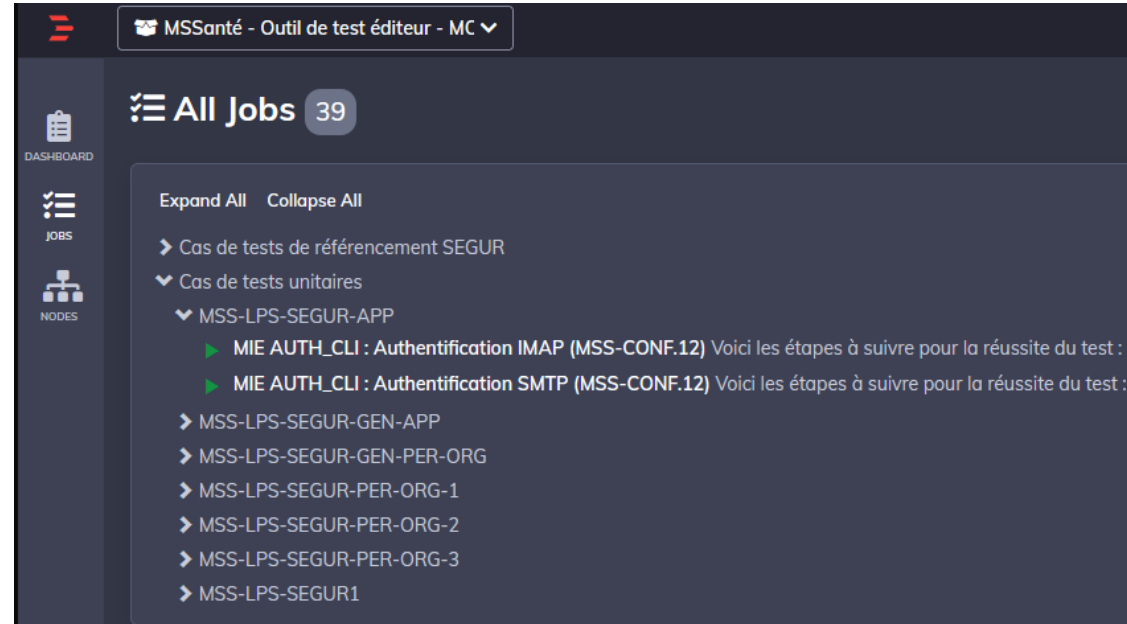
PRINCIPE DE FONCTIONNEMENT

- Cas de tests unitaires
 - **BAL PER&ORG** : MOTCO2 présente 18 tests unitaires qui permettent de vérifier des exigences liées aux BAL PER ou ORG du Référentiel #2
 - **BAL APP** : MOTCO2 présente 16 tests unitaires qui permettent de vérifier des exigences liées au BAL APP du Référentiel #2
- Cas de tests de référencement
 - **BAL PER&ORG** : permet de valider sa conformité à tous les tests unitaires concernant les BAL PER ou ORG (tous les tests sont lancés par un seul job)
 - **BAL APP** : permet de valider sa conformité à tous les tests unitaires concernant les BAL APP (tous les tests sont lancés par un seul job)

Liste de comptes

Référence produit (NIL)	Identifiant national PSC	Identifiant national AUTH_CLI	Statut	Action	Accès à l'outil
123456789	871112231433	18900456	Créé	Modifier	Accès à l'outil

[Créer un nouveau compte](#)



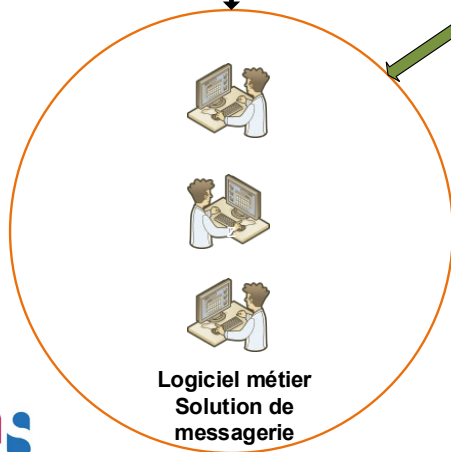
The screenshot shows the 'MSSanté - Outil de test éditeur - MC' interface. It features a sidebar with 'DASHBOARD', 'JOBS', and 'NODES' sections. The main area displays 'All Jobs 39' with a tree view of test cases. The tree is expanded to show 'Cas de tests unitaires' with sub-items like 'MSS-LPS-SEGUR-APP' and 'MSS-LPS-SEGUR-GEN-APP'. Each item has a right-pointing arrow and a brief description.

MOTCO2 : environnement de test/recette pour l'API LPS

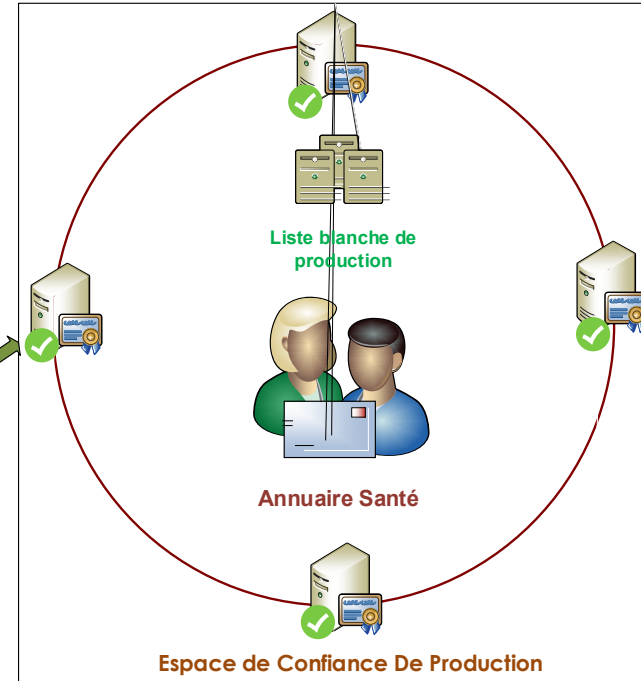
✓ API LPS déployée



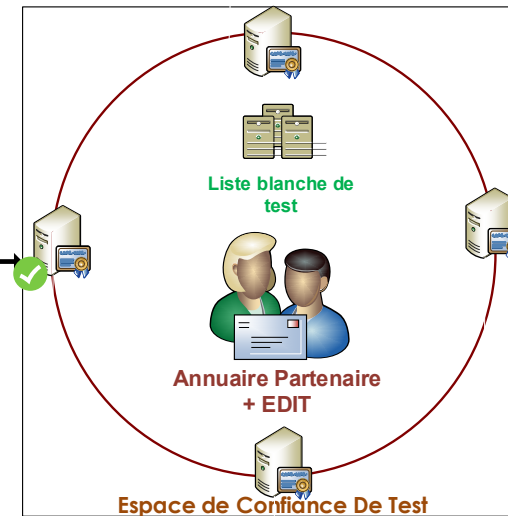
1 - mise en œuvre API LPS



2 - interfaçage en production



mise en œuvre API LPS
facultatif



RESSOURCES

- **REFERENTIEL #2 v1.0.1 client de messagerie MSSanté** (publié le 18/01/2024)
<https://mssante.fr/is/doc-technique#ref2>
- **Guide utilisateur et lien d'accès à MOTCO2**
<https://mssante.fr/is/doc-technique>

SUPPORT

- **MOTCO2** : toute question liée à MOTCO2 doit être adressée à la BAL « monserviceclient.mssante@esante.gouv.fr ». Avec dans l'objet du mail le mot clé **[MOTCO2]** pour une meilleure prise en charge
- **API LPS** : toute question liée à l'API LPS doit également être adressée à la même BAL avec le mot clé **[API LPS]** dans l'objet du mail toute difficulté d'interfaçage avec un Opérateur pourra nous être remontée
- **PSC** : en intégrant Pro Santé Connect, vous bénéficiez du support de l'ANS sur l'authentification par CPS et e-CPS :
 - <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect>
 - Formulaire de contact « industriels ANS » : <https://industriels.esante.gouv.fr/contactez-nous/formulaire>
 - Email : prosanteconnect.editeurs@esante.gouv.fr

Inscription à la liste de diffusion 'éditeurs MSSanté' pour recevoir les actualités relatives aux Référentiel #2 et l'API LPS (webinaires, MAJ MOTCO2, ...).

Sélectionnez « Editeur » comme « entité » et cocher inscription à la newsletter « Les actualités techniques MSSanté »

<https://esante.gouv.fr/formulaire-mssante>

OBJECTIFS :

Permettre de tester (hors prod) la réception et l'intégration d'une archive IHE_XDM par messagerie MSSanté en respectant le format d'échange décrit dans le référentiel #2 MSSanté

FONCTIONNEMENT :

1. Le LPS envoie un message MSSanté à une des adresses MSSanté de test du répondeur
2. Le répondeur retourne un message automatique à l'expéditeur contenant un document d'un patient test : CR de biologie ou volet de synthèse médicale

MODALITES :

1. Configurer dans le LPS une BAL de test d'un Opérateur branché sur l'espace de confiance de test

Rq : par exemple via [l'environnement dit « de formation » de Mailiz](#) qui permet d'obtenir une BAL de test depuis une CPS de test

2. Ecrire à vsm@repondeur.formation.mssante.fr ou crbio-xdm@repondeur.formation.mssante.fr

PERSPECTIVES :

Un nouvel outil sera prochainement proposé pour retourner n'importe quel exemple de documents disponible coté CI-SIS, mais aussi les entêtes SMTP décrites dans la vague 2 Ségur



Questions / réponses



Conclusion et prochaines étapes

Synthèse :

1. L'API LPS répond à une problématique d'interopérabilité ancienne remontée par les éditeurs
2. L'API LPS est maintenant disponible chez les Opérateurs
3. Les ressources et les outils de test sont disponibles

=> L'ANS/DNS incite les éditeurs à intégrer l'API LPS sans attendre le lancement de la vague 2 du Ségur

Prochaines étapes :

- **Outil de test MOTCO2 :**
 - A l'écoute de vos retours
 - Besoin de confirmer le fonctionnement des cas de test avec plus d'éditeurs pour sortir de la phase Beta
- **Support éditeurs LPS à l'intégration de l'API LPS**
 - En fonction des questions reçues, on envisage de proposer des instances d'échanges périodiques avec les éditeurs
- **Suivi des accrochages LPS/Opérateurs en production via l'API LPS**
- **Lancement de la vague 2 Ségur**



Questions / réponses



Merci pour votre participation !



Annexes



L'ouverture officielle de l'API LPS pour les éditeurs de logiciels LPS/DUI. Cela signifie que vous pouvez dès à présent :

- intégrer l'API LPS dans vos solutions,
- recetter vos développements avec un nouvel outil de tests et de contrôles éditeurs MOTCO2 (informations ci-après),
- les interfacier en production avec les API LPS des Opérateurs MSSanté (via un mécanisme d'autoconfiguration).

Pourquoi une interface standardisée ?

Un des freins au déploiement de la MSSanté était la difficulté d'intégrer les accès aux BAL des Opérateurs dans les solutions des LPS/DUI, du fait de l'existence de multiples interfaces propriétaires des Opérateurs MSSanté.

L'objectif de l'API LPS est de simplifier vos développements et déploiements, et de vous permettre d'offrir de la souplesse à vos clients pour accéder aux BAL et Opérateurs MSSanté de leur choix.

Conception et déploiement de l'API LPS :

Depuis fin 2021, l'ANS et les Opérateurs MSSanté ont lancé une démarche de mise en œuvre d'une interface commune : l'API LPS. Celle-ci définit un unique protocole (IMAPS/SMTPS), ainsi que des méthodes d'authentification associées à chaque type de BAL (PSC et certificat). Depuis novembre 2023 tous les Opérateurs MSSanté ont été certifiés conformes avec l'API LPS via le dispositif Ségur TF Opérateurs.

Côté éditeurs de LPS/DUI, l'ANS publiait en janvier 2023 la [version 1.0 du référentiel #2 Clients de messagerie MSSanté](#) qui

spécifie l'API LPS. Ces mêmes exigences seront reprises dans les référentiels des différents couloirs de la vague 2 Ségur. Les éditeurs peuvent donc intégrer l'API LPS sans attendre la publication de la vague 2 Ségur.

Doctrine d'utilisation de l'API LPS :

Tout LPS/DUI devra s'interfacier avec l'API/LPS d'un Opérateur. Pour autant, un logiciel peut continuer à s'interconnecter avec une interface propriétaire d'un Opérateur, qui devra être conforme avec la PGSSI-S. Ceci a en particulier été prévu pour les accès aux BAL nominatives et organisationnelles des établissements de santé. La bascule des usages sur l'API LPS n'est pas imposée dans le cas où l'accès via PSC n'est actuellement pas possible.

Ouverture de l'outil de tests et de contrôle MOTCO2* :

Après une phase pilote, l'outil MOTCO2 vient d'être ouvert en beta à tous les éditeurs. Il propose à chaque éditeur :

- des BAL de test exposant l'API LPS (indépendante de tout Opérateur),
- un ensemble de cas de tests passants et non passants permettant d'évaluer la conformité du logiciel testé aux exigences MSSanté.

Pour plus d'informations, se référer à la [page industriel](#) du site www.mssante.fr, rubrique « Documentation technique ».

Accompagnement éditeurs :

Afin de mieux appréhender l'état des lieux des interfaçages actuels des LPS/DUI avec les Opérateurs, nous demandons à chaque éditeur concerné de déclarer les interfaces propriétaires

des Opérateurs qu'il a implémentées jusqu'à présent, en remplissant ce [formulaire](#) d'ici le 12 janvier 2024. C'est une information importante, qui sera prise en compte pour la transition vers l'API LPS avec le moins d'impact possible sur les professionnels. C'est en particulier le cas des éditeurs s'interfaçant avec Mailiz via les WS SOAP.

Un Webinaire sera organisé le 19 janvier 2024 à 14h afin d'accompagner les éditeurs dans l'intégration de l'API LPS : inscription. Si besoin des sessions régulières d'échange avec les équipes MSSanté afin de répondre rapidement aux questions des éditeurs.

Le support monserviceclient.mssante@esante.gouv.fr reste à votre disposition pour toute demande de précision concernant l'outil MOTCO2 ou le référentiel #2 v1.0. Merci d'indiquer dans l'objet de votre demande le mot clé "[MOTCO2]".

Nous vous invitons aussi à vous inscrire sur [notre liste de diffusion « éditeurs MSSanté »](#) pour continuer à recevoir les informations MSSanté relatives à l'API LPS (webinaires, MAJ MOTCO2, ...). Sélectionnez « Editeur » comme « entité » et cocher inscription à la newsletter « Les actualités techniques MSSanté ».

Bien cordialement,

L'équipe projet MSSanté

*MSSanté Outil de Tests et de Conformité au Référentiel #2