MS Santé
Système de messageries sécurisées, données protégées.

Segur vague 2

Concertation exigences MSSanté

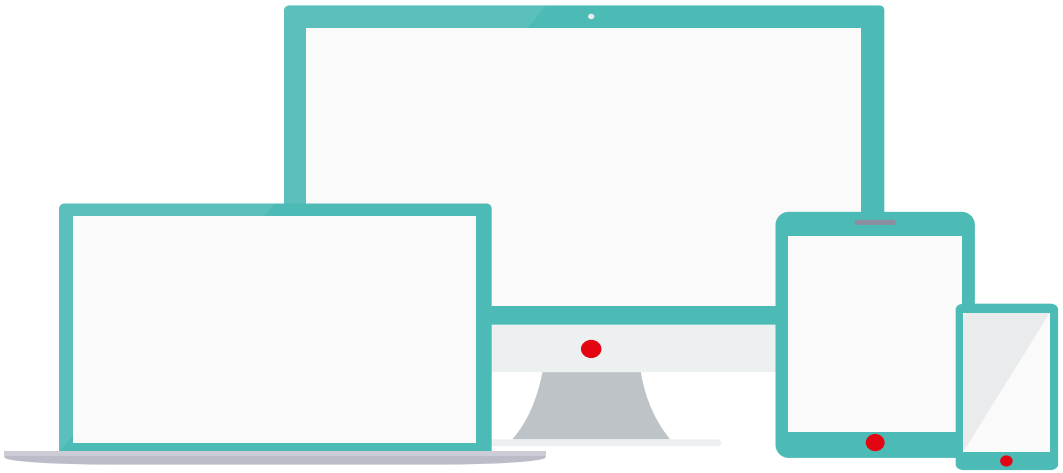
Atelier Editeurs #2 du 03/06/2022

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

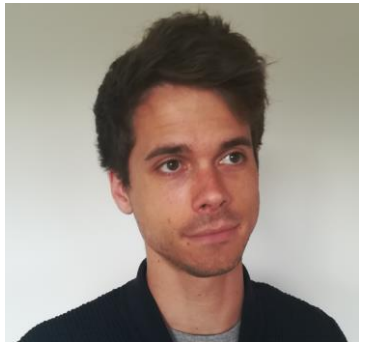
MSSanté
Système de messageries sécurisées, données protégées.

Introduction

Intervenants et organisateurs

Gestion de l'Espace de Confiance MSSanté
Edouard BRIS

Gestion de l'Espace de Confiance MSSanté
Mike GUEYE



Architecte applicatif MSSanté
Bastien DANGIN

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

Retour sur les questions posées en atelier #1

Publication des ressources des ateliers :

https://www.mssante.fr/chantiers-segur

- Contient supports, CR, enregistrement et draft de référentiel d'exigences (à venir)
- Le CR de l'atelier 1 contient 30 questions/réponses, posées en séance, regroupées par thème

Précisions suites à vos questions :

- Q1 : L'utilisation de l'API LPS / PSC demande encore des travaux pour être utilisables pour certaines professions (secrétaire médicale, préparateur en pharmacie…) -> travaux en cours en dehors de ces ateliers
- Q6 : Un des apports de l'API LPS / PSC est de permettre de mutualiser l'authentification LPS et opérateurs MSSanté
- Q9 : L'API LPS n'a pas retenu d'interfacage via WS, mais uniquement via IMAP/SMTP
- Q16, Q18, Q19 : L'usage, finalité et les MIE des 3 types de BAL MSSanté doivent être clarifiées -> Les indicateurs Ségur à remonter à l'ANS sur le contenu des messages envoyés
- Q20 : L'usage de l'API LPS en établissment à travers une PFI devra faire l'objet d'un focus particulier
- Q22 : Pour utiliser l'API LPS / PSC l'opérateur LPS devra nécessairement connaitre l'IdNAT lors de la création de la BAL, afin de réaliser les authentifications ultérieures
- Q24 : PSC CIBA est actuellement disponible en environnement de test (BAS). Production prévue courant juin

I Focus API LPS et PSC :

Suite

API LPS et PSC – Précisions sur OpenID Connect (OIDC)

PSC repose sur le standard **OpenID Connect** :

- Standard bâti au-dessus de **OAuth**, utilisable pour les technologies Web
- OAuth introduit la notion d'**Access Token** : permet d'autoriser l'accès à un service (API Web en général, service mesagerie MSSanté) après validation d'une authentifciation auprès d'un fournisseur d'identité (PSC)
- OAuth défini également la notion de **Refresh Token** qui permet de renouveler l'Access Token sans redemander systématiquement une authentification utilisateur
- OpenID Connect introduit « en plus » la notion d'**ID Token** : porte les informations d'identité de la personne authentifiée

Pour MSSanté : Access Token, ID Token et Refresh Token sont récupérées par le LPS après authentification auprès de PSC et :

- L'Access Token est **transmis à l'opérateur MSSanté par le LPS**
- L'entretien du Refresh Token est de **la responsabilité du LPS** (cf. détails à suivre)
- L'ID Token peut être utilisé pour obtenir les informations d'identité du PS

API LPS et PSC – Terminologie et choix de conception

Précision sur la **terminologie** :

- Un **LPS/DUI** (i.e. Editeur) est un **fournisseur de service**, i.e. il procède à la demande de l'Access Token / Refresh Token (authentification) auprès de PSC
- Un **service de messagerie de MSSanté** (i.e. Opérateur) est un **fournisseur de données**, i.e. il reçoit l'Access Token d'un fournisseur de service (quel que soit le flux d'authentification utilisé, redirection ou CIBA) et doit procéder à sa validation auprès de PSC

- Particularité API LPS MSSanté : ce n'est pas une connexion Web (entretenue par une transmission systématique de l'Access Token) mais une connexion de type **session SMTP ou IMAP** (sans transmission systématique de l'Access Token).

Choix techniques concernant la nouvelle API LPS réalisés sur la base :

- D'une **étude** des solutions possibles (3 candidats : IMAP / SMTP, WS, JMAP) avec mise en œuvre de PSC (OpenID Connect)
- De **démonstrateurs techniques**
- D'une **concertation avec les Opérateurs** (4 ateliers T1 2022)

- A l'issue de ces travaux, le choix a été arrêté sur **IMAP / SMTP** car cette interface satisfaisait le mieux les critères retenus pour l'étude : standard établi, compatible authentification IODC / PSC, auto-configuration, accusé de réception, …
- Transit du jeton PSC par mécanisme **SASL avec implémentation XOAUTH2** (authentification OAuth 2.0) sur SMTP et IMAP validé par un démonstrateur, nécessaire du fait de l'utilisation de protocoles non Web (pré-requis à l'utilisation des flux standards OIDC / PSC)

API LPS et PSC – Durée de vie des sessions IMAP / SMTP

Causes possibles de clôture de session IMAP / SMTP :

- A l'initiative du **LPS/DUI** (i.e. éditeur)
  - **Demande volontaire** de déconnexion du PS => déclenche la fin de session
  - **Fin de validité** du Refresh Token => le LPS/DUI doit gérer le Refresh Token , i.e. le rafraichir et terminer la session si le Refresh Token expire
    - Durée de vie Access Token : 2 min
    - Durée de vie Refresh : 3 min. Renouvellement à faire pour maintenir la session (endpoint RefreshToken PSC)
    - Durée session max : 4 h

    https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/documentation-technique#paragraph-id--2760
- A l'initiative du **service de messagerie de MSSanté** (i.e. opérateur)
  - Sur **inactivité de la session** (i.e. aucune commande IMAP / SMTP envoyée par le client LPS/DUI) : 15 min
  - **Durée session max** : 4h (calqué sur la durée maximale de la session PSC)

API LPS et PSC – 2 niveaux de déconnexion à gérer dans le LPS/DUI

- **Déconnexion de l'opérateur MSSanté** => liée à la durée de session IMAP / SMTP
  - En effet, contrairement aux flux Web « stateless », IMAP et SMTP sont des **protocoles à session**. La durée de la session peut donc être gérée par le client (i.e. LPS/DUI / éditeur) et par le serveur (i.e. service de messagerie / opérateur)
- **Déconnexion de PSC** => liée à la durée de vie du jeton PSC (Access Token a durée de vie courte puis Refresh Token pour l'entretien)
  - Cette gestion permet au PS d'utiliser **plusieurs services de santé** numérique à partir d'une **seule authentification PSC**
  - **N.B. :** La déconnexion de PSC depuis un service n'est pour l'instant pas propagée à un autre service. C'est donc la fin de validité du Refresh Token au niveau du fournisseur de service (LPS/DUI dans le cas présent) qui doit déconnecter l'utilisateur

Conclusion : au-delà de gérer la déconnexion de l'opérateur MSSanté, chaque LPS/DUI / éditeur doit se positionner par rapport à la déconnexion PSC.

Exemple : lors de la demande explicite de déconnexion faite par le PS, une « pop-up » demande au PS s'il souhaite se déconnecter ou pas de PSC

API LPS et PSC - Présentation synthèse des exigences sur l'API LPS du Référentiel #2

Contenu

- Synthèse présentée sous la forme d'un **ensemble d'exigences** avec lesquelles le LPS/DUI doit se mettre en conformité
- Exemples (« non contractuels ») :

Le système DOIT se connecter aux serveurs de messagerie respectant le référentiel MSSanté #1 via une interface d'envoi de messages utilisant le protocole SMTP avec STARTTLS sur le port 587, conformément à la RFC 5321

Sur les interfaces de l'API LPS, le système DOIT impérativement se connecter aux serveurs de messagerie en utilisant la version 1.2 (RFC 5246) ou une version ultérieure (TLS 1.3...) de TLS

Planning de mise à disposition

- Une première version (v0.1) sera envoyée le **09/06/2022**
- Retours (remarques et questions) attendu pour le **14/06/2022** au soir

MS Santé
Système de messageries sécurisées, données protégées.

Questions / réponses

Modalités de test/recette à proposer aux éditeurs

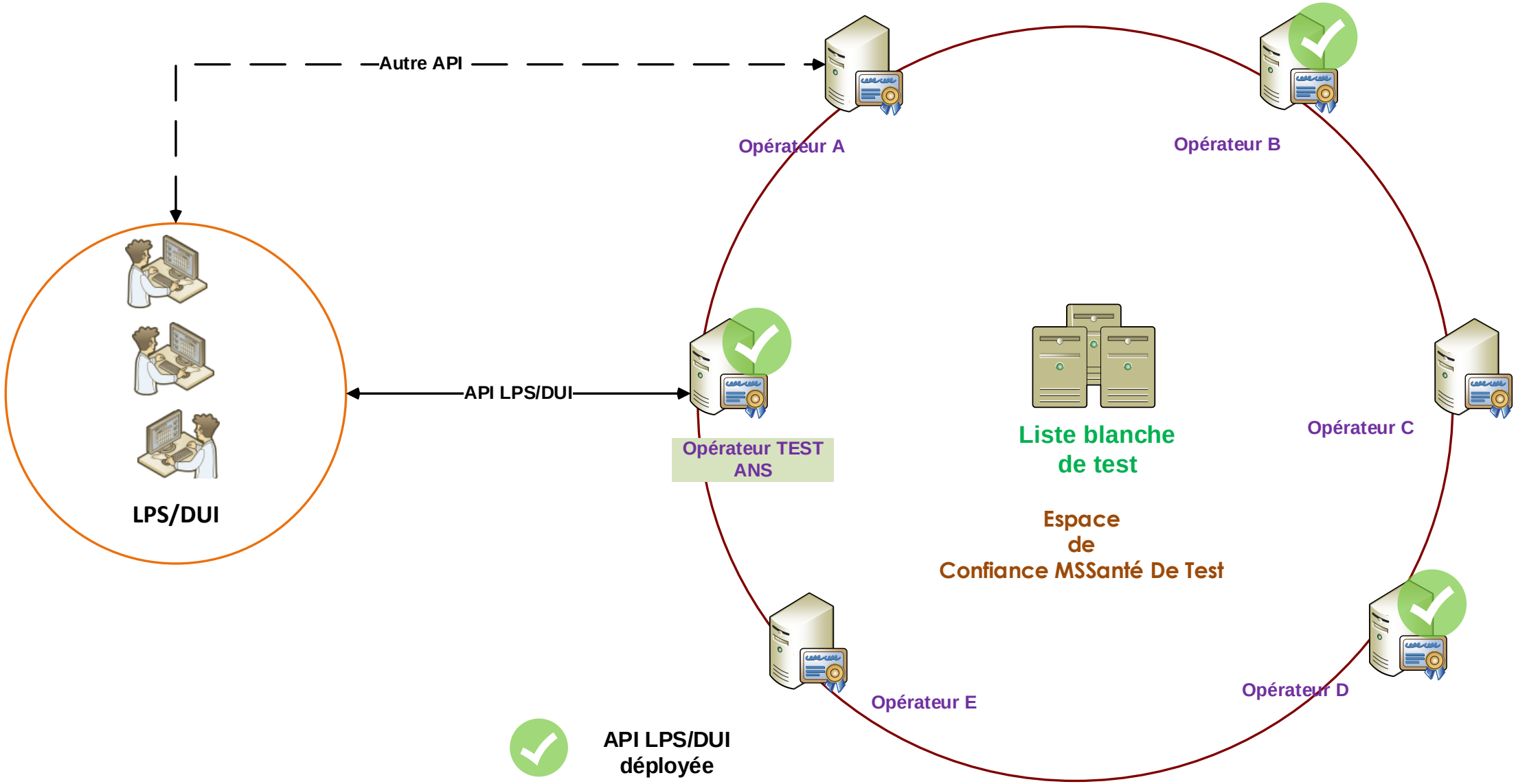
OBJECTIFS

- Mettre à disposition un environnement opérateur de test pour les développements des fonctions de messagerie des LPS/DUI
- Permettre aux solutions de messagerie de vérifier leur conformité à certaines exigences du Ref #2
- Produire un CR de test attestant de la conformité de la solution aux exigences du Ref #2 (Ségur vague 2)
- Permettre aux solutions de messagerie de vérifier la bonne structuration et le bon échange de documents de santé (en lien avec Gazelle)

MODALITES

- Simulation d'un Opérateur « de référence » en Espace de Confiance de test
- Opérateur accessible à travers l'API LPS/DUI et probablement un webmail
- 2 MIE possibles pour la connexion :
  - Pro Santé Connect (BAL personnelle, organisationnelle)
  - Certificat IGC Santé AUTH_CLI (BAL applicative)

Modalités de test/recette à proposer aux éditeurs



MS Santé
Système de messageries sécurisées, données protégées.

Questions / réponses

II Indicateurs d'usage demandés aux LPS/DUI

Entêtes spécifiques MSSanté insérées aux messages envoyés

OBJECTIF : suivre le déploiement de l'INS et l'échange de données structurées

1

Indiquer la présence d'un INS qualifié

Positionnement de l'entête « **X-MSS-INS** »
O – présence d'un INS qualifié
N – absence d'INS qualifié

2

Renseigner le type de document CDA transmis

Positionnement de l'entête **« X-MSS-CODECDA »**
Reprendre la valeur de l'attribut code* présent dans l'entête de chaque document CDA transmis

3

Transmettre le NIL du client de messagerie

Positionnement de l'entête **« X-MSS-NIL »**
Valeur issue du CNDA pour identification du logiciel homologué

X-MSS-INS

'O' présence d'un INS qualifié au sens du §5.3.3 du Référentiel Identifiant National de Santé v2.0
'N' absence d'INS qualifié

X-MSS-CODECDA

* un document structuré fait référence à l'*exigence ECO.2.1.1 du Ref #2*

si pas de document structuré : ne pas positionner l'entête

si un seul document CDA joint : le type de document CDA correspondant à l'attribut ***'code'*** de l'en-tête CDA
Exemple :
X*-MSS-*CODECDA = 34112-3

Si plusieurs documents CDA joints : tous types de document CDA correspondant à l'attribut ***'code'*** de l'en-tête de chaque CDA
Exemple :
X*-MSS-*CODECDA = 34112-3, PRESC-BIO, 15508-5
/!\ séparer les valeurs avec la 'virgule'
Possibilité de préciser le niveau de structuration du document (à discuter)

X-MSS-NIL (Num Identification Logiciel)

NIL obtenu auprès du CNDA afin d'identifier le logiciel
Quelle cible pour le NIL :

1. *Donner la possibilité aux opérateurs d'identifier les connexions à leurs interfaces*
2. *Meilleure gestion des montées de version des interfaces*
3. *Possibilité d'interdire les connexions malveillantes*

Les Webmail ne sont pas soumis à cette exigence

*code défini dans le « Volet Structuration Minimale de Documents de Santé – CI-SIS Juin 2021, §3.5.5.5 »

Entêtes spécifiques MSSanté insérées aux messages envoyés

QUESTION 1 : le NIL vous parait-il pertinent afin d'identifier le logiciel ?

QUESTION 2 : à chaud, voyez-vous des difficultés à implémenter les différents entêtes ?

1

Indiquer la présence d'un INS qualifié

Positionnement de l'entête « **X-MSS-INS** »
O – présence d'un INS qualifié
N – absence d'INS qualifié

2

Renseigner le type de document CDA transmis

Positionnement de l'entête **« X-MSS-CODECDA »**
Reprendre la valeur de l'attribut code* présent dans l'entête de chaque document CDA transmis

3

Transmettre le NIL de la solution de messagerie

Positionnement de l'entête **« X-MSS-NIL »**
Valeur issue du CNDA pour identification du logiciel homologué

code défini dans le « Volet Structuration Minimale de Documents de Santé – CI-SIS Juin 2021, §3.5.5.5 »

MS Santé
Système de messageries sécurisées, données protégées.

Questions / réponses

III Echanges avec la messagerie patients de MES

Echanges avec la messagerie patients de MES

- **Mon espace santé est intégré depuis août 2021 dans l'Espace de confiance MSSanté.**
- **Cette intégration a permis l'ouverture de Mon espace santé et de sa fonctionnalité de Messagerie dans trois territoires Pilote en août 2021. Depuis fin janvier, le service est disponible pour les usagers de l'ensemble des territoires.**
- **Le processus de création automatique a démarré début mai et se termine mi-juillet.**

Création automatique de Mon espace santé pour tous les assurés sauf opposition de la personne (opt-out)*

Toutes les personnes rattachées** à un régime d'assurance maladie français sont notifiées de l'arrivée de Mon espace santé

Un courrier (email ou postal) fournit les modes d'opposition et d'accès au service

Si l'usager active son accès, Mon espace santé est créé

Si l'usager s'oppose, Mon espace santé ne sera pas créé

À la fin de la période d'opposition, après l'envoi du courrier ou de l'email, si l'usager ne s'est pas connecté ni opposé, son profil **Mon espace santé est automatiquement créé.**
Un professionnel peut alors écrire sur la messagerie de santé du patient et alimenter son dossier médical.

Echanges avec la messagerie patients de MES

- **Pour faciliter l'intégration des Messagerie de Professionnels avec la Messagerie de Mon espace santé, une note technico-fonctionnelle sur le client de messagerie Mon Espace Santé est publiée depuis décembre 2021 sur la page https://www.mssante.fr/is/doc-technique**

- **Les éléments d'information de cette note ont vocation à intégrer la prochaine version du référentiel #2 : en tant qu'informations, préconisations, ou nouvelles exigences.**

- **Nous vous proposons aujourd'hui d'aborder quelques points importants sur le fonctionnement de la Messagerie Mon espace santé et sur les évolutions à concerter pour la prochaine version du référentiel #2 :**
  - L'affichage d'informations sur les Professionnels qui échangent avec les usagers
  - L'envoi des messages vers les professionnels
  - La gestion des documents reçus
  - Les messages de retour de Mon espace santé selon les statuts des messagerie usagers
  - Les accusés de lecture
  - La possibilité pour les Professionnels de mettre fin aux échanges avec un usager
  - L'identification des messages émis par les patients

Echanges avec la messagerie patients de MES

Affichage d'informations sur les Professionnels

- **L'exigence ECO 2.2.7 du référentiel #2 permet de véhiculer un libellé signifiant dans chaque message envoyé par un Professionnel. Ce libellé est affiché dans mon espace santé et facilite l'identification du Professionnel associé à l'adresse de messagerie expéditeur du message.**

- **Affichage du nom du Professionnel avec qui l'usager échange :**

Lorsqu'un message est envoyé dans Mon espace santé avec l'entête :	Mon espace santé affiche comme expéditeur du message :
… *Subject: vos documents* *From: Dr Marie MARTIN <marie.martin@medecin.mssante.fr>* *To: <123456789012345@patient.mssante.fr>* …	Dr Marie MARTIN
… *Subject: vos documents* *From: <secr-medical-ortho.021@sante-plus.mssante.fr>* *To: <123456789012345@patient.mssante.fr>* …	secr-medical-ortho.021

Evolution du référentiel #2 à concerter : le libellé présent dans les messages envoyés par un Professionnel doit être connu et paramétrable par le Professionnel

Echanges avec la messagerie patients de MES

Envoi des messages vers les Professionnels

- **Le corps des messages envoyés par un usager depuis Mon espace santé est au format HTML.**

- **Techniquement, il s'agit d'un message multipart/alternative, valorisé avec :**
  - La partie text/html qui contient le message de l'usager et le cas échéant l'historique des messages échangés,
  - La partie text/plain qui contient un message indiquant : "Utilisez la visualisation HTML pour consulter le contenu de ce message".

- **De ce fait, les clients de messageries pour les Professionnels doivent employer un rendu html afin de permettre l'affichage du message aux Professionnels.**

- **La valorisation de la partie text/plain pour les messages envoyés par les usagers sera réalisée dans Mon espace santé d'ici fin 2022.**

Echanges avec la messagerie patients de MES

Gestion des documents reçus

- **Les fichiers au format IHE_XDM ne sont pas encore exploitables dans Mon espace santé**

- **Seul le document au format PDF qui est associé à un envoi de fichier IHE_XDM (exigences ECO 2.1.1, 2.1.4 et 2.1.5 du référentiel #2) peut être ouvert dans Mon espace santé et enregistré par le patient dans les documents de santé.**

- **D'autres formats de fichiers sont pris en compte dans Mon espace santé :**
  - Fichiers au format PDF, JPG ou PNG : visualisables dans Mon espace santé et enregistrables dans les documents de santé,
  - Fichiers au format TIF, RTF et TXT : ne peuvent pas être visualisés mais peuvent être enregistrés dans les documents de Santé.

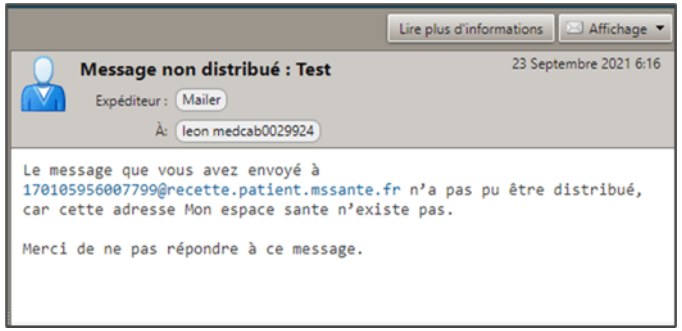
Echanges avec la messagerie patients de MES

Messages de retour selon le statut de la Messagerie Mon espace santé

- **L'envoi d'un message sur une adresse de messagerie patient peut donner lieu à des réponses automatiques liées au statut de la Messagerie de l'usager destinataire du message :**
  - Cas d'une messagerie « inexistante » :
    - Si l'adresse destinataire utilise un INS inconnu de Mon espace santé,
    - Si un usager n'a pas activé son espace santé et s'il n'y a pas encore eu de processus de création automatique pour cet usager,
    - Si un usager s'est explicitement opposé à la création de son espace santé,
    - Si un usager, dans son espace santé, a demandé la suppression de son compte et de toutes les données le concernant.

  - Cas d'un messagerie « clôturée » :
    - Si l'usager à décidé de clôturer son compte sans demander la suppression de toutes ses informations

Cas d'une messagerie inexistante *



Cas d'une messagerie « clôturée » *

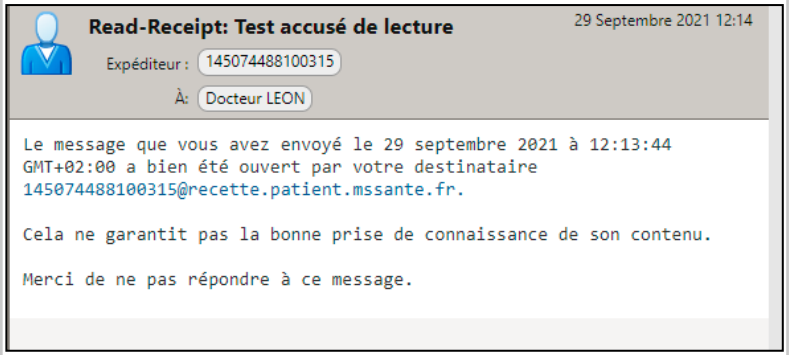
**Captures d'écran issues de Mailiz*

Echanges avec la messagerie patients de MES

Accusés de lecture

- Il est possible d'envoyer un message à un usager en demandant un Accusé de lecture.
- Cet accusé de lecture est renvoyé automatiquement dès lors que l'usager clique sur le message et que celui-ci s'affiche dans sa Messagerie Mon espace santé. Ceci sans demande de confirmation explicite à l'usager.

Accusé de lecture *



*Capture d'écran issue de Mailiz

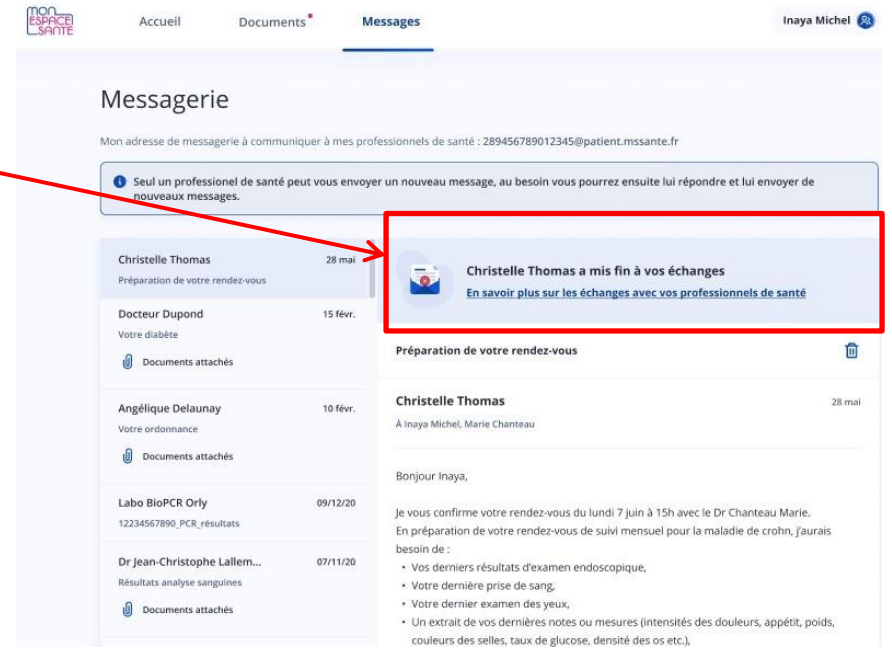
Evolution du référentiel #2 à concerter : Permettre la demande d'accusé de lecture lors de l'envoi des messages, intégrer la réception de ces accusés pour faciliter le suivi des messages envoyés

Echanges avec la messagerie patients de MES

Possibilité pour les Professionnels de mettre fin aux échanges avec un usager

- **Pour le professionnel, utiliser cette possibilité se fait par l'envoi d'un message aux caractéristiques suivantes :**
  - Expéditeur : adresse MSS du Professionnel qui ne souhaite plus recevoir de message d'un usager donné
  - Destinataire : adresse de Messagerie Sécurisée de l'usager concerné
  - Objet du message : **[FIN]**

Dans Mon espace santé, apparition d'un bandeau sur le/les messages concernés :



Evolutions du référentiel #2 à concerter :

- Faciliter dans l'interface utilisateur du professionnel la possibilité de mettre fin aux échanges avec un usager :
- Remplacer l'envoi du message [FIN] par l'utilisation d'une nouvelle entête SMTP permettant, dans un message, d'indiquer qu'il n'est pas possible d'y répondre.

Echanges avec la messagerie patients de MES

Identification des messages émis par les patients

- **Le prénom et nom de l'usager tel que connu dans Mon espace santé est transmis dans les messages envoyés par un usager :**
  - Le champ "From:" d'un message envoyé par un usager contient, en plus de son adresse de messagerie, ses prénom et nom connus dans Mon espace santé.

Exemple : « From: Léo Dupond <123456789012345@patient.mssante.fr> »

Evolution du référentiel #2 à concerter : Permettre la distinction entre les messages envoyés par les Professionnels des messages envoyés par les usagers

MS Santé
Système de messageries sécurisées, données protégées.

Questions / réponses

Conclusion et prochaines étapes

Conclusion

Prochaines étapes :

- **Jeudi 9 juin :** publication du tableau d'exigences Ref#2 v0.1
- **Mardi 14 juin** (au soir) : retours éditeurs par email sur les tableau d'exigences Ref#2 v0.1

- **Vendredi 17 juin 15h** : Atelier #3
  - Echange sur vos retours de concertation des exigences API LPS
  - Concertation sur certains exigences en particulier
  - Modalités de consultation de l'Annuaire Santé par les éditeurs de LPS/DUI
- **S26 :** publication du tableau d'exigences Ref#2 v0.2

- **Vendredi 8 juillet 15h** : Atelier #4 - Proposition dernier atelier avant la période de congés
  - Ordre du jour à définir

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