MSSanté
Système de messageries sécurisées, données protégées.

Task Force MSSanté

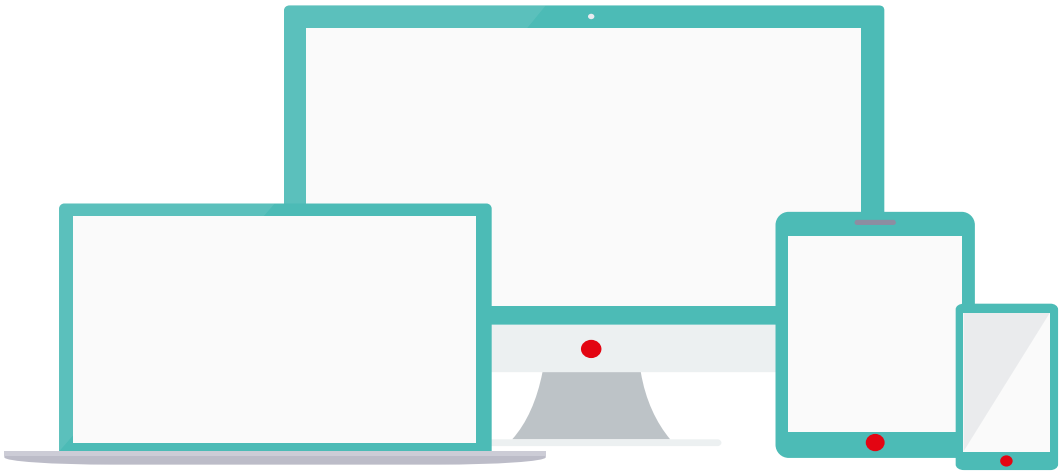
Atelier industriel #2 du 21/01/2022

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



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.

Introduction

MSSanté
Système de messageries sécurisées, données protégées.

2h00

SOMMAIRE

I. Retour sur concertation REM v0.1

II. Focus MIE
- Authentification PSC via LPS
- Présentation de l'authentification OTP par l'opérateur
- Maintien d'une authentification CPS locale à l'opérateurs ?
- Authentification par certificat IGC Santé pour les BAL applicatives

III. Entête spécifiques MSSanté côté client de messagerie

IV. Evolution des indicateurs d'usage MSS côté opérateur

V. Rationalisation des BAL publiées dans l'annuaire

Exigences v0.1 – Concertation opérateurs / éditeurs

Merci pour vos retours sur la v0.1 : 6 opérateurs et 8 éditeurs ont contribués

V0.2 publiée le 14/01 : réponses et précisions apportées colonne Q

NB : les exigences sont formulées pour des opérateurs (et non des logiciels métiers client)

Exigences modifiées

- MSS 7 : Le système DOIT permettre à une personne physique identifiée dans l'annuaire santé de se connecter à une BAL personnelle ou organisationnelle en IMAP/SMTP ~~en mettant en oeuvre un flux d'authentification CIBA~~ en se basant sur l'Access Token PSC transmis par le LPS.
- MSS 8 : ~~Le système DOIT permettre à une personne physique identifiée dans l'annuaire santé de se connecter à une BAL personnelle ou organisationnelle en IMAP/SMTP en mettant en oeuvre un flux de redirection PSC (norme OpenID Connect)~~

car l'authentification PSC doit être initiée par le logiciel métier et non par l'opérateur

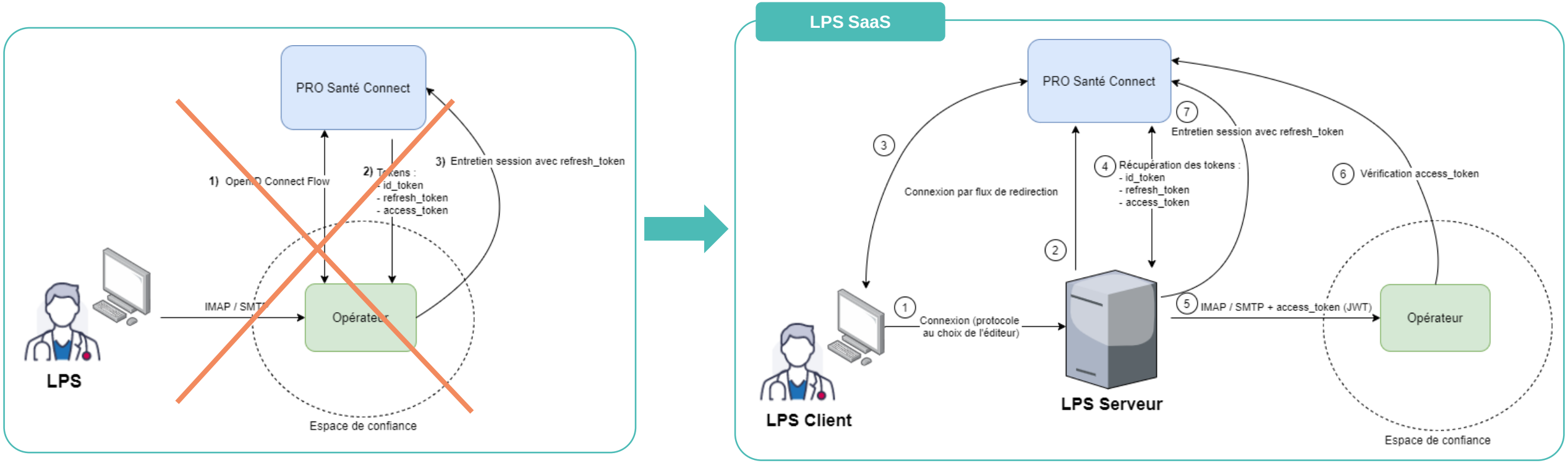
- MSS 9 : Le système DOIT permettre à une personne physique habilitée à échanger des données de santé ~~identifiée dans l'annuaire santé~~ de se connecter à une BAL personnelle ou organisationnelle en IMAP/SMTP en se basant sur un échange OTP ~~(probablement via~~ SMS)

car un mécanisme d'authentification OTP SMS a été identifié
car le MIE OTP ne s'adosse pas nécessairement sur l'annuaire santé

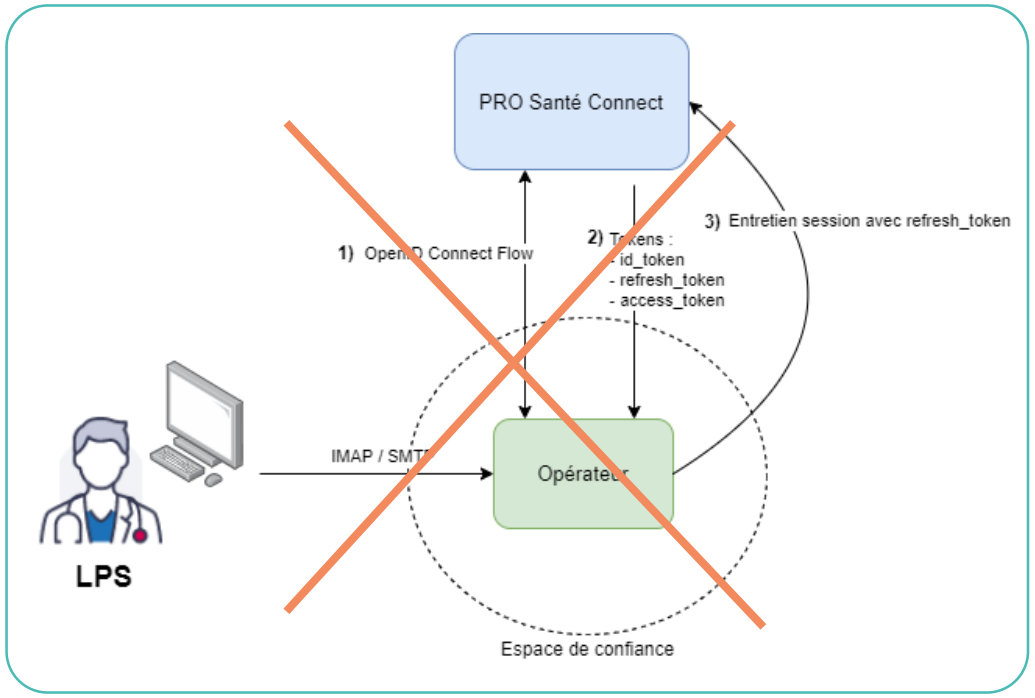
MIE – Authentification PSC via LPS (1/5)

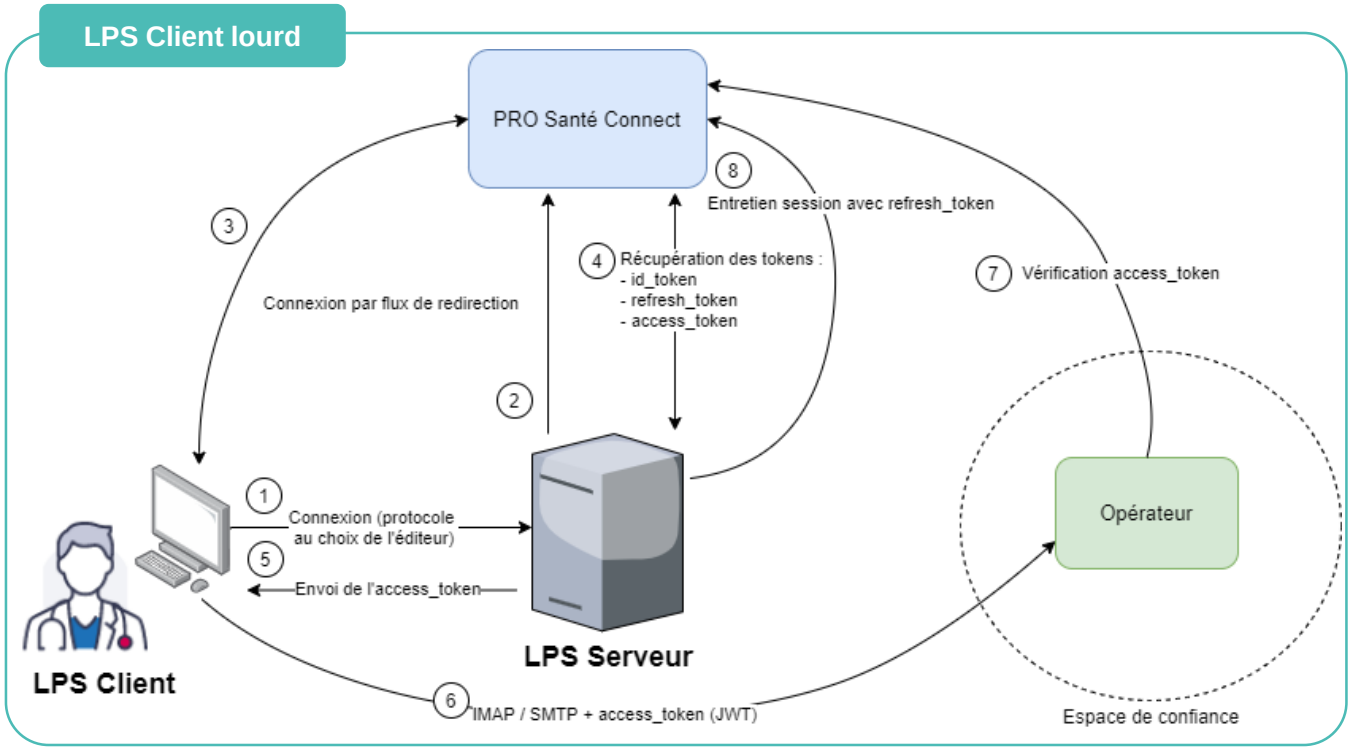
Nouveau paradigme

- L'authentification auprès de PSC est réalisée en amont par le LPS via le flux de redirection navigateur
- Le LPS souhaitant accéder au service de messagerie d'un opérateur de l'espace de confiance devra transmettre le jeton d'accès délivré par PSC



MIE – Authentification PSC via LPS (2/5)





MIE – Authentification PSC via LPS (3/5)

Quels impacts pour les éditeurs et les opérateurs ?

Editeur

Déjà demandé via les DSR vague 1 :

- Disposer d'un serveur intermédiaire responsable de la connexion avec PSC (déjà le cas pour les LPS SaaS)
- Entretenir la connexion auprès de PSC pour fournir un Access Token valide

Nouveautés introduites par MSSanté (vague 2 Ségur) :

- Transmettre l'Access Token à l'opérateur auquel on souhaite se connecter en suivant la RFC 7628 (voir slide suivante)
- Sur déconnexion PSC, fermer les éventuelles sessions IMAP / SMTP en cours
- Pour les LPS « Client lourd », envoyer l'Access_Token depuis le serveur intermédiaire au client

Opérateur

- Implémenter la RFC 7628 pour consommer l'Access Token:
  - Réponse à retourner en cas de succès
  - Réponse à retourner en cas d'erreur
- Valider l'Access Token auprès de PSC sur l'établissement d'une session IMAP ou SMTP.
- S'assurer que la durée de session ne dépasse pas une certaine limite (qui reste à définir).

MIE – Authentification PSC via LPS (4/5)

Détails techniques

- Objectif : Transmettre un Access Token de type JWT (rfc7519) comme Bearer token (rfc6750) dans une session IMAP et SMTP
- 2 solutions très proches reposant sur SASL :
  - OAUTHBEARER (rfc7628) : Standard établi mais peu répandu à l'heure actuelle
  - XOAUTH2 : Solution non standard mais largement utilisée par Google et Microsoft pour permettre l'accès à leurs boites aux lettres

IMAP

```
[Initial connection and TLS establishment...]
S: * OK IMAP4rev1 Server Ready
C: t0 CAPABILITY
S: * CAPABILITY IMAP4rev1 AUTH=OAUTHBEARER SASL-IR
S: t0 OK Completed
C: t1 AUTHENTICATE OAUTHBEARER bixhPXVzZXJAZXhhbXBsZS5jb20sAWhv
     c3Q9c2VydmVyLmV4YW1wbGUuY29tAXBvcnQ9MTQzAWF1dGg9QmVhcmVyI
     HZGOWRmdDRxbVRjMk52YjNSbGNrQmhiSFJoZG1semRHRXVZMjl0Q2c9PQ
     EB
S: t1 OK SASL authentication succeeded
```

SMTP

```
[connection begins]
S: 220 mx.example.com ESMTP 12sm2095603fks.9
C: EHLO sender.example.com
S: 250-mx.example.com at your service,[172.31.135.47]
S: 250-SIZE 35651584
S: 250-8BITMIME
S: 250-AUTH LOGIN PLAIN OAUTHBEARER
S: 250-ENHANCEDSTATUSCODES
S: 250-STARTTLS
S: 250 PIPELINING
[Negotiate TLS...]
C: t1 AUTH OAUTHBEARER bixhPXVzZXJAZXhhbXBsZS5jb20sAWhvc3Q9c2Vy
     dmVyLmV4YW1wbGUuY29tAXBvcnQ9NTg3AWF1dGg9QmVhcmVyIHZGOWRmd
     DRxbVRjMk52YjNSbGNrQmhiSFJoZG1semRHRXVZMjl0Q2c9PQEB
S: 235 Authentication successful.
```

- Valeur du champ OAUTHBEARER : base64("user=" {User} "^Aauth=Bearer " {Access Token} "^A^A")

MIE – Authentification PSC via LPS (5/5)

Conclusion

- Pas d'arbitrage sur la solution retenue à date
- Les 2 solutions sont techniquement très proches

Calendrier

- Retour prévu sur la solution retenue :
  - Le 04/02 dans la nouvelle version du REM
  - Le 11/02 au prochain atelier Task Force MSSanté

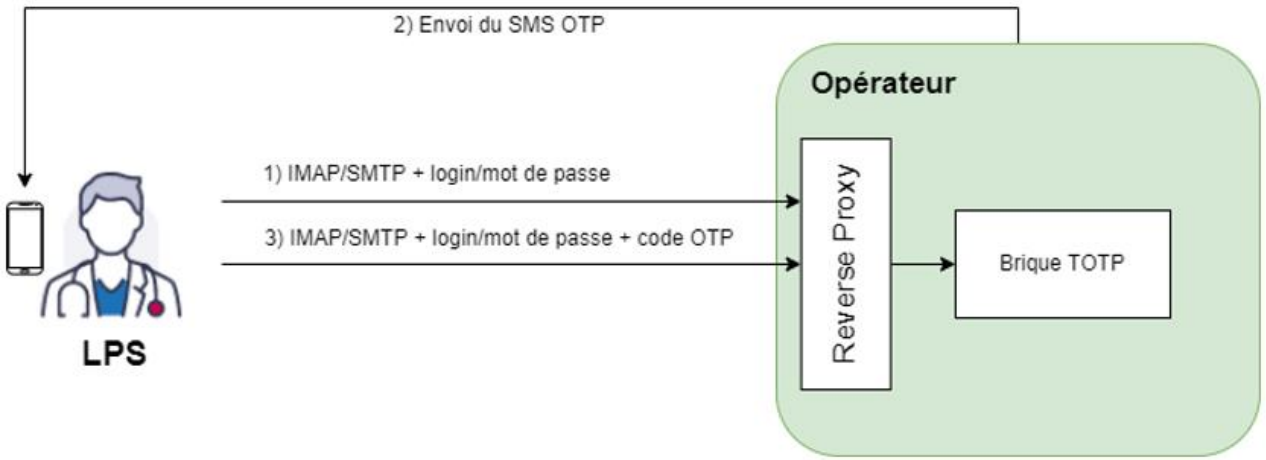
MS Santé
Système de messageries sécurisées, données protégées.

Questions / réponses

MIE – Authentification opérateur via OTP (1/2)

Solution retenue

1. Envoi d'une requête contenant login + mot de passe
2. La requête tombe en erreur mais déclenche l'envoi du code OTP sur le mobile du professionnel
3. Nouvel envoi de requête contenant login + mot de passe + code OTP



- Ne repose pas sur un standard SASL pour IMAP / SMTP
- Génération du code basé sur la RFC 6238
- Création d'un mécanisme SASL spécifique à présenter dans les capabilities des serveurs :
  - X-MSS-TOTP ?

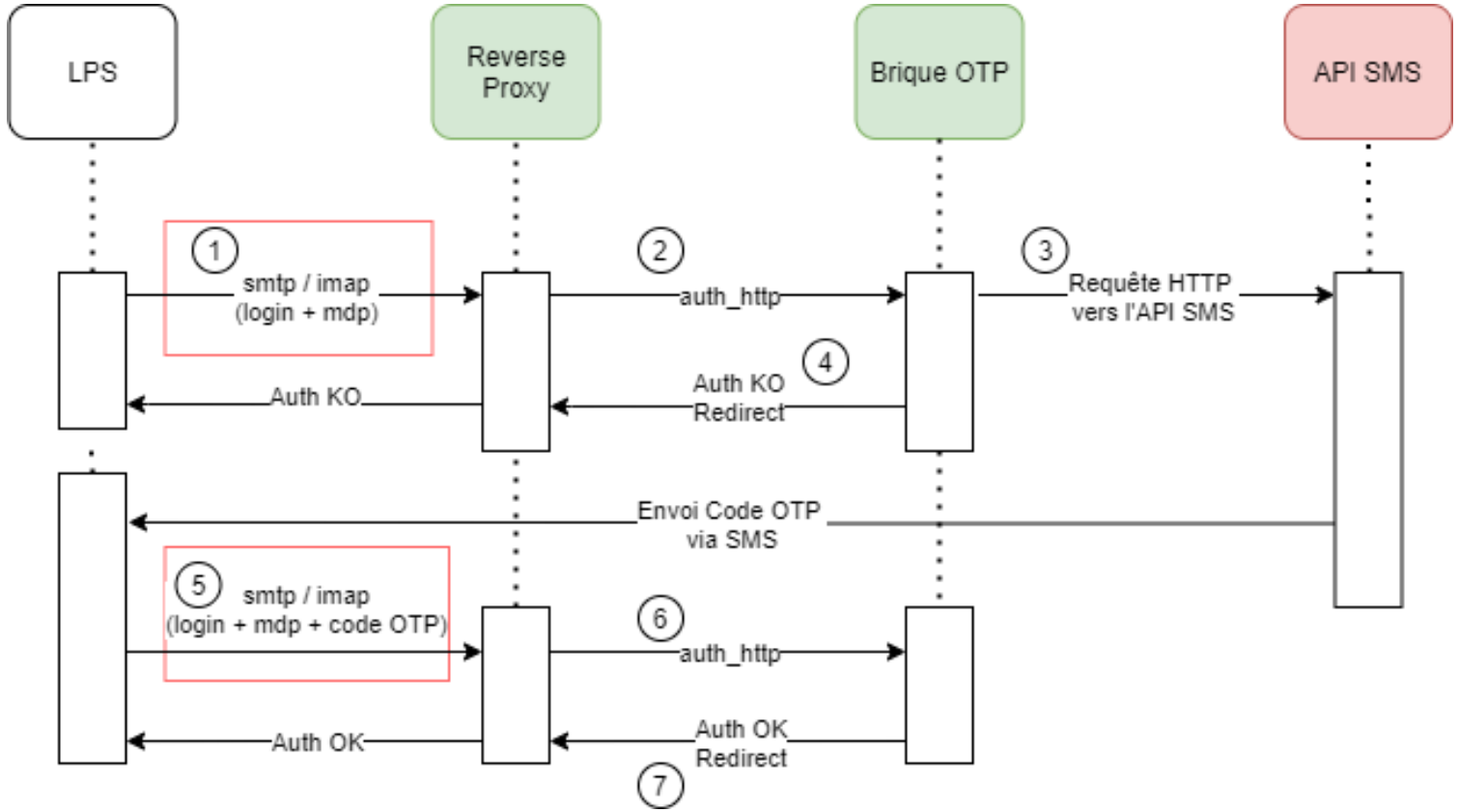
Impacts

- Opérateur :
  - Implémenter la logique associée, notamment la brique de TOTP (génération du code, envoi par SMS et vérification)
  - Disposer d'un service d'envoi de SMS, possibilité d'utiliser des services existants
- Editeur :
  - Implémenter la logique associée

Précision concertation

"des administrateurs ou techniciens du service IT peuvent avoir besoin d'accéder à une BAL pour analyser un problème" :
L'OTP est généralement utilisé pour accéder à des BAL de test en production, l'accès à une BAL par un service IT n'est actuellement pas encadré (sauf prise en main à distance)

MIE – Authentification opérateur via OTP (2/2)



MS Santé
Système de messageries sécurisées, données protégées.

Questions / réponses

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté Égalité Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ

MIE – CPS authentifiée par l'opérateur

Question pour les éditeurs logiciels métier :

Est-il obligatoire d'imposer aux opérateurs le MIE « CPS authentifiée par l'opérateur » dans l'API LPS ?

Arguments

- En attendant la disponibilité de CIBA et son implémentation par les éditeurs de logiciel métier, le flux de redirection doit être nécessairement employé. Il propose nativement l'authentification CPS via PSC.
- Le MIE OTP peut déjà être vu comme un backup à PSC
- Pour les logiciels métier en client lourd, l'ergonomie de l'authentification CPS locale à l'opérateur est meilleure que celle de PSC par flux de redirection (qui sollicite un navigateur externe). Pour autant cette authentification devrait pouvoir être maintenue par le LPS (voir durée)

Avis ANS

- Le flux de redirection est demandé via les DSR vague 1 aux éditeurs de logiciels métier
- La trajectoire voudrait que l'authentification CPS soit partout déléguée à PSC
- Le mécanisme d'authentification par certification IGC-Santé sera demandé aux opérateurs pour les BAL APP. Il est presque équivalent à celui des CPS.
- Les opérateurs implémentant l'authentification CPS « locale » vont la maintenir le temps de la transition

⇒ NON a priori afin de limiter le nombre de MIE

Avis éditeurs LPS ?

MIE – Certificat sur BAL applicative : contraintes sécurité

Impacts du prochain référentiel PGSSIS - identification des personnes morales :

A savoir

- [EXI 04] : Applicable au plus tard en juin 2022
- [EXI 03] : Dans le cas d'un service partagé comme MSSanté, le seul moyen d'authentification autorisé pour une personne morale est un certificat X509 de l'IGC Santé
- [EXI 05] : L'opérateur doit contrôler la validité du certificat dont le statut de révocation
- [EXI 02] Un service numérique en santé ne doit pas imposer la présence d'un nom applicatif particulier ou d'un nom de machine spécifique dans les attributs du certificat utilisé pour l'identification électronique d'une personne morale.

Référentiel identification Personnes Morales (v0,25 – oct. 2021) :
https://participez.esante.gouv.fr/media/default/0001/01/8fee76b80bc4f7151846b0932eb42d7a702545bf.pdf

MIE – Certificat sur BAL applicative : modalités proposées

Utiliser un certificat ORG AUTH-CLI par BAL applicative :

CN=<IdBAL>, 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) ET communication de l'IdBAL au client

2. Connexion sur la BAL applicative :
   - Contrôle de la validé du certificat
   - Extraction de l'IdNatStruc et de l'IdBAL du certificat
   - Vérification de la cohérence avec l'adresse BAL

Coté structure ou éditeurs logiciel

Remarque : La majorité des structures ont déjà dû générer un certificat ORG AUTH_CLI pour l'alimentation du DMP :
CN=Authentification DMP, OU=<IdNatStruc>, O=<NomStruc>, ST=<département> (XX), C=FR

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

Vos avis ?

MSSanté
Système de messageries sécurisées, données protégées.

Questions / réponses

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 NIL pour les éditeurs de client de messagerie ?
NIL du GIE-SV ?
Autre ?

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>*

Rationalisation des BAL publiées dans l'annuaire

Question pour les opérateurs :

- Quelles actions mettre à disposition d'un PS qui souhaite fermer une/plusieurs BAL détenues par un autre opérateur ?

Arguments

- L'objectif est de pouvoir retirer des BAL inactives de l'annuaire santé
- Profiter de la création d'une BAL afin de mettre en visibilité du PS toutes ses BAL
- Pouvoir déclencher des actions de suppression de BAL à l'initiative de l'opérateur

Proposition

- Mettre en place un processus transverse de suppression de BAL (à travers l'annuaire ?)
- À une fréquence à déterminer, mettre en visibilité toutes les BAL détenues par le PS

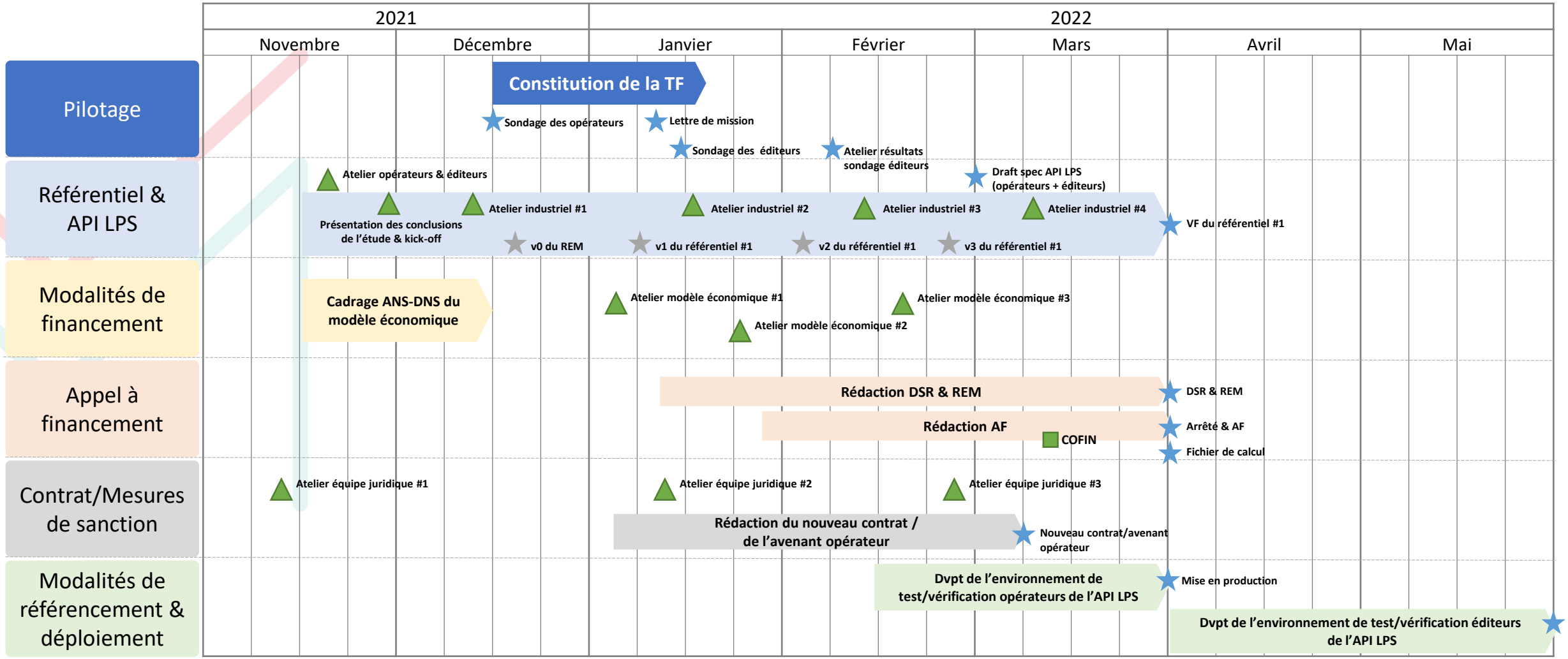
MS Santé
Système de messageries sécurisées, données protégées.

Questions / réponses

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté Égalité Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ

Rappel du calendrier de la Task Force



Légende ★ Livrable ★ Livrable intermédiaire ▲ Atelier ■ Réunion institutionnelle

Conclusion

Prochaines étapes :

- 28/01 : Opérateurs : atelier modèle économique #2
- Du 24/01 au 11/02 : entretiens bilatéraux entre les opérateurs membres de la TF et l'ANS
- 04/02 : Editeurs : atelier de présentation des résultats du sondage éditeurs
- 04/02 : Envoi de la v0.3 des exigences – **Merci de nous faire vos retours sur la v0.2 d'ici le 28/01**
- 11/02 : Atelier industriel #3

Merci pour votre attention !