MSSanté
Système de messageries sécurisées, données protégées.

Segur vague 2

Concertation exigences MSSanté

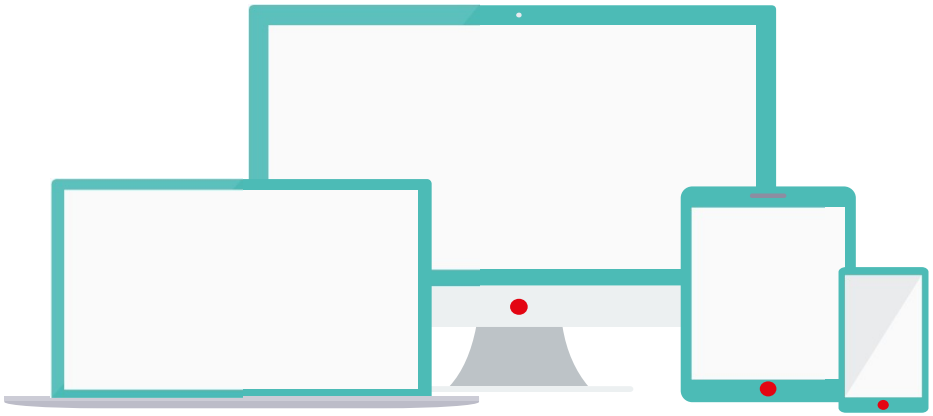
Atelier Editeurs #5 du 23/09/2022

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 :

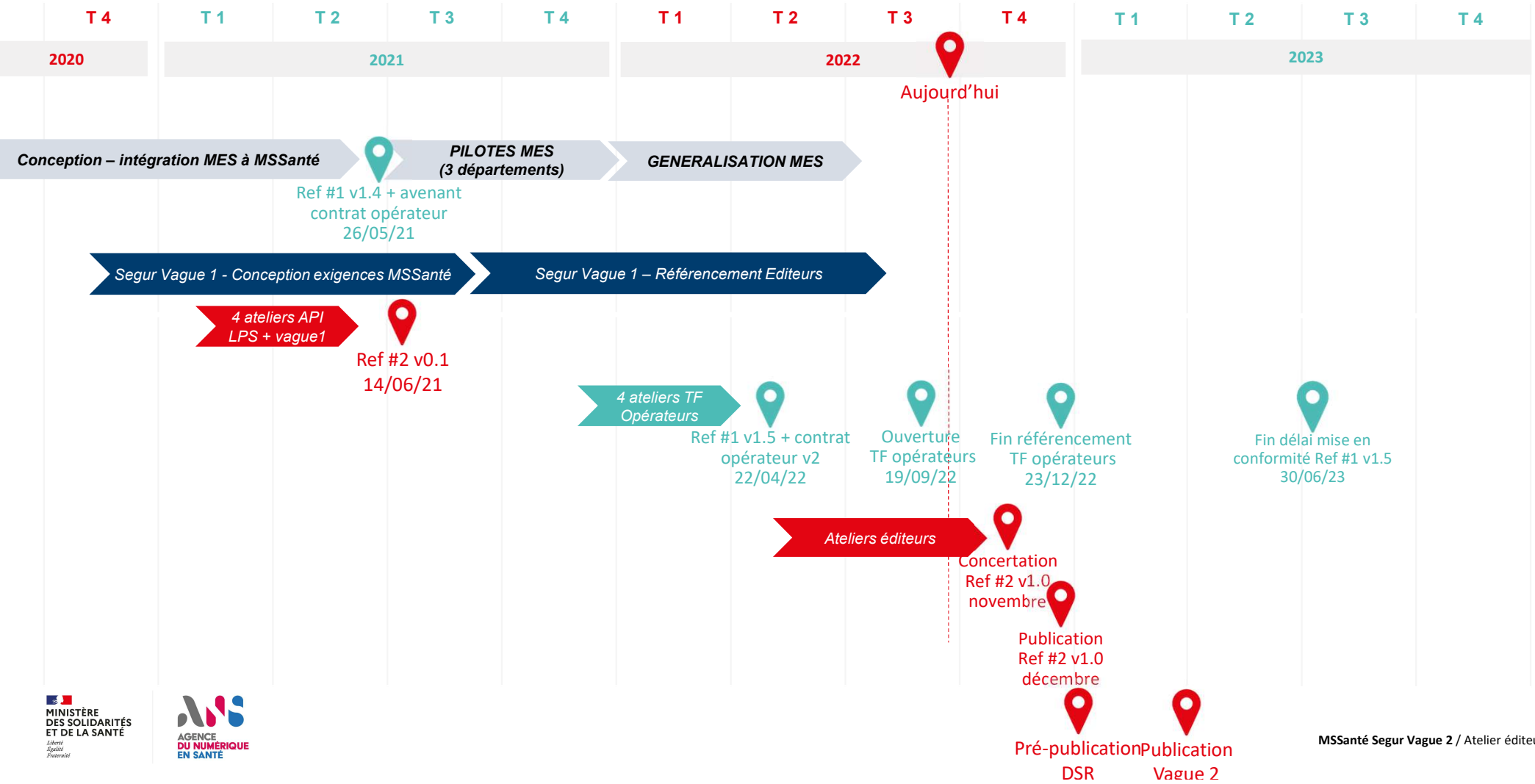
- L'API LPS
- Les modalités d'échange avec la messagerie de MES
- Les indicateurs Ségur à remonter à l'ANS sur le contenu des messages envoyés
- Les modalités de consultation de l'annuaire santé
- Autres sujets proposés par les éditeurs …

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

Segur – Macro planning MSSanté



II - Retours sur certaines questions posées en atelier 4

Retour sur certaines questions posées en atelier #4

Le CR de l'atelier 4 (mssante.fr/chantiers-segur) contient 14 questions/réponses, posées en séance ou a posteriori, regroupées par thème :

- Q#68 : **Format CDA** pas obligatoire en entrée de PFI -> problématique pour produire les indicateurs
- Q#72 : **Environnement de test éditeurs pour l'API LPS** = environnement de référence quelque soit le ou les opérateurs avec lesquels un LPS s'interface généralement

III - Modifications apportées aux exigences v0.2

Exigences du référentiel #2 : Modifications

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	Statut exigence
API LPS	EXIGENCE	1.1	Le système DOIT savoir établir une connexion avec l'API LPS d'un système de messagerie MSSanté en utilisant la version TLS 1.2 (RFC 5246) ~~ou une version ultérieure de TLS (1.3...)~~.	Un service de messagerie MSSanté (opérateur) accepte obligatoirement les connexions TLS 1.2. Le service de messagerie MSSanté doit refuser cette connexion la version de TLS est inférieur à 1.2.	Revue v0.2
API LPS	RECOMMENDATION	1.1.1	Le système PEUT établir une connexion avec l'API LPS d'un système de messagerie MSSanté en utilisant a minima la version TLS 1.2 (RFC 5246) ou une version ultérieure de TLS (1.3...).	Un service de messagerie MSSanté (opérateur) peut accepter les connexions en TLS 1.3 au supérieure.	Ajoutée v0.2
API LPS	EXIGENCE	1.3	Le système DOIT 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
API LPS	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
API LPS	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 et/ou renouvellement de l'Acces Token via le Refresh Token ?	Modifiée v0.2

Questions ANS :

- 1.1 : Ajout d'une recommandation pour TLS 1.3, afin de rendre obligatoire TLS 1.2
- 1.3 : Rendue obligatoire, sauf si le LPS ne propose que l'interface avec les BAL applicatives
- 1.7, 1.10 : Reformulations suite à vos remarques

Exigences du référentiel #2: Ajouts

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
MES	EXIGENCE	3.7	Le système DOIT pouvoir positionner un entête SMTP "X-MSS-MES", dans les messages envoyés vers un patient (Mon espace santé), avec la valeur "FIN" (3 caractères en majuscules), lorsque le professionnel émetteur ne souhaite pas que le patient puisse lui répondre en retour.	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-FIN" valorisée à "FIN". Ne pas envoyer imédiatement un message contenant des données médicales, suivi d'un message de FIN, au risque de bloquer la réception du premier message Un message de FIN envoyé sans finalité de transmettre des données de santé devra contenir un objet et un corps de message expliquant au passant que l'émetteur met fin à l'échange.
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.	Les traces fonctionnelles sont les traces des actions réalisées par tout utilisateur professionnel ou processus automatisé. Durée de rétention à préciser
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 et 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
Interropérabilité	EXIGENCE	4.4	Le système DOIT utiliser un encodage UTF-8 pour tous les messages envoyés	Complète la recommandation ECO 2.2.3 du référentiel #2 v0.1 qui ne portait que sur l'encodage de la partie text du message
Annuaire santé	EXIGENCE	4.5	Lors de la production d'un message, avant envoi, le système DOIT proposer à l'utilisateur une fonctionalité permettrant de rechercher l'adresse d'un professionnel dans l'Annuaire Santé	Présenter les différentes méthode possible : extraction publique, LDAP, FHIR, en précisant que la cible est FHIR et que autres méthodes ont vocation à terme à être décomissionnée, aucune date n'étant définie actuellement

Questions ANS :

- 4.2, 4.3 : Des exigences relatives aux traces portent-elles déjà sur les éditeurs de LPS ?
- 4.3 : Disposez-vous de bonnes pratiques à appliquer sur l'encodage des messages lors du transport
- 4.5 : existe-t-il des contextes où cette exigence ne serait pas applicable ?

Exigences/recommandations MSS «expérience utilisateur »

Bloc	Fonction	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
Consultation message	Type d'émetteur	EXIGENCE	3.3	Si le système propose une IHM présentant des messages recus, cette dernière DOIT distinguer les messages émis par des professionnels, des messages émis par des patients via MES.	Cette distinction doit être plus immédiate que la consultation du nom de domaine. Mettre en avant la distinction utilisée dans les preuves	Ajoutée v0.2
Consultation message	Ergonomie	RECOMMANDATION	3.4	Si le système propose une IHM présentant des messages recus, cette dernière PEUT proposer d'utiliser un mode d'affichage sous forme de conversation	La vague 1 impose aux LPS de positionner des ID de message nécessaires à cette fonctionalité "conversation". -> débat avec éditeurs (atelier 5) si on connait la source	Ajoutée v0.2
Consultation message	Ergonomie	RECOMMANDATION	3.5	Si le système propose une IHM présentant des messages recus, le système PEUT proposer plusieurs modes de tri des messages		Ajoutée v0.2
Consultation message	Ergonomie	EXIGENCE	3.6	Si le système propose une IHM présentant des messages recus, cette dernière DOIT masquer au professionnel le préfixe "XDM/1.0/DDM+" de l'objet des messages recus contenant un document structuré	Le préfixe d'un message structuré n'est pas compréhensible par un profession. Utile uniquement dans le cas d'un traitement automatisé du message par un LPS	Ajoutée v0.2
Emission de message	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	Ajoutée v0.2
MES	Reception de message	EXIGENCE	3.9	Si le système propose une IHM présentant des messages recus, un message recu d'un patient (Mon Espace Santé) DOIT être affiché en utilisant les nom, prenom et le matricule INS du patient, et pas uniquement l'adresse email INS@patient.mssante.fr	Ne disposant pas d'annuaire national des patients, le système doit afficher le nom et le prénom du patient tel que transmis par MES dans le libellé From , et extraire l'INS de l'adresse émettrice du patient Statuer sur l'usage de trait d'identité présents dans le CDA	Ajoutée v0.2
MES	Recherche destinataire patient	EXIGENCE	3.10	Le système DOIT permettre au professionnel d'écrire à un patient en le sélectionnant dans une liste construite à partir de la base patients connus du système ou directement depuis le dossier d'une patient. Le système récupère l'INS qualifiée du patient et renseigne le champs To: du message avec l'adresse MSSanté du patient ainsi constituée.	Rappel : Attention la saisie d'INS patient n'est pas permise	Ajoutée v0.2
Configuration		RECOMMANDATION	3.17	Le système PEUT permettre de configurer plusieurs BAL MSSanté simultanément		Ajoutée v0.2

Questions / Remarques ANS :

- Dans un onglet distinct : n'intègreront probablement pas le référentiel #2, mais les REM de certains couloirs
- 3.9 : Permet d'afficher les nom / prénom du patient sans disposer d'un accès à un référentiel d'identité

MSSanté
Système de messageries sécurisées, données protégées.

Questions / réponses

III Focus sur certaines exigences en cours de rédaction

Interfaces d'accès aux BAL : Lesquelles sont obligatoires ?

2 interfaces API LPS avec 2 MIE distincts

- **BALs PER & ORG :** MIE PSC -> 5 exigences (1.6 à 1.10)
- **BALs APP :** MIE certificat ORG_AUTH_CLI -> 1 exigence (1.11)
- Rq : La recommandation 1.12 permet d'utiliser une interface propriétaire (conforme avec référentiel identification électronique de la PGSSI-S), principalement dans un contexte où le MIE PSC n'est pas encore adapté (établissements…)

RAPPEL : Coté opérateurs (Référentiel #1 v1.5 / couloir Ségur opérateur)

- **Interface BALs PER & ORG (MIE PSC) : OBLIGATOIRE**
- **Interface BALs APP (MIE certificat ORG_AUTH_CLI) :** OPTIONNELLE

Position envisagée dans le Référentiel #2 v1.0

- **Rendre obligatoire au moins l'une des 2 interfaces de l'API LPS**
- Certains couloirs Segur pourraient rendre obligatoire les 2 interfaces suivant les besoins des utilisateurs finaux

Notification du système émetteur : Nature des accusés

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	Statut exigence
Accusé de lecture	EXIGENCE	3.11	Le système DOIT permettre de demander au destinatire un accusé lors de l'émission de tous les courriels. [la nature du ou des accusés (reception, lecture, intégration) reste à statuer avec les éditeurs]		Ajoutée v0.2
Accusé de lecture	EXIGENCE	3.12	Le système DOIT retourner un accusé lors de la réception/consultation d'un message qui contient une demande d'accusé. [la nature du ou des accusés (reception, lecture, intégration) reste à statuer avec les éditeurs]	MES supporte deja cette fonctionalité	Ajoutée v0.2
Accusé de lecture	EXIGENCE	3.13	Le système DOIT traiter rapprocher les accusés retournés par les destinataires des messages émis correspondants,	Faisabilité à vérifier	Ajoutée v0.2

RAPPELS :

3 types d'accusés possibles pour l'émetteur :

- Accusé de réception dans le boite du destinataire (retourné par l'opérateur destinataire)
- Accusé de lecture retourné par le LPS destinataire lors de l'affichage du message (avec acquittement utilisateur ou non)
- Accusé « de bonne intégration » du CDA par le LPS destinataire (voir CI-SIS Volet Echange §3.2.8.2)

Référentiel #2 v0.1 / Vague 1 Ségur :

- OBLIGATION : Savoir demandé un accusé de réception DSN (retourné par l'opérateur de destination)
- OPTIONNEL : Demandé un accusé de lecture MDN lors des envois à MES

Questions / Remarques ANS :

- Quels sont les couloirs qui nécessitent de disposer d'une preuve de bonne réception de la part du destinataire ?
- Quel est le niveau minimal de gestion des accusés à avoir entre tous les LPS ?
- Connaissez-vous / proposez-vous des dispositifs de rapprochement des erreurs de réception avec les messages envoyés ?

Exigence 2.1 : Présence d'un INS qualifié dans un document CDA

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	Statut exigence
Indicateurs	EXIGENCE	2.1	Le système DOIT positionner l'entête SMTP "X-MSS-INS" dans un messages 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'un "INS qualifié" *. - 'N' (Non) en cas d'absence d'un "INS qualifié" *, 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	L'objectif est de pouvoir déterminer la part des messages contenant un INS qualifié * INS qualifié au sens du §5.3.3 du Référentiel Identifiant National de Santé v2.0 La présence d'un INS qualifié est caractérisé 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 Exemple : X-MSS-INS = O X-MSS-INS = N	Modifiée v0.2

Modification apportée

- Entête SMTP à ne positionner que si IHE_XDM/CDA présent en PJ

Questions / Remarques ANS :

- Tous les LPS seront-ils bien en capacité de vérifier la présence des 6 champs dans l'entete CDA ?

Exigence 2.3 : Identification du LPS

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	Statut exigence
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 ~~brique~~ solution logiciel qui a produit le message SMTP.		Modifiée v0.2

Questions / Remarques ANS :

- Tous les LPS ne disposant pas de NIL CNDA, proposition d'utiliser l'identifiant convergence attribué lors du processus de référencement Segur
- Modalités pratiques restent à décrire

MSSanté
Système de messageries sécurisées, données protégées.

Questions / réponses

IV Suite des travaux

Conclusion

Prochaines étapes :

- **Vendredi 30 septembre** (au soir) : Retours éditeurs sur draft d'exigences Ref#2 v0.2
  - Renseigner la colonne AS des 2 onglets
  - Retourner par email à ans-n3_espaceconfiancemssante@esante.gouv.fr

- **Vendredi 14 octobre 15h** : Atelier #6
  - Echange sur vos retours de concertation du draft d'exigences v0.2
  - Dernier atelier avant concertation publique

- **Début novembre** : Concertation publique de la version rédigée du Référentiel #2 v1.0

- Rq : en parallèle chaque TF va itérer avec les éditeurs de chaque couloir sur les exigences du REM

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