MS Santé
Système de messageries sécurisées, données protégées.

Segur vague 2

Concertation exigences MSSanté

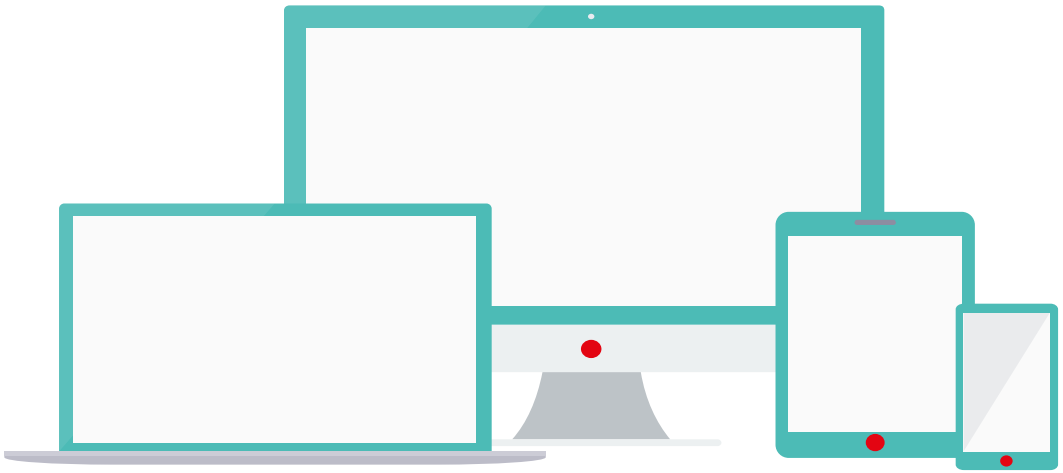
Atelier Editeurs #1 du 20/05/2022

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ

Afin que la réunion soit agréable pour tous

- Mettre son micro **en muet** lors des temps d'explication
- Privilégier le chat en ligne pour poser ses questions
- **La réunion sera enregistrée sauf opposition**



Pour intervenir :

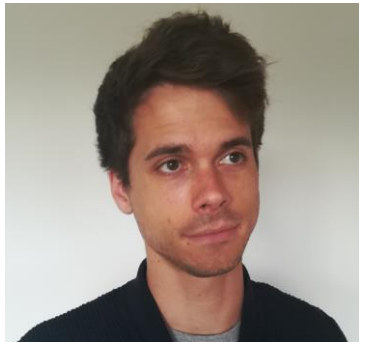
- Utiliser la fonction « lever la main » et attendre l'aval des conférenciers
- Ou **utiliser le chat en ligne.** Nous vous répondrons à la fin de la présentation de chaque l'intervenant.

Introduction

Intervenants et organisateurs

Gestion de l'Espace de Confiance MSSanté
Edouard BRIS

Gestion de l'Espace de Confiance MSSanté
Mike GUEYE



Architecte applicatif MSSanté
Bastien DANGIN

Pro Santé Connect
Joachim METZGER

Objectifs / démarche des ateliers

Objectifs :

1. Présenter en détail la nouvelle API LPS que les opérateurs doivent proposer avant fin 2022
2. Définir les exigences du référentiel #2 v1.0. Cad les exigences MSSanté communes à l'ensemble de TF Ségur

Thématiques des exigences à concerter :

- L'API LPS
- Les modalités d'échange avec la messagerie de MES
- Les indicateurs Ségur à remonter à l'ANS sur le contenu des messages envoyés
- Les modalités de consultation de l'annuaire santé
- Autres sujets proposés par les éditeurs ...

Démarche proposée :

- 3 ateliers planifiés avec les éditeurs de toutes les TF (~40 éditeurs inscrits). Probablement d'autres nécessaires.
- Partage d'un tableau d'exigences « draft » pour remarques des éditeurs (à partir de l'atelier 2)
- Concertation publique du référentiel avant publication v1.0

SOMMAIRE

I Positionnement des travaux MSSanté dans le Ségur

Rappel : Enjeux et objectifs du Segur pour MSSanté

Enjeux

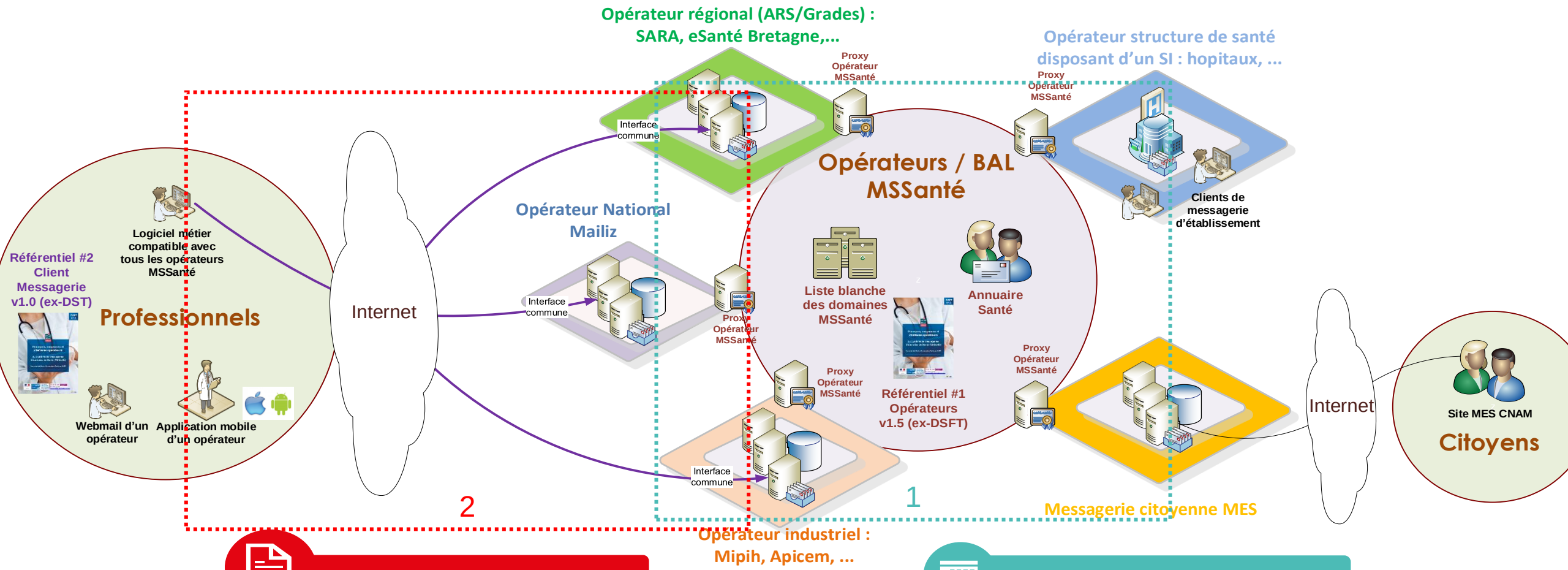
- Les LPS/DUI ne peuvent proposer leur solution qu'aux clients qui ont choisi certains opérateurs MSSanté -> déploiements complexes et ralentis
- La diversité des solutions d'interfacage proposés par les opérateurs empêche de:
  - garantir un niveau de sécurité commun lors du transport des messages,
  - 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 l'opérateur quelque soit celui choisi par son client (professionnel ou structure)
- Permettre aux professionnels de changer :
  - d'opérateur en conservant son logiciel professionnel
  - de logiciel professionnel sans changer d'opérateur

- Améliorer les modalités de régulation de l'espace de confiance MSSanté
- Disposer de nouveaux indicateurs d'usage : INS et documents structurés

Rappel : Espace de confiance MSSanté – Etat des API



2 - Interfaces LPS/DUI - opérateurs

- Jusqu'à présent aucune API commune n'était imposée par les référentiels MSSanté pour les échanges LPS/DUI
- Pas de référentiel MSSanté opposable aux éditeurs de LPS/DUI, mais le référencement Ségur va permettre d'introduire une API commune entre opérateurs et éditeurs

1 - Interface entre opérateurs MSSanté

- Est standardisée depuis le lancement de l'Espace de Confiance MSSanté en 2014

Segur – 3 grandes étapes pour MSSanté

1
Editeurs : TF vague 1 par couloir
=> Référentiel #2 v0.1 MSSanté

2
Opérateurs : TF Opérateurs MSSanté
=> Référentiel #1 v1.5 MSSanté

3
Editeurs : TF vague 2 par couloir
=> Référentiel #2 v1.0 MSSanté

Standardiser les échanges des documents de santé entre PS et vers les patients :

- PJ CDA + PDF
- Objet du message
- Adresses patients MES
- Gestion des conversations
- Gestion de l'adresse de retour
- Accusés de réception

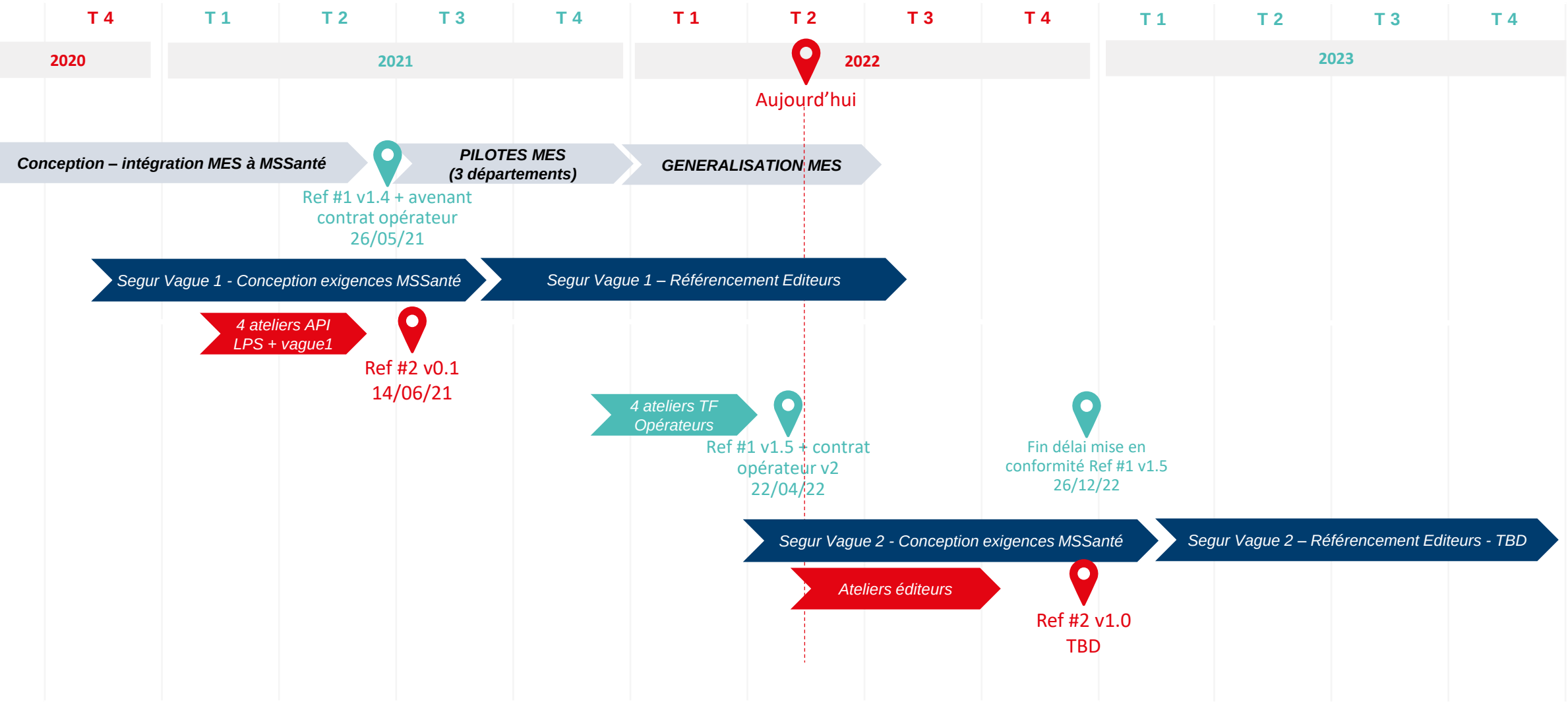
Préparer le socle d'interopérabilité avec l'ensemble des éditeurs LPS/DUI :

- API LPS obligatoire (serveur)
- Transmission des nouveaux indicateurs d'usage
- Renforcement des mesures de contrôle et de sanction

Standardiser la connexion entre LPS/DUI et opérateurs :

- API LPS obligatoire (client)
- Intégration d'exigences liées à la messagerie MES
- Accusés de lecture / bonne intégration
- Consultation de l'annuaire Santé (LDAP / FIHR)

Segur – Macro planning pour MSSanté



Segur – Retour sur le Task Force Opérateurs

Objectifs :

- Spécifier la nouvelle API LPS avec les opérateurs et éditeurs
- Adapter les modalités de régulation de l'Espace de Confiance (contrôles – sanctions en cas de non-conformité)
- Définir des exigences opérateurs permettant le référencement des opérateurs « développeurs »
- Evaluer le coût de mise en conformité pour un opérateur MSSanté avec le référentiel #1 v1.5, afin de proposer un financement adapté (dispositif SONS)

Participants :

13 opérateurs MSSanté

15 éditeurs de logiciel

Mise en conformité au référentiel #1 v1.5 : avant le 26/12/2022

Publication de l'arrêté de financement de la TF : A venir (probablement fin mai – début juin)

MS Santé
Système de messageries sécurisées, données protégées.

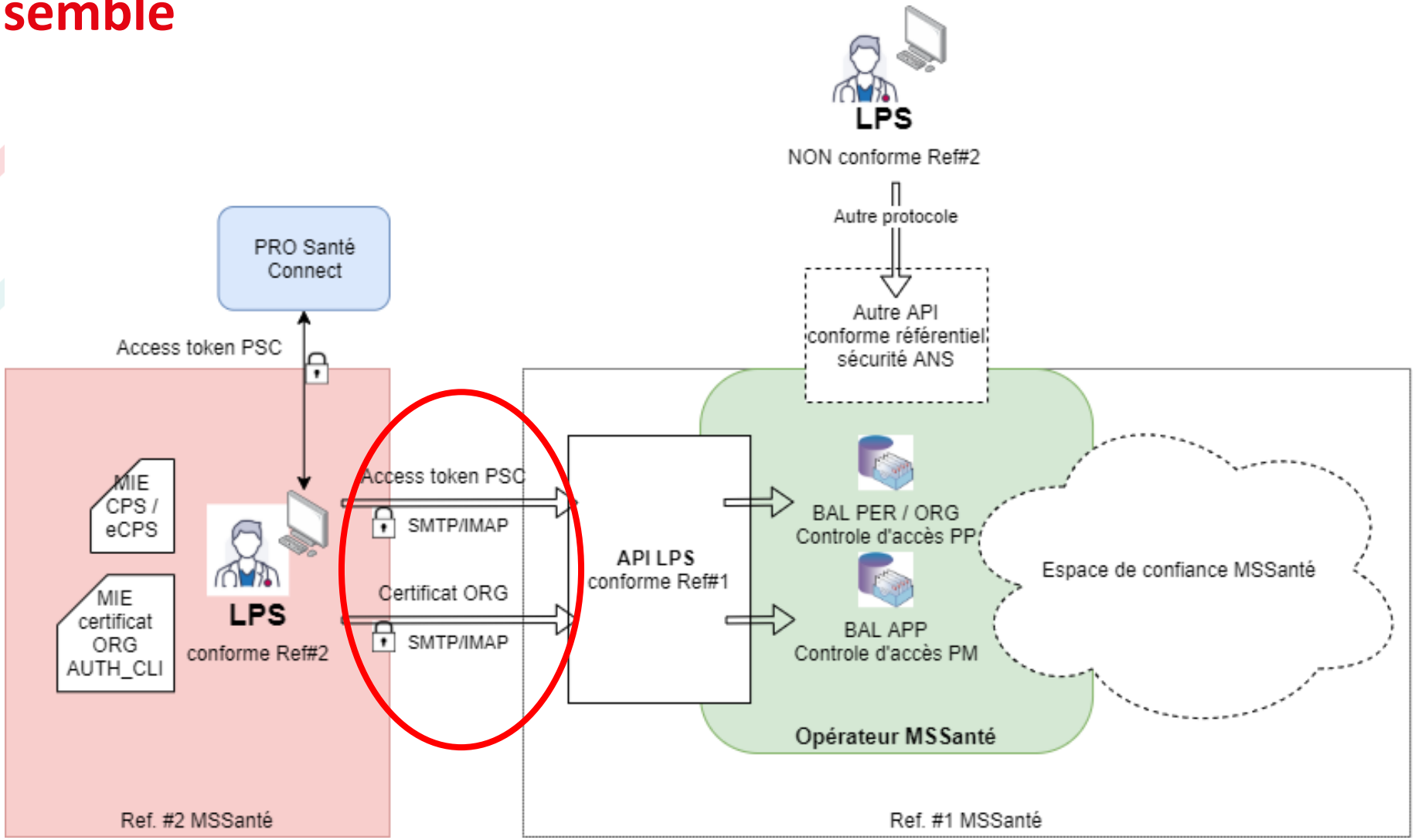
Questions / réponses

II Focus API LPS :

Grands principes

Grands principes de l'API LPS

Vue d'ensemble



Grands principes de l'API LPS

Dans le détail …

- Utilisation des protocoles applicatifs :
  - **SMTP** avec STARTLS sur le port 587 (RFC 5321)
  - **IMAP4** rev1 ou rev2 avec STARTTLS sur le port 143 (RFC 3501, 9051)
- Choix réalisés à l'issue de la consultation des opérateurs (et éditeurs) - ateliers menés T2 2022 - et d'une évaluation faite au moyen d'un POC

- Niveau minimum de TLS requis : **1.2** (RFC 5246)

- 2 Moyens d'Identification Electronique (MIE) :
  - **Pro Santé Connect** : CPS / eCPS (personne physique) pour accès **BAL personnelles et organisationnelles**. Transmission de l'Access Token à l'opérateur
  - **Certificat ORG AUTH_CLI** (personne morale) pour accès **BAL applicatives**

Grands principes de l'API LPS

Dans le détail …

- Mécanisme d'autoconfiguration proposé par chaque opérateur pour décrire les 2 points d'entrée de l'API LPS :

https://autoconfig.{emailaddressdomain}/mail/config-v1.1.xml

```
<incomingServer type="imap">
                <hostname>{front-mie-psc-operateur}</hostname>
                <port>143</port>
                <socketType>STARTTLS</socketType>
                <authentication>OAuth2</authentication>
                <username>%EMAILADDRESS%</username>
 </incomingServer>
```

MS Santé
Système de messageries sécurisées, données protégées.

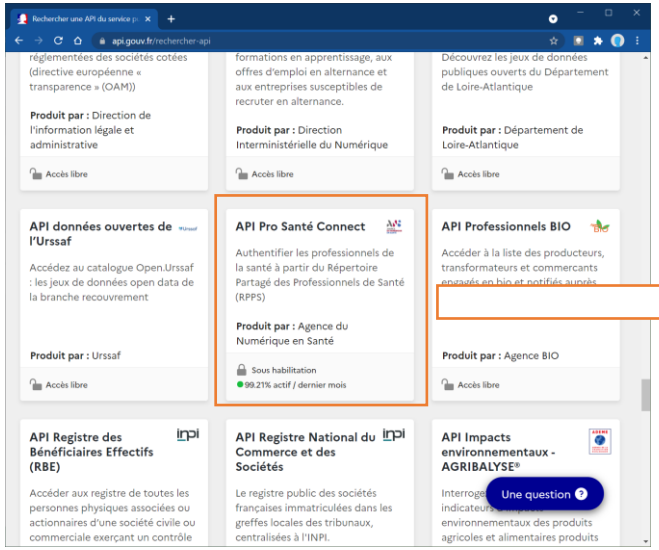
Questions / réponses

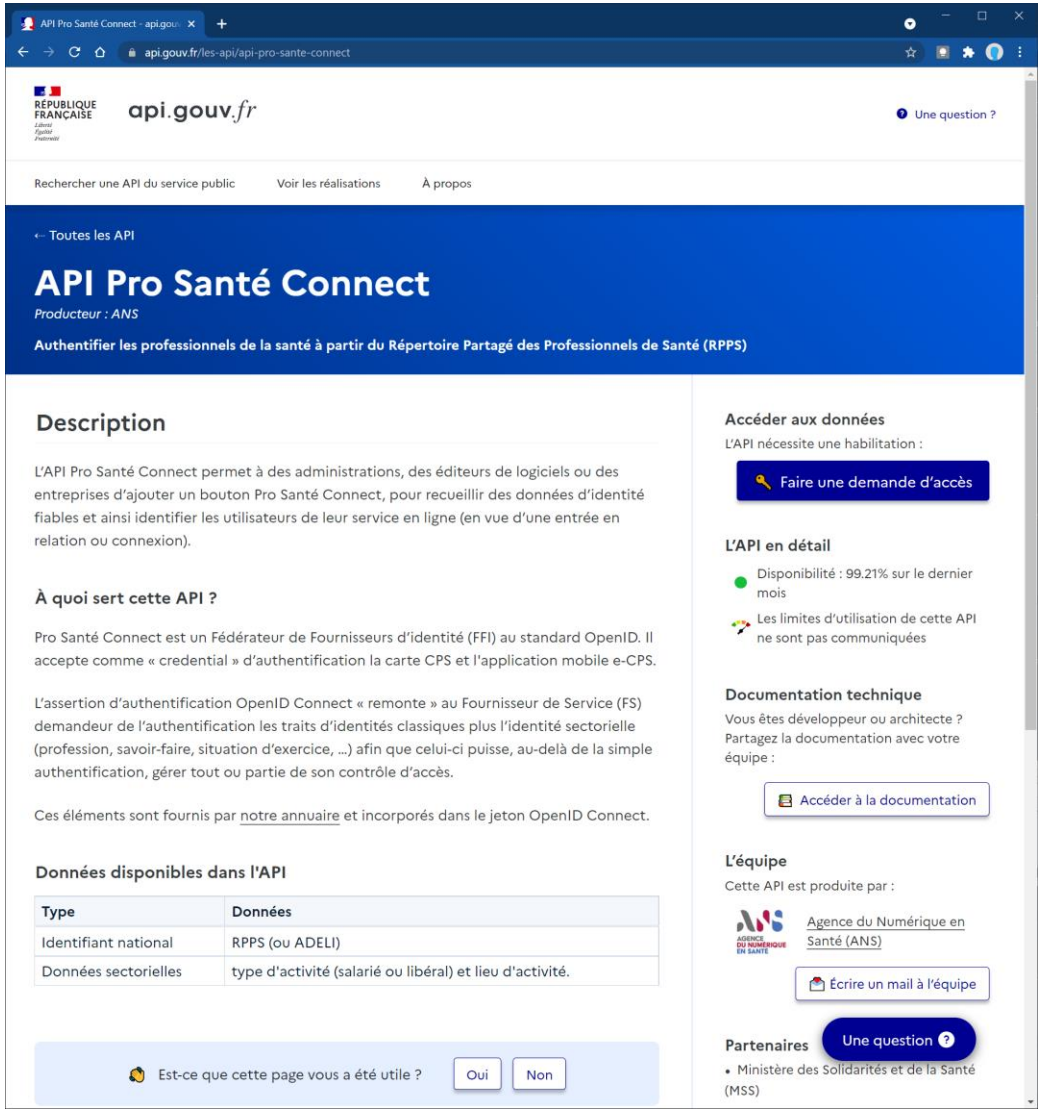
II Focus API LPS :

Modalités d’utilisation de PSC sur une API

Parcours Industriel Pro Santé Connect

Pro Santé Connect est disponible via API.gouv

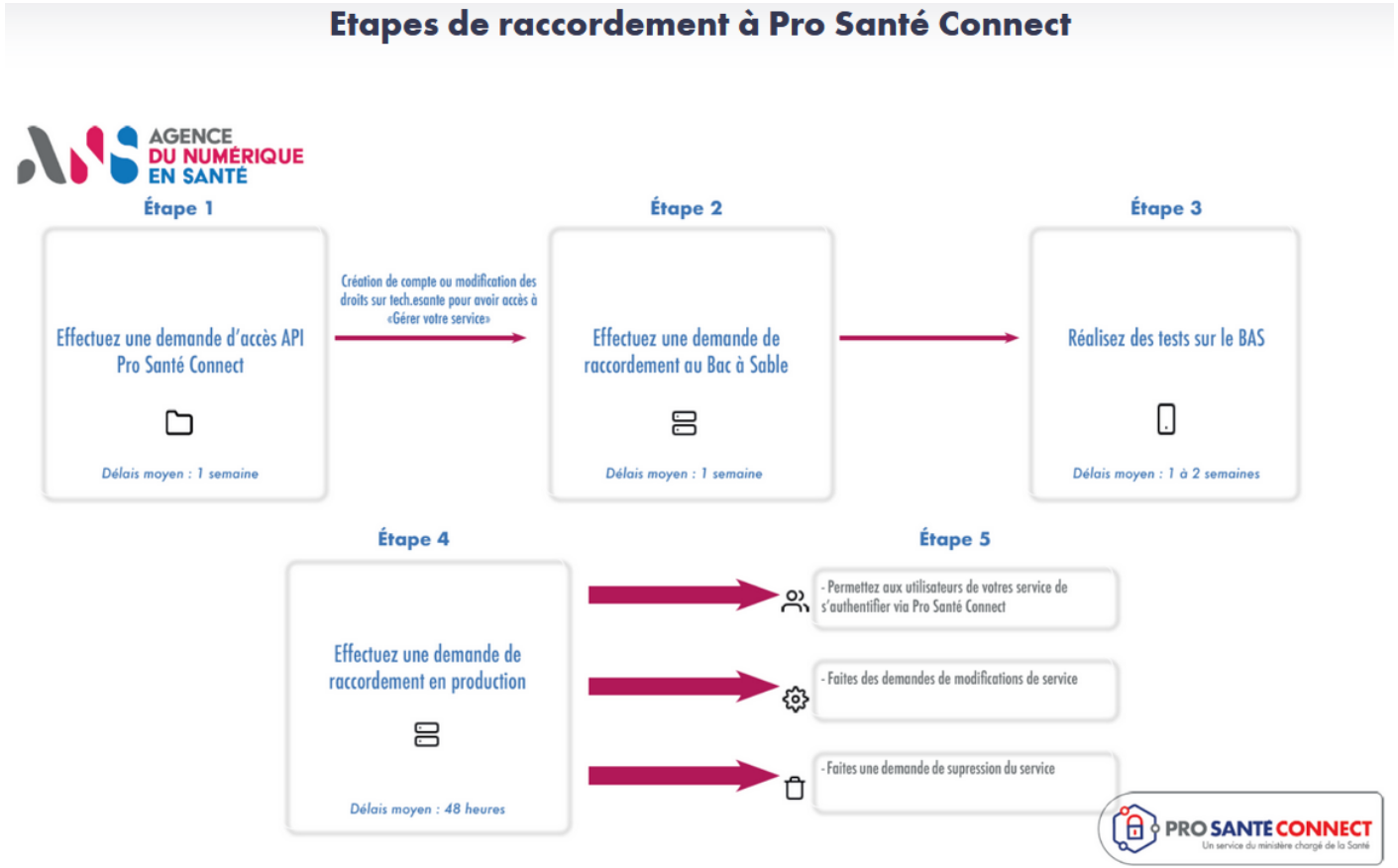




Parcours Industriel Pro Santé Connect

Une fois l'inscription sur API.gouv validée, les demandes d'accès et de gestion du service s'effectuent sur le Portail Industriels :

https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect



Arrêté e-CPS et Pro Santé Connect

L’arrêté relatif à des moyens d'identification électronique immatériels mis à disposition des professionnels, personnes physiques des secteurs sanitaire, social et médico-social pour l'utilisation des services numériques en santé a été **publié le 4 avril 2022**

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045551195

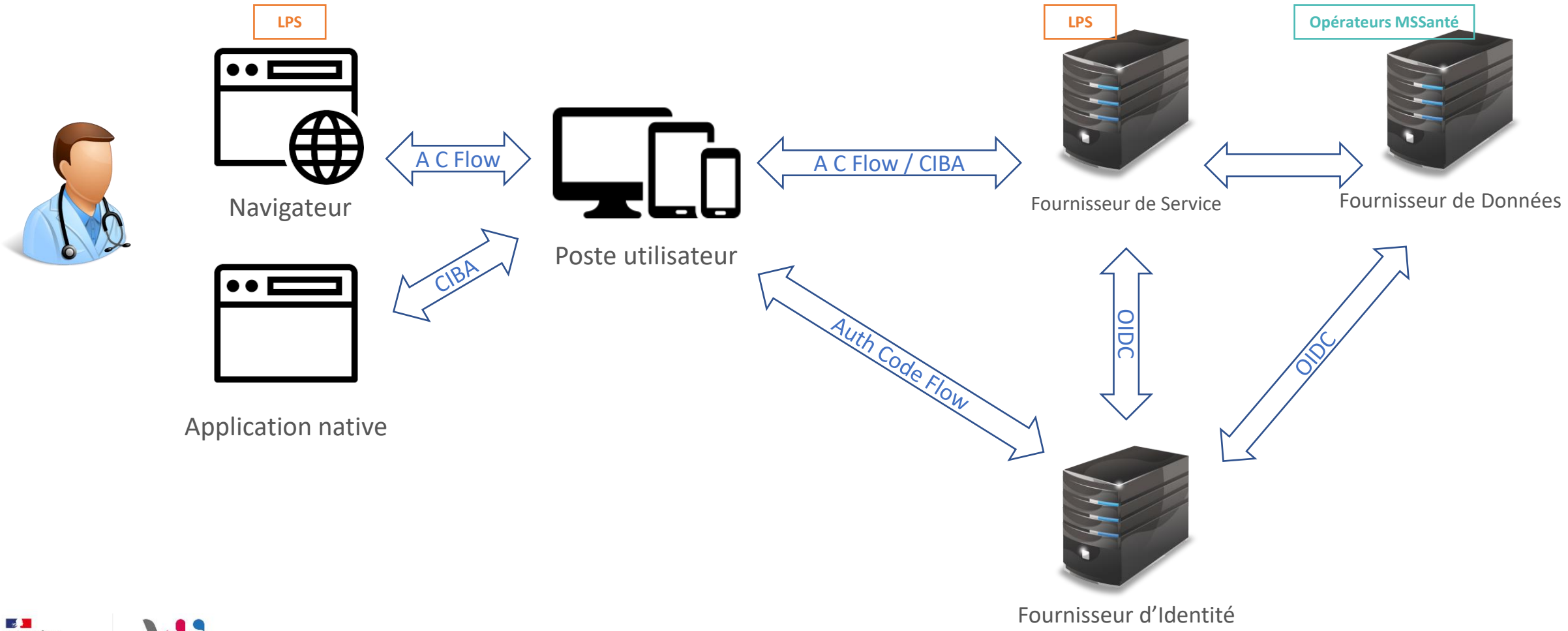
Référentiel Pro Santé Connect

L’arrêté rend opposable le référentiel dans sa version 1.8.4.

https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/referentiel-psc

Modalités d'utilisation de PSC sur une API

La version 1.8.4 du Référentiel PSC introduit la notion de Fournisseur de Données.
Les opérateurs MSSanté sont des Fournisseurs de Données.



Modalités d'utilisation de PSC sur une API

Choix : Authentification Code Flow ou CIBA :

- Le choix technique d'intégrer Pro Santé Connect en « Authentification Code Flow » ou en CIBA est laissé libre à l'industriel pour ses solutions en mode SaaS comme en Client lourd.
- L'ensemble des Exigences du Référentiel PSC sont applicables en « Authentification Code Flow » comme en CIBA.
- Pour rappel, actuellement seule la e-CPS est utilisable en CIBA. Une évolution prochaine permettra l'usage de la CPS.

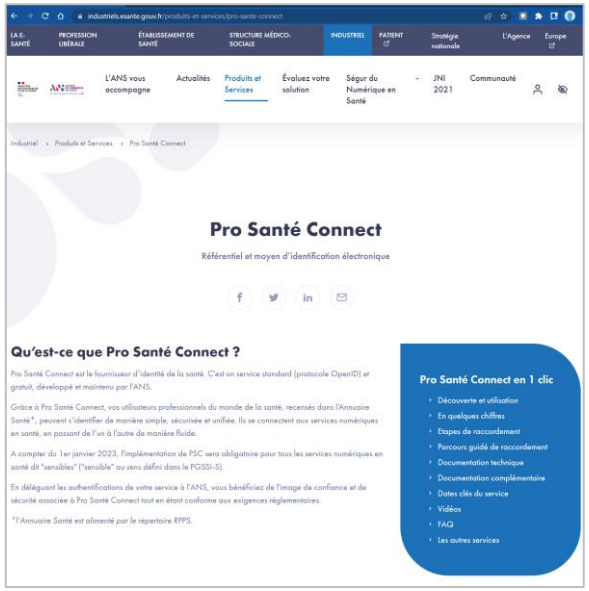
Impacts de l'usage d'une API « Pro Santé Connectée » sur les LPS/DUI :

Le Fournisseur de Service (LPS/DUI) et le Fournisseur de Données (Opérateurs) doivent conserver le client ID et le Secret au niveau d'un serveur (EXI PSC 22) et doivent proposer un unique point de contact à Pro Santé Connect (EXI PSC 23). Par conséquent, pour des considérations de sécurité :

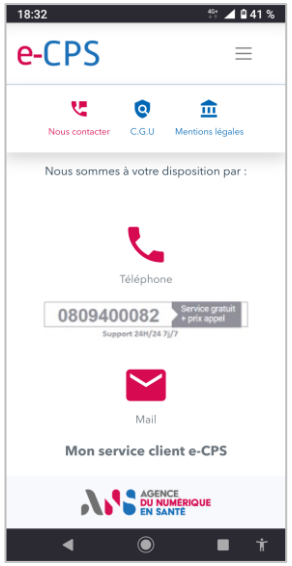
- Pro Santé Connect ne peut pas communiquer directement avec chacune des installations de LPS/DUI en client lourd.
- Un « serveur intermédiaire » doit être mis en place par l'éditeur du LPS/DUI entre ses installations en client lourd et Pro Santé Connect.

PSC : support / ressources disponibles

- 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
  - Ou par email prosanteconnect.editeurs@esante.gouv.fr



- Les Professionnels de Santé peuvent contacter le support :
  - par téléphone
  - par email
  - 24h24 - 7j/7



MSSanté
Système de messageries sécurisées, données protégées.

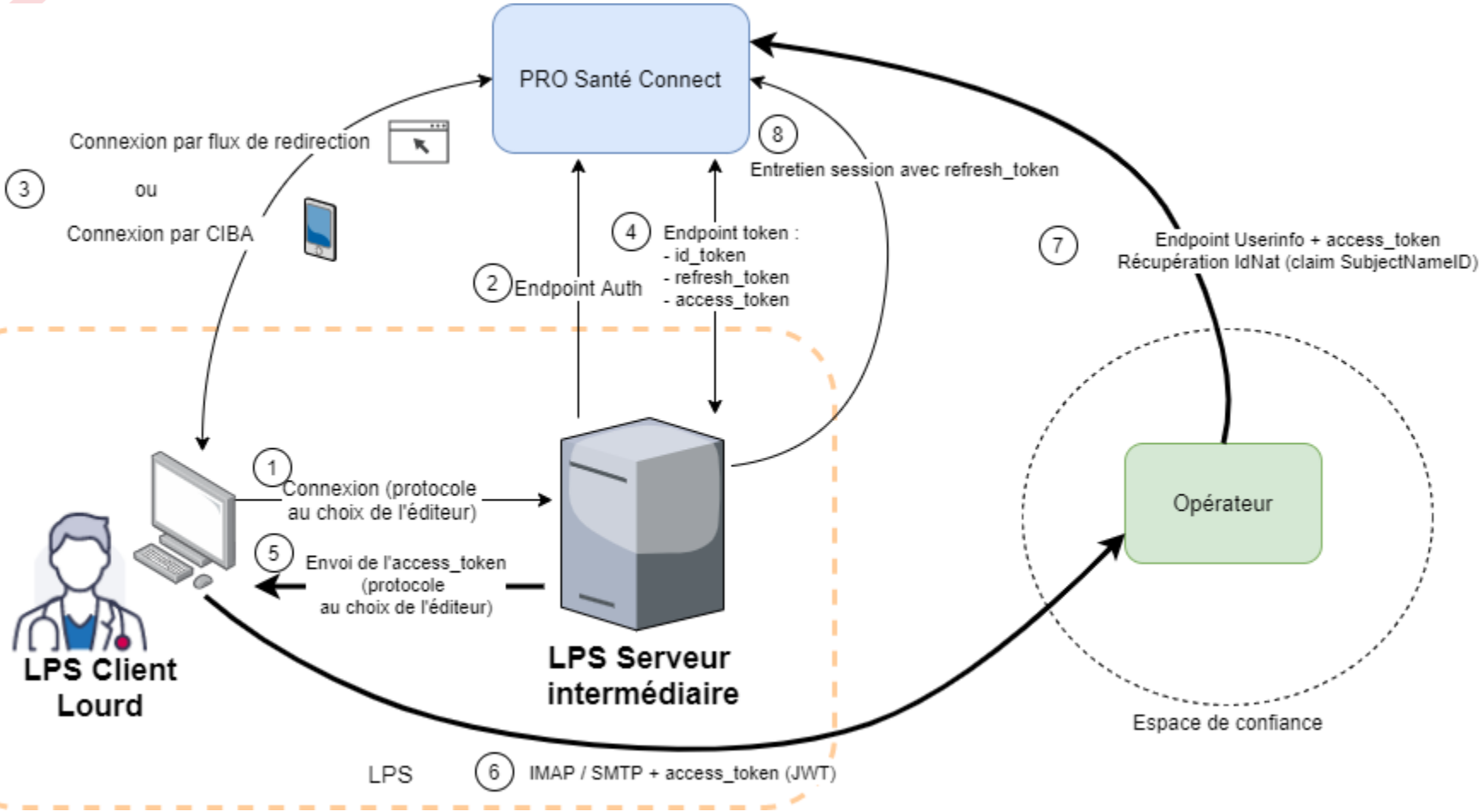
Questions / réponses

II Focus API LPS :

Cinématique d'échanges : LPS/DUI – PSC – Opérateurs

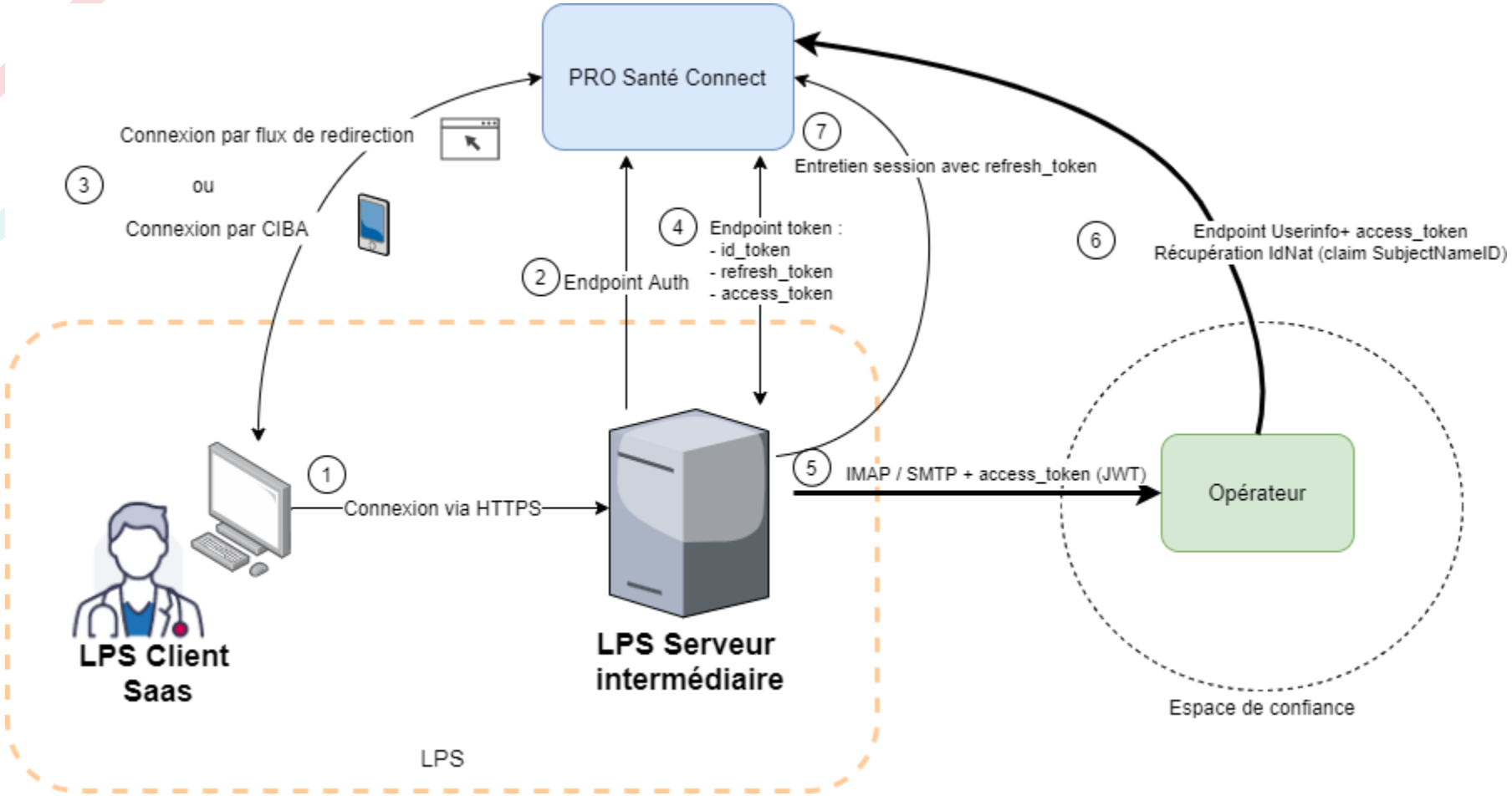
Cinématique d'échanges API LPS

BAL personnelles et organisationnelles - Architecture LPS client lourd



Cinématique d'échanges API LPS

BAL personnelles et organisationnelles - Architecture LPS SaaS



Cinématique d’échanges API LPS

BAL personnelles et organisationnelles - Dans le détail …

- La démarche de raccordement du Serveur Intermédiaire à PSC doit être menée par l’éditeur LPS/DUI
- Le mécanisme SASL d'authentification OAuth 2.0 avec l’implémentation XOAUTH2 pour transmettre via IMAP et SMTP, l'Access Token PSC à l’opérateur
- L’éditeur doit gérer les codes d’erreur d’authentification (IMAP : RFC 5530, SMTP : RFC 4954) transmis par l’opérateur

Cinématique d'échanges API LPS

BAL personnelles et organisationnelles - Dans le détail …

- Exemple IMAP : succès authentification

```
C: C01 CAPABILITY

S: * CAPABILITY IMAP4rev1 … SASL-IR AUTH=XOAUTH2 …

S: C01 OK Completed
```

```
C: A01 AUTHENTICATE XOAUTH2 dXNlcj1zb21ldXNlckBleGFtcGxlLmNvb

QFhdXRoPUJlYXJlciB5YTI5LnZGOWRmdDRxbVRjMk52YjNSbGNrQmhkSFJoZG

1semRHRXVZMjl0Q2cBAQ==

S: A01 OK Success
```

Access token

Cinématique d'échanges API LPS

BAL personnelles et organisationnelles - Dans le détail …

- Exemple IMAP : échec authentification

```
C: C01 CAPABILITY

S: * CAPABILITY IMAP4rev1 … SASL-IR AUTH=XOAUTH2 …

S: C01 OK Completed
```

```
C: A01 AUTHENTICATE XOAUTH2 dXNlcj1zb21ldXNlckBleGFtcGxlLmNvb

QFhdXRoPUJlYXJlciB5YTI5LnZGOWRmdDRxbVRjMk52YjNSbGNrQmhkSFJoZG

1semRHRXVZMjl0Q2cBAQ==

S: A01 NO Authentication failed
```

Cinématique d'échanges API LPS

BAL personnelles et organisationnelles - Dans le détail …

- Exemple SMTP : succès authentification

```
C: EHLO sender.example.com

S: 250-mx.exempl.com at your service, [145.87.123.47]

…

S: 250-AUTH LOGIN PLAIN XOAUTH2

…
```

```
C: AUTH XOAUTH2 dXNlcj1zb21ldXNlckBleGFtcGxlLmNvbQFhdXRoPUJlY

XJlciB5YTI5LnZGOWRmdDRxbVRjMk52YjNSbGNrQmhkSFJoZG1semRHRXVZMj

l0Q2cBAQ==

S: 235 2.7.0 Accepted
```

Cinématique d'échanges API LPS

BAL personnelles et organisationnelles - Dans le détail …

- Exemple SMTP : échec authentification

```
C: EHLO sender.example.com

S: 250-mx.exempl.com at your service, [145.87.123.47]

…

S: 250-AUTH LOGIN PLAIN XOAUTH2

…
```

```
C: AUTH XOAUTH2 dXNlcj1zb21ldXNlckBleGFtcGxlLmNvbQFhdXRoPUJlY

XJlciB5YTI5LnZGOWRmdDRxbVRjMk52YjNSbGNrQmhkSFJoZG1semRHRXVZMj

l0Q2cBAQ==

S: 535 5.7.8 Authentication credentials invalid
```

Cinématique d'échanges API LPS

BAL personnelles et organisationnelles - Dans le détail …

Structure de la chaine d'authentification XOAUTH2 :

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

Avec :

- ^A représente le caractère contrôle+A (\001)
- User : adresse mail demandée par le PS

Cinématique d'échanges API LPS

BAL personnelles et organisationnelles - Dans le détail …

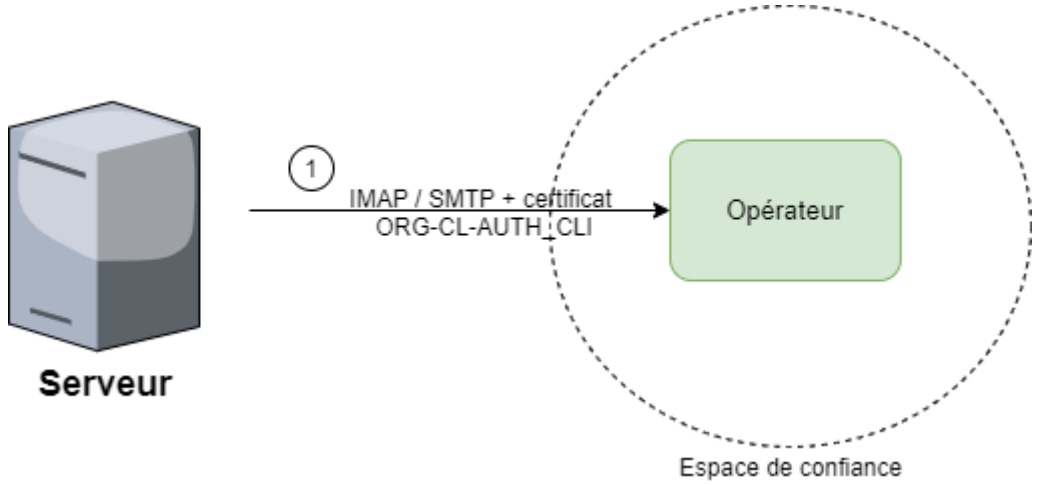
2 problématiques à aborder plus spécifiquement (prochain atelier) :

- 2 niveaux de déconnexion à gérer dans le LPS :
  1. Déconnexion de MSSanté
  2. Déconnexion de Pro Santé Connect

- Gestion de la durée de vie des sessions IMAP et SMTP :
  - Durée de vie liée à l'authentification auprès de Pro Santé Connect (gestion de Refresh Token)
  - Durée de vie liée à l'activité (ou l'inactivité) de LPS vis-à-vis du serveur de l'Opérateur (fréquence d'envoi des commandes IMAP ou SMTP)

Cinématique d'échanges API LPS

BAL applicatives - Architecture



- Certificat ORG-CL-AUTH_CLI doit être issu de l'IGC Santé

- Structure du DN

CN=Authentification MSS, OU=<IdNatStruc>, O=<NomStruc>, ST=<département> (XX), C=FR

MS Santé
Système de messageries sécurisées, données protégées.

Questions / réponses

Focus API LPS :

Modalités de test/recette à proposer aux éditeurs

Modalités de test/recette à proposer aux éditeurs

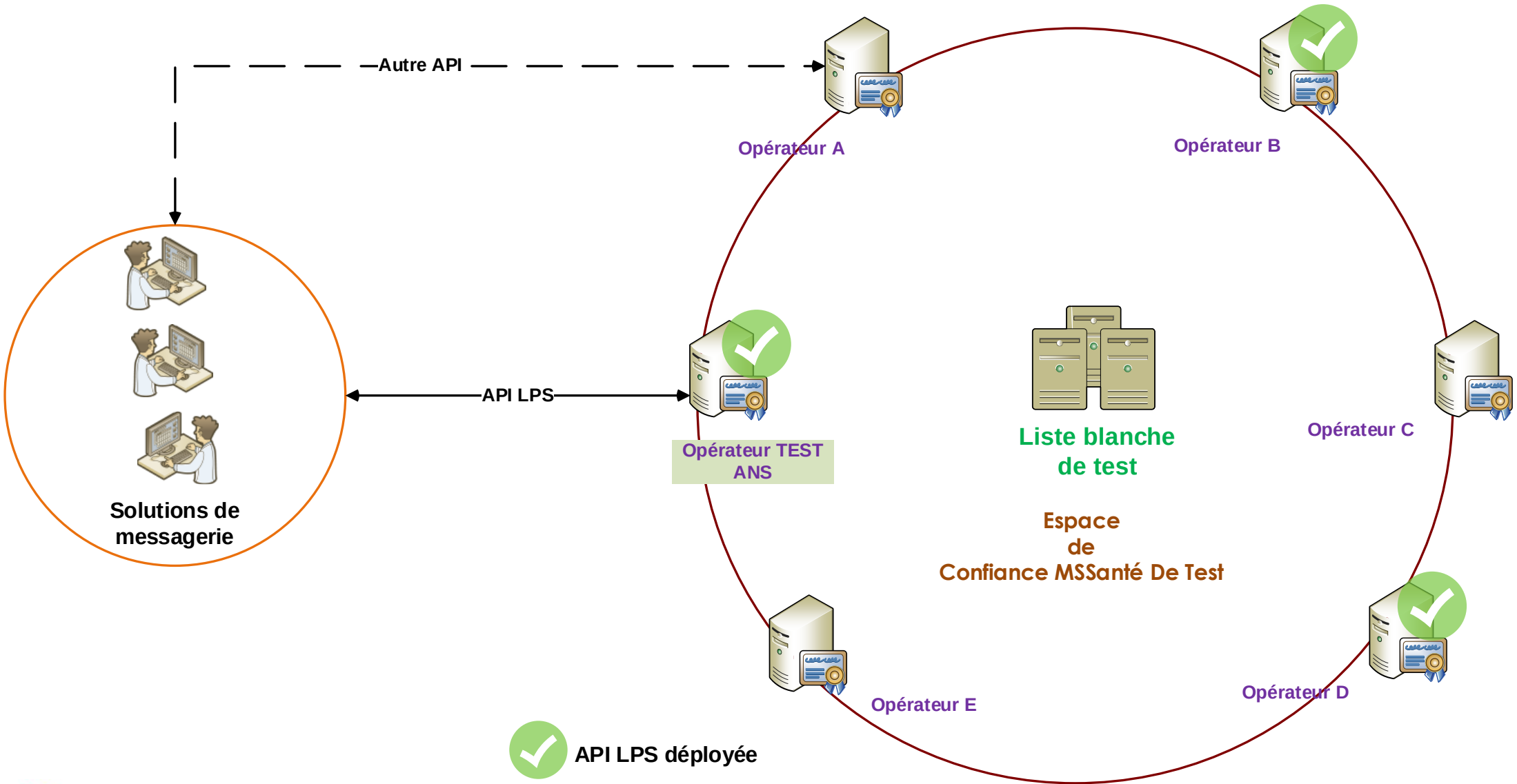
OBJECTIFS

- Mettre à disposition un environnement de test pour les développements de solutions de messagerie
- Permettre aux solutions de messagerie de vérifier leur conformité à certaines exigences du Ref #2
- Produire un CR de test attestant de la conformité de la solution aux exigences du Ref #2
- Permettre aux solutions de messagerie de vérifier la bonne structuration et le bon échange de documents de santé

MODALITES

- Simulation d'un Opérateur « de référence » en Espace de Confiance de test
- Opérateur accessible à travers l'API LPS et probablement un webmail
- 2 MIE possibles pour la connexion
  - Pro Santé Connect (BAL personnelle, organisationnelle)
  - Certificat IGC Santé AUTH_CLI (BAL applicative)

Modalités de test/recette à proposer aux éditeurs



Conclusion et prochaines étapes

Conclusion

Prochaines étapes :

- **Vendredi 3 juin 15h** : Atelier #2
  - Suite API LPS
  - Indicateurs d'usage
  - Echanges avec MES

- **S23 :** initialisation du tableau d'exigences Ref#2 pour remarques éditeurs

- **Vendredi 17 juin 15h** : Atelier #3
  - Ordre du jour à définir

Merci pour votre participation !