



Task Force MSSanté

Atelier #1 du 10/12/2021



SOMMAIRE

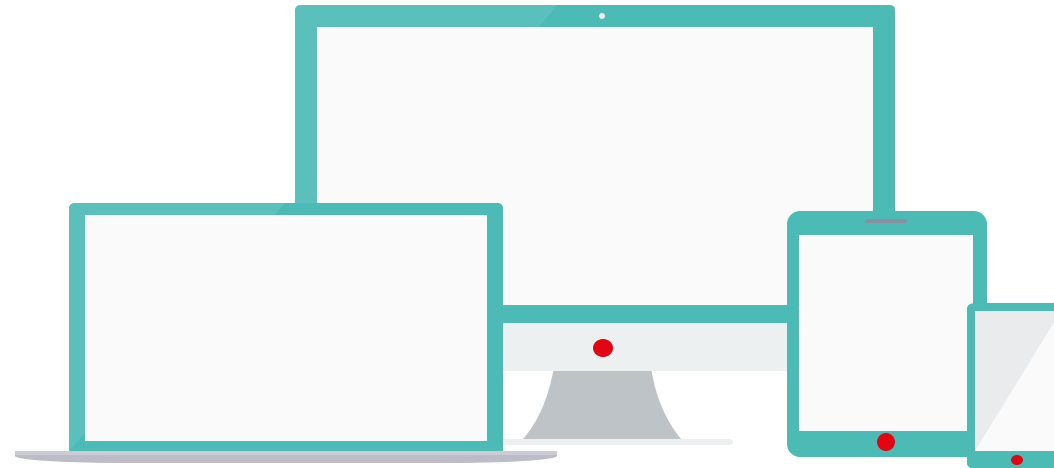
2h00

- | | |
|--------|--|
| 15 min | I. Introduction |
| 10 min | II. Enjeux et positionnement de la TF MSSanté dans le Segur |
| 30 min | III. Nouvelle API Clients – Opérateurs (dont POC CIBA) |
| 15 min | IV. Evolutions envisagées des exigences des référentiels |
| 50 min | V. Sujets à concerter (atelier #1) <ul style="list-style-type: none">• Méthodes d’authentification communes• Authentification OTP à retenir |

Afin que la réunion soit agréable pour tous



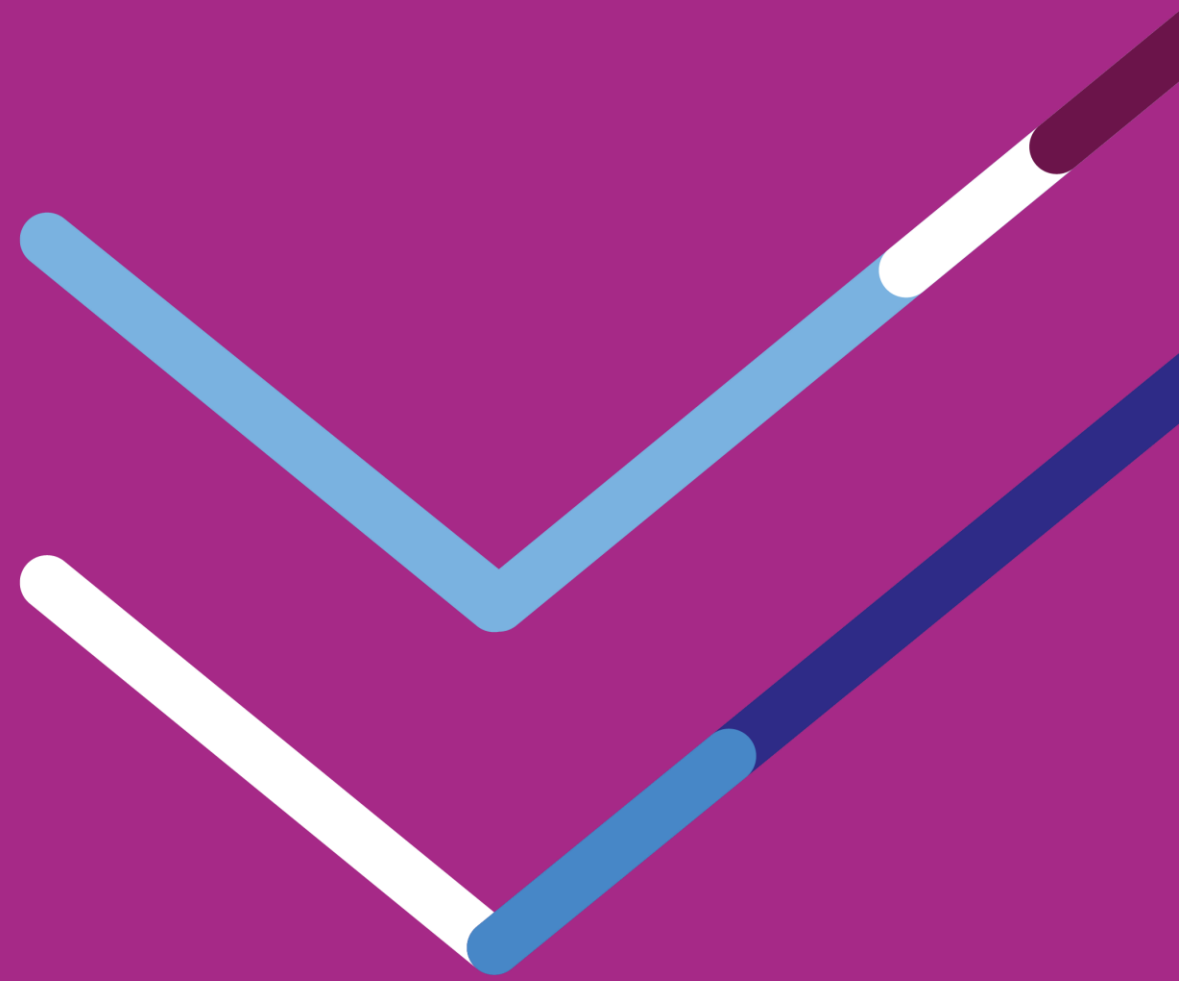
- Mettre son micro **en muet** lors des temps d'explication
- Privilégier le chat en ligne pour poser ses questions



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 intervenant.

Introduction



En septembre 2021, le déploiement et les usages MSSanté représentent :

Raccordement

81%

des établissements de santé

52%

des professionnels libéraux

36%

des EHPAD

71%

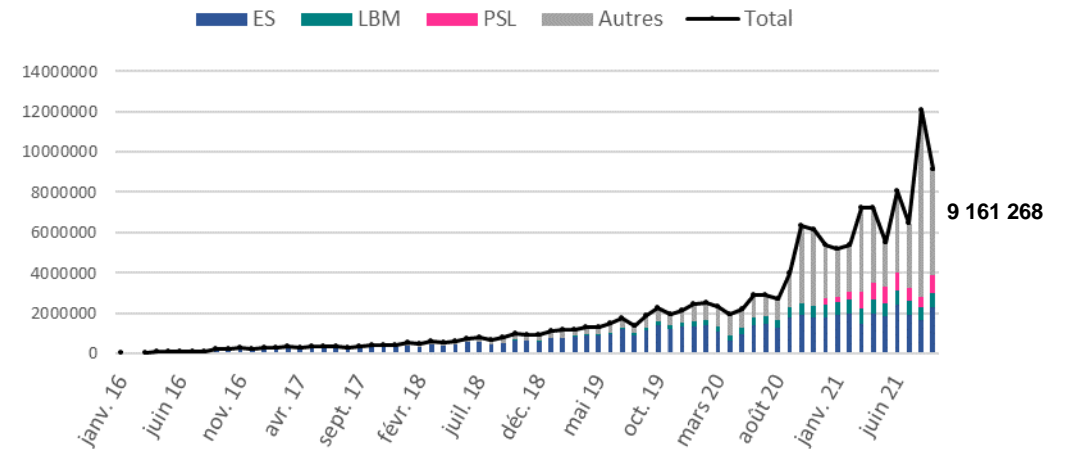
des laboratoires de biologie médicale

Une utilisation croissante des messageries sécurisées par les professionnels de santé et les structures de soins.

Usages

+ de 12 millions

de messages émis au mois d'août 2021



L'objectif est d'améliorer l'échange des données de santé essentiel au parcours de soins du patient et optimiser le parcours digital du professionnel de santé. Afin d'atteindre cet objectif, un financement est proposé.

- **Objectifs du financement**

- ▶ Faciliter l'intégration des messageries dans les outils métier via la nouvelle API
- ▶ Permettre la remontée d'indicateurs sur l'INS et la structuration des données
- ▶ Adapter les modalités de régulation de l'Espace de Confiance (Audits – Sanctions en cas de non-conformité)



Calendrier général

A partir de décembre 2021

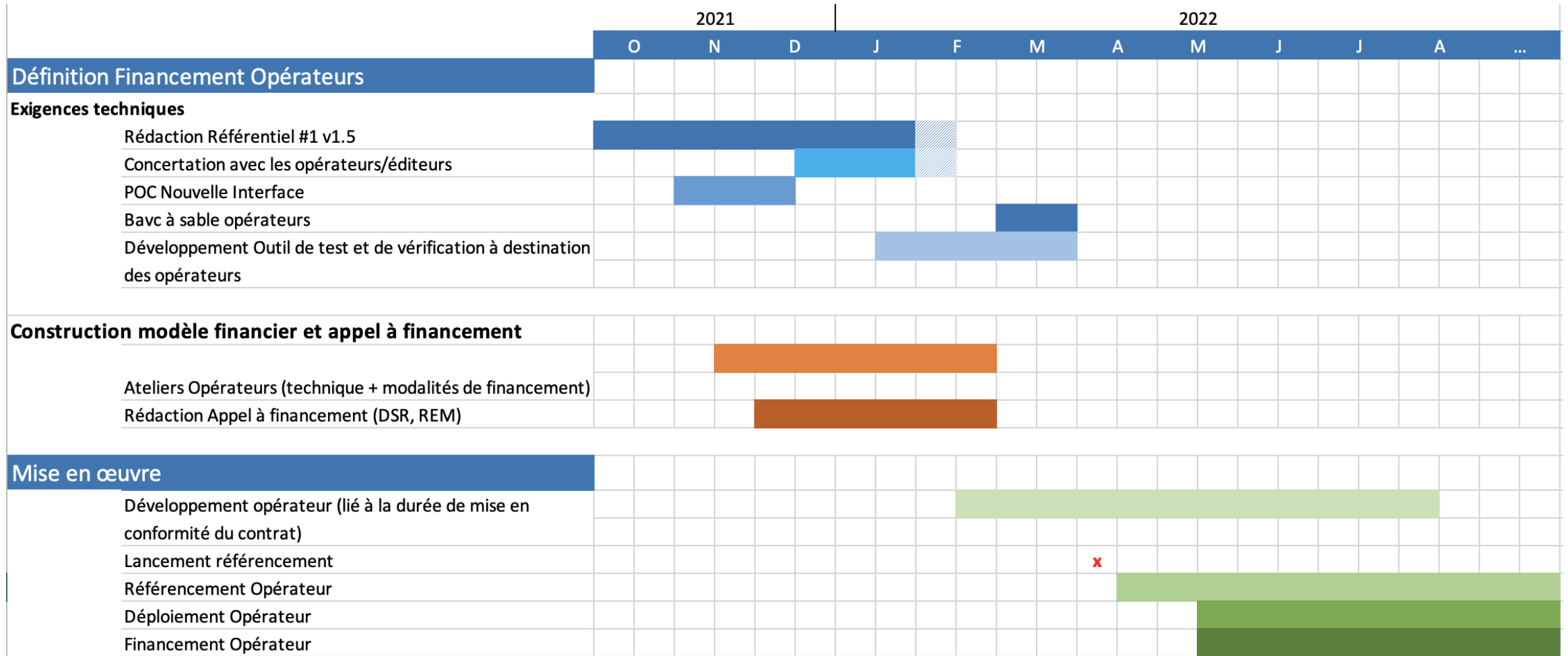
..... Ateliers avec les opérateurs

Fin décembre 2021

..... Début de la concertation sur le nouveau référentiel
Opérateurs

T2 2022

..... Lancement du référencement



Un fonctionnement en sprints de 3 semaines

J0

Publication de la version N du référentiel

Atelier technique #1 le 10/12 avec XX participants

J+7

Atelier API & référentiel avec les experts techniques

Atelier destiné aux éditeurs et opérateurs

J+14

Atelier modèle économique & éléments juridiques

Atelier destiné aux opérateurs

J+21

Publication de la version N+1 du référentiel

Congés scolaires

Vacances de Noël :
du 18 décembre au 3 janvier

Vacances d'hiver :
du 5 février au 7 mars
Paris du 19 février au 7 mars

Nous invitons les participants à s'engager activement dans la Task Force pour alimenter la réflexion de l'Etat dans la mise en œuvre des mesures Ségur.

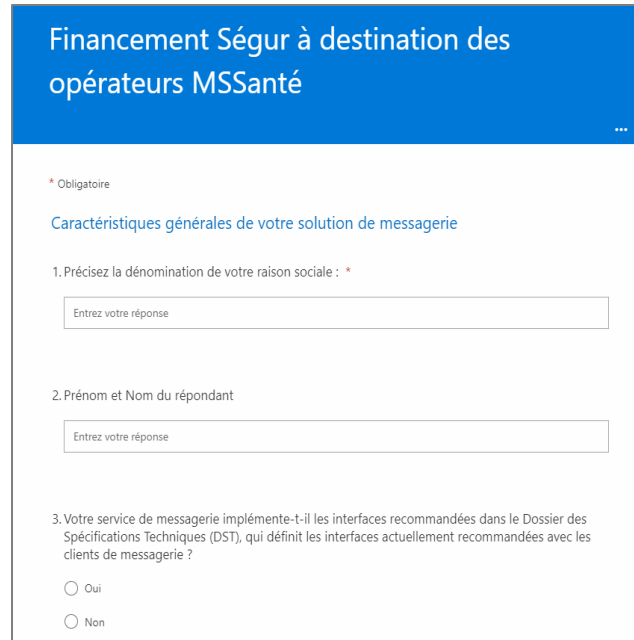
20 questions divisées en 3 sections

Nombres de réponses déjà obtenues :

7

- **Objectifs du questionnaire :**

- Connaitre votre solution de messagerie (type de proxy, d'interfaces).
- Connaitre les coûts d'installation et de création d'une solution messagerie pour une juste répartition de l'enveloppe de financement entre les opérateurs.



Financement Ségur à destination des opérateurs MSSanté

* Obligatoire

Caractéristiques générales de votre solution de messagerie

1. Précisez la dénomination de votre raison sociale : *

Entrez votre réponse

2. Prénom et Nom du répondant

Entrez votre réponse

3. Votre service de messagerie implémente-t-il les interfaces recommandées dans le Dossier des Spécifications Techniques (DST), qui définit les interfaces actuellement recommandées avec les clients de messagerie ?

Oui

Non



QR Code

Accéder au questionnaire



Questions / réponses



Enjeux et positionnement de la TF MSSanté dans le Segur

Enjeux et positionnement de la TF MSSanté dans le Segur

- Permettre aux éditeurs de logiciels professionnels (LPS...) de pouvoir s'accrocher avec l'opérateur choisi par un 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

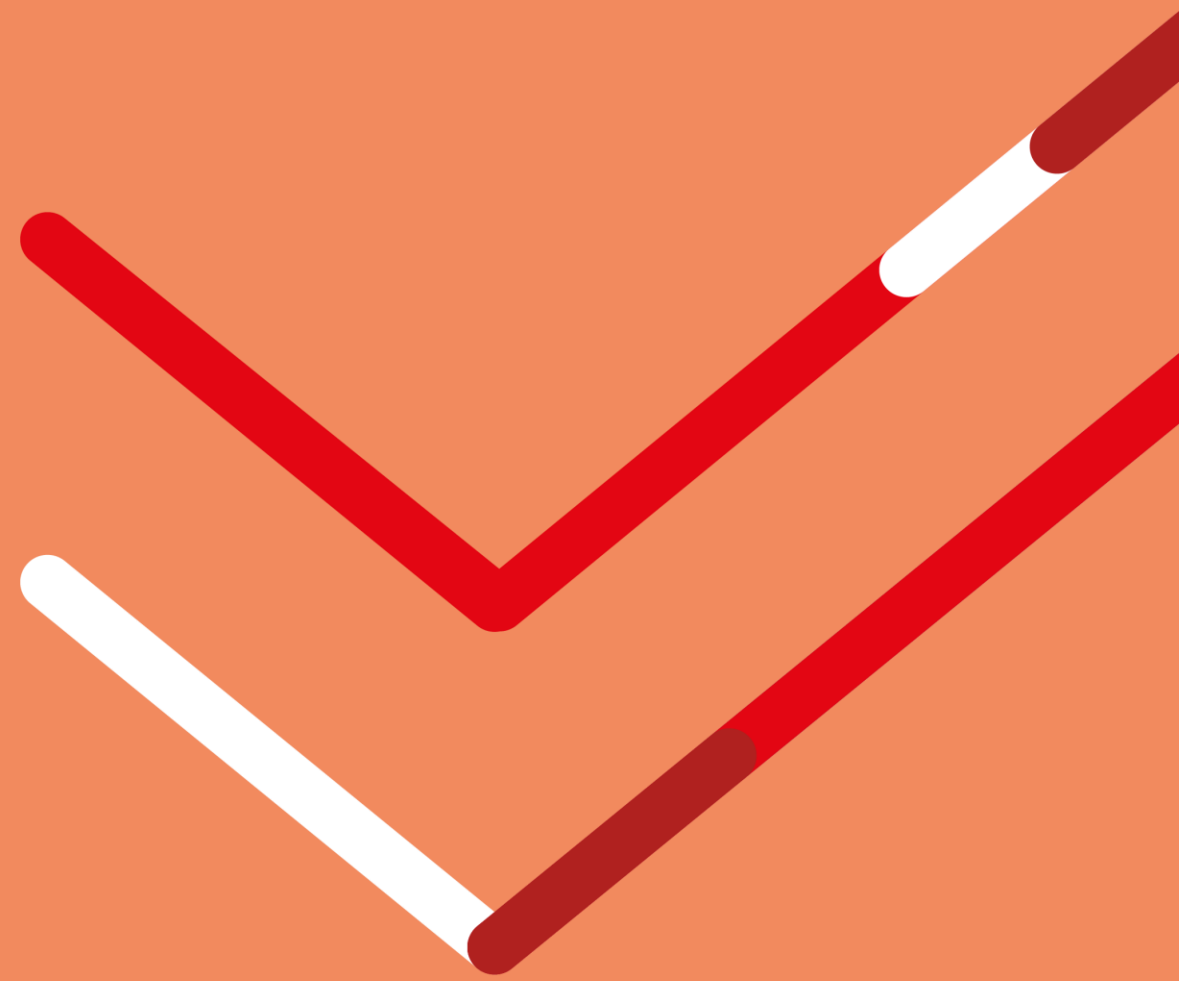




Questions / réponses



Nouvelle API Clients - Opérateurs



Objectifs de l'API

Aboutir à un système interopérable entre éditeurs et opérateurs MSSanté :

- L'API LPS définira un **seul protocole et une liste de méthodes d'authentification** à proposer par tous les opérateurs
- Proposer des **moyens de tests et de contrôles** aux éditeurs ET opérateurs pour s'assurer de l'interopérabilité
- Généraliser l'usage d'une **authentification nominative à double facteur** (BAL personnelles ET organisationnelles) avec une transition entre les méthodes d'authentification actuelles (CPS, OTP), et les "nouvelles" (eCPS, ...)

Proposition à concerter

- Protocoles : **IMAP/SMTP** (à confirmer avec les résultats du POC)
- 3 méthodes d'authentification pour les **BAL personnelles et organisationnelles** :
 - CPS via opérateur** : car nécessaire pour la transition des LPS en attendant la CPS via PSC CIBA
 - OTP** : car largement employée dans des contextes sans CPS (OTP email à exclure)
 - eCPS via PSC CIBA** : pour nouveaux usages en remplacement de l'OTP
- 1 méthode d'authentification pour les **BAL applicatives** :
 - Certificat IGC Santé** rattaché à une personne morale connue de l'annuaire santé

Remarques :

- JMAP manque de maturité : à étudier pour version ultérieure de API
- L'authentification CPS via PSC CIBA ne sera pas disponible pour la première version de l'API
- L'authentification PSC (via navigateur) serait optionnelle car cible CIBA retenue pour les logiciels en client lourd



Questions / réponses

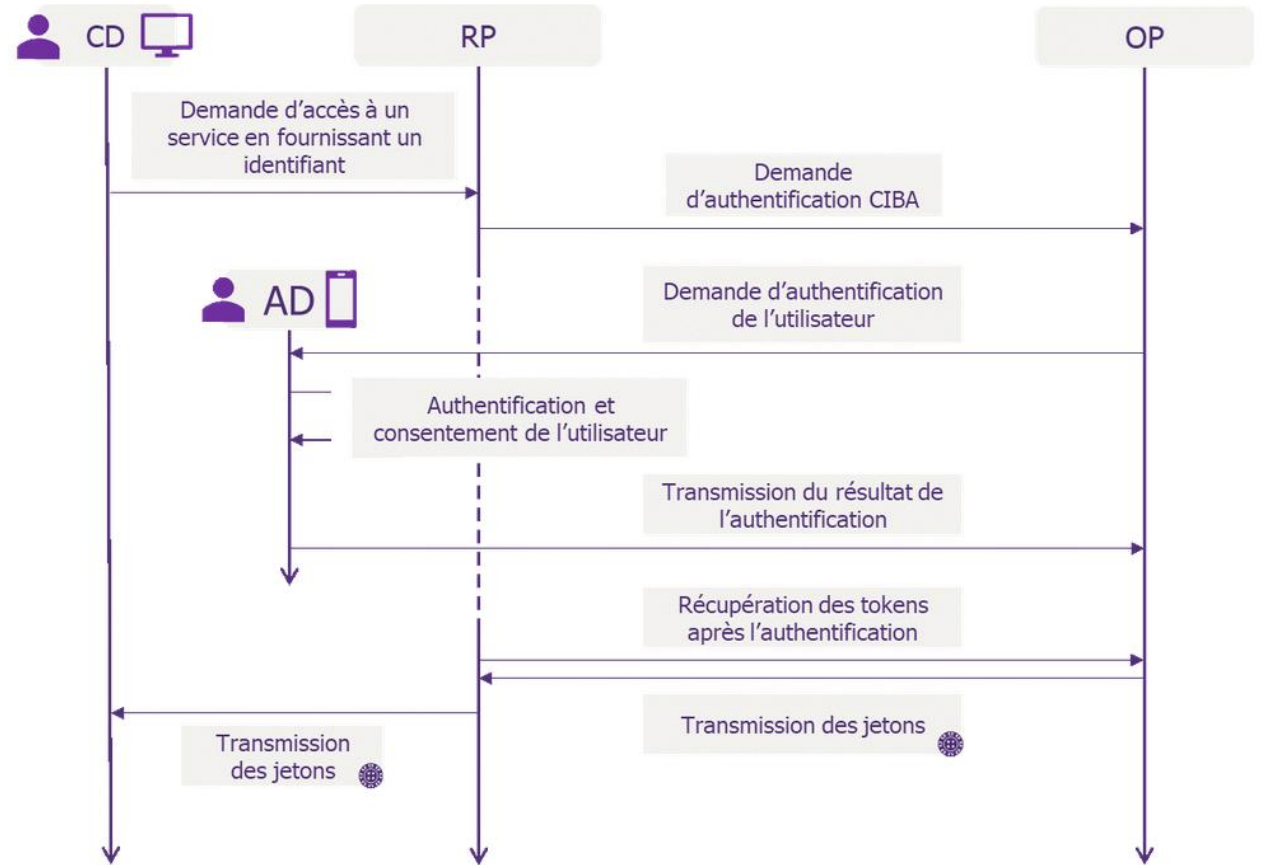


Objectif :

- Valider la faisabilité technique de l'utilisation de PRO Santé Connect comme fournisseur d'identité pour la nouvelle API

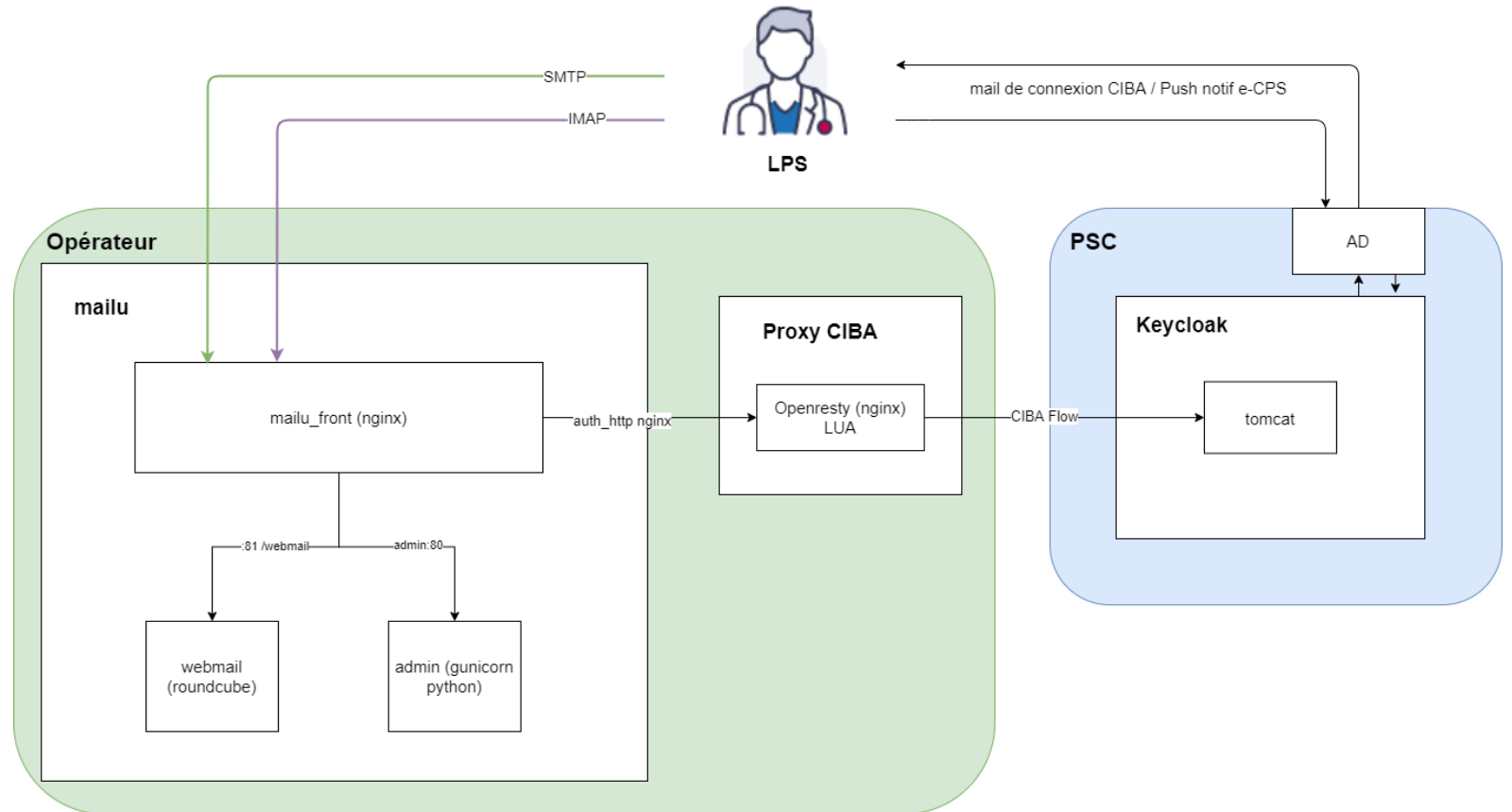
Spécificités de l'API :

- Utilisation par des LPS de type client lourd
- Flow OpenID Connect classique par redirection dans un navigateur non compatible
- CIBA : Nouveau flow OpenID Connect ne nécessitant pas d'ouverture de navigateur



Conclusions :

- Faisabilité technique vérifiée
 - Envoi et réception de mails avec Thunderbird
- Nécessite d'intégrer un « Proxy CIBA » côté opérateur
 - Délégation de l'authentification depuis le reverse proxy opérateur
- Transparent pour les éditeurs
- Compatible avec le standard IMAP/SMTP



Point validés

- Authentification PSC CIBA compatible avec IMAP/SMTP

Points à valider / concerter

- Faisabilité d'utiliser authentification OTP sur IMAP/SMTP
- Définir une authentification OTP « standard » (TOTP, SMS, ...) sur IMAP/SMTP
- Faisabilité de proposer 4 méthodes d'authentification sur IMAP/SMTP : eCPS, CPS « locale », OTP et certificats IGC-Santé rattaché à des personnes morales
- Calendrier disponibilité service PSC CIBA (eCPS)

Opérateurs

Le contrat / référentiel #1 v1.5 et le DSR MSSanté imposeraient l'implémentation de l'API client de messagerie :

- A tous les opérateurs de l'espace de confiance MSSanté (excepté le cas particulier de MES)
- En fonction des types de BAL proposées par l'opérateur, l'intégralité des méthodes d'authentification retenues devront être proposées

Remarque :

Le référentiel #1 n'interdira pas de proposer **en complément** d'autres protocoles/authentification non interopérables avec l'ensemble des clients

Clients de messagerie

Le référentiel #2 v1.0 décrira :

- L'implémentation de l'API pour les éditeurs
- Les modalités d'authentification à respecter pour chaque type de BAL

Rq : L'authentification eCPS CIBA pourrait être imposée pour tous les contextes d'usage

Suivant les couloirs les DSR Vague 2 imposeront :

- l'implémentation de l'API
- les méthodes d'authentification obligatoires (fonction des utilisateurs ciblés)

Proposition de nommage des API MSSanté :

- API MSS-OE : pour la nouvelle API Opérateurs – Editeurs (IMAP/SMTP)
- API MSS-IO : pour l'API existante entre opérateurs : Interop Opérateurs (SMTP via certificat serveur)



Questions / réponses



Evolutions envisagées des exigences des référentiels



Contrat opérateurs

- Engagement de conformité remplacé par des **contrôles a priori** (lors des MAJ de référentiel) et à la demande
- Gradation des **sanctions** possibles en fonction des non conformités détectées lors des contrôles

Référentiel #1

Exigences relatives :

- à l'API Clients de messagerie (pour implémentation par les opérateurs)
- aux nouveaux indicateurs d'usage : présence INS qualifié, type de document
- aux extractions annuaires utilisées
- à la suppression de toutes les BAL lors d'un retrait de NDD
- suppression de tout NDD sans exploitation
- au rattachement des BAL au bon FINESS G ou J

Modalités de contrôles / audit

2 modalités de contrôle à distinguer :

- Le contrôle unitaire (référencement) réalisé **via le DSR TF MSSanté** pour les opérateurs qui postulent. Portent sur :
 - API Client de messagerie
 - nouveaux indicateurs d'usage
- Les contrôles « récurrents » réalisés **via le contrat opérateur** pour l'ensemble des opérateurs de l'espace de confiance :
 - Sécurisation du canal entre opérateurs : TLS, liste blanche, DNS ...
 - API Client de messagerie
 - Suppression des BAL inactives
 - ...

Référentiel #2 (hors périmètre TF MSSanté)

Exigences relatives :

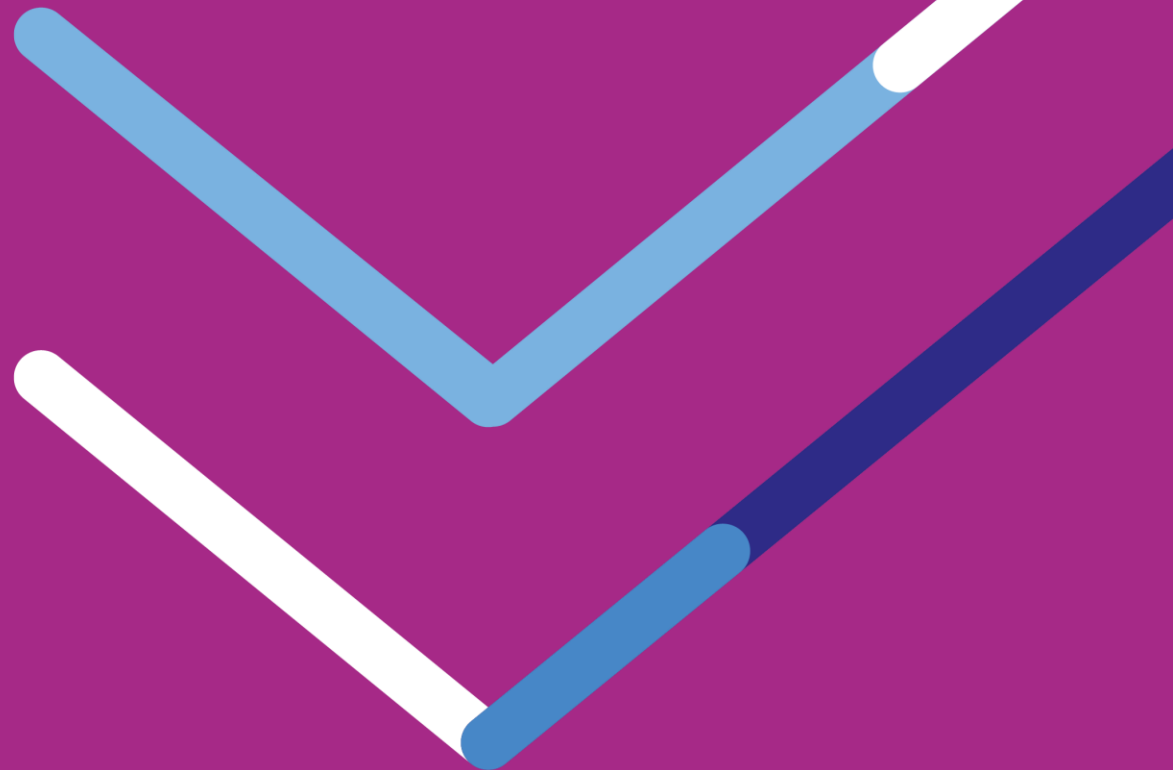
- à l'API Clients de messagerie (pour implémentation par les éditeurs)
- à la consultation de l'annuaire santé (LDAP/extractions)
- aux accusés de lecture et de bonne intégration



Questions / réponses



Sujets à concerter (atelier #1)



Objectif :

- Valider la faisabilité technique de proposer les 4 moyens d'authentification suivants sur l'API MSS-OE :
 - Via PRO Santé Connect : CIBA
 - En local chez l'opérateur : CPS, OTP et certificats IGC-Santé rattaché à des personnes morales

Points clés :

- Calendrier :
 - Fin du POC prévue fin d'année
 - Partage des éléments en comité mi-janvier
- 2 réserves techniques sont notamment à lever :
 - Possibilité d'utiliser une solution standard d'OTP sur le protocole IMAP et SMTP ?
 - Comment proposer « simplement » plusieurs moyens d'authentifications sur l'API MSS-OE ?
- Pistes privilégiées :
 - Multi-authentications : 2 pistes
 - Utilisation de endpoints différents
 - Utilisation de ports différents
 - OTP : 2 pistes
 - Utilisation du TOTP

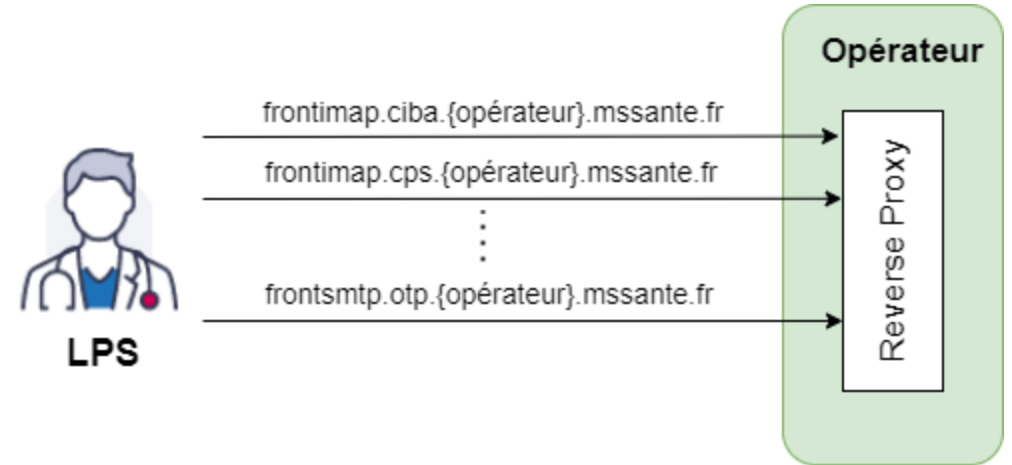
Implémentation du CIBA chez l'opérateur

Options possibles :

- Utilisation de [SASL](#) sur un endpoint unique
 - Standard rendant possible l'utilisation de moyens d'authentification classiques sur IMAP / SMTP
 - Problème :
 - Standard théorique, pas ou peu d'implémentations existantes
 - Ne gère pas les authentifications spécifiques comme la CPS par exemple
- Utilisation de ports différents
 - Problèmes potentiels :
 - Nécessite l'utilisation de ports non standards pour IMAP / SMTP
 - Nécessite une configuration spécifique du pare-feu pour le PS
- Utilisation de endpoints différents
 - Proposer un FQDN par moyen d'authentification. Exemple : frontimap.ciba.{opérateur}.mssante.fr
 - Piste privilégiée à date car peu de réserves techniques à lever

Scénario multi-endpoints :

- Côté opérateur
 - 8 certificats IGC Santé à maintenir côté opérateur (4 IMAP + 4 SMTP)
 - 8 entrées DNS
 - Implémentable « simplement » côté opérateur par configuration d'un reverse proxy
 - Permet de bien séparer les logiques d'authentification
- Côté éditeur
 - Utilisation de la totalité ou d'une partie des moyens d'authentifications
 - Implémentation « simple » par appel à l'URL proposant l'authentification souhaitée
 - Capacité à gérer plusieurs URL pour accéder au même service
- Autre option ? Utiliser des ports dédiés à chaque moyen d'authentification



Contraintes

- Maintient de 8 certificats différents
- Enregistrement de 8 entrées dans le DNS
- Nécessite 8 IP publiques pour exposer les 8 URL

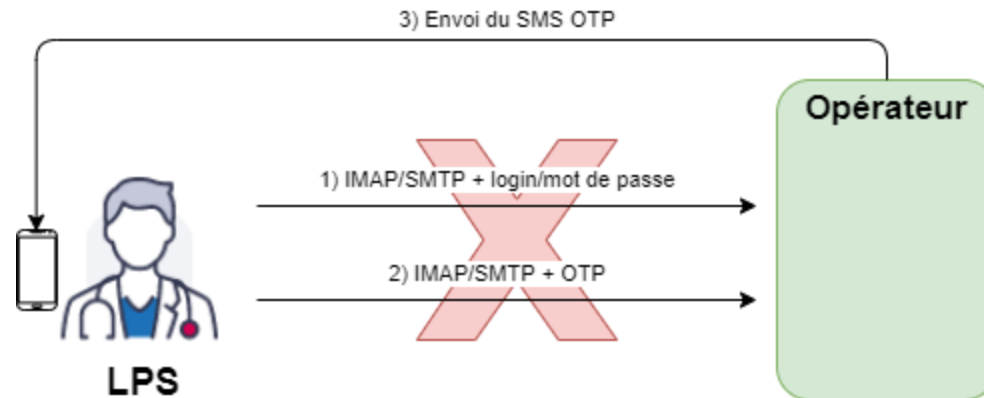


Questions / réponses



Pourquoi un OTP spécifique ?

- L'utilisation de l'OTP SMS « classique » est incompatible avec le protocole SMTP/IMAP
- Ces protocoles n'ont pas la flexibilité de HTTP et ne permettent pas de gérer de challenge/réponse tel que le demande l'OTP SMS



- Besoin de trouver une solution OTP compatible avec les contraintes de IMAP et SMTP

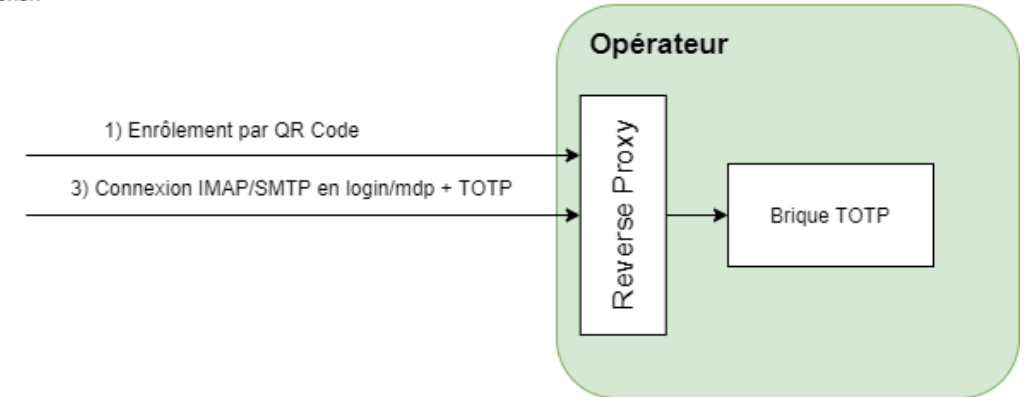
Option 1 : Utilisation TOTP

- Basé sur la RFC [6238](#)
- Utilise le principe d'enrôlement et de token
- Envoi en une requête du login/mot de passe et du TOTP
- Côté opérateur
 - Nécessite d'implémenter la logique TOTP (des solutions standards existent) et de proposer une page d'enrôlement par QR code
- Côté éditeur
 - A priori pas d'impact
 - Contrainte PS : disposer de l'application [FreeOTP](#) sur son mobile

Réserve :

- Comment envoyer le TOTP depuis le LPS vers l'opérateur ?

2) Déverrouillage du token

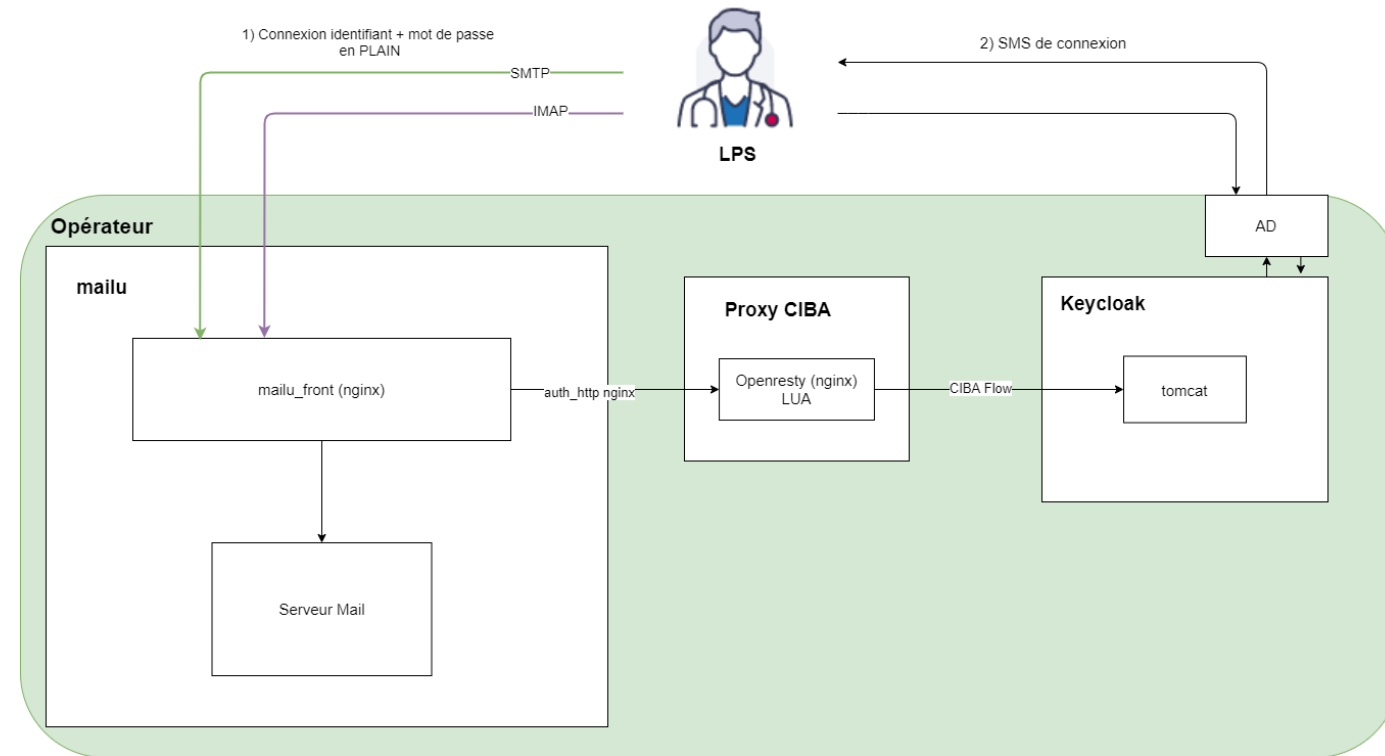


Contraintes

- Implémentation de la logique TOTP côté opérateur (génération des codes, génération des QR code pour l'enrôlement etc ..)
- Installation d'une application sur le mobile du PS
- Enrôlement préalable du PS auprès de l'opérateur

Option 2 : CIBA opérateur

- Basé sur la norme [OpenID Connect](#)
- Un SMS est envoyé par l'opérateur sur le téléphone du PS contenant un lien cliquable
- Côté opérateur
 - Nécessite l'implémentation d'un Keycloak et de la brique AD (Authentication Device - qui sera chargée de faire l'envoi de SMS)
- Côté éditeur
 - A priori pas d'impact
 - Contrainte PS : Disposer d'un mobile avec accès à internet



Contraintes

- Déploiement d'une solution CIBA (Keycloak) et d'une brique d'AD
- Contraction abonnement SMS auprès d'un fournisseur tiers
- Accès internet sur le mobile du PS nécessaire pour valider l'authentification



Questions / réponses



Autres sujets concerter :

- Modalité de tests et de contrôle des 2 API MSS
- Adéquation de l'IGC Santé avec les contraintes des industriels pour les certificats des BAL applicatives
- ...

Prochaines étapes :

- 10/12 : diffusion d'un premier draft des exigences de la TF MSSanté
 - Retour attendus début janvier (date à définir)
- 21/01 : Atelier #2 suite aux réponses à la lettre de mission