MSSanté
Système de messageries sécurisées, données protégées.

Segur vague 2

Concertation exigences MSSanté

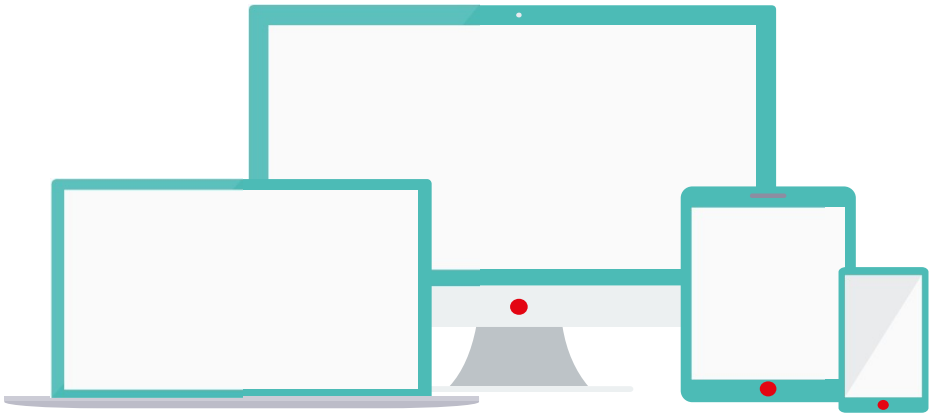
Atelier Editeurs #6 du 21/10/2022

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 :

- **Rappeler le nom de son entité / DSR** pour contextualiser l'intervention
- **Utiliser le chat en ligne.** Nous vous répondrons à la fin de la présentation de chaque l'intervenant.
- **Utiliser la fonction « lever la main »** et attendre l'aval des conférenciers

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

Introduction

Depuis le comité #5 :

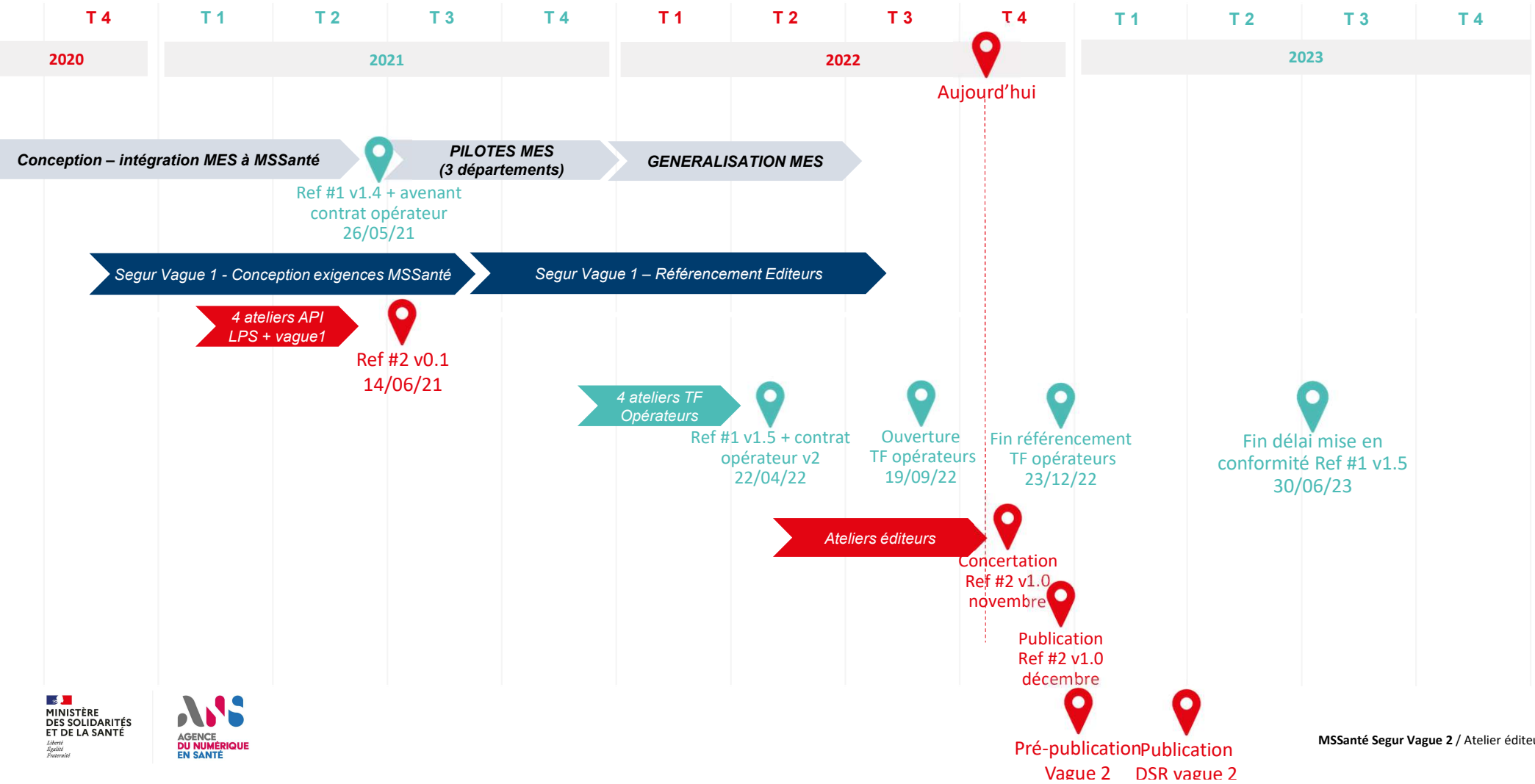
- **Intégration des exigences socle MSSanté vague 2 dans l'itération 1 des REM des TF**

- **Prise en compte des retours éditeurs** :
  - Via le référentiel d'exigences MSS v0.2 : 5 retours reçus : 3 du couloir Hôpital, 2du couloir MDV
  - Via l'itération 1 des REM des TF

  => Le terme « client de messagerie MSSanté » entraine une confusion avec la notion d'IHM de client de messagerie

- **20 octobre :** Publication sur mssante.fr du :
  - CR de l'atelier #5 avec la réponse aux questions posées en séance
  - Référentiel d'exigences v0.3 comportant :
    - les réponses aux remarques éditeurs (colonne AT),
    - les exigences modifiées (en rouge)

Segur – Macro planning MSSanté



I - Modifications apportées aux exigences v0.3

3 natures d'exigences définies dans le Référentiel #2

Exigences générales

Exigences applicables à tous les LPS quel que soit le couloir :

- 5 exigences API LPS communes aux 3 types de BAL
- 3 exigences indicateurs
- 4 autres exigences : MES, traces, encodage
- + exigences vague 1 adaptées aux évolutions vague 2

Exigences spécifiques BAL PER & ORG

Voir profil « BAL PER & ORG » dans l'Excel :

- 5 exigences MIE PSC (1.6 à 1.10)
- 12 exigences « expérience utilisateurs » pour les LPS proposant une IHM avec arborescence de BAL

ou / et

Exigences spécifiques BAL APP

Voir profil « BAL APP» dans l'Excel :

- 1 exigence MIE certificat ORG_AUTH_CLI (1.11)

Remarque

Il est toutefois possible d'utiliser **en complément** une interface propriétaire (conforme avec référentiel identification électronique de la PGSSI-S et aux guides de l'ANSSI en termes de sécurisation du canal d'échange) principalement dans un contexte où le MIE PSC n'est pas adapté (établissements…)

Exigences du référentiel #2 : Modifications (1/2)

Bloc	Nature de l'exigence	N° exigence temporaire	Enoncé de l'exigence (DOIT) ou de la préconisation (PEUT)	Verbatim explicatif à reprendre dans le Référentiel #2 v1.0
API LPS	EXIGENCE	1.2	Le système DOIT uniquement utiliser l'une des suites de chiffrement suivantes, lors de la négociation TLS pour établir une connexion avec l'API LPS d'un système de messagerie : • 0xC030: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • 0xC02F: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • 0xC028: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • 0xC027: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • 0x009F: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • 0x009E: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 Durant l'établissement de la connexion TLS, la longueur du groupe DH utilisé DOIT être >= 2048 bits ou >= 256 bits en cas d'utilisation du groupe elliptique ECDH. ~~La confidentialité persistante (PFS - perfect foward secrecy) de DH doit être utilisée (DHE ou ECDHE).~~ Dans le cas contraire, la connexion ne doit pas être établie.	Le service de messagerie MSSanté doit refuser cette connexion si cette exigence n'est pas respectée. Cette exigence s'appuie sur les recommandations TLS de l'ANSSI : https://www.ssi.gouv.fr/uploads/2020/03/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf
API LPS	EXIGENCE	1.5	Le système DOIT disposer d'une interface d'accès ~~de consultation de~~ aux BAL utilisant le protocole IMAP 4 rev1 ou rev2 avec STARTTLS conformes respectivement à la RFC 3501 ou RFC 9051.	Rappel de l'exigence imposée aux opérateurs dans le Ref#1 : "Tout service de messagerie MSSanté a l'obligation de proposer sur l'API LPS une interface IMAP conforme à la RFC 3501 ou RFC 9051 sur le port 143".
Autres interfaces	~~RECOMMANDATION~~ REMARQUE	1.12	En complément de l'API LPS, le système PEUT se connecter à un service de messagerie MSSanté exposant des interfaces propriétaires, dans la mesure où ces dernières sont conformes avec le référentiel d'identification électronique de la PGSSI-S et à l'état de l'art en termes de sécurisation des flux de données.	Guides ANSSI : https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf https://www.ssi.gouv.fr/uploads/2020/03/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf
Indicateurs	EXIGENCE	2.1	Le système DOIT positionner l'entête SMTP "X-MSS-INS" dans un message envoyé qui comporte en PJ un document de santé CDA encapsulé dans une archive IHE_XDM. La valeur de cet entete DOIT être : - 'O' (Oui) en cas de présence d'une Identité Nationale de Santé (INS qualifiée")* dans une archive IHE_XDM. - 'N' (Non) en cas d'absence d'une Identité Nationale de Santé "INS qualifiée"* dans une archive IHE_XDM, En cas d'absence en PJ d'un document de santé CDA encapsulé dans une archive IHE_XDM, l'entête ne doit pas être positionnée. * INS qualifiée au sens du §5.3.3 du Référentiel Identifiant National de Santé v2.0. La présence d'une INS qualifiée est caractérisée par la présence de l'INS (matricule, OID) et des 4 traits d'identité suivants dans l'entete CDA : nom de naissance, 1er prenom, date de naissance et sexe	Pour rappel, l'échange de données de santé via MSSanté sans Identité Nationale de Santé (qualifiée) est possible. C'est notamment le cas des patients pour lesquels le professionnel n'aura pas pu qualifier l'INS ou bien lorsque le patient n'en dispose pas. Le matricule INS et l'OID sont alors absents, et seuls les traits nom de naissance, 1er prénom de naissance, date de naissance et sexe sont transmis. L'objectif est de pouvoir suivre le déploiement de l'INS dans les échanges MSSanté et de déterminer la part des messages contenant une INS qualifiée. Exemple : X-MSS-INS = O X-MSS-INS = N

Nature des modifications :

- 1.2 : Précisions pour clarifier la partie échanges de clés
- 1.5 : Cette exigence API LPS n'impose en rien aux LPS d'implémenter une IHM de consultation de message.
- 1.12 : Ne sera pas présentée dans le référentiel comme une recommandation, mais comme une remarque
- 2.1 : Précisions apportées pour décrire les cas de CDA sans INS

Exigences du référentiel #2 : Modifications (2/2)

Bloc	Nature de l'exigence	N° exigence temporaire	Enoncé de l'exigence (DOIT) ou de la préconisation (PEUT)	Verbatim explicatif à reprendre dans le Référentiel #2 v1.0
Indicateurs	EXIGENCE	2.2	Le système DOIT positionner un entête SMTP "X-MSS-CODECDA" dans un message envoyé qui comporte en PJ un document de santé CDA encapsulé dans une archive IHE_XDM. La valeur de cet entete DOIT être égale à celle du champ code** présent dans l'entête du document CDA. En cas de présence de plusieurs documents CDA, l'entête sera multi-valeurs. En cas d'absence en PJ d'un document de santé CDA encapsulé dans une archive IHE_XDM, l'entête ne doit pas être positionné	* définition document structuré dans le « Volet Structuration Minimale de Documents de Santé – CI-SIS Juin 2021, §1 » ** code défini dans le « Volet Structuration Minimale de Documents de Santé – CI-SIS Juin 2021, §3.5.5.5 » Exemple : X-MSS-CODECDA = 34112-3 X-MSS-CODECDA = 34112-3,PRESC-BIO,15508-5
Securité	EXIGENCE	4.2	Le système DOIT générer des traces fonctionnelles pour toutes les traitements opérés (envoi, consultation, suppression...) sur les BAL MSSanté et leur contenu. Ces traces doivent être conservée pendant une durée de 6 mois	Les traces fonctionnelles sont les traces des actions réalisées par tout utilisateur professionnel ou processus automatisé. Il n'est pas demandé que les traces soient accessibles aux professionnels. Elles doivent par contre pouvoir être accessibles aux équipes de support de l'éditeur
Securité	EXIGENCE	4.3	Chaque action tracée DOIT préciser : - le type d'action - l'identifiant de son auteur dûment authentifié ~~(ou les informations permettant de la déterminer indirectement)~~ - horodatage locale du poste, - ~~le contenu de~~ la demande effectuée sur le serveur de messagerie MSSanté - la réponse fournie par ce dernier (y compris en cas d'échec) ~~- plus généralement toute information utile à la recherche des causes et des effets d'un incident et à la constitution d'un faisceau de preuve.~~	Les traces fonctionnelles de doivent pas contenir de données de santé à caractère personnel. Le contenu des messages eux-mêmes n'est pas tracé

Nature des modifications :

- 2.2 : Précision sur la nature du contrôle à effectuer
- 4.2 : Précision de la durée de conservation attendue
- 4.3 : Simplification des données attendues

Exigences «expérience utilisateur » : Modifications

Section	Bloc	Nature de l'exigence	N° exigence temporaire	Enoncé de l'exigence (DOIT) ou de la préconisation (PEUT)	Verbatim explicatif à reprendre dans le Référentiel #2 v1.0
Échanges via MS-Santé	Accusé de lecture	EXIGENCE	3.11	Le système DOIT permettre de demander au destinataire un accusé de lecture (MDN) lors de l'émission de tous les courriels.	Le référentiel comporte déjà une exigence sur l'envoi de l'accusé de réception Remplace la recommendation ECO.2.3.2 RFC 8098
Échanges via MS-Santé	Accusé de lecture	EXIGENCE	3.12	Le système DOIT savoir retourner un accusé de lecture (MDN) lorsque qu'un message recu le demande,	La modalité de validation de la lecture est laissé à l'appreciation de l'éditeur RFC 8098 MES supporte deja cette fonctionnalité

Nature des modifications :

- Rappel : Demande d'accusé de réception déjà imposée en vague 1
- 3.11 & 3.12 : Propositions suite à vos retours, pour les LPS accédant à des BAL PER et ORG uniquement :
  - Savoir traiter des accusés de lecture
  - La gestion des accusés de bonnes intégration seront réétudiés dans une prochaine version du référentiel #2

MSSanté
Système de messageries sécurisées, données protégées.

Questions / réponses

II Focus sur certaines exigences à finaliser

Exigences à finaliser

Bloc	Nature de l'exigence	N° exigence temporaire	Enoncé de l'exigence (DOIT) ou de la préconisation (PEUT)	Verbatim explicatif à reprendre dans le Référentiel #2 v1.0
Emission de message	EXIGENCE	3.8	Le système DOIT indiquer à l'utilisateur lorsque le message émis n'a pas pu être délivré au destinataire, ainsi que le motif de l'échec.	Rappeler le comportement de MES en cas de MES inexistant ou cloturé Faisabilité de rapprocher le message de non distribution au message envoyé à vérifier
Accusé de lecture	EXIGENCE	3.13	Le système DOIT rapprocher les accusés de réception et de lecture retournés par les destinataires des messages émis correspondants,	
Indicateurs	EXIGENCE	2.3	Le système DOIT positionner l'entête SMTP "X-MSS-NIL" dans tous les mails envoyés. Elle sera renseignée du numéro d'identification logiciel attribué lors du référencement ségur de la solution logiciel qui a produit le message SMTP.	

Statut / Points à préciser

- 3.8 et 3.13 : la faisabilité d'exploiter les ID de message pour faire les rapprochements demandés n'est pas encore validée. Avez-vous déjà vu ce genre de mécanisme ?
- 2.3 : l'identifiant à confirmer : probablement identifiant de candidature vague 2 (format 10 caractères en majuscules)

=> propositions à faire pour la concertation publique

- La dérogation vague 1 permettant d'écrire à un patient sans INS qualifié s'achève à fin 2022

=> Nouvelle formulation et nouvelle date d'échéance en cours de rédaction

MSSanté
Système de messageries sécurisées, données protégées.

Questions / réponses

III Suite des travaux

Conclusion

Prochaines étapes :

- **7 novembre :** Publication itération 3 des REM TF
  - Comprendra les exigences MSSanté dans l'état du référentiel d'exigences v0.3 MSSanté publié le 20/10/22
- **2eme quinzaine de novembre** : Concertation publique de la version rédigée du Référentiel #2 v1.0
  - Concertation ouverte sur 2 semaines uniquement, compte tenu des concertations faites en ateliers
- **Mi décembre** : Publication de la version finale du Référentiel #2 v1.0
  - Doit intervenir avant la prépublication des REM vague 2
- **T1 2023** : Mise à disposition d'un outillage de test/référence des exigences API LPS
  - Calendrier en cours de définition : objectif ouverture pilote fin janvier

Merci pour votre participation !

MSSanté

Système de messageries sécurisées,
données protégées.

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ