MS Santé
Système de messageries sécurisées, données protégées.

Segur vague 2

Concertation exigences MSSanté

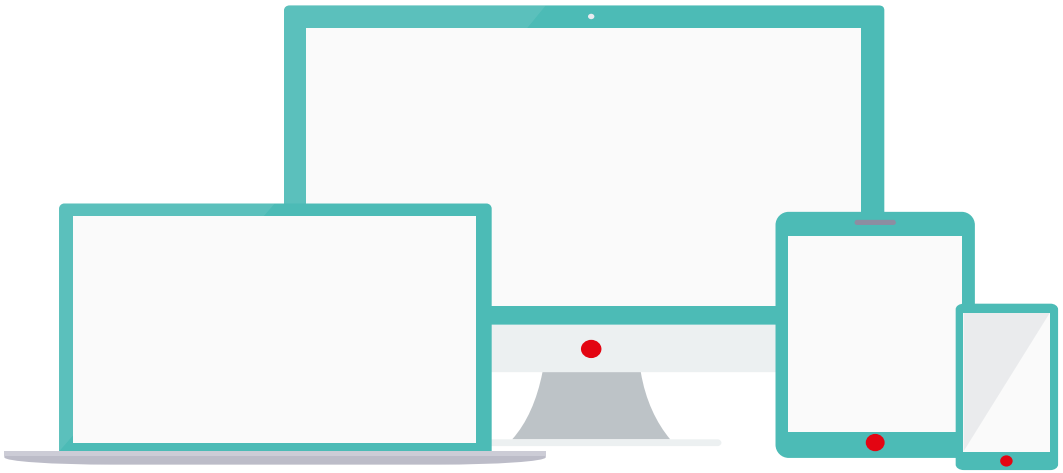
Atelier Editeurs #4 du 08/07/2022

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

MSSanté
Système de messageries sécurisées, données protégées.

Introduction

Intervenants et organisateurs

Gestion de l'Espace de Confiance MSSanté
Edouard BRIS

Gestion de l'Espace de Confiance MSSanté
Mike GUEYE

Gestion de l'Espace de Confiance MSSanté
Adrien COSME

Annuaire Santé

Alexis BREITHOFF

Architecte applicatif MSSanté
Régis MAUGET

Messagerie Mon Espace Santé
Philippe DECLERCQ (CNAM)

Pro Santé Connect

Joachim METZGER

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

I Retours sur certaines questions posées en atelier 3

Retour sur certaines questions posées en atelier #3

Le CR de l'atelier 3 (www.mssante.fr/chantiers-segur) contient 12 questions/réponses, posées en séance ou a posteriori, regroupées par thème :

- Q#51 : MES : La BAL patient existe dès l'autocréation de MES (ou création explicite)

- Q#52 : MES : En cas d'autocréation, le patient ne recevra des notifications à l'arrivée de nouveaux messages dans sa BAL si la CNAM ne disposait pas déjà dans ses systèmes d'une adresse de contact valide. Par contre, un **courrier papier récapitulatif** sera adressé à une fréquence à définir.

II Prise en compte des remarques éditeurs sur synthèse exigences v0.1

Retours provenant de 6 éditeurs

Exigences API LPS : Choix des types de BAL / MIE à implémenter

Remarques éditeurs :

PROFIL	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	Statut exigence	Remarques / Réponses des l'éditeurs
Général	EXIGENCE	1.6	Le système DOIT réaliser des demande d'ouverture de connexion SMTP et IMAP sur l'interface BAL personnelle ou organisationnelle de l'API LPS d'un service de messagerie MSSanté en respectant la cinématique suivante : 1- Ouvrir la session TLS avec STARTTLS comme défini dans les RFC 3207 et RFC 2246 2- Réaliser une authentification du professionnel via le mécanisme SASL OAuth 2.0, en envoyant le mot clé AUTHENTICATE XOAUTH2 pour IMAP ou AUTH XOAUTH2 pour SMTP + chaine de caractères encodée en base64 contenant à la fois l'adresse de la BAL dans le champ « user » et l'Access Token au format JWT 3- Attendre la validation de la connexion IMAP ou SMTP par le service de messagerie MSSanté utilisé 4- Envoyer les commandes SMTP ou IMAP	Pré-requis : après authentification du professionnel, le système a obtenu un Access Token Pro Santé Connect valide, via un flux d'authentification redirection ou CIBA.	Ajoutée v0.1	Editeur #2 : Sommes-nous dans l'obligation d'implémenter tous les domaines en termes de BAL ? Est ce que la bal applicative est suffisante? Editeur #4 : Non Applicable tel que rédigé aux Systèmes du couloir Hôpital qui n'accèdent en SMTP ou IMAP qu'à des boites aux lettres APPLICATIVES. Il devrait être possible à un Système de n'accéder qu'à des BAL Applicatives. Editeur #5 : Nous passons par une BàL applicative. Editeur #5 : Il faut aussi sécuriser le canal système <-> PFI quand la PFI est client de messagerie.

Proposition ANS

L'éditeur doit être conforme à l'interface BAL APP (MIE auth_cli) ou à l'interface BAL PER/ORG (MIE PSC)

Exigences #1.1 à 1.12 : Interface API LPS et PFI

Remarques éditeurs :

Les éditeurs qui passent par une PFI ne peuvent pas répondre aux exigences de l'API LPS

Les PFI pourront-elles proposer des interfaces BAL PER/ORG basées sur PSC ?

Proposition ANS

Quels sont les couloirs concernés : Hôpital, MS, BIO ?

Introduire un profil « client MSSanté » ?

Exigence #1.7 & 1.10 : Gestion des erreurs

Remarques éditeurs :

PROFIL	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	Statut exigence	Remarques / Réponses des l'éditeurs
Général	EXIGENCE	1.7	Le système DOIT traiter les erreurs techniques rencontrées lors du processus de connexion SMTP/IMAP ~~sans empêcher le professionnel de continuer à utiliser nominalement le système~~ de sorte à ce qu'elles ne perturbent pas les autres fonctions du système (hors messagerie).	Le service de messagerie peut par exemple retourner les erreurs suivantes lors de la connexion : - Pour IMAP : réponse NO Authentication failed, conformément au RFC 5530 (https://datatracker.ietf.org/doc/html/rfc5530#section-3) - Pour SMTP : réponse 535 5.7.8 Authentication credentials invalid code, conforément au RFC 4954 (https://datatracker.ietf.org/doc/html/rfc4954#section-6)	Modifiée v0.2	Editeur #4 : Non Applicable tel que rédigé aux Systèmes du couloir Hôpital où aucun utilisateur n'utilise le Système, ce sont des applications. Editeur #6 :Qu'entendez-vous par utiliser nominalement le système car si il est impossible de se connecter au serveur MSS il sera impossible de lui présenter ses messages par exemple ?
Général	EXIGENCE	1.10	Le système DOIT pouvoir réouvrir automatiquement (i.e. sans intervention humaine) une session IMAP ou SMTP lors de la détection d'une fin de session IMAP ou SMTP déclenchée par le service de messagerie MSSanté (causes possibles : inactivité du LPS/DUI, durée maximale de session SMTP/IMAP) ~~sans empêcher le professionnel de continuer à utiliser nominalement le système.~~	~~Cad sans interruption utilisateur.~~ Le système peut par exemple reouvrir une session IMAP/SMTP avec un Access Token valide, quitte à redemander une nouvelle connexion PSC	Modifiée v0.2	Editeur #5 : Nous passons par une BàL applicative.

Proposition ANS

Proposition de reformulations en rouge ci-dessus

Exigence #1.2 : Suites de chiffres TLS

Remarques éditeurs :

N° exigence (temporaire)	Enoncé de l'exigence (DOIT) ou de la préconisation (PEUT)	Verbatim explicatif à reprendre dans le Référentiel #2 v1.0	Statut exigence	Remarques / Réponses des l'éditeurs
1.2	Le système DOIT uniquement utiliser l'une des suites de chiffrement suivantes, lors de la négociation TLS 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 La longueur du groupe DH doit être >= 2048 bits ou la longueur du groupe elliptique ECDH doit être >= 256 bits. La confidentialité persistante (PFS - perfect foward secrecy) de DH doit être utilisée (DHE ou ECDHE).	Le service de messagerie MSSanté doit refuser cette connexion si cette exigence n'est pas respecté.	Ajoutée v0.1	Editeur #3 : Ne serait-ce pas aux opérateurs de ne gérer côté serveur que ces 6 suites de chiffrement avec les caractéristiques DH/ECDH/PFS ? Une exigence côté LPS pourrait être alors: être en mesure d'établir une connexion sécurisée avec les serveurs de l'opérateur dont voici les caractéristiques: suite de chiffrement, ... Editeur #5 : Ces ciphers suite sont bien utilisées dans notre socle.

Proposition ANS

Compte tenu du nombre important d'opérateurs et des potentielles non conformités, il est souhaitable que cette exigence sur les suites de chiffrement soit portée à la fois par les opérateurs, mais aussi par les éditeurs.

Exigence #1.3 : Auto-configuration

Remarques éditeurs :

PROFIL	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	Statut exigence	Remarques / Réponses des l'éditeurs
BAL PER ORG	~~RECOMMANDATION~~ EXIGENCE	1.3	Le système PEUT proposer à ses utilisateurs une fonctionalité d'autoconfiguration de BAL soit lors de la configration de la BAL, soit à la demande : 1 – A partir de l'adresse de la BAL à configurer, consulter l'URL d'autoconfiguration du système de messagerie MSSanté 2 – Configurer automatiquement les paramètres de configuration spécifiques à l'API LPS du système de messagerie MSSanté proposant la BAL 3 – Procéder à un test de connexion pour validation la configuration	Tout service de messagerie MSSanté a l'obligation de proposer sur l'API LPS une URL (https://autoconfig.<emailaddressdomain>/mail/config-v1.1.xml) permettant d'utiliser un mécanisme d'auto-configuration des BAL, avec un format conforme au ConfigFileFormat (cf. https://wiki.mozilla.org/Thunderbird:Autoconfiguration:ConfigFileFormat) décrivant les configuration des 2 points d'entrée de l'API LPS (BAL personnelles et organisationnelles, BAL applicatives).	Modifiée v0.2	Editeur #5 : Ok pour une recommandation. Editeur #5 : Cette exigence a un sens si le système accède à des BALs personnelles et organisationnelles (il propose une IHM pour consulter/envoyer des mails). Si le système n'accède qu'à des BALs applicative, il n'y a qu'une configuration de BAL à réaliser (manuellement).

Proposition ANS

Proposition de passer en exigence pour les système qui s'interfacent avec des BAL PER ou ORG, mais optionnel pour les BAL APP via l'introduction d'un profil « BAL PER ORG »

Exigence #2.3 : Indicateurs

Remarques éditeurs :

PROFIL	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	Statut exigence	Remarques / Réponses des éditeurs	Réponse ANS
Général	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 (NIL*) de la ~~**brique**~~ **solution** logiciel qui a produit le message SMTP.	* NIL obtenu auprès du CNDA (Centre National de Dépôt et d'Agrément de l'Assurance Maladie) Exemple 1 : X-MSS-NIL = AAAAAAAA Exemple 2 : la solution logiciel **S01** de l'éditeur **ANO** utilise dans son architecture 3 briques techniques (**B01, B02 & B03**) développées par l'éditeur **NYME**. La brique **B02** est celle qui fournit la fonction MSSanté. Dans ce cas de figure c'est bien le **NIL** du logiciel **S01** qui devra être positionné dans l'entête **X-MSS-NIL**	Ajoutée v0.1	Editeur #2 : Nous avons consulté le site du CNDA et les différents protocoles proposés, et sauf erreur de notre part nous n'avons pas trouvé de protocole permettant d'obtenir un numéro de logiciel NIL pour la MSSANTE, pouvez nous détailler la méthode pour obtenir ce numéro pour nos différentes solutions ?	Effectivement, la MSSanté ne porte pas à date de certification auprès du CNDA. La cible n'étant pas une certification mais plutôt une identification unique par logiciel. La possibilité d'identification par la plateforme convergence est également instruite

Proposition ANS

Exigence #2.3 : Indicateurs

Remarques éditeurs :

PROFIL	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	Statut exigence	Remarques / Réponses des éditeurs	Réponse ANS
Général	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 (NIL*) de la ~~**brique**~~ **solution** logiciel qui a produit le message SMTP.	* NIL obtenu auprès du CNDA (Centre National de Dépôt et d'Agrément de l'Assurance Maladie) Exemple 1 : X-MSS-NIL = AAAAAAAA Exemple 2 : la solution logiciel **S01** de l'éditeur **ANO** utilise dans son architecture 3 briques techniques (**B01, B02 & B03**) développées par l'éditeur **NYME**. La brique **B02** est celle qui fournit la fonction MSSanté. Dans ce cas de figure c'est bien le **NIL** du logiciel **S01** qui devra être positionné dans l'entête **X-MSS-NIL**	Ajoutée v0.1	Editeur #4 : Tous les Systèmes Clients de Messagerie n'auront pas toujours un NIL puisque l'obtention du NIL est obtenu suite à une certification auprès du CNDA. Or un logiciel pourrait être client de messagerie, mais sans avoir eu de certification auprès du CNDA qui portent sur des sujets hors MSSanté. Il faudrait autoriser les éditeurs à obtenir des NIL auprès du CNDA même pour des logiciels qui n'ont pas de certification CNDA à passer.	Ce sujet est en cours d'instruction. La cible est de pouvoir identifier tout logiciel qui fait de la MSSanté sans adhérence avec les autres besoins de certification

Proposition ANS

MS Santé
Système de messageries sécurisées, données protégées.

Questions / réponses

III Exigences candidates à instruire :

- Communes aux TF
- Spécifiques à des TF

Exigences candidates : Fonctionnalités LPS/DUI

Interdire réponse patient/usager :

- **Objectif :** remplacer le dispositif pilote basé sur un email avec comme objet le texte « FIN »
- **Proposition :** Dans les messages envoyés vers Mon espace santé, le système PEUT positionner une entête SMTP "X-MSS-MES". Lorsque la valeur de cet entête sera égale à « FIN » (3 caractères en majuscules), Mon Espace Santé empêchera l'usager de répondre au message reçu. L'usager ne pourra plus contacter par messagerie le Professionnel émetteur du message. L'usager retrouvera la possibilité de contacter le Professionnel dès lors que ce dernier lui aura envoyé un nouveau message sans l'entête "X-MSS-MES" valorisée à "FIN".

Ecrire à un patient/usager à partir de la base patient/usager du LPS/DUI

- **Objectif :** simplifier pour un utilisateur professionnel la génération du champ To: d'un nouveau message à partir des données patient disponibles
- **Question :** comment cibler les LPS/DUI concernés ?

Rechercher un destinataire professionnel à qui écrire

- **Objectif :** Permettre à un utilisateur professionnel de rechercher dans l'annuaire santé un professionnel ou une structure disposant d'une BAL MSSanté
- **Questions :** Comment cibler les LPS/DUI concernés ? Quels critères de recherche retenir ? Quelle interface annuaire utiliser ?

Exigences candidates : Fonctionnalités LPS/DUI

Configurer plusieurs BAL MSSanté :

- **Objectif :** Permettre à un professionnel d'accéder à plusieurs BAL MSSanté depuis son LPS/DUI. Par exemple, une BAL PER et une BAL ORG.
- **Question :** Comment cibler les LPS/DUI concernés ? Combien de BALs ?

Supprimer les messages « traités » de la BAL :

- **Objectif :** En l'absence d'annuaire patient MES, imposer la récupération et l'affichage au professionnel :
  - Conformité CNIL : la messagerie MSSanté n'est pas un lieu de stockage « long terme » des données de santé
  - Limiter la tailler des BAL
- **Proposition :** Utiliser les comptes rendu de bonne intégration dans le système cible du CI-SIS ?

Exigences candidates : Ergonomie – Affichage des messages

Distinguer dans la boite de réception les messages émis par des professionnels et des patients

- **Objectif :** Faciliter le travail de l'utilisateur professionnel dans la gestion de ses BAL
- **Question :** Comment atteindre l'objectif sans contraindre les éditeurs et rendre l'exigence vérifiable ?

Afficher les informations patients depuis un message patient recu :

- **Objectif :** En l'absence d'annuaire patient MES, imposer la récupération et l'affichage au professionnel :
  - du libellé du champs From: positionné par MES
  - De l'INS contenu dans l'adresse email @patient.mssante.fr
- **Question :** comment cibler les LPS/DUI concernés ?

Exigences candidates : Ergonomie – Affichage des messages

Simplifier l'affichage des objets des messages contenant des documents structurés

- **Objectif :** Rendre plus lisible les objets des messages avec PJ structurées reçus par les professionnels
- **Questions :** Comment cibler les LPS/DUI concernés ?

Afficher les messages en mode conversation

- **Objectif :** Proposer à l'utilisateur professionnel la possibilité d'afficher ses messages en mode conversation
- **Question :** Comment cibler les LPS/DUI concernés ?

Exigences candidates : Identifiants BAL APP

Définir des règles permettant de choisir l'identifiant BAL APP à utiliser

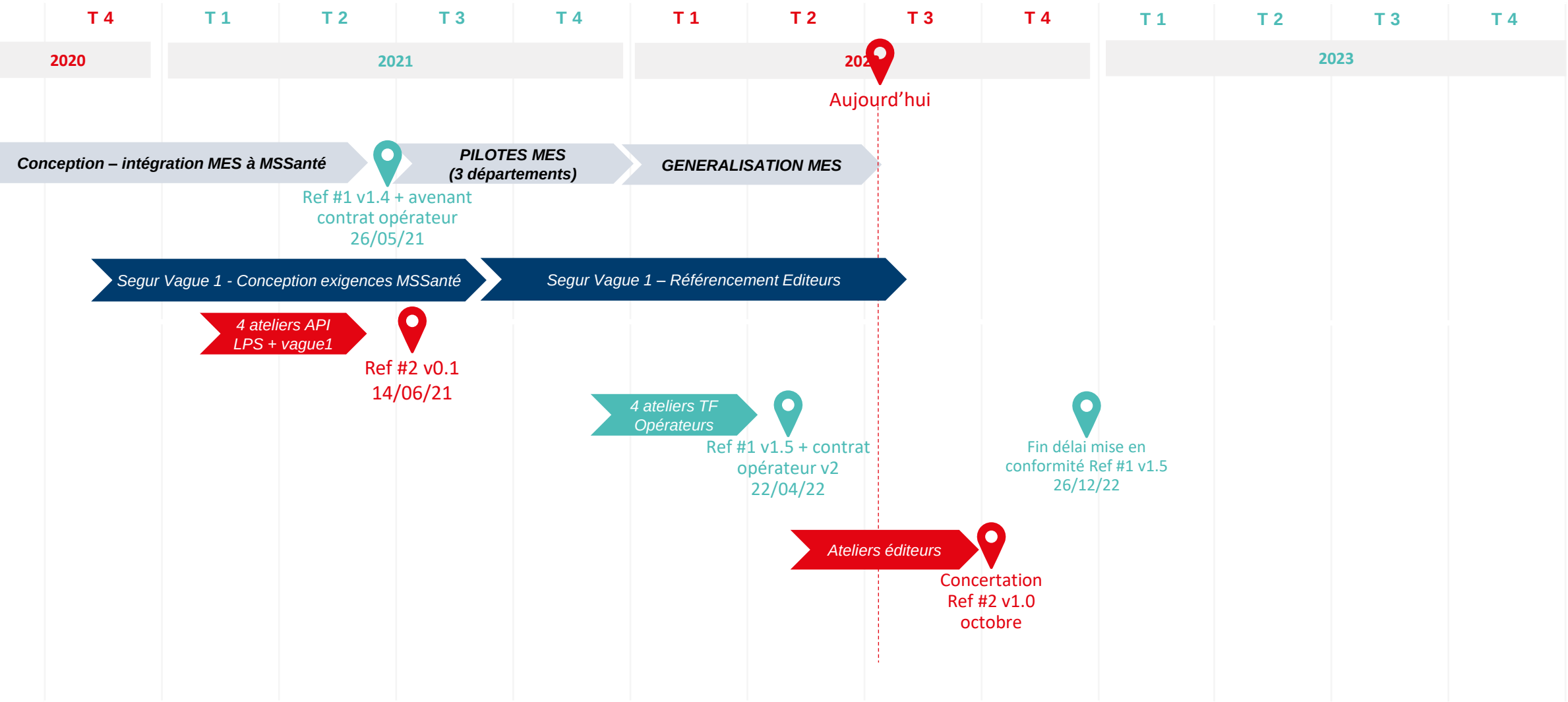
- **Contexte :** Un identifiant de structure (FINESS EG/EJ) est utilisé :
  - Dans le certificat qui sert à se connecter à la BAL APP, et potentiellement à d'autres services nationaux
  - Pour rattacher la BAL APP à une structure de l'annuaire santé. Cette information est utilisée pour remonter les statistiques d'usage et donc de financement (ROSP, …)
- **Objectif :** Clarifier le choix et l'usage de ces identifiants de structures dans les certificats et lors de la création des BAL APP

MS Santé
Système de messageries sécurisées, données protégées.

Questions / réponses

IV Suite des travaux

Segur – Macro planning pour MSSanté



Conclusion

Prochaines étapes :

- **Semaine du 18 juillet** : Diffusion CR atelier #4 et draft d'exigences Ref#2 v0.2
- **D'ici septembre :** Travaux avec les TF sur les exigences MSS spécifiques aux TF
- **Semaine du 12 septembre** : Diffusion draft d'exigences Ref#2 v0.3
- **Vendredi 23 septembre 15h** : Atelier #5
  - Echange sur vos retours de concertation du draft d'exigences v0.3
  - Dernier atelier avant concertation publique
- **Semaine du 10 octobre** : Concertation publique

Merci pour votre participation !

MS Santé

Système de messageries sécurisées,
données protégées.

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ