MSSanté
Système de messageries sécurisées, données protégées.

Task Force MSSanté

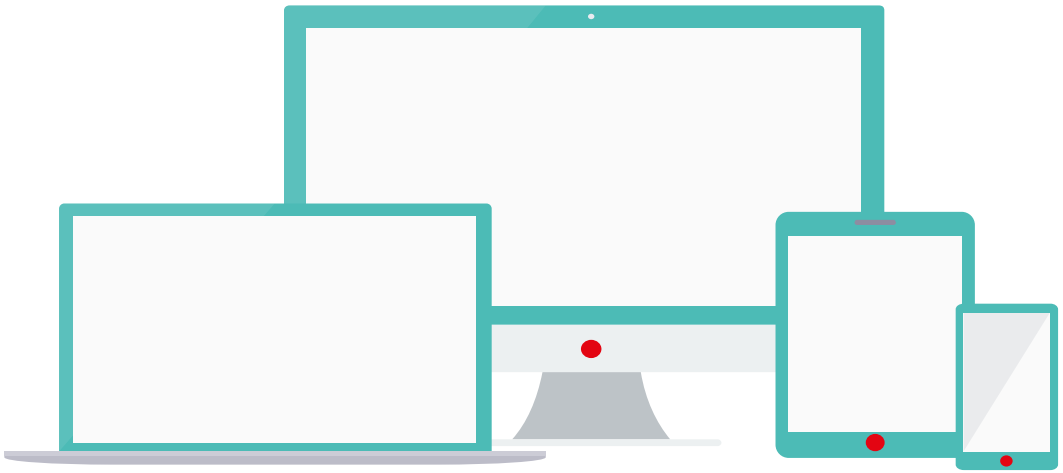
Atelier industriel #4 du 11/03/2022

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.

SOMMAIRE

MSSanté
Système de messageries sécurisées, données protégées.

Introduction

Exigences – MAJ récentes

v0.3 : merci pour vos retours - 5 opérateurs ont contribués

v0.4 : publiée le 10/03 - dernière version avant publication pour concertation publique

- Prendre connaissance des réponses ANS (colonne S) sur les remarques opérateurs formulées en v0.3
- Pas de nouvelles exigences

Remarques notables

- IMAP / conservation des données : IMAP permet de conserver les messages des professionnels sur le serveur jusqu'à leur suppression par ce dernier. Outre la suppression des BAL sur inactivité, il faudra instruire en vague 2 Ségur des exigences LPS visant à limiter les messages stockés chez l'opérateur
- Durée de session utilisateur : La session PSC sera maintenue par le LPS. Elle sera fermée après 15 minutes d'inactivité (4h totale)
- Transition TLS 1.2 de l'interface opérateurs : Pour garantir l'interopérabilité des opérateurs TLS 1.0 devra être arrêté qu'à l'issue de la période de mise en conformité le Ref#1 v1.5.

Exigences modifiées

- MSS 6 : Proposer, pour les personnes physiques, un MIE indépendant de PSC passé d'exigence à recommandation
- MSS 7.2 & 7.4 : méthode de transport de l'Access Token arrêtée. (voir explications ci-après)
- MSS 19 à 25 : les délais relatifs aux contrôles et aux sanctions ont été précisés (voir détail plus loin)

API LPS

API LPS – Transmission de l'Access Token à l'opérateur

Détails techniques

- Objectif : Transmettre un Access Token de type JWT (rfc7519) comme Bearer token (rfc6750) pour l'établissement d'une session IMAP et SMTP
- Implémentation retenue : XOAUTH2
  - XOAUTH2 : Solution la plus utilisée pour faire transiter un Access Token sur IMAP et SMTP (utilisée par Google et Microsoft notamment et proposée dans Thunderbird)
  - Pour IMAP, la capability SASL-IR doit être proposée par le serveur. Cette fonctionnalité permet au client d'envoyer le mode d'authentification choisi en même temps que la chaine d'authentification
  - Exigences modifiées : 7.2 et 7.4

IMAP

```
[connection begins]
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
```

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 XOAUTH2
S: 250-ENHANCEDSTATUSCODES
S: 250 PIPELINING
C: AUTH XOAUTH2 dXNlcj1zb21ldXNlckBleGFtcGxlLmNvbQFhdXRoPUJlY
XJlciB5YTI5LnZGOWRmdDRxbVRjMk52YjNSbGNrQmhkSFJoZG1semRHRXVZMj
l0Q2cBAQ==
S: 235 2.7.0 Accepted
```

- Valeur du champ XOAUTH2 : base64("user=" {User} "^Aauth=Bearer " {Access Token PSC} "^A^A")

API LPS - Moyen de test / recette pour les opérateurs (1/2)

Finalités :

- Permettre à l'opérateur de tester ses développements de l'interface API LPS sur des données de test PSC, essentiellement sur des cas passants

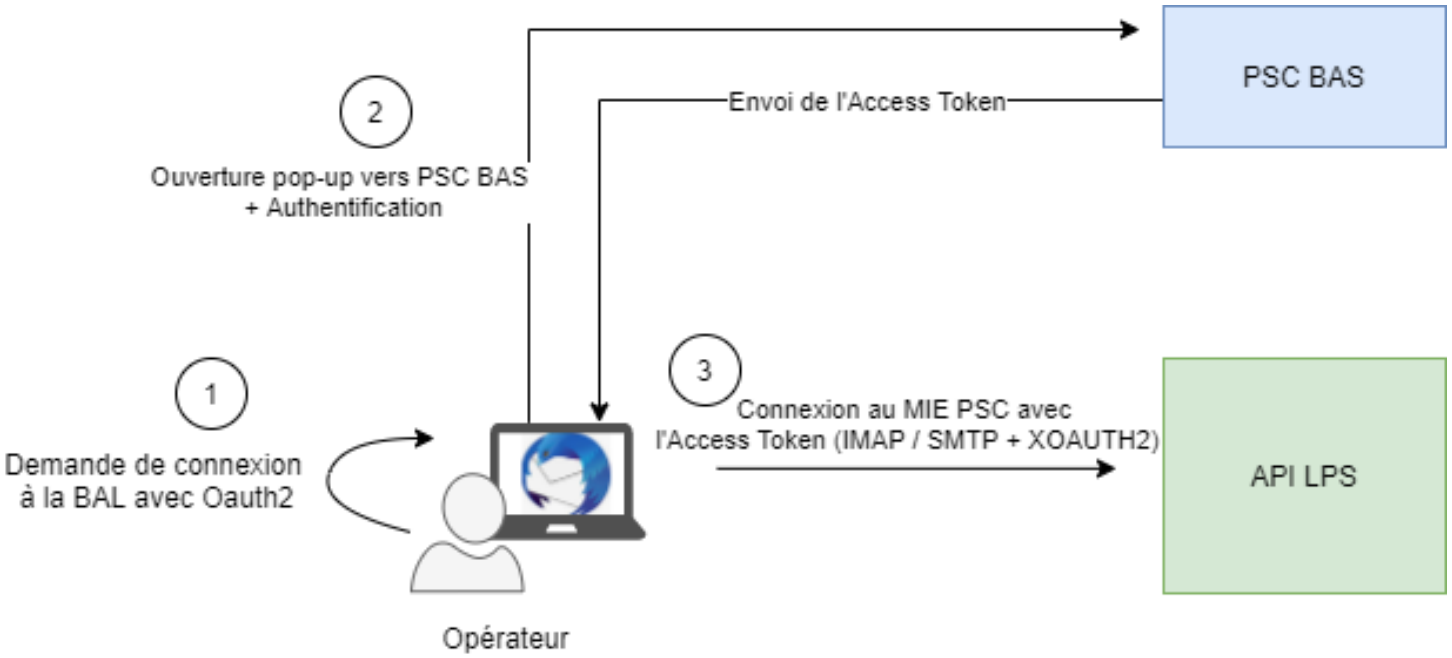
Mozilla Thunderbird + environnement "Bac à sable" PSC :

- Pour le MIE PSC :
  - Propose depuis la version 38 le mode d'authentification « OAuth2 », qui correspond concrètement à XOAUTH2
  - Nécessite une modification de la configuration de Thunderbird pour fonctionner avec PSC (ajout des URL PSC BAS, du client_id et du client_secret)
  - L'authentification à PSC sera réalisée à l'intérieur d'une pop-up et aboutira à la production d'un Access Token PSC de test
  - La documentation pour effectuer cette modification sera fourni par l'ANS
- Pour le MIE AUTH_CLI :
  - Propose le mode d'authentification « certificat client »
  - L'opérateur devra générer des certificat ORG AUTH_CLI de l'IGC Santé de TEST, puis les ajouter au magasin de certificat de Thunderbird
  - Ne nécessite pas de modification de la configuration de Thunderbird

Mise en garde

Le client mail Thunderbird est proposé comme moyen de test uniquement sur le BAS PSC. Thunderbird ne répond pas aux exigences du référentiel PRO Santé Connect et ne PEUT PAS être utilisé en production comme client MSSanté

API LPS - Moyen de test / recette pour les opérateurs (2/2)



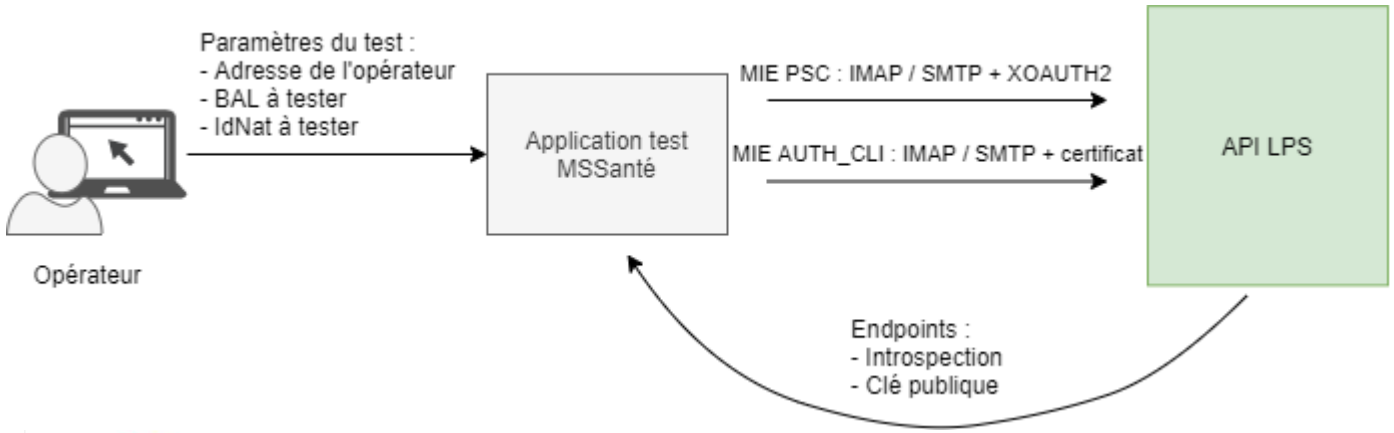
API LPS - Application de test et de contrôle opérateurs

Finalités :

- Permettre à l'opérateur de tester ses développements de l'API LPS, y compris sur des cas non passants difficiles à reproduire
  - Access Token non PSC, Access Token expiré
- Permettre de produire le rapport de conformité demandé par l'ANS pour le Ségur

Cinématique

1. Connexion de l'opérateur via son navigateur sur la plateforme de test MSSanté
2. Lancement du test en cliquant sur le Job correspondant
3. Saisie des éventuels paramètres : Adresse de l'API LPS opérateur à tester, BAL à tester, IDNAT utilisé
4. Affichage du résultat du test dans l'application



A retenir

- L'application agit comme un « Bouchon » à PSC en exposant des services OpenID Connect
- Nécessite de modifier le FI utilisé côté opérateur
- Nécessite de fournir des paramètres pour lancer le test dans l'application

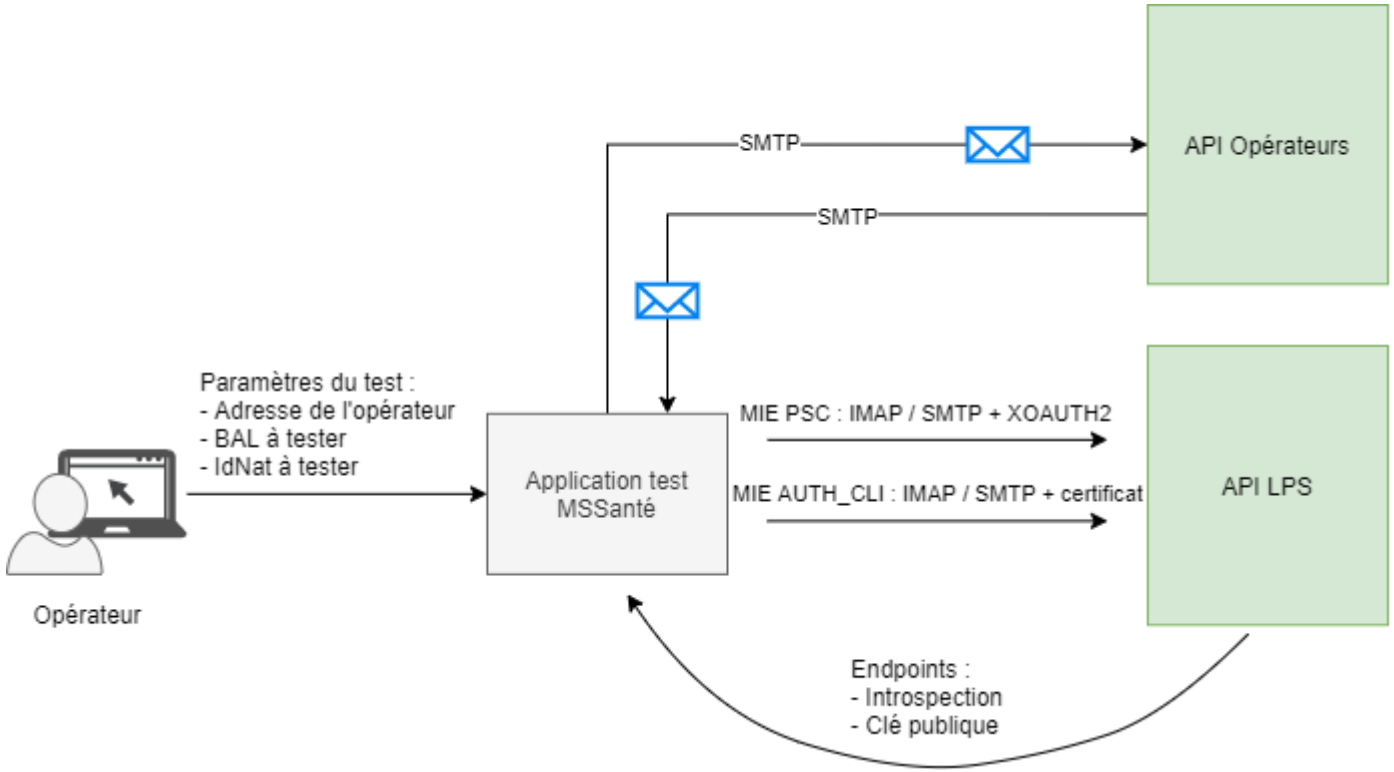
Interface Opérateur - Application de test et de contrôle opérateurs

Finalités :

- Permettre à l'opérateur de tester ses développements de l'interface Opérateur, y compris sur des cas non passants difficiles à reproduire
- Permettre de produire le rapport de conformité demandé par l'ANS pour la conformité au Référentiel #1

Cinématique

- Identique à l'interface API LPS mais nécessite que le système opérateur envoi des mails sur la BAL de l'application de test



A retenir

- En cours de construction
- Solution unifiée pour le test des 2 interfaces de l'opérateur
- Nécessite que le système de l'opérateur envoi des mails sur des BAL de l'application de test
- Nécessite que l'opérateur se trouve dans l'espace de confiance de test

Focus sur certaines exigences ou principes

Contrat – Principes de contrôle / audit des opérateurs

Jusqu'à aujourd'hui (cad Ref#1 1.4) :

- Principe de l'engagement de conformité accompagné de contrôles a posteriori
- Les tests de l'opérateur se faisaient directement dans l'espace de confiance de production

A l'entrée dans l'EC ou MAJ majeure Ref#1 (A priori)

- Engagement de conformité (annexe 2 au contrat) à signer par l'opérateur

Dans l'espace de confiance MSSanté (A posteriori)

- Contrôles ponctuels déclenchés à l'initiative de l'ANS

Contrat – Principes de contrôle / audit des opérateurs

Demain (cad à partir de Ref#1 1.5) :

- Passage à un principe de contrôles a priori, accompagné d'un engagement de conformité
- Maintien de la possibilité de contrôles a posteriori
- Les tests de l'opérateur se font sur l'espace de confiance de test

A l'entrée dans l'EC ou MAJ majeure Ref#1 (A priori)

- Contrôle de l'API LPS : rapport de test généré par l'outil de contrôle
  - Demandé aussi ponctuellement comme preuve lors du référencement Ségur
- Contrôle de l'interface opérateurs : rapport de test (généré par l'outil de contrôle) à produire avant fin de période de mise en conformité du référentiel
- Engagement de conformité à l'ensemble des exigences du Ref#1

Dans l'espace de confiance MSSanté (A posteriori)

- Contrôles périodiques des interfaces opérateurs en production (type "monitoring") : tests de sécurité réalisés sans intervention des opérateurs
- Audits ponctuels d'opérateurs déclenchés à l'initiative de l'ANS

Evolution des modalités d'intégration à l'Espace de Confiance

Opérateur éditeur de proxy

1. Intégration en Espace de Confiance de test
2. Délai de mise en conformité de 6 mois (renouvelable une fois)
3. Production d'un CR de conformité + engagement de conformité

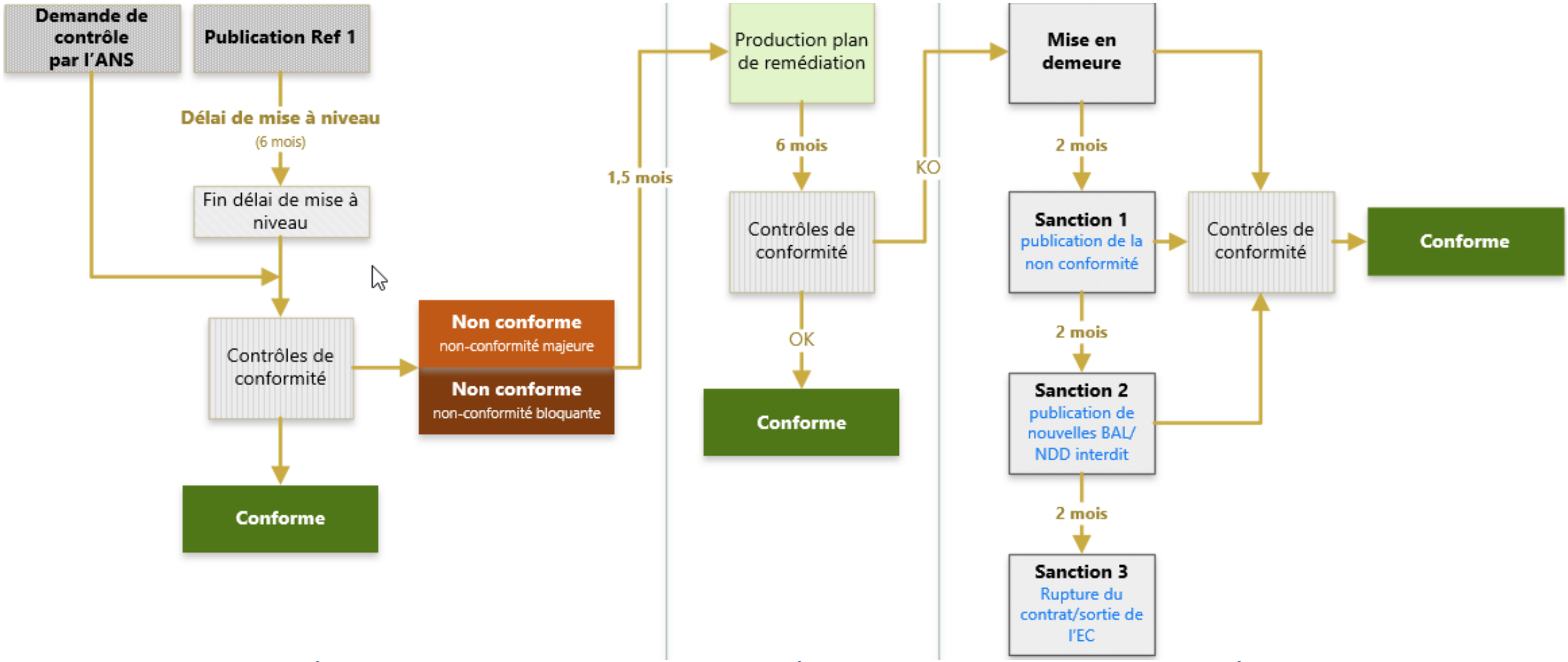
4. Intégration en Espace de Confiance de Production

Opérateur utilisant un proxy développé par un tiers

1. Production du CR de conformité de la solution choisie
2. Engagement de conformité

3. Intégration en Espace de Confiance de Production

Contrat : nouvelles modalités de contrôles / sanctions



Contrat : nouvelles modalités de contrôles / sanctions

MSS 20 : Tout opérateur présent en Espace de Confiance de production DOIT produire un niveau de conforme, 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

Conforme	Non-conforme	Non-conforme
pas de non-conformités ou présence de non-conformités mineures	présence de non-conformités majeures	présence de non-conformités bloquantes

Question

- **T0 : le délai entre le constat de non-conformité et la fourniture du plan de remédiation ?**
- **T1 : le délai pour la mise en conformité après fourniture du plan de remédiation ?**
- **T2 : le délai entre la mise en demeure et l'arrivée de la sanction 1 ?**
- **T3 : quel délai de mise en conformité après la sanction 1 ?**
- **T4 : quel délai de mise en conformité après la sanction 2 ?**

Proposition

- **T0 : un délai de 6 semaines**
- **T1 : un délai de 6 mois**
- **T2 : un délai de 2 mois**
- **T3 : un délai de 2 mois**
- **T4 : un délai de 2 mois**

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

Arbitrages

- **MSS 14** : l'exigence reste inchangée. Le délai de **12 mois** avant procédure de suppression de BAL est conservé
- **MSS 19** : toutes BAL **avec minimum 1 an d'existence** et n'ayant pas fait l'objet d'une authentification sur **60 jours** consécutifs, devront être dépubliées de l'Annuaire Santé
- **MSS 17** : le listing des BAL ouvertes devrait parvenir au PS par sa BAL non sécurisée

Conclusion et prochaines étapes

Conclusion

Prochaines étapes :

- **Fin mars / début avril** : concertation publique du contrat opérateur et du référentiel #1 v1.5
  - Durée courte : probablement 10 jours
  - Emplacement : site de concertation ANS : participez.esante.gouv.fr
  - Les modifications apportées depuis la précédente version publiée seront visibles dans les documents
  - Retours : attendus sous forme de fiches de lecture
- **2eme quinzaine d'avril** : publication versions finales du contrat opérateur et du référentiel #1 v1.5

Merci pour votre attention !

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