MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Référentiel socle MSSanté #2

Clients de Messageries Sécurisées de Santé

Version : 1.0
Date : 31 janvier 2023

MSSanté
Système de messageries sécurisées, données protégées.

Identification du document	
Référence ANS	**ANS_MSS_Ref2_Clients_de_messageries_MSSanté_v1.0_20230131.docx**
Classification	**Non sensible publique**
Nombre de pages	57

Historique du document		
Version	Date	Commentaires
V1.0	31/01/2023	Modifications notables suite à concertation : - ECO.1.1.3 : Reformulations/précisions apportées - ECO.1.1.10 : IGC santé doit être la seule AC autorisée - ECO.2.1.5 : Précision modalité génération PDF - ECO.3.1.6 : Porte sur l'obligation de proposer la fonction - ECO.4.1.1 : Durée de conservation non imposée (recommandée)
V1.0 - Concertation	29/11/2023	Version « 1.0- concertation » diffusée pour concertation publique. Les principaux apports concernent : - l'introduction de la spécification de l'API LPS pour les éditeurs de LPS - la définition de 2 familles de LPS Clients de Messagerie - l'usage d'entêtes spécifiques MSSanté - la définition d'exigences portant sur les IHM des LPS (hors BAL APP) Version utilisée pour les REM de la vague 2 Segur.
V0.1	14/06/2021	Version publiée utilisée par la vague 1 Segur Suppression de l'exigence (EX_DC_1.1) sur l'interdiction d'envoi d'un mail avec un usager et un professionnel en copie Suppression de l'exigence (EX_DC_1.4) portant sur les clients de messagerie non intégrés avec un référentiel d'identité Numérotation des exigences au format de l'outil Exigence
V0.1 - Draft	01/06/2021	Version 0.1 diffusée pour concertation éditeurs

SOMMAIRE

1. INTRODUCTION

1.1. Destinataires du document

Le présent document s'adresse aux éditeurs de c**lients de messageries MSSanté.**

Il s'applique à tout logiciel métier (client lourd ou SaaS) utilisé par un professionnel habilité comportant des fonctions d'échange par messagerie MSSanté. Il ne s'applique donc pas aux interfaces webmail ou clients de messageries standards (type Outlook ou Thunderbird).

1.2. Objet du document

Le référentiel #1 Opérateurs de Messageries Sécurisées de Santé [REF1-MSSANTE], qui existe depuis 2014 est une annexe au contrat Opérateur qui lie les opérateurs à l'ANS en tant que régulateur de l'Espace de Confiance MSSanté.

Le présent document est le second référentiel du service socle des Messageries Sécurisées de Santé (MSSanté). Il a été publié dans sa première version en 2021 et il s'adresse aux **éditeurs de clients de messageries MSSanté (également désignés « éditeurs »)**.

Le présent document a pour objectif de définir les modalités (techniques, fonctionnelles, organisationnelles) applicables aux éditeurs de clients de messageries MSSanté afin de garantir une bonne interopérabilité des échanges de messages au sein du système MSSanté, et plus particulièrement entre clients de messageries MSSanté et opérateurs MSSanté.

Les dispositions du présent Référentiel #2 sont obligatoires pour tout éditeur de clients de messageries MSSanté participant aux dispositifs de référencement et de financement du programme Segur (à compter de la vague 2).

Le document aborde successivement les thématiques suivantes :

- Les **modalités de transport et de sécurisation** des courriels applicables aux clients de messagerie MSSanté dans les échanges avec les Opérateurs MSSanté. Cette partie comporte un ensemble d'exigences visant à sécuriser ce transport. Elle décrit en particulier l'API LPS qui est obligatoirement mise à disposition des clients de messageries MSSanté par chacun des Opérateurs de l'Espace de confiance MSSanté.
- Les règles à respecter pour **échanger des documents de santé** via des courriels MSSanté et pour transmettre l'identité INS de l'usager. Les exigences s'appuient sur le volet échanges du CI-SIS [CI-ECH-DOC]. Elles concernent notamment le nommage de l'objet des courriels, le nombre, le format et le nommage des pièces jointes.
- Des exigences générales visant à assurer **l'interopérabilité des échanges entre clients de messageries MSSanté**, y compris lorsqu'un document de santé n'est pas joint au courriel. Elles s'appliquent au formatage du corps des courriels, à la manière de déterminer les adresses de messagerie des destinataires, au nommage de l'expéditeur, ainsi qu'à la gestion des accusés de réception et de lecture.
- Des exigences touchant à la manière dont les messages sont restitués dans les interfaces utilisateurs des clients de messageries MSSanté (lorsque ceux-ci en proposent). L'objectif est de s'assurer que certaines fonctions jugées essentielles soient bien proposées aux utilisateurs.

1.3. Définitions

Un **« professionnel habilité »** désigne tout professionnel de santé ou non professionnel de santé des secteurs social et médico-social mentionné à l'article L.1110-4 du code de la santé publique et autorisé à collecter, échanger et partager des données de santé à caractère personnel relatives à un usager pour lequel il intervient dans la prise en charge. La liste de ces professionnels a été définie à l'article R.1110-2 2 du code de la santé publique.

Un « **usager** » désigne toute personne physique prise en charge par un professionnel habilité dans le secteur sanitaire ou le secteur social. Elle recouvre donc aussi la notion de **patient** utilisée généralement dans le domaine sanitaire.

Un « **client de messagerie MSSanté** » (également désigné « **système** » ou « **LPS** compatible MSSanté ») désigne un logiciel en capacité d'envoyer ou de recevoir des courriels, en se connectant au service d'un Opérateur MSSanté, pour le compte d'un professionnel habilité. En effet, les échanges de messages peuvent être réalisés soit « manuellement » par le professionnel habilité (via une IHM : LGC…), soit de façon automatisée (DPI, SIL, RIS, …). Le terme « client de messagerie MSSanté » n'implique pas nécessairement de proposer une IHM présentant au professionnel une arborescence de BAL. Le présent référentiel peut s'appliquer à tout logiciel métier (client lourd ou SaaS) utilisé par un professionnel, accédant à des dossiers patients/usagers et comportant des fonctions d'échange par messagerie MSSanté. Il ne s'applique donc pas aux interfaces webmail ou client de messagerie standard (type Outlook ou Thunderbird).

Un « Opérateur de Messageries Sécurisées de Santé » ou « Opérateur » est une personne physique ou morale qui développe et fournit un service de Messageries Sécurisées de Santé au profit d'utilisateurs finaux (professionnels et usagers).

Il existe deux catégories d'Opérateurs MSSanté :

- L'Opérateur professionnels : désigne toute personne physique ou morale qui développe et fournit un service de Messageries Sécurisées de Santé au profit d'utilisateurs professionnels. Il permet aux professionnels habilités d'échanger entre eux ainsi qu'avec les utilisateurs usagers. Les Opérateurs professionnels sont notamment un établissement de santé ou plus largement toute structure de soins, un groupement de coopération sanitaire, un industriel etc...
- L'Opérateur usagers : désigne une personne physique ou morale qui développe et fournit un service de Messageries Sécurisées de Santé au profit d'utilisateurs usagers. La Cnam agit en qualité d'Opérateur usagers fournissant un service de messagerie aux usagers dans le cadre de Mon espace santé.

L'« **API LPS** » désigne l'API utilisée par un client de messagerie MSSanté pour se connecter à un Opérateur de l'Espace de Confiance de MSSanté, quel que soit le type de BAL utilisé.

« Pro Santé Connect » est un téléservice mis en œuvre par l'ANS contribuant à simplifier l'identification électronique des professionnels intervenant en santé. C'est un fédérateur d'identité permettant aux utilisateurs de services numériques en santé de s'authentifier par le biais de leurs cartes CPS ou e-CPS.

1.4. Gestion des versions successives

Le présent référentiel sera mis à jour notamment pour prendre en compte les évolutions, fonctionnelles ou techniques, apportées au système MSSanté ainsi que toute évolution du cadre juridique applicable système MSSanté.

Toute évolution substantielle du référentiel fait l'objection d'une concertation publique qui fait l'objet d'une publicité auprès de l'écosystème. De plus, il est possible d'être automatiquement informé des actualités du système MSSanté en s'abonnant à une liste de diffusion (voir mssante.fr).

1.5. Rappel des principes de l'Espace de Confiance MSSanté

1.5.1. Définition et principes de l'Espace de Confiance MSSanté

L'ANS est le groupement d'intérêt public, prévu à l'article L.1111-24 du code de la santé publique, chargé de favoriser le développement et la régulation des systèmes d'information, services ou outils numériques utilisés dans le domaine de la santé et du médico-social. À ce titre, elle assure la mise en œuvre du système MSSanté et la gestion de l'Espace de Confiance.

Le **système MSSanté** est un système de messageries électroniques qui permet l'échange sécurisé d'informations et de documents de santé entre professionnels habilités et entre professionnels habilités et usagers. Ce dernier est composé **« d'Opérateurs MSSanté professionnels »** offrant un service MSSanté à des professionnels habilités, ainsi qu'un **« Opérateur usagers** » unique offrant son service MSSanté aux usagers du système de santé (« Mon espace santé »).

Le système MSSanté est fondé sur « **l'Espace de Confiance MSSanté** » qui se caractérise également par :

- L'**Annuaire Santé** s'appuyant notamment sur le répertoire partagé des professionnels de santé et ayant vocation à référencer l'ensemble des professionnels habilités à échanger des données de santé à caractère personnel ;
- Une « **liste blanche »** qui regroupe l'ensemble des domaines de messageries des Opérateurs MSSanté » autorisés à échanger dans l'Espace de Confiance MSSanté ;
- 2 référentiels permettant à l'écosystème de développer des offres conformes et interopérables entre elles : le présent **Référentiel #2** Clients de messageries et le **Référentiel #1** Opérateurs de Messageries Sécurisées de Santé.

1.5.2. Présentation de la messagerie usagers de Mon espace santé

L'intégralité des personnes couvertes par les régimes obligatoires de l'Assurance Maladie, ainsi que tout usager du système de soins disposant d'un INS, peut disposer d'un Espace Numérique de Santé (ENS) mis à disposition par la Cnam sous la forme du service intitulé Mon espace santé.

Cependant, toute personne qui répond à ces conditions ne dispose pas nécessairement de Mon espace santé. Un usager peut en effet exercer son droit d'opposition et le fermer à tout moment.

Mon espace santé propose un client de messagerie interfacé à l'Opérateur usagers. L'usager peut y accéder à l'aide d'un navigateur internet ou d'une application mobile.

Pour plus de précisions sur les fonctionnalités du client de messagerie de MES et les interactions possibles avec les professionnels, veuillez-vous reporter à la note produite par la Cnam à destination des [MES-EDITEURS].

1.6. Cadre juridique

Au regard de sa finalité, le système MSSanté implique le traitement de données à caractère personnel, dont des données de santé. Il est donc développé et mis en œuvre dans le respect du Règlement européen n°2016/679/UE du 27 avril 2016 (« RGPD »), de la loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et des dispositions du code de la santé publique.

En outre, tout traitement de données à caractère personnel, dont des données de santé, doit être effectué en conformité avec les dispositions du RGPD, de la loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et du code de la santé publique.

Les échanges entre les professionnels habilités et les usagers doivent s'effectuer en conformité avec le cadre juridique général relatif à l'échange de données de santé et au secret professionnel.

En particulier, les échanges de données de santé entre professionnels habilités doivent être réalisés dans les conditions prévues aux articles L. 1110-4 et R. 1110-2 du code précité.

Ces échanges doivent également respecter les articles L. 1470-5 du code de la santé publique, relatifs à l'utilisation de systèmes d'informations conformes aux référentiels de sécurité et d'interopérabilité.

La conservation des données de santé échangées par messagerie MSSanté doit être réalisée dans le respect de l'article L. 1111-8 du code de la santé publique qui impose à toute personne qui héberge des données de santé pour le compte d'un tiers d'être titulaire du certificat de conformité prévu à cet effet.

Les moyens mis en œuvre par les différents acteurs du système MSSanté doivent permettre de garantir la disponibilité, l'intégrité, la confidentialité et l'audibilité des données de santé échangées.

Toute utilisation de l'Identité Nationale de Santé (INS) doit être réalisée en conformité avec le cadre juridique applicable et notamment, le décret n°2019-1036 du 8 octobre 2019 modifiant le décret n°2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé, les articles R. 1111-8-1 et suivants du code de la santé publique et le Référentiel Identifiant National de Santé.

Remarque : le présent Référentiel n'a pas vocation à dresser une liste exhaustive du cadre juridique applicable. Il appartient donc à chaque acteur de veiller à ce que le service de messagerie fourni et/ou utilisé réponde à l'ensemble des obligations légales qui lui incombe.

1.7. Exigences applicables par famille de client de messagerie

Le référentiel comporte 2 types de description des règles de gestion : les exigences et les recommandations. Elles sont identifiées par des pictogrammes spécifiques.

EXIGENCE
Une exigence est une règle de gestion (fonctionnelle ou technique) obligatoire que l'éditeur de client de messagerie MSSanté doit nécessairement implémenter dans son logiciel afin de disposer d'une version compatible MSSanté.

RECOMMANDATION
Une recommandation vise à aider l'éditeur de client de messagerie MSSanté lors de la mise en œuvre ou la maintenance de son logiciel. La mise en œuvre d'une recommandation n'est pas obligatoire.

La version 1.0 du référentiel #2 MSSanté introduit la distinction entre 2 familles de clients de messagerie MSSanté :

- Ceux qui accèdent uniquement à une ou plusieurs **BAL applicatives MSSanté** pour envoyer ou recevoir des messages de façon automatique, sans nécessairement présenter à l'utilisateur une IHM permettant d'afficher ou d'interagir avec les messages,
- Ceux qui accèdent à des **BAL personnelles et/ou organisationnelles** et mettent leurs contenus à disposition de professionnels habilités. Ces logiciels proposent donc nécessairement une IHM permettant d'afficher ou d'interagir avec les messages.

Portée des exigences :

Famille de client de messagerie	**BAL personnelle ou organisationnelle**	**BAL applicative**
Exigences applicables	Voir tableau de synthèse du **§6.1.1** cad toutes les exigences à l'exception de celles définies au **§2.1.1.4**	Voir tableau de synthèse du **§6.1.2** cad toutes les exigences à l'exception de celles définies aux **§2.1.1.3** & **§4**

Pour une liste exhaustive des exigences applicables par famille de LPS se reporter au tableau de synthèse du §6.1.

2. TRANSPORT DES COURRIELS MSSANTE ENTRE OPERATEURS ET CLIENTS DE MESSAGERIES

Une des ambitions principales des référentiels #1 et #2 MSSanté est de généraliser l'usage d'une API commune entre Opérateurs et les clients de messagerie MSSanté.

Toutefois, dans certains contextes particuliers, en complément de cette l'API commune, il est possible d'utiliser une API « propriétaire » telle que décrite au § 2.1.2.

2.1.1. L'API LPS

L'ANS, avec le concours des Opérateurs et des éditeurs de clients de messageries MSSanté, a spécifié l'API LPS afin :

- de permettre à tout professionnel habilité d'utiliser un LPS compatible MSSanté de son choix avec l'Opérateur MSSanté de son choix,
- de standardiser les modes l'identification électronique à utiliser en fonction des types de BAL MSSanté (personnelle, organisationnelle, applicative),
- de proposer une identification électronique des professionnels habilités avec Pro Santé Connect (BAL personnelles et organisationnelles).

Les Opérateurs MSSanté ont l'obligation de l'implémenter via le contrat Opérateurs MSSanté. Le présent paragraphe décrit les modalités d'implémentation de l'API LPS par les éditeurs de clients de messagerie MSSanté.

Comme indiqué dans la figure ci-dessus l'API LPS présentée par les opérateurs MSSanté comporte 2 points d'entrée distincts utilisant tous les 2 les protocoles SMTP et IMAP :

- L'un est dédié à la connexion aux BAL personnelles ou organisationnelles au moyen d'une identification électronique des professionnels habilités via Pro Santé Connect,
- L'autre est dédié à la connexion aux BAL applicatives via une identification électronique de la structure à laquelle est rattachées une BAL applicatives. La connexion se fait via un certificat ORG AUTH_CLI de l'IGC Santé.

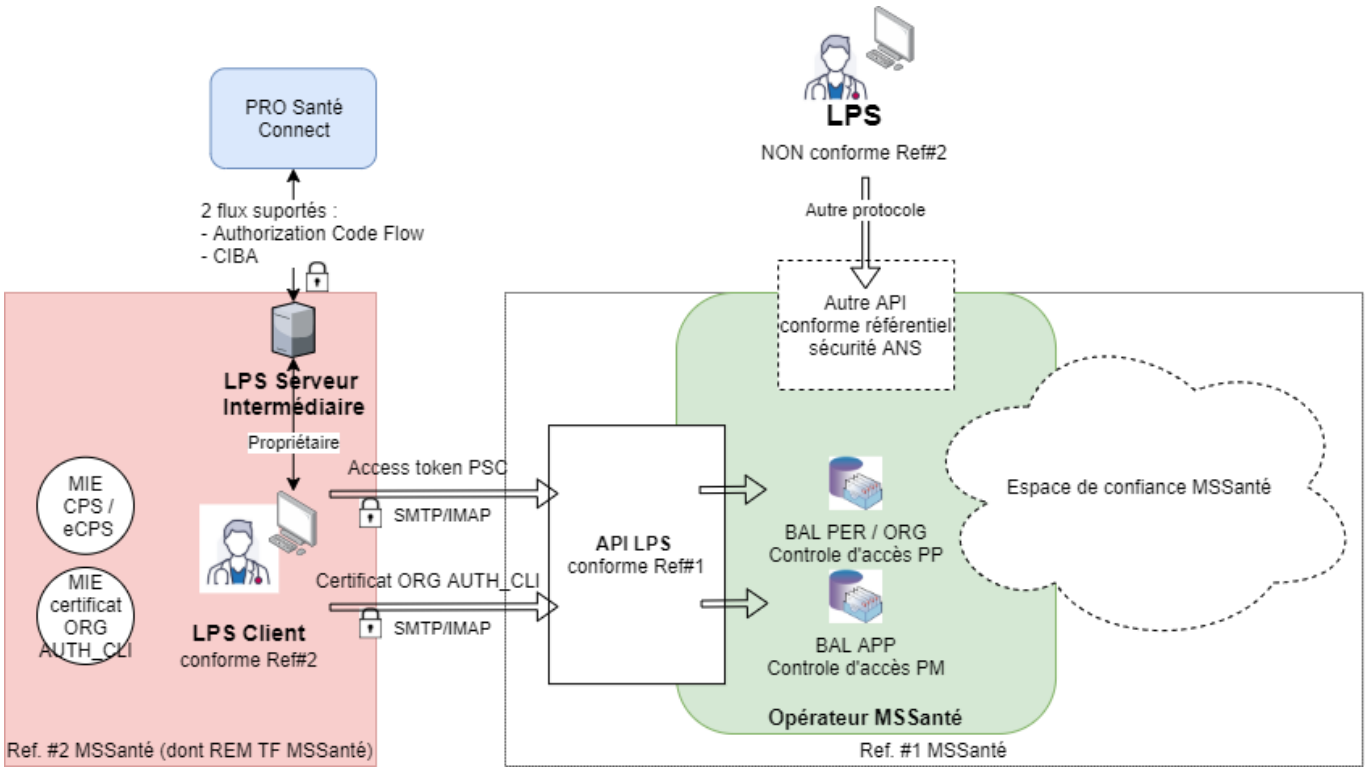

Figure 1 : Vue d'ensemble de l'API LPS

Dans la suite du présent paragraphe, les exigences génériques qui définissent l'API LPS, valables quel que soit le type de BAL et le moyen d'identification électronique utilisés, sont présentées en premier. Sont ensuite décrites les exigences présentant des spécificités pour les BAL personnelles et organisationnelles (avec identification électronique Pro Santé Connect), puis pour les BAL applicatives (avec identification électronique par certificat d'authentification ORG AUTH_CLI).

2.1.1.1. L'API LPS pour les Opérateurs MSSanté

Pour les Opérateurs MSSanté, l'API LPS a été introduite dans la version 1.5 du référentiel #1 Opérateurs [REF1-MSSANTE] publiée en avril 2022. Tout Opérateur doit *a minima* proposer des BAL personnelles et organisationnelles. De manière optionnelle, ils peuvent aussi proposer des BAL applicatives. Quelque soir le type de BAL, l'accès doit pouvoir se faire conformément aux exigences relatives à l'API LPS.

2.1.1.2. Exigences génériques de l'API LPS

2.1.1.2.1. Protocoles de messagerie

Les protocoles de messagerie utilisés par l'API LPS sont les protocoles standards SMTP et IMAP dans leur version sécurisée.

Le référentiel #1 précise que tout Opérateur MSSanté a l'obligation de proposer sur l'API LPS une interface SMTP sur le port 587.

E	**ECO.1.0.1** 
	Le système DOIT disposer d'une interface d'envoi de messages utilisant le protocole SMTP conforme à la RFC 5321 avec STARTTLS comme défini dans le RFC 3207.

Le référentiel #1 précise que tout Opérateur MSSanté a l'obligation de proposer sur l'API LPS une interface IMAP sur le port 143.

E	**ECO.1.0.2** 
	Le système DOIT disposer d'une interface d'accès aux BAL utilisant le protocole IMAP 4 (rev1 ou rev2) conforme respectivement à la RFC 3501 ou RFC 9051 avec STARTTLS comme défini dans la RFC 5246.

2.1.1.2.2. Chiffrement du canal de communication

Afin de garantir un haut niveau de sécurité tout en assurant l'interopérabilité entre Opérateurs et éditeurs, les exigences suivantes doivent être appliquées par les éditeurs de clients de messageries MSSanté.

Le référentiel #1 indique qu'un Opérateur MSSanté doit obligatoirement accepter les connexions TLS 1.2 sur l'API LPS. Il doit refuser la connexion si la version de TLS est inférieure à 1.2. Mais il peut aussi accepter des versions supérieures à 1.2 (sans obligation).

En conséquence, un éditeur de client de messagerie MSSanté doit obligatoirement savoir établir une connexion TLS 1.2, mais peut aussi utiliser une version supérieure de TLS si l'Opérateur la supporte.

E	**ECO.1.1.1** 
	Le système DOIT savoir établir une connexion TLS avec l'API LPS d'un Opérateur MSSanté en utilisant la version TLS 1.2 (RFC 5246) a minima.

R	**ECO.1.1.2** 
	Le système PEUT établir une connexion avec l'API LPS d'un Opérateur MSSanté en utilisant une version de TLS ultérieure à la version 1.2-de TLS (1.3...).

E	**ECO.1.1.3**  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 Opérateur MSSanté : • 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 Pour l'échange des clés de chiffrement TLS, le système DOIT utiliser : • soit le protocole DHE en configurant un groupe DH >= 2048bits, • soit le protocole ECHDE en configurant un groupe elliptique ECDH >= 256 bits. Si l'Opérateur présente des groupes de longueur inférieure, le système doit rejeter la connexion TLS.

.

Cette exigence s'appuie sur les recommandations TLS de l'ANSSI [ANSSI-TLS].

2.1.1.2.3. Vérification du certificat présenté par l'Opérateur MSSanté

Chaque Opérateur MSSanté présente un certificat serveur de l'IGC Santé sur l'API LPS qui lui permet de s'authentifier et de communiquer de façon sécurisée avec les clients de messageries MSSanté. Pour autant, il ne s'agit pas d'une authentification mutuelle car le client de messagerie ne présente pas de certificat.

E	**ECO.1.1.10**  Le système DOIT accepter uniquement un certificat issu de l'IGC Santé gamme Elementaire Organisation lorsqu'il se connecte à une interface API LPS d'un système de messagerie MSSanté.

E	**ECO.1.1.5**  Le système DOIT vérifier que le certificat présenté par l'Opérateur MSSanté n'est pas expiré.

E	**ECO.1.1.6**  Le système MSSanté DOIT vérifier que le certificat présenté par l'Opérateur MSSanté n'est pas révoqué au moyen des CRL ou du répondeur OCSP.

E	**ECO.1.1.7**  Le système DOIT s'assurer de conserver la dernière CRL non expirée, lorsque le contrôle de révocation est réalisé au moyen des CRL, afin d'éviter tout échec de connexion avec l'Opérateur MSSanté en cas d'erreur lors de la récupération de la CRL courante.

2.1.1.2.4. Autoconfiguration

Dans le but d'éviter les erreurs de paramétrage manuel et d'accélérer les procédures de déploiement, un mécanisme d'autoconfiguration est systématiquement proposé par chaque Opérateur MSSanté pour définir les paramètres techniques des points d'entrée de l'API LPS.

Ce mécanisme se présente sous la forme d'un Web Service spécifique nommé AutoConfig (également connu sous le nom AutoConfigure), accessible via l'URL standardisée dédiée, avec un format conforme au `ConfigFileFormat` décrivant les configurations des 2 points d'entrée de l'API LPS (BAL personnelles et organisationnelles, BAL applicatives) : https://wiki.mozilla.org/Thunderbird:Autoconfiguration:ConfigFileFormat.

E	**ECO.1.1.9**  Le système DOIT proposer une fonctionnalité d'autoconfiguration de BAL, soit lors de la configuration de la BAL, soit à la demande, en respectant les étapes ci-dessous : 1 – A partir de l'adresse de la BAL à configurer, consulter l'URL d'autoconfiguration de l'Opérateur MSSanté : **`https://autoconfig.<emailaddressdomain>/mail/config-v1.1.xml`** `(*)` 2 – Configurer automatiquement les paramètres de configuration spécifiques à l'API LPS de l'Opérateur MSSanté proposant la BAL, 3 – Procéder à un test de connexion pour validation de la configuration. * : les opérateurs présentent un certificat serveur de l'IGC Santé ou d'une IGC commerciale usuellement acceptée par les navigateurs Internet.

Tout Opérateur 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'autoconfiguration des BAL, avec un format conforme au ConfigFileFormat décrivant les configurations des 2 points d'entrée de l'API LPS (BAL personnelles et organisationnelles, BAL applicatives).

Un exemple de fichier de configuration mis à disposition par un Opérateur qui présente les protocoles IMAP et SMTP avec les méthodes d'authentification SASL OAuth 2.0 et certificat ORG AUTH-CLI est fourni ci-dessous.

Les éléments apparaissant entre **[ ] et en gras** sont des valeurs que l'Opérateur peut choisir librement.

```
<?xml version="1.0"?>
<clientConfig version="1.1">
    <emailProvider id="[sous domaine Operateur].mssante.fr ">
      <domain>[sous domaine Operateur].mssante.fr</domain>

      <displayName>[Nom complet service Opérateur]</displayName>
      <displayShortName>[Nom court service Opérateur]</displayShortName>

      <incomingServer type="imap">
         <hostname>[front mail psc sous-domaine Opérateur].mssante.fr</hostname>
         <port>143</port>
         <socketType>STARTTLS</socketType>
         <username>%EMAILLOCALPART%</username>
         <authentication>OAuth2</authentication>
      </incomingServer>

      <outgoingServer type="smtp">
         <hostname>[front mail psc sous domaine-Opérateur].mssante.fr</hostname>
         <port>587</port>
         <socketType>STARTTLS</socketType>
         <username>%EMAILLOCALPART%</username>
         <authentication>OAuth2</authentication>
      </outgoingServer>

      <incomingServer type="imap">
         <hostname>[front mail authcli sous domaine Opérateur].mssante.fr</hostname>
         <port>143</port>
         <socketType>STARTTLS</socketType>
         <username>%EMAILLOCALPART%</username>
         <authentication>TLS-client-cert</authentication>
      </incomingServer>

      <outgoingServer type="smtp">
         <hostname>[front mail authcli sous domaine Opérateur].mssante.fr</hostname>
         <port>587</port>
         <socketType>STARTTLS</socketType>
         <username>%EMAILLOCALPART%</username>
         <authentication>TLS-client-cert</authentication>
      </outgoingServer>

    </emailProvider>
</clientConfig>
```

2.1.1.3. Exigences spécifiques aux BAL personnelles et organisationnelles

Les exigences présentes dans ce paragraphe ne s'appliquent qu'aux éditeurs qui se connectent à des BAL personnelles et organisationnelles qui ont la particularité de s'appuyer sur Pro Santé Connect (PSC) comme unique moyen d'identification électronique.

2.1.1.3.1. Architecture d'identification électronique

Les 2 figures suivantes présentent les 2 alternatives d'architecture d'identification électronique via l'API LPS qu'il est possible de rencontrer côté client de messagerie (Client Lourd et SaaS) pour les BAL personnelles et organisationnelles.

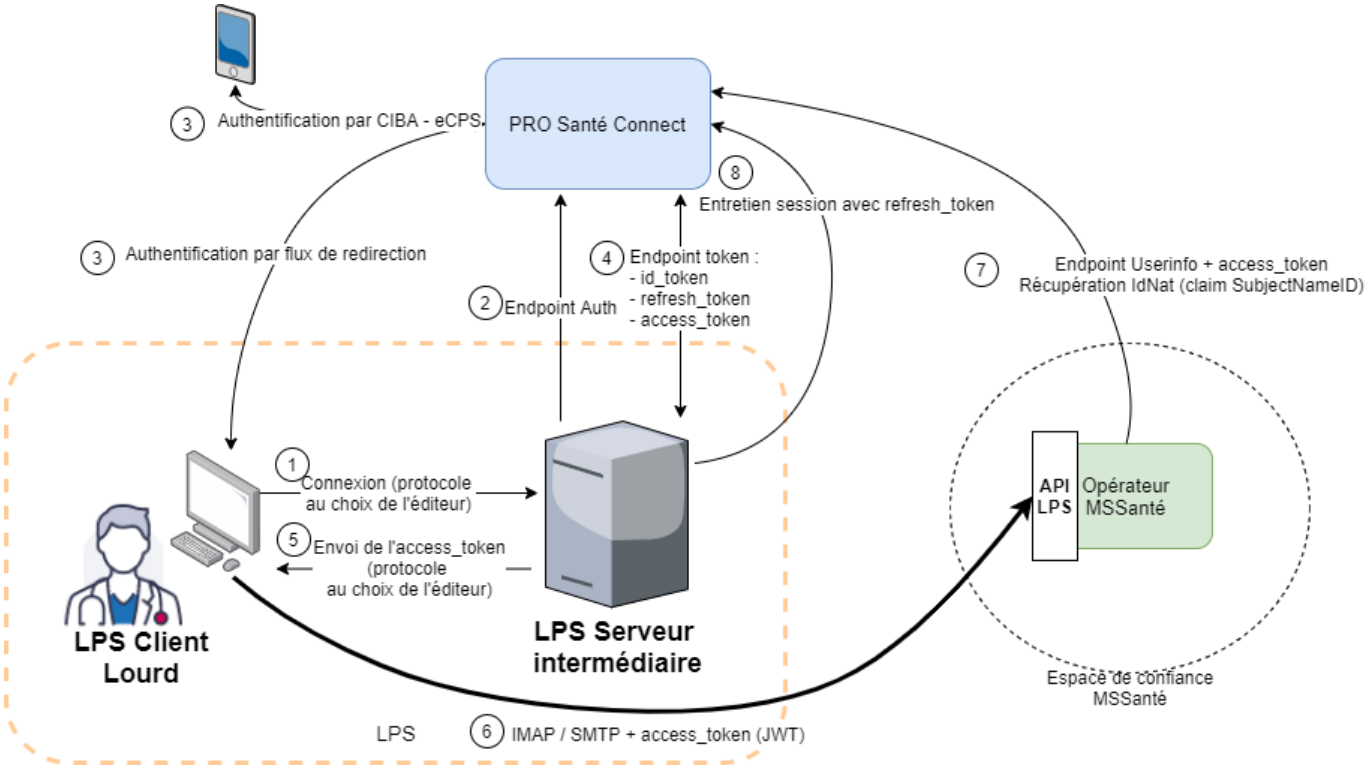

Figure 2 : Authentification sur l'API LPS pour BAL personnelles et organisationnelles avec un LPS Client Lourd

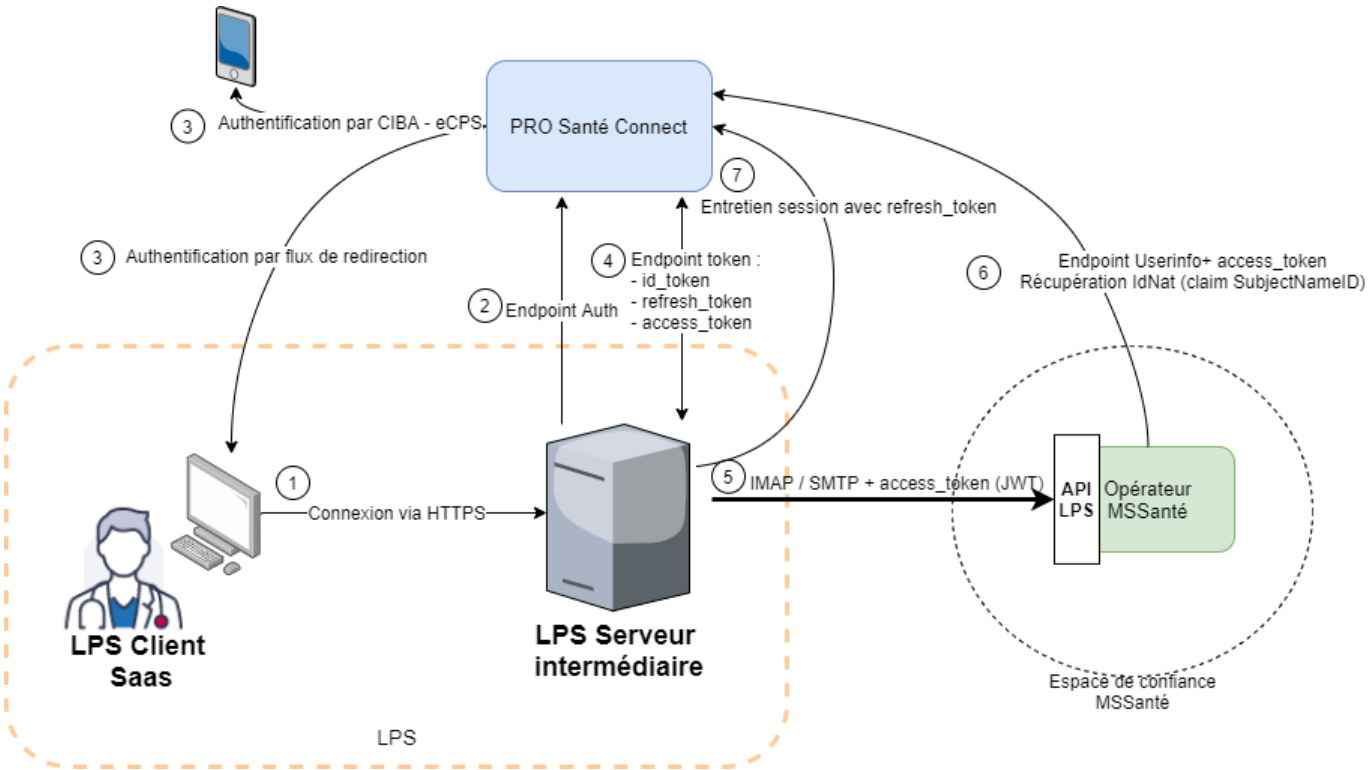

Figure 3 : Authentification sur l'API LPS pour BAL personnelles et organisationnelles avec un LPS SaaS

Ces figures permettent d'indiquer que :

- quel que soit le type de client de messagerie utilisé, la mise en place d'un serveur LPS intermédiaire est nécessaire pour assurer les échanges auprès de PSC (il n'est en effet pas envisageable que chaque client

lourd sollicite unitairement PSC, car un enregistrement de chaque client de PSC est nécessaire). Les communications entre le serveur LPS intermédiaire et le serveur PSC (fournisseur d'identités) utilisent les technologies Web (HTTPS) et le standard Open ID Connect (OIDC).

- PSC offre 2 moyens distincts pour confirmer l'identification électronique d'un professionnel (étape 3) :
  - soit utilisation du flux de redirection qui passe par une mire de connexion PSC. Elle implique l'utilisation d'un flux Web et la connexion par CPS ou eCPS sur le LPS),
  - soit le mécanisme CIBA qui permet une identification électronique sur le terminal contenant la eCPS. Le support de la CPS est prévu fin 2022.
- c'est l'Access Token récupéré après identification électronique auprès de PSC qui doit être transmis à l'Opérateur MSSanté au moyen du mécanisme d'authentification SASL OAuth 2.0.

A noter que le reste du chapitre ne présente que la partie communication entre le client de messagerie et le serveur de messagerie de l'Opérateur, cette communication se faisant avec les protocoles de messagerie standard SMTP et IMAP.

Ainsi, la partie identification électronique avec PSC n'est pas présentée plus en détails dans le présent document. Toute la documentation et le processus nécessaires pour que le client de messagerie d'un éditeur puisse utiliser PSC est accessible sur [PSC-REF].

L'utilisation de PSC pour l'identification électronique peut amener un éditeur à devoir faire évoluer l'architecture de sa solution de LPS, du fait de la nécessité de la mise en place du serveur LPS intermédiaire tel que présenté sur les 2 figures précédentes. A noter que dans le cas d'un LPS installé dans une structure de type établissement de santé, les fonctions assurées par ce serveur intermédiaire peuvent déjà exister dans la structure. Dans ce cas, le LPS pourraient s'y connecter sans les implémenter lui-même.

2.1.1.3.2. Gestion de l'identification électronique

Le client de messagerie MSSanté doit disposer d'un Access Token PSC valide afin de permettre l'identification électronique d'un professionnel habilité sur un service de messageries MSSanté.

E	**ECO.1.2.1**  Le système DOIT réaliser des demandes d'ouverture de connexion SMTP et IMAP sur l'interface BAL personnelle ou organisationnelle de l'API LPS d'un Opérateur MSSanté en respectant la cinématique suivante : 1- Ouvrir la session TLS avec STARTTLS 2- Réaliser une authentification du PS via le mécanisme SASL OAuth 2.0, en envoyant le mot clé AUTHENTICATE XOAUTH2 pour IMAP ou AUTH XOAUTH2 pour SMTP avec la chaine de caractères encodée en base64 contenant à la fois l'adresse de la BAL dans le champ « user » et l'Access Token PSC au format JWT. Le formatage de cette chaine de caractères est le suivant : • Chaine fixe : "`user=`", • Adresse mail de la BAL, • Chaine fixe : "`^Aauth=Bearer` " (avec un espace à la fin), • Access Token PSC, • Chaine fixe : "`^A^A`". 3- Attendre la validation de la connexion IMAP ou SMTP par l'Opérateur MSSanté utilisé 4- Envoyer les commandes SMTP ou IMAP

Exemple de chaine de caractères envoyée à l'étape 2 :

```
user=jean.dupond@medecin.mssante.fr^Aauth=Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJBV19DTUZjaUYtQUMyeGlTdHUtNiIsImF1ZCI6WyJzZzQ4Q
2RBWW9oUlBlUldaOWoxSCJdLCJhdXRoX3R5cGUiOiJwYXNzd29yZCIsIm5ld191c2VyIjp0cnVlLCJlbWFpbF92ZXJpZml
lZCI6ZmFsc2UsInVwZGF0ZWRfYXQiOiIyMDIwLTAxLTIwVDA5OjAyOjI1Ljk1NVoiLCJjdXN0b21fZmllbGRzIjp7fSwiY
XV0aF90aW1lIjoxNTc5NTEwOTQ1LCJpc3MiOiJodHRwczovL2xvY2FsLXNhbmRib3gub2c0Lm1lIiwiZXhwIjoxNTc5NTk
3MzQ1LCJpYXQiOjE1Nzk1MTA5NDUsImVtYWlsIjoiZ2l2ZXJhbmRvbXRva2VuNEByZWFjaDUuY28ifQ.kR0RRpNi4gFPUE
OwuR1Tilx4imYjM1Owrbrtw6liZv0^A^A
```

avec ^A représente le caractère Contrôle + A (\001).

Pour implémenter la gestion des erreurs lors de l'identification électronique via l'API LPS, le client de messagerie MSSanté peut s'appuyer sur les réponses types retournées par les opérateurs :

- 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, conformément au RFC 4954 (https://datatracker.ietf.org/doc/html/rfc4954#section-6)

E	**ECO.1.2.3** 
	Le système DOIT traiter les erreurs techniques rencontrées lors du processus de connexion et d'authentification SMTP/IMAP de sorte qu'elles ne perturbent pas les autres fonctions de l'application (hors messagerie).

La capacité SASL-IR permet le passage de l'Access Token en une commande au lieu de deux. Cela évite un aller-retour entre le client et le serveur de messagerie.

R	**ECO.1.2.4** 
	Lors d'une connexion IMAP, le système PEUT utiliser la capability SASL-IR pour transmettre l'Access Token en une seule transaction comme défini dans le RFC 4959.

E	**ECO.1.2.5** 
	Pour des raisons de sécurité, l'Access Token PSC au format JWT ne doit pas être stocké de façon permanente sur le poste de travail du professionnel. Il doit être mémorisé de façon temporaire, pour une durée correspondant à sa durée de vie. Ainsi, lors de l'utilisation d'un Client Lourd, le moyen de mémorisation de l'Access Token PSC doit être protégé des accès et attaques externes. Le niveau de sécurisation utilisé pour la mémorisation temporaire doit être éprouvée.

La gestion de la durée de vie du jeton Refresh Token (qui définit une durée maximale d'une authentification auprès de PSC) est de la responsabilité du LPS, car c'est le serveur intermédiaire du LPS qui a reçu ce token (qu'il ne doit partager avec personne).

Pour cette raison, pour éviter d'avoir à redemander une identification électronique au PS à la fin de la durée de vie du Refresh Token et comme le Refresh Token (et donc l'identification électronique PSC) devient invalide au bout de sa durée de vie, c'est au LPS (en l'occurrence au serveur intermédiaire du LPS) de redemander la génération

d'un Access Token et un nouveau Refresh Token juste avant que la fin de la durée de vie du Refresh Token courant ne soit atteinte.

Le renouvellement du Refresh Token est limité à la durée maximale d'une session et PSC finira par clore la connexion (durées maximales d'expiration identifiées ici : https://industriels.esante.gouv.fr/produits-services/pro-sante-connect/documentation-technique). Dans ce cas, pour assurer la sécurité de MSSanté, le LPS doit déclencher de lui-même la fin de la connexion SMTP / IMAP auprès du serveur de messagerie de l'Opérateur.

E	**ECO.1.2.6** 
	Dès que le Refresh Token PSC de l'utilisateur connecté devient invalide (durée de vie maximale atteinte, déconnexion PSC, ...), le système DOIT déclencher la fin de session IMAP et SMTP avec le serveur de messagerie.

Dans le cas de l'utilisation d'un Client Lourd, le Refresh Token n'est connu que du serveur intermédiaire LPS. Aussi, un mécanisme de communication doit être mis en place pour que le Client Lourd soit informé par le serveur intermédiaire LPS, que le Refresh Token est devenu invalide. Ainsi le Client Lourd peut déclencher la fin de session.

Dans certains cas, une fin de session SMTP / IMAP pourra être déclenchée par le serveur de messagerie de l'Opérateur. Par exemple : si une certaine durée d'inactivité est atteinte, si la durée maximale de session SMTP / IMAP paramétrée au niveau du serveur est atteinte. Dans ce cas, si les conditions d'une reconnexion automatique au serveur de messagerie de l'Opérateur sont remplies, cette reconnexion doit avoir lieu.

E	**ECO.1.2.7** 
	Suite à la détection d'une fin de session IMAP ou SMTP déclenchée par l'Opérateur MSSanté, lorsque l'authentification PSC est toujours valide, le système DOIT pouvoir réouvrir automatiquement (i.e. sans intervention humaine) une session IMAP ou SMTP

Pour procéder à cette réouverture, deux cas possibles :

1. Si l'Access Token est valide (i.e. qu'il est non expiré) :
   Il suffit de procéder à la réouverture de la session SMTP / IMAP. Dans le cas de l'utilisation d'un Client Lourd, ce token est mémorisé temporairement au niveau de ce client.
2. Si l'Access Token est invalide et le Refresh Token est valide (i.e. qu'il est non expiré) :
   Le serveur intermédiaire LPS doit redemander un Access Token valide à PSC, qui sera transmis à la réouverture de la session SMTP / IMAP. Dans le cas de l'utilisation d'un Client Lourd, le nouveau token doit être transmis du serveur intermédiaire LPS vers le Client Lourd.

2.1.1.4. Exigences spécifiques aux BAL applicatives

Les exigences présentes dans ce paragraphe ne s'appliquent qu'aux éditeurs qui se connectent à des BAL applicatives. L'unique moyen d'identification électronique proposé est un certificat d'authentification ORG-CL-AUTH_CLI prévu par l'API LPS.

2.1.1.4.1. Architecture d'identification électronique

La figure suivante présente l'architecture d'identification électronique de l'API LPS dans le cas des BAL applicatives.

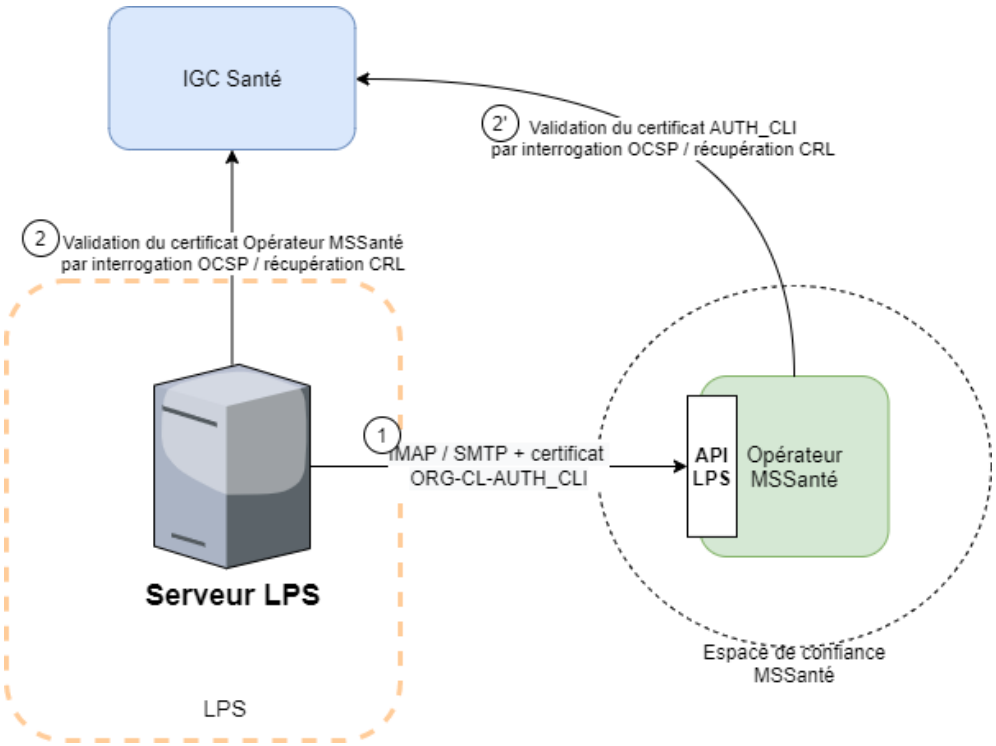

Figure 4 : Identification électronique sur API LPS pour BAL applicatives

2.1.1.4.2. Gestion de l'identification électronique

E	**ECO.1.3.1** 
	Le système DOIT réaliser des demandes d'ouverture de connexions SMTP et IMAP sur l'interface BAL applicative de l'API LPS d'un Opérateur MSSanté en respectant la cinématique suivante : 1- Monter la session TLS avec STARTTLS en présentant un certificat ORG AUTH_CLI à l'Opérateur MSSanté utilisé comme défini dans la RFC 5246, 2- Transmettre l'adresse de la BAL dans le login de la méthode d'authentification PLAIN comme défini dans la RFC 3501 ou RFC 9051, 3- Envoyer les commandes SMTP ou IMAP.

Le certificat ORG AUTH_CLI doit contenir l'IdNat de la structure détentrice de la BAL applicative dans le champ OU du DN du certificat.

2.1.2. Interfaces complémentaires entre Opérateurs et clients de messagerie MSSanté

Les Opérateurs MSSanté et les éditeurs de clients de messagerie MSSanté doivent obligatoirement implémenter l'API LPS conformément aux référentiels #1 et #2 MSSanté. En complément de ces interfaces interopérables, les Opérateurs peuvent proposer d'autres interfaces. C'est par exemple le cas lorsqu'une structure utilise des clients de messagerie standards du marché non intégrés à un logiciel métier (type Microsoft Outlook).

En complément de l'API LPS, un client de messagerie MSSanté peut se connecter à un Opérateur MSSanté exposant des interfaces propriétaires, dans la mesure où ces dernières sont conformes avec le référentiel d'identification électronique de la PGSSI-S [PG-REF-IDENT] et à l'état de l'art en termes de sécurisation des flux de données (voir en particulier [ANSSI-TLS] et [ANSSI-CRYPTO]).

3. STANDARDISATION DES COURRIELS MSSANTE

Ce chapitre décrit l'ensemble des exigences que doivent respecter les éditeurs de clients de messageries MSSanté pour produire ou recevoir des messages MSSanté.

3.1. Transmission de documents de santé d'un usager

L'arrêté du 26 avril 2022, pris en application de l'article L. 1111-15 du code de la santé publique, fixe la liste des documents de santé devant être transmis par une messagerie sécurisée au médecin traitant, au médecin prescripteur s'il y a lieu, ainsi qu'à tout professionnel dont l'intervention dans la prise en charge du patient est pertinente ainsi qu'aux usagers concernés. Ce paragraphe détaille, dans le cadre du système MSSanté, les exigences à respecter lorsque le message contient un ou plusieurs de ces documents de santé.

3.1.1. Fichiers en pièces jointes d'un message

Lors de la réception d'un message provenant d'un professionnel contenant un (des) document(s) de santé, le destinataire doit pouvoir :

- Intégrer dans le dossier usager du LPS le(s) document(s) CDA contenu(s) dans l'archive IHE_XDM,
- En prendre directement connaissance sans avoir besoin d'un LPS (cas d'un webmail ou d'une application mobile) grâce au(x) fichier(s) PDF. Ces derniers n'ont pas vocation à être intégrés dans le LPS.

E	**ECO.2.1.1** 

	Un courriel MSSanté utilisé pour transmettre un (des) document(s) de santé DOIT :
	• Concerner qu'un seul et même usager,
	• Contenir en pièces jointes du courriel :
	  ○ une archive ZIP au format IHE_XDM contenant **un ou plusieurs** documents CDA R2 niveau 1 et/ou niveau 3 (suivant les spécifications du volet échange de documents de santé [CI-ECH-DOC]),
	  ○ les mêmes documents médicaux au format PDF/A-1.

E	**ECO.2.1.5** 

	Chaque PDF/A-1 rattaché au courriel MSSanté DOIT être **généré à partir du ou des documents CDA correspondants contenus dans l'archive ZIP au format IHE_XDM** :
	- Cas d'un document CDA R2 N3, le PDF/A-1 doit comporter :
	  ○ les données suivantes de l'entête CDA : Titre, Type de document, Date et heure de création, Auteur / Responsable du document, Organisation conservant le document,
	  ○ une transcription fidèle du contenu clinique porté dans la partie narrative de chaque section du document CDA qui a été validé par le responsable du document CDA.
	- Sinon le PDF/A-1 doit être identique au PDF encapsulé dans le CDA R2 N1.

Par rapport au volet échange de documents de santé [CI-ECH-DOC] aucune normalisation complémentaire n'est imposée sur le nom des documents xml au format CDA.

Dans le cas d'un message provenant d'un usager via la messagerie de MES, le système peut proposer l'intégration des pièces jointes (PDF, bureautique, …) dans le dossier patient de l'usager.

E	**ECO.2.1.6** 
	Les fichiers au format PDF présents en pièce jointe DOIVENT respecter la convention de nommage suivante, afin de faciliter l'identification des documents de santé : <date de l'acte>_<type document>_<NOM>_<prenom>_<numéro de dossier>.pdf Tous les champs sont obligatoires à l'exception du champ <numéro de dossier> qui est optionnel.

Avec :

- <date de l'acte> : date à laquelle l'acte a été réalisé (AAAAMMJJ) : correspond à la valeur de `documentationOf/serviceEvent/effectiveTime/low` de l'élément d'en-tête CDA ou à la métadonnée XDS: `serviceStartTime` du document en pièce jointe.
- « _ » : caractère underscore (ASCII - décimal 95) ;
- <type document> : attribut `displayName` de l'élément `code` de l'en-tête CDA ou métadonnée XDS `typeCodeDisplayName` du document en pièce jointe. Pour une meilleure lisibilité du nom de la pièce jointe, ce libellé doit être tronqué à 40 caractères, si sa longue est supérieure,
- « _ » : caractère underscore (ASCII - décimal 95) ;
- <NOM> est le nom de naissance de l'usager **en majuscule**, si disponible sinon renseigner avec le nom usuel, champ obligatoire ;
- « _ » : caractère underscore (ASCII - décimal 95) ;
- <prenom> est le prénom de l'usager,
- « _ » : caractère underscore (ASCII - décimal 95) ;
- <numéro de dossier> est un numéro d'identification propre à l'émetteur et partagé avec le destinataire. Pour les comptes rendus d'examens de biologie, il correspond au numéro d'enregistrement de la prescription initiale reçue par le laboratoire principal.

Exemples de nommage :

Exemple 1:* Cas d'un document contenu dans l'IHE_XDM.ZIP au format CDA R2 avec taille du <type document> inférieure à 40 caractères*:

- code@displayName : CR d'examens biologiques
- Numéro de dossier = numéro d'enregistrement de la prescription initiale : « 12150302014578 »
- =>Nommage pdf : 20150802_CR d'examens biologiques_VIAL_Paul_12150302014578.pdf

Exemple 2:* Cas d'un document contenu dans l'IHE_XDM.ZIP au format CDA R2 avec taille du <type document> supérieure à 40 caractères *:

- code@displayName : Lettre de liaison à la sortie d'un établissement de soins
- Libellé : Lettre de liaison à la sortie d'un établ
- *=>Nommage pdf : 20150802_Lettre de liaison à la sortie d'un établ_VIAL_Paul.pdf*

***Exemple 3:* Cas d'un document contenu dans l'IHE_XDM.ZIP au format CDA R2**

- code@displayName : CR d'anesthésie
- Libellé : CR d'anesthésie
- =>Nommage pdf : *20150802_CR d'anesthésie_VIAL_Paul*.pdf

3.1.2. Transmission de l'identité de l'usager

Les données d'identité de l'usager (matricule INS, OID, traits d'identité) sont présentes dans le ou les documents de santé transmis en pièces jointes. Le client de messagerie MSSanté émetteur n'a pas besoin de dupliquer ces données d'identité ailleurs dans le courriel.

E	**ECO.2.1.2** 
	Pour identifier l'usager concerné par un courriel, le système destinataire DOIT se référer à la métadonnée `patientId` (matricule INS) contenu dans le fichier METADATA.XML du document CDA contenu dans la pièce jointe IHE_XDM.zip du courriel.

Le statut de l'identité INS (qualifié, …) n'est pas transmis dans le courrier. On considère que **l'identité INS de l'usager** est **« qualifiée » par l'émetteur du courrier si le document reçu en pièce jointe contient le matricule INS et son OID.**

3.1.3. Format de l'objet d'un courriel MSSanté

L'objet du courriel doit permettre :

- Au client de messagerie MSSanté réceptionnant un courriel MSSanté, d'identifier automatiquement s'il contient les documents de santé en pièces jointes au format défini dans le présent référentiel,
- Au professionnel habilité, destinataire du courriel, d'identifier le type de document et l'usager concerné sans devoir nécessairement ouvrir la ou les pièces jointes.

Selon les recommandations du profil IHE-XDM et du volet échange du CI-SIS [CI-ECH-DOC], l'objet du courriel doit débuter par la chaine de caractères non significative "XDM/1.0/DDM", suivi du caractère séparateur "+", lui-même suivi d'une chaîne de caractères significative dont le contenu et la structuration doivent respecter le formalisme ci-dessous :

E	**ECO.2.1.3** 
	L'objet du courriel DOIT respecter le format suivant : XDM/1.0/DDM+<libellé> <NOM> <prenom> <date de naissance> Tous les champs sont obligatoires à l'exception du champ <date de naissance> qui est optionnel.

Les détails du format sont les suivants :

- « XDM/1.0/DDM » : précise que le message contient des documents de santé respectant la standardisation du CI-SIS ;
- « + » : caractère séparateur (caractères ASCII - décimal 43) ;
- <libellé> :
  - Si **un et un seul document CDA joint** :
    Le type de document CDA correspondant à l'attribut `displayName` de l'élément `code` de l'en-tête CDA ou à la métadonnée XDS `typeCodeDisplayName` du document en pièce jointe. Pour une meilleure lisibilité de l'objet, le libellé doit être tronqué à 40 caractères, si sa longue est supérieure.
  - Si **plusieurs documents CDA joints de type différents** :
    La chaîne de caractères `N documents`, où N est le nombre de documents CDA présents dans l'archive IHE XDM jointe au courriel MSSanté.
- « » : caractère séparateur (caractères ASCII « espace » - décimal 32) ;
- <NOM> : nom de naissance de l'usager **en majuscule** (si disponible sinon renseigner avec le nom usuel) ; Reprendre le contenu des entêtes du document CDA. Conformément au [INS-RNIV], le nom sera en caractères majuscules non accentués, sans signe diacritique et sans abréviation,
- « » : caractère séparateur (caractères ASCII « espace » - décimal 32) ;
- <prenom> : prénom de l'usager; Reprendre le contenu des entêtes du document CDA. Conformément au [INS-RNIV], le prénom sera en caractères majuscules non accentués, sans signe diacritique et sans abréviation,
- « » : caractère séparateur (caractères ASCII « espace » - décimal 32) ;
- <date de naissance> est la date de naissance de l'usager (format calendaire ou lunaire accepté, JJ/MM/AAAA); Reprendre le contenu des entêtes du document CDA.

Exemples de nommage de l'objet :

Exemple 1 **: Cas d'un seul document joint au format CDA R2 niveau 3 (structuré) avec taille du <libellé typeCode> inférieure à 40 caractères**

- code@displayName : CR d'examens biologiques
- Libellé : CR d'examens biologiques
- => Objet : XDM/1.0/DDM+CR d'examens biologiques VIAL Paul 26/11/1978

Exemple 2 **: Cas d'un seul document joint au format CDA R2 niveau 3 (structuré) avec taille du <libellé typeCode > supérieure à 40 caractères**

- code@displayName : Lettre de liaison à la sortie d'un établissement de soins
- Libellé : Lettre de liaison à la sortie d'un établ
- => Objet : XDM/1.0/DDM+Lettre de liaison à la sortie d'un établ VIAL Paul 26/11/1978

Exemple 3 **: *Cas de deux* documents joints (CR d'examens biologiques et VSM)**

- Libellé : 2 documents
- => Objet : XDM/1.0/DDM+2 documents VIAL Paul 26/11/1978

Exemple 4 **: Cas de trois documents joints (CR d'examens biologiques, VSM et CR d'anesthésie)**

- Libellé : 3 documents
- =>Objet : XDM/1.0/DDM+3 documents VIAL Paul 26/11/1978

3.2. Support du mode conversation

Pour que les clients de messageries qui le souhaitent puisse présenter les courriels MSSanté sous forme de conversation (comme le client de messagerie de Mon espace santé), tous les clients de messageries MSSanté doivent respecter les exigences suivantes :

E	**ECO.2.2.1**
	Le système DOIT renseigner l'entête « Message-ID » conformément à la RFC 5322 dans tout nouveau courriel produit.

E	**ECO.2.2.2**
	Le système DOIT renseigner les entêtes « `Message-ID` », « `in-Reply-To` » et « `References` » conformément à la RFC 5322 dans toute réponse à un courriel.

3.3. Corps du courriel

3.3.1. Encodage

Pour que l'affichage des messages au format texte soit correctement restitué aux destinataires, il est important que l'émetteur MSSanté utilise toujours l'encodage UTF-8.

E	**ECO.2.2.3** 
	Le système MSSante DOIT utiliser l'encodage UTF-8 pour les parties `text` du corps des courriels.

Exemples d'entêtes de message :

```
Content-Type: text/plain; charset=utf-8
```

```
Content-Type: text/html; charset=utf-8
```

3.3.2. Format des courriels

Le corps des courriel MSSanté peuvent utiliser une présentation au format HTML. Mais dans ce cas, afin d'assurer l'interopérabilité avec des clients de messageries qui ne supporteraient pas le rendu HTML, le contenu du corps du courriel doit aussi être disponible au format texte brut.

E	**ECO.2.2.4** 

	Le corps du courriel indiqué dans entête `Content-Type` du courriel, doit être :
	• Soit `text/plain`, c'est-à-dire en texte brut sans formatage,
	• Soit `multipart/alternative` avec 2 parties identiques en termes de contenu rédactionnel:
	  o La première en `text/plain`,
	  o La seconde en `text/html`.

Pour plus de précisions se référer à la RFC2046 (multipart/alternative).

Exemple :

```
…
Date: xxx
From: xxx@xxx.mssante.fr
Message-ID: xxxx
Subject: xxxx
MIME-Version: 1.0
Content-Type: multipart/alternative;
------=_Part_1_xxxxx
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
xxxxxxxxx
------=_Part_2_xxx
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
<html>xxxx</html>
…
```

3.3.3. Cas des courriels envoyés par une BAL applicative

Pour des courriels envoyés depuis une BAL personnelle ou organisationnelle, aucune exigence particulière ne porte sur le contenu du corps du courriel. Le contenu est laissé à l'appréciation de l'émetteur du courriel.

Lors d'un envoi de courriels depuis des BAL applicatives (par exemple depuis des DPI, SIL, …), l'émetteur du message doit proposer aux destinataires du courriel un moyen de contacter l'émetteur via un courriel MSSanté.

Par ailleurs pour rappel, le référentiel #1 Opérateurs de Messageries Sécurisées de Santé impose que les BAL applicatives puissent recevoir des messages techniques de type « bounce ».

L'utilisateur d'une BAL applicative, utilisée en émission, doit disposer d'une BAL personnelle ou organisationnelle destinée à recevoir et traiter les messages des professionnels habilités ou usagers qui souhaiteraient contacter l'émetteur d'un courriel envoyé depuis une BAL applicative.

E	**ECO.2.2.5**  Un courriel envoyé depuis une BAL applicative doit : • Contenir une mention à la fin du message précisant que le message a été généré automatiquement et en indiquant une adresse de BAL MSSanté personnelle ou organisationnelle permettant de contacter l'émetteur, • Positionner un entête « Reply-To » contenant l'adresse de cette BAL personnelle ou organisationnelle.

Le système définit l'entete « Reply-To » en fonction d'un paramétrage donné par l'utilisateur de la BAL applicative. Il n'est pas en mesure de contrôler le type de BAL paramétré.

3.4. Destinataires d'un courriel

3.4.1. Professionnels habilités destinataires d'un courriel

La notion de « professionnel habilité » désigne tout professionnel de santé ou non professionnel de santé des secteurs social et médico-social mentionné à l'article L.1110-4 du code de la santé publique et autorisé à collecter, échanger et partager **des données de santé à caractère personnel relatives à un usager pour lequel il intervient dans la prise en charge**.

La liste de ces professionnels a été définie à l'article R.1110-2 2° du code de la santé publique.

Toutes les BAL MSSanté créées par les Opérateurs MSSanté, à l'exception des BAL utilisées par les usagers, sont déclarées dans l'Annuaire Santé et rattachées aux identités des personnes physiques ou morales présentes dans l'Annuaire Santé.

Les clients de messageries disposent de 3 méthodes pour rechercher une adresse MSSanté dans l'Annuaire santé :

1. Interface LDAP afin d'effectuer en interactif des recherches de BAL, voir [AS-LDAP-MSS].
2. Extraction publique des données de l'annuaire afin de constituer un annuaire local synchronisé avec l'annuaire national, voir [AS-EXTRAC-LIBRE],

3. Interface FIHR, nouveau service permettant d'exposer des données des référentiels Personnes physiques/Personnes morales au format JSON, structurées selon le standard d'interopérabilité FHIR, voir [AS-API-FIHR].

3.4.2. Usager destinataire d'un courriel

3.4.2.1. Existence et format des adresses usagers

L'intégralité des personnes couvertes par les régimes obligatoires de l'Assurance Maladie, ainsi que tout usager du système de soins disposant d'un INS ou bénéficiant de l'AME (Aide Médicale d'Etat), peuvent disposer de MES mis à disposition par la Cnam.

Cependant, toute personne qui répond à ces conditions ne dispose pas nécessairement de MES et d'une adresse de messagerie usager MSSanté. En effet, conformément aux articles R. 1111-26 et suivants du code de la santé publique, un usager peut s'opposer à la création de MES, et peut par ailleurs demander sa fermeture à tout moment.

L'existence d'un compte MES et d'une BAL usager n'est donc pas garantie. Etant précisé qu'il n'existe pas d'annuaire « usagers » dans l'Espace de Confiance permettant de contrôler l'existence d'une BAL usager.

À la création de Mon espace santé, une adresse de messagerie usager MSSanté est automatiquement attribuée à l'usager et rattachée à Mon espace santé. Cette adresse est constituée à partir du matricule INS de l'usager et du nom de domaine de l'Opérateur de Mon espace santé, selon le format suivant :

<matricule INS de l'usager>`@patient.mssante.fr`

Pour rappel le matricule INS est constitué du NIR ou NIA et d'une clé de contrôle. Il comporte 15 caractères alphanumériques.

3.4.2.2. Usage des adresses usagers en destinataire de courriels

L'adresse de messagerie d'un usager ne pouvant être vérifiée ou obtenue depuis un annuaire national, elle doit être produite à partir du matricule INS de l'usager. Seule une identité INS au statut « qualifiée » apporte les garanties suffisantes pour construire une adresse de messagerie usager et transmettre des documents de santé à un usager.

E	**ECO.2.2.6** 
	Un système, **qui envoie des courriels MSSanté à des usagers,** DOIT utiliser des adresses usagers construites à partir d'Identités Nationale de Santé « qualifiées ».

Dérogation valable jusqu'à fin 2023 (renouvelable [1]) :

Dans le cas où un client de messagerie MSSanté ne disposerait pas de l'INS qualifiée pour construire une adresse usager, il peut utiliser une adresse MSSanté usager :

- soit construite à partir du NIR bénéficiaire préalablement connu du client de messagerie MSSanté,
- soit saisie par le professionnel habilité.

[1] Dérogation valable a minima jusqu'à fin 2023, puis renouvelable jusqu'à sa révocation qui sera annoncée dans une future version de ce présent référentiel.

Pour sécuriser l'envoi du courriel au bon destinataire usager, le client de messagerie doit mettre en œuvre des contrôles complémentaires avant envoi du courrier :

- vérification de la clé de contrôle du numéro utilisé en guise de matricule INS (afin d'alerter au plus tôt le professionnel sur une saisie erronée, qui empêchera la transmission du courriel à son destinataire),
- message d'alerte demandant au professionnel de confirmer l'identité de l'usager en affichant sa date de naissance et son sexe. Ces informations peuvent être déduites du numéro utilisé en guise de matricule INS (afin d'alerter le professionnel sur une éventuelle incohérence entre l'usager qu'il souhaite contacter et celui à qui il s'apprête à transmettre un courriel).

3.4.2.3. Interdire la réponse d'un usager via Mon espace santé

Comme décrit dans la spécification de Mon espace santé pour les éditeurs de LPS [MES-EDITEURS], MES propose une fonctionnalité permettant à un usager d'écrire à un professionnel habilité sur sa BAL MSSanté.

L'envoi d'un message par un professionnel habilité à un usager donné, permet à ce dernier de lui envoyer des messages sans limitation dans le nombre de réponses et sans limite de temps.

Lorsqu'un professionnel habilité souhaite retirer la possibilité à un usager de lui envoyer des messages, il doit en informer MES en utilisant la méthode décrite ci-dessous.

E	**ECO.2.2.8** 
	Le système DOIT pouvoir positionner un entête SMTP "`X-MSS-MES`", dans les messages envoyés vers un usager (Mon espace santé), avec la valeur "`FIN`" (3 caractères en majuscules), lorsque le professionnel émetteur ne souhaite pas que l'usager puisse lui répondre en retour.

Pour plus de précisions concernant ce dispositif, se référer à la spécification de Mon espace santé pour les éditeurs de LPS [MES-EDITEURS].

3.5. Expéditeur d'un courriel

Afin de faciliter l'identification de l'expéditeur d'un courriel par le destinataire de celui-ci, le client de messagerie MSSanté émetteur doit indiquer un libellé « signifiant » qui correspond à l'adresse expéditeur.

E	**ECO.2.2.7** 
	Le système DOIT spécifier un libellé signifiant en complément de l'adresse de messagerie de l'expéditeur : Intitulé_BAL <xxx@xxx.mssante.fr> Avec : • Dans le cas d'une BAL personnelle professionnelle : Intitulé_BAL = <Titre>_<Prénom>_<NOM>_<Entité fonctionnelle> Seuls les champs nom et prénom sont obligatoires. • Dans le cas d'une BAL organisationnelle ou applicative : Intitulé_BAL = <Entité fonctionnelle>

Les détails du format sont les suivants :

- <Titre> est placé avant le prénom et joue le rôle de la civilité pour les personnes exerçant des professions de soins réglementées ;
- « _ » : caractère underscore (caractères ASCII - décimal 95) ;
- <Prénom> est le prénom du professionnel de santé ;
- « _ » : caractère underscore (caractères ASCII - décimal 95) ;
- <NOM> est le nom d'exercice du professionnel de santé, **en majuscule** ;
- « _ » : caractère underscore (caractères ASCII - décimal 95) ;
- <Entité fonctionnelle> est le nom de la structure de soins ou du nom du service rattaché à cette structure.

Exemples de nommage lorsque l'entête From est utilisée :

- BAL personnelle professionnelle : **Dr Marie MARTIN** <marie.martin@medecin.mssante.fr>
- BAL organisationnelle : **Hôpital A – Service Cardiologie** <nom du service@hopitalA.mssante.fr>
- BAL applicative : **Hôpital C – Biologie** <resultat_biologie@hopitalC.mssante.fr>

3.6. Demande d'accusé de réception par l'Opérateur destinataire (DSN)

Le mécanisme Delivery Status Notification (DSN) permet de savoir si un message a été remis avec succès dans la BAL du destinataire du message. mais ne permet pas de savoir si le destinataire a pris connaissance du message.

Ce mécanisme étant activé par la majorité des Opérateurs, les éditeurs de clients de messageries MSSanté doivent proposer une fonctionnalité permettant à l'utilisateur de demander des accusés de réception de type DSN.

NB : Dans les prochaines versions de référentiel #1 Opérateurs de Messageries Sécurisées de Santé la fonctionnalité DSN sera rendue obligatoire.

E	**ECO.2.3.1** 
	Le système DOIT permettre de demander un accusé de réception de type DSN lors de l'émission d'un courriel. L'entête ci-dessous doit être positionné dans le message : **`Return-Receipt-To: <BAL_MSSanté_emetteur>`**

Le mécanisme DSN est décrit dans les RFC 3461 à 3464 et 6522.

3.7. Demande d'accusé de lecture par le destinataire (MDN)

Le mécanisme Message Disposition Notification (MDN) permet de savoir que le message a bien été reçu par le destinataire et quel traitement il a effectué lors de la réception du message : lecture, intégration des pièces jointes dans le système cible, … Il est décrit par la RFC 8098.

Les accusés de réception par l'Opérateur de type DSN ne permettent pas d'obtenir la preuve que le courriel (et les documents de santé joints) a été correctement traité par le destinataire ou son LPS.

Le volet Echange de Documents de Santé du cadre d'Interopérabilité [CI-ECH-DOC] (paragraphe 3.2.8) indique qu'une réponse applicative peut être demandée par l'émetteur du courriel afin de statuer sur la bonne (ou mauvaise) importation du courriel par le destinataire. Dans la présente version du référentiel, seule l'information sur la « lecture » du message est demandée en retour, mais l'intégration des PJ dans le système cible pourrait être confirmé par le même mécanisme.

E	**ECO.2.3.2** 
	Le système DOIT permettre de demander au destinataire un accusé de lecture (MDN) lors de l'émission d'un courriel.

Ce mécanisme peut aussi être utilisé avec les usagers de Mon espace santé. Ce dernier renvoie un accusé de lecture dès que le courriel a été passé à l'état « lu » dans l'interface de l'usager.

3.8. Entêtes de message spécifiques à MSSanté

Les Opérateurs MSSanté ont l'obligation de remonter mensuellement des indicateurs d'usage à l'ANS en sa qualité de régulateur de l'Espace de Confiance. Les données (adresse e-mail, horodatage des échanges, taille des e-mails, présence d'un INS qualifié à l'intérieur du document structuré, type du ou des documents structurés véhiculés, identifiant du client de messagerie) sont collectées, transmises et traitées par l'ANS afin de lui permettre d'établir des indicateurs anonymes. Pour plus d'informations se reporter au Référentiel #1 Opérateurs de Messageries Sécurisées de Santé [REF1-MSSANTE]. Les données à caractère personnel sont conservées 3 mois pour construire le

rapport d'indicateur mensuel qui exploite et diffuse anonymement les informations des 3 derniers mois. Ces données sont ensuite anonymisées.

Depuis la version 1.5 du Référentiel #1 [REF1-MSSANTE], les Opérateurs ont aussi la charge de remonter via ces indicateurs des données positionnées par les clients de messagerie MSSanté via des entêtes SMTP spécifiques MSSanté.

3.8.1. Présence / type de document CDA émis

Cet entête a pour objectif de suivre d'un point de vue statistique la volumétrie et le type de documents structurés véhiculés à travers les messages MSSanté. Pour ce faire, le système à l'origine du message doit respecter l'exigence suivante.

E	**ECO.2.4.1**  Le système DOIT positionner un entête SMTP "`X-MSS-CODECDA`" dans un message envoyé qui comporte en PJ un ou plusieurs documents CDA encapsulés dans une archive IHE_XDM. La valeur de cet entête 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-valué. 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.

**code* défini dans le Volet Structuration Minimale de Documents de Santé du CI-SIS [CI-STRU-ENTETE]

Exemples de valeurs de l'entête :

```
X-MSS-CODECDA: 34112-3
X-MSS-CODECDA: 34112-3,PRESC-BIO,15508-5
```

3.8.2. Présence d'une Identité Nationale de Santé dans le document CDA émis

Depuis le 1er janvier 2021, toute donnée de santé doit réglementairement être référencée avec l'INS qualifiée de l'usager. Néanmoins, il peut exister des cas dans lesquels l'INS qualifiée n'est pas disponible au moment de l'échange de données de santé : usagers n'ayant pas vocation à avoir d'INS, usagers pour lesquels un doute sur l'identité empêche la qualification de l'INS, etc. Dans ces cas, l'absence d'INS qualifiée ne doit pas empêcher l'échange de données de santé via MSSanté.

Il est intéressant de connaitre la proportion de documents structurés transmis via MSSanté sans INS qualifiée. Il est demandé lors de la création du message positionner un entête « X-MSS-INS » qui sera traité par l'Opérateur, et ainsi consolidé dans les indicateurs de l'Espace de Confiance MSSanté.

E	**ECO.2.4.2**  Le système DOIT positionner l'entête SMTP "`X-MSS-INS`" dans un message envoyé qui comporte en PJ au moins un document de santé CDA encapsulé dans une archive IHE_XDM. La valeur de cet entête 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.

*la notion d'**INS qualifiée** est définie dans le Référentiel Identifiant National de Santé [INS-REF]. La présence d'une INS qualifiée est caractérisée par la présence dans l'entête CDA de l'INS (matricule, OID) et des 4 traits d'identité suivants dans l'entête CDA : nom de naissance, 1er prénom, date de naissance et sexe.

Une identité où seuls les traits nom de naissance, 1er prénom de naissance, date de naissance et sexe sont présents dans le CDA (en l'absence matricule INS et l'OID), n'est donc pas considérée comme une INS qualifiée.

Exemples d'entête :

```
X-MSS-INS: O
X-MSS-INS: N
```

3.8.3. Identifiant du LPS émetteur du message

L'identification du LPS à l'origine d'un message vise 2 objectifs :

- Permettre à chaque Opérateur d'identifier facilement le LPS à l'origine de l'envoi d'un message, qui permet de réduire les temps de résolution en cas d'incidents,
- Permettre au gestionnaire de l'espace de confiance de suivre l'évolution des usages en termes de déploiement des LPS.

E	**ECO.2.4.3**  Le système DOIT positionner l'entête SMTP "`X-MSS-NIL`" dans tous les courriels envoyés. Elle sera renseignée du numéro « référence produit » attribué lors de la déclaration du produit sur la plateforme convergence.esante.gouv.fr. Le numéro « référence produit » à renseigner est celui du logiciel qui a produit le message SMTP.

4. GESTION DES MESSAGES VIA L'IHM DU LPS

4.1. Affichage des messages émis par les professionnels et les usagers

Les professionnels pouvant recevoir des courriels envoyés par des professionnels, mais aussi d'usagers, le LPS doit proposer un moyen permettant au professionnel de distinguer aisément dans une liste de messages les 2 types d'émetteur sans avoir besoin de se référer au nom de domaine (contenant au nom le sous-domaine « patient.mssante.fr »).

E	**ECO.3.1.1** 
	Dans la liste des messages reçus, le système DOIT distinguer les messages émis par des professionnels, des messages émis par des usagers via MES.

Les modalités d'implémentation de cette exigence sont laissées au choix de l'éditeur.

4.2. Affichage de l'identité d'un usager

Les adresses MSSanté des professionnels (sauf cas particulier de la liste rouge) sont contenues dans l'Annuaire Santé . Ceci permet de vérifier l'identité d'un professionnel depuis son adresse MSSanté (et inversement).

Pour les usagers, il n'existe pas d'annuaire des adresses MSSanté des usagers et leur adresse email ne contient que leur matricule INS.

Lorsqu'un usager écrit à un professionnel depuis Mon espace santé, ce dernier transmet le nom de naissance et le premier prénom de l'usager dans le libellé du champ "From:". Il s'agit d'un moyen rapide d'obtenir les nom/prénom de l'usager.

Exemple : lorsque l'usager Léo Dupond répond au message d'un Professionnel, le champ « `From:` » de l'entête du message envoyé sera de la forme :

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

E	**ECO.3.1.2** 
	Le système DOIT afficher le nom de naissance, le 1er prénom et le matricule INS d'usager (et pas uniquement l'adresse email INS@patient.mssante.fr) dans un message reçu d'un usager (depuis Mon espace santé).

4.3. Affichage de l'objet d'un message contenant un document de santé structuré

La standardisation des messages MSSanté impose qu'un message contenant en pièce-jointe un document CDA encapsulé dans une archive IHE_XDM utilise en préfixe de l'objet du message la chaine de texte "XDM/1.0/DDM+". Elle permet au LPS d'identifier automatiquement ce type de message. En revanche, pour un professionnel qui consulte ses messages, ce préfixe n'a pas de signification et alourdi inutilement la lecture de l'objet.

E	**ECO.3.1.3** 
	Le système DOIT masquer au professionnel le préfixe "XDM/1.0/DDM+" de l'objet des messages reçus contenant un document CDA dans l'archive IHE_XDM en pièce jointe.

4.4. Recherche d'un destinataire professionnel

L'adresse MSSanté d'un professionnel destinataire d'un courriel peut être préalablement connue du LPS. Cependant, lorsque ce n'est pas le cas l'utilisateur doit pourvoir avoir accès à une fonctionnalité de recherche multicritères basée sur l'Annuaire Santé.

E	**ECO.3.1.4** 
	Lors de la composition d'un message, le système DOIT proposer au professionnel une fonctionnalité permettant de rechercher l'adresse MSSanté d'une personne physique ou d'une personne morale dans l'Annuaire Santé.

Les différentes méthodes permettant de consulter l'Annuaire Santé sont rappelées au §3.4.1.

4.5. Recherche d'un destinataire usager

Contrairement aux professionnels, il n'existe pas d'annuaire national permettant de rechercher l'adresse MSSanté d'un usager. De plus, une adresse MSSanté usager ne doit être utilisée que si l'Identité Nationale de Santé de l'usager qualifiée est connue de l'émetteur. Il est donc important que le LPS permette de générer des adresses MSSanté à partir des Identités Nationales de Santé qualifiées connues du LPS.

E	**ECO.3.1.5** 
	Le système DOIT permettre au professionnel d'écrire à un usager en le sélectionnant dans une liste construite à partir de la base des usagers connus du système ou directement depuis le dossier d'un usager. Le système doit s'assurer que l'Identité Nationale de Santé est qualifiée, puis génère le champs To: du message à partir du matricule INS.

Lorsque l'Identité Nationale de Santé d'un usager n'est pas qualifiée, une dérogation décrite au §3.4.2.2 permet dans certains cas de pouvoir générer une adresse MSSanté.

4.6. Accusés de réception par le destinataire (MDN)

Le mécanisme Message Disposition Notification (MDN) permet de savoir que le message a bien été reçu par le destinataire et quel traitement il a effectué lors de la réception du message : lecture, intégration des pièces jointes dans le système cible, … Il est décrit par la RFC 8098.

E	**ECO.3.1.6** 
	Le système DOIT permettre de retourner un accusé de lecture (MDN) lorsqu'un message reçu le demande.

L'interaction utilisateur à l'origine de l'envoi de l'accusé de lecture est laissé à l'appréciation de l'éditeur. Il devra toutefois s'assurer que l'utilisateur a bien pu prendre connaissance du contenu du message, par exemple après avoir affiché le corps du message.

4.7. Recommandations

Dans cette section, sont regroupées des recommandations dont les éditeurs peuvent se saisir pour améliorer l'expérience utilisateur. En fonction des remontées des utilisateurs et des concertations avec les éditeurs, elles pourront devenir des exigences dans les prochaines versions du présent référentiel.

4.7.1. Mode d'affichage sous forme de conversation

Comme décrit au §3.2, tous LPS a l'obligation de positionner des ID de message dans tous les messages envoyés et dans toutes les réponses produites. Ainsi le mode conversation peut être activité.

R	**ECO.3.2.1** 
	Dans une liste des messages affichés, le système PEUT proposer d'utiliser un mode d'affichage sous forme de conversation.

4.7.2. Mode de tri des messages

Afin de facilité la recherche d'un message dans une liste, il est souhaitable que l'utilisateur puisse définir l'ordre d'affiche d'une liste de messages.

R	**ECO.3.2.2** 
	Dans une liste des messages, le système PEUT proposer plusieurs modes de tri des messages.

4.7.3. Consultation de plusieurs boites aux lettres

Suivant les contextes d'utilisation, il est possible qu'un utilisateur souhaite accéder simultanément dans son LPS au contenu de plusieurs BAL MSSanté et envoyer des messages au choix depuis plusieurs BAL MSSanté. Par exemple, une BAL personnelle et une BAL organisationnelle.

R	**ECO.3.2.3** 
	Le système PEUT permettre de configurer plusieurs BAL MSSanté simultanément.

Pour rappel, les Opérateurs doivent proposer des mécanismes d'autoconfiguration des BAL.

5. AUTRES EXIGENCES

5.1. Gestion des traces

En application du Référentiel #1 MSSanté [REF1-MSSANTE], les Opérateurs MSSanté ont l'obligation de conserver des traces fonctionnelles des messages qu'ils traitent afin de :

- Contribuer à la détection, à l'investigation et au traitement d'incidents de sécurité ;
- Contribuer à la résolution de litiges entre l'éditeur et des utilisateurs du système ;
- Permettre à une autorité compétente de s'assurer de la conformité du traitement aux dispositions règlementaires qui l'encadrent.

Les traces fonctionnelles sont les traces des actions réalisées par tout utilisateur final ou processus automatisé. Elles doivent être accessibles à toutes personnes dûment habilitées dont par exemple les équipes de support de l'éditeur...

Les actions réalisées sur une BAL hébergée par un Opérateur étant initiées par un client de messagerie MSSanté, ce dernier doit également conserver des traces fonctionnelles en respectant les exigences ci-dessous.

E	**ECO.4.1.1**
	Le système DOIT générer des traces fonctionnelles pour tous les traitements opérés (envoi, consultation, suppression...) sur les BAL MSSanté et leur contenu.

Sans se substituer aux responsabilités de l'éditeur du système, une conservation de ces traces fonctionnelles sur une durée de 6 mois est recommandée.

E	**ECO.4.1.2**
	Chaque action tracée DOIT préciser : • l'identifiant de son auteur dûment authentifié, • l'horodatage local du poste, • le type d'action réalisée (connexion, …), • la demande effectuée sur le serveur de messagerie MSSanté, • la réponse fournie par ce dernier (y compris en cas d'échec).

L'exigence ECO.4.1.1 n'implique pas l'obligation de proposer une interface d'accès à ces traces pour en simplifier l'accès aux utilisateurs finaux.

Il appartient au responsable de traitement d'appliquer aux traces fonctionnelles les mêmes mesures que celles appliquées aux données auxquelles elles se rattachent (mesures organisationnelles, mesures techniques, etc.), pour assurer leur sécurité et leur confidentialité et de définir les règles de durée de conservation de ces traces.

6. ANNEXES

6.1. Synthèse des exigences applicables aux éditeurs MSSanté

Les exigences applicables aux éditeurs de clients de messageries définies dans les différents chapitres sont synthétisées dans les 2 chapitres suivants. D'abord celles applicables aux LPS accédants à des BAL personnelles ou organisationnelles, puis celles applicables aux LPS accédants à des BAL applicatives. Les recommandations ou préconisations ne sont pas reprises.

6.1.1. Exigences applicables aux BAL personnelles et organisationnelles

ECO.1.0.1
Le système DOIT disposer d'une interface d'envoi de messages utilisant le protocole SMTP conforme à la RFC 5321 avec STARTTLS comme défini dans le RFC 3207.

ECO.1.0.2
Le système DOIT disposer d'une interface d'accès aux BAL utilisant le protocole IMAP 4 (rev1 ou rev2) conforme respectivement à la RFC 3501 ou RFC 9051 avec STARTTLS comme défini dans la RFC 5246.

ECO.1.1.1
Le système DOIT savoir établir une connexion TLS avec l'API LPS d'un Opérateur MSSanté en utilisant la version TLS 1.2 (RFC 5246) a minima.

ECO.1.1.3
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 Opérateur MSSanté : • 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 Pour l'échange des clés de chiffrement TLS, le système DOIT utiliser : • soit le protocole DHE en configurant un groupe DH >= 2048bits, • soit le protocole ECHDE en configurant un groupe elliptique ECDH >= 256 bits. Si l'Opérateur présente des groupes de longueur inférieure, le système doit rejeter la connexion TLS.

ECO.1.1.10

Le système DOIT accepter uniquement un certificat issu de l'IGC Santé gamme Elementaire Organisation lorsqu'il se connecte à une interface API LPS d'un système de messagerie MSSanté.

ECO.1.1.5

Le système DOIT vérifier que le certificat présenté par l'Opérateur MSSanté n'est pas expiré.

ECO.1.1.6

Le système MSSanté DOIT vérifier que le certificat présenté par l'Opérateur MSSanté n'est pas révoqué au moyen des CRL ou du répondeur OCSP.

ECO.1.1.7

Le système DOIT s'assurer de conserver la dernière CRL non expirée, lorsque le contrôle de révocation est réalisé au moyen des CRL, afin d'éviter tout échec de connexion avec l'Opérateur MSSanté en cas d'erreur lors de la récupération de la CRL courante.

ECO.1.1.9

Le système DOIT proposer une fonctionnalité d'autoconfiguration de BAL, soit lors de la configuration de la BAL, soit à la demande, en respectant les étapes ci-dessous :

1 – A partir de l'adresse de la BAL à configurer, consulter l'URL d'autoconfiguration de l'Opérateur MSSanté :

`https://autoconfig.<emailaddressdomain>/mail/config-v1.1.xml` (*)

2 – Configurer automatiquement les paramètres de configuration spécifiques à l'API LPS de l'Opérateur MSSanté proposant la BAL,

3 – Procéder à un test de connexion pour validation de la configuration.

* : les opérateurs présentent un certificat serveur de l'IGC Santé ou d'une IGC commerciale usuellement acceptée par les navigateurs Internet.

ECO.1.2.1

Le système DOIT réaliser des demandes d'ouverture de connexion SMTP et IMAP sur l'interface BAL personnelle ou organisationnelle de l'API LPS d'un Opérateur MSSanté en respectant la cinématique suivante :

1- Ouvrir la session TLS avec STARTTLS

2- Réaliser une authentification du PS via le mécanisme SASL OAuth 2.0, en envoyant le mot clé AUTHENTICATE XOAUTH2 pour IMAP ou AUTH XOAUTH2 pour SMTP avec la chaine de caractères encodée en base64 contenant à la fois l'adresse de la BAL dans le champ « user » et l'Access Token PSC au format JWT. Le formatage de cette chaine de caractères est le suivant :

- Chaine fixe : "`user=`",
- Adresse mail de la BAL,
- Chaine fixe : "`^Aauth=Bearer` " (avec un espace à la fin),
- Access Token PSC,
- Chaine fixe : "`^A^A`".

3- Attendre la validation de la connexion IMAP ou SMTP par l'Opérateur MSSanté utilisé

4- Envoyer les commandes SMTP ou IMAP

ECO.1.2.3

Le système DOIT traiter les erreurs techniques rencontrées lors du processus de connexion et d'authentification SMTP/IMAP de sorte qu'elles ne perturbent pas les autres fonctions de l'application (hors messagerie).

ECO.1.2.5

Pour des raisons de sécurité, l'Access Token PSC au format JWT ne doit pas être stocké de façon permanente sur le poste de travail du professionnel. Il doit être mémorisé de façon temporaire, pour une durée correspondant à sa durée de vie. Ainsi, lors de l'utilisation d'un Client Lourd, le moyen de mémorisation de l'Access Token PSC doit être protégé des accès et attaques externes. Le niveau de sécurisation utilisé pour la mémorisation temporaire doit être éprouvée.

ECO.1.2.5

Pour des raisons de sécurité, l'Access Token PSC au format JWT ne doit pas être stocké de façon permanente sur le poste de travail du professionnel. Il doit être mémorisé de façon temporaire, pour une durée correspondant à sa durée de vie. Ainsi, lors de l'utilisation d'un Client Lourd, le moyen de mémorisation de l'Access Token PSC doit être protégé des accès et attaques externes. Le niveau de sécurisation utilisé pour la mémorisation temporaire doit être éprouvée.

ECO.1.2.6

Dès que le Refresh Token PSC de l'utilisateur connecté devient invalide (durée de vie maximale atteinte, déconnexion PSC, ...), le système DOIT déclencher la fin de session IMAP et SMTP avec le serveur de messagerie.

ECO.1.2.7
Suite à la détection d'une fin de session IMAP ou SMTP déclenchée par l'Opérateur MSSanté, lorsque l'authentification PSC est toujours valide, le système DOIT pouvoir réouvrir automatiquement (i.e. sans intervention humaine) une session IMAP ou SMTP

ECO.2.1.1
Un courriel MSSanté utilisé pour transmettre un (des) document(s) de santé DOIT : • Concerner qu'un seul et même usager, • Contenir en pièces jointes du courriel : o une archive ZIP au format IHE_XDM contenant **un ou plusieurs** documents CDA R2 niveau 1 et/ou niveau 3 (suivant les spécifications du volet échange de documents de santé [CI-ECH-DOC]), o les mêmes documents médicaux au format PDF/A-1.

ECO.2.1.5
Chaque PDF/A-1 rattaché au courriel MSSanté DOIT **être généré à partir du ou des documents CDA correspondants contenus dans l'archive ZIP au format** IHE_XDM : Cas d'un document CDA R2 N3, le PDF/A-1 doit comporter : les données suivantes de l'entête CDA : Titre, Type de document, Date et heure de création, Auteur / Responsable du document, Organisation conservant le document, o une transcription fidèle du contenu clinique porté dans la partie narrative de chaque section du document CDA qui a été validé par le responsable du document CDA. - Sinon le PDF/A-1 doit être identique au PDF encapsulé dans le CDA R2 N1.

ECO.2.1.6
Les fichiers au format PDF présents en pièce jointe DOIVENT respecter la convention de nommage suivante, afin de faciliter l'identification des documents de santé : <date de l'acte>_<type document>_<NOM>_<prenom>_<numéro de dossier>.pdf Tous les champs sont obligatoires à l'exception du champ <numéro de dossier> qui est optionnel.

ECO.2.1.2
Pour identifier l'usager concerné par un courriel, le système destinataire DOIT se référer à la métadonnée `patientId` (matricule INS) contenu dans le fichier METADATA.XML du document CDA contenu dans la pièce jointe IHE_XDM.zip du courriel.

ECO.2.1.3
L'objet du courriel DOIT respecter le format suivant :

XDM/1.0/DDM+<libellé> <NOM> <prenom> <date de naissance>

Tous les champs sont obligatoires à l'exception du champ <date de naissance> qui est optionnel.

ECO.2.2.1

Le système DOIT renseigner l'entête « Message-ID » conformément à la RFC 5322 dans tout nouveau courriel produit.

ECO.2.2.2

Le système DOIT renseigner les entêtes « Message-ID », « in-Reply-To » et « References » conformément à la RFC 5322 dans toute réponse à un courriel.

ECO.2.2.3

Le système MSSante DOIT utiliser l'encodage UTF-8 pour les parties `text` du corps des courriels.

ECO.2.2.4

Le corps du courriel indiqué dans entête `Content-Type` du courriel, doit être :

- Soit `text/plain`, c'est-à-dire en texte brut sans formatage,
- Soit `multipart/alternative` avec 2 parties identiques en termes de contenu rédactionnel:
  - La première en `text/plain`,
  - La seconde en `text/html`.

ECO.2.2.5

Un courriel envoyé depuis une BAL applicative doit :

- Contenir une mention à la fin du message précisant que le message a été généré automatiquement et en indiquant une adresse de BAL MSSanté personnelle ou organisationnelle permettant de contacter l'émetteur,
- Positionner un entête « Reply-To » contenant l'adresse de cette BAL personnelle ou organisationnelle.

ECO.2.2.6

Un système, **qui envoie des courriels MSSanté à des usagers,** DOIT utiliser des adresses usagers construites à partir d'Identités Nationale de Santé « qualifiées ».

ECO.2.2.8

Le système DOIT pouvoir positionner un entête SMTP "`X-MSS-MES`", dans les messages envoyés vers un usager (Mon espace santé), avec la valeur "`FIN`" (3 caractères en majuscules), lorsque le professionnel émetteur ne souhaite pas que l'usager puisse lui répondre en retour.

ECO.2.2.7

Le système DOIT spécifier un libellé signifiant en complément de l'adresse de messagerie de l'expéditeur :

Intitulé_BAL <xxx@xxx.mssante.fr>

Avec :

- Dans le cas d'une BAL personnelle professionnelle :

  Intitulé_BAL = <Titre>_<Prénom>_<NOM>_<Entité fonctionnelle>

  Seuls les champs nom et prénom sont obligatoires.

- Dans le cas d'une BAL organisationnelle ou applicative :

  Intitulé_BAL = <Entité fonctionnelle>

ECO.2.3.1

Le système DOIT permettre de demander un accusé de réception de type DSN lors de l'émission d'un courriel. L'entête ci-dessous doit être positionné dans le message :

`Return-Receipt-To: <BAL_MSSanté_emetteur>`

ECO.2.3.2

Le système DOIT permettre de demander au destinataire un accusé de lecture (MDN) lors de l'émission d'un courriel.

ECO.2.4.1

Le système DOIT positionner un entête SMTP "`X-MSS-CODECDA`" dans un message envoyé qui comporte en PJ un ou plusieurs documents CDA encapsulés dans une archive IHE_XDM.

La valeur de cet entête 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-valué.

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.

ECO.2.4.2

Le système DOIT positionner l'entête SMTP "X-MSS-INS" dans un message envoyé qui comporte en PJ au moins un document de santé CDA encapsulé dans une archive IHE_XDM. La valeur de cet entête 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.

ECO.2.4.3

Le système DOIT positionner l'entête SMTP "X-MSS-NIL" dans tous les courriels envoyés. Elle sera renseignée du numéro « référence produit » attribué lors de la déclaration du produit sur la plateforme convergence.esante.gouv.fr.

Le numéro « référence produit » à renseigner est celui du logiciel qui a produit le message SMTP.

ECO.3.1.1

Dans la liste des messages reçus, le système DOIT distinguer les messages émis par des professionnels, des messages émis par des usagers via MES.

ECO.3.1.2

Le système DOIT afficher le nom de naissance, le 1er prénom et le matricule INS d'usager (et pas uniquement l'adresse email INS@patient.mssante.fr) dans un message reçu d'un usager (depuis Mon espace santé).

ECO.3.1.3

Le système DOIT masquer au professionnel le préfixe "XDM/1.0/DDM+" de l'objet des messages reçus contenant un document CDA dans l'archive IHE_XDM en pièce jointe.

ECO.3.1.4

Lors de la composition d'un message, le système DOIT proposer au professionnel une fonctionnalité permettant de rechercher l'adresse MSSanté d'une personne physique ou d'une personne morale dans l'Annuaire Santé.

ECO.3.1.5

Le système DOIT permettre au professionnel d'écrire à un usager en le sélectionnant dans une liste construite à partir de la base des usagers connus du système ou directement depuis le dossier d'un usager. Le système doit

s'assurer que l'Identité Nationale de Santé est qualifiée, puis génère le champs To: du message à partir du matricule INS.

ECO.3.1.6

Le système DOIT permettre de retourner un accusé de lecture (MDN) lorsqu'un message reçu le demande.

ECO.4.1.1

Le système DOIT générer des traces fonctionnelles pour tous les traitements opérés (envoi, consultation, suppression...) sur les BAL MSSanté et leur contenu.

ECO.4.1.2

Chaque action tracée DOIT préciser :

- l'identifiant de son auteur dûment authentifié,
- l'horodatage local du poste,
- le type d'action réalisée (connexion, …),
- la demande effectuée sur le serveur de messagerie MSSanté,
- la réponse fournie par ce dernier (y compris en cas d'échec).

6.1.2. Exigences applicables aux BAL applicatives

ECO.1.0.1
Le système DOIT disposer d'une interface d'envoi de messages utilisant le protocole SMTP conforme à la RFC 5321 avec STARTTLS comme défini dans le RFC 3207.

ECO.1.0.2
Le système DOIT disposer d'une interface d'accès aux BAL utilisant le protocole IMAP 4 (rev1 ou rev2) conforme respectivement à la RFC 3501 ou RFC 9051 avec STARTTLS comme défini dans la RFC 5246.

ECO.1.1.1
Le système DOIT savoir établir une connexion TLS avec l'API LPS d'un Opérateur MSSanté en utilisant la version TLS 1.2 (RFC 5246) a minima.

ECO.1.1.3
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 Opérateur MSSanté : • 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 Pour l'échange des clés de chiffrement TLS, le système DOIT utiliser : • soit le protocole DHE en configurant un groupe DH >= 2048bits, • soit le protocole ECHDE en configurant un groupe elliptique ECDH >= 256 bits. Si l'Opérateur présente des groupes de longueur inférieure, le système doit rejeter la connexion TLS.

ECO.1.1.10
Le système DOIT accepter uniquement un certificat issu de l'IGC Santé gamme Elementaire Organisation lorsqu'il se connecte à une interface API LPS d'un système de messagerie MSSanté.

ECO.1.1.5
Le système DOIT vérifier que le certificat présenté par l'Opérateur MSSanté n'est pas expiré.

ECO.1.1.6
Le système MSSanté DOIT vérifier que le certificat présenté par l'Opérateur MSSanté n'est pas révoqué au moyen des CRL ou du répondeur OCSP.

ECO.1.1.7
Le système DOIT s'assurer de conserver la dernière CRL non expirée, lorsque le contrôle de révocation est réalisé au moyen des CRL, afin d'éviter tout échec de connexion avec l'Opérateur MSSanté en cas d'erreur lors de la récupération de la CRL courante.

ECO.1.1.9
Le système DOIT proposer une fonctionnalité d'autoconfiguration de BAL, soit lors de la configuration de la BAL, soit à la demande, en respectant les étapes ci-dessous : 1 – A partir de l'adresse de la BAL à configurer, consulter l'URL d'autoconfiguration de l'Opérateur MSSanté : **`https://autoconfig.<emailaddressdomain>/mail/config-v1.1.xml`** (*) 2 – Configurer automatiquement les paramètres de configuration spécifiques à l'API LPS de l'Opérateur MSSanté proposant la BAL, 3 – Procéder à un test de connexion pour validation de la configuration. * : les opérateurs présentent un certificat serveur de l'IGC Santé ou d'une IGC commerciale usuellement acceptée par les navigateurs Internet.

ECO.1.3.1
Le système DOIT réaliser des demandes d'ouverture de connexions SMTP et IMAP sur l'interface BAL applicative de l'API LPS d'un Opérateur MSSanté en respectant la cinématique suivante : 1- Monter la session TLS avec STARTTLS en présentant un certificat ORG AUTH_CLI à l'Opérateur MSSanté utilisé comme défini dans la RFC 5246, 2- Transmettre l'adresse de la BAL dans le login de la méthode d'authentification PLAIN comme défini dans la RFC 3501 ou RFC 9051, 3- Envoyer les commandes SMTP ou IMAP.

ECO.2.1.1

Un courriel MSSanté utilisé pour transmettre un (des) document(s) de santé DOIT :

- Concerner qu'un seul et même usager,
- Contenir en pièces jointes du courriel :
  - une archive ZIP au format IHE_XDM contenant **un ou plusieurs** documents CDA R2 niveau 1 et/ou niveau 3 (suivant les spécifications du volet échange de documents de santé [CI-ECH-DOC]),
  - les mêmes documents médicaux au format PDF/A-1.

ECO.2.1.5

Chaque PDF/A-1 rattaché au courriel MSSanté DOIT **être généré à partir du ou des documents CDA correspondants contenus dans l'archive ZIP au format** IHE_XDM :
Cas d'un document CDA R2 N3, le PDF/A-1 doit comporter :
les données suivantes de l'entête CDA : Titre, Type de document, Date et heure de création, Auteur / Responsable du document, Organisation conservant le document,

- une transcription fidèle du contenu clinique porté dans la partie narrative de chaque section du document CDA qui a été validé par le responsable du document CDA.

- Sinon le PDF/A-1 doit être identique au PDF encapsulé dans le CDA R2 N1.

ECO.2.1.6

Les fichiers au format PDF présents en pièce jointe DOIVENT respecter la convention de nommage suivante, afin de faciliter l'identification des documents de santé :

<date de l'acte>_<type document>_<NOM>_<prenom>_<numéro de dossier>.pdf

Tous les champs sont obligatoires à l'exception du champ <numéro de dossier> qui est optionnel.

ECO.2.1.2

Pour identifier l'usager concerné par un courriel, le système destinataire DOIT se référer à la métadonnée patientId (matricule INS) contenu dans le fichier METADATA.XML du document CDA contenu dans la pièce jointe IHE_XDM.zip du courriel.

ECO.2.1.3

L'objet du courriel DOIT respecter le format suivant :

XDM/1.0/DDM+<libellé> <NOM> <prenom> <date de naissance>

Tous les champs sont obligatoires à l'exception du champ <date de naissance> qui est optionnel.

ECO.2.2.1

Le système DOIT renseigner l'entête « Message-ID » conformément à la RFC 5322 dans tout nouveau courriel produit.

ECO.2.2.2

Le système DOIT renseigner les entêtes « Message-ID », « in-Reply-To » et « References » conformément à la RFC 5322 dans toute réponse à un courriel.

ECO.2.2.3

Le système MSSante DOIT utiliser l'encodage UTF-8 pour les parties `text` du corps des courriels.

ECO.2.2.4

Le corps du courriel indiqué dans entête `Content-Type` du courriel, doit être :

- Soit `text/plain`, c'est-à-dire en texte brut sans formatage,
- Soit `multipart/alternative` avec 2 parties identiques en termes de contenu rédactionnel:
  - La première en `text/plain`,
  - La seconde en `text/html`.

ECO.2.2.5

Un courriel envoyé depuis une BAL applicative doit :

- Contenir une mention à la fin du message précisant que le message a été généré automatiquement et en indiquant une adresse de BAL MSSanté personnelle ou organisationnelle permettant de contacter l'émetteur,
- Positionner un entête « Reply-To » contenant l'adresse de cette BAL personnelle ou organisationnelle.

ECO.2.2.6

Un système, **qui envoie des courriels MSSanté à des usagers,** DOIT utiliser des adresses usagers construites à partir d'Identités Nationale de Santé « qualifiées ».

ECO.2.2.8

Le système DOIT pouvoir positionner un entête SMTP "`X-MSS-MES`", dans les messages envoyés vers un usager (Mon espace santé), avec la valeur "`FIN`" (3 caractères en majuscules), lorsque le professionnel émetteur ne souhaite pas que l'usager puisse lui répondre en retour.

ECO.2.2.7

Le système DOIT spécifier un libellé signifiant en complément de l'adresse de messagerie de l'expéditeur :

Intitulé_BAL <xxx@xxx.mssante.fr>

Avec :

- Dans le cas d'une BAL personnelle professionnelle :

  Intitulé_BAL = <Titre>_<Prénom>_<NOM>_<Entité fonctionnelle>

  Seuls les champs nom et prénom sont obligatoires.

- Dans le cas d'une BAL organisationnelle ou applicative :

  Intitulé_BAL = <Entité fonctionnelle>

ECO.2.3.1

Le système DOIT permettre de demander un accusé de réception de type DSN lors de l'émission d'un courriel. L'entête ci-dessous doit être positionné dans le message :

`Return-Receipt-To: <BAL_MSSanté_emetteur>`

ECO.2.3.2

Le système DOIT permettre de demander au destinataire un accusé de lecture (MDN) lors de l'émission d'un courriel.

ECO.2.4.1

Le système DOIT positionner un entête SMTP "`X-MSS-CODECDA`" dans un message envoyé qui comporte en PJ un ou plusieurs documents CDA encapsulés dans une archive IHE_XDM.

La valeur de cet entête 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-valué.

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.

ECO.2.4.2

Le système DOIT positionner l'entête SMTP "`X-MSS-INS`" dans un message envoyé qui comporte en PJ au moins un document de santé CDA encapsulé dans une archive IHE_XDM. La valeur de cet entête 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.

ECO.2.4.3
Le système DOIT positionner l'entête SMTP "`X-MSS-NIL`" dans tous les courriels envoyés. Elle sera renseignée du numéro « référence produit » attribué lors de la déclaration du produit sur la plateforme convergence.esante.gouv.fr. Le numéro « référence produit » à renseigner est celui du logiciel qui a produit le message SMTP.

ECO.4.1.1
Le système DOIT générer des traces fonctionnelles pour tous les traitements opérés (envoi, consultation, suppression...) sur les BAL MSSanté et leur contenu.

ECO.4.1.2
Chaque action tracée DOIT préciser : • l'identifiant de son auteur dûment authentifié, • l'horodatage local du poste, • le type d'action réalisée (connexion, …), • la demande effectuée sur le serveur de messagerie MSSanté, • la réponse fournie par ce dernier (y compris en cas d'échec).

6.2. Glossaire

Le tableau ci-dessous précise la signification des termes et abréviations utilisés dans ce document :

Abréviations	Signification
AC	Autorité de Certification
ADELI	Automatisation des Listes (répertoire de professionnels de santé en cours de remplacement par le RPPS)
AE	Autorité d'Enregistrement
Annuaire Santé	L'Annuaire Santé recense les professionnels de santé enregistrés dans les répertoires nationaux RPPS et Adeli et leurs situations d'exercice. Ces données proviennent des autorités chargées de leur enregistrement (ordres professionnels, ARS, service de santé des armées)
ANSSI	Agence Nationale pour la Sécurité des Systèmes d'Information
BAL	Boîte aux lettres
BAL personnelle	Boîte aux lettres nominatives, rattachée dans l'annuaire santé à une personne physique. Elles sont réservées à l'usage d'un professionnel habilité ou d'un usager.
BAL organisationnelle	Boîte aux lettres dont l'accès est possible pour un ensemble de professionnels habilités. Est rattachée dans l'annuaire santé à une personne morale.
BAL applicative	Boite aux lettres accédée par à un logiciel métier ou à une machine. Est rattachée dans l'annuaire santé à une personne morale.
CI-SIS	Cadre d'interopérabilité des Systèmes d'Information de Santé de l'ANS
CGU	Conditions Générales d'Utilisation
Cnam	Caisse Nationale d'Assurance Maladie
CNIL	Commission Nationale de l'Informatique et des Libertés
CPA	Carte de Personnel Autorisé
CPE	Carte de Professionnel d'Etablissement
CPS	Carte de Professionnel de Santé
CRL	Certificate Revocation List
DMP	Dossier Médical Personnel
DN	Distinguished Name
DNS	Domain Name Server
DSN	Delivery Status Notification
DSFT	Dossier des Spécifications Fonctionnelles et Techniques
ES	Etablissement de Santé : terme recouvrant les établissements de soins publics et privés, incluant les plateaux techniques en ville et en hôpital
FAQ	Foire Aux Questions
IETF	Internet Engineering Task Force
HDS	Hébergeur de données de santé
IGC	Infrastructure de Gestion de Clés
INS	Identité Nationale de Santé
IMAP	Internet Mail Access Protocol
LDAP	Lightweight Directory Access Protocol
LGC	Logiciel de Gestion de Cabinet
LPS	Logiciel de Professionnel de Santé (abréviation générique désignant une application utilisée par un professionnel habilité en structure ou libéral). Le terme DUI pourrait aussi bien être utilisé dans les secteurs médico-sociaux et sociaux.
MES	Mon espace santé
MIME	Multipurpose Internet Mail Extensions

Abréviations	Signification
MDN	Message Disposition Notification
MSSanté	Messagerie Sécurisée de Santé
MTA	Mail Transport Agent
MUA	Mail User Agent (client de messagerie)
NAS	Nomenclature des Acteurs de Santé
NDR	Non-Delivery Report
OCSP	Online Certificate Status Protocol
PM	Personne Morale
Professionnel habilité	Désigne les professionnels de santé et tout professionnel habilité par la loi à collecter et échanger des données de santé à caractère personnel.
PS	Professionnel de Santé - Acteur de Santé humain
PSC	Pro Santé Connect
PSSI	Politique de Sécurité des Systèmes d'Information
Référentiel des identités PP/PM	Référentiel des identités de personnes et de structures issus du RPPS, FINESS et ADELI
RFC	Request For comments Série numérotée de documents officiels publiés par l'IETF
RGPD	Règlement Général sur la Protection des Données
RNIV	Référentiel National d'Identitovigilance
RPPS	Répertoire Partagé des Professionnels de Santé
SI	Système d'Information
SSI	Sécurité du Système d'Information
SMTP	Simple Mail Transport Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security - Norme de sécurisation par chiffrement du transport de l'information au sein des réseaux (anciennement SSL)
Usagers	Désigne les usagers du système de santé utilisant la MSSanté pour échanger avec des professionnels habilités

Tableau 1 : Liste des acronymes et de leur signification

6.3. Documents applicables

Documents applicables (désignés dans le document par le code présent dans la colonne « Référence »)		
N°	**Référence**	**Document**
Référentiel Socle MSSanté (accessible sur le site mssante.fr)		
DA01	[REF1-MSSANTE]	**Référentiel #1 Opérateurs de Messageries Sécurisées de Santé - Principes, exigences et interfaces Opérateurs (anciennement DSFT)**
DA02	[MES-EDITEURS]	**Note technico-fonctionnelle sur le client de messagerie Mon espace santé (produit par la Cnam)**
Documents de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) (accessibles sur le site de l'ANS)		
DA11	[PG-REF-IDENT]	**Référentiel d'identification électronique des acteurs des secteurs sanitaire, médicosocial et social**
Documents du Cadre d'interopérabilité des Systèmes d'Information de Santé (CI-SIS) (accessibles sur le site de l'ANS)		
DA21	[CI-CHAP]	**Document Chapeau du CI-SIS**
DA22	[CI-ECH-DOC]	**Volet Echange des Documents de Santé**
DA24	[CI-STRU-ENTETE]	**Couche Contenu Volet Structuration Minimale de Documents Médicaux**
Documents du Référentiel de l'Annuaire Santé (accessibles sur le site de l'ANS)		
DA31	[AS-EXTRAC-LIBRE]	**DSFT - Fichiers d'extraction des données en libre accès**
DA32	[AS-API-FIHR]	**Documentation technique de l'API FHIR Annuaire Santé en libre accès**
DA33	[AS-LDAP-MSS]	**DSFT - Consultation des données MSSanté de l'Annuaire Santé par le protocole LDAP**
Documents du Référentiel INS (accessibles sur le site de l'ANS)		
DA41	[INS-REF]	**Référentiel Identifiant National de Santé**
DA42	[INS-RNIV]	**Référentiel National d'Identitovigilance**
Guides de bonnes pratiques ANSSI (accessibles sur le site de l'ANSSI)		
DA51	[ANSSI-TLS]	**Recommandations de sécurité relatives à TLS**
DA52	[ANSSI-CRYPTO]	**Guide de mécanismes cryptographiques**
Documents du Référentiel PSC (accessibles sur le site de l'ANS)		
DA61	[PSC-REF]	**Référentiel Pro Sante Connect**

Tableau 2 : Documents applicables

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante