MSSanté
Système de messageries sécurisées, données protégées.

Task Force MSSanté

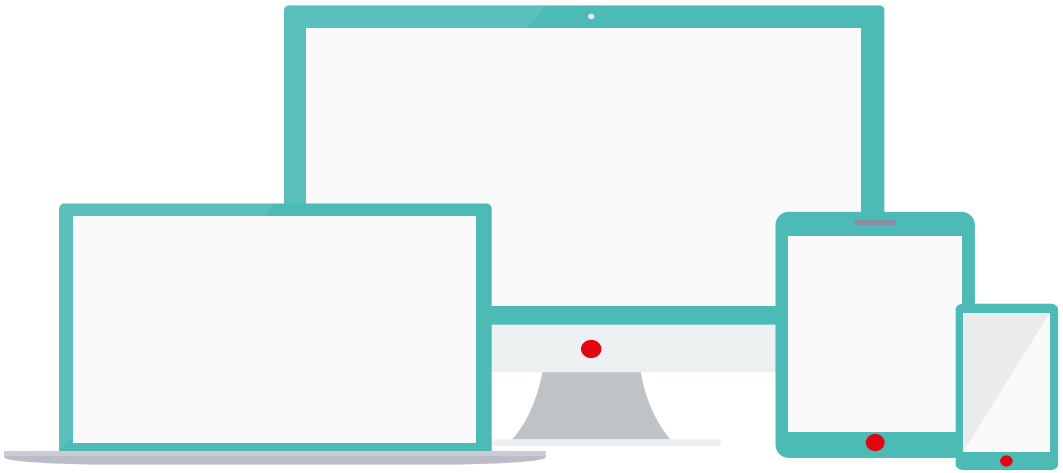
Atelier industriel #3 du 11/02/2022

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.

MSSanté
Système de messageries sécurisées, données protégées.

SOMMAIRE

Introduction

Exigences – MAJ récentes

v0.2 : Merci pour vos retours - 3 opérateurs et 2 éditeurs ont contribués

v**0.3** : publiée le 04/02

- Prendre connaissance des réponses ANS (colonne AP) sur v0.2
- Peu d'exigences modifiées (à part autorisation TLS 1.3 en complément de 1.2), mais de nombreux ajouts

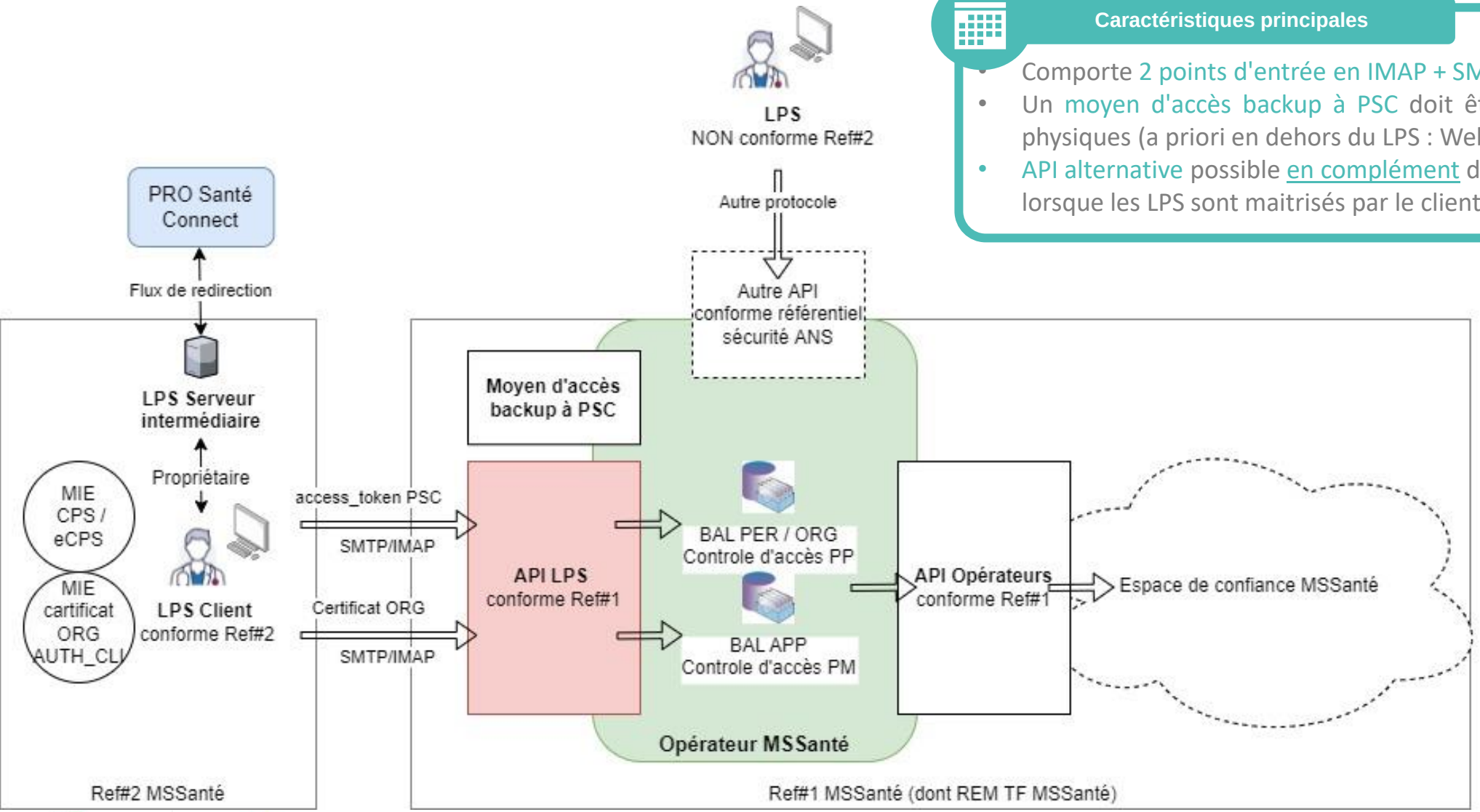
Nouvelles exigences API LPS

- MSS 7.x : Précisions sur les modalités d'authentification PSC dont procédure détaillée des étapes à réaliser par l'opérateur
- MSS 10.x : Précisions sur les modalités d'authentification BAL APP dont procédure détaillée des étapes à réaliser par l'opérateur
- MSS 10.9 : Recommandation permettant d'utiliser une autre interface LPS, en complément de l'API LPS standardisée, si elle est conforme aux référentiels d'identification / authentification ANS

Nouvelles exigences - autres

- MSS 19 : Dépublication dans l'annuaire national des BAL sans connexion depuis X jours (à concerter)
- MSS 20-25 : Nouveau contrat opérateur : nouvelles modalités de contrôle et nouvelles mesures de sanction graduées (à concerter)
- MSS 10.2-4 : Trajectoire permettant de ne supporter que TLS 1.2 et supérieur entre opérateurs. Actuellement TLS 1.0 toujours obligatoire comme socle commun.

API LPS – Synthèse des concertations à date



Caractéristiques principales

- Comporte 2 points d'entrée en IMAP + SMTP pour 2 types de MIE
- Un moyen d'accès backup à PSC doit être proposé pour les personnes physiques (a priori en dehors du LPS : Webmail OTP, CPS, ...)
- API alternative possible en complément de l'API LPS (conforme ref. sécu) lorsque les LPS sont maitrisés par le client de l'opérateur (Exchange ...)

Transition Segur

Le Ref#1 v1.5 prévoit la transition entre les interfaces existantes et les interfaces conformes Ségur

Les éditeurs disposeront de cette même tolérance cad prévoir :

- prévoir 1 interface conforme Ségur
- maintenir 1 interface conforme aux solutions actuelles le temps de la transition

MSSanté
Système de messageries sécurisées, données protégées.

Questions / réponses

Nouvelles exigences hors API LPS

Entêtes spécifiques MSSanté côté client de messagerie

OBJECTIF : suivre le déploiement de l'INS et l'échange de données structurées

1

Indiquer la présence d'un INS qualifié

Positionnement de l'entête « **X-MSS-INS** »
O – présence d'un INS qualifié
N – absence d'INS qualifié

2

Renseigner le type de document CDA transmis

Positionnement de l'entête « **X-MSS-CODECDA** »
reprendre la valeur de l'attribut 'code' de chaque document CDA transmis

3

Transmettre le NIL du client de messagerie

Positionnement de l'entête « **X-MSS-NIL** »
Valeur possible :
<idEditeur/idLogiciel/idVersion>

Les Webmail ne sont pas soumis à cette exigence

X-MSS-INS

'O' présence d'un INS qualifié au sens du §5.3.3 du Référentiel Identifiant National de Santé v2.0
'N' absence d'INS qualifié

X-MSS-NIL (Num Identification Logiciel)

en cours, le besoin étant d'obtenir des infos sur l'éditeur/le logiciel/le num de version logiciel et de s'appuyer sur un id déjà existant

X-MSS-CODECDA

* un document structuré fait référence à l'*exigence ECO.2.1.1 du Ref #2*

si pas de document structuré : ne pas positionner l'entête

si un seul document CDA joint : le type de document CDA correspondant à l'attribut ***'code'*** de l'en-tête CDA
Exemple :
X*-MSS-*CODECDA = 34112-3

Si plusieurs documents CDA joints : tous types de document CDA correspondant à l'attribut ***'code'*** de l'en-tête de chaque CDA
Exemple :
X*-MSS-*CODECDA = 34112-3, PRESC-BIO, 15508-5
/!\ séparer les valeurs avec la 'virgule'

?

Quel id pour les clients de messagerie ? (Editeur/Logiciel/Version)

*** Quels sont les identifiants obtenus par le GIE-SV**
*** Quels est l'identifiant obtenus par le CNDA**

Evolution des indicateurs d'usage MSS côté opérateur

Indications ANS

Introduction de 3 colonnes dans le fichier des indicateurs

Colonne « **INS** »
Colonne « **CODECDA** »
Colonne « **NIL** »

L'opérateur devra lire les entêtes SMTP de chaque message émis afin de récolter les valeurs des nouvelles entêtes positionnées par le client de messagerie.
Les valeurs alimenteront les nouvelles colonnes

Entête X-MSS-INS → INS
Entête X-MSS-CODECDA → CODECDA
Entête X-MSS-NIL → NIL

					évolution		
MAIL_ID	EXPEDITEUR	DESTINATAIRE	DATE	TAILLE	INS	CODECDA	NIL
1256321	ans@mssante.fr	ans-2@mssante.fr	2020-08-11 14:55:40	21	*O*	*34112-3*	*<idEditeur/idLogiciel/idVersion>*
2257301	ans@mssante.fr	ans-4@mssante.fr	2020-07-12 07:36:12	92	*N*	*34112-3, PRESC-BIO, 15508-5*	*<idEditeur/idLogiciel/idVersion>*

Qualité des BAL présentes dans l'annuaire

MSS 14 : Le système DOIT comporter un dispositif permettant de supprimer les boîtes aux lettres en cas d'absence d'authentification de l'utilisateur pendant une période d'un an, conformément aux recommandations de la CNIL.

MSS 19 : L'opérateur doit dépublier de l'Annuaire Santé toute BAL 'personnelle' ou 'organisationnelle' qui n'a pas fait l'objet d'une connexion par un utilisateur final depuis plus de X jours.

MSS 17 : Le système DOIT avant de créer une BAL personnelle informer le futur titulaire de la présence éventuelle d'autres BAL à son nom

Questions

- **MSS 14** : quel délai avant le début de la procédure de suppression d'une BAL ?
- **MSS 19** : quel délai avant la dépublication d'une BAL non consultée de l'Annuaire Santé ?
- **MSS 17** : sur quel canal informer le PS de la présence d'autres BAL à son nom

Proposition

- **MSS 14** : peut-on considérer qu'une BAL non consultée au-delà de 3 mois est une BAL qui ne le sera plus ?
- **MSS 19** : peut-on considérer qu'une BAL qui ne fait pas l'objet de consultation sur 30 jours doit être retirée de l'Annuaire Santé (pas de suppression de la BAL)
- **MSS 17** : le listing des BAL ouvertes devrait parvenir au PS par sa BAL non sécurisée

Contrat : nouvelles modalités de contrôles / sanctions

MSS 14 : Tout opérateur présent en Espace de Confiance de production DOIT produire un niveau de conformité 1, à travers un CR d'audit, avant la fin du délai de mise à niveau déclenchée par la publication d'une version majeure du Référentiel #1

Conformité Niv 1

Aucune non-conformité bloquante ou critique constatée

Conformité Niv 2

Présence de non-conformités bloquantes constatées

Conformité Niv 3

Présence de non-conformités critiques constatées

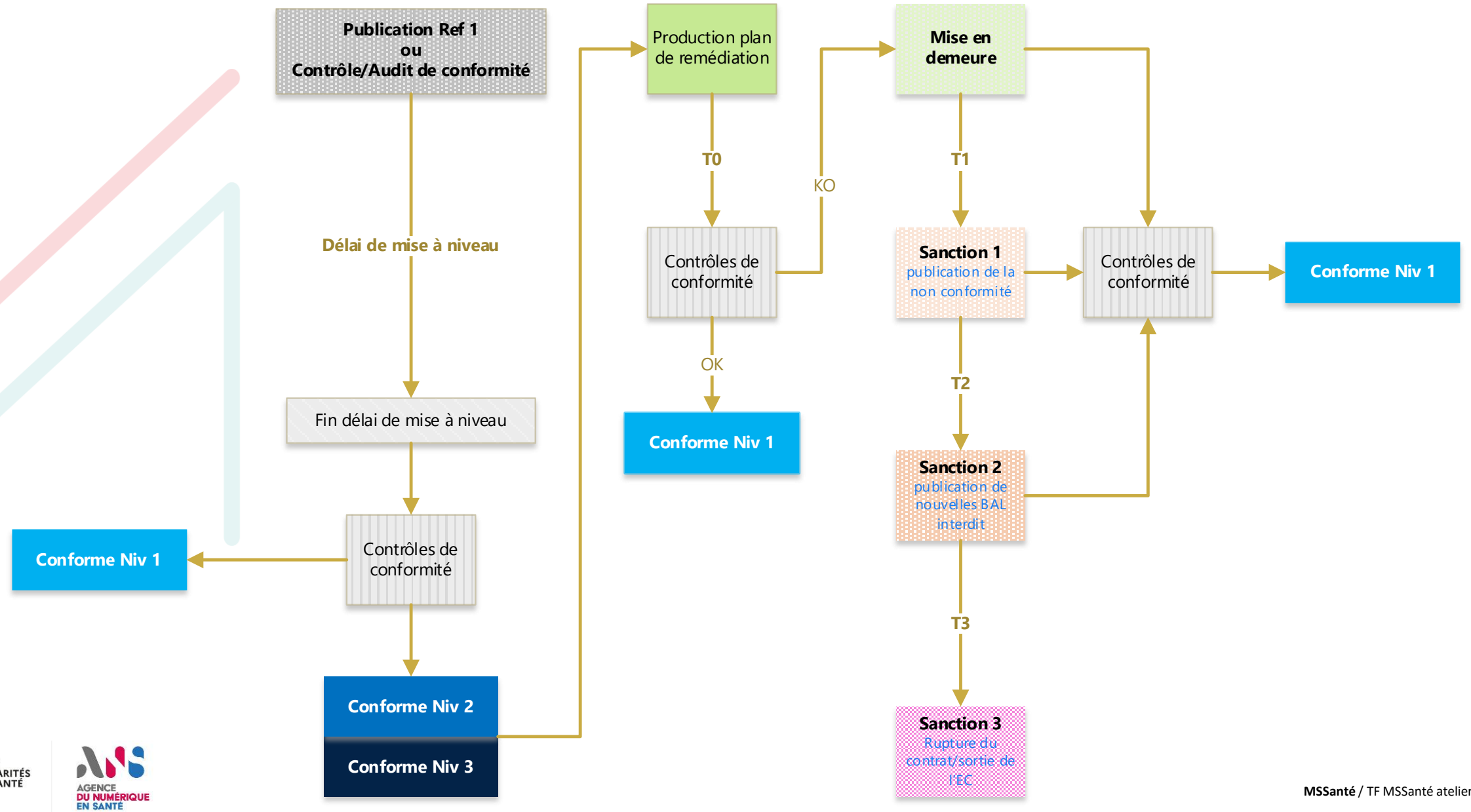
Questions

- **T0 :** quel délai après la production du plan de remédiation pour la mise à niveau du système de l'opérateur
- **T1** : quel délai convenable après la mise en demeure pour application de la Sanction 1 ?
- **T2** : quel délai convenable après la mise en demeure pour application de la Sanction 1 ?
- **T3** : quel délai convenable après la mise en demeure pour application de la Sanction 1 ?

Proposition

- **T0 :**
- **T1** :
- **T2** :
- **T3** :

Contrat : nouvelles modalités de contrôles / sanctions



MSSanté
Système de messageries sécurisées, données protégées.

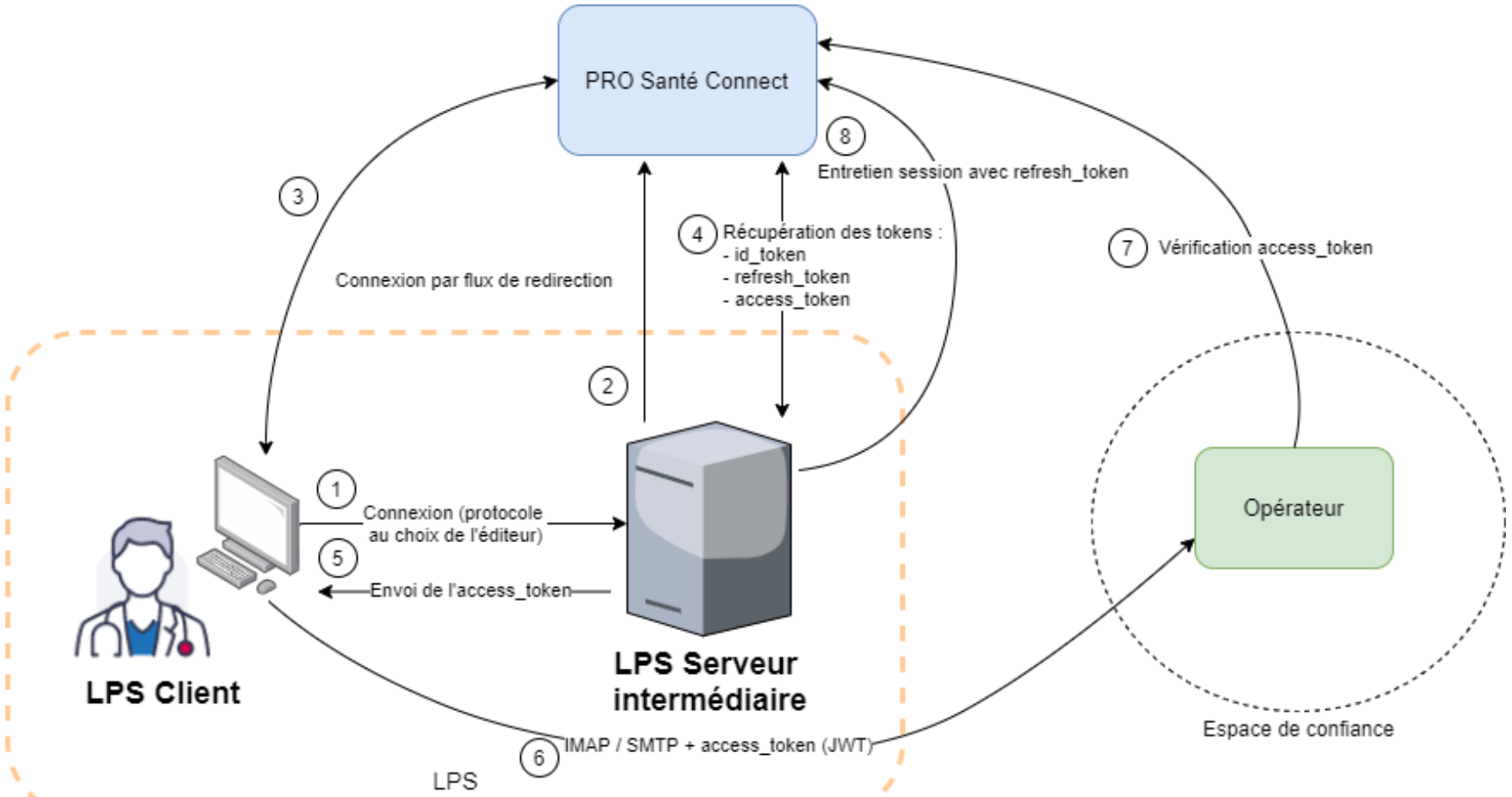
Questions / réponses

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ

Focus MIE de l'API LPS

MIE – Authentification PSC : Cinématique LPS client lourd



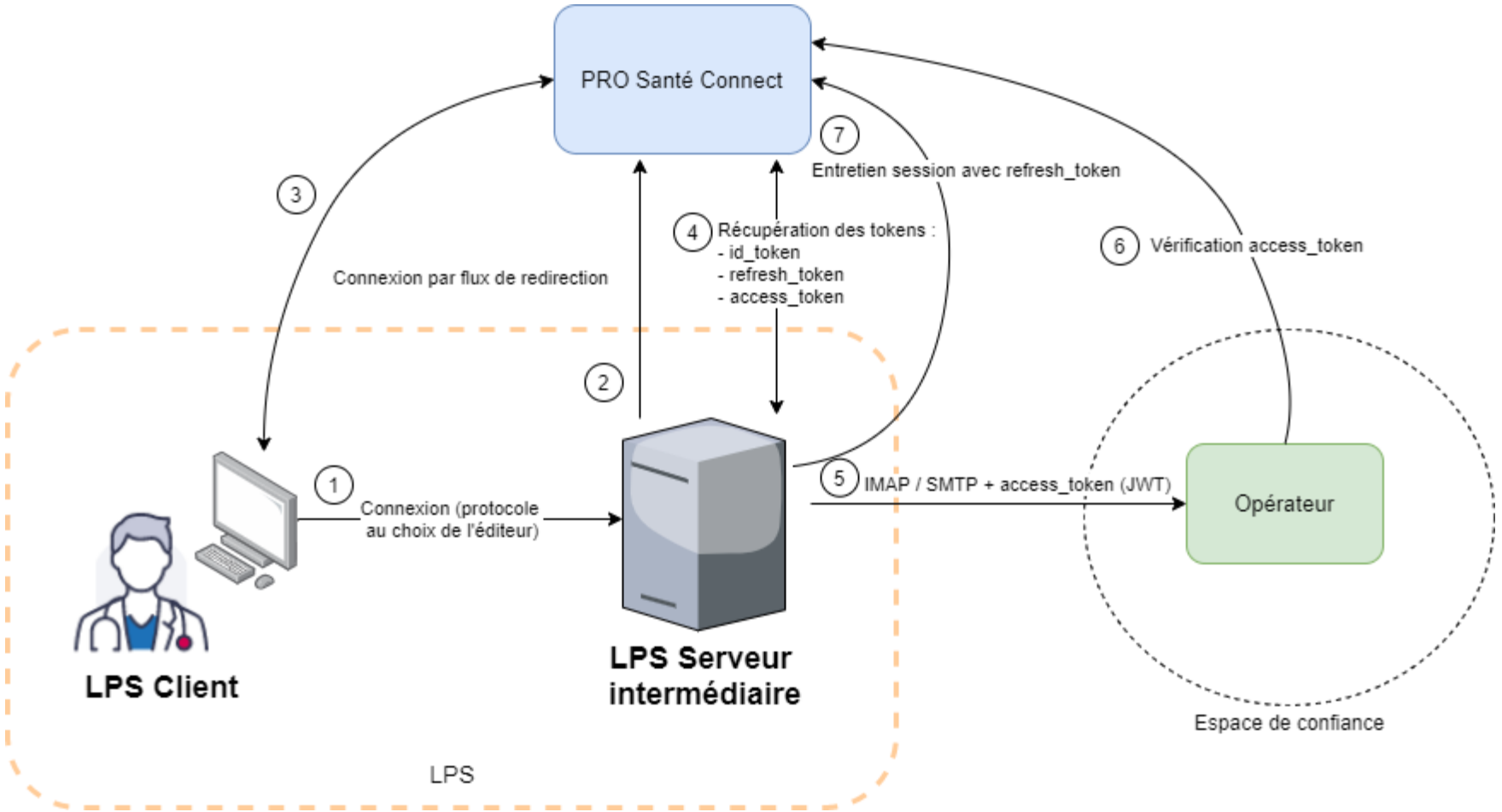
Questions

- Disposez-vous déjà d'une brique équivalente au « LPS Serveur intermédiaire » ?
- De quelle manière est réalisée l'authentification du PS à l'heure actuelle sur le LPS Client ?

Description des étapes

1. Connexion du LPS Client au LPS Serveur intermédiaire
2. Le serveur intermédiaire du LPS contacte PSC pour lancer l'authentification
3. Le serveur intermédiaire redirige le PS sur le site de PSC via son navigateur. Ce dernier réalise alors son authentification avec CPS ou e-CPS
4. L'authentification réussie, le serveur intermédiaire récupère 3 tokens de PSC : ID Token, Refresh Token et Access Token
5. Le serveur intermédiaire envoie l'Access Token au LPS Client
6. Lorsque le PS souhaite accéder à sa BAL MSSanté, le LPS Client monte une session IMAP ou SMTP en envoyant l'Access Token à l'opérateur
7. L'opérateur réalise les vérifications métier appropriées puis contacte PSC pour valider l'Access Token
8. Le maintien de la connexion auprès de PSC est assuré par le serveur intermédiaire grâce à l'envoi du Refresh Token

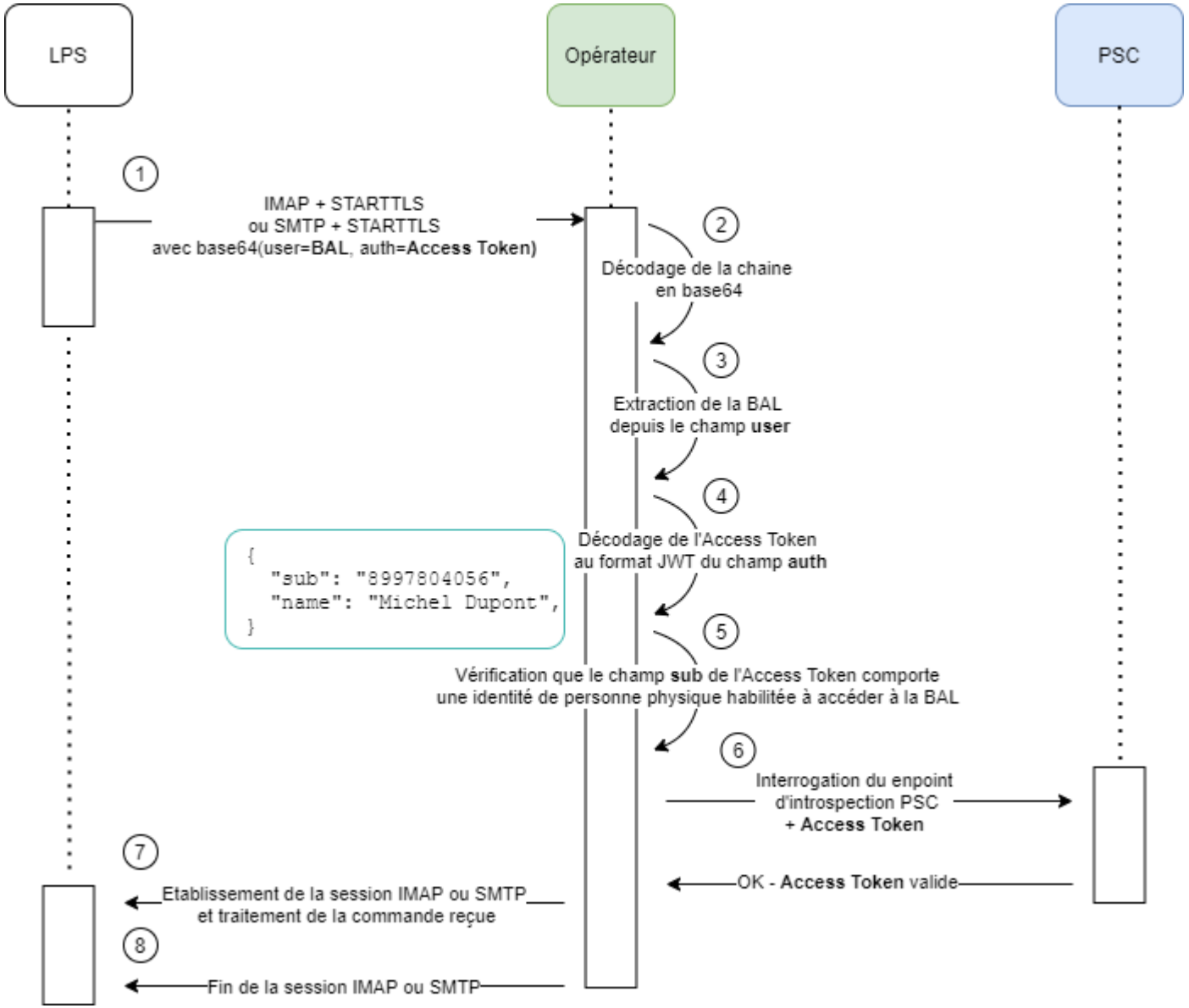
MIE – Authentification PSC : Cinématique LPS Saas



Description des étapes

1. Connexion du LPS Client au LPS Serveur intermédiaire
2. Le serveur intermédiaire du LPS contacte PSC pour lancer l'authentification
3. Le serveur intermédiaire redirige le PS sur le site de PSC via son navigateur. Ce dernier réalise alors son authentification avec CPS ou e-CPS
4. L'authentification réussie, le serveur intermédiaire récupère 3 tokens de PSC : ID Token, Refresh Token et Access Token
5. Lorsque le PS souhaite accéder à sa BAL MSSanté, le serveur intermédiaire monte une session IMAP ou SMTP en envoyant l'Access Token à l'opérateur
6. L'opérateur réalise les vérifications métier appropriées puis contacte PSC pour valider l'Access Token
7. Le maintien de la connexion auprès de PSC est assuré par le serveur intermédiaire grâce à l'envoi du Refresh Token

MIE – Authentification PSC : Cinématique opérateur



Réflexion en cours

Quelle durée de session imposer ?

- Courte : durée de vie équivalente à l'envoi de la commande IMAP / SMTP depuis le LPS
- Longue : persiste dans le temps et permet d'envoyer plusieurs commandes IMAP / SMTP à travers celle-ci

MIE – Certificat IGC Santé pour accès BAL applicative

Suite à instruction sécurité, le certificat n'a pas besoin d'être spécifique à la BAL :

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

Coté opérateur

1. Création d'une BAL applicative associée à l'identifiant de structure connu de l'annuaire santé (IdNatStruc)

2. Connexion sur la BAL applicative :
   - Contrôle de la validé du certificat
   - Extraction de l'IdNatStruc du certificat
   - Extraction de l'adresse de la BAL (login authen PLAIN)
   - Vérification de la cohérence BAL avec IdNatStruc

Coté structure ou éditeur logiciel

1. Génération d'un certificat ORG AUTH-CLI par la structure ou par l'éditeur par délégation de la structure

2. Déploiement du certificat sur l'application en charge d'utiliser la BAL applicative

3. Demande de connexion IMAP ou SMTP par l'application en fournissant :
   - L'adresse de la BAL applicative
   - Le certificat ORG AUTH_CLI

MSSanté
Système de messageries sécurisées, données protégées.

Questions / réponses

Rappels : spécifications ENS disponibles pour les éditeurs

Rappels – Spécifications ENS disponibles pour les éditeurs

Documents de référence

ANS : Ref#2 MSSanté v0.1 (juin 2021) :

https://mssante.fr/is/doc-technique

- Format adresse de messagerie patient ENS
- Usage d'un INS qualifie + dérogation temporaire

CNAM : Eléments d'information à destination des éditeurs de solution MSSanté pour les professionnels (décembre 2021)

https://mssante.fr/is/doc-technique

- Décrit les principaux comportements de la messagerie de MES. Voir focus à droite.

ANS : Ref#2 MSSanté v1.0 (juin 2022)

- Nouvelles exigences pour la vague 2 Ségur : proposer aux professionnels certaines fonctionnalités : mettre fin aux échanges avec un patient, demande d'accusé de lecture, distinction des messages émis par patient et professionnels...

Focus spécification CNAM messagerie MES

- Demande d'arrêt des échanges avec un patient
- Cas d'un MES fermé par l'usager
- Cas d'un MES non trouvé : non ouvert, opposé ou INS inexistant
- Taille des messages acceptés : < 25 Mo
- Demande d'accusé de lecture au patient
- Format des messages envoyés par MES : uniquement HTML
- Transmission de l'identité du patient (prenom nom)
- Modalité de l'affichage du professionnel dans MES
- Traitement des messages envoyés par les professionnels

Comme tout opérateur MES publie une BAL de réponse automatique en production :

reponse.automatique-test@patient.mssante.fr

Ouverture par l'opérateur CNAM d'un espace de test MES pour éditeurs : date non définie

MSSanté
Système de messageries sécurisées, données protégées.

Questions / réponses

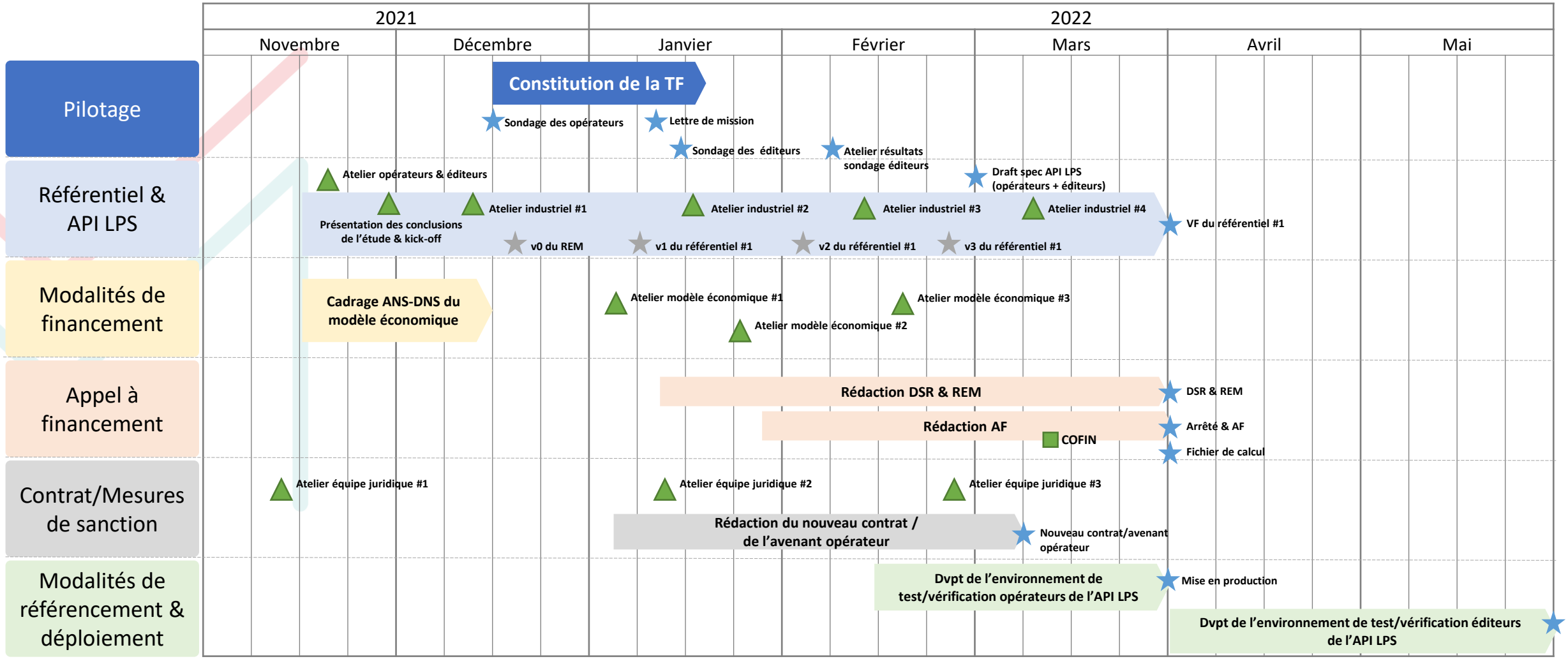
Conclusion

Prochaines étapes :

- 18/02 : Fin des retours opérateurs / éditeurs LPS sur v0.3 des exigences
- 18/02 : Opérateurs : atelier modèle économique #3
- Semaine du 11/03 : Envoi de la v0.4 des exigences + draft Ref #1 v1.5 incluant l'API LPS
- 11/03 : Atelier industriel #4
- TBD : Concertation publique

Merci pour votre attention !

Rappel du calendrier de la Task Force



Légende : Livrable ; Livrable intermédiaire ; Atelier ; Réunion institutionnelle