MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Référentiel socle MSSanté #1

Opérateurs de Messageries Sécurisées de Santé

Version : 1.6.0
Date : 20/03/2024

MSSanté
Système de messageries sécurisées, données protégées.

Identification du document	
Référence ANS	**MSS_Référentiel_#1_Opérateurs_MSSanté_v1.6.0.pdf**
Date de dernière mise à jour	**20/03/2024**
Classification	**Non sensible public**
Nombre de pages	239

Historique du document		
Version	Date	Commentaires
V0.9.0	06/05/2013	Version de travail soumise pour avis aux acteurs de terrain
V0.9.5	12/09/2013	Version diffusée pour concertation
V1.0.0	19/03/2014	Version initiale
V1.0.9	06/07/2016	Version diffusée pour concertation
V1.1.0	15/09/2016	Version introduisant notamment l'utilisation de certificats IGC-Santé dans l'Espace de Confiance. Elle nécessite un réengagement de conformité.
V1.2	15/05/2018	Version introduisant principalement le changement des coordonnées de contacts.
V1.2.1	21/12/2018	Version apportant des précisions sur certains éléments existants du Référentiel #1 et de nouvelles recommandations.
V1.3	14/11/2019	Version introduisant : - Le cycle de vie des BAL - Les nouveaux indicateurs et la procédure de dépôt - Nouvelles règles de publication dans l'Annuaire Santé concernant les codes professions et l'identifiant structure
V1.3.1	11/03/2020	Version apportant certaines modifications/corrections mineures au document et concernant : - la suspension des BAL : les exigences précédemment publiées sont dorénavant des recommandations - les statistiques d'utilisation : la valeur du champ Date du fichier Connexions est précisée dans le cas où l'information de connexion n'est pas disponible - les statistiques d'utilisation : recommandation apportée concernant les BAL applicatives et la date de dernière connexion
V1.4	26/05/2021	Version introduisant : - l'existence d'un Opérateur usagers hébergeant les BAL des usagers ; - la notion d'Opérateur professionnels pour qualifier les Opérateurs offrant un service MSSanté à des professionnels habilités ; - une précision portant sur les exigences relatives à la production des statistiques d'utilisation EX_PSU_5020 afin de ne pas transmettre l'INS présent dans les adresses mail des usagers ; - la modification de l'exigence EX_DCU_5010 portant sur les clauses CGU à intégrer dans celles des services Opérateurs.
V 1.5	22/04/2022	Version publiée après concertation publique du 28/03/22 au 06/04/22.
V 1.5.1	09/09/2022	Version modificative portant sur l'exigence EX_GBM_4440 et le délai de mise en conformité de la v1.5
V 1.6-concertation	30/10/2023	Version publiée pour concertation publique.
V1.6.0	20/03/2024	Version majeure (nécessitant mise en conformité) introduisant en particulier les notions de délégation de BAL et BAL organisationnelles rattachées à des personnes physiques. Pour plus de détails se reporter au §1.4.

Sommaire

1 Introduction

1.1 Objet du document

Ce document décrit les principes, les exigences à respecter, les interfaces d'accès et les fonctionnalités à prendre en compte pour tout Opérateur de messagerie souhaitant intégrer le système de « ***Messageries Sécurisées de Santé*** » (*ci-après désigné système MSSanté*). Ce système assure l'**interopérabilité des services de l'ensemble des Opérateurs raccordés à l'Espace de Confiance MSSanté (ci-après « Opérateurs »)** en permettant l'échange de données de santé en toute sécurité.

Outre ce chapitre 1 introductif, le document est composé des chapitres suivants :

- Le chapitre 2 présente le **contexte du système MSSanté** au regard des missions et projets de l'ANS ;
- Le chapitre 3 décrit **la procédure d'intégration à l'Espace de Confiance MSSanté** ;
- Le chapitre 4 expose les **principes généraux du système MSSanté** ;
- Le chapitre 5 présente le **cycle de vie des boites aux lettres MSSanté** ;
- Le chapitre 6 décrit les **transactions pour les Opérateurs MSSanté (exigences fonctionnelles et techniques)** ;
- Le chapitre 7 définit les modalités **de contrôle et les sanctions** applicables ;
- Le chapitre 8 présente une **synthèse des exigences** applicables ;
- Le chapitre 9 regroupe les **annexes** qui présentent en particulier la définition des termes et abréviations utilisées, les canaux de contacts, ainsi que la liste des documents applicables.

1.2 Guide de lecture

Ce document est destiné en premier lieu aux Opérateurs de messagerie candidats à l'intégration à l'Espace de Confiance MSSanté, mais il permet aussi à tout acteur de l'écosystème e-santé (dont en particulier les éditeurs de LPS) d'appréhender les principes de l'Espace de Confiance MSSanté.

Profil du lecteur / chapitres à lire en priorité

Selon son profil, le lecteur pourra se concentrer sur certains chapitres spécifiques :

Profil du lecteur	Chapitres
Décideurs	2 et 4
Directeurs techniques, Chefs de projets	2 à 7
Développeurs, architectes logiciels, consultants techniques	5 et 6

Exigence

EXIGENCE

Une exigence est une règle de gestion (fonctionnelle ou technique) obligatoire que l'Opérateur doit nécessairement implémenter dans son service de messagerie pour intégrer l'Espace de Confiance.

Généralement les exigences s'appliquent aux deux types d'Opérateurs (professionnels / usagers). Dans certains cas, elles peuvent s'appliquer qu'à un seul type d'Opérateur.

L'applicabilité se distingue par les logos suivants :

 exigence uniquement applicable aux Opérateurs professionnels

 exigence uniquement applicable à l'Opérateur usagers

  exigence applicable aux Opérateurs professionnels **ET** à l'Opérateur usagers

Recommandation

RECOMMANDATION

Une recommandation vise à aider l'Opérateur lors de la mise en œuvre ou la maintenance de son service de messagerie. La mise en œuvre d'une recommandation n'est pas obligatoire.

1.3 Gestion des versions successives

Le **Référentiel #1** sera mis à jour notamment pour prendre en compte les évolutions fonctionnelles, juridiques, techniques ou de sécurités apportées au système MSSanté.

Une version majeure « vX.Y » du Référentiel #1 présente des évolutions (ajout/retrait/modification) d'exigences qui impliquent une mise en conformité des Opérateurs présents dans l'Espace de Confiance. A l'inverse une version mineure « vX.Y.z » n'entraine pas d'évolution des exigences et n'impose pas de mise en conformité des Opérateurs. Elles permettent d'apporter des correctifs ou des précisions aux spécifications, mais ne nécessitent pas de mise en conformité de la part des Opérateurs.

Les nouvelles versions du Référentiel #1 sont produites en concertation avec les Opérateurs. L'ANS informe les Opérateurs de la publication d'une nouvelle version du Référentiel #1.

La date de publication du Référentiel #1 constitue le début du délai de mise en conformité défini au §1.5.

Les Opérateurs sont informés des dernières mises à jour du Référentiel #1 par courrier électronique.

Toute autre personne peut être informée des évolutions du Référentiel #1 en s'abonnant à la liste de diffusion sur simple demande à l'adresse monserviceclient.mssante@esante.gouv.fr.

1.4 Différences avec la précédente version

Le tableau suivant référence les **différences majeures avec la version 1.5.1 du 22/04/2022**.

Paragraphe Réf. #1 v1.6	Changement
2.3	Précision des conditions d'échange dans le système MSSanté
2.4.3	Ajout de nouveaux rôles et reformulation de rôles existants
3	Nouvelle procédure de déclaration de conformité au Référentiel #1
5.1	Ajout de 2 exigences sur les types de BAL à proposer par les opérateurs (EX_GBM_3010, EX_GBM_3040) et introduction des BAL ORG utilisable dans des structures sans FINESS (cabinets libéraux, …)
5.1.4	Notion de BAL active : délai d'inactivité passé de 30 à 60J afin de s'aligner avec la fonction de dépublication
5.2	Précisions des acteurs éligibles par type de BAL
5.3	Nouvelle exigence sur le nommage des BAL personnelles
5.4.2	Introduction des exigences relatives aux mécanismes de délégation des BAL
6.2.1	Arrêt de la compatibilité TLS 1.0/1.1 sur l'interface SMTP entre opérateurs. Seul TLS 1.2 ou supérieur sont supportés
6.4	Nouvelles exigences sur l'emploi des FINESS géographiques (EX_PBA_5011) Suppression de l'utilisation de la notion de « dématérialisation / zéro papier » Fichier d'alimentation annuaire modifié pour supporter les BAL ORG avec cotitulaires (voir §6.4.2.3.3.4)
6.5	Modification des structures de données permettant de récupérer les données des BAL afin de supporter la restitution des cotitulaires des BAL ORG sous-type CAB
6.5.2	La transaction TM2.1.3 de téléchargement d'une extraction de l'Annuaire Santé sera décommissionnée courant 2025
6.8.3	Modification de l'exigence relative au mécanisme d'autoconfiguration (usage du DNS)
6.9.3	Adaptation des CGU : augmentation de la durée de conservation de traces (2 ans) par l'ANS afin de faire face à des recours éventuels à la suite des dispositifs de financement, introduction

Paragraphe Réf. #1 v1.6	Changement
	des fonctions de délégation, bascule d'exigences opérateurs vers les utilisateurs professionnels
9.5	DR5 modifié afin d'adapter les schémas (XSD) pour les transactions d'alimentation de l'Annuaire Santé et de téléchargement d'une extraction de l'Annuaire Santé

Tableau 1 : Principales modifications introduites dans la v1.6

Les exigences ajoutées ou modifiées dans cette version sont surlignées en jaune dans le tableau de synthèse de exigences au §8.

1.5 Délai de mise en conformité au Référentiel #1 Opérateur v1.6

Comme prévu dans le contrat « Opérateur MSSanté v2 », ce paragraphe précise le délai de mise en conformité des Opérateurs suivant la publication d'une version majeure du Référentiel #1.

Après concertation avec les opérateurs MSSanté, un délai de 10 mois après publication de la version finale du Référentiel #1 version 1.6 a été retenu. La limite de mise en conformité est donc fixée au 19/01/2025.

L'Opérateur doit, avant la fin du délai de mise en conformité, transmettre à l'ANS un rapport des tests effectué sur l'Outil de tests et de contrôles qui devra démontrer sa conformité au Référentiel #1 version 1.6.

Le rapport de tests doit être envoyé à l'ANS à l'adresse suivante : monserviceclient.mssante@esante.gouv.fr

1.6 Obligations des Opérateurs suite à une publication d'une version majeure du Référentiel #1

EX_GEN_0100

Pour chaque nouvelle version majeure du Référentiel #1, tous les Opérateurs présents dans l'Espace de Confiance de production doivent démontrer leur conformité à la dernière version du Référentiel #1 publié, par le biais de l'Outil de tests et de contrôles, dans le respect du délai de mise en conformité précisé dans le Référentiel #1. La mise en conformité de l'Opérateur est vérifiée par l'ANS à travers les résultats de ce rapport de tests conformément à la procédure de contrôle définie au chapitre 7.1.

Le rapport de tests doit être adressé à l'ANS à l'adresse monserviceclient.mssante@esante.gouv.fr.

À défaut de production et transmission du rapport de tests, la procédure de sanction prévue au §7.2 peut être mise en œuvre.

2 Les principes du système de Messageries Sécurisées de Santé

2.1 Contexte de mise en œuvre du système de Messageries Sécurisées de Santé

Depuis le lancement du système MSSanté en 2012, la loi a défini de nouveaux modes d'exercice médical et ouvert la voie au développement de la « e-santé » pour l'ensemble des professions de santé. Elle a également confirmé la place centrale du patient en renforçant ses droits et en lui proposant de nouveaux services. Dans ce cadre, le rôle de l'ANS consiste à structurer les systèmes d'information qui pourront répondre aux besoins des professionnels de santé, au bénéfice du patient. L'enjeu est donc de familiariser les professionnels de santé à la logique de l'échange et du partage des donnés de santé tout en garantissant aux patients la qualité de la relation soignant/patient qui nécessite de garantir la confidentialité de leurs données de santé.

Avant le lancement du projet, des messageries nationales, régionales ou locales, s'étaient développées, mais de façon limitée par le nombre de professionnels de santé concernés, par l'absence d'interopérabilité, et par le respect partiel des obligations liées à la confidentialité des données de santé à caractère personnel. Partant de ce constat, les pouvoirs publics ont décidé, en concertation avec les ordres professionnels, d'accélérer la mise à disposition d'une offre de service interopérable à destination des professionnels habilités à collecter et échanger des données de santé à caractère personnel. L'ANS promeut ainsi un système de Messageries Sécurisées de Santé (MSSanté) en mettant en place le cadre pour le développement de services interopérables de messageries sécurisées de santé et en permettant aux messageries existantes de développer leurs usages en s'inscrivant dans un Espace de Confiance commun.

La conception du système MSSanté est réalisée en concertation avec les industriels et les organisations représentatives des professionnels de santé.

En outre, la prise en charge des patients dépasse aujourd'hui l'échange de données de santé entre les seuls professionnels de santé. Le législateur autorise ainsi d'autres professionnels à collecter des données de santé dans le cadre de la prise en charge sanitaire, sociale et médico-sociale d'une personne. L'échange de données de santé est donc possible entre professionnels de santé et plus largement entre tous professionnels habilités par la loi à collecter et échanger des données de santé dans le cadre de ses missions de prise en charge d'un patient (cf. article L.1110-4 du code de la santé publique).
Le système MSSanté est donc destiné à l'ensemble des professionnels susvisés. L'ANS conduit des travaux pour permettre une ouverture de l'Espace de Confiance MSSanté à l'ensemble des professionnels cités.

Conformément aux dispositions de la loi n°2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé et ses textes d'application, le champ du système MSSanté est élargi afin d'intégrer dès 2021 les échanges entre les professionnels habilités et les usagers du système de santé.

Par convention, le présent Référentiel #1 utilise **la notion de « professionnel habilité »** pour désigner 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 patient pour lequel il intervient dans la prise en charge. La liste de ces professionnels a été définie par le décret n° 2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel (cf. article R.1110-2 2° du code de la santé publique).

La notion « d'usager » désigne toute personne physique pouvant bénéficier du système de santé français.

2.2 Définition du système de Messageries Sécurisées de Santé

En définissant les conditions de développement du système MSSanté, les pouvoirs publics répondent à une attente des acteurs de faciliter leurs échanges interprofessionnels, indispensables à la prise en charge de leurs patients, ainsi que leurs échanges avec les usagers dans le respect de la loi et de l'éthique professionnelle.

Afin que des professionnels adhèrent à l'utilisation de messageries sécurisées de santé, les Opérateurs doivent proposer des services de messagerie répondant aux principes suivants :

- Universalité : tous les professionnels habilités, quels que soient leurs modes d'exercice, doivent être en capacité de disposer d'un compte de messagerie sécurisée permettant d'échanger avec tous les professionnels habilités, quels que soient les outils utilisés ;
- Simplicité : l'émission et la consultation des messages sécurisées ne modifient pas les pratiques habituelles sur d'autres outils de messageries, y compris en mobilité ;
- Sécurité : l'utilisation d'une Messagerie Sécurisée de Santé doit assurer la confidentialité des données de santé à caractère personnel échangées.

Le système MSSanté est un système de messagerie électronique « standard » d'émission et de réception de messages électroniques qui permet :

- d'échanger par voie électronique de façon sécurisée et dans un espace fermé des données de santé à caractère personnel entre professionnels habilités (messagerie interprofessionnelle) ainsi qu'entre ces professionnels habilités et les usagers ;
- d'échanger des contenus structurés entre applicatifs en s'appuyant sur la messagerie (messagerie inter-applicative) ;
- d'alimenter des systèmes d'information (SI) de l'Espace de Confiance à l'occasion d'échanges de messages entre acteurs de santé.

Le système MSSanté est fondé sur « l'Espace de Confiance MSSanté »

L'Espace de Confiance MSSanté est le regroupement de tous les Opérateurs de messageries sécurisées de santé respectant les règles du Référentiel #1 et ayant contractualisé avec l'ANS qui en assure sa régulation. L'Espace de Confiance garantit la confidentialité, l'intégrité et la traçabilité des données qui sont échangées entre les Opérateurs qui le composent.

Les services ANS de l'Espace de Confiance MSSanté de production désigne l'environnement de production mis à disposition par l'ANS aux Opérateurs, leur permettant de fournir un service de messageries sécurisées de santé pour l'échange sécurisé de données à caractère personnel, dont des données de santé, entre professionnel habilité et usager. Il est constitué de :

- l'Annuaire Santé des professionnels intervenant dans le système de santé et des structures de santé s'appuyant notamment sur le répertoire partagé des professionnels intervenant dans le système de santé ;
- une liste blanche de domaines MSSanté regroupant les domaines des Opérateurs intégrés à l'Espace de Confiance ;

- un service permettant la soumission et la production de statistiques d'utilisation des BAL MSSanté ;
- des référentiels permettant aux industriels de développer des offres conformes et interopérables entre elles. Ces référentiels comportent les documents de référence : le présent **Référentiel #1** Opérateurs de messagerie, le Référentiel #2 Clients de Messageries Sécurisées de Santé [MSS-REF2].

Les services ANS de l'Espace de Confiance MSSanté de test désigne l'environnement mis à disposition par l'ANS aux Opérateurs, leur permettant de réaliser des tests de bout en bout dans un environnement disjoint de l'environnement de production. L'utilisation de l'Espace de Confiance de test n'implique pas le traitement de données à caractère personnel réelles. Il est constitué de :

- l'Annuaire Santé de test ;
- une liste blanche de domaines MSSanté de test ;
  un service permettant la gestion de statistiques d'utilisation des BAL MSSanté de test ;
- les outils de test de conformité (MOTCO 1 & 2) ;
- le Référentiel #1.

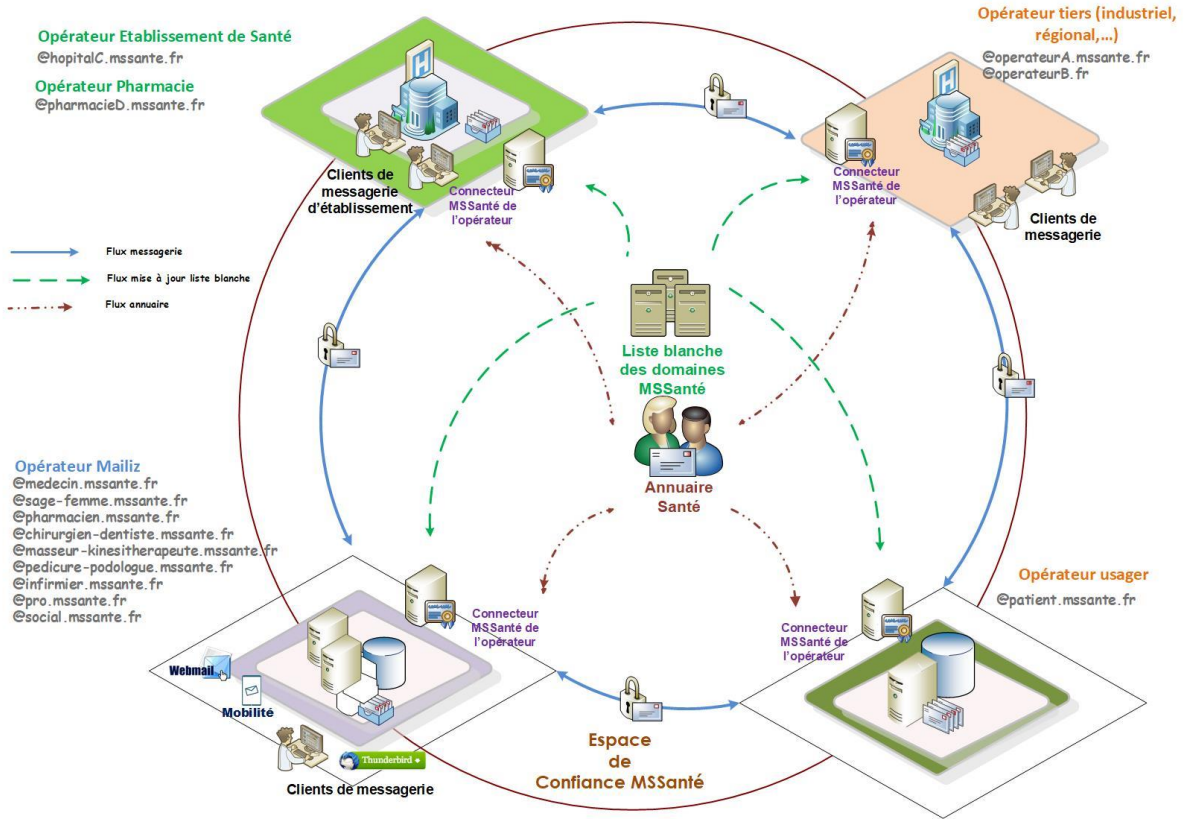


Figure 1 : Échanges au sein du système MSSanté

2.3 Un système de Messageries Sécurisées de Santé conforme au cadre juridique

Au regard de sa finalité, qui est d'échanger des données à caractère personnel dont des données de santé, le système MSSanté est développé dans le respect du Règlement général sur la protection des données, ci-après RGPD[1], ainsi que de la loi n°78-17 du 6 janvier 1978.

Depuis l'entrée en vigueur du RGPD, les responsables de traitement n'ont plus à effectuer d'engagement de conformité à l'autorisation unique CNIL n°37 (« AU 37 »), et doivent désormais documenter leur conformité au RGPD via leur documentation interne (registre des traitements de données à caractère personnel, AIPD, etc.).

En outre, le système MSSanté est développé dans le respect des dispositions 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.

L'article L. 1110-4 du code précité définit les conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social. Cela signifie qu'en principe les professionnels qui pourront utiliser une BAL MSSanté doivent être des professionnels habilités par le code de la santé publique à échanger et partager des données relatives au patient qu'ils prennent en charge.

Conformément aux dispositions de l'article L. 1110-4 du code précité, un professionnel habilité peut échanger avec un ou plusieurs professionnels habilités des informations relatives à un même patient, à condition qu'ils participent tous à sa prise en charge et que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou à son suivi médico-social et social.

Le partage, entre professionnels ne faisant pas partie de la même équipe de soins (cf. article L. 1110-2 du code de la santé publique), d'informations nécessaires à la prise en charge d'un patient requiert son consentement préalable, recueilli par tout moyen, y compris de façon dématérialisée.

Lorsque les professionnels appartiennent à la même équipe de soins, ils peuvent échanger les informations strictement nécessaires à la coordination, à la continuité des soins ou au suivi médico-social et social du patient pris en charge. Ces informations sont présumées confiées par le patient à l'ensemble de l'équipe.

L'échange et le partage des informations nécessaires à la prise en charge d'une personne aux professionnels agissant sous la responsabilité d'un professionnel habilité s'effectuent dans le respect de l'article R.4127-72 du code de la santé publique.

La personne prise en charge dispose du droit de s'opposer, à tout moment, à l'échange et au partage de ses données. Cette dernière doit être dûment informée de son droit d'exercer une opposition à l'échange et au partage d'informations la concernant.

Toute atteinte au secret professionnel par un professionnel habilité ou tout professionnel agissant sous sa responsabilité peut faire l'objet de sanctions pénales ou disciplinaires. Conformément à l'article 226-13 du code pénal, la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

d'une fonction ou d'une mission temporaire (professionnel de santé ou médico-social, personnel administratif, etc.), est punie d'un an d'emprisonnement et de 15 000 euros d'amende.

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, parmi lesquels figurent les référentiels de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S).

Dans la mesure où un service de messageries sécurisées de santé assure l'échange de données de santé à caractère personnel, l'Opérateur doit également organiser la conservation des données de santé échangées par les utilisateurs de son service. Cette conservation 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 (Opérateur ou prestataire de l'Opérateur) pour le compte d'un tiers d'être titulaire de l'agrément ou du certificat de conformité prévu à cet effet.

La procédure d'agrément définie par le décret 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel (anciens articles R.1111-9 et suivants du code de la santé publique) a été remplacée par une procédure de certification précisée par le décret n° 2018-137 du 26 février 2018, lui-même précisé par un référentiel d'accréditation et un référentiel de certification rendus opposables par voie d'arrêté.

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.

Remarque : le présent Référentiel #1 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.

2.4 Les acteurs de l'Espace de Confiance MSSanté

2.4.1 L'ANS

Dans le cadre du système MSSanté, l'ANS assure deux rôles :

- **Gestionnaire de l'Espace de Confiance MSSanté** : qui inclut la gestion de l'Annuaire Santé et l'administration de la liste blanche qui regroupe l'ensemble des domaines de messagerie des Opérateurs autorisés à échanger au sein de l'Espace de Confiance MSSanté. En cette qualité, l'ANS définit les règles d'intégration à l'Espace de Confiance MSSanté. Ces règles sont énoncées dans le contrat relatif à l'intégration à l'Espace de Confiance appelé contrat « Opérateur MSSanté v2 » [CONTRAT-MSSANTE] conclu entre l'ANS et tout Opérateur souhaitant intégrer l'Espace de Confiance MSSanté.
- **Opérateur du service Mailiz en lien avec des Ordres professionnels :** L'ANS offre un service standard de messagerie, mis à disposition des professionnels habilités afin d'amorcer la dynamique du système, en lien avec les Ordres professionnels.

2.4.2 Les Opérateurs de messageries sécurisées de santé

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

Un service de messageries sécurisées de santé (« service MSSanté ») désigne le service proposé par un Opérateur à des Utilisateurs professionnel ou usager (« utilisateurs finaux »).

Il s'agit d'un service standard d'émission et de réception de messages électroniques accompagnés ou non de documents (pièces-jointes) qui intègre des fonctionnalités spécifiques répondant aux besoins de garantir la sécurité et la confidentialité des données de santé échangées.

L'arrivée des usagers au sein de l'Espace de Confiance conduit à distinguer la notion d'Opérateur professionnels et d'Opérateur usagers :

- **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 peuvent être une structure de soins (établissement de santé, …), un ESMS, 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 MES.

L'ANS, comme indiqué ci-dessus, est un Opérateur de l'Espace de Confiance, via le service de messagerie Mailiz.

Pour proposer un service de Messageries Sécurisées de Santé raccordé à l'Espace de Confiance, un Opérateur MSSanté doit avoir conclu le contrat « Opérateur MSSanté v2 » [CONTRAT-MSSANTE] avec l'ANS, qui a pour objet de déterminer les conditions d'intégration de l'Opérateur à l'Espace de Confiance MSSanté (se reporter au § 2.5 du présent **Référentiel #1**) et respecter les obligations qui y sont définies.

Afin de permettre l'ouverture de l'Espace de Confiance aux usagers, l'ANS a conclu avec la Cnam une convention venant encadrer les conditions de son intégration au sein du système MSSanté, en sa qualité d'Opérateur usagers. La Cnam est chargée, avec le Ministère chargé de la santé, du développement de MES, dont l'une des composantes est la messagerie usagers, conformément aux dispositions de la loi n°2019-774 du 24 juillet 2019 et de ses textes d'application.

Pour plus d'information concernant l'intégration des Opérateurs à l'Espace de Confiance MSSanté, se reporter au §2.5 «Intégration des Opérateurs professionnels à l'Espace de Confiance MSSanté ».

La sécurité du service de messagerie mis en œuvre par l'Opérateur repose sur des fonctions de sécurité du Connecteur MSSanté de l'Opérateur mais aussi sur des conditions de gestion du service conformes à une politique de sécurité des systèmes d'information (PSSI) à l'état de l'art. Le terme « Connecteur MSSanté » utilisé dans la suite du document correspond à l'ensemble des équipements qui concourent à l'interconnexion à l'Espace de Confiance MSSanté.

L'Opérateur a le libre choix des solutions techniques, logicielles et organisationnelles pour la mise en œuvre des mesures de sécurité dans le respect des exigences présentées dans le présent **Référentiel #1** et des besoins de sécurité du service.

L'Opérateur est aussi en charge de la sécurité des échanges avec les logiciels métiers qui fournissent des fonctionnalités de messagerie aux utilisateurs finaux. L'API LPS, décrite au §6.8, présente les modalités de sécurisation à respecter, ainsi que les transactions à proposer.

2.4.3 Les personnes physiques intervenant dans l'Espace de Confiance MSSanté

Le tableau ci-dessous a pour objectif de lister l'ensemble des rôles que peuvent jouer les personnes physiques intervenant dans l'Espace de Confiance MSSanté.

Rôle	Description
Utilisateur professionnel d'une BAL MSSanté	Désigne tout professionnel habilité par la loi à échanger des données de santé à caractère personnel, conformément aux articles L.1110-4 et R. 1110-2 du code de la santé publique, ainsi que les professionnels intervenant dans le système de santé agissant sous la responsabilité d'un professionnel habilité. C'est un utilisateur d'un service MSSanté proposé par un Opérateur professionnels. L'Utilisateur professionnel désigne tout Responsable opérationnel, Cotitulaire ou Délégataire d'une BAL MSSanté.
Utilisateur usager d'une BAL MSSanté	Désigne les usagers du système de santé utilisant la MSSanté pour échanger avec des professionnels habilités. C'est un utilisateur du service MSSanté proposé par l'Opérateur usagers.
Utilisateur final	Désigne les Utilisateurs professionnel et Utilisateurs usager.
Responsable opérationnel d'une BAL MSSanté	Le rôle du Responsable opérationnel varie en fonction du type de BAL concerné : • **Le Responsable opérationnel d'une BAL personnelle** est le professionnel habilité titulaire de la BAL. Il est responsable de la création et de suppression de sa propre BAL. Il peut déléguer l'accès à sa boite à un professionnel agissant sous sa responsabilité (le « Délégataire »). • **Le Responsable opérationnel d'une BAL organisationnelle rattachée à une structure FINESS** désigne un professionnel habilité ou un professionnel exerçant son activité au sein de la structure. Il est chargé de la création et de la suppression de la BAL et bénéficie du droit d'autoriser l'accès à la BAL organisationnelle. Dans le cas où le Responsable opérationnel n'est pas un professionnel habilité, il n'est pas habilité à accéder à la BAL organisationnelle et aux données des patients pris en charges. • **Le Responsable opérationnel d'une BAL organisationnelle rattachée à une personne physique** désigne le professionnel habilité chargé de la création et de la suppression de la BAL. Il dispose du droit d'autoriser l'accès à la BAL organisationnelle à un Cotitulaire ainsi que du droit de déléguer l'accès à un Délégataire. • **Le Responsable opérationnel d'une BAL applicative** désigne un professionnel habilité ou professionnel exerçant son activité au sein de la structure, chargé de la création et de la suppression de la BAL. Dans le cas où le Responsable opérationnel n'est pas un professionnel habilité, il n'est pas habilité à accéder à la BAL et aux données des patients pris en charge. Il s'assure que les échanges réalisés au moyen de la BAL respectent les finalités de prise en charge précisées dans les dispositions relatives à l'échange et au partage de données de santé. Le Responsable opérationnel est responsable des accès qu'il pourrait ouvrir par délégation ou pour toute autre habilitation d'accès à la BAL organisationnelle. Il doit notamment s'assurer que les professionnels qu'il ajoute sont habilités à accéder aux informations relatives aux patients pris en charge conformément aux dispositions relatives au secret professionnel et à l'échange et au partage de données de santé rappelées au §2.3 du présent Référentiel #1. Seul le Responsable opérationnel agissant en qualité de professionnel habilité peut accéder à une BAL organisationnelle. Le responsable de traitement s'assure qu'un Responsable opérationnel soit identifié pour chaque BAL personnelle, organisationnelle ou applicative.

Cotitulaire d'une BAL organisationnelle (ou Cotitulaire)	Désigne un professionnel habilité qui a été autorisé par le Responsable opérationnel ou un Cotitulaire à accéder à une BAL organisationnelle. Un Cotitulaire dispose du droit d'autoriser l'accès à la BAL organisationnelle à un autre Cotitulaire ainsi que du droit de déléguer l'accès à un professionnel agissant sous sa responsabilité (le « Délégataire »). Un Cotitulaire ne peut pas demander la création / suppression de la BAL organisationnelle. Chaque Cotitulaire est responsable des informations qu'il va échanger et partager dans le cadre de son utilisation de la BAL. Il est également responsable des accès qu'il pourrait ouvrir par délégation ou pour toute autre habilitation d'accès à la BAL organisationnelle. Il doit notamment s'assurer que les professionnels qu'il ajoute sont habilités à accéder aux informations relatives aux patients pris en charge conformément aux dispositions sur le secret professionnel et l'échange et le partage de données de santé rappelées à l'article 2.3 du présent Référentiel #1. L'ouverture de tout nouvel accès à la BAL organisationnelle par un Cotitulaire est conditionnée par l'information, par tout moyen, de l'ensemble de Cotitulaires de la BAL.
Délégataire d'une BAL personnelle ou organisationnelle	Désigne un professionnel, qui a été autorisé par le Responsable opérationnel ou un Cotitulaire à accéder à la BAL organisationnelle ou personnelle dont il a la charge. Un Délégataire est un professionnel intervenant dans le système de santé (secrétaire, assistant médicale, médecin remplaçant, etc.) agissant sous la responsabilité et pour le compte du Responsable opérationnel ou Cotitulaire auquel il est rattaché. Un Délégataire dispose du droit de consulter et/ou d'envoyer des messages via la BAL à laquelle il a accès. Un Délégataire ne peut accéder aux données relatives aux patients que sous la responsabilité d'un professionnel habilité, dans le strict cadre de ses missions et dans le respect des obligations relatives au secret professionnel.
Gestionnaire des BAL MSSanté au sein de la structure	Désigne la personne rattachée à une structure et chargée de gérer la liste des professionnels habilités à disposer d'une BAL MSSanté (nominative ou non) au sein de sa structure (établissement de santé, etc.). C'est lui qui communique à l'Opérateur les changements à opérer sur les BAL : création, suppression, modification des accès (BAL organisationnelles).
Le chef de projet technique	Désigne la personne exerçant pour le compte de l'Opérateur MSSanté et identifié comme le point de contact de l'Opérateur dans la liste blanche avec ses coordonnées. Le régulateur de l'Espace de Confiance ou tout Opérateur doit pouvoir le contacter pour toute question d'ordre technique.
Le chef de projet fonctionnel	Désigne la personne exerçant pour le compte de l'Opérateur MSSanté et identifié comme le point de contact de l'Opérateur dans la liste blanche avec ses coordonnées. Le régulateur de l'Espace de Confiance ou tout Opérateur doit pouvoir le contacter pour toute question d'ordre fonctionnelle.
Administrateur technique	Désigne la personne en charge des taches d'administration de l'Opérateur MSSanté. A ce titre, il a signé avec son employeur un engagement de confidentialité du fait de la nature des données traitées par l'Opérateur.

2.5 Intégration des Opérateurs professionnels à l'Espace de Confiance MSSanté

On distingue deux modalités d'accès à l'Espace de Confiance MSSanté.

2.5.1 Devenir Opérateur MSSanté.

Un Opérateur professionnels MSSanté opère et propose un service de Messageries Sécurisées de Santé pour répondre aux besoins d'échanges de données de santé des professionnels qui exercent en son sein ou qui sont rattachés à lui dans le cadre d'une organisation de prise en charge des patients et qui met ce service à disposition de ses professionnels habilités. Ce sera par exemple le cas d'une structure de soins qui souhaite proposer la messagerie sécurisée MSSanté pour le bénéfice des professionnels qu'elle emploie.

Pour proposer un service de Messageries Sécurisées de Santé raccordé à l'Espace de Confiance, un Opérateur doit avoir conclu le contrat « Opérateur MSSanté v2 » [CONTRAT-MSSANTE] avec l'ANS qui définit les conditions d'intégration de l'Opérateur à l'Espace de Confiance MSSanté.

L'intégration des Opérateurs à l'Espace de Confiance s'effectue en deux temps. Ils intègrent dans un premier temps l'Espace de Confiance de tests avant de pouvoir ensuite intégrer l'Espace de Confiance de production.

Pour plus d'information concernant le contrat « Opérateur MSSanté v2 » ainsi que la procédure d'intégration, se reporter au §3.

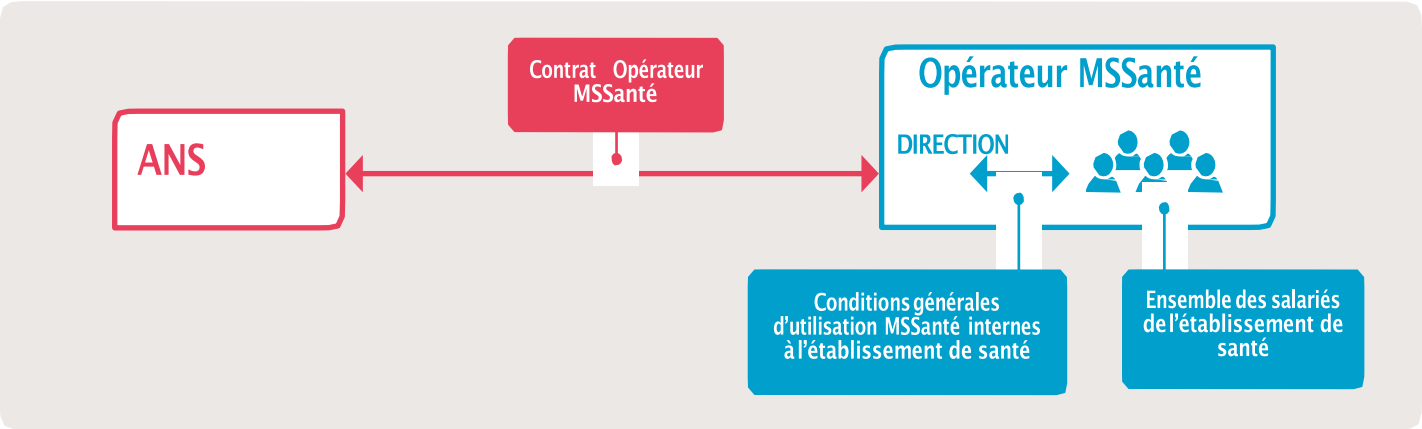


Figure 2 : « Chaîne contractuelle » pour un Etablissement de santé qui est Opérateur MSSanté

2.5.2 Utiliser les services d'un Opérateur MSSanté déjà intégré à l'Espace de Confiance

Dans ce cas, il s'agit de passer par un Opérateur professionnels qui opère et propose un service de Messageries Sécurisées de Santé pour le compte d'entités ou de personnes tierces dans le cadre d'un contrat de prestation de service (ou équivalent). Cet Opérateur professionnels peut être par exemple un industriel qui propose des services de messagerie sécurisée à des clients qui peuvent aussi bien être des structures sanitaires, médico-sociales ou sociales que des professionnels libéraux.

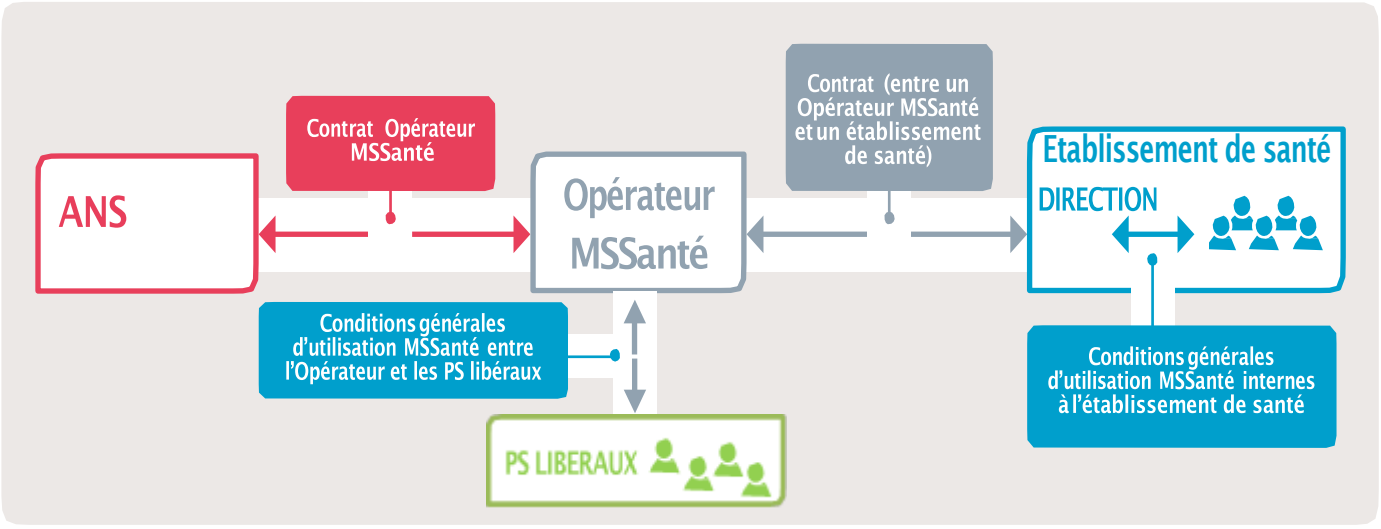


Figure 3 : « Chaîne contractuelle » pour un Opérateur MSSanté qui propose un service de Messageries Sécurisées de Santé à des professionnels de santé libéraux ainsi qu'à un établissement de santé.

2.6 Focus sur la documentation relative aux données personnelles à mettre en place par le responsable de traitement

Les responsables de traitement n'ont plus à réaliser l'engagement de conformité à l'autorisation unique n°37 mais doivent documenter leur conformité conformément aux dispositions du RGPD.

L'obligation de mettre en place la documentation relative aux données personnelles :

Avant l'entrée en vigueur du RGPD, pour permettre aux professionnels habilités utilisant une Messageries Sécurisées de Santé de respecter les obligations de la loi Informatique et Libertés, la CNIL avait élaboré une autorisation unique dont l'objet était de définir les conditions de mise en œuvre d'un traitement de données de santé à caractère personnel au moyen d'un outil de Messageries Sécurisées de Santé.

C'était l'objet de la délibération n° 2014-239 du 12 juin 2014 portant autorisation unique AU-037 de mise en œuvre, par les professionnels et établissements de santé ainsi que par les professionnels du secteur médico-social habilités par une loi, de traitements de données à

caractère personnel ayant pour finalité l'échange par voie électronique de données de santé à travers un système de messagerie sécurisée[2].

Après l'entrée en vigueur du RGPD, les professionnels n'ont plus à effectuer d'engagement de conformité à l'autorisation unique CNIL n°37 (« AU 37 »), et doivent désormais documenter leur conformité au RGPD via leur documentation interne (registre des traitements de données à caractère personnel, AIPD, etc.).

Détermination de la qualité de responsable de traitement :

Dans le cadre du système MSSanté, les professionnels habilités utilisant des services de Messageries Sécurisées de Santé proposés par un Opérateur, ou dans certains cas la structure de rattachement de ces professionnels, ont la qualité de responsable de traitement. En effet, ils détiennent la responsabilité :

- de décider de la mise en œuvre d'un service de messagerie sécurisée ;
- de choisir les moyens afférents à ce service.

Cette responsabilité est attachée soit au professionnel habilité lui-même, soit à la structure sanitaire, médico-sociale ou sociale au sein de laquelle il exerce, en fonction des statuts et des missions de ladite structure.

Les usagers utilisant un service de Messageries Sécurisées de Santé ne sont pas qualifiés comme responsables de traitement.

Détermination des obligations en matière de sous-traitance

Lorsque le responsable de traitement fait appel à un sous-traitant pour la mise à disposition d'un service de Messageries Sécurisées de Santé, il veille à ce que son sous-traitant présente des garanties suffisantes en matière de protection des données. La relation entre le responsable de traitement et son sous-traitant doit être encadrée contractuellement, conformément à l'article 28 du RGPD.

Le contrat de sous-traitance permet notamment de :

- formaliser les rôles et responsabilités du responsable de traitement et de son sous-traitant ;
- prévoir les obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données ;
- s'assurer que le sous-traitant ne traite les données que sur ordre et pour le compte du responsable de traitement, et qu'il ne fasse pas appel à un autre sous-traitant sans l'autorisation préalable du responsable de traitement ;
- prévoir les modalités d'intervention du sous-traitant pour la réalisation de l'AIPD, l'exercice des droits des personnes, la suppression des données, la notification en cas de violation de données à caractère personnel, etc. ;
- encadrer l'assistance du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations.

L'article 28 du RGPD donne une liste précise des exigences qui doivent être prévues dans le contrat de sous-traitance.

De plus, lorsqu'un Opérateur traite l'INS, en qualité de sous-traitant, pour l'activité de référencement des données de santé, le contrat de sous-traitance doit aussi prévoir des dispositions relatives au traitement de l'INS conformément à la règlementation qui lui est applicable.

[2] JORF n°0162 du 16 juillet 2014, Texte n°96

Dans ce cadre le contrat de sous-traitance doit notamment préciser les conditions et modalités dans lesquelles le sous-traitant agit au nom et pour le compte du responsable de traitement afin de procéder au référencement des données de santé avec l'INS. Le contrat doit formaliser l'engagement du sous-traitant à être conforme à la règlementation encadrant l'INS, et notamment au référentiel INS, et décrire les mesures mises en place pour en assurer le respect.

Cas n°1 – vous fournissez un service de Messageries Sécurisées de Santé et vos Utilisateurs professionnel exercent à titre libéral

Dans ce cas,

- **Vos Utilisateurs professionnel sont** :
  - Responsables du traitement de Messageries Sécurisées de Santé ;
  - En charge de la mise en conformité au RGPD à réaliser pour les traitements de données personnelles effectués via le service MSSanté.
- **Vous êtes** :
  - Opérateur professionnels.

En tant qu'Opérateur, vous êtes considéré comme un « sous-traitant » au sens de la loi Informatique et Libertés.

Vous devez garantir à vos Utilisateurs professionnel que votre service respecte le cadre juridique applicable aux traitements de messageries sécurisées de santé.

Pour rappel, vous restez responsable des traitements internes relatifs à l'exercice de votre activité (fichiers, clients, ressources humaines, etc.).

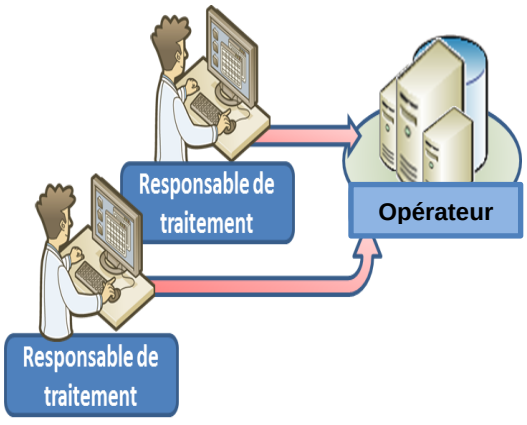


Figure 4 : PS libéral utilisant le service MSSanté proposé par un Opérateur

Cas n°2 - Une structure sanitaire, médico-sociale ou sociale (établissement de santé, laboratoire de biologie médicale, EHPAD, etc.) décide de mettre à la disposition de ses professionnels habilités salariés le service de Messageries Sécurisées de Santé que vous fournissez en tant qu'Opérateur professionnels

Vous proposez le service de Messageries Sécurisées de Santé pour cette structure.

Dans ce cas,

- **La structure est :**
  - Le responsable du traitement de Messageries Sécurisées de Santé ;
  - En charge de la mise en conformité au RGPD à réaliser pour les traitements de données personnelles effectués via le service MSSanté.
- **La structure n'est pas :**
  - Opérateur professionnels.

Vous êtes l'Opérateur du service et êtes considéré comme un « sous-traitant » au sens de la loi Informatique et libertés des traitements de données de santé réalisés via le service de messagerie sécurisée que vous proposez. C'est la structure, en sa qualité de responsable de traitement, qui devra assurer la conformité du traitement au RGPD.

Toutefois, vous devez permettre à la structure de s'assurer du respect de certaines exigences liées à la conformité au RGPD, inhérentes au fonctionnement du service de messagerie.

Pour rappel, vous restez responsable des traitements internes relatifs à l'exercice de votre activité (fichiers, clients, ressources humaines, etc…).

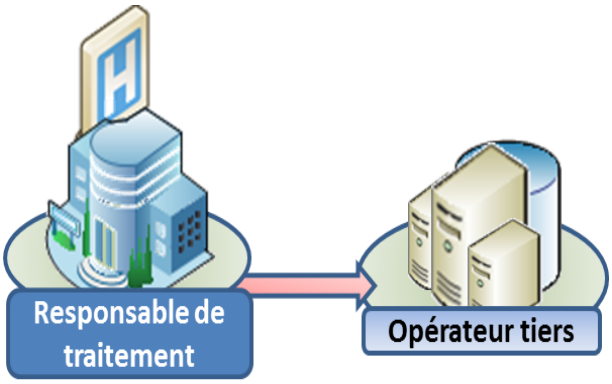


Figure 5 : Structure utilisant le service MSSanté proposé par un Opérateur « tiers »

Cas n°3 - Vous êtes une structure sanitaire, médico-sociale ou sociale et décidez d'opérer votre propre service de Messageries Sécurisées de Santé à destination d'Utilisateurs professionnel

Dans ce cas,

Vous êtes :

- Le responsable du traitement de Messageries Sécurisées de Santé ;
- En charge de la mise en conformité au RGPD à réaliser pour les traitements de données personnelles effectués via le service MSSanté ;
- Opérateur.

Vous avez la qualité d'Opérateur et devez conclure le contrat « Opérateur MSSanté v2 » [CONTRAT-MSSANTE].

Vous avez la qualité de responsable de traitement des données à caractère personnel échangées au moyen du service de Messageries Sécurisées de Santé que vous proposez. À ce titre vous devez assurer la conformité du traitement au RGPD.

Vous devez encadrer l'utilisation de votre service de Messageries Sécurisées de Santé par vos utilisateurs (charte, CGU, etc…).

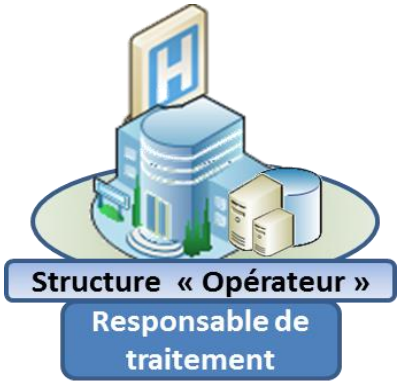


Figure 6 : Structure utilisant son propre service MSSanté en tant qu'Opérateur

2.7 Le domaine mssante.fr, une marque de confiance

Le système MSSanté permet à tout professionnel habilité et à tout usager du système de santé**,** de disposer d'au moins une adresse mail sécurisée. Le système MSSanté est fondé sur la certification des identités des titulaires d'un compte de messagerie et garantit ainsi que l'émetteur et le destinataire du message font partie de l'Espace de Confiance MSSanté.

Un service de Messageries Sécurisées de Santé est identifié dans les adresses mails par la présence du domaine « mssante.fr » marque de reconnaissance de cet Espace de Confiance. Ce domaine doit être intégré dans toutes les adresses de messagerie par les Opérateurs qui le souhaitent.

Les Opérateurs, qu'ils soient publics ou privés (structures de soins, groupements de coopération sanitaire, industriels, etc.) peuvent disposer d'un domaine de messagerie sécurisée correspondant à leur domaine internet, lorsqu'ils en ont un, sur le modèle suivant : xxx@ch-xyz.mssante.fr (ou xxx@ch-xyz.groupe-abc.mssante.fr) ;

L'usage d'une terminaison « mssante.fr » par tous les acteurs de l'Espace de Confiance [3] pour leur adresse de messagerie est une marque de reconnaissance du caractère sécurisé des messages, visible par tout utilisateur et constitue donc un facteur important d'appropriation du système MSSanté.

L'ANS est propriétaire du nom de domaine « mssante.fr », régulièrement enregistré auprès d'un bureau d'enregistrement. Pour le fonctionnement de l'Espace de Confiance MSSanté et des services de Messagerie Sécurisée de Santé, l'ANS concède à l'Opérateur intégré à l'Espace de Confiance le droit d'utiliser le nom de domaine « mssante.fr », dans la limite de l'application des dispositions relatives aux sanctions.

Pour plus d'information sur les conditions d'utilisation du nom de domaine « mssante.fr » l'Opérateur est invité à prendre connaissance du §3 du présent Référentiel #1.

PS : Au sein de l'Espace de Confiance, il existe une exception au domaine « mssante.fr ». Cette exception est portée par le domaine « interop-mssante.apicrypt.org ».

[3] Une exception pour le domaine interop-mssante.apicrypt.org

3 Procédure d'intégration à l'Espace de Confiance MSSanté

EX_GEN_0200

Tout Opérateur doit respecter les conditions et modalités d'utilisation de la procédure d'intégration à l'Espace de Confiance MSSanté décrite dans le présent chapitre.

L'Opérateur doit intégrer dans un premier temps l'Espace de Confiance de tests qui est dédié à la mise en conformité de son service de Messageries Sécurisées de Santé avec les exigences du Référentiel #1.

Suite à un contrôle de conformité, l'Opérateur ayant démontré sa conformité aux exigences du Référentiel #1 en vigueur peut intégrer l'Espace de Confiance de production.

L'intégration à l'Espace de Confiance de production s'effectue en plusieurs étapes.

1. La contractualisation avec l'ANS
    a. Adhésion aux services d'identification électronique de l'ANS
    b. Le contrat « Opérateur MSSanté v2 »
    c. L'Annexe 1 : « Déclaration de domaine MSSanté »
2. L'intégration en Espace de Confiance de test
    a. Validation des tests de conformité au Référentiel #1
3. L'intégration à l'Espace de Confiance de production.

3.1 La Contractualisation avec l'ANS

3.1.1 Le contrat d'adhésion

Avant toute démarche contractuelle sur les sujets MSSanté, la structure souhaitant devenir Opérateur doit, pour pouvoir commander des certificats serveur, être titulaire d'un « Contrat d'adhésion aux services de l'Agence du Numérique en Santé relatifs aux moyens d'identification électronique ».

Accès aux informations et aux démarches en ligne sur le lien suivant : https://esante.gouv.fr/vos-demarches-1.

3.1.2 Le contrat « Opérateur MSSanté V2 »

Pour proposer un service de messageries sécurisées de santé, l'Opérateur doit dans un premier temps conclure un contrat Opérateur avec l'ANS, qui définit les conditions d'intégration de l'Opérateur à l'Espace de Confiance MSSanté.

La signature du contrat Opérateur MSSanté V2 s'effectue uniquement par procédé électronique disponible à l'adresse suivante : https://mssante.fr/is/doc-technique

3.1.3 Commande de certificats serveur (production/test)

La commande de certificat serveur est nécessaire afin de pouvoir assurer des échanges au sein de l'Espace de Confiance de test ou de production. Il est possible de commander dans un premier temps un certificat de test pour la phase de recette qui se déroulera en Espace de

Confiance de test. Le certificat de production pourra être commandé pour l'intégration en Espace de Confiance de production, une fois la phase de recette réussie.

La signature du contrat d'adhésion relatif aux MIE est le prérequis pour la commande de certificats. Cela nécessite que :

- le représentant légal de la structure ou le mandataire (personne désignée par le représentant légal pour gérer les produits de certification rattachés à la structure) ait commandé ou en sa possession une carte CPx à jour. Le représentant légal pourra alors désigner un ou plusieurs administrateurs techniques qui seront les seules personnes de la structure habilitées à pouvoir générer des certificats.

- l'administrateur technique ait commandé et retiré le certificat à l'aide des formulaires suivants (https://esante.gouv.fr/index-des-formulaires#content-23241) :
  - le formulaire n°414 – commande de certificat de test
  - le formulaire n°413 – commande de certificat de production

Ces formulaires permettent d'habiliter la carte (CPA) de l'administrateur technique afin de générer le certificat serveur utilisé par le connecteur MSSanté. Ce certificat est émis par l'autorité de certification IGC Santé de l'ANS (sur la branche Élémentaire domaine Organisations).

3.1.4 L'Annexe 1 : « Déclaration de domaine MSSanté »

Elle permet à l'Opérateur de renseigner les informations techniques (nom de domaine, certificat, etc.) nécessaires à son entrée dans l'Espace de Confiance de production/test.

Elle permet aussi de réaliser des ajouts, mises à jour ou suppressions de domaines MSSanté, dans l'Espace de Confiance de test ou de production.

Elle doit être nécessairement signée. La signature doit être précédée du nom et prénom du signataire et accompagné du cachet de la structure. Elle doit être adressée par mail à l'adresse : **monserviceclient.mssante@esante.gouv.fr**.

L'ANS est propriétaire du nom de domaine « mssante.fr », régulièrement enregistré auprès d'un bureau d'enregistrement. Pour le fonctionnement de l'Espace de Confiance MSSanté et des services de Messagerie Sécurisée de Santé, l'ANS concède à l'Opérateur intégré à l'Espace de Confiance le droit d'utiliser le nom de domaine « mssante.fr », dans les conditions définies dans le contrat « Opérateur MSSanté v2 ».

Au travers du contrat « Opérateur MSSanté v2 », l'ANS autorise les autorités de certification compétentes à délivrer aux Opérateurs intégrés à l'Espace de Confiance, des certificats numériques relatifs au domaine « mssante.fr ».

Le nom de domaine « mssante.fr » ainsi que les certificats délivrés à l'Opérateur doivent être utilisés exclusivement à des fins de fonctionnement du service de Messagerie Sécurisée de Santé, dans le respect des conditions définies dans le contrat « Opérateur MSSanté v2 ».

L'autorisation d'utilisation du nom de domaine « mssante.fr » et de production de certificats numériques ne vaut que pour les noms de domaines enregistrés sur la liste blanche de l'Espace de Confiance de test et/ou de production. Cette autorisation n'est valable que pendant la seule durée du contrat « Opérateur MSSanté v2 » et exclusivement dans les limites de son objet.

L'ANS en sa qualité de gestionnaire de l'Espace de Confiance MSSanté se réserve le droit de refuser et de retirer l'enregistrement d'un nom de domaine de la liste blanche si celui-ci est susceptible de porter atteinte à l'ordre public, aux bonnes mœurs ou à des droits de propriété intellectuelle.

Remarque :

L'ANS applique pour l'enregistrement des noms de domaines des Opérateurs dans la liste blanche, la même règle que celle de la Charte de nommage de l'AFNIC : « premier arrivé – premier servi ».

Conformément aux dispositions du contrat « Opérateur MSSanté v2 » l'Opérateur s'engage à déclarer auprès de l'ANS les domaines MSSanté utilisés pour proposer son service de Messagerie Sécurisée de Santé afin qu'ils soient enregistrés dans la liste blanche, en respectant les modalités d'enregistrement suivantes :

- réaliser les demandes de référencement de noms de domaine de bonne foi et s'engager à ce que les noms de domaines référencés ne soient pas susceptibles de porter atteinte à l'ordre public ou aux droits de propriété intellectuelle d'un tiers. L'Opérateur professionnels est responsable de tout litige ou contentieux liés au nom de domaine qu'il a référencé dans la liste blanche ;
- utiliser un sous-domaine rattaché au nom de domaine « mssante.fr » dont l'ANS est titulaire. Par exception, l'Opérateur professionnels « interop-mssante.apicrypt.org » ayant enregistré un nom de domaine sans l'utilisation du sous-domaine « mssante.fr », en application des dispositions de l'ancienne procédure de nommage applicable à l'Espace de Confiance, n'a pas l'obligation de modifier les noms de domaine déjà enregistrés sur la liste blanche.

3.2 Intégration à l'Espace de confiance de test

3.2.1 Présentation de l'Espace de Confiance de tests

L'Espace de Confiance de test permet aux Opérateurs de tester leurs interfaces MSSanté (décrites au §7) en utilisant uniquement des données de test.

Il présente des outils, simulant un client de messagerie ou un Opérateur, qui permet d'effectuer des tests de bout en bout d'authentification et d'échange de messages.

Il contient notamment un Outil de tests et de contrôles qui désigne la solution logicielle dédiée aux tests et aux contrôles d'une ou plusieurs exigences du Référentiel #1 (MOTCO1 – MSSanté Outil de Test et de Conformité au Ref#1). Il permet à l'Opérateur de produire des preuves permettant d'attester de sa conformité au Référentiel #1.

Le détail de la procédure de contrôle et les modalités de réalisation des contrôles que doit respecter l'Opérateur sont précisées dans le document « Outil de test et de contrôle de conformité » [MSS-OUTIL-TEST] disponible à l'adresse suivante : https://mssante.fr/is/doc-technique .

3.2.2 Modalités d'accès et d'utilisation de l'Espace de Confiance de test

Pour accéder à l'Espace de Confiance de test, l'Opérateur doit avoir contractualisé avec l'ANS et envoyé son Annexe 1 de test au support de l'ANS. Pour pouvoir renseigner l'Annexe 1 et accéder techniquement à l'Espace de Confiance de test, l'Opérateur doit disposer d'un ou plusieurs certificats serveur applicatif de test délivrés par l'ANS et dont l'utilisation doit être dédiée au service de messageries sécurisées de santé.

L'ANS intègre l'Opérateur à l'Espace de Confiance de test en l'enregistrant au sein de la liste blanche de test (https://espacedeConfiance.test.mssante.fr/listeblanchemssante.xml) qui contient un enregistrement de l'ensemble des domaines de messagerie de test des Opérateurs intégrés en Espace de Confiance de test.

Une fois intégré en Espace de Confiance de test, l'Opérateur dispose de 6 mois pour attester de sa conformité au présent référentiel en produisant un rapport de tests et le transmettre à l'ANS à l'adresse suivante : monserviceclient.mssante@esante.gouv.fr.

L'Opérateur est invité à envoyer avec le rapport de tests, une nouvelle Annexe 1 comprenant notamment les éléments techniques relatifs à l'Espace de Confiance de production.

Dès réception du rapport de tests, l'ANS procède à la vérification de la conformité de l'Opérateur au Référentiel #1. À l'issue de cette vérification deux scénarios sont possibles :

- l'ANS valide le rapport de tests et l'intégration en Espace de Confiance de production peut être effectuée ;
- l'ANS ne valide pas le rapport de tests, l'Opérateur est alors invité à corriger les non conformités et à produire un nouveau rapport de tests et le transmettre à l'ANS ;

L'ANS notifie sa décision de validation ou d'invalidation à l'Opérateur par courrier électronique.

La procédure et les modalités de contrôles sont définies au §7.1.

Les Opérateurs faisant appel à un prestataire extérieur, par exemple un éditeur tiers, pour la fourniture du Connecteur MSSanté ont la possibilité d'intégrer directement l'Espace de Confiance de production à condition d'apporter la preuve de la conformité de leur prestataire aux exigences du Référentiel #1, sous réserve du respect des conditions détaillées au §7.

3.2.3 Obligations de l'Opérateur sur l'Espace de Confiance de test

L'Opérateur accédant à l'Espace de Confiance de test est notamment tenu de respecter dispositions suivantes :

- réaliser les tests de conformité avec diligence et compétence ;
- restreindre strictement l'usage de son service de Messagerie Sécurisée de Santé à des envois de test, uniquement depuis et vers des boites aux lettres de test. Interdiction de traiter des données à caractère personnel, et notamment des données de santé, réelles ;
- le ou les noms de domaine utilisés par l'Opérateur et enregistrés au sein de la liste blanche de tests doivent être conformes aux éléments définis au § 0.

3.3 Intégration de l'Espace de Confiance de production

Une fois le rapport de tests validé par l'ANS, l'intégration en Espace de Confiance de production de l'Opérateur peut être effectuée, sous réserve de l'envoi par l'Opérateur de l'Annexe 1.

L'Opérateur adresse à l'ANS :

- **Une Annexe 1 « Déclaration de domaine MSSanté »** : Elle doit être nécessairement signée. La signature doit être précédée du nom et prénom du signataire et accompagné du cachet de la structure. Elle peut être adressée, au même moment que le rapport de tests, soit par courrier ; soit par mail à l'adresse monserviceclient.mssante@esante.gouv.fr.

L'Opérateur est ajouté à la liste blanche de production (https://espacedeconfiance.mssante.fr/listeblanchemssante.xml) qui contient l'ensemble des domaines MSSanté des Opérateurs présents en Espace de Confiance de production.

Toute mise à jour de la liste blanche (ajout/retrait de nom de domaine, contacts, DNS, …) s'effectue à travers l'envoi d'une nouvelle Annexe 1 à l'ANS.

La liste de l'ensemble des noms de domaine et Opérateurs présents en Espace de Confiance de production est disponible à la page suivante : https://mssante.fr/home/etab-operateurs

L'Opérateur intégré à l'Espace de Confiance de production est tenu de respecter un ensemble de règles, et notamment, :

- les exigences du Référentiel #1 ;
- le cadre juridique général applicable à son service de Messagerie Sécurisée de Santé ;
- les dispositions relatives à l'hébergement de données de santé prévues par l'article L.1111-8 du code de la santé publique ;

Un Opérateur s'appuyant sur un Connecteur MSSanté édité par un sous-traitant, peut intégrer l'Espace de Confiance de production sans passer par l'Espace de Confiance de Test, à condition :

- de compléter le Pack Opérateur avec une annexe 1 en vue d'intégrer l'Espace de Confiance de production ;
- de produire le rapport de conformité technique des interfaces du connecteur aux exigences du Référentiel #1 de son prestataire ;
- du bon de commande (ou devis signé) du connecteur de son prestataire.

4 Description du fonctionnement du système de Messageries Sécurisées de Santé

Le système MSSanté est avant tout un système de messageries électroniques « standard » d'émission et de réception de messages électroniques, c'est-à-dire qu'il s'appuie sur le protocole SMTP. À ce titre, le service MSSanté ne garantit formellement ni le bon acheminement des messages à leurs destinataires ni le délai d'acheminement. On admet que des messages puissent être perdus mais pas qu'ils puissent être modifiés.

Le système MSSanté intègre des fonctionnalités spécifiques répondant aux attentes et obligations des utilisateurs du monde de la santé (voir **§2** « Les principes du système de Messageries Sécurisées de Santé ») et à des besoins de sécurité (confidentialité, intégrité et traçabilité) liés à la nature personnelle et sanitaire des données pouvant être échangées.

Il permet l'envoi et la réception de messages entre des domaines de messagerie dédiés spécifiquement à la MSSanté. Ces messages doivent pouvoir être accompagnés de documents en pièce-jointe.

4.1 Domaine MSSanté et groupe de domaines autorisés

Le système MSSanté repose sur un groupe autorisé de domaines de messageries fonctionnant en vase clos, appelés domaines MSSanté.

Un domaine de messagerie sert à identifier l'environnement de messagerie sur lequel sont hébergées une ou plusieurs boites aux lettres.

Les échanges de messages ne sont autorisés qu'entre les domaines de messagerie MSSanté répertoriés au sein d'une « liste blanche ». La liste blanche est un fichier géré par l'ANS et propre au système MSSanté, qui permet de filtrer et contrôler les domaines de messagerie autorisés à échanger des messages au travers du système MSSanté.

Les domaines MSSanté sont mis en œuvre par les Opérateurs MSSanté.

Le schéma ci-dessous illustre le principe des échanges entre les différents types d'Opérateurs appartenant à l'Espace de Confiance MSSanté :

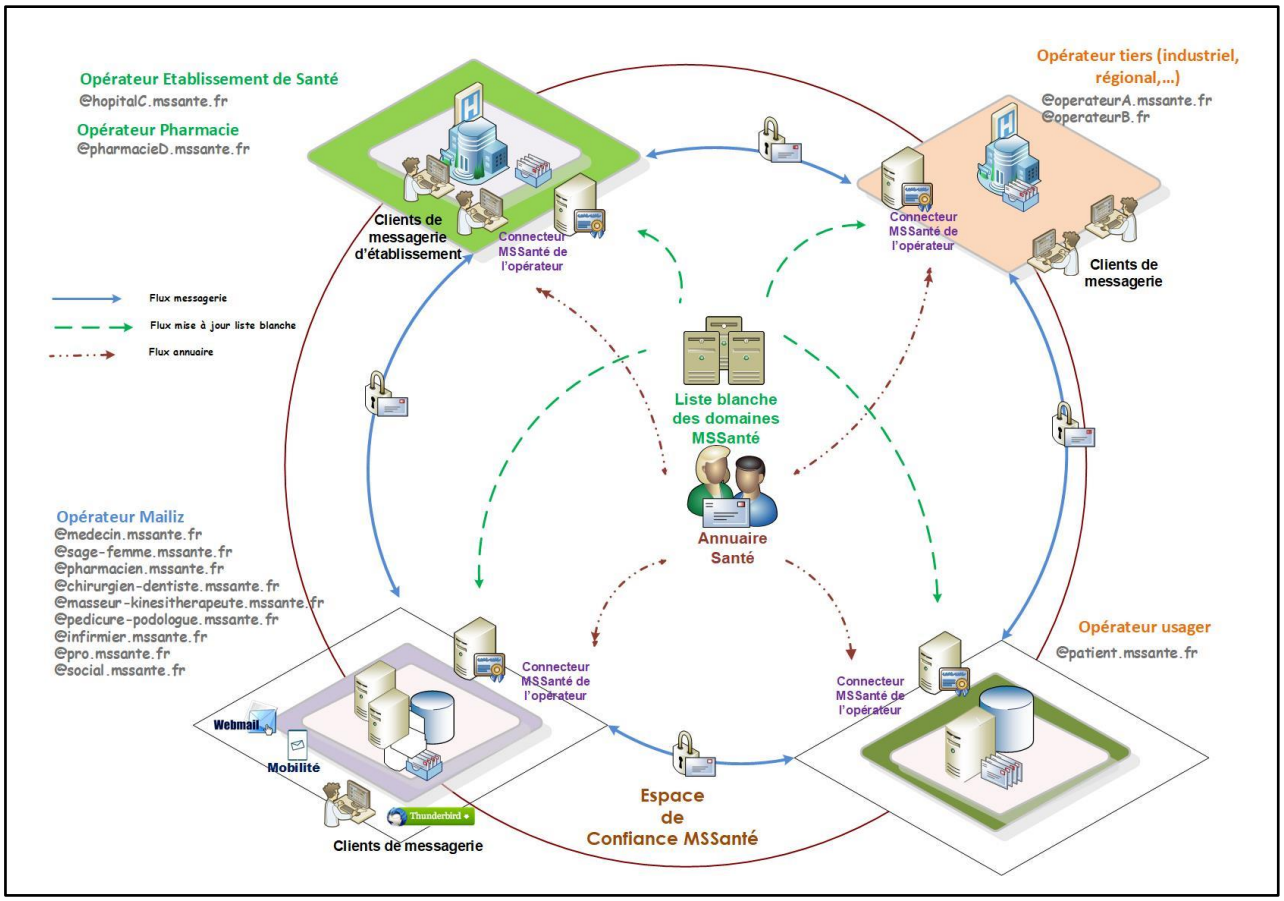


Figure 7 : Échanges au sein du système MSSanté

Les Opérateurs de messagerie signent un contrat « Opérateur MSSanté v2 » avec l'ANS décrivant leurs engagements pour rejoindre l'Espace de Confiance.

Dans tous les cas, ils sont tenus d'utiliser une solution technique de « Connecteur MSSanté » afin de pouvoir se raccorder techniquement à l'Espace de Confiance MSSanté.

Les échanges de messages se font donc entre utilisateurs professionnels, et entre ces professionnels et les usagers utilisant des services de messagerie mis en œuvre par les Opérateurs MSSanté (Opérateurs professionnels et Opérateur usagers).

Il n'y a pas de centralisation des échanges de messages dans l'Espace de Confiance. Les échanges sont directs d'Opérateur MSSanté à Opérateur MSSanté.

4.2 L’Annuaire Santé des professionnels habilités

Les Utilisateurs usager et les Utilisateurs professionnel du système MSSanté, doivent pouvoir sélectionner de manière sûre et aisée les destinataires de leurs messages.

L’ANS met en oeuvre et maintient l’Annuaire Santé des professionnels habilités du système MSSanté. La finalité de l’utilisation de l’Annuaire Santé dans la MSSanté est d’identifier l’expéditeur de tout message reçu sur sa BAL MSSanté et de permettre à tout utilisateur de retrouver facilement l’adresse d’un professionnel habilité disposant d’une BAL MSSanté afin de lui adresser un message de façon sécurisée.

Pour atteindre cet objectif, l’Annuaire Santé recense l’ensemble des professionnels habilités à échanger des données de santé personnelles via MSSanté, ainsi que les informations concernant les BAL applicatives et organisationnelles.

Les Opérateurs professionnels doivent publier l’ensemble des BAL des utilisateurs finaux de leur(s) domaine(s) dans l’Annuaire Santé.

Les Utilisateurs professionnels devront être identifiés par leur numéro d’identification national (RPPS ou ADELI). Lorsque, dans des cas particuliers, l’Utilisateur professionnel ne dispose pas de numéro d’identification national, la certification de son identité est réalisée sous la responsabilité du directeur de la structure de soins qui l’emploie et qui lui attribuera un numéro d’identification local. Le directeur de la structure de soins est ainsi considéré comme une autorité d’enregistrement locale.

L’Annuaire Santé utilisé dans le cadre de la MSSanté contient ainsi des données qui permettent :

- D’identifier les professionnels habilités du système MSSanté ;
- De rechercher l’adresse de messagerie MSSanté d’un destinataire professionnel sur le principe de recherche multicritères ;
- D’afficher les traits d’identité des professionnels habilités répondants aux critères de recherche.

La gestion des fonctions de l’Annuaire Santé nécessite de disposer d’un ensemble d’interfaces en adéquation avec les usages et besoins présentés supra ; ces interfaces sont présentées de manière plus détaillée aux § 6.4 « Publication de BAL MSSanté dans l’Annuaire » et § 6.5.1 « TM2.1.1A - Consultation de l’Annuaire ».

Remarque : l’ANS gère l’Annuaire Santé dans les conditions de service suivantes :

- Production opérationnelle en 24/7 ;
- Durée maximale unitaire d’interruption de service : 1 h ;
- Durée maximale mensuelle cumulée d’interruption de service : 4h ;

4.3 Identification des usagers

Sous réserve des dispositions précisées par décret, 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'État), peuvent disposer de Mon Espace Santé (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 patient 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. Étant précisé qu'il n'existe pas d'annuaire « usagers » dans l'Espace de Confiance permettant de contrôler l'existence d'une BAL usager. L'expéditeur d'un message à destination d'un usager est informé de l'inexistence ou de la suspension d'une BAL usager par la réception d'un message type.

À la création d'un compte MES, une adresse de messagerie patient MSSanté est automatiquement attribuée à l'usager et rattachée à MES. Cette adresse est constituée à partir du matricule INS de l'usager et du nom de domaine de l'Opérateur de MES, 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.

Afin de favoriser l'usage des professionnels de santé, les correspondances entre professionnels et usagers ne pourront être initiées que par les professionnels. La messagerie de MES ne permettra pas à un usager d'initier un échange avec un professionnel. Un premier message provenant du professionnel devra avoir été reçu au préalable par le patient, pour que ce dernier puisse y répondre. Le détail de ces règles implémentées par MES seront décrites dans le Référentiel #2 clients de messagerie [MSS-REF2].

4.4 Connecteur MSSanté d'un Opérateur

Le Connecteur MSSanté de l'Opérateur doit être vu comme un relais de messagerie permettant le raccordement de son serveur de messagerie à l'Espace de Confiance MSSanté dans le respect des exigences fonctionnelles et techniques définies par l'ANS.

Un Connecteur MSSanté d'un Opérateur communique uniquement avec un autre Connecteur MSSanté d'un autre Opérateur.

Le Connecteur MSSanté de l'Opérateur permet :

- de prendre en charge les échanges de messages entre Opérateurs au sein de l'Espace de Confiance ;
- de contrôler l'identité du destinataire du message ;
- de contrôler l'identité de l'expéditeur d'un message ;
- de contrôler l'appartenance de l'adresse de messagerie du destinataire d'un message à un domaine de messagerie de la liste blanche ;
- de gérer le cycle de vie des boîtes aux lettres (publication des créations ou modifications des BAL du domaine géré par l'Opérateur dans l'Annuaire Santé) ;
- de consulter l'Annuaire Santé et d'en télécharger une extraction (transaction optionnelle) ;
- de télécharger des données d'identités des futurs utilisateurs finaux (transaction optionnelle).

Interopérabilité entre les domaines MSSanté

L'interopérabilité entre tous les domaines MSSanté est assurée par l'échange des messages en protocole SMTP dans des canaux sécurisés TLS par authentification réciproque entre les domaines (les Connecteurs MSSanté des Opérateurs présentent des certificats d'authentification émis par l'ANS).

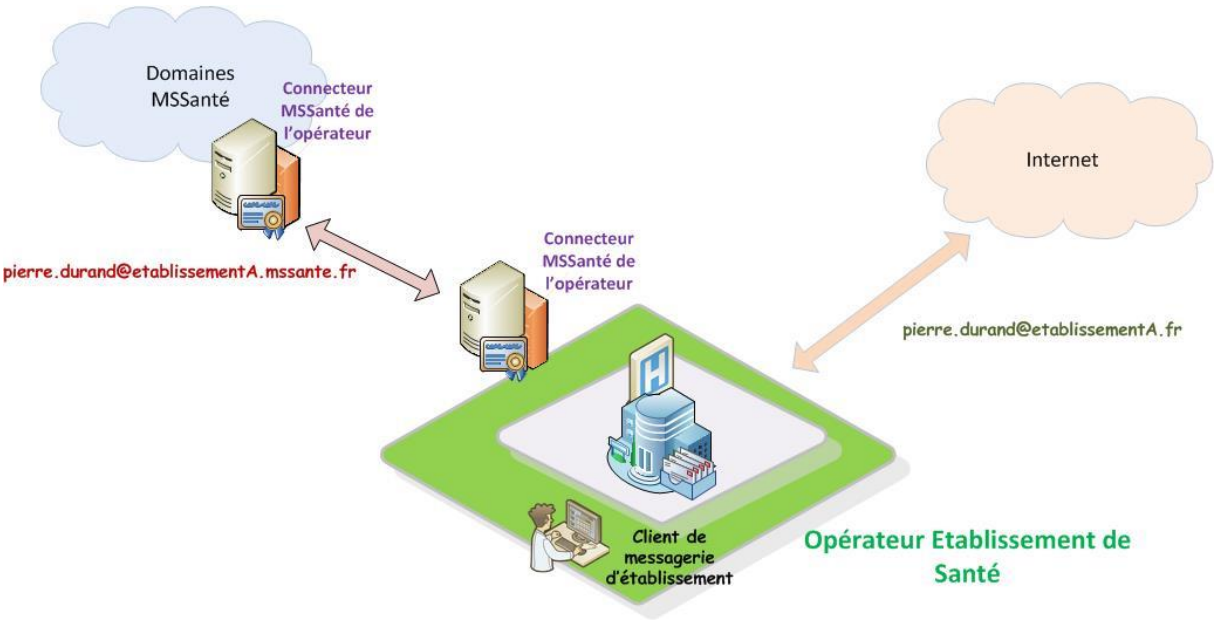


Figure 8 : Connecteur MSSanté de l'Opérateur

4.5 Connecteur à l'Annuaire Santé

Le **Connecteur à l'Annuaire Santé** n'est pas un composant obligatoire dans l'Espace de Confiance MSSanté. Néanmoins, son implémentation est fortement recommandée car elle présente les avantages suivants :

- Offrir un niveau de service garanti :
  - En consolidant les requêtes ;
  - En permettant de s'affranchir des problématiques de temps de réponse (rôle de cache local) ;
  - En dirigeant ou transformant de façon transparente les requêtes adressées à l'Annuaire Santé ;
- Réaliser des recherches de correspondants dans l'Annuaire Santé ;
  - Via le client de messagerie ;
  - Par une vue unifiée des adresses MSSanté au sein de l'établissement.

Des exemples d'implémentations sont disponibles au § ***4.8*** *« Exemples de mise en œuvre ».*

4.6 Les clients de messagerie MSSanté professionnels

Le « Référentiel socle MSSanté #2 – Clients de Messageries Sécurisées de Santé » [MSS-REF2] désigne un « Client de messagerie MSSanté » (également désigné « LPS compatible MSSanté ») comme 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.

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 une arborescence de BAL au professionnel habilité. Il s'applique aussi à tout logiciel métier (client lourd ou SaaS) utilisé par un professionnel habilité, 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).

4.6.1 Le LPS/DUI doit pouvoir se connecter à l'opérateur via l'API LPS

Le logiciel de professionnel de santé (LPS ou DUI), outil quotidien du professionnel, tant en secteur libéral qu'en établissement, est un outil privilégié pour les échanges par messagerie entre professionnels habilités. L'objectif de l'ANS est donc de permettre une intégration aussi harmonieuse que possible entre le LPS et les messageries sécurisées du système MSSanté.

Chaque Opérateur a l'obligation d'implémenter les interfaces standards de l'Espace de Confiance MSSanté dites « API LPS » (décrites au §6.8.1)

Ainsi, chaque LPS/DUI MSSanté peut permettre à ses utilisateurs de paramétrer une adresse mail sécurisée ainsi que d'intégrer les fonctionnalités d'interrogation de l'Annuaire Santé proposées par l'ANS et les fonctionnalités d'émission et de réception de messages proposées par les Opérateurs MSSanté, en implémentant les interfaces standards MSSanté (décrites dans le document « Référentiel socle MSSanté #2 – Clients de Messageries Sécurisées de Santé » [MSS-REF2].

Remarque :

En complément des interfaces standard API LPS, un Opérateur peut donc choisir d'offrir un service de messagerie pour des clients propriétaires, par exemple intégrés à son

logiciel, à l'aide d'interfaces complémentaires. Le service d'un tel Opérateur pourra néanmoins intégrer l'Espace de Confiance MSSanté dès lors qu'il répond aux exigences contractuelles. L'Opérateur informera utilement ses clients sur les interfaces qu'il met en œuvre.

4.6.2 Le client de messagerie de Mon Espace Santé

Mon Espace Santé (MES) est doté d'un client de messagerie interfacé à l'Opérateur usagers. L'usager peut y accéder depuis un navigateur internet depuis un ordinateur ou un terminal mobile.

Le client de messagerie de MES permet en particulier :

- La consultation de pièces jointes des messages provenant de professionnels,
- L'enregistrement de ces pièces jointes dans MES de l'usager,
- La réponse au message d'un professionnel avec possibilité d'inclure des pièces jointes en provenance de l'appareil de l'usager ou de MES,
- Le transfert de message à un professionnel, mais pas à un autre usager,
- La notification de réception de messages via le système de notification de MES,
- D'afficher un document CDA R2 reçu en pièce jointe.

Le client de messagerie de MES n'affiche pas au patient l'adresse de la BAL du professionnel. Elle est remplacée par les nom/prénom/profession des professionnels ou la raison sociale des structures issus de l'annuaire santé.

4.7 Le cadre d'interopérabilité des SIS et interopérabilité des échanges de données de santé structurées

Le cadre d'interopérabilité des systèmes d'information de santé (CI-SIS) de l'ANS définit les standards (techniques, sémantiques et de sécurité) à utiliser par les industriels du secteur de la santé et les utilisateurs des systèmes d'information de santé.

Des références au CI-SIS, et éventuellement à d'autres standards utilisés par les messageries MSSanté, sont citées dans ce document (les références au CI-SIS sont de la forme [CI-XXXX] conformément aux références du tableau de l'annexe **§ 0** « Documents applicables »).

Pour les lecteurs de « profil 1 » (décideur) ou de « profil 2 » (directeur technique ou chef de projet), il est vivement conseillé, à ce stade de lecture du document, de lire le « document chapeau » du CI-SIS [CI-CHAP].

Afin de favoriser l'interopérabilité des Systèmes d'Information (SI) de Santé, les modalités d'échange de documents de santé via la messagerie électronique sécurisée ont été définies et sont décrites dans le volet « Échange de Documents de Santé » ([CI-ECH-DOC]) du Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS).

Ces modalités reposent en particulier sur le profil IHE-XDM qui prévoit l'envoi en pièce jointe d'un fichier zip IHE_XDM contenant les documents de santé.

En complément de la pièce jointe IHE_XDM, il est imposé de joindre les documents au format PDF afin de faciliter la lecture pour les destinataires qui ne seraient pas en capacité d'exploiter le format XDM.

C'est au client de messagerie émetteur de s'assurer de la cohérence entre les documents contenus dans la pièce jointe IHE_XDM et ceux transmis au format bureautique.

Il est à noter qu'un message ne doit contenir qu'une seule pièce jointe IHE_XDM, qui peut elle-même contenir plusieurs documents de santé (concept de lot de soumission) concernant le même patient.

La bonne pratique est toujours : un message ne concerne qu'un seul patient.

4.8 Exemples de mise en œuvre pour les Utilisateurs professionnels

Il existe de nombreux modèles d'intégration de la messagerie de santé sécurisée que ce soit au sein d'un établissement ou en ville.

Les paragraphes suivants présentent plusieurs exemples de mise en œuvre d'implémentations techniques des interfaces MSSanté (clients de messagerie et Connecteur MSSanté Opérateur). Ces exemples ont pour but de fournir des axes de réflexion sur les types d'intégration de la Messagerie Sécurisée de Santé.

4.8.1 Accès à l'Espace de Confiance

4.8.1.1 Services de messagerie distincts

L'exemple d'implémentation présenté ci-dessous décrit un service de messagerie complètement dédié aux Messageries Sécurisées de Santé, qui est implémenté directement dans l'environnement d'un Établissement de Santé.

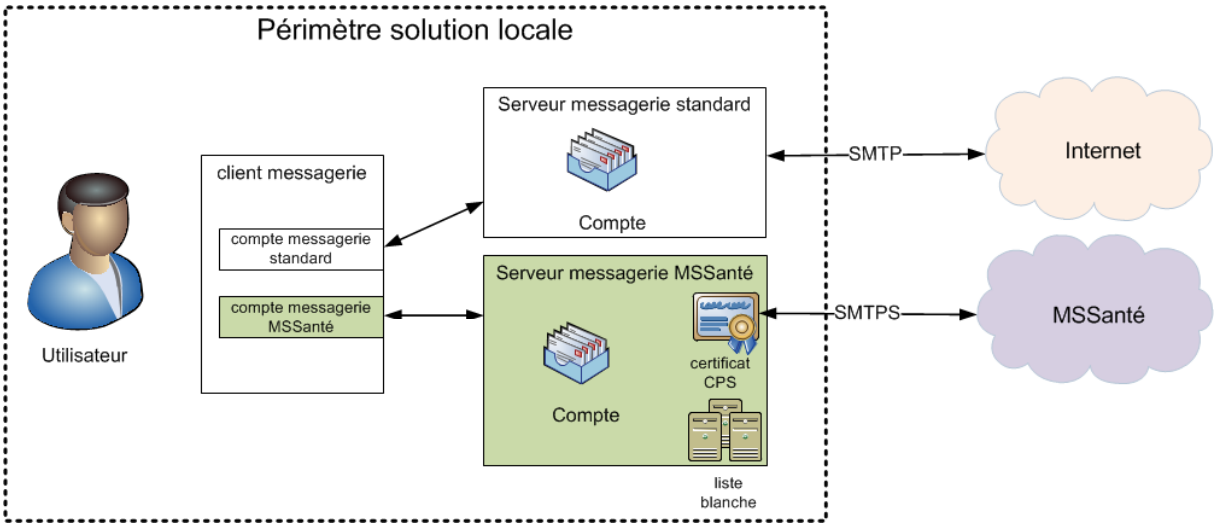


Figure 9 : Services de messagerie distincts

Dans cet exemple, l'Utilisateur professionnel utilise spécifiquement deux types de comptes de messagerie configurés dans son client de messagerie :

- Son compte de messagerie standard ;
- Son compte de messagerie MSSanté.

Il choisit son adresse d'émission en fonction de ses destinataires (et du domaine de messagerie auquel leur BAL est rattachée).

Remarque : le Connecteur MSSanté de l'Opérateur est intégré au serveur de messagerie.

4.8.1.2 Service de messagerie unifié

L'exemple d'implémentation présenté ci-dessous décrit un service de Messageries Sécurisées de Santé intégré au service de messagerie standard dans l'environnement d'un Etablissement de Santé ou d'un autre type d'Opérateur.

Le service de messagerie unifié permet de gérer à la fois les adresses de messagerie MSSanté et les adresses liées à l'établissement. Il est en capacité de positionner lui-même l'adresse d'émission en fonction des destinataires.

Dans le cas où la liste des destinataires ne comporte pas que des adresses de destinataires sur des domaines MSSanté, le service doit refuser l'émission du message vers les adresses non MSSanté à partir de la BAL MSSanté.

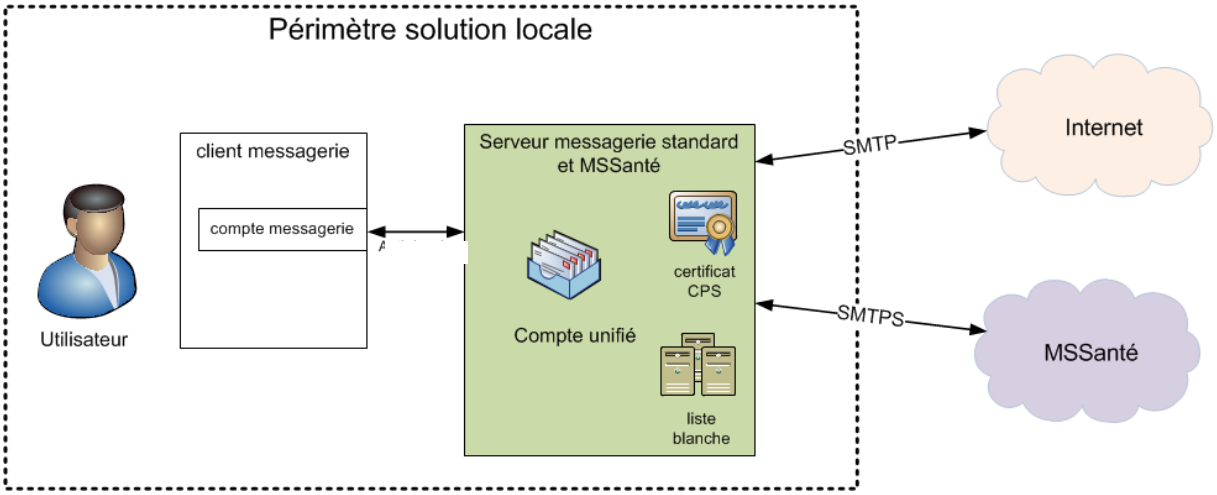


Figure 10 : Service de messagerie unifié

Dans cet exemple, l'utilisateur utilise un seul compte de messagerie dans son client de messagerie.

Remarque : le Connecteur MSSanté de l'Opérateur est intégré au serveur de messagerie.

4.8.1.3 Fonction Connecteur MSSanté d'Opérateur non intégré dans le serveur de messagerie

L'exemple d'intégration présenté ci-dessous décrit la mise en œuvre d'un Connecteur MSSanté non intégré dans le serveur de messagerie d'un établissement de santé Opérateur ou d'un autre type d'Opérateur.

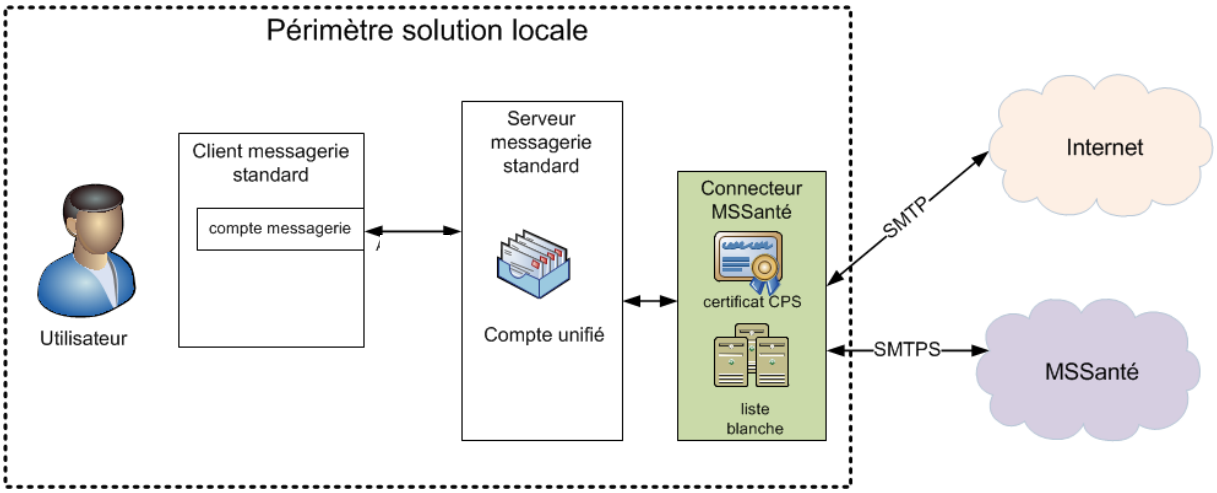


Figure 11 : Connecteur MSSanté d'Opérateur non intégré au serveur de messagerie

Il gère les messages MSSanté en offrant une interface unique d'accès au compte pour les utilisateurs.

Il gère également la correspondance entre l'adresse de messagerie connue du serveur de messagerie standard et l'adresse de messagerie MSSanté correspondante adresses MSSanté.

Exemple : prenom.nom@nom_etablissement.fr <=> prenom.nom@nom_etablissement.mssante.fr

Dans le cas où la liste des destinataires ne comporte pas que des adresses de destinataires sur des domaines MSSanté, le Connecteur MSSanté de l'Opérateur doit refuser l'émission du message vers les adresses non MSSanté à partir de la BAL MSSanté.

4.8.1.4 Échange de messages sécurisés depuis ou vers des applications

L'exemple d'implémentation présenté ci-dessous décrit la mise en œuvre d'un Connecteur MSSanté d'Opérateur dédié aux échanges entre applications.

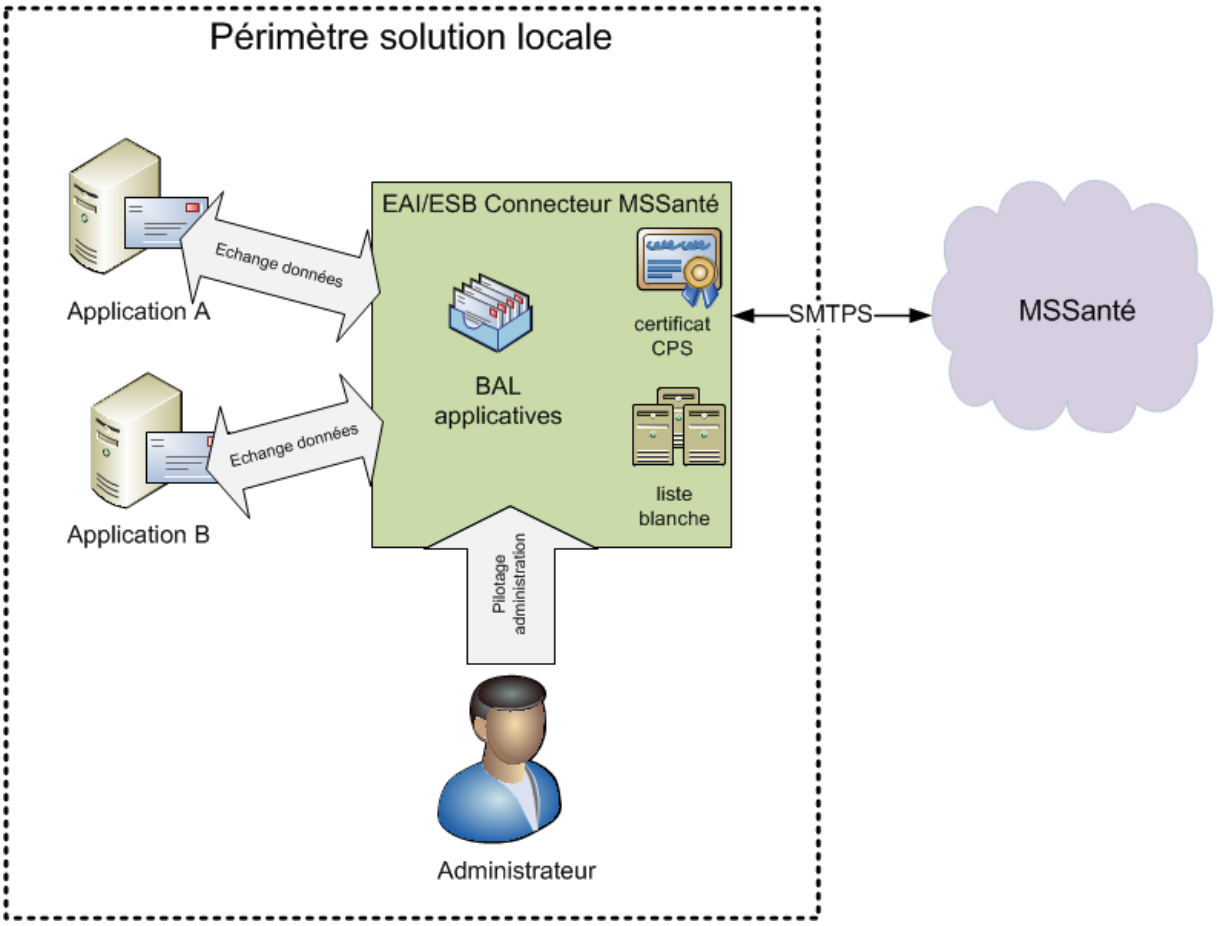


Figure 12 : Échange de messages sécurisés depuis ou vers des applications

Dans cet exemple, une boîte aux lettres MSSanté applicative peut être mise en place pour la diffusion par messagerie sécurisée de données fournies par les systèmes de production de soin.

4.8.2 Accès à une BAL MSSanté d'un professionnel

4.8.2.1 Par client de messagerie et carte CPS ou e-CPS

Dans cet exemple, l'Utilisateur professionnel utilise spécifiquement deux types de comptes configurés dans son client de messagerie :

- Son compte de messagerie standard, configuré pour accéder à sa boîte aux lettres hébergée dans un service de messagerie standard ;
- Son compte de messagerie MSSanté, configuré pour accéder à sa boîte aux lettres MSSanté.

Le poste de travail de l'Utilisateur professionnel doit être équipé d'un lecteur de carte CPS pour permettre l'accès à son compte MSSanté.

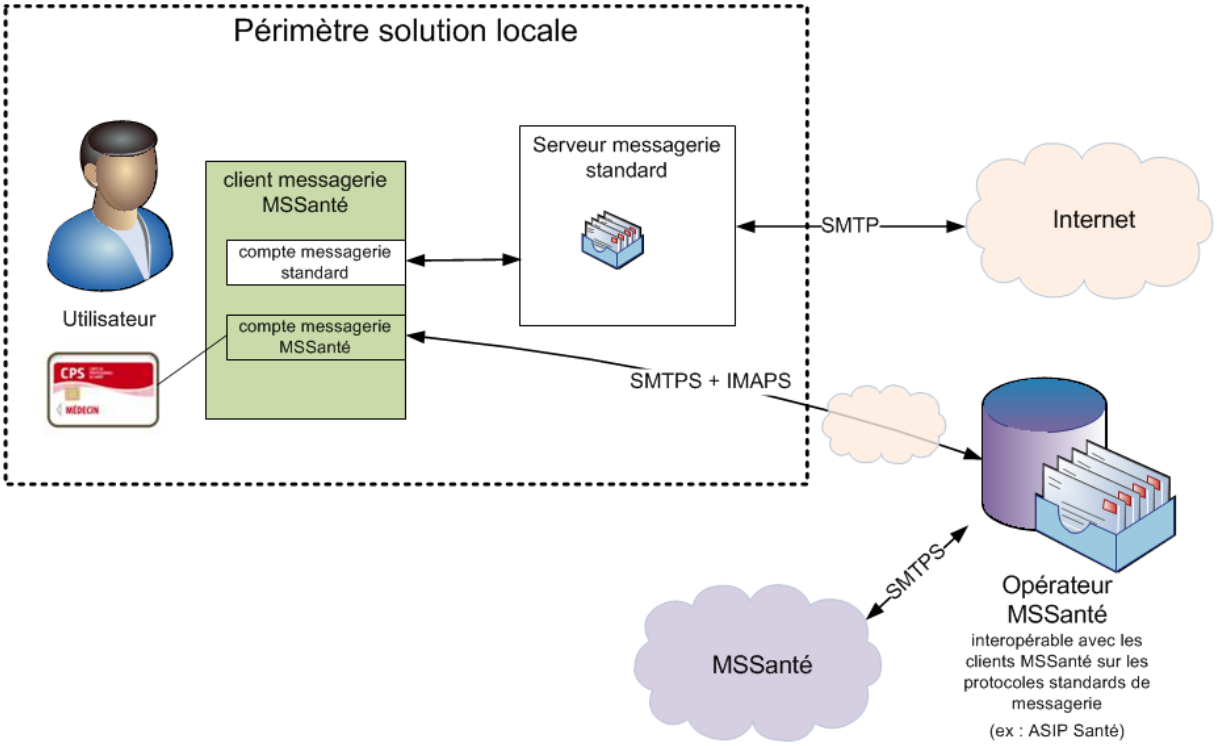


Figure 13 : Accès MSSanté par client de messagerie et carte CPS ou e-CPS

4.8.2.2 Par Webmail et carte CPS ou e-CPS

Dans cet exemple, l'Utilisateur professionnel utilise spécifiquement deux types de comptes de messagerie :

- Son compte de messagerie standard, configuré dans son client de messagerie pour accéder à sa boîte aux lettres hébergée par le service de messagerie standard ;
- Son compte de messagerie MSSanté, pour accéder à sa boîte aux lettres MSSanté hébergée par l'Opérateur MSSanté via un navigateur internet.

Le poste de travail de l'Utilisateur professionnel doit être équipé d'un lecteur de carte CPS pour permettre l'accès à son compte MSSanté.

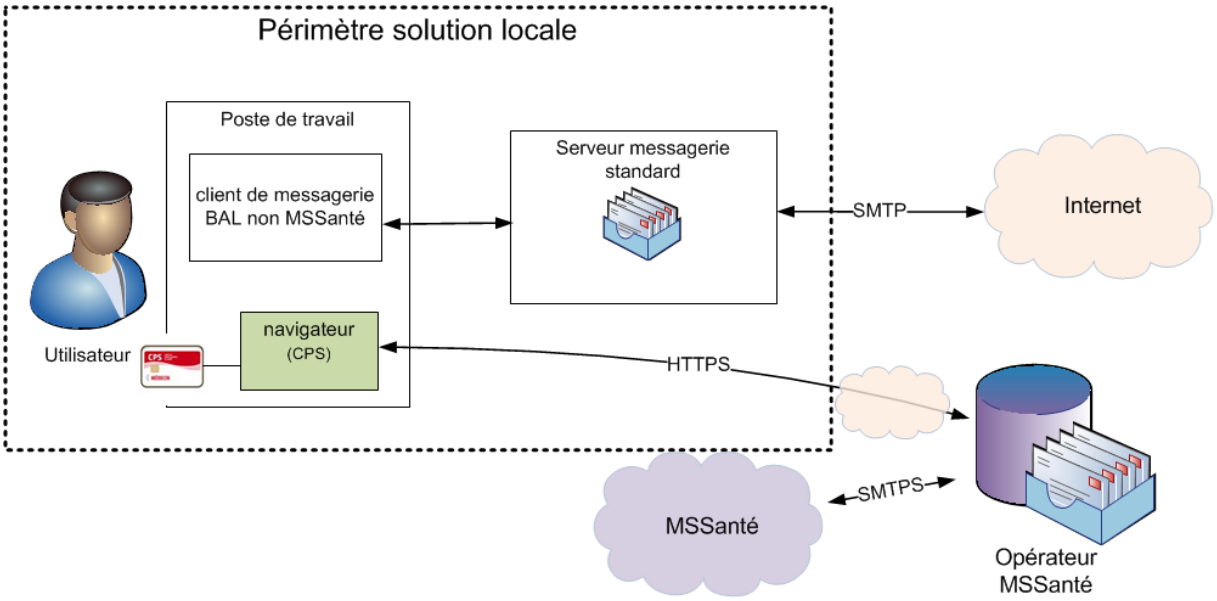


Figure 14 : Accès MSSanté par Webmail et par carte CPS ou e-CPS

4.8.3 Consultation de l'Annuaire Santé

4.8.3.1 Vue d'ensemble de l'Annuaire Santé

Le schéma présenté ci-dessous montre les flux d'alimentation des données d'identité des professionnels habilités dans l'Annuaire Santé :

- Via les répertoires et annuaires nationaux (RPPS et ADELI) ;
- Via les flux d'alimentation des Opérateurs MSSanté, avec les adresses des utilisateurs de ces domaines.

L'Annuaire Santé permet à l'Utilisateur professionnel de sélectionner les destinataires de ses messages. Les destinataires doivent être titulaires d'un compte de messagerie attaché à un des domaines MSSanté.

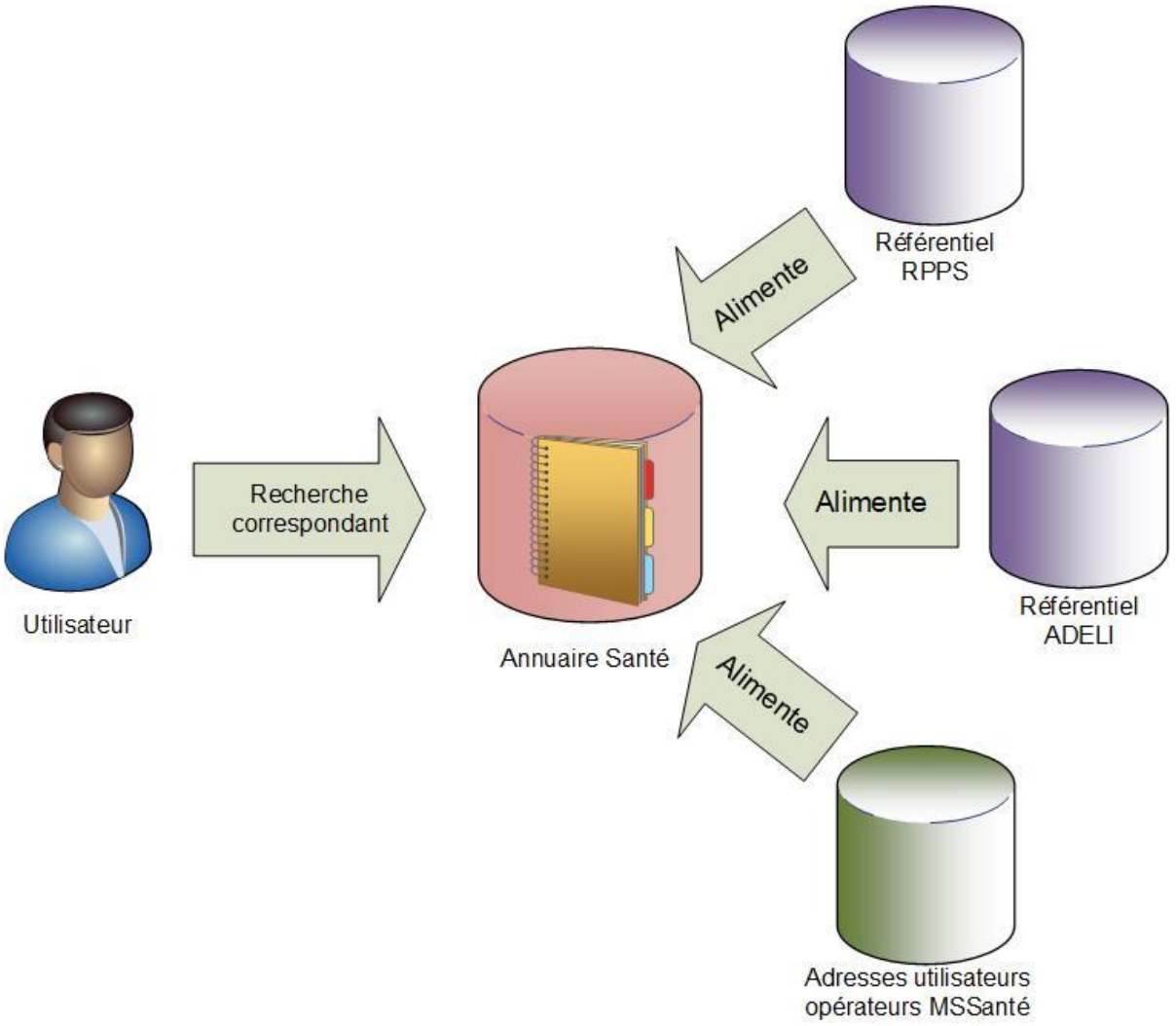


Figure 15 : Principe d'alimentation de l'Annuaire Santé

4.8.3.2 Recherche de correspondants professionnels MSSanté

4.8.3.2.1 Accès direct à l'Annuaire Santé via le client de messagerie

Dans cet exemple, l'Utilisateur professionnel utilise spécifiquement deux types de comptes d'annuaire depuis son client de messagerie :

- Un compte d'annuaire local pour réaliser des recherches dans l'annuaire de messagerie local ;
- Un compte d'annuaire spécifiquement dédié à la MSSanté.

Un connecteur avec l'Annuaire Santé pourra éventuellement être implémenté par l'établissement de santé ou les autres types d'Opérateurs pour :

- Centraliser les requêtes réalisées par les professionnels habilités locaux ;
- S'affranchir des problématiques de temps de réponse, en jouant le rôle de cache local.

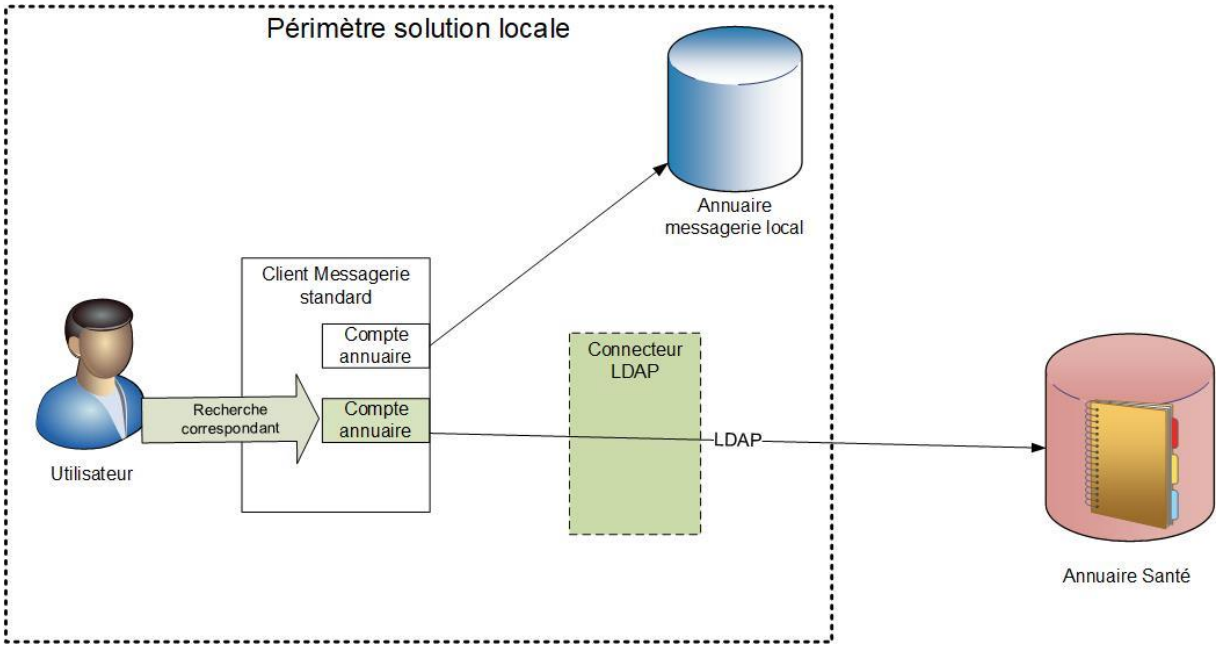


Figure 16 : Accès direct à l'Annuaire Santé via le client de messagerie

4.8.3.2.2 Vue unifiée de l'annuaire au sein de l'établissement

Dans l'exemple présenté ci-dessous, l'Utilisateur professionnel recherche un correspondant, qu'il soit enregistré dans son annuaire de messagerie local ou dans l'Annuaire Santé, à partir du même compte annuaire configuré dans son client de messagerie.

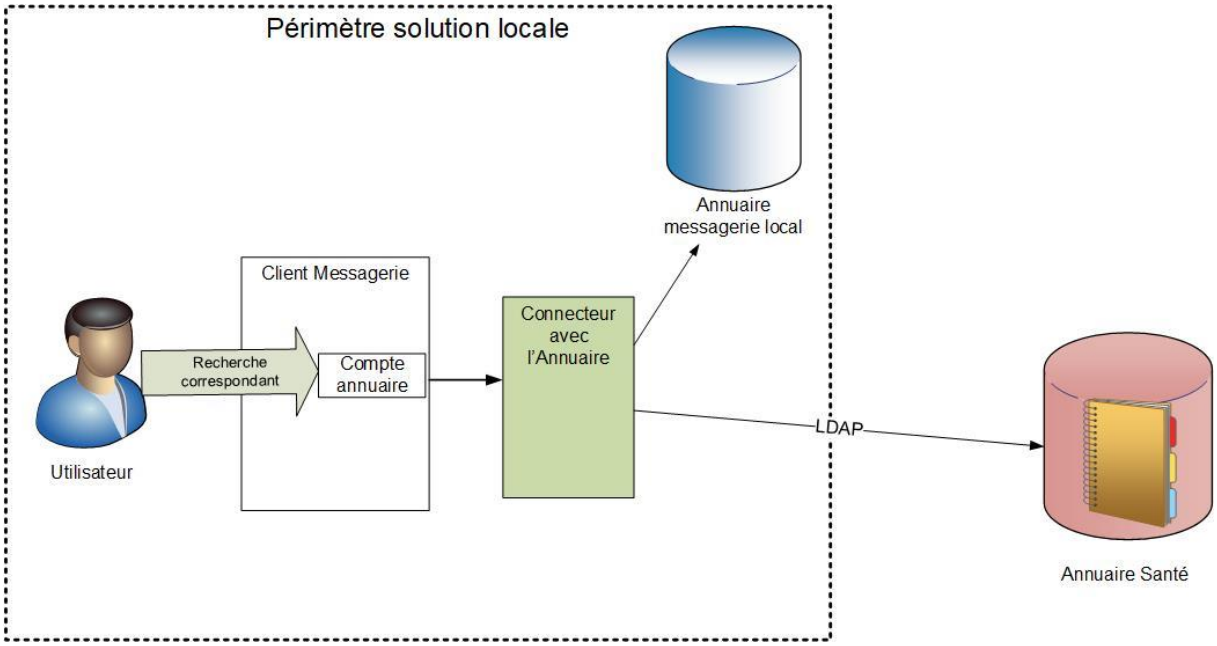


Figure 17 : Vue unifiée de l'annuaire au sein du domaine MSSanté

Le Connecteur avec l'Annuaire Santé permet alors de proposer une vue unifiée dans les réponses renvoyées à l'Utilisateur professionnel.

4.8.3.2.3 Intégration de l'Annuaire Santé

Dans l'exemple présenté ci-dessous, une extraction quotidienne de l'Annuaire Santé est mise à disposition des Opérateurs MSSanté.

Le contenu de cette extraction est ensuite intégré à l'annuaire de messagerie local de l'Opérateur MSSanté ; les Utilisateurs professionnels sont alors vus comme des contacts.

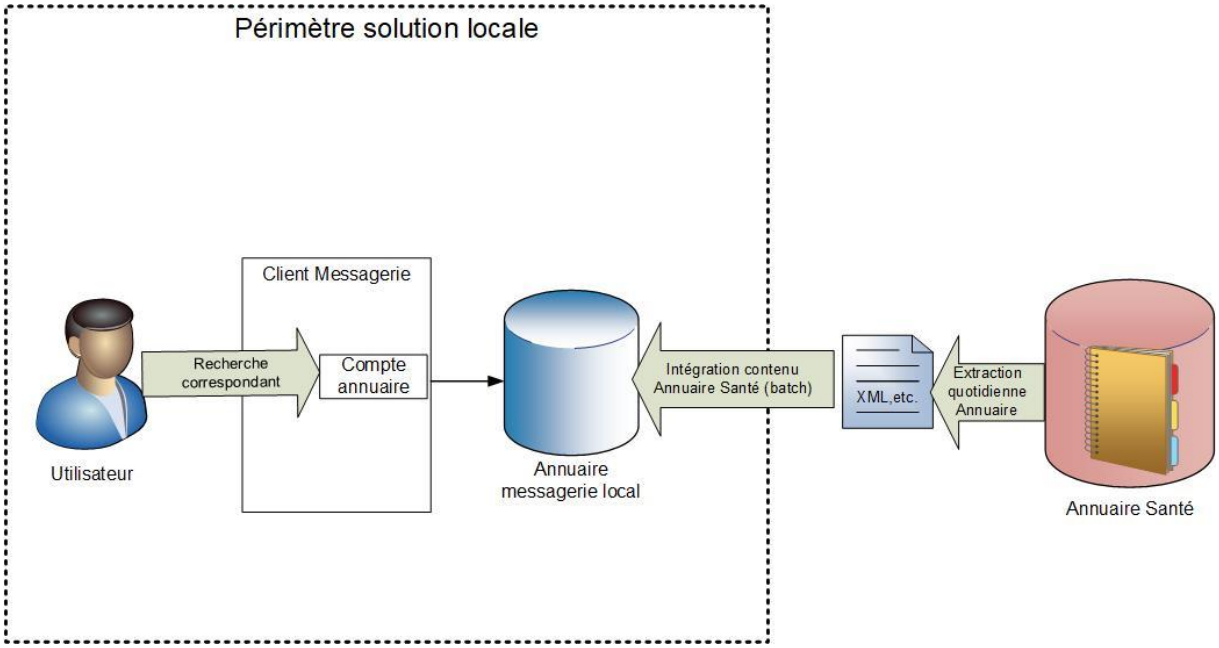


Figure 18 : Intégration de l'Annuaire Santé au sein du domaine MSSanté

L'utilisateur recherche un correspondant, MSSanté ou non, à partir du même compte d'annuaire configuré dans son client de messagerie.

4.8.4 Publication des adresses MSSanté par les Opérateurs

L'exemple ci-dessous présente le flux de publication des adresses MSSanté (correspondant aux comptes enregistrés dans des établissements de santé ou d'autres types d'Opérateurs) dans l'Annuaire Santé.

Ce flux est géré localement par un administrateur local propre à l'Opérateur MSSanté.

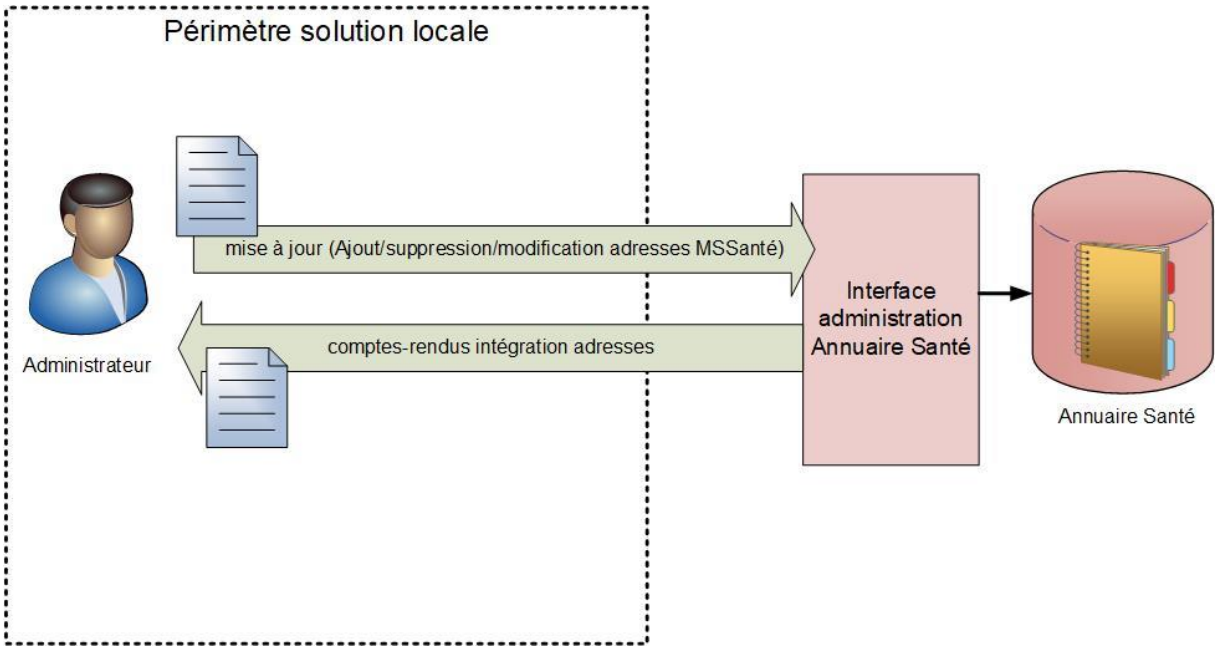


Figure 19 : Publication dans l'Annuaire Santé

Un compte-rendu d'intégration est envoyé à l'administrateur local après chaque demande de mise à jour.

5 Gestion des boites aux lettres au sein de l'Espace de Confiance MSSanté

5.1 Les Boîtes Aux Lettres (BAL) MSSanté

Le système MSSanté répond aux deux attentes principales exprimées par les acteurs :

- L'envoi, par un émetteur habilité et dont l'identité est certifiée, d'un message pouvant contenir des données de santé à caractère personnel à un destinataire habilité et dont l'identité est certifiée ;
- La consultation, par le destinataire, d'un message reçu pouvant contenir des données de santé à caractère personnel.

Le service d'échange attendu des acteurs fonctionne de manière asynchrone : l'entité destinataire peut récupérer un message à sa propre initiative, dans un laps de temps plus ou moins long après qu'il ait été émis. Le système MSSanté est donc en capacité de conserver dans le temps les messages qui ont été émis jusqu'à leur suppression par l'utilisateur final.

L'Utilisateur professionnel du système MSSanté peut disposer de plusieurs boîtes aux lettres, fournies par différents Opérateurs de l'Espace de Confiance, par exemple :

- Une boîte aux lettres ordinale, de type @<profession>.mssante.fr ;
- Une boîte aux lettres au titre de son exercice dans des établissements de santé, de type @<etablissementA>.mssante.fr;
- Une boîte aux lettres sur le domaine hébergé par un Opérateur tiers (industriel, régional, …), du type @<domaineY>.mssante.fr.

Ces différentes adresses de l'Utilisateur professionnel sont référencées dans l'Annuaire Santé.

Dans le cadre de MES, les BAL des Utilisateurs usagers sont produites par la Cnam en sa qualité d'Opérateur usagers. Sous réserve des dispositions prévues par décret, les BAL de MES sont construites comme suit :

<matricule_INS>@patient.mssante.fr

Un Opérateur professionnels doit proposer à ses Utilisateurs professionnel d'accéder aux boîtes aux lettres. Cet accès peut se faire de plusieurs manières :

- A minima en proposant l'interface API LPS décrite au §6.8**.** Cette solution est nécessaire afin de garantir l'interopérabilité avec tout client de messagerie MSSanté ;
- En utilisant un mode d'accès spécifique propriétaire ou non (exemples : Webmail, ou client de messagerie propriétaire à l'Opérateur) tout en restant conforme aux exigences du Référentiel #1 et autres référentiels portés par l'ANS, dont le référentiel d'identification électronique [PG-IDENT] (voir §6.8.6) ;

Quel que soit le ou les modes d'accès proposés, les Opérateurs professionnels MSSanté doivent s'assurer que :

- Les Utilisateurs professionnel du service MSSanté sont identifiés et authentifiés individuellement, conformément aux exigences légales et aux référentiels de sécurité de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) ;
- Les Utilisateurs professionnel n'accèdent qu'aux BAL MSSanté sur lesquelles ils disposent d'une habilitation d'accès.

5.1.1 Types de boîtes aux lettres (« BAL »)

Il existe trois types de boîtes aux lettres sécurisées dans l'Espace de Confiance MSSanté. Celles-ci peuvent être affectées à des personnes physiques (boite aux lettres nominatives des Utilisateurs professionnel et usager), à des groupes d'Utilisateurs professionnel (boite aux lettres organisationnelles) ou à des applications (boite aux lettres applicatives).

EX_GBM_3010 
Un Opérateur DOIT proposer à ses utilisateurs finaux des BAL personnelles ou des BAL organisationnelles ou les 2 types de BAL. En complément l'Opérateur peut de façon optionnelle proposer des BAL applicatives.

EX_GBM_3040 
L'Opérateur DOIT communiquer auprès des utilisateurs finaux uniquement via les dénominations des 3 types de BAL du Référentiel #1 : personnelle, organisationnelle, applicative.

Dans un objectif de simplification de la présentation de l'offre MSS auprès des utilisateurs finaux, il n'existe donc qu'une seule dénomination pour les BAL organisationnelles qu'elles soient rattachées à des FINESS ou des RPPS. Les types ORG et CAB sont des libellés techniques qui ne doivent être utilisés que lors des déclarations dans l'Annuaire Santé.

5.1.1.1 Boîte aux lettres personnelle

Une boîte aux lettres personnelle (« BAL personnelle ») est rattachée à une personne physique pouvant être un professionnel habilité, qui en est le « Responsable opérationnel » (Voir §2.4.3), ou un usager.

Un professionnel habilité, Responsable opérationnel d'une BAL personnelle, peut déléguer l'accès à sa boite à un professionnel agissant sous sa responsabilité (le « Délégataire ») sous réserve du respect des dispositions relatives au secret professionnel et à l'échange et au partage de données de santé rappelées à l'article 2.3 du présent Référentiel#1.

L'Opérateur doit être en capacité d'identifier les personnes physiques qui ont utilisé la BAL et de tracer les accès à la BAL (voir exigence au §6.9.2).

5.1.1.2 Boîte aux lettres organisationnelle

Une boîte aux lettres organisationnelle (« BAL organisationnelle ») est accessible par un ou plusieurs professionnels habilités, ainsi que les professionnels intervenant dans le système de santé agissant sous leur responsabilité. Elle peut ainsi être utilisé par le Responsable opérationnel (s'il s'agit d'un professionnel habilité), les Cotitulaires, ainsi que les Délégataires déclarés (voir §2.4 pour la définition des rôles).
Dans le cas où le Responsable opérationnel n'est pas un professionnel habilité, il n'est pas habilité à accéder à la BAL et aux données des patients pris en charge.

Le Responsable opérationnel d'une BAL organisationnelle est en charge de la création et suppression de la BAL.

Un professionnel habilité, Responsable opérationnel et/ou Cotitulaire d'une BAL organisationnelle, peut déléguer l'accès à sa boite à un professionnel agissant sous sa responsabilité (le « Délégataire ») sous réserve du respect des dispositions relatives au secret professionnel et à l'échange et au partage de données de santé rappelées à l'article 2.3 du présent Référentiel#1.

L'Opérateur doit être en capacité d'identifier les personnes physiques qui ont utilisé la BAL et de tracer les accès à la BAL (voir par exemple EX_GDT_5060).

Une BAL organisationnelle peut, par exemple, être attribuée à un secrétariat médical, un service, un pôle, etc. et peut être utilisée par un ou plusieurs professionnels exerçant au sein d'une même structure (exemple : services de neurologie, de psychiatrie, centre d'imagerie, cabinet médical, secrétariat médical, etc…).

Les professionnels habilités auront donc la capacité d'accéder à la même BAL organisationnelle et d'émettre des messages au nom du secrétariat médical/cabinet médical/service/pôle (et non pas à titre personnel) sous réserve du respect du cadre juridique relatif à l'échange et au partage de données de santé rappelé au §2.3 du présent Référentiel #1.

Une BAL organisationnelle peut être utilisée par une structure dotée d'un FINESS (établissement de santé, centre de santé, etc.) ou par une structure libérale qui n'en dispose pas (cabinet de groupe, etc.). La déclaration dans l'Annuaire Santé diffère en fonction du type de structure concerné.

En application des dispositions de l'article L. 1110-4 du code de la santé publique et 226-13 du code pénal, chaque professionnel habilité accédant à une BAL organisationnelle doit s'assurer du respect des règles relatives au secret, et notamment que les informations ne soient accessibles qu'aux professionnels intervenant dans le cadre de la prise en charge des patients. Les secrétaires, assistants médicaux et tout autre Délégataire ne peuvent accéder aux données relatives aux patients que sous la responsabilité d'un professionnel habilité, dans le strict cadre de leurs missions et dans le respect du secret professionnel.

EX_GBM_3020

Pour une structure disposant d'un FINESS : L'Opérateur doit rattacher dans l'Annuaire Santé la BAL organisationnelle à la structure en renseignant les informations suivantes : typeBAL "ORG" ; TypeIdentifiantPM ; IdentifiantPM. La déclaration par l'Opérateur de la liste des cotitulaires de la BAL dans l'Annuaire Santé n'est pas possible.

EX_GBM_3030

Pour une structure libérale ne disposant pas de FINESS : L'Opérateur doit rattacher dans l'Annuaire Santé la BAL organisationnelle au numéro RPPS du Responsable opérationnel en renseignant les informations suivantes : typeBAL "CAB" ; TypeIdentifiantPP ; IdentifiantPP. Lorsqu'un ou plusieurs Cotitulaires accèdent à la BAL, l'Opérateur a l'obligation de déclarer dans l'Annuaire santé la liste des Cotitulaires de la BAL (limitée à 20 dont le responsable opérationnel).

Comme précisé au §5.4.2, les délégataires d'une BAL personnelle ou organisationnelle ne sont pas déclarés auprès de l'Annuaire Santé.

Une BAL organisationnelle rattachée à tort à une personne physique dans l'Annuaire Santé alors qu'elle pouvait être rattachée à une structure disposant d'un FINESS aurait pour conséquence de fausser les indicateurs d'usage et les possibilités de financement proposées

à la structure. L'Opérateur doit être vigilant dans la vérification de l'absence de FINESS pour la structure qui souscrit auprès de lui une BAL organisationnelle.

5.1.1.3 Boite aux lettres applicative

Une boîte aux lettres applicative (« BAL applicative ») est associée à un logiciel métier ou à une machine (dossier patient informatisé, système d'information de laboratoire, serveur de résultats, etc.) et est accessible directement par le logiciel ou la machine. Elle est utilisée à des fins d'envoi ou de réception automatisés. Elle doit être créée sous la responsabilité du Responsable opérationnel, qui s'assure que les échanges réalisés au moyen de la BAL respectent les finalités de prise en charge précisées dans les dispositions relatives à l'échange et au partage de données de santé.

Exemple de mise en œuvre : Si un Dossier Patient Informatisé (DPI) dispose du nom du médecin traitant, et son adresse MSSanté, le compte-rendu peut partir directement du Dossier Patient Informatisé vers la BAL du médecin.

5.1.2 Cas particulier des boites aux lettres de test

Un Opérateur peut ouvrir un nombre limité (25) des boites aux lettres de test dans l'Espace de Confiance MSSanté de production. Il n'existe pas de type particulier pour une boite aux lettres de test, l'Opérateur peut donc choisir d'ouvrir une boite de type personnelle, organisationnelle ou applicative en fonction de son besoin.

EX_GBM_4000
Les boites aux lettres de test doivent comporter dans leur dénomination la mention « test ». La dénomination d'une boîte aux lettres de tests ne doit pas comporter de données à caractère personnel (nom, prénom, etc.)

Comme toutes les boites aux lettres de l'Espace de Confiance MSSanté, les boites aux lettres de test doivent pouvoir être tracées et l'Opérateur doit être en capacité d'identifier les professionnels y ayant accès.

EX_GBM_4010
Les boites aux lettres de test ne doivent **ni émettre ni recevoir des données à caractère personnel et des données de santé**. Elles ne sont autorisées à échanger qu'avec : • Les boites aux lettres de test appartenant aux domaines de l'Opérateur • Les boites aux lettres de test des autres domaines

5.1.3 Boites aux lettres de test avec réponse automatique

Pour faciliter l'interopérabilité entre les systèmes de messagerie, l'Opérateur doit mettre à disposition une boite aux lettres de test à réponse automatique pour chacun des noms de domaine qu'il administre.

Elle doit donc répondre aux mêmes exigences qu'une BAL de test, mais doit en plus être configurée pour répondre aux messages qu'elle reçoit de manière automatique.

Ces boites aux lettres n'ont pas un objectif de supervision et ne sont pas destinées à être interrogées par des dispositifs comme des sondes mais par des messages de test unitaires permettant de vérifier l'interconnexion entre Opérateurs

EX_GBM_4020 
Chaque Opérateur doit mettre à disposition une boite aux lettres de réponse automatique par nom de domaine qu'il gère dans la liste blanche en respectant le nommage suivant : reponse.automatique-test@<domaineoperateur>.mssante.fr

EX_GBM_4030 
Les messages contenus dans la boite aux lettres de réponse automatique doivent être supprimés au maximum un mois après leur réception.

5.1.4 Les statuts (états) des BAL de l'Espace de Confiance MSSanté

Le tableau ci-dessous dénomme les états que peut prendre une boite aux lettres au sein de l'Espace de Confiance MSSanté.

État de BAL	Description
Active	Une boite aux lettres est active lorsque la dernière date de connexion est inférieure à **60 jours**.
Inactive	Une boite aux lettres est considérée comme inactive lorsque la date de dernière connexion est supérieure à **60 jours**. Cette notion est utilisée afin de caractériser l'activité des boites aux lettres dans les indicateurs remontés par chaque Opérateur
Suspendue	La BAL existe toujours et contient des messages mais il n'est plus possible pour les utilisateurs de s'y connecter, ni d'y recevoir des messages.
Supprimée	La BAL n'existe plus physiquement. À noter que les traces fonctionnelles de la BAL ne sont pas supprimées

Remarque : Les états des BAL décrits ci-dessus ont une représentation fonctionnelle, ils ne sont pas disponibles comme attribut de la BAL dans l'Annuaire Santé.

5.2 Les acteurs éligibles à l'Espace de Confiance MSSanté

A tout instant, l'Opérateur doit être en capacité d'identifier chacun des utilisateurs qui accède ou a accédé à une BAL personnelle ou organisationnelle.

EX_GBM_4230  
L'Opérateur doit tenir une base interne des utilisateurs finaux de son service MSSanté permettant de faire le lien entre les BAL personnelles et organisationnelles MSSanté de ses domaines et ses utilisateurs finaux.

5.2.1 Quels acteurs peuvent s'équiper d'une boite aux lettres personnelle ?

Un professionnel est éligible à s'équiper d'une BAL personnelle dans l'Espace de Confiance s'il répond aux trois critères suivants :

- Le professionnel est habilité par la loi à échanger des données de santé.
  L'article R. 1110-2 du code de santé publique établit une liste des professionnels habilités à échanger des données de santé (professionnel de santé, etc.) ;
- La finalité des échanges réalisés au moyen de la BAL personnelle doit être conforme à l'article L. 1110-4 du code de la santé publique (notamment les points II et III). La BAL personnelle doit donc être utilisée à des fins de prise en charge du patient et les informations échangées doivent être strictement nécessaires à la coordination, à la continuité des soins, à la prévention ou à son suivi médico-social et social ;
- Le professionnel est identifié dans le Répertoire Partagé des Professionnels intervenant dans le système de Santé (RPPS).

Dans les terminologies de référence ([NOS-RES-TERMI]) maintenue par l'ANS, le jeu de valeurs « JDV_J71-ProfessionFonction-MSSante » liste les professions et les rôles couverts par l'Espace de confiance MSSanté. L'Annuaire Santé s'appuie sur ce jeu de valeur pour valider la création des BAL aux professionnels. Ce jeu de valeurs JDV_J71 évolue en fonction des professions intégrées dans l'Annuaire Santé.

Un Délégataire peut accéder à une BAL personnelle dans l'Espace de Confiance à condition :

- D'avoir été autorisé à accéder à la BAL par le professionnel habilité titulaire de la BAL personnelle (le Responsable opérationnel) ;
- D'agir sous la responsabilité du professionnel habilité titulaire de la BAL personnelle ;
- D'être identifié dans le Répertoire Partagé des Professionnels intervenant dans le système de Santé (RPPS) ou un annuaire local (ex : structures sanitaire, médico-sociale ou sociale) ;
- D'accéder à la BAL personnelle dans le strict cadre de ses missions et sous réserve du respect des dispositions relatives au secret professionnel et à l'échange et au partage de données de santé rappelées à l'article 2.3 du présent Référentiel#1.

Un usager du système de santé dispose, s'il ne s'y oppose pas, d'une adresse de messagerie personnelle MSSanté mise à disposition par MES (Utilisateur usager). Toutefois l'usager a la possibilité de supprimer son adresse. Le cas échéant, l'usager pourra de nouveau réouvrir l'accès à sa BAL MSSanté.

EX_GBM_4200	 
L'Opérateur doit s'assurer que les BAL MSSanté personnelles sont exclusivement utilisées sous la responsabilité du professionnel habilité ou de l'Utilisateur usager titulaire de cette adresse (ou de ses représentants légaux).	

Exemple de mise en œuvre[4] :
Ci-dessous un médecin libéral en exercice individuel qui délègue l'accès à sa BAL personnel à la secrétaire médicale qu'il emploie.

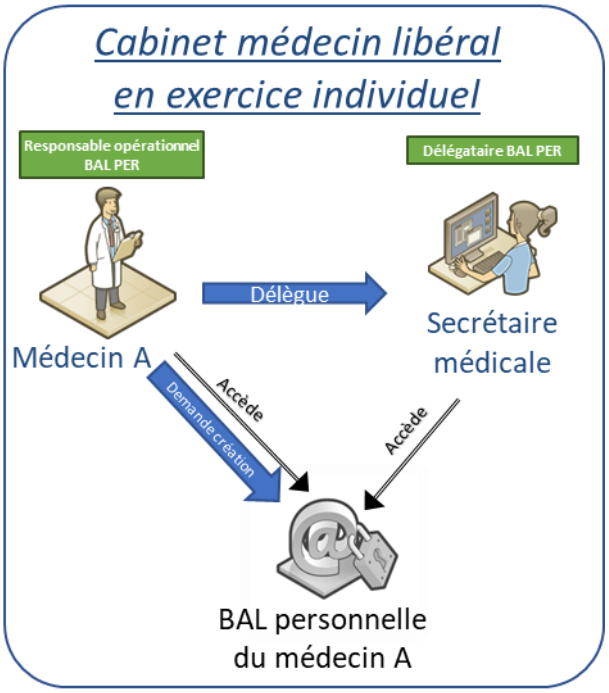


Figure 20 : Exemple de BAL personnelle déléguée

5.2.2 Quels acteurs peuvent accéder à une boite aux lettres organisationnelle ?

L'ouverture d'une BAL organisationnelle dans l'Espace de Confiance MSSanté se fait selon les conditions suivantes :

- Elle doit être créée par le Responsable opérationnel chargé de la création / suppression de la BAL organisationnelle.
- **Les professionnels accédant à la BAL doivent être habilités par la loi à échanger des données de santé conformément aux dispositions de l'article L. 1110-4 du code de la santé publique. L'article R1110-2 du code de santé publique établit une liste des professionnels habilités à échanger des données de santé.**
- La finalité des échanges réalisés au moyen de la BAL organisationnelle doit être conforme à l'article L. 1110-4 du code de la santé publique (notamment les points II et III). La BAL organisationnelle doit donc être utilisée à des fins de prise en charge d'un même patient et les informations échangées doivent être strictement nécessaires à la coordination, à la continuité des soins, à la prévention ou à son suivi médico-social et social.

[4] Sous réserve du respect des dispositions relatives au secret professionnel et à l'échange et au partage de données de santé rappelées au §2.3 du présent Référentiel #1

- La BAL organisationnelle doit :
    - **Pour une structure sanitaire ou médico-sociale disposant d'un numéro FINESS,** être rattachée à la structure dans l'Annuaire Santé ;
    - **Pour une structure sanitaire ou médico-sociale ne bénéficiant pas d'un FINESS,** être rattachée dans l'Annuaire Santé au numéro RPPS du « Responsable opérationnel ».

Un Délégataire peut accéder à une BAL organisationnelle dans l'Espace de Confiance à condition :

- D'avoir été autorisé à accéder à la BAL par un Cotitulaire ou le Responsable opérationnel de la BAL organisationnelle ;
- D'agir sous la responsabilité du Cotitulaire de la BAL ;
- D'être identifié dans le Répertoire Partagé des Professionnels intervenant dans le système de Santé (RPPS) ou de l'annuaire local (contexte structures sanitaire, médico-sociale ou sociale) ;
- D'accéder à la BAL organisationnelle dans le strict cadre de ses missions et sous réserve du respect des dispositions relatives au secret professionnel et à l'échange et au partage de données de santé rappelées au §2.3 du présent Référentiel #1.

Exemples de mise en œuvre[5] :
Une BAL organisationnelle peut être utilisée, par exemple par les secrétaires médicales, sous la responsabilité d'un médecin conformément aux dispositions de l'article R. 4127-72 du code de la santé publique, pour faciliter l'envoi de compte-rendu et la réception de mail dans un établissement de santé et/ou un cabinet médical. Dans ce cas, c'est à l'établissement de santé ou au cabinet médical de gérer les habilitations et les accès à cette BAL organisationnelle en fonction de la politique de sécurité de son SI.

[5] Sous réserve du respect des dispositions relatives au secret professionnel et à l'échange et au partage de données de santé rappelées au §2.3 du présent Référentiel #1

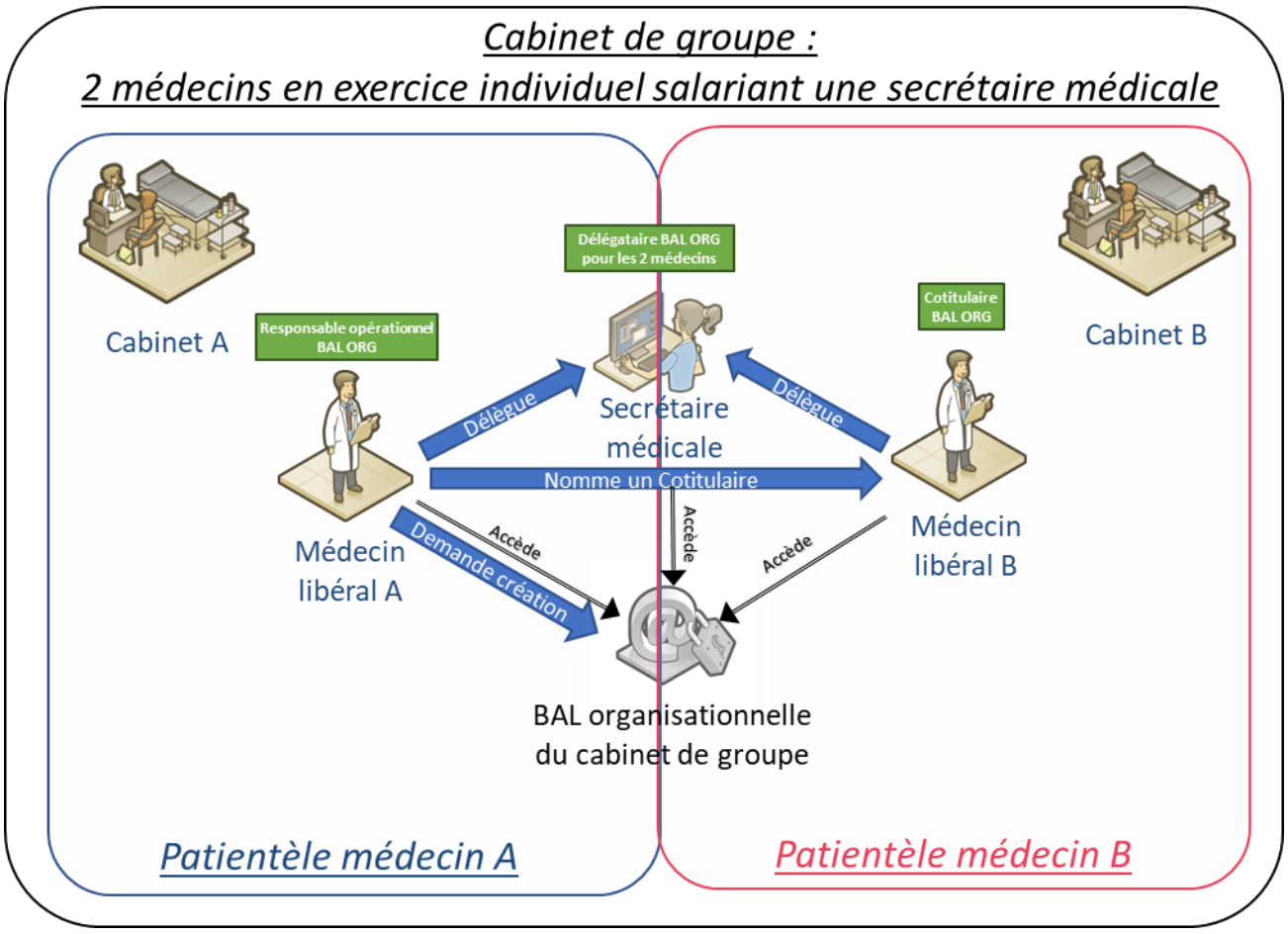


Figure 21 : Exemple de BAL organisationnelle en cabinet de groupe

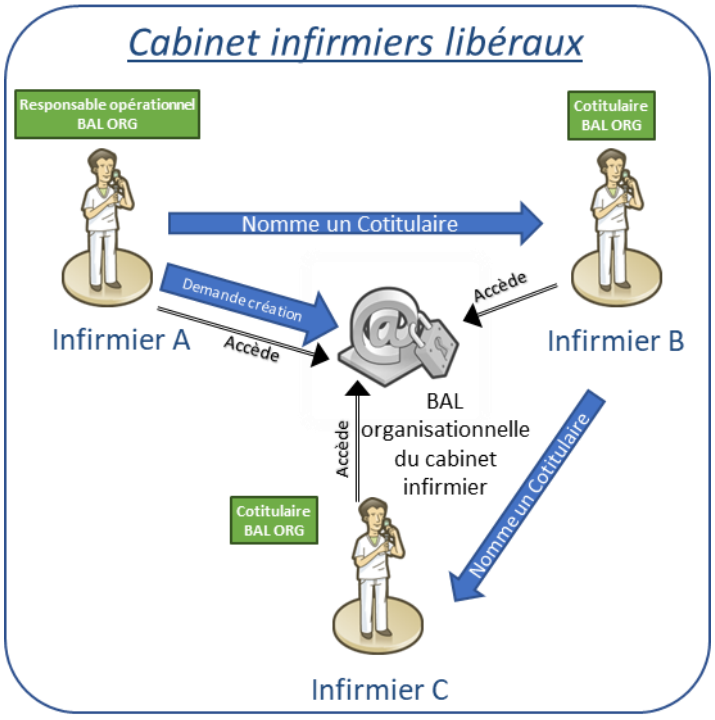


Figure 22 : Exemple de BAL Organisationnelle dans un cabinet d'infirmiers libéraux

5.2.3 Quels acteurs peuvent accéder à une boite aux lettres applicative ?

L'ouverture d'une BAL applicative dans l'Espace de Confiance MSSanté se fait selon les conditions suivantes :

- Les BAL applicatives sont ouvertes sur demande de la structure.
- La structure doit désigner un Responsable opérationnel. Le Responsable opérationnel s'assure que les échanges réalisés au moyen de la BAL respectent les finalités de prise en charge précisées dans les dispositions de l'article L.1110-4 du code de la santé publique. La BAL applicative doit donc être utilisée à des fins de prise en charge d'un même patient et les informations échangées doivent être strictement nécessaires à la coordination, à la continuité des soins, à la prévention ou à son suivi médico-social et social.
- Les professionnels accédant à la BAL applicative doivent être des professionnels habilités par la loi à échanger des données de santé conformément aux dispositions de l'article L. 1110-4 du code de la santé publique. L'article R1110-2 du code de santé publique établit une liste des professionnels habilités à échanger des données de santé.
- Les BAL applicatives doivent être rattachées à une structure sanitaire ou médico-sociale possédant un numéro FINESS ou bien un numéro SIRET/SIREN référencé dans l'Annuaire Santé.

EX_GBM_4220

Le professionnel déclaré comme Responsable opérationnel d'une BAL Organisationnelle ou Applicative doit être :

- être un professionnel identifié dans l'Annuaire Santé ou par un fournisseur d'identité local ;
- lorsqu'il accède au contenu de la BAL, être un professionnel habilité par la loi à échanger des données de santé conformément aux dispositions de l'article L. 1110-4 du code de la santé publique ;
- lorsqu'il n'accède pas au contenu de la BAL, être représentant légal de la structure, ou de tout professionnel agissant en son nom et pour son compte.

5.3 L’ouverture de boites aux lettres au sein de l’Espace de Confiance MSSanté

L’Opérateur a pour charge de veiller à ce que les boites aux lettres créées dans l’Espace de Confiance MSSanté respectent les exigences de nommage suivantes :

EX_GBM_4300


E

L'Opérateur DOIT utiliser des formats d'adresses de messagerie qui respectent les conditions suivantes :

- la RFC 5321 (https://datatracker.ietf.org/doc/html/rfc5321).
- les contraintes de l'Annuaire Santé, à savoir que seuls les caractères suivants sont autorisés (ne pas prendre en compte les points-virgules) : caractères alphanumériques ; . ; _ ; - ; +.

EX_GBM_4310

E

L’Opérateur ne doit pas décrire une BAL applicative ou organisationnelle avec des informations nominatives relatives à un utilisateur de type personne physique. Il est toutefois possible de recourir à un nom d’organisation ou de structure dans le nommage de la BAL, comme par exemple :

- service-cardiologie@xyz.mssante.fr ;
- cabinet-dr-martin@xyz.mssante.fr ;
- service-pr-dupont@xyz.mssantefr ;
- institut-pasteur.secretariat@xyz.mssante.fr.

EX_GBM_4311

E

L’Opérateur doit créer les BAL personnelles au format : prenom.nom@<domaineOpérateur>.mssante.fr. Cette exigence n’est applicable que pour les BAL créées après la mise en conformité au référentiel v1.6.

Toutefois l’opérateur peut déroger à cette règle en cas d’homonymie sur un même nom de domaine.

RE_GBM_4320
L'Opérateur doit être vigilant quant aux dénominations des adresses de messagerie demandées par ses utilisateurs. Elles doivent être explicites, pour permettre aux autres utilisateurs de facilement identifier la personne physique ou l'entité fonctionnelle ou technique titulaires de cette adresse de messagerie. Voici quelques exemples de nommage : • Pour les BAL personnelles : ○ prenom.nom@<domaine>.mssante.fr ○ matricule_INS@patient.mssante.fr • Pour les BAL organisationnelles : ○ service-nom_du_service@<domaine>.mssante.fr ○ service-cardiologie@<domaine>.mssante.fr ○ cabinet-dr-martin@<domaine>.mssante.fr ○ service-pr-dupont@<domaine>.mssante.fr ○ institut-pasteur.secretariat@<domaine>.mssante.fr • Pour les BAL applicatives (pour des BAL rattachées à des applications ou des machines) : ○ automate_biologie_14@<domaine>.mssante.fr ○ dispositif_médical_XYZ@<domaine>.mssante.fr ○ notification_SIH_ABC@<domaine>.mssante.fr

L'ensemble des boites aux lettres ouvertes dans l'Espace de Confiance doivent être publiées dans l'Annuaire Santé à l'exception des boites aux lettres personnelles des usagers (Utilisateurs usager) et des boites aux lettres de test.

RE_ GBM_4330
L'Opérateur devrait être vigilant sur la gestion de la réattribution des BAL MSSanté, et notamment sur la période nécessaire avant de pouvoir réattribuer une BAL à un autre professionnel habilité.

5.4 Les règles de fonctionnement des boites aux lettres au sein de l'Espace de Confiance MSSanté

5.4.1 Fonctionnalités relatives aux BAL de l'Espace de Confiance MSSanté

Les boites aux lettres de l'Espace de Confiance doivent répondre aux exigences suivantes :

EX_GBM_4410


Afin de garantir l'interopérabilité entre systèmes MSSanté, tous les Opérateurs doivent permettre l'échange de messages de taille inférieur ou égale à 10 Mo (pièces jointes encodées comprises).

L'Opérateur a la possibilité d'autoriser des échanges de messages de taille supérieure à 10 Mo.

EX_GBM_4420


Afin de minimiser les risques d'émission de messages non sollicités, les Opérateurs doivent limiter le nombre de destinataires d'un message à 40 au maximum.

EX_GBM_4430

L'Opérateur émetteur de messages depuis des BAL applicatives doit s'assurer qu'il est en mesure d'exploiter en réception des messages de type « indicateur d'absence » ou « message de saturation de BAL » afin de pouvoir déclencher les actions appropriées.

RE_GBM_4410

La RFC 5321 précise les bonnes pratiques de notification du statut de remise de message (voir § 6.7.1.1).

Afin de favoriser les usages et la dématérialisation des échanges, et afin de permettre aux destinataires d'entreprendre les actions adaptées en fonction des différents cas d'usage rencontrés, il est fortement recommandé au service MSSanté réceptionnant une notification à destination d'un utilisateur final de son service (accusé de réception, non remise de message pour cause de boîte pleine ou inexistante, non remise de message pour cause de domaine destinataire ne faisant pas partie de l'Espace de Confiance, détection de virus, etc.), de faire en sorte que cette notification soit facilement interprétable pour l'utilisateur final (habillage spécifique, traduction, etc.).

EX_GBM_5410

L'Opérateur DOIT mettre à disposition des Cotitulaires d'une BAL organisationnelle, rattachée à un Responsable opérationnel, un dispositif (écran, procédure, ...) lui permettant de modifier les attributs suivants :

- d'ajouter / supprimer des Cotitulaires et des Délégataires à la liste des professionnels habilités à accéder à la BAL ;
- de modifier le champ "description" de la BAL ;
- de changer de « Responsable opérationnel » de la BAL.

L'historique de ces actions doit être conservé au titre des traces fonctionnelles (voir §6.9.2).

5.4.2 Délégation d'accès aux BAL MSSanté

La délégation d'accès permet à un Cotitulaire ou un Responsable opérationnel d'autoriser l'accès d'un Délégataire à une BAL personnelle ou organisationnelle (voir définition au §2.4).

La délégation permet au Délégataire d'accéder à une BAL organisationnelle ou personnelle, pour le compte du Responsable opérationnel ou du Cotitulaire auquel il est rattaché.

La mise en place d'une délégation d'accès est effectuée sous la responsabilité du Cotitulaire et/ou du Responsable opérationnel de la BAL MSSanté à l'initiative de l'action.

À titre d'exemple les secrétaires, assistants médicaux ou médecins remplaçant peuvent être identifiés comme des Délégataires sous réserve du respect des conditions énoncées au §2.4 du présent Référentiel #1.

Le Délégataire dispose uniquement du droit de consulter et/ou d'envoyer des messages via la BAL à laquelle il a accès. Il ne peut pas déclarer de nouveaux Délégataires, Cotitulaires et Responsables opérationnel.

EX_GBM_5411

L'Opérateur DOIT proposer la fonction de délégation pour toutes les BAL personnelles ou organisationnelles, tel que décrit au §5.4.2 du présent Référentiel #1 Opérateur. Les BAL applicatives ne proposent pas de fonction de délégation.

Le Cotitulaire et/ou le Responsable opérationnel d'une BAL doit avoir la capacité de choisir le ou les Délégataires identifiés dans l'Annuaire Santé ou dans un annuaire local (dans le contexte d'un établissement de santé). Comme précisé au §2.4.3, le Cotitulaire et/ou le Responsable opérationnel d'une BAL est responsable des accès qu'il pourrait ouvrir par délégation.

EX_GBM_5413

L'Opérateur DOIT proposer aux utilisateurs finaux un dispositif (écran, procédure, ...) de gestion des délégations d'accès (création, consultation, modification, suppression).

L'Opérateur maintient la liste des délégataires habilités à accéder à une BAL MSSanté. Ils ne sont pas déclarés auprès de l'annuaire santé. Il n'est donc pas possible via l'annuaire santé d'effectuer une recherche de BAL MSSanté à partir d'un délégataire.

EX_GBM_5414

L'Opérateur DOIT permettre aux Délégataires d'accéder aux BAL MSSanté à travers les mêmes interfaces (API LPS, mode d'accès spécifique à l'opérateur, …) que les Responsables opérationnel et Cotitulaires des BAL MSSanté.

L'historique des actions de délégation doit être conservé au titre des traces fonctionnelles (voir §6.8.2).

5.4.3 Mesures de sécurité propres aux BAL MSSanté

De par sa conception basée sur une liste blanche des domaines autorisés, l'Annuaire Santé et des mesures de sécurité spécifiques, le système MSSanté constitue un espace sécurisé garantissant l'authenticité et la confidentialité des messages échangés.

Néanmoins, comme tout système de messagerie et malgré les mesures de sécurité mises en œuvre, les Opérateurs MSSanté peuvent faire l'objet de tentatives d'attaque comme l'envoi en masse (« spamming ») et l'hameçonnage (« phishing »), technique d'attaque par l'envoi de messages malveillants invitant le destinataire à cliquer sur les liens ayant pour effet d'installer un logiciel malveillant et/ou d'amener le destinataire à divulguer sur un site malveillant ses identifiants et mots de passe de sa BAL, de sa session Windows, etc. La BAL compromise permet ensuite de compromettre d'autres BAL par rebond.

Ces attaques peuvent être facilitées par les messageries professionnelles unifiées qui combinent au sein d'une même BAL une messagerie standard (non sécurisée) et une messagerie MSSanté. Ainsi la compromission de la BAL au travers du canal de la messagerie standard permet de propager l'attaque dans l'Espace de Confiance MSSanté.

Ces méthodes d'attaque sont très répandues et constituent une menace réelle pour les Opérateurs MSSanté, leurs utilisateurs et les données échangées pour lesquels il convient de prendre des mesures de sécurité adaptées qui dépassent le cadre du Référentiel #1 Opérateurs.

5.4.3.1 Mesures préventives

Dans l'objectif de réduire le risque de ces actes de malveillance, une vigilance s'impose à tous les Opérateurs MSSanté et aux utilisateurs de BAL MSSanté par le biais des bonnes pratiques suivantes (liste non limitative) :

- Opter pour des méthodes d'authentifications fortes (à double facteurs) des utilisateurs conformes à la PGSSI-S ;
- Sensibiliser les utilisateurs sur les bonnes pratiques de mots de passe, d'utilisation d'une messagerie et notamment sur les réflexes à avoir en cas de réception de mails suspicieux ;
- Installer des outils anti-phishing pour les BAL ou les navigateurs tels que SpamAssassin, ClamAV, etc.

5.4.3.2 Mesures correctives

En cas de compromission avérée d'une ou plusieurs BAL, il convient pour l'Opérateur d'agir très rapidement en s'appuyant sur les consignes suivantes :

- Couper les accès à la messagerie ou en restreindre l'accès (par exemple suppression des accès depuis l'extérieur) ;
- Couper le lien entre le système de messagerie et le connecteur MSSanté ;
- Identifier les BAL compromises par retour des utilisateurs victimes d'hameçonnage, analyse de la date du dernier changement de mot de passe, etc. ;
- Couper l'accès au réseau à ces postes utilisateurs ;
- Déterminer la profondeur de l'infection du poste de travail : présence de virus, portes dérobées, etc. et le réinstaller en cas de doute ;
- Changer le mot de passe de la BAL compromises et des autres comptes de l'utilisateur (qui sont généralement compromis également).

L'ensemble des exigences de sécurité relatives au fonctionnement de l'Espace de Confiance MSSanté et à implémenter par l'Opérateur MSSanté se trouvent dans le chapitre §6.9.5.

5.5 Suspension d'une boite aux lettres de l'Espace de Confiance MSSanté

5.5.1 Caractéristiques d'une BAL suspendue

Lorsqu'une boite aux lettres de l'Espace de Confiance MSSanté présente un risque (sécurité ou autre), l'Opérateur est autorisé à la suspendre temporairement de l'Espace de Confiance MSSanté en attendant de mettre en place les mesures nécessaires pour éliminer ce risque.

Une boite aux lettres suspendue de l'Espace de Confiance MSSanté n'est plus accessible par son ou ses utilisateurs. Cette boite aux lettres ne peut plus émettre ni recevoir de messages.

Les boites aux lettres suspendues ne doivent plus être publiées dans l'Annuaire Santé, il faut également les exclure des extractions mensuelles.

RE_GBM_4420
Il est recommandé aux Opérateurs de prévoir un dispositif permettant de suspendre des boites aux lettres de l'Espace de Confiance MSSanté. La suspension d'une boite aux lettres implique le blocage de l'accès de cette BAL à son ou ses utilisateurs et également le rejet des messages entrants. Pour une meilleure clarté, il est également recommandé de ne pas publier dans l'Annuaire Santé les boites aux lettres suspendues Pour les Opérateurs souhaitant mettre en place le dispositif de suspension des boites aux lettres, il est possible de se baser sur les DSN décrits dans la RFC 3463 pour rejeter les messages à destination d'une BAL suspendue (voir la partie : Mailbox status - x.2.1 Mailbox disabled, not accepting message).

5.5.2 Comment suspendre une boite aux lettres de l'Espace de Confiance

Un Opérateur peut, lorsqu'il constate un mésusage d'une boite aux lettres créée sur un de ses noms de domaines vis-à-vis de ses conditions générales d'utilisation (CGU), prendre des mesures allant jusqu'à la suspension de la boite aux lettres. Il doit cependant notifier le responsable de la structure dans un délai prévu par les CGU de la suspension de la boite aux lettres. Cette notification doit comprendre le motif de la suspension.

L'ANS, en sa qualité de gestionnaire de l'Espace de Confiance MSSanté, peut demander à tout Opérateur de procéder à la suspension d'une BAL qu'il considère comme non conforme aux conditions d'utilisation au sein de l'Espace de Confiance MSSanté.

RE_GBM_4430
Un Opérateur doit pouvoir transmettre au responsable de la structure la liste des boites aux lettres suspendues dont il a la charge ainsi que le motif de la suspension.

RE_GBM_4440
L'Opérateur implémentant un dispositif de suspension d'une boite aux lettres de l'Espace de Confiance MSSanté doit prévoir un dispositif permettant la réactivation de cette même boite aux lettres.

RE_GBM_4450
L'Opérateur doit prévoir un système permettant aux utilisateurs qui en feraient la demande de récupérer les messages stockés dans leur boite aux lettres lorsque cette dernière est suspendue.

5.6 Dépublication d’une boite aux lettres de l’Annuaire Santé

L’objectif de cette exigence est de ne plus faire apparaitre dans l’Annuaire Santé les BAL inactives, c'est-à-dire celles qui n'ont pas fait l'objet d'une connexion de l'utilisateur final depuis plus de 2 mois.

Pour se faire, le mécanisme de publication des BAL « en liste rouge » dans l’Annuaire Santé va être utilisé. Cette mise en liste rouge s’effectue à l’initiative de l’Opérateur et non à celle du professionnel.

Les boites aux lettres de l’Espace de Confiance dépubliées de l’Annuaire Santé existent toujours, ainsi que les messages qu’elles contiennent. Elles restent hébergées par l’Opérateur et sont intégralement fonctionnelles.

EX_GBM_4440

L’Opérateur doit positionner en liste rouge sur l’Annuaire Santé toute BAL 'personnelle' ou 'organisationnelle' créée depuis plus d’un an et qui n’a pas fait l’objet d’une connexion par un utilisateur final depuis plus de 60 jours consécutifs.

Cette action doit être systématiquement précédée, quinze jours avant, d’une information de l’utilisateur par le canal de son choix (hors envoi via l’Espace de Confiance), afin de lui permettre, le cas échéant, de s’opposer à cette dépublication en se connectant de nouveau à sa BAL MSSanté.

Les modalités d’envoi de ce message d’alerte, ainsi que le principe de mise en liste rouge, sont portées par tout moyen à la connaissance de l’utilisateur, par exemple dans les conditions générales d’utilisation du service de messagerie sécurisée.

La connexion d’un utilisateur final à une BAL mise en liste rouge par ce principe sur l’Annuaire Santé, doit entrainer son retrait de ladite liste rouge, sauf si l’utilisateur avait préalablement explicitement demandé la mise en liste rouge.

Il est recommandé dans le message d’alerte envoyé au professionnel d’utiliser le terme « dépublié pour cause d’inactivité », plutôt que le terme en « liste rouge » qui est à réservé à la fonctionnalité de dépublication à son initiative. Cela permet d’éviter toute confusion entre les deux motifs de dépublication de l’Annuaire Santé.

5.7 Suppression d’une boite aux lettres de l’Espace de Confiance MSSanté

Les boites aux lettres de l’Espace de Confiance MSSanté supprimées n’existent plus physiquement.

EX_GBM_6010

Le service de messagerie Messageries Sécurisées de Santé de l’Opérateur doit comporter un dispositif permettant de supprimer les boîtes aux lettres en cas d’absence d’authentification de l’utilisateur final pendant une période d’un an, conformément aux recommandations de la CNIL.

Toute suppression doit être systématiquement précédée, deux mois avant échéance, d’une information de l’utilisateur par le canal de son choix, hors envoi via l’Espace de Confiance, afin de lui permettre, le cas échéant, de s’opposer à cette suppression.

Les modalités et le rythme d’envoi de ce message d’alerte sont portés par tout moyen à la connaissance de l’utilisateur, par exemple dans les conditions générales d’utilisation du service de Messageries sécurisées de Santé.

Cette exigence implique la fermeture de la BAL et la suppression des messages et pièces jointes associées de manière irrévocable.

Les traces fonctionnelles et techniques associées à cette BAL doivent quant à elles faire l’objet d’une conservation conformément à l’exigence EX_GDT_5070.

Les boites aux lettres supprimées ne doivent plus être publiées dans l’Annuaire Santé.

EX_GBM_6020

Avant de retirer un nom de domaine de la liste blanche, et donc de l’Espace de Confiance MSSanté, l’Opérateur doit supprimer de l’Annuaire Santé l’ensemble des BAL MSSanté rattachées à ce domaine.

6 Transactions à implémenter par les Opérateurs MSSanté

Le contrat « Opérateur MSSanté v2 » [CONTRAT-MSSANTE] conditionne l'intégration validée de l'Opérateur à l'Espace de Confiance au respect d'un ensemble de dispositions techniques et fonctionnelles identifiées dans le présent **Référentiel #1** sous la notion d'« exigences » (cf. § 1.2).

Ces exigences sont définies dans le présent document et sont susceptibles d'évoluer. Leur évolution donne lieu à la publication d'une nouvelle version du **Référentiel #1** (voir § 1.3 « Gestion des versions successives »).

Ces exigences concernent :

- Les transactions à implémenter par l'Opérateur (voir § 6.1) ;
- La mise en œuvre globale d'un service d'Opérateur (voir § 6.9) incluant la :
    - Synchronisation du temps (§ 6.9.1),
    - Gestion des traces (§ 6.9.2),
    - Production de statistiques d'utilisation (§ 6.9.3),
    - Définition de Conditions Générales d'Utilisation (CGU) du service MSSanté (§ 6.9.4),
    - Exigences complémentaires de sécurité (§ 6.9.5).

L'Opérateur MSSanté doit :

- **mettre en œuvre un Connecteur MSSanté** pour le raccordement de son serveur de messagerie à l'Espace de Confiance MSSanté ;
- **mettre en œuvre l'API LPS** pour le raccordement de son serveur de messagerie à des logiciels métiers comportant des fonctionnalités de messagerie MSSanté ;
- **fournir lui-même des BAL MSSanté aux utilisateurs de son service**.

L'Opérateur MSSanté peut également mettre en œuvre un Connecteur à l'Annuaire Santé pour la recherche dans l'Annuaire Santé par les utilisateurs de son service de messagerie.

6.1 Choix des transactions à implémenter pour le Connecteur MSSanté d'un Opérateur

Le tableau ci-après présente les transactions MSSanté qu'il est nécessaire ou possible de mettre en œuvre en tant qu'Opérateur MSSanté.

Les transactions « requises » doivent impérativement être implémentées dans la solution présentée par l'Opérateur souhaitant intégrer l'Espace de Confiance MSSanté.

Les transactions « optionnelles » peuvent être mise en œuvre, selon les besoins des utilisateurs et le planning de l'Opérateur ou l'usage qu'il prévoit pour les utilisateurs, leur métier, etc.

Chaque transaction implique ses propres règles de gestion qui peuvent se traduire, soit par des exigences obligatoirement mises en œuvre par l'Opérateur, soit par des recommandations laissées à la libre appréciation de l'Opérateur.

Transactions MSSanté pour les Opérateurs MSSanté		Description	Obligatoire Optionnel	Protocoles
Publication des BAL MSSanté dans l'Annuaire Santé				
TM1.1.1P	Mise à jour des BAL dans l'Annuaire Santé en **Web Services en mode global** et récupération du compte-rendu d'alimentation	Transaction de publication des BAL MSSanté d'un domaine de messagerie dans l'Annuaire Santé	Obligatoire (sauf pour un Opérateur usagers)	Web Services SOAP
Consultation / Téléchargement d'une extraction de l'Annuaire Santé				
TM2.1.1A	Consultation de l'Annuaire Santé par le protocole LDAP	Recherche multicritère de correspondants dans l'Annuaire Santé	Option	LDAP
TM2.1.3A	Téléchargement d'une extraction de l'Annuaire Santé	Récupération d'une copie des données de l'Annuaire Santé par téléchargement d'une extraction (**décommissionné courant 2025)**		Web Services REST
TM2.1.4A	Téléchargement des données d'identités des futurs utilisateurs finaux	Récupération des données à caractère personnel de personnes physiques des secteurs sanitaire et médico-social - porteurs et non porteurs de cartes CPS. Ces données sont issues de répertoires nationaux d'identité. **(décommissionné courant 2024)**	Option	Web Services REST
Liste Blanche				
TM4.1P	Interrogation de la liste blanche des domaines de messagerie MSSanté	Fonction de récupération de la liste blanche des domaines de messagerie autorisés à échanger dans l'Espace de Confiance MSSanté	Obligatoire	HTTPS
Échange de messages entre Opérateurs MSSanté (API Opérateurs)				
TM3.1P	Réception de messages	Fonctions de réception de messages depuis des domaines de l'Espace de Confiance MSSanté, sur le protocole SMTP avec extension STARTTLS	Obligatoire	SMTP + Starts
TM3.2P	Émission de messages	Fonctions d'émission de messages vers des domaines de l'Espace de Confiance MSSanté, sur le protocole SMTP avec extension STARTTLS	Obligatoire	SMTP+ Starts
Services de messagerie à proposer aux logiciels métiers (API LPS)				
TM5.1P	Autoconfiguration de l'API LPS	Autoconfiguration du LPS à partir des informations présentes dans les entrées DNS. Évite la saisie manuelle des paramètres de configuration	Obligatoire (sauf pour un Opérateur usagers)	DNS
TM5.2P	Émission de messages d'une BAL personnelle ou organisationnelle via API LPS	Fonctions d'envoi de messages depuis une BAL personnelle ou organisationnelle sur le protocole SMTP avec extension STARTTLS	Obligatoire (sauf pour un Opérateur usagers)	SMTP + StartTLS

TM5.3P	Consultation de messages d'une BAL personnelle ou organisationnelle via API LPS	Fonctions de consultation de messages depuis une BAL personnelle ou organisationnelle sur le protocole IMAP avec extension STARTTLS	Obligatoire (sauf pour un Opérateur usagers)	IMAP + StartTLS
TM5.4P	Émission et consultation de messages d'une BAL applicative via API LPS	Fonctions d'envoi et de consultation de messages depuis une BAL applicative sur les protocoles SMTP et IMAP avec extension STARTTLS	Option	SMTP / IMAP + StartTLS
TM5.5A	Autre interface avec les LPS	Fonctions gestion de messages	Option	adhoc

Tableau 2 : Liste des transactions MSSanté pour les Opérateurs MSSanté

6.2 Modalités techniques pour assurer la sécurisation des échanges entre opérateurs

Ce chapitre décrit les modalités de raccordement des Connecteurs MSSanté mis en œuvre par les Opérateurs pour accéder à l'Espace de Confiance MSSanté.

6.2.1 Principes de raccordement des Connecteurs MSSanté des Opérateurs à l'Espace de Confiance MSSanté

L'intégration des Opérateurs MSSanté à l'Espace de Confiance MSSanté repose sur les principes décrits ci-dessous.

Une liste fermée de domaines de messagerie autorisés

Les utilisateurs des domaines MSSanté ne peuvent ni envoyer ni recevoir de messages d'utilisateurs situés dans des domaines de messagerie non MSSanté.

Les Connecteurs MSSanté des Opérateurs doivent s'assurer que les émissions et réceptions de messages se font respectivement vers et depuis des domaines MSSanté, référencés comme tels dans la liste blanche (fermée) des domaines autorisés MSSanté (cette liste contient notamment des informations sur leurs certificats d'authentification associés). Tout domaine de messagerie MSSanté doit ainsi filtrer, sur la base de cette liste, les domaines avec lesquels il accepte d'établir des échanges de messages sécurisés.

Ainsi, seuls les domaines de messagerie MSSanté peuvent échanger entre eux.

Cette liste est gérée et publiée par l'ANS et tous les Connecteurs MSSanté des Opérateurs doivent la prendre en compte (voir **§** 6.6.1 « TM4.1P - Interrogation de la liste blanche des domaines de messagerie MSSanté »).

Remarque : en dehors de cet aspect spécifique, le système MSSanté repose sur l'utilisation du réseau Internet public et sur une gestion standard des domaines de messagerie dans le serveur de noms de domaines (DNS).

Sécurisation des échanges de messages

Les échanges réalisés entre les domaines de messagerie MSSanté reposent sur le protocole SMTP, c'est-à-dire le protocole SMTP standard, sécurisé par une connexion TLS mettant en œuvre une authentification mutuelle des deux MTA par certificats X509 (délivrés par l'ANS), et d'assurer l'intégrité et la confidentialité des échanges.

EX_OPE_5010


Le connecteur MSSanté de l'Opérateur DOIT supporter TLS 1.2 (cf. RFC 5246 - http://tools.ietf.org/html/rfc5246), avec uniquement les suites de chiffrement TLS1.2 suivantes :

- 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

Dans le cas contraire, la connexion ne doit pas être établie.

Les versions SSLv2, SSLv3 ne doivent pas être activées.

La longueur du groupe DH doit être >= 2048 bits ou la longueur du groupe elliptique ECDH doit être >= 256 bits.

La confidentialité persistante (PFS - perfect forward secrecy) de DH doit être utilisée (DHE ou ECDHE).

La compatibilité TLS 1.0 et TLS 1.1 est arrêtée depuis la fin de mise en conformité avec le Référentiel #1 v1.5 en septembre 2023.

RE_OPE_5015

En complément de TLS 1.2, le connecteur MSSanté PEUT supporter TLS 1.3 ou toute version supérieure.

6.2.2 Validation des certificats serveur

EX_OPE_5020	 
Le Connecteur MSSanté de l'Opérateur doit initialiser ou accepter les connexions SMTP uniquement après validation d'un certificat serveur X509 délivré par l'ANS selon la norme PKIX (voir RFC 5280 (http://tools.ietf.org/html/rfc5280), RFC 2246 (http://tools.ietf.org/html/rfc2246), RFC 3207 (http://tools.ietf.org/html/rfc3207) et RFC 2034 (http://tools.ietf.org/html/rfc2034) et ayant une correspondance dans la Liste Blanche (DN du certificat).	

Le certificat serveur présenté par les acteurs techniques de l'échange est émis par l'ANS.

Des précisions sur les certificats IGC-Santé utilisés par les serveurs des Opérateurs MSSanté sont disponibles aux adresses suivantes : http://igc-sante.esante.gouv.fr/PC/#ca et https://esante.gouv.fr/securite/cartes-et-certificats

EX_OPE_5030	 
Sur l'interface SMTP, les connecteurs de messagerie MSSanté des Opérateurs doivent gérer la chaîne de certification de l'IGC-Santé gamme Élémentaire.	

Chaines de certification

L'ANS assure le rôle d'autorité de certification (AC) pour les certificats qu'elle délivre.

EX_OPE_5040
Les certificats utilisés par les serveurs de messagerie des Opérateurs MSSanté DOIVENT être issus de la branche gamme Élémentaire / domaine Organisation de l'IGC Santé. Les certificats racine et intermédiaire de cette branche sont donc nécessaires pour valider les certificats serveurs. Ils doivent être récupérés sur le site http://igc-sante.esante.gouv.fr/PC/#ca, et déployés dans le magasin de confiance du Connecteur MSSanté de l'Opérateur.

Lors de l'envoi du certificat serveur par un Connecteur, il n'est pas nécessaire d'envoyer en complément les certificats racine et intermédiaire.

En effet pour la validation de la chaine du certificat serveur envoyé par un Connecteur distant, il est recommandé de se baser sur les certificats racine et intermédiaire stockés dans le magasin de confiance du Connecteur et non sur ceux envoyés par le Connecteur distant.

Lorsque cette validation échoue, la tentative de connexion doit être interrompue (il est recommandé d'en informer l'utilisateur par un message d'erreur spécifique).

Contrôle de non révocation

EX_OPE_5050
Le Connecteur MSSanté de l'Opérateur DOIT faire un contrôle de non révocation des certificats serveurs présentés par les Opérateurs distants de messagerie MSSanté.

L'ANS, en sa qualité d'autorité de certification dispose d'un service OCSP (Online Certificate Status Protocol). De plus les CRL de l'IGC-Santé sont publiées en totalité une fois par jour, des delta-CRL sont publiées également quotidiennement. Ces CRL peuvent être téléchargées par le Connecteur MSSanté au moyen d'une tâche planifiée.

Les informations et ressources (fichiers) sur les AC et les listes de révocation (CRL) sont disponibles sur le site https://industriels.esante.gouv.fr/produits-et-services/igc-sante-certificats-personnes-morales-et-serveurset sur le site http://igc-sante.esante.gouv.fr/PC/#ca pour les AC du domaine Organisations de l'IGC-Santé.

Vérification des certificats des AC installés

RE_OPE_5040
Pour assurer la sécurité de l'Espace de Confiance, il est recommandé de vérifier lors de l'installation du connecteur et régulièrement par la suite que les certificats racine et intermédiaire de l'AC IGC Santé installés sont identiques à ceux de la source de Confiance. : http://igc-sante.esante.gouv.fr/PC/#ca

Cette vérification est basée sur la comparaison des empreintes numériques des certificats installés avec celles de la source de Confiance.

Le calcul de l'empreinte peut être effectué de la manière suivante :

- Utilisation de la visionneuse de certificat Windows (onglet "Détail", "<tout>", dernière ligne) ;
- Utilisation de la commande "openssl x509 -fingerprint" sur le fichier certificat ;
- Utilisation des commandes "sha1sum" ou "sha256sum" sur le certificat dans sa forme DER.

6.3 Modalités techniques spécifiques aux Web Services de l'Annuaire Santé

6.3.1 Sécurisation des échanges

EX_WSA_5010  
L'authentification mutuelle du Connecteur MSSanté avec le serveur de l'Annuaire Santé constitue un prérequis transverse à l'appel de tout Web Service d'interfaçage avec l'Annuaire Santé (ces fonctions sont définies dans les chapitres suivants de ce document).

Le certificat logiciel d'authentification de l'Opérateur MSSanté est aussi utilisé pour l'authentification TLS mutuelle vers l'Annuaire Santé.

Le contrôle d'accès est réalisé par rapport au DN du certificat d'authentification utilisé par le système initiateur. Pour qu'un système soit autorisé à utiliser les Web Services de l'Annuaire Santé, le DN du certificat serveur utilisé doit être référencé dans la liste blanche des domaines autorisés.

EX_WSA_5020  
Cette authentification mutuelle permet d'authentifier la structure d'activité à l'origine de l'appel du Web Service, mais pas l'utilisateur (humain ou machine) à l'initiative de l'action métier. Par conséquent, celui-ci doit être authentifié localement (au sein de la structure d'exercice dans le cas des Opérateurs de type « producteurs de soins », ou sur le service de messagerie dans le cas d'autres types d'Opérateurs), conformément aux exigences légales (CPS ou dispositifs équivalents).

6.3.2 Web Services de l'Annuaire Santé en SOAP

6.3.2.1 Encodage et espace de nommage

EX_WSA_5030	
Les spécifications du **§6.3.2.1** concernant l'encodage et les espaces de nommage, pour les Web Services de l'Annuaire Santé en SOAP, doivent être respectées.	

L'encodage standard pour les documents XML est l'UTF8.

Les espaces de nommage des entités manipulées ont le format suivant :

https://ws.annuaire.mssante.fr/webservices/VERSION/ACTION/<Nom du WS>

« VERSION » : correspond à la version des Web Services (1011 pour la version courante)

« ACTION » : Alimentation ou CR

« NOM DU WS » :

NOM DU WS	DESCRIPTION
WSALIMENTATIONMSS	Web Service d'alimentation des comptes MSSanté d'un ou plusieurs domaines de messagerie
WSCRALIMENTATIONMSS	Web Service de récupération du compte-rendu de chargement des données de l'Opérateur dans l'Annuaire Santé

Tableau 3 : Liste des Web Services de l'Annuaire Santé en SOAP

Les types de données utilisés pour les représentations des entités de type terminologie de référence sont ceux définis par le standard du schéma XML (http://www.w3.org/TR/xmlschema-2/).

Pour qualifier les types de données, le préfixe « xsd » est utilisé pour distinguer les données standards. Il est déclaré ainsi :

xmlns:xsd="http://www.w3.org/2001/XMLSchema"

- Pour les types primitifs : xsd:decimal, xsd:date, xsd:time, xsd:dateTime, xsd:base64Binary, xsd:boolean ;
- Pour les types dérivés : xsd:token, xsd :positiveInteger, xsd:nonNegativeInteger.

Les types de données spécifiques sont déclarés comme suit :

xmlns:mssante="http://annuaire.mssante.fr/webservices/commun"
xmlns:mssanteEntete="http://annuaire.mssante.fr/webservices/commun/entete"

6.3.2.2 Sécurité et intégrité

EX_WSA_5040

Les spécifications du **§6.3.2.2** concernant la sécurité et l'intégrité, pour les Web Services de l'Annuaire Santé en SOAP, doivent être respectées.

La sécurité des échanges avec l'Annuaire Santé comporte plusieurs niveaux :

- Le transport ;
- La non répudiation des messages ;
- La validation des données.

Pour être conforme au CI-SIS, un système émetteur d'une demande d'utilisation des Web Services doit s'appuyer sur un certificat serveur.

Les échanges se font sur le protocole HTTP 1.1 encapsulé dans une connexion sécurisée TLS. La version TLS minimale admise est la 1.0.

Les exigences de sécurité et d'intégrité sont détaillées dans le document [CI-TR-CLI-LRD].

Principe d'identification et d'authentification

Seul le mode d'authentification indirecte est utilisé pour les Web Services de l'Annuaire Santé en SOAP. Pour en savoir plus sur les modes d'authentification, voir les documents [CI-TR-CLI-LRD].

L'élément fonctionnel qui est récupéré afin d'effectuer l'authentification est le certificat serveur utilisé par le système initiateur.

Le contrôle d'accès est réalisé par rapport au DN du certificat d'authentification utilisé par le système initiateur. Pour qu'un système soit autorisé à utiliser les Web Services de l'Annuaire Santé, le DN du certificat serveur doit être référencé dans la liste blanche des domaines autorisés.

Le schéma ci-dessous présente le diagramme de séquences d'identification et d'authentification d'un utilisateur à partir du jeton VIHF.

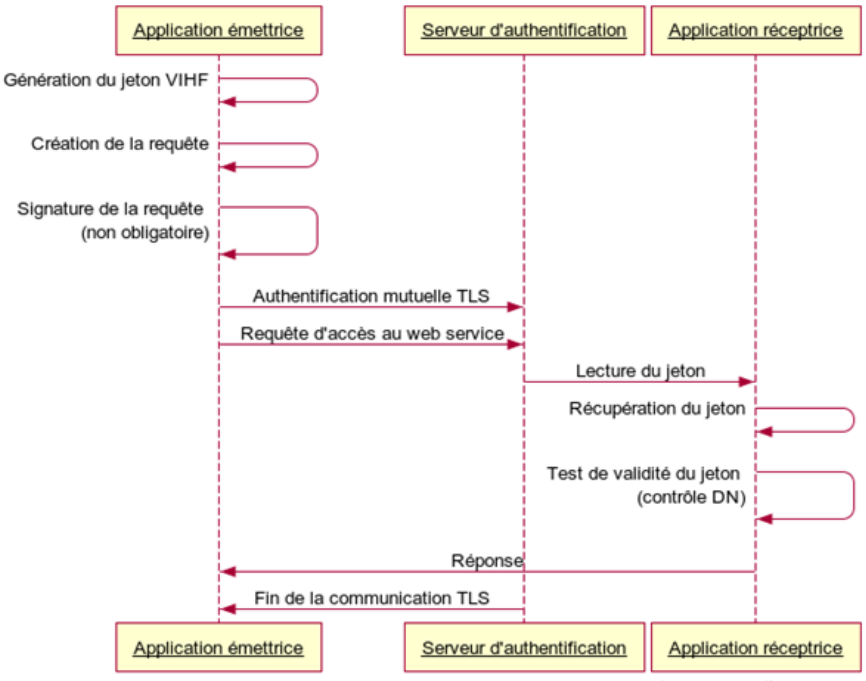


Figure 23 : Principe d'identification et d'authentification

Pour chaque appel d'un Web Service exposé par l'Annuaire Santé la cinématique est la suivante :

- Établissement d'une session TLS avec authentification mutuelle entre le serveur de l'Annuaire Santé et le système initiateur de la demande d'utilisation d'un Web Service ; les certificats utilisés sont :
  - Le certificat du système initiateur (avec DN référencé dans la liste blanche) ;
  - Le certificat serveur de l'Annuaire Santé ;
- Présentation du jeton VIHF (qui intègre le certificat d'authentification) ;
- Récupération du DN du certificat utilisé ;
- Contrôle de sécurité effectué par le serveur de l'Annuaire Santé par rapport à la liste blanche des domaines autorisés ;
- Réponse de l'Annuaire Santé par rapport à l'état du traitement ;
- Fin de la session TLS.

6.3.2.3 Description des échanges

Les messages s'appuient sur les descriptions détaillées dans le CI-SIS ainsi que sur l'utilisation du protocole SOAP.

6.3.2.3.1 Principe d'échanges

Les échanges via les Web Services d'alimentation des comptes MSSanté de personnes physiques et de personnes morales sont de type requête/réponse, donc synchrones.

Les WS d'alimentation sont toutefois qualifiés « d'asynchrone » dans la mesure où le traitement d'alimentation effectif n'est pas réalisé directement à la réception du message : l'utilisateur reçoit en réponse un ticket qu'il doit ensuite utiliser pour interroger le Web Service de suivi de l'avancement de l'alimentation (ou « Web Service de rapport d'alimentation »).

6.3.2.3.2 Versionning des Web Services

Le versionning est porté par l'URL d'invocation du Web Service. Chaque version est considérée comme un service différent à part entière.

Chaque service est associé à un namespace différent, portant le numéro de version.

Exemple : https://ws.annuaire.mssante.fr/webservices/V1011/Alimentation/WSALIMENTATIONMSS.

6.3.2.3.3 Principe de construction des messages

EX_WSA_5050

Les spécifications du **§ 6.3.2.3.3** (et sous-chapitres) concernant la construction des messages, pour les Web Services de l'Annuaire Santé en SOAP, doivent être respectées.

Chaque message est constitué d'une `Envelope` (Enveloppe) qui contient :

- un élément `Header` (en-tête) et
- un élément `Body` (corps).

6.3.2.3.3.1 *L'enveloppe constitue la racine du document XML et spécifie le namespace SOAP-ENV http://schemas.xmlsoap.org/soap/envelope/En-tête du message*

Dans le cas des SIS français, l'élément `Header` (en-tête) du message SOAP est obligatoire et aucun nœud intermédiaire n'est prévu entre système initiateur et système cible.

Dans le cadre de l'Annuaire Santé, l'élément `Header` du message contient :

- l'extension **WS-Adressing** qui étend les spécifications du protocole SOAP 1.2 et qui permet d'indiquer le destinataire du message (élément `<To>`), l'identifiant du message (élément `<MessageID>`), l'action à réaliser (élément `<Action>`) et l'adresse à laquelle le message de réponse doit être envoyé (élément `<ReplyTo>`). Ces éléments sont obligatoires.
- le **jeton VIHF** qui permet d'identifier le système initiateur.

Remarque : le modèle de l'en-tête « ENTETE » est identique pour tous les Web Services SOAP.

Entrée WS-Addressing

Le paramètre est actif dans le message SOAP avec la syntaxe suivante :

```
<wsaw:UsingAddressing wsdl:required="true" />
```

ATTRIBUT	DEFINITION	REQUIS	TYPE
ACTION	Action à réaliser sur le message	Oui	X(I)
TO	Destinataire du message	Oui	X(I)
MESSAGEID	Identifiant du message	Oui	X(I)
REPLYTO	Adresse à laquelle le message de réponse doit être envoyé	Oui	X(I)
FAULTO	Identité du consommateur	Oui	X(1024)

Tableau 4 : Eléments du WS-Addressing

Contenu du jeton VIHF

Le modèle VIHF impose l'utilisation du jeton de sécurité SAML 2.0.

Le jeton VIHF est transmis à chaque requête car il contient l'identité de l'utilisateur et les éléments nécessaires à la détermination des droits d'accès.

Le tableau suivant présente les champs présents dans le jeton VIHF avec leur valorisation. Ce tableau complète les spécifications d'utilisation et de format définies dans le document de référence [CI-TR-CLI-LRD].

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
CHAMPS STANDARDS				
//Assertion/@xmlns:saml2	*namespace XML SAML*	Oui	Alpha numérique	**Constante** : "urn:oasis:names:tc:SAML:2.0:assertion"
//Assertion/@Version	*Version utilisée*	Oui	Alpha numérique	**Constante** : "2.0"
//Assertion/@ID	*Identifiant unique de l'assertion*	Oui	Alpha numérique	Id de l'assertion
//Assertion/@IssueInstant	*Date et heure d'émission de l'assertion SAML*	Oui	xs: dateTime	issueInstant (temps Opérateur) < notBefore (temps Opérateur) < now (temps de reception de la requête par l'Annuaire Santé)) < NotOnOrAfter (issueInstant (temps Opérateur) + 1 heure)
//Assertion/Issuer	*Identité de l'émetteur contenue dans le certificat.* *(DN)*	Oui	DN (Distinguished Name)	DN du certificat de l'Opérateur qui a émis l'assertion. Si le jeton est signé, prendre le DN présent dans le certificat X509 de signature, sinon prendre le DN issu du certificat X.509 d'authentification ayant initié la connexion TLS. **Cet attribut est utilisé pour l'authentification de l'utilisateur.**
//Assertion/Issuer/@Format	*Type de valeur utilisée pour renseigner le champ Issuer (X509)*	Oui	Alpha numérique	**Constante** : "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
//Assertion/ds:Signature	*Emplacement réservé à la signature*	Oui pour les jetons signés	Alpha numérique	Eléments de la signature
//Assertion/Subject/NameID	*L'identifiant de l'utilisateur final envoyé par le système initiateur*	Oui	Alpha numérique	**En authentification indirecte** (authent serveur) : information déclarative - pas de contrôle.
//Assertion/AuthnStatement/AuthnContext/AuthnContextClassRef	*La méthode d'authentification de l'utilisateur*	Oui	Alpha numérique	**En authentification indirecte**, la valeur est laissée au choix de l'émetteur de l'assertion dès lors qu'elle est sélectionnée dans le document http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf
//Assertion/AuthnStatement/@AuthnInstant	*La date et l'heure exprimée en UTC à laquelle l'authentification a été réalisée par le système initiateur*	Oui	xs: dateTime	Date/heure d'authentification SI

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
//Assertion/Conditions/AudienceRestriction	*Plusieurs champs Audience qui contiennent chacun un URI qui référence la PSSI du système initiateur applicable pour traiter l'assertion*	Non	OID	Présent si une PSSI est définie
//Assertion/Conditions/@NotBefore	*La date et l'heure UTC de début de validité de l'assertion*	Oui	xs: dateTime	issueInstant (temps Opérateur) < notBefore (temps Opérateur) < now (temps de reception de la requête par l'Annuaire Santé)) < NotOnOrAfter (issueInstant (temps Opérateur) + 1 heure)
//Assertion/Conditions/@NotOnOrAfter	*La date et l'heure UTC de fin de validité de l'assertion*	Oui	xs: dateTime	issueInstant (temps Opérateur) < notBefore (temps Opérateur) < now (temps de reception de la requête par l'Annuaire Santé)) < NotOnOrAfter (issueInstant (temps Opérateur) + 1 heure)
CHAMPS COMPLEMENTAIRES - SITUES DANS LA BALISE <SAML:ATTRIBUTESTATEMENT> DU JETON SAML				
VIHF_Version	*Version du VIHF utilisée*	Oui	Numérique	**Constante :** "2.0"
urn:oasis:names:tc:xacml:2.0:subject:role	*Rôle fonctionnel de l'utilisateur (profession), qui peut être multi-valeur*	Oui	Type de donnée CE d'HL7 v3	Les règles de valorisation sont détaillées au § 4.3.1.5.3.2 du Volet Transport Synchrone (du CI-SIS)
Secteur_Activite	*Secteur d'activité dans lequel exerce l'utilisateur*	Non	OID	**code** : code du secteur d'activité **codeSystem**: "1.2.250.1.71.4.2.4" **codeSystemName** : optionnel **displayName :** optionnel Attribut non significatif dans le contexte MSSanté
urn:oasis:names:tc:xacml:2.0:resource:resource-id	*Identifiant du patient concerné par la requête*	Non	CX de HL7 v2.5.	Vide (car non significatif dans le contexte MSSanté)
Ressource_URN	*Ressource visée par l'utilisateur.*	Oui	URN	**Constante:** "`urn:MSSANTE`"
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	*Indique le mode d'accès demandé par l'utilisateur*	Oui	CE d'HL7 v3	`code="normal" codeSystem="1.2.250.1.213.1.1.4.248" codeSystemName="modes accès VIHF 1.0" displayName="Accès normal"` car non significatif dans le contexte MSSanté.
Mode_Acces_Raison	*Explication de la raison de l'usage du bris de glace.*	Non	Alpha numérique	Vide (car non significatif dans le contexte MSSanté)

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
urn:oasis:names:tc:xspa:1.0:subject:subject-id	*Identité de l'utilisateur*	Oui	Alpha numérique	Identification explicite de l'utilisateur (ex : nom, prénom, service au sein d'un établissement…) ou identification explicite de la machine (ex. nom du logiciel, nom du modèle, service au sein d'un établissement…).
Identifiant_Structure	*Identifiant de L'établissement de santé depuis lequel la requête a été émise*	Oui	Alpha Numérique	L'identifiant national de la structure « **Struct_IdNat »**
LPS_Nom	*Nom du logiciel utilisé*	Oui	Alpha numérique	Champ technique non vérifié dans ce contexte de requête par un Opérateur.
LPS_Version	*Version du logiciel utilisé*	Oui	Alpha numérique	Champ technique non vérifié dans ce contexte de requête par un Opérateur.
LPS_ID	*Numéro de série ou identifiant de l'installation du logiciel*	Oui	Alpha numérique	Champ technique non vérifié dans ce contexte de requête par un Opérateur.
PROFIL_UTILISATEUR	*Le profil de l'utilisateur*	Oui	OID	`code="OPER" codeSystem="1.2.250.1.213.1.9.1.1" codeSystemName="R84" displayName="Opérateur MSSanté"`
PROFIL_UTILISATEUR_PERIMETRE	*Le contexte métier ou périmètre de l'utilisateur*	Non	OID	Vide (car non significatif dans le contexte MSSanté)
VIHF_PROFIL	*Le profil VIHF*	Oui	OID	`code="profil_annuaire_PS" codeSystem="1.2.250.1.213.1.1.4.312" codeSystemName="profil VIHF" displayName="Profil pour annuaire de professionnels de santé du VIHF 2.0"`

Tableau 5 : Descriptif des attributs du jeton SAML 2.0

L'authentification de l'émetteur se fera à partir des attributs `Issuer`.

Exemple d'en-tête (avec le WS-Adressing et le jeton VIHF)

Pour l'Annuaire Santé (authentification indirecte).

```
-----------------------------------------------------------------------
ws-adressing
-----------------------------------------------------------------------

<soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <wsa:Action>http://annuaire.mssante.fr/webservices/V1011/alimentation/WSAlimentat
ionMSS/alimentationMSS</wsa:Action>
  <wsa:MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:f0df39db-d564-
412d-b29e-37f0555b2a94</wsa:MessageID>
  <wsa:To
xmlns="http://www.w3.org/2005/08/addressing">https://ws.annuaire.mssante.fr/webserv
ices/V1011/Alimentation/WSALIMENTATIONMSS?wsdl</wsa:To>
    <wsa:ReplyTo xmlns="http://www.w3.org/2005/08/addressing ">
     <Address>http://www.w3.org/2005/08/addressing/anonymous</Address>
   </wsa:ReplyTo>

   <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd">

-----------------------------------------------------------------------
VIHF
-----------------------------------------------------------------------

Champs standards du jeton SAML :

     <saml2:Assertion xmlns:hl7="urn:hl7-org:v3"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
ID="8e2c8d40-0624-422a-9666-bf1e3c6b2153"
IssueInstant="2015-02-03T13:20:12Z"
Version="2.0">
       <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:X509SubjectName"> CN=[CN du certificat],OU=318751275100020,O=AGENCE DES
SYSTEMES D'INFORMATION PARTAG,ST=Paris (75),C=FR </saml2:Issuer>
       <saml2:Subject>
         <saml2:NameID>[CN du certificat]</saml2:NameID>
       </saml2:Subject>
       <saml2:Conditions NotBefore="2015-02-03T13:20:12Z" NotOnOrAfter="2015-02-
03T14:20:11Z"></saml2:Conditions>
       <saml2:AuthnStatement AuthnInstant="2015-02-03T13:20:12Z ">
         <saml2:AuthnContext>
           <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Passw
ord</saml2:AuthnContextClassRef>
         </saml2:AuthnContext>

Champs complémentaires du jeton SAML :

       </saml2:AuthnStatement>
       <saml2:AttributeStatement>
         <saml2:Attribute Name="VIHF_Version">
           <saml2:AttributeValue>2.0</saml2:AttributeValue>
         </saml2:Attribute>
         <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role"/>
         <saml2:Attribute Name="Secteur_Activite">
           <saml2:AttributeValue>SA07^1.2.250.1.71.4.2.4</saml2:AttributeValue>
         </saml2:Attribute>
         <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
           <saml2:AttributeValue/>
         </saml2:Attribute>
         <saml2:Attribute Name="Ressource_URN">
           <saml2:AttributeValue>urn:MSSANTE</saml2:AttributeValue>
         </saml2:Attribute>
```

```
          </saml2:Attribute>
          <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
            <saml2:AttributeValue>
              <PurposeOfUse xmlns="urn:hl7-org:v3" xmlns:xsi="urn:hl7-org:v3"
hl7:code="normal" hl7:codeSystem="1.2.250.1.213.1.1.4.248"
hl7:codeSystemName="modes accès VIHF 1.0" hl7:displayName="Accès normal"
xsi:type="CE"/>
            </saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
            <saml2:AttributeValue>[RAISON SOCIALE DE LA
STRUCTURE]</saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute Name="Identifiant_Structure">
            <saml2:AttributeValue>[ID NAT DE LA STRUCTURE]</saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute Name="LPS_Nom">
            <saml2:AttributeValue>Nom-du-LPS</saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute Name="LPS_Version">
            <saml2:AttributeValue>version-du-LPS</saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute Name="LPS_ID">
            <saml2:AttributeValue>ID-LPS</saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute Name="Profil_Utilisateur">
            <saml2:AttributeValue>
              <Profil_Utilisateur xmlns="urn:hl7-org:v3" xmlns:xsi="urn:hl7-org:v3"
hl7:code="OPER" hl7:codeSystem="1.2.250.1.213.1.9.1.1" hl7:codeSystemName="R84"
hl7:displayName="Opérateur MSSanté" xsi:type="CE"/>
            </saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute Name="VIHF_Profil">
            <saml2:AttributeValue>
              <VIHF_Profil xmlns="urn:hl7-org:v3" xmlns:xsi="urn:hl7-org:v3"
hl7:code="profil_annuaire_PS" hl7:codeSystem="1.2.250.1.213.1.1.4.312"
hl7:codeSystemName="profil VIHF" hl7:displayName="Profil pour annuaire de
professionnels de santé du VIHF 2.0" xsi:type="CE"/>
            </saml2:AttributeValue>
          </saml2:Attribute>
        </saml2:AttributeStatement>
      </saml2:Assertion>

   </wsse:Security>
</soap:Header>
```

Figure 24 : Exemple de jeton VIHF pour l'Annuaire Santé (authentification indirecte)

6.3.2.3.3.2 Corps du message

Le corps du message `BODY` véhicule un ensemble d'éléments composés chacun d'un espace de noms avec des attributs portant les données métiers.

Généralement, le corps du message contient un élément `FAULT` qui permet éventuellement de renvoyer vers l'émetteur le type d'erreur intervenue lors du traitement du message par le destinataire.

6.3.2.3.3.3 Description des ressources terminologiques

Les ressources terminologiques utilisées dans les échanges sont gérées dans le NOS (Nomenclatures des Objets de Santé).

Ce sont des concepts avec une structuration des valeurs codées conformément à la description donnée au paragraphe 3.5.7.3 « Types de données "CS", "CV", "CE", "CD" » du document [CI-STRU-ENTETE].

Pour rappel la structuration d'une ressource terminologique est la suivante :

- `code` (cs) : valeur du code du concept ;
- `codeSystem` (uid): OID de la table de la terminologie de référence source ;
- `codeSystemName` (st) : nom lisible de la terminologie source qui correspond à l'information "Code Table" ;
- `codeSystemVersion` (st): version de la terminologie source ;
- `displayName` (st): libellé court associé au code dans la terminologie source qui correspond au libellé de la table ;
- `originalText` (ED) : texte ou phrase utilisé comme base du codage.

Le schéma ci-dessous montre, pour exemple, la structure de la terminologie de référence type d'identifiant personne physique :

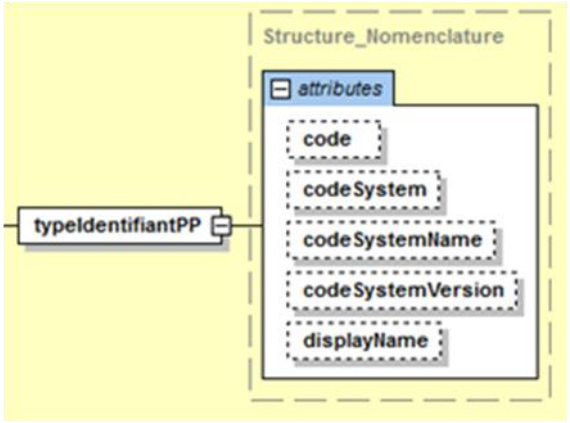


Figure 25 : Structure de la terminologie de référence type d'identifiant d'une personne physique

Remarque : aucune valeur n'est transmise pour le CodeSystemVersion.

Les terminologies de référence ([NOS-RES-TERMI]) utilisées dans le cadre de MSSanté sont disponibles sur https://esante.gouv.fr/interoperabilite/mos-nos.

Les terminologies de référence utilisées dans le cadre de MSSanté sont les suivantes :

Table	Nom (code) de TR CodeSystemName	Nom de la table
Type d'Identifiant National de la Personne Morale	G07	RNR_G07.tab
Type d'Identifiant National de la personne physique	G08	RNR_G08.tab
Profession	G15	RNR_G15.tab
Civilité d'exercice	R11	RNR_R11.tab
Code Commune	R13	RNR_R13.tab
Pays	R20	RNR_R20.tab
Type de voie	R35	RNR_R35.tab
Catégorie de profession	R37	RNR_R37.tab
Spécialité Compétences exclusives Qualification PAC	R38 R40 R44	RNR_R38.tab RNR_R40.tab RNR_R44.tab
Profil_VIHF	Profil VIHF	RNR_Profil_VIHF.tab
Profil d'accès à l'annuaire MSSanté	R84	RNR_R84.tab

Tableau 6 : Terminologies de référence utilisées dans le cadre de MSSanté

6.3.2.3.4 Gestion des erreurs

EX_WSA_5060


Les spécifications du **§ 6.3.2.3.4** (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'Annuaire Santé en SOAP, doivent être respectées.

6.3.2.3.4.1 Réponses standards en cas d'erreur

Pour chaque service, une « réponse with failure » renvoie une `SOAP Fault` à l'appelant en cas d'exception.

```
<soap:Fault>
    <soap:Code>
      <soap:Value>soap:Receiver</soap:Value>
      <soap:Subcode>
        <soap:Value>soap:code erreur</soap:Value>
      </soap:Subcode>
    </soap:Code>
    <soap:Reason>
      <soap:Text xml:lang="fr">message</soap:Text>
    </soap:Reason>
</soap:Fault>
```

Figure 26 : Exemple de SOAP Fault exception

Les messages d'erreurs de la couche technique et d'échange sont définis au **§ 9.**7.1 « Codes d'erreurs pour les Web Services de l'Annuaire Santé en SOAP - couche technique et d'échange ».

6.3.2.3.4.2 Erreur d'authentification

Si le processus d'authentification se déroule normalement alors, le service s'exécute comme prévu.

Si une erreur se produit dans ce processus, alors une erreur `SOAP Fault` est retournée avec les codes d'erreur.

6.3.3 Web Services de l'Annuaire Santé en REST

6.3.3.1 Encodage et espace de nommage

EX_WSA_5070
Les spécifications du **§ 6.3.3.1** concernant l'encodage et les espaces de nommage, pour les Web Services de l'Annuaire Santé en REST, doivent être respectées.

Les URIs doivent avoir la forme suivante :

https://<host>/<silo>/<version>/<ressource>[?<param_N>=<val_N>]

- En bleu la 1ère partie du chemin : obligatoire quelle que soit la ressource manipulée et la méthode HTTP utilisée ;
- En vert les paramètres d'URL

La réponse à une opération réussie a le code de statut HTTP suivant :

STATUT	CODE	DESCRIPTION
200	OK	Requête effectuée avec succès

Tableau 7 : Codes de statuts HTTP pour les Web Services REST

6.3.3.2 Sécurité et intégrité

EX_WSA_5080
Les spécifications du **§ 6.3.3.2** concernant la sécurité et l'intégrité, pour les Web Services de l'Annuaire Santé en REST, doivent être respectées.

La sécurité des échanges avec l'Annuaire Santé comporte plusieurs niveaux :

- Le transport ;
- La non-répudiation des messages ;
- La validation des données.

Pour être conforme, un système émetteur d'une demande d'utilisation des Web Services doit s'appuyer sur un certificat serveur.

Les échanges se font sur le protocole HTTP 1.1 encapsulé dans une connexion sécurisée TLS. La version TLS minimale admise est la 1.0.

Principe d'identification et d'authentification

Seul le mode d'authentification indirecte est utilisé pour les Web Services de l'Annuaire Santé en REST.

Pour en savoir plus sur les modes d'authentification, voir les documents [CI-TR-CLI-LRD].

L'élément fonctionnel qui est récupéré afin d'effectuer l'authentification est le certificat serveur utilisé par le système initiateur.

Le contrôle d'accès est réalisé par rapport au DN du certificat d'authentification utilisé par le système initiateur. Pour qu'un système soit autorisé à utiliser les Web Services REST de l'annuaire Santé, le DN du certificat serveur doit être référencé dans la liste blanche des domaines autorisés.

Remarque : contrairement aux web services SOAP, les web services REST ne reposent pas sur la fourniture d'un jeton VIHF ; l'authentification ne se fait qu'à travers le certificat utilisateur.

Pour chaque appel d'un Web Service exposé par l'Annuaire Santé la cinématique est la suivante :

- Etablissement d'une session TLS avec authentification mutuelle entre l'Annuaire Santé et le système initiateur de la demande d'utilisation d'un Web Service ; les certificats utilisés sont :
  - Le certificat du système initiateur (avec DN référencé dans la liste blanche des domaines autorisés) ;
  - Le certificat serveur de l'Annuaire Santé ;
- Présentation du certificat d'authentification ;
- Récupération du DN du certificat utilisé ;
- Contrôle de sécurité effectué par l'Annuaire Santé par rapport à la liste blanche des domaines autorisés ;
- Réponse de l'Annuaire Santé par rapport à l'état du traitement ;
- Fin de la session TLS.

6.3.3.3 Description des échanges

6.3.3.3.1 Principes d'échanges

EX_WSA_5090  
Les spécifications du **§ 6.3.3.3.1** (et sous-chapitres) concernant les échanges, pour les Web Services de l'Annuaire Santé en REST, doivent être respectées.

6.3.3.3.2 Récupération d'une ressource unique

Requête

Un Web Service REST permettant la récupération d'une ressource unique doit implémenter la méthode `GET` de la manière suivante :

https://<host>/<silo>/<version>/<ressource>[?<param_N>=<val_N>]

Le body de la requête est vide.

Réponse

En cas de succès, la réponse est la suivante :

STATUT	CODE	DESCRIPTION	ENTÊTE	BODY
200	OK	La ressource demandée existe		1 retour contenant la ressource

Tableau 8 : Réponse du Web Service REST de récupération d'une ressource unique

En cas d'échec de l'opération, les codes d'erreur définis au **§ 9.7.2** « Codes d'erreurs pour les Web Services de l'Annuaire Santé en REST - couche technique et d'échange » doivent être utilisés.

6.3.3.3.3 Gestion des erreurs

EX_WSA_5100

Les spécifications du **§ 6.3.3.3.3** (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'Annuaire Santé en REST, doivent être respectées.

Les messages d'erreur de la couche technique et d'échange sont définis au **§ 9.7.2** « Codes d'erreurs pour les Web Services de l'Annuaire Santé en REST - couche technique et d'échange ».

Le message d'erreur est retourné dans le body de la réponse, un document XML ayant la structure suivante :

ELEMENT	DESCRIPTION	TYPE
Error	Racine	<root>
Code	Code d'erreur du Web Service	xsd:string
Message	Message d'erreur	xsd:string

Tableau 9 : Structure du message d'erreur des Web Services REST

6.4 Publication de BAL MSSanté dans l'Annuaire Santé

6.4.1 Description fonctionnelle

EX_PBA_5010

Un Opérateur professionnels MSSanté doit obligatoirement implémenter la transaction TM1.1.1P afin d'être en mesure de gérer le cycle de vie des comptes de messagerie des utilisateurs du domaine MSSanté auquel il est rattaché. Cela consiste à être en capacité de :

- Publier dans l'Annuaire Santé les BAL créées sur le domaine pour les nouveaux utilisateurs MSSanté (par exemple : à l'occasion de leur arrivée dans l'organisation à laquelle est rattaché le domaine de messagerie) ;
- Modifier dans l'Annuaire Santé les données des BAL utilisateurs MSSanté sur le domaine de l'Opérateur (par exemple : à l'occasion d'un changement de service au sein de l'organisation) ;
- Supprimer de l'Annuaire Santé les BAL utilisateurs MSSanté suspendues ou supprimées sur le domaine de l'Opérateur (par exemple : à l'occasion de leur départ de l'organisation à laquelle est rattaché le domaine de messagerie) ;
- Supprimer la totalité des BAL d'un domaine lorsque celui-ci est retiré de la liste blanche.

L'ensemble des boites aux lettres ouvertes dans l'Espace de Confiance doivent être publiées dans l'Annuaire Santé à l'exception des boites aux lettres de test et des BAL usagers.

EX_PBA_5030

L'Opérateur ne doit pas publier de BAL fonctionnelles de type « liste de diffusion » dans l'Annuaire Santé (toute adresse MSSanté doit correspondre à une et une seule BAL physique).

6.4.1.1 Type de FINESS à associer aux BAL pour la déclaration dans l'Annuaire Santé

Une BAL MSSanté, suivant son type, peut/doit être rattachée à une structure qui emploie les utilisateurs professionnels de cette BAL :

- Une BAL personnelle (rattachement structure recommandée, mais optionnelle) ;
- Une BAL organisationnelle ;
- Une BAL applicative ;

Pour que le rattachement à une structure soit possible, il est nécessaire qu'elle soit au préalable déclarée dans l'Annuaire Santé, via les processus de déclaration obligatoires mis en place par les autorités d'enregistrement (ordres, …).

Toutes les structures FINESS sont présentes dans l'Annuaire Santé. Cependant, les structures SIREN/SIRET des cabinets libéraux individuels ou de groupe ne sont généralement pas identifiées dans l'Annuaire Santé.

Pour des besoins de pilotage et de financement des structures sanitaires, médico-sociales ou sociales, il est nécessaire de disposer d'indicateurs d'usage MSSanté de l'Espace de Confiance à la maille la plus fine. La production de ces indicateurs est uniquement possible lorsque les BAL déclarées dans l'Annuaire Santé sont associées au FINESS Géographique du site auquel elles sont rattachées.

EX_PBA_5011


Un Opérateur professionnel MSSanté, qui est immatriculé au FINESS, doit associer un FINESS de type géographique à toutes ses BAL MSSanté déclarées dans l'Annuaire Santé. Le FINESS géographique associé est celui de la structure (site annexe) à laquelle appartient la BAL.

Sauf dans le cas où la BAL appartient à une structure (maison mère, siège social, …) doté d'un FINESS juridique et correspond à un usage mutualisé entre plusieurs structures géographiques (sites annexes) : la BAL peut être associée au FINESS juridique du site de rattachement.

EX_PBA_5012

Un Opérateur professionnels MSSanté, non immatriculé au FINESS, doit permettre aux utilisateurs finaux de lier un FINESS géographique à toutes BAL MSSanté déclarées dans l'Annuaire Santé.

6.4.1.2 Présence des Utilisateurs professionnel en « Liste rouge »

Si l'Utilisateur professionnel choisit de mettre sa BAL en « liste rouge », cette dernière ne sera pas affichée lors des recherches dans l'Annuaire Santé. Cela n'empêchera pas pour autant l'Utilisateur professionnel d'envoyer et de recevoir des messages via sa messagerie MSSanté, pour peu que ses interlocuteurs connaissent son adresse de messagerie.

Cette option s'applique également pour les BAL applicatives ou organisationnelles.

L'identité des Utilisateurs professionnel inscrits en liste rouge est communiquée à la Direction générale de la santé pour l'émission de messages d'alerte sanitaire. Les Utilisateurs professionnels sont informés et peuvent s'y opposer pour motif légitime.

EX_PBA_5040

L'Opérateur doit, par un moyen technique ou organisationnel, permettre à chacun des utilisateurs de son service d'indiquer explicitement s'il souhaite être inscrit en liste rouge.

Ce choix, non imposés par défaut, peut être mis en œuvre lors de la création de la BAL MSSanté via un mécanisme technique (case à cocher) ou organisationnel, et doit pouvoir être modifié à tout moment par l'utilisateur.

EX_PBA_5050

L'Opérateur doit mettre en œuvre les mécanismes techniques permettant de transmettre à l'Annuaire Santé le choix de l'utilisateur concernant son inscription en liste rouge.

EX_PBA_5140	
L'Opérateur doit s'assurer que les BAL MSSanté liées à son service de messagerie MSSanté suspendues ou supprimées ne soient plus publiées dans l'Annuaire Santé.	

EX_PBA_5150	
L'Opérateur doit veiller à ce que les informations de description des BAL liées à son service de messagerie MSSanté publiées dans l'Annuaire Santé soient fiables.	

EX_PBA_5230	
L'Opérateur ne doit pas publier dans l'Annuaire Santé les boites aux lettres de tests.	

6.4.1.3 BAL personnelles

Dans le cas des BAL rattachées à des personnes physiques, les données qui doivent être fournies par l'Opérateur professionnels à l'annuaire santé sont détaillées dans le **§6.4.2.3.3.1.**

EX_PBA_5090	
L'identifiant du titulaire d'une BAL personnelle MSSanté transmis par l'Opérateur lors de l'alimentation de l'Annuaire Santé doit impérativement être l'identifiant national (RPPS/ADELI) si le titulaire de la BAL en dispose. Pour le cas particulier des professionnels habilités ne disposant pas d'identifiant national, un identifiant interne (**en pratique : l'adresse de la BAL MSSanté attribuée à l'utilisateur**) à la structure d'activité pourra être transmis.	

Remarque : Le numéro RPPS ou ADELI peut être trouvé à l'aide de l'extraction décrite en TM2.1.4A ou sur le site annuaire.sante.fr

Les informations fournies par l'Opérateur viennent enrichir les informations d'identité de l'utilisateur déjà présentes dans l'Annuaire Santé (les données préchargées dans l'Annuaire Santé étant issues des données sources RPPS et ADELI fournies par les autorités d'enregistrement des professionnels de santé).

Il est possible de rattacher au numéro RPPS/ADELI d'un professionnel de santé à plusieurs BAL MSSanté.

EX_PBA_5100
L'Annuaire Santé peut identifier une erreur sur l'identifiant national du professionnel de santé transmis par l'Opérateur et en retour lui transmettre l'identifiant valide. L'Opérateur MSSanté doit le prendre en compte et le mettre à jour dans son service de messagerie.

Dans le cadre de la gestion du passage de ADELI vers RPPS, il sera possible pour un Opérateur MSSanté d'obtenir auprès des services concernés de l'ANS, un fichier de correspondance ADELI/RPPS afin de faciliter la mise à jour des informations des titulaires de BAL MSSanté de son domaine de messagerie.

6.4.1.3.1 Rattachement dans l'Annuaire Santé d'une BAL personnelle avec les situations d'exercice du professionnel habilité

La manière dont un Opérateur déclare une BAL dans l'Annuaire Santé a un impact sur la façon dont l'adresse de la BAL pourra être retrouvée lors d'une recherche dans l'Annuaire Santé.

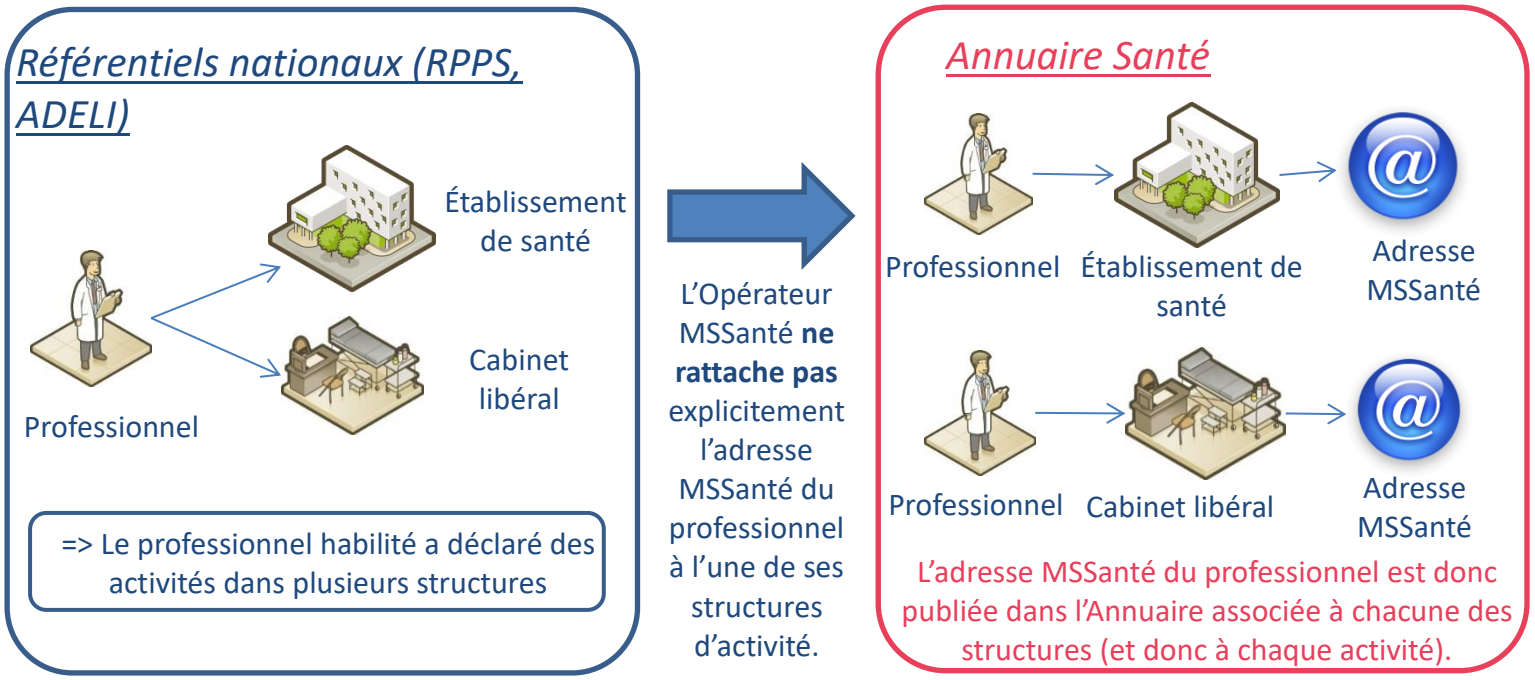


Figure 27 : Publication d'adresses MSSanté dans l'Annuaire Santé dans le cas où l'Opérateur MSSanté ne rattache pas explicitement l'adresse MSSanté du professionnel à l'une de ses structures d'activité

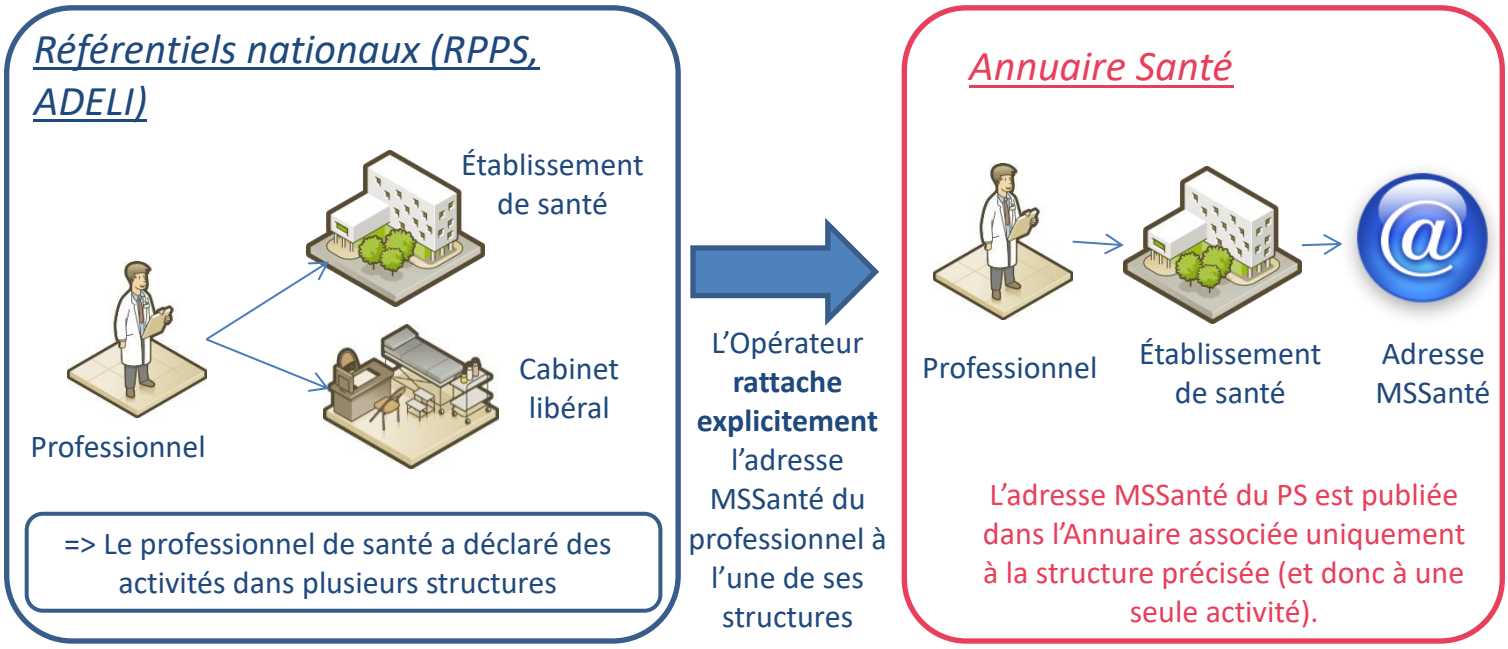


Figure 28 : Publication des adresses MSSanté dans l'Annuaire Santé dans le cas où l'Opérateur rattache explicitement l'adresse MSSanté du professionnel à l'une de ses structures d'activité.

Comme le montrent les figures ci-dessus, dans le cas où le professionnel habilité a déclaré des activités dans plusieurs structures, la publication de son adresse MSSanté peut apparaître de deux manières différentes dans l'Annuaire Santé :

- L'adresse MSSanté du professionnel habilité peut être publiée dans l'Annuaire associée à chacune de ses structures d'activité, si l'Opérateur ne rattache pas explicitement l'adresse MSSanté du professionnel habilité à l'une de ces structures.
- L'adresse MSSanté du professionnel habilité peut être publiée dans l'Annuaire Santé associée uniquement à une de ses structures d'activité si l'Opérateur rattache explicitement l'adresse MSSanté du professionnel habilité à cette structure.

Il appartient à l'Opérateur de choisir de manière cohérente le rattachement ou non des adresses MSSanté du professionnel habilité à une structure d'activité.

EX_PBA_5220

Dans le cas de BAL personnelles utilisées par des professionnels exerçant à titre salarié ou libéral dans des structures sanitaires et médico-sociales, l'Opérateur DOIT rattacher explicitement les BAL personnelles au numéro FINESS Géographique de la structure.

Cette exigence a pour but d'améliorer la publication dans l'Annuaire Santé en facilitant ainsi l'identification de la « bonne » adresse à utiliser pour les professionnels disposant de plusieurs adresses MSSanté et ayant un exercice mixte (salarié et libéral). Cela permet également de favoriser le pilotage du déploiement des BAL personnelles dites « hospitalières » ainsi que des BAL personnelles dites plutôt « de ville » (l'objectif est de considérer qu'une BAL personnelle est dite « de ville » dans la mesure où aucun numéro FINESS y est rattaché).

6.4.1.3.2 Cas particulier des professionnels habilités sans identifiant national RPPS ou ADELI

Dans le cas d'un professionnel habilité ne disposant pas de numéro d'identification national (en particulier professionnel de santé étranger), la certification de son identité est réalisée sous la responsabilité du directeur de la structure qui l'emploie. Le directeur de la structure est ainsi considéré comme une autorité d'enregistrement locale.

L'identifiant d'un professionnel habilité ne disposant pas d'identifiant national RPPS ou ADELI est son adresse de BAL MSSanté.

La création de cet identifiant local et l'enregistrement du professionnel au sein de l'Annuaire Santé ne l'exonèrent pas du respect des différentes obligations attachées à l'exercice de sa profession.

6.4.1.4 BAL organisationnelle d'une structure disposant d'un FINESS

Dans le cas des BAL organisationnelles, les données qui doivent être fournies par l'Opérateur sont détaillées dans le **§6.4.2.3.3.3**

La déclaration par un Opérateur d'une BAL MSSanté organisationnelle dans l'Annuaire Santé nécessite l'existence préalable d'un enregistrement correspondant à la structure d'activité de rattachement dans l'Annuaire Santé. Le rapprochement entre les données de l'Annuaire Santé et celles fournies par l'Opérateur est effectué à partir de l'identifiant de la structure.

6.4.1.5 BAL organisationnelle d'une structure ne disposant pas d'un FINESS

Dans le cas des BAL organisationnelles, les données qui doivent être fournies par l'Opérateur sont détaillées dans le **§6.4.2.3.3.4.**

6.4.1.6 BAL applicative d'une structure ne disposant pas d'un FINESS

Dans le cas des BAL applicatives, les données qui doivent être fournies par l'Opérateur sont détaillées dans le **§6.4.2.3.3.3.**

6.4.2 TM1.1.1P - Mise à jour des BAL dans l'Annuaire Santé en Web Services en mode global et récupération du compte–rendu d'alimentation

La transaction de mise à jour de l'Annuaire Santé en Web Service en mode « global » pour le domaine concerné (de type « annule et remplace ») nécessite une authentification par certificat logiciel de personne morale délivré par l'ANS.

E

EX_1.1.1_5010

Dans le cas où l'Opérateur implémente la transaction « TM1.1.1P – Web Service en mode global », il doit respecter les spécifications d'implémentation décrites dans le chapitre **§ 6.4.2** (et sous-chapitres).

Le Web Service en mode global permet de réaliser un chargement complet de toutes les BAL du ou des domaines de l'Opérateur dans l'Annuaire Santé.

Dans ce cas d'usage, l'Opérateur envoie à l'Annuaire Santé une liste exhaustive des BAL de son domaine MSSanté. Le traitement de ces informations entraîne dans l'Annuaire Santé :

1. Une suppression des comptes de messageries tels qu'ils étaient connus pour ce domaine ;
2. Un remplacement par les données courantes envoyées par le Web Service.

Dans ce mode de fonctionnement, l'Opérateur n'a pas à gérer le cycle de vie des BAL MSSanté au cas par cas : il lui suffit d'envoyer une extraction complète des BAL du domaine lorsque des mouvements d'ajouts, mises à jour ou suppressions se produisent dans l'annuaire interne de son domaine.

RE_1.1.1_5020

R

Il est recommandé que l'envoi des BAL soit effectué :

- Si au moins une modification (ajout, mise à jour, suppression) de compte est identifiée dans l'annuaire interne du domaine ;
- Pas plus d'une fois par jour ;
- Au moins une fois par semaine même si aucune modification n'a été apportée. Remarque : en effet, l'identifiant national de rattachement d'une personne disposant d'une BAL MSSanté peut ne plus être valide dans l'Annuaire Santé (exemple : professionnel de santé radié de l'ordre des médecins) ; Cette personne n'est donc plus habilitée à accéder à MSSanté. C'est à l'Opérateur MSSanté de traiter les codes retours de l'Annuaire Santé comme indiqué dans l'**EX_WSA_5060**.

6.4.2.1 Cinématique

La cinématique d'alimentation de l'Annuaire Santé avec les BAL gérées par l'Opérateur MSSanté est la suivante :

- [Opérateur] : appel au WS d'alimentation global pour dépôt du message d'alimentation dans un sas de stockage ;
- [Serveur national d'annuaire MSSanté] :
    - Identifie et authentifie l'Opérateur puis contrôle le respect du schéma XML attendu ;
    - Retourne à l'Opérateur un accusé de réception du flux, avec un numéro de ticket horodaté ou un message d'erreur ;

[Le serveur de l'Annuaire Santé traite en différé les messages d'alimentation dans leur ordre d'arrivée et génère le compte-rendu d'alimentation, avec les anomalies détectées, à destination de l'Opérateur MSSanté]

- [Opérateur] : récupère le rapport de chargement par appel à un Web Service de récupération du compte-rendu.

6.4.2.2 Description fonctionnelle

Le Web Service d'alimentation global permet à un Opérateur d'envoyer, en mode synchrone, un flux d'alimentation avec l'ensemble des BAL MSSanté d'un ou plusieurs domaines.

Cas d'utilisation	Utilisation du Web Service global d'alimentation
Résumé	Permettre à un système initiateur d'un Opérateur de charger dans le référentiel des identités la liste des BAL MSSanté d'un ou plusieurs domaines
Déclencheur	Invocation de l'URL correspondant au Web Service d'alimentation global exposé
Objectif	Réceptionner, en vue du chargement, le flux d'alimentation des BAL MSSanté d'un ou plusieurs domaines gérés par l'Opérateur
Fréquence d'utilisation	À chaque modification, pas plus d'une fois par jour ou une fois par semaine au minimum
Acteur principal	Opérateur MSSanté initiateur de la demande
Pré conditions	Le DN du certificat utilisé et le(s) domaine(s) qui font l'objet de l'alimentation sont référencés dans la liste blanche des domaines autorisés
Post conditions	Suite à l'exécution de ce Web Service un message d'alimentation est déposé dans le sas de stockage et une réponse avec un numéro de ticket (ou un code d'erreur) est renvoyée à l'Opérateur

Tableau 10 : Cas d'utilisation du Web Service global d'alimentation de l'Annuaire Santé

Scénario principal

Étapes	Activité	Scénario Alternatif
1	Un Opérateur qui souhaite mettre à jour la liste des BAL MSSanté qu'il gère invoque par l'intermédiaire d'un système initiateur le Web Service d'alimentation en établissant une session TLS avec authentification mutuelle. Il envoie un flux avec la liste des BAL MSSanté d'un ou plusieurs domaines, accompagné des données d'identification et d'authentification : DN du certificat d'authentification utilisé pour les échanges SMTP.	SA1 SA6 SA7
2	L'Annuaire Santé réceptionne le message et procède à son interprétation.	SA2
3	L'Annuaire Santé identifie l'utilisateur et effectue le contrôle d'accès par rapport à la liste blanche des domaines autorisés.	SA3 SA4
4	L'Annuaire Santé effectue un contrôle syntaxique du contenu du flux (contrôle du respect du schéma XML attendu).	SA2
5	L'Annuaire Santé traite la demande : • Génère un ticket horodaté qu'il attribue au flux ; • Dépose le fichier d'alimentation dans un sas de stockage en l'horodatant. Sans contrôle de cohérence des informations transmises ; le batch d'alimentation traitera les fichiers dans l'ordre de cet horodatage ; le nom du fichier d'alimentation contient le DN du certificat de l'Opérateur et la date de dépôt du fichier (*aaaammjjhhmmss)* ; • Envoie en réponse au système initiateur le numéro de ticket généré pour le suivi des demandes d'alimentation.	SA5

Tableau 11 : Scénario principal d'utilisation du Web service global

Scénarios alternatifs

Étapes	Activité
SA1 : Le service n'est pas disponible	
1	Il n'y a pas de message de réponse de la part de l'Annuaire Santé.
SA2 : Le message envoyé est mal formaté	
2, 4	L'Annuaire Santé envoie un message d'erreur sans traiter la demande d'alimentation (message WSMSS 12).
SA3 : Les informations d'identification et d'authentification sont insuffisantes	
3	Si les informations d'identification/authentification sont insuffisantes pour déterminer l'identité de l'utilisateur et le contrôle de droit d'accès, l'Annuaire Santé envoie un message d'erreur sans traiter la demande d'alimentation (message WSMSS 6).
SA4 : Le DN n'est pas référencé dans la liste blanche	
3	Si le domaine et/ou le DN ne sont pas référencés dans la liste blanche, l'Annuaire Santé envoie un message d'erreur sans traiter la demande (message WSMSS 6).
SA6 : Le certificat est révoqué	
3	Si le certificat est référencé dans la liste des certificats révoqués, l'Annuaire Santé envoie un message d'erreur sans traiter la demande (message : certificate_revoked).
SA7 : Le certificat n'est pas valide	
3	Si le certificat n'est pas valide (expiré), l'Annuaire Santé envoie un message d'erreur sans traiter la demande (message : 401: Authorization Required).
SA5 : Le message ne peut pas être déposé dans le SAS de stockage de l'Annuaire Santé	
5	Si un message ne peut pas être déposé dans le sas de stockage, l'Annuaire Santé envoie un message d'erreur sans traiter la demande (message WSMSS 15).

Tableau 12 : Scénarios alternatifs d'utilisation du Web service global

6.4.2.3 Principe de construction du flux d'alimentation de l'Annuaire Santé

La description WSDL et le schéma XSD du Web Service d'alimentation globale de l'Annuaire Santé (WSDL) associés correspondent respectivement aux documents de référence DR2 et DR3 définis au **§ 9.5.**

6.4.2.3.1 Présentation du flux d'alimentation – en entrée de l'Annuaire Santé

Le flux d'alimentation global est constitué de deux parties :

- **L'en-tête du message** qui contient des informations d'identification et d'authentification (voir **§ 6.3.2.3.3.1**) ;
- **Le corps du message** qui comporte un ou plusieurs messages d'alimentation par domaine. Chaque message d'alimentation par domaine comporte deux entrées :
  - Une entrée qui contient le nom de domaine à alimenter – `DOMAINE` ;
  - Une entrée qui contient l'ensemble des BAL MSSanté du domaine – `COMPTEMSS`.

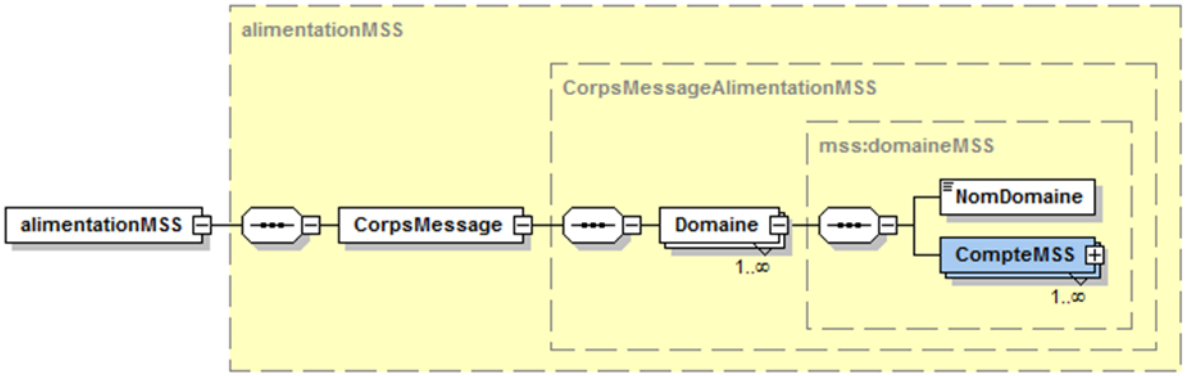


Figure 29 : Corps du message d'alimentation des comptes MSSanté d'un domaine

6.4.2.3.2 Structure DOMAINE

La structure du domaine des BAL est identique à la structure définie pour le nom du domaine dans la liste blanche des domaines autorisés.

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTRÔLE
Domaine	Domaine de messagerie des BAL MSSanté	Oui	X(255)		RG_CTR_000

Tableau 13 : Structure du domaine des BAL MSSanté

6.4.2.3.3 Structure COMPTESMSS

Les champs présents dans la structure (COMPTESMSS) varient beaucoup suivant le type de BAL, et aussi le type d'identifiant de personne physique Pour simplifier, la structure COMPTEMSS est décrite par type de BAL.

6.4.2.3.3.1 Structure COMPTESMSS d'une BAL personnelle avec identifiant national RPPS ou ADELI

La création d'une BAL personnelle rattachée à un identifiant national RPPS ou ADELI permet la réutilisation des données de l'annuaire RPPS ou ADELI. Certaines données n'ont donc pas besoin d'être transmises (Ex : profession…).

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTRÔLE
TypeBAL	PER pour BAL Personnelle	Oui	X(3)	Une BAL de type PER est rattachée à une personne physique.	RG_CTR_002 RG_CTR_003
AdresseBAL	Adresse unique de messagerie dans un domaine de messagerie MSSanté	Oui	X(256)	La RFC 5321 précise que le pattern d'une adresse de messagerie doit respecter la règle suivante : X(64)@Y(255) ; avec un maximum de **256** caractères au total pour X+@+Y.	RG_CTR_001 RG_CTR_004 RG_CTR_044 RG_CTR_046
TypeIdentifiantPP	Valeurs possibles : • 0 si identifiant ADELI • 8 si identifiant RPPS	Oui		Nomenclature : **CodeSystemName =** G08 **CodeSystem =** 1.2.250.1.71.1.2.15	RG_CTR_005 RG_CTR_006 RG_CTR_037
IdentifiantPP	Identifiant ADELI ou Identifiant RPPS ou Identifiant interne (adresse de la BAL)	Oui	ADELI :X(9) RPPS : X(11)		RG_CTR_007 RG_CTR_008 RG_CTR_035 RG_CTR_045
TypeIdentifiantPM	Type de structure à laquelle la BAL est associée. Valeurs possibles : • 1 si FINESS • 2 si SIREN • 3 si SIRET	Non		Nomenclature : TypeIdentifiantPM **CodeSystemName =** G07 **CodeSystem =** 1.2.250.1.71.1.2.14 Cet attribut est facultatif pour les BAL ayant un TypeIdentifiantPP = 0 ou 8 (ADELI/RPPS) mais il est possible de le fournir afin de pouvoir associer la BAL spécifiquement à une structure donnée lors des recherches sur l'annuaire.	RG_CTR_009 RG_CTR_011 RG_CTR_012 RG_CTR_015 RG_CTR_038 RG_CTR_039

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTRÔLE
IdentifiantPM	Numéro FINESS Géographique ou Numéro SIREN ou Numéro SIRET	Non	X(32)	Obligation de renseigner cet attribut lorsque la donnée est disponible afin de pouvoir associer la BAL spécifiquement à une structure donnée lors des recherches sur l'annuaire.	RG_CTR_013 RG_CTR_014 RG_CTR_016 RG_CTR_033 RG_CTR_034
NomExercice	Nom d'exercice de l'utilisateur (nom sous lequel il exerce)	Oui	X(80)		RG_CTR_019 RG_CTR_021
PrenomExercice	Prénom d'exercice de l'utilisateur (prénom sous lequel il exerce)	Oui	X(50)		RG_CTR_020 RG_CTR_021
Telephone	Téléphone (de type fixe ou mobile) lié à la BAL (PER, ORG ou APP)	Non	X(20)		
Dematerialisation	Indicateur d'acceptation de la dématérialisation. Valeurs possibles : • O – dématérialisation acceptée • N – dématérialisation refusée	Non	X(1)		
ListeRouge	Indicateur liste rouge Valeurs possibles : • O – BAL en liste rouge • N – la BAL peut être publiée	Oui	X(1)	Les BAL en liste rouge ne sont pas publiées par l'Annuaire Santé.	RG_CTR_032

Tableau 14 : Structure COMPTESMSS dans le cas de BAL personnelles avec identifiant national RPPS ou ADELI

6.4.2.3.3.2 Structure COMPTESMSS dans le cas particulier d'une BAL personnelle SANS identifiant national RPPS ou ADELI

Dans le cas particulier de la création d'une BAL personnelle pour un professionnel qui ne peut pas disposer d'identifiant national RPPS ou ADELI, il est nécessaire de fournir l'ensemble des attributs relatifs à la personne physique, puisqu'elle n'est pas préalablement présente dans l'Annuaire Santé.

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTRÔLE
TypeBAL	PER pour BAL Personnelle	Oui	X(3)	Une BAL de type PER est rattachée à une personne physique.	RG_CTR_002 RG_CTR_003
AdresseBAL	Adresse unique de messagerie dans un domaine de messagerie MSSanté	Oui	X(256)	La RFC 5321 précise que le pattern d'une adresse de messagerie doit respecter la règle suivante : X(64)@Y(255) ; avec un maximum de **256** caractères au total pour X+@+Y.	RG_CTR_001 RG_CTR_004 RG_CTR_044 RG_CTR_046
TypeIdentifiantPP	Valeurs : • 10 pour identifiant interne (adresse de la BAL)	Oui		Nomenclature : **CodeSystemName =** G08 **CodeSystem =** 1.2.250.1.71.1.2.15 L'utilisation de l'identifiant 10 doit faire l'object d'une approbation de l'ANS	RG_CTR_005 RG_CTR_006 RG_CTR_037
IdentifiantPP	Identifiant interne (adresse de la BAL)	Oui	Interne : X(256)	Dans le cas d'un identifiant interne, il s'agira de l'adresse de la BAL	RG_CTR_007 RG_CTR_008 RG_CTR_035 RG_CTR_045
TypeIdentifiantPM	Type de structure à laquelle la BAL est associée. Valeurs possibles : • 1 si FINESS • 2 si SIREN • 3 si SIRET	Oui		Nomenclature : TypeIdentifiantPM **CodeSystemName =** G07 **CodeSystem =** 1.2.250.1.71.1.2.14	RG_CTR_009 RG_CTR_011 RG_CTR_012 RG_CTR_015 RG_CTR_038 RG_CTR_039
IdentifiantPM	Numéro FINESS géographique ou	Oui	X(32)		RG_CTR_013 RG_CTR_014 RG_CTR_016

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTRÔLE
	Numéro SIREN ou Numéro SIRET				RG_CTR_033 RG_CTR_034
ServiceRattachement	Nom et description du service de rattachement de l'utilisateur dans l'organisation	Non	X(160)	Texte libre Cet attribut permet de renseigner le service de rattachement de l'utilisateur (PER) dans l'organisation.	RG_CTR_036
CiviliteExercice	Civilité de la situation d'exercice de l'utilisateur	Oui		Nomenclature : CiviliteExercice **CodeSystemName =** R11 **CodeSystem =** 1.2.250.1.213.1.6.1.11 Attribut renseigné uniquement si typeBAL = PER avec un identifiant interne. La civilité d'exercice ne concerne que les professions de médecin, pharmacien, chirurgien-dentiste et doit être : • Médecin : PR (Professeur) / MG (Médecin Général) / MC (Médecin chef) / DR (Docteur) • Pharmacien : PR (Professeur) / PC (Pharmacien Chef) / PG (Pharmacien Général) / DR (Docteur) • Chirurgien-dentiste : PR (Professeur) / DR (Docteur) En cas d'erreur sur la civilité d'exercice par rapport à la profession saisie, un code erreur **MSS017** sera remonté dans le rapport d'alimentation.	RG_CTR_017 RG_CTR_018 RG_CTR_040
NomExercice	Nom d'exercice de l'utilisateur (nom sous lequel il exerce)	Oui	X(80)	Attribut renseigné uniquement si typeBAL = PER.	RG_CTR_019 RG_CTR_021
PrenomExercice	Prénom d'exercice de l'utilisateur (prénom sous lequel il exerce)	Oui	X(50)	Attribut renseigné uniquement si typeBAL = PER.	RG_CTR_020 RG_CTR_021

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTRÔLE
CategorieProfessions	Catégorie de professions de l'utilisateur Exemple : • 01 pour les professionnels de santé • 06 pour des fonctions dans des expérimentations	Oui		**CodeSystem =** 1.2.250.1.213.1.6.1.3 En cas d'erreur, les codes erreurs **MSS022** et **MSS023** seront présents dans le rapport d'alimentation. Attribut renseigné uniquement si typeBAL = PER avec un identifiant interne.	RG_CTR_022 RG_CTR_023 RG_CTR_024 RG_CTR_041
Profession	Profession de l'utilisateur	Oui		**CodeSystem =** 1.2.250.1.71.1.2.7 En cas d'erreur, les codes erreurs **MSS024** à **MSS026,** selon la typologie d'erreur, seront présents dans le rapport d'alimentation. Attribut renseigné uniquement si typeBAL = PER avec un identifiant interne.	RG_CTR_025 RG_CTR_026 RG_CTR_042
Specialite	Spécialité de l'utilisateur *Cet attribut correspond à la spécialité ordinale et est dépendant de la profession ou à la compétence exclusive ou à la qualification PAC.*	Non Recommandé pour les médecins, pharmaciens et chirurgiens-dentistes si typeBAL = PER avec un identifiant interne. Ne pas renseigner dans les autres cas.		Nomenclature : Jeux de valeurs Spécialité CodeSystemName **=** R38 (spécialité ordinale) **CodeSystem =** 1.2.250.1.213.2.28 ou CodeSystemName **=** R40 (compétence exclusive) **CodeSystem =** 1.2.250.1.213.2.30 ou CodeSystemName **=** R44 (qualification PAC) **CodeSystem =** 1.2.250.1.213.2.34 Attribut renseigné uniquement pour les médecins et chirurgiens-dentistes si typeBAL = PER avec un identifiant interne. La saisie d'une spécialité est facultative pour un chirurgien-dentiste, tous ne possédant pas de spécialité. La spécialité est à choisir parmi les 3 codes suivants issus de la nomenclature R38 : SCD01, SCD02 et SCD03. La saisie d'une spécialité est facultative pour un pharmacien, tous ne possédant pas de spécialité.	RG_CTR_027 RG_CTR_028 RG_CTR_043

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTRÔLE
				La spécialité est à choisir parmi les 4 codes suivants : SP01, SP02, SP03 et SP04. La saisie d'une spécialité est recommandée pour un médecin. La spécialité est à choisir parmi tous les codes issus des nomenclatures R38, R40 et R44, à l'exception des codes cités ci-dessus. En cas d'erreur sur l'attribution d'une spécialité par rapport à la profession saisie, un code erreur **MSS027** sera remonté dans le rapport d'alimentation.	
Telephone	Téléphone (de type fixe ou mobile) lié à la BAL (PER, ORG ou APP)	Non	X(20)		
Dematerialisation	Indicateur d'acceptation de la dématérialisation. Valeurs possibles : • O – dématérialisation acceptée • N – dématérialisation refusée	Non	X(1)		
ListeRouge	Indicateur liste rouge Valeurs possibles : • O – BAL en liste rouge • N – la BAL peut être publiée	Oui	X(1)	Les BAL en liste rouge ne sont pas publiées par l'Annuaire Santé.	RG_CTR_032

Tableau 15 : Structure COMPTESMSS dans le cas de BAL personnelles sans identifiant national RPPS ou ADELI

6.4.2.3.3.3 Structure COMPTESMSS d'une BAL applicative ou organisationnelle rattachée à une structure déclarée dans l'Annuaire Santé

Ces BAL organisationnelles ou applicatives sont rattachées à des structures déclarées dans l'Annuaire Santé.

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTRÔLE
TypeBAL	Valeurs possibles : • ORG pour BAL Organisationnelle • APP pour BAL Applicative	Oui	X(3)	Une BAL de type ORG ou APP est rattachée à une personne morale (entité géographique ou entité juridique), et son usage s'effectue sous la responsabilité d'un ou plusieurs professionnels habilités à échanger des données de santé personnelles.	RG_CTR_002 RG_CTR_003
AdresseBAL	Adresse unique de messagerie dans un domaine de messagerie MSSanté	Oui	X(256)	La RFC 5321 précise que le pattern d'une adresse de messagerie doit respecter la règle suivante : X(64)@Y(255) ; avec un maximum de **256** caractères au total pour X+@+Y.	RG_CTR_001 RG_CTR_004 RG_CTR_044 RG_CTR_046
TypeIdentifiantPM	Type de structure à laquelle la BAL est associée. Valeurs possibles : • 1 si FINESS • 2 si SIREN • 3 si SIRET	Oui		Nomenclature : TypeIdentifiantPM **CodeSystemName =** G07 **CodeSystem =** 1.2.250.1.71.1.2.14	RG_CTR_009 RG_CTR_011 RG_CTR_012 RG_CTR_015 RG_CTR_038 RG_CTR_039
IdentifiantPM	Numéro FINESS géographique ou Numéro SIREN ou Numéro SIRET	Oui	X(32)	Seules les structures FINESS font l'objet d'une déclaration obligatoire. De ce fait toutes les structures FINESS sont dans l'annuaire santé et peuvent faire l'objet de rattachement. Ce n'est pas le cas de l'ensemble structures SIREN/SIRET.	RG_CTR_013 RG_CTR_014 RG_CTR_016 RG_CTR_033 RG_CTR_034
ServiceRattachement	Nom et description du service de rattachement de l'utilisateur dans l'organisation	Non	X(160)	Texte libre Cet attribut permet de renseigner le service de rattachement de l'utilisateur (PER) ou de la BAL (APP ou ORG) dans l'organisation.	RG_CTR_036

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTRÔLE
Responsable	Texte libre donnant les coordonnées de la (ou des) personne(s) responsable(s) au niveau opérationnel de la BAL. *Exemple : le chef de service….*	Oui	X(160)		RG_CTR_029
Description	Description fonctionnelle de la BAL	Oui si typeBAL = ORG ou APP	X(160)		RG_CTR_030
Telephone	Téléphone (de type fixe ou mobile) lié à la BAL (PER, ORG ou APP)	Non	X(20)		
Dematerialisation	Indicateur d'acceptation de la dématérialisation. Valeurs possibles : • O – dématérialisation acceptée • N – dématérialisation refusée	Non	X(1)		
ListeRouge	Indicateur liste rouge Valeurs possibles : • O – BAL en liste rouge • N – la BAL peut être publiée	Oui	X(1)	Les BAL en liste rouge ne sont pas publiées par l'Annuaire Santé.	RG_CTR_032

Tableau 16 : Structure COMPTESMSS dans le cas de BAL applicatives et organisationnelles rattachée à une structure déclarée dans l'Annuaire Santé

6.4.2.3.3.4 Structure COMPTESMSS d'une BAL organisationnelle rattachées à une personne physique exerçant dans une structure ne disposant pas de numéro FINESS (exemple cabinets libéraux).

Cas de BAL organisationnelles rattachées à une personne physique exerçant dans une structure ne disposant pas de numéro FINESS (exemple cabinets libéraux). Une liste de cotitulaires doit être transmise contenant a minima un professionnel habilité déclaré comme responsable de la BAL.

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
TypeBAL	Correspond au type de BAL. La valeur doit être « CAB »	Oui	X(3)	Une BAL de type CAB regroupe un ou plusieurs professionnels de santé	RG_CTR_102
AdresseBAL	Adresse unique de messagerie dans un domaine de messagerie MSSanté	Oui	X(256)	La RFC 5321 précise que le pattern d'une adresse de messagerie doit respecter la règle suivante : X(64)@Y(255) ; avec un maximum de 256 caractères au total pour X+@+Y	RG_CTR_001 RG_CTR_004 RG_CTR_044 RG_CTR_050
ListeRouge	Ajout de l'adresse MSSanté dans la liste rouge Valeurs possibles : O : L'adresse MSSanté n'est pas publiée N : L'adresse MSSanté est publiée	Oui	X(1)		RG_CTR_104
Description	Description fonctionnelle de la BAL	Oui	X(160)		RG_CTR_108

- - Cette BAL CAB va contenir une balise « ListeCotitulaires » avec à l'intérieur une ou plusieurs balises « Cotitulaire ». Chaque balise « Cotitulaire » va comprendre les attributs suivants :

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
TypeIdentifiantPP	Type Identifiant PS. Valeurs possibles : • 0 si ADELI • 8 si RPPS	Oui	X(1)	Nomenclature : **CodeSystemName =** G08 **CodeSystem =** 1.2.250.1.71.1.2.15	RG_CTR_120 RG_CTR_140
IdentifiantPP	Identifiant RPPS, identifiant ADELI	Oui	Adeli : X(9) RPPS : (X11)		RG_CTR_121 RG_CTR_141
NomExercice	Nom de la situation d'exercice de l'utilisateur	Oui	X(80)		RG_CTR_122 RG_CTR_142
PrenomExercice	Prénom de la situation d'exercice de l'utilisateur	Oui	X(50)		RG_CTR_123 RG_CTR_143
EstResponsable	Correspond au responsable de la BAL CAB. Valeurs possibles : O : Le PS est le responsable N : Le PS est un cotitulaire	Oui	X(1)	Un seul cotitulaire de la liste pour être déclaré comme responsable	RG_CTR_106

6.4.2.3.4 Présentation du flux d'alimentation – en sortie de l'Annuaire Santé

En retour, le serveur de l'Annuaire Santé envoie un accusé de réception du message, avec le numéro de ticket attribué pour le traitement d'alimentation, ou un message d'erreur.

En sortie le message est composé de deux entrées :

- Une entrée contenant un numéro de ticket attribué à la réception flux d'alimentation – `TICKET` ;
- Une entrée contenant l'exception en cas d'erreur (voir **§ 6.3.2.3.4** « Gestion des erreurs ») – `FAULT`.

Remarque : le numéro de ticket sert à récupérer le compte-rendu du chargement du flux d'alimentation.

Figure 30 : Message d'accusé de réception ou SOAP Fault

6.4.2.4 Traitement de l'alimentation des messages par le serveur de l'Annuaire Santé

Remarque : le paragraphe suivant fournit à titre d'information une synthèse du traitement d'alimentation du serveur de l'Annuaire Santé.

A l'heure planifiée, les messages d'alimentation des comptes MSSanté sont traités dans l'ordre d'arrivée par un traitement batch d'alimentation sur le serveur de l'Annuaire Santé.

Afin de calculer la date de dernière mise à jour des BAL MSSanté tout en assurant la cohérence des informations, le traitement d'alimentation s'articule autour des étapes suivantes :

- À partir du SAS de stockage, chargement des fichiers dans une table de travail dans l'ordre de leur réception ;
- Identification du delta par rapport aux BAL existantes dans la base de données :
    - Le calcul s'effectue par domaine ;
    - Le calcul du delta s'effectue enregistrement par enregistrement, avec un rapprochement par rapport à la clé fonctionnelle des adresses de BAL MSSanté ;
    - Pour chaque enregistrement traité, le système identifie l'opération à effectuer selon 3 cas possibles :
        1. Création : si la valeur de la clé fonctionnelle de l'enregistrement n'existe pas dans la table cible ;
        2. Mise à jour : si la valeur de la clé fonctionnelle de l'enregistrement a un enregistrement correspondant dans la table cible et si au moins l'un des attributs d'alimentation a été modifié ;
        3. Suppression : si la valeur de la clé fonctionnelle de l'enregistrement n'a pas de correspondant dans la table source ;
- Contrôle de cohérence et vérification des règles d'alimentation ;
- Constitution des deltas intégrables ;
- Alimentation de la base cible de l'Annuaire Santé ;
- production du compte-rendu d'alimentation.

6.4.2.5 Web Service de recherche du compte-rendu d'alimentation

En retour d'un message d'alimentation et après traitement, le serveur de l'Annuaire Santé émet un compte-rendu positif ou négatif.

Les messages d'alimentation des comptes MSSanté sont traités dans l'ordre d'arrivée par un traitement batch d'alimentation sur le serveur de l'Annuaire Santé. Le traitement est exécuté **entre 2 h et 4 h** durant la nuit.

Par conséquent :

- **toutes les tentatives d'alimentations doivent être réalisées avant 2 h**.
- **il est inutile de tenter la récupération du compte-rendu avant 4 h**.

Les comptes rendus concernent aussi bien les erreurs de syntaxe ou de nomenclature que les rejets ou alertes sur règles fonctionnelles.

Remarque : les comptes rendus d'alimentation sont transmis sous forme d'un fichier compressé d'extension .zip basé sur l'algorithme « deflate ».

Le fichier ZIP contient deux fichiers :

- Un fichier nommé « cralimentationmss_numero_de_ticket_ AAAAMMJJHHmmss.xml » ;
- Un fichier nommé « cralimentationmss_numero_de_ticket_ AAAAMMJJHHmmss _checksum.txt ».

Le fichier XML contient les données du compte-rendu.

Le fichier TXT contient l'empreinte du fichier XML calculé avec l'algorithme SHA256. Il permet de vérifier l'intégrité du fichier XML avant utilisation. Cette vérification est optionnelle.

E

EX_1.1.1_5020

Pour récupérer le compte-rendu d'alimentation, le même certificat d'authentification que celui utilisé lors de l'alimentation correspondante doit être utilisé.

E

EX_1.1.1_5030

Afin de s'assurer de la bonne publication des BAL MSSanté dans l'Annuaire Santé, les rapports d'alimentation doivent être téléchargés et les erreurs traitées après chaque alimentation.

Cas d'utilisation	Utilisation d'un Web Service de récupération d'un fichier XML de compte-rendu d'alimentation pour un flux identifié.
Résumé	Permettre à un Opérateur, via son système, de récupérer le compte-rendu d'un flux d'alimentation envoyé précédemment.
Déclencheur	Invocation de l'URL correspondant au Web Service de récupération du compte-rendu.
Mode	Interactif.
Objectif	Fournir un fichier compressé d'extension .zip contenant deux fichiers : • Un fichier XML comportant le compte-rendu d'alimentation ; • Un fichier TXT contenant l'empreinte du fichier XML calculé avec l'algorithme SHA256 (afin de pouvoir vérifier, si besoin, l'intégrité du fichier XML avant utilisation).
Fréquence d'utilisation	Le lendemain de chaque publication (après 4h si la publication a eu lieu avant 2h).
Acteur principal	Opérateur MSSanté initiateur de la demande.
Pré conditions	Le DN du certificat utilisé est référencé dans la liste blanche des domaines autorisés.
Post conditions	L'exécution de l'opération ne provoque aucune modification des informations intégrées dans le fichier.

Tableau 17 : Cas d'utilisation du Web Service de récupération de compte-rendu de traitement

Scénario principal

Étapes	Activité	Scénario Alternatif
1	Un Opérateur qui souhaite récupérer des informations concernant l'alimentation d'un flux envoyé précédemment invoque le Web Service de récupération du compte-rendu : • En établissant une session TLS avec authentification mutuelle ; • En passant en paramètre le numéro du ticket attribué par l'Annuaire Santé. Les comptes rendus d'alimentation disponibles sont les X derniers générés, où X est un nombre paramétrable (de l'Annuaire Santé), dont le maximum est 20.	SA1
2	Le serveur de l'Annuaire Santé réceptionne le message et procède à son interprétation.	SA2
3	Le serveur de l'Annuaire Santé identifie l'utilisateur et effectue le contrôle d'accès par rapport à la liste blanche des domaines autorisés.	SA3, SA4
4	Le système : • Récupère le fichier XML de compte-rendu rattaché au ticket (ainsi que le fichier TXT contenant l'empreinte du fichier XML) ; • Crée un message SOAP et attache le fichier compressé d'extension .zip contenant les deux fichiers (le fichier XML + le fichier TXT associé).	SA5

Tableau 18 : Scénario principal d'utilisation du Web Service de récupération de compte-rendu de traitement

Scénarios alternatifs

Étapes	Activité
SA1 : Le service n'est pas disponible	
1	Il n'y a pas de message de réponse de la part du système.
SA2 : Le message envoyé est mal formaté	
2	Le système envoie un message d'erreur sans traiter la demande (message WSMSS 12).
SA3 : Le DN n'est pas référencé dans la liste blanche	
3	Si le DN n'est pas référencé dans la liste blanche, l'Annuaire Santé envoie un message d'erreur sans traiter la demande (message WSMSS 6).
SA4 : Le numéro de ticket ne correspond pas au DN	
3	Le système envoie un message d'erreur sans traiter la demande (message WSMSS 16).
SA5 : Le traitement n'est pas démarré ou est en cours de traitement	
4	Le Web Service renvoie un message « traitement en cours » (message WSMSS 17).

Tableau 19 : Scénarios alternatifs d'utilisation du Web Service de récupération de compte-rendu de traitement

6.4.2.5.1 Principe de construction du flux

6.4.2.5.1.1 Présentation du flux en entrée du serveur d'Annuaire Santé

Chaque message en entrée est constitué de deux parties :

- Une structure d'en-tête, qui contient les informations propres au flux de données (utilisées par la couche technique) - `ENTETE` ;
- Le corps du message, qui contient les critères en entrée du Web Service, en l'occurrence le numéro de ticket attribué lors du dépôt du fichier d'alimentation – `TICKET`.

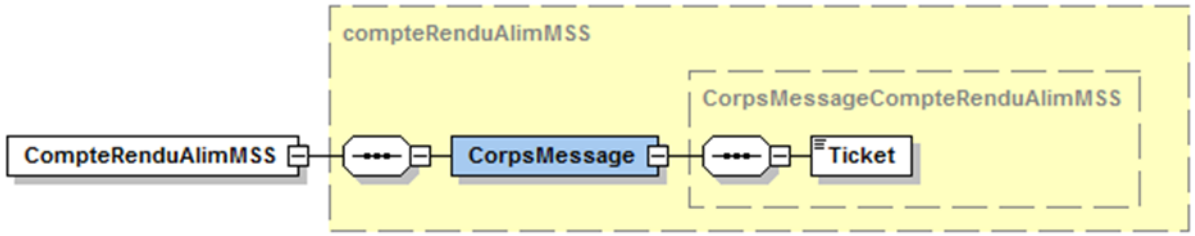


Figure 31 : Corps du message pour la recherche de compte-rendu de traitement

6.4.2.5.1.2 Présentation du flux en sortie du serveur d'Annuaire Santé

En retour le serveur d'Annuaire Santé envoie un fichier .zip en pièce jointe, ou un message d'information si le traitement d'alimentation n'a pas été réalisé.

Le message est composé de deux entrées :

- Une entrée comportant un fichier compressé d'extension .zip contenant les deux fichiers (le fichier contenant le compte-rendu d'alimentation au format XML + le fichier contenant l'empreinte du fichier XML au format TXT) – `TICKET` ;
- Une entrée permettant de transmettre un message fonctionnel « Le flux d'alimentation rattaché au ticket [No.Ticket] n'a pas été traité. Veuillez essayer ultérieurement » si le flux n'a pas été traité – `FAULT`.

Figure 32 : Corps du message pour la réponse du Web Service de recherche d'un compte-rendu

6.4.2.5.1.3 Description du fichier de compte-rendu d'alimentation

Le fichier de compte-rendu d'alimentation est libellé «cralimentationmss_numero_de_ticket_AAAAMMJJHHmmss.xml».

Ce fichier est structuré en :

- Un bloc d'en-tête qui comporte :
  - Le numéro de ticket (pour rappel) ;
  - Le rappel de la règle RG_CTR_021 (MSS020) car c'est l'erreur la plus fréquemment constatée.
- Et un ou plusieurs blocs de détail de compte-rendu (un bloc par domaine de messagerie).

Chaque bloc comporte les éléments suivants :

- Le nom du domaine chargé ;
- Les éléments statistiques d'alimentation ;
- La liste des anomalies détectées, groupées par enregistrement, puis par criticité (anomalies bloquantes suivies des anomalies qui sont en alerte).

Structure – Ticket

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
Ticket	N° de ticket	Oui	X(50)	N° de ticket correspondant au compte-rendu de l'alimentation

Tableau 20 : Bloc d'en-tête, structure du ticket

Structure – Liste des règles de contrôle

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
RegleControle		Oui	X(320)	Description de la règle de contrôle Exemple : Le contrôle de cohérence vérifie que la première lettre du prénom et les deux premières lettres du nom - après la normalisation (sans : accents-tirets-apostrophe-espaces) - sont identiques aux valeurs connues dans l'Annuaire Santé.
CodeMSS0	Code fonctionnel de l'erreur associée au contrôle	Oui	X(6)	Exemple : MSS020

Tableau 21 : Bloc d'en-tête, structure de la liste des contrôles

Structure – Domaine

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
Domaine	Domaine de l'adresse de messagerie	Oui	X(255)	

Tableau 22 : Bloc de détail, structure des domaines de messagerie

Structure – Éléments statistiques

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
NbBALLus	Nombre d'enregistrements lus pour le domaine chargé	Oui	N(5)	
NbBALDelta	Nombre d'enregistrements en modification (création, modification, suppression) avant contrôle du domaine chargé	Oui	N(5)	
NbBALCrees	Nombre d'enregistrements créés pour le domaine chargé	Oui	N(5)	
NbBALMaj	Nombre d'enregistrements mis à jour pour le domaine chargé	Oui	N(5)	
NbBALSup	Nombre d'enregistrements supprimés pour le domaine chargé	Oui	N(5)	
NbBALErrBlo	Nombre d'enregistrements en erreur bloquante pour le domaine chargé	Oui	N(5)	Une BAL comportant plusieurs erreurs n'est comptée qu'une seule fois ; si elle comporte une erreur bloquante et une ou plusieurs erreurs non bloquantes elle n'est comptabilisée que dans le compteur des BAL avec erreur bloquante
NbBALErrNBlo	Nombre d'enregistrements en erreur non bloquante pour le domaine chargé	Oui	N(5)	

Tableau 23 : Bloc de détail, structure des éléments statistiques

Structure – Liste des anomalies

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
CodeMSS0	Code fonctionnel de l'erreur	Oui	X(6)	Généré par le processus d'alimentation
MotifErreur	Description fonctionnelle du rejet	Oui	X(320)	Généré par le processus d'alimentation
CriticiteErreur	Criticité	Oui	X(20)	Généré par le processus d'alimentation : Bloquante ou Warning
TypeBAL	Valeurs possibles : • ORG pour la BAL Organisationnelle • APP pour la BAL Applicative • PER pour la BAL Personnelle	Non	X(3)	La BAL de type PER est rattachée à une personne physique La BAL de type ORG ou APP est rattachée à une personne morale (entité géographique ou entité juridique)
AdresseBAL	Adresse unique de messagerie dans un domaine de messagerie MSSanté	Non	X(256)	La RFC 5321 précise qu'une adresse de messagerie « XXX@YYY » ne doit pas dépasser **256** caractères (avec au maximum 64 caractères pour XXX et au maximum 255 caractères pour YYY, en prenant

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
				en compte « @ » dans les 256 caractères maximums autorisés)
TypeIdentifiantPP	Identifiant RPPS, ADELI, interne à la structure d'activité. Valeurs possibles : • 0 si ADELI • 8 si RPPS • 10 si identifiant interne	Non	X(2)	Nomenclature : TypeIdentifiantPP **CodeSystemName =** G08 **CodeSystem =** 1.2.250.1.71.1.2.15
IdentifiantPP	Identifiant RPPS ou ADELI du titulaire de la BAL ou identifiant interne (si type 10)	Non	X(256)	Les attributs « IdentifiantPP » et « TypeIdentifiantPP) sont renseignés avec les valeurs indiquées dans le fichier d'alimentation transmis par l'Opérateur.
TypeIdentifiantPM	Type de structure à laquelle la BAL est associée. Valeurs possibles : • 1 si FINESS • 2 si SIREN • 3 si SIRET	Non	X(2)	Nomenclature : TypeIdentifiantPM **CodeSystemName =** G07 **CodeSystem =** 1.2.250.1.71.1.2.14
IdentifiantPM	Numéro FINESS EJ ou EG ou le numéro SIREN ou le numéro SIRET	Non	X(32)	
NomExerciceAnnuaire	Nom d'exercice connu dans l'Annuaire Santé	Oui pour un type de BAL PER avec un identifiant de type RPPS ou ADELI (type 0 ou 8), dans le cas où le contrôle RG_CTR_021 est négatif Sinon n'est pas renseigné	X(80)	<u>Remarque</u> : l'exercice professionnel pris en compte pour renseigner ces données est l'exercice professionnel le plus récemment ouvert ou le plus récemment fermé, si aucun exercice n'est ouvert
PrenomExerciceAnnuaire	Prénom d'exercice connu dans l'Annuaire Santé	Oui pour un type de BAL PER avec un identifiant de type RPPS ou ADELI (type 0 ou 8), dans le cas où le contrôle RG_CTR_021 est négatif Sinon n'est pas renseigné	X(50)	
TypeIdentifiantPPAnnuaire	Type de l'identifiant national connu dans l'Annuaire Santé	Oui pour un type de BAL PER dans le cas où le contrôle RG_CTR_045 est négatif Sinon n'est pas renseigné	X(2)	Nomenclature : TypeIdentifiantPP **CodeSystemName** = G08 **CodeSystem** = 1.2.250.1.71.1.2.15
IdentifiantPPAnnuaire	Identifiant national connu dans l'Annuaire Santé		X(256)	

Tableau 24 : Bloc de détail, structure des anomalies détectées

La liste des contrôles effectués, des codes d'erreurs et des messages associés est définie au **§ 9.**7.3 « Codes d'erreurs pour la TM1.1.xP - Mise à jour des comptes de messagerie dans l'Annuaire ».

Remarque : un exemple de feuille de style que les Opérateurs peuvent utiliser pour l'affichage du compte-rendu est disponible en annexe et correspond au document de référence DR5 défini au **§ 9.5**.

6.5 Consultation de l'Annuaire Santé

EX_2.1_5010  
L'Opérateur MSSanté doit synchroniser les données des utilisateurs de son service avec celles provenant de l'Annuaire Santé .

RE_2.1_5030
Parmi les solutions disponibles, nous recommandons d'utiliser le service permettant d'exposer des données des référentiels Personnes physiques/Personnes morales au format JSON, structurées selon le standard d'interopérabilité FHIR, voir [ANN-EXT-API]. En effet, celle-ci permet une mise en cache locale par l'Opérateur de l'Annuaire Santé, dans un objectif d'assurer de meilleures performances et une meilleure résilience, contrairement à la solution TM2.1.1A consistant à consulter l'Annuaire Santé par le protocole LDAP.

L'Opérateur MSSanté peut intégrer le contenu de l'Annuaire Santé dans son annuaire local et y ajouter d'autres données. Mais il ne doit pas altérer les données issues de l'Annuaire Santé.

6.5.1 TM2.1.1A - Consultation de l'Annuaire Santé par le protocole LDAP

La fonction de consultation de l'Annuaire Santé permet de rechercher un correspondant sur la base de multiples critères et de récupérer en retour de la requête les informations d'identité, l'adresse de messagerie et les coordonnées de contact des destinataires potentiels répondants aux critères de recherche utilisés.

Remarque : le renseignement des destinataires de messages ne passe pas nécessairement par une recherche sur l'annuaire et peut être directement effectué par la saisie de l'adresse du correspondant, le copier/coller depuis une source d'information externe, ou encore la sélection d'une entrée du carnet d'adresses local au client de messagerie.

Critères de recherche

La recherche peut être réalisée selon plusieurs critères : nom d'exercice, prénom d'exercice, profession, spécialité, lieu d'exercice (raison sociale ou enseigne commerciale, ville, département ou code postal).

Plusieurs critères peuvent être associés entre eux (avec un Opérateur logique de type « ET »).

Les recherches de type « CONTIENT » sont autorisées sur les champs de type texte (mise en place de métacaractères « wildcards »).

La recherche peut être réalisée en incluant ou non les enregistrements sans BAL MSSanté associée.

RE_2.1_5010

Nous recommandons pour les recherches de type « CONTIENT » de préciser à l'utilisateur que cette fonctionnalité est disponible et de faciliter son utilisation via les interfaces graphiques du client de messagerie.

Résultats fournis par l'Annuaire Santé

Un nombre maximum de résultats est prévu : au-delà, l'Annuaire Santé renvoie un code d'erreur que le **Connecteur à l'Annuaire Santé** de l'Opérateur doit interpréter comme une invitation de l'utilisateur à affiner ses critères de recherche.

Les messages d'erreur qui sont issus d'un paramétrage spécifique sont les suivants :

- TimeLimitExceeded : ce message d'erreur est envoyé quand le temps de traitement de la requête LDAP dépasse le paramètre TIMELIMIT défini côté serveur ;
- SizeLimitExceeded : ce message d'erreur est envoyé quand le nombre de résultat retourné dépasse le paramètre SIZELIMIT défini côté serveur.

Pour information, les valeurs configurées par défaut sur l'Annuaire Santé sont :

- TimeLimitExceeded : 1 minute ;
- SizeLimitExceeded : 100 entrées.

RE_2.1_5020

Nous recommandons que le **Connecteur à l'Annuaire Santé** privilégie autant que possible les opérations de filtre des résultats de la recherche en local, sur la base des résultats fournis par l'Annuaire Santé, lorsque, après récupération d'une première liste de résultats du serveur d'Annuaire Santé, l'utilisateur souhaite affiner ses critères de recherche.

Remarque :

- Le nom DNS de l'Annuaire Santé pour les interfaces LDAP est : **ldap.annuaire.mssante.fr**
- L'URL d'accès permettant d'accéder aux interfaces LDAP est : **ldap://ldap.annuaire.mssante.fr**

EX_2.1.1_5010


La transaction « TM2.1.1.A - Interrogation de l'Annuaire Santé par le protocole LDAP » est réservée à la recherche de BAL MSSanté par les utilisateurs finaux et ne doit pas être utilisée pour récupérer l'intégralité du contenu de l'Annuaire Santé de manière automatisée.

6.5.2 TM2.1.3A - Téléchargement d'une extraction de l'Annuaire Santé

NB : Cette extraction spécifique aux opérateurs MSSanté sera décommissionnée courant 2025. Les nouvelles modalités d'interrogation sont communiquées aux opérateurs afin de préparer les opérations de bascule.

EX_2.1.3_5010


Dans le cas où l'Opérateur implémente la transaction « TM2.1.3A - Téléchargement d'une extraction de l'Annuaire Santé », il doit respecter les spécifications d'implémentation décrites dans le chapitre **§ 6.5.2** (et sous-chapitres associés).

L'ANS met à la disposition des Opérateurs une extraction de l'Annuaire Santé, contenant l'ensemble des BAL des professionnels habilités, tous domaines de messagerie confondus, exception faite de celle déclarée en liste rouge par le détenteur de la BAL.

Cette extraction permet l'utilisation des données de l'Annuaire Santé localement dans la structure.

EX_2.1.3_5020


L'Opérateur, qui consomme le téléchargement de l'extraction de l'Annuaire Santé, doit mettre en œuvre un mécanisme permettant d'assurer le fonctionnement de son système de messagerie en cas d'indisponibilité de l'interface fournie par l'ANS. Il pourra s'agir d'un système de cache local.

6.5.2.1 Principes de fonctionnement

Les adresses de BAL MSSanté sont extraites, dans un fichier au format XML par un traitement batch. Le fichier, généré à une fréquence quotidienne, est mis à disposition pour être récupéré par Web Service. Le schéma XSD associé correspond au document de référence DR3 défini au **§ 9.5**.

Les règles d'extraction du fichier sont les suivantes :

Description	Concerne
Les extractions portent sur l'ensemble des adresses de BAL MSSanté référencées dans l'Annuaire Santé avec l'indicateur Liste rouge positionné à « N ».	Informations extraites
Les extractions portent sur les adresses de BAL MSSanté déclarées par l'ensemble des Opérateurs MSSanté	Règle de sélection
Les informations extraites sont triées dans l'ordre suivant : par domaine, par identifiant de personne physique, par identifiant de personne morale, par BAL.	Tri
Les extractions sont transmises sous forme d'un fichier compressé d'extension .zip basé sur l'algorithme « deflate ». Le fichier zip contient deux fichiers : • « ExtractionMSSGlobale_AAAAMMJJHHmmss.xml » ; • « ExtractionMSSGlobale_AAAAMMJJHHmmss_checksum.txt ». Le fichier XML contient les données extraites. Le fichier TXT contient l'empreinte du fichier XML calculé avec l'algorithme SHA256. Il permet de vérifier l'intégrité du fichier XML avant utilisation. Cette vérification est optionnelle.	Format du fichier
Les fichiers d'extraction sont libellés *« ExtractionMSSGlobale_AAAAMMJJHHmmss»,* où *AAAAMMJJHHmmss* est la date et heure de création des fichiers.	Nom du fichier
L'identifiant PM (type et valeur) extrait est en priorité le n° FINESS, s'il existe ; sinon, il s'agit du n° SIRET pour une entité géographique ou du n° SIREN pour une entité juridique.	Identifiant PM
Données relatives aux structures extraites pour les BAL personnelles : • Pour les BAL personnelles enregistrées avec la référence d'une structure : ces BAL sont restituées associées à cette structure, que cette dernière soit ouverte ou fermée ; • Pour les BAL personnelles enregistrées sans référence à une structure : ces BAL sont restituées associées à toutes les structures correspondant à des activités ouvertes de la personne. Remarques : Dans le cas où la personne aurait plusieurs activités ouvertes dans une même structure, cette structure ne serait extraite qu'une fois ; Une BAL peut être extraite sans aucune donnée sur la structure (cas où la personne n'aurait aucune activité ouverte).	Structures extraites pour des BAL personnelles
Les données extraites relatives à l'exercice professionnel (nom et prénom d'exercice, civilité d'exercice, catégorie de profession, profession) sont celles de l'exercice professionnel le plus récemment ouvert ou le plus récemment fermé (si aucun exercice n'est ouvert à la date de l'extraction).	Données de l'exercice professionnel
Pour des personnes possédant plusieurs savoir-faire : • Pour les médecins, le seul savoir-faire extrait est celui de type S, CEX ou PAC (spécialité, compétence exclusive, qualification PAC) ; • Pour les chirurgiens-dentistes, le savoir-faire extrait est celui de type S, s'il existe (sinon aucun savoir-faire n'est extrait). Pour les autres professions aucun savoir-faire n'est extrait.	Données du savoir-faire
Les adresses (postales) extraites sont celles des structures	Adresse

Tableau 25 : Règles d'extraction du fichier des BAL MSSanté

6.5.2.2 Description fonctionnelle

Cas d'utilisation	Utilisation d'un Web Service REST de récupération d'un fichier XML d'extraction de l'ensemble des BAL MSSanté du Référentiel des identités PP/PM qui peuvent être publiées (BAL dont l'indicateur Liste rouge associé est à Non).
Résumé	Permettre à un système initiateur de récupérer l'extraction de l'ensemble des BAL MSSanté publiables.
Déclencheur	Invocation de l'URL correspondant au Web Service d'extraction.
Objectif	Fournir un fichier compressé d'extension .zip contenant deux fichiers : • Un fichier XML comportant une extraction globale de l'ensemble des BAL MSSanté publiables ; • Un fichier TXT contenant l'empreinte du fichier XML calculé avec l'algorithme SHA256 (afin de pouvoir vérifier l'intégrité du fichier XML avant utilisation).
Fréquence d'utilisation	À la demande (quotidiennement de préférence).
Acteur principal	Opérateur MSSanté initiateur de la demande.
Pré conditions	Le DN du certificat utilisé est référencé dans la liste blanche des domaines autorisés.
Post conditions	L'exécution de l'opération ne provoque aucune modification des informations intégrées dans le fichier.

Tableau 26 : Cas d'utilisation du Web Service de téléchargement des BAL MSSanté

Scénario principal

Étapes	Activité	Scénario Alternatif
1	Un Opérateur qui souhaite récupérer le fichier d'extraction globale des BAL MSSanté invoque par l'intermédiaire d'un système initiateur le Web Service d'extraction en passant en paramètre le type du fichier (ceci en prévision des autres formats d'extractions à venir (csv, ldif etc.)) Url du type : https://<host>/<silo>/<version>/<ressource>?format=xml	SA1
2	Le système réceptionne le message et procède à son interprétation.	SA2
3	Le système identifie l'utilisateur et effectue le contrôle d'accès par rapport à la liste blanche des domaines autorisés.	SA3
4	Le système : • Récupère le dernier fichier XML de l'extraction (ainsi que le fichier TXT contenant l'empreinte du fichier XML) ; • Retourne un fichier compressé d'extension .zip contenant les deux fichiers (le fichier XML + le fichier TXT associé) dans la réponse.	

Tableau 27 : Scénario principal d'utilisation du Web Service de téléchargement des BAL MSSanté

Scénarios alternatifs

Étapes	Activité	Scénario Alternatif
SA1 : Le service n'est pas disponible		
1	404 Not found	
SA2 : L'URL est mal formatée		
1	400 Bad Request	
SA3 : Le DN n'est pas référencé dans la liste blanche des domaines autorisés		
3	Si le DN n'est pas référencé dans la liste blanche des domaines autorisés, le système envoie un message d'erreur sans traiter la demande : 401 Access Denied	

Tableau 28 : Scénarios alternatifs d'utilisation du Web Service de téléchargement des BAL MSSanté

6.5.2.3 Principe de construction du flux d'extraction de l'Annuaire Santé

6.5.2.3.1 Présentation du flux d'entrée

L'appel se fait via URL :

GET https://ws.annuaire.mssante.fr/webservices/<version>/extractionMSSante/?format=xml

6.5.2.3.2 Présentation du flux en sortie

En sortie le message contient un fichier compressé d'extension .zip contenant les deux fichiers (le fichier global d'extraction au format XML + le fichier contenant l'empreinte du fichier XML au format TXT).

STATUT	CODE	DESCRIPTION	ENTÊTE	BODY
200	OK	La ressource demandée existe		1 retour contenant la ressource

Tableau 29 : Réponse du Web Service de demande de téléchargement de l'extraction de l'Annuaire Santé en cas de succès

Le corps de la réponse fournie par le Web Service en cas de succès est le suivant :

ELÉMENT	DESCRIPTION	TYPE	OBLIGATOIRE
Extraction	L'extraction au format demandé encodé en base 64	xsd:base64 Binary	Oui

Tableau 30 : Corps de la réponse du Web Service de demande de téléchargement de l'extraction de l'Annuaire Santé en cas de succès

6.5.2.3.3 Messages d'erreur

En cas d'erreur la réponse fournie par le Web Service est la suivante :

STATUT	CODE	MESSAGE
400	Bad Request	Le format est obligatoire Le format n'est pas valide (csv, xml, ldif, dml)
403	Forbidden	Échec d'authentification - L'identité de l'émetteur contenue dans le certificat n'est pas présente dans la liste blanche des domaines autorisés
		Échec d'authentification - L'identité de l'émetteur contenue dans le certificat n'est pas valide
404	Not found	Le fichier d'extraction ne peut être récupéré du SAS de stockage

Tableau 31 : Réponse du Web Service de demande de téléchargement de l'extraction de l'Annuaire Santé en cas d'erreur

6.5.2.3.4 Format du fichier d'extraction

Le fichier d'extraction est libellé «ExtractionMSSGlobale_AAAAMMJJHHmmss.xml».

Le tableau ci-dessous liste les attributs extraits :

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
TYPEBAL	Valeurs possibles : • ORG pour une BAL Organisationnelle • APP pour une BAL Applicative • PER pour une BAL Personnelle	Oui	X(3)	
ADRESSEBAL	Adresse unique de messagerie dans un domaine de messagerie MSSanté	Oui	X(256)	
TYPEIDENTIFIANTPP	Identifiant RPPS, ADELI, interne à la structure d'activité. Valeurs possibles : • 0 si ADELI • 8 si RPPS • 10 si identifiant interne	Oui pour une BAL de type PER Non pour les autres types		Nomenclature : TypeIdentifiantPP **CodeSystemName =** G08 **CodeSystem =** 1.2.250.1.71.1.2.15 L'utilisation de l'identifiant 10 doit faire l'objet d'une approbation de l'ANS
IDENTIFIANTPP	Identifiant RPPS ou ADELI du titulaire de la BAL ou identifiant interne (si type 10)	Oui pour une BAL de type PER Non pour les autres types	X(256)	Dans le cas des BAL de type « PER » (ADELI / RPPS) l'identifiant national associé au PS qui sera extrait sera le plus récent (par exemple, RPPS à la place du numéro ADELI le cas échéant).
TYPEIDENTIFIANTPM	Type de structure à laquelle la BAL est associée. Valeurs possibles : • 1 si FINESS • 2 si SIREN • 3 si SIRET	Oui pour une BAL de type ORG ou APP et pour type de BAL PER avec un identifiant interne (type 10)		Nomenclature : TypeIdentifiantPM **CodeSystemName =** G07 **CodeSystem =** 1.2.250.1.71.1.2.14
IDENTIFIANTPM	Numéro FINESS EJ ou EG, ou le numéro SIREN, ou le numéro SIRET	Oui pour une BAL de type ORG ou APP et pour type de	X(32)	

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
		BAL PER avec un identifiant interne (type 10)		
SERVICERATTACHEMENT	Nom et description du service de rattachement de l'utilisateur dans l'organisation	Non	X(160)	Il s'agit du service de rattachement de l'utilisateur (PP) ou de la BAL (PM) dans l'organisation.
NCIVILITEEXERCICE	Civilité de la situation d'exercice de l'utilisateur	Non		Nomenclature : CiviliteExercice **CodeSystemName =** R11 **CodeSystem =** 1.2.250.1.213.1.6.1.11 La civilité d'exercice ne concerne que les professions de médecin, pharmacien, chirurgien-dentiste. Remarque : Il ne s'agit pas des valeurs « Monsieur », « Madame », consulter la nomenclature pour plus de détails.
NOMEXERCICE	Nom d'exercice de l'utilisateur (nom sous lequel il exerce)	Oui pour une BAL de type PER	X(80)	
PRENOMEXERCICE	Prénom d'exercice de l'utilisateur (prénom sous lequel il exerce)	Oui pour une BAL de type PER	X(50)	
NCATEGORIEPROFESSION	Catégorie de profession de l'utilisateur	Oui pour une BAL de type PER		Nomenclature : CatégorieDeProfessions **CodeSystemName =** R37 **CodeSystem =** 1.2.250.1.213.1.6.1.3
NPROFESSION	Profession de l'utilisateur	Oui pour une BAL de type PER		Nomenclature : Profession **CodeSystemName =** G15 **CodeSystem =** 1.2.250.1.71.1.2.7
NSPECIALITE	Spécialité de l'utilisateur (ou compétence exclusive ou qualification PAC le cas échéant)	Non		Nomenclature : Jeux de valeurs Spécialité **CodeSystemName =** R38 **CodeSystem =** 1.2.250.1.213.2.28 Ou **CodeSystemName =** R40 **CodeSystem =** 1.2.250.1.213.2.30 Ou **CodeSystemName =** R44 **CodeSystem =** 1.2.250.1.213.2.34
RESPONSABLE	Texte libre donnant les coordonnées de la personne responsable au niveau opérationnel de la BAL. Exemples : le chef de service, l'administrateur de l'application	Oui pour une BAL de type ORG ou APP	X(160)	
DESCRIPTION	Description fonctionnelle de la BAL	Oui pour une BAL de type ORG, CAB ou APP	X(160)	
LISTECOTITULAIRES	Liste des cotitulaires déclarés sur une BAL CAB	Oui pour BAL CAB	N/A	Voir tableau ci-dessous
TELEPHONE	Téléphone (de type fixe ou mobile) lié aux BAL (PER, ORG ou APP)	Non	X(20)	
DEMATERIALISATION	Décommissionné	Non	X(1)	Conservé pour rétrocompatibilité
RAISONSOCIALE	Raison sociale de la Structure d'activité	Non	X (164)	
ENSEIGNECOMMERCIALE	Enseigne commerciale de la Structure d'activité	Non	X(50)	

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
L2COMPLEMENTLOCALISATION	Ligne 2 de l'adresse Complément d'identification du destinataire ou du point de remise : personne, N° d'appartement, escalier…	Non	X(38)	
L3COMPLEMENTDISTRIBUTION	Ligne 3 de l'adresse Complément d'identification du point géographique : entrée, Tour, Résidence, Zone industrielle…	Non	X(38)	
L4NUMEROVOIE	Ligne 4 de l'adresse N° de la voie	Non	X(4)	
L4COMPLEMENTNUMEROVOIE	Ligne 4 de l'adresse Indice de répétition du n° dans la voie : bis, ter…	Non	X(3)	
NL4TYPEVOIE	Type de voie	Non		Nomenclature : TypeVoie **CodeSystemName =** R35 **CodeSystem =** 1.2.250.1.213.2.44
L4LIBELLEVOIE	Ligne 4 de l'adresse Libellé de la voie : Nom de la rue, de l'avenue	Non	X(38)	
L5LIEUDITMENTION	Ligne 5 de l'adresse Permet d'indiquer le lieu-dit ou un service particulier de distribution : BP 28, Bat A …	Non	X(38)	
L6LIGNEACHEMINEMENT	Ligne 6 libellé acheminement	Non	X(38)	
NCODEPOSTAL	Code postal	Non		
NCOMMUNE	Commune	Non		Nomenclature : Commune **CodeSystemName =** R13 **CodeSystem =** 1.2.250.1.213.2.23
NDEPARTEMENT	Département	Non		Nomenclature : Département **CodeSystemName =** G09 **CodeSystem =** 1.2.250.1.71.1.2.16
NPAYS	Pays	Non		Nomenclature : Pays **CodeSystemName =** R20 **CodeSystem =** 1.2.250.1.213.2.24

Tableau 32 : Liste des attributs présents dans le fichier d'extraction des comptes MSSanté

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
TYPEIDENTIFIANTPP	Identifiant RPPS, ADELI, interne à la structure d'activité. Valeurs possibles : • 0 si ADELI • 8 si RPPS	Oui pour une BAL de type CAB Non pour les autres types		Nomenclature : TypeIdentifiantPP **CodeSystemName =** G08 **CodeSystem =** 1.2.250.1.71.1.2.15
IDENTIFIANTPP	Identifiant RPPS ou ADELI du titulaire de la BAL	Oui pour une BAL de type CAB Non pour les autres types	X(256)	
NOMEXERCICE	Nom d'exercice de l'utilisateur (nom sous lequel il exerce)	Oui pour une BAL de type CAB Non pour les autres types	X(80)	
PRENOMEXERCICE	Prénom d'exercice de l'utilisateur (prénom sous lequel il exerce)	Oui pour une BAL de type CAB Non pour les autres types	X(50)	
ESTRESPONSABLE	O : Le professionnel est le responsable N : Le professionnel est un cotitulaire	Oui pour une BAL de type CAB Non pour les autres types	X(1)	Un seul responsable parmi les cotitulaires de la BAL CAB

Tableau 33 : Liste des attributs présents dans l'objet Cotitulaires des BAL CAB

6.5.3 TM2.1.4A - Téléchargement des données d'identités des futurs utilisateurs finaux

NB : Cette extraction de l'Annuaire Santé spécifique aux opérateurs MSSanté sera décommissionnée courant 2024. Une extraction publique similaire est déjà disponible [ANN-EXT-PUB]. Une nouvelle interface de consultation FHIR est aussi mise à disposition par l'annuaire Santé depuis S2 2022 [ANN-EXT-API]. Les opérateurs utilisant cette extraction seront contactés afin de procéder à la migration.

EX_2.1.4_5010


Dans le cas où l'Opérateur implémente la transaction « TM2.1.4A - Téléchargement des données d'identités des futurs utilisateurs finaux », il doit respecter les spécifications d'implémentation décrites dans le chapitre **§ 6.5.3** (et sous-chapitres associés).

Afin de permettre aux Opérateurs de préparer la publication des BAL MSSanté de leurs utilisateurs professionnels dans l'Annuaire Santé, l'ANS met à la disposition de chaque Opérateur les données à caractère personnel de personnes physiques des secteurs sanitaire et médico-social - porteurs et non porteurs de cartes CPS. Ces données sont issues de répertoires nationaux d'identité qui comprennent notamment les identifiants nationaux. Ces données sont mises à la disposition de l'Opérateur à cette fin.

Seuls les professionnels habilités référencés dans les répertoires RPPS ou ADELI seront retournés par cette transaction. La majorité des professionnels du domaine social ne sont donc pas retournés par cette transaction. Ceci ne signifie pas nécessairement qu'il ne s'agit pas de professionnels habilités.

6.5.3.1 Principes de fonctionnement

Les données à caractère personnel sont extraites, dans un fichier au format CSV, par un traitement batch. Le fichier, généré à une fréquence quotidienne, est mis à disposition pour être récupéré par Web Service.

Les règles d'extraction du fichier sont les suivantes :

Description	Concerne
Les extractions portent sur l'ensemble des personnes physiques (porteurs et non porteurs de cartes CPS) possédant un identifiant national. Ces données sont issues de répertoires nationaux d'identité et répondent aux critères ci-dessous.	Périmètre des Informations extraites
Professionnels de Santé RPPS : Pour les professionnels de santé civils de profession : Sage-femme, médecin, chirurgien-dentiste, infirmiers sont extraits uniquement les PS inscrits à l'Ordre. Pour les pharmaciens civils, sont extraits les PS ayant au moins une activité en cours (c'est-à-dire dont la date de début d'activité est renseignée et antérieure à la date du jour, et, dont la date de fin d'activité n'est pas renseignée ou est postérieure à la date du jour). Pour les professionnels de santé militaires, sont extraits les PS ayant au moins un exercice professionnel. Les professionnels de santé en formation ne sont pas extraits. Professionnels de Santé non RPPS : Ensemble des professionnels de santé non RPPS porteurs ou non porteurs d'une carte CPS ayant une situation d'exercice active.	Règle de sélection
Les données extraites, liées aux personnes physiques, sont les données qui se rapportent à une situation d'exercice active.	Données de l'exercice professionnel
Pour un PS ayant plusieurs situations d'exercice actives, l'extraction comporte autant de lignes que de situations d'exercice : 1 ligne par situation d'exercice.	Tri
Un PS sans structure d'activité (PS remplaçant par ex) ou sans activité sera extrait sans identifiant de structure, ni adresse.	Tri
Seuls sont restitués les identifiants de structure de type 1, 2 et 3 (FINESS, SIRET ou SIREN). Toute adresse de structure est extraite, même dans le cas où le type d'identifiant de Personne Morale (PM) n'est pas restitué (cas des cabinets libéraux).	Données liées aux Structures
L'identifiant PM (type et valeur) extrait est en priorité le n° FINESS, s'il existe ; sinon, il s'agit du n° SIRET pour une entité géographique ou du n° SIREN pour une entité juridique.	Identifiant PM
Pour des personnes possédant plusieurs savoir-faire : • Pour les médecins, le seul savoir-faire extrait est celui de type S (Spécialité), CEX (compétence exclusive) ou PAC (qualification PAC) ; • Pour les chirurgiens-dentistes, le savoir-faire extrait est celui de type S (Spécialité) s'il existe (sinon aucun savoir-faire n'est extrait). Pour les autres professions aucun savoir-faire n'est extrait.	Données du savoir-faire
Les adresses (postales) extraites sont celles des structures.	Adresse
Le fichier d'extraction des données des personnes physiques **porteuses de carte CPS** est nommé : • « extraction_identites_Avec_CPS_aaaammjjhhmm.csv ». Le fichier d'extraction des données des personnes physiques **non porteuses de carte CPS** est nommé : • « extraction_identites_Sans_CPS_ aaaammjjhhmm.csv ».	Nom des fichiers

Description	Concerne
où aaaammjjhhmm est la date et heure de création du fichier.	
Les fichiers sont mis à disposition sous forme d'un fichier compressé d'extension .zip basé sur l'algorithme « deflate ». Le fichier ZIP est nommé « extraction_identites_ aaaammjjhhmm.zip ». Le fichier ZIP contient quatre fichiers : • « extraction_identites_Avec_CPS_aaaammjjhhmm.csv » ; • « extraction_identites_Sans_CPS_aaaammjjhhmm.csv » ; • « extraction_identites_Avec_CPS_aaaammjjhhmm_checksum.txt » ; • « extraction_identites_Sans_CPS_aaaammjjhhmm_checksum.txt ». Les fichiers CSV contiennent les données d'identités définies précédemment. Chaque fichier TXT contient l'empreinte du fichier CSV associé, calculé avec l'algorithme SHA256. Ils permettent de vérifier l'intégrité du fichier CSV avant utilisation. Remarque : l'ensemble des fichiers sont donc disponible via une seule transaction qui récupère en sortie le fichier zip.	Format du fichier
Les données sont séparées par le caractère « ; »	Séparateur de données
La restitution des données est réalisée en colonne et l'ordre de présentation des attributs dans les fichiers est identique à l'ordre du tableau « Liste des attributs présents dans les fichiers des données d'identités ».	Ordre de présentation des données
La première ligne du fichier contient le nom des attributs.	Ligne d'en-tête
Le fichier d'extraction des données des personnes physiques est généré chaque jour.	Fréquence de mise à disposition

Tableau 34 : Règles d'extraction des fichiers des données d'identités des futurs utilisateurs finaux

6.5.3.2 Description fonctionnelle

Cas d'utilisation	Utilisation d'un Web Service REST de récupération de fichiers CSV des données d'identités des futurs utilisateurs finaux.
Résumé	Permettre à un système initiateur de récupérer l'extraction.
Déclencheur	Invocation de l'URL correspondant au Web Service d'extraction.
Objectif	Fournir un fichier compressé d'extension .zip contenant les quatre fichiers : • « extraction_identites_Avec_CPS_aaaammjjhhmm.csv » ; • « extraction_identites_Sans_CPS_aaaammjjhhmm.csv » ; • « extraction_identites_Avec_CPS_aaaammjjhhmm_checksum.txt » ; • « extraction_identites_Sans_CPS_aaaammjjhhmm_checksum.txt ».
Fréquence d'utilisation	À la demande.
Acteur principal	Opérateur MSSanté initiateur de la demande.
Pré conditions	Le DN du certificat utilisé est référencé dans la liste blanche des domaines autorisés.
Post conditions	L'exécution de l'opération ne provoque aucune modification des informations intégrées dans le fichier.

Tableau 35 : Cas d'utilisation du Web Service de récupération des fichiers des données d'identités

Scénario principal

Étapes	Activité	Scénario Alternatif
1	Un Opérateur qui souhaite récupérer le fichier d'extraction des identités invoque par l'intermédiaire d'un système initiateur le Web Service d'extraction en passant en paramètre le type du fichier (ceci en prévision des autres formats d'extractions à venir (csv, ldif etc.)) Url du type : https://<host>/<silo>/<version>/<ressource>?format=csv	SA1
2	Le système réceptionne le message et procède à son interprétation.	SA2
3	Le système identifie l'utilisateur et effectue le contrôle d'accès par rapport à la liste blanche des domaines autorisés.	SA3
4	Le système : • Récupère les derniers fichiers CSV (ainsi que les fichiers TXT contenant les empreintes des fichiers CSV) ; • Retourne un fichier compressé d'extension .zip contenant les quatre fichiers dans la réponse.	

Tableau 36 : Scénario principal d'utilisation du Web Service de récupération des fichiers des données d'identités

Scénarios alternatifs

Étapes	Activité	Scénario Alternatif
SA1 : Le service n'est pas disponible		
1	404 Not found	
SA2 : L'URL est mal formatée		
1	400 Bad Request	
SA3 : Le DN n'est pas référencé dans la liste blanche des domaines autorisés		
3	Si le DN n'est pas référencé dans la liste blanche des domaines autorisés, le système envoie un message d'erreur sans traiter la demande : 401 Access Denied	

Tableau 37 : Scénarios alternatifs d'utilisation du Web Service de récupération des fichiers des données d'identités

6.5.3.3 Principe de construction du flux d'extraction de l'Annuaire Santé

6.5.3.3.1 Présentation du flux d'entrée

L'appel se fait via URL :

GET https://ws.annuaire.mssante.fr/webservices/<version>/extractionIdentitePS/?format=csv

6.5.3.3.2 Présentation du flux en sortie

En sortie le message contient un fichier compressé d'extension .zip contenant les quatre fichiers (les deux fichiers au format CSV + les deux fichiers TXT contenant les empreintes des fichiers CSV).

STATUT	CODE	DESCRIPTION	ENTÊTE	BODY
200	OK	La ressource demandée existe		1 retour contenant la ressource

Tableau 38 : Réponse du Web Service de récupération des fichiers des données d'identités en cas de succès

Le corps de la réponse fournie par le Web Service en cas de succès est le suivant :

ELÉMENT	DESCRIPTION	TYPE	OBLIGATOIRE
Extraction	L'extraction au format demandé encodé en base 64	xsd:base64 Binary	Oui

Tableau 39 : Corps de la réponse du Web Service de récupération des fichiers des données d'identités en cas de succès

6.5.3.3.3 Messages d'erreur

En cas d'erreur la réponse fournie par le Web Service est la suivante :

STATUT	CODE	MESSAGE
400	Bad Request	Le format est obligatoire Le format n'est pas valide (csv, xml, ldif, dml)
403	Forbidden	Échec d'authentification - L'identité de l'émetteur contenue dans le certificat n'est pas présente dans la liste blanche des domaines autorisés
		Échec d'authentification - L'identité de l'émetteur contenue dans le certificat n'est pas valide
404	Not found	Le fichier d'extraction ne peut être récupéré du SAS de stockage

Tableau 40 : Réponse du Web Service de récupération des fichiers des données d'identités en cas d'erreur

6.5.3.3.4 Format du fichier d'extraction

Les fichiers d'extraction sont libellés :

- extraction_identites_Avec_CPS_aaaammjjhhmm.csv ;
- extraction_identites_Sans_CPS_aaaammjjhhmm.csv.

Remarques :

- La restitution des données est réalisée en colonne et l'ordre de présentation des attributs dans les fichiers est identique à l'ordre du tableau ci-dessous ;
- La première ligne du fichier contient le nom des attributs.

Le tableau ci-dessous liste les attributs extraits :

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
TYPEIDENTIFIANTPP	Identifiant RPPS, ADELI Valeurs possibles : • 0 si ADELI • 8 si RPPS	Oui		Nomenclature : TypeIdentifiantPP **CodeSystemName =** G08 **CodeSystem =** 1.2.250.1.71.1.2.15
LIB_TYPEIDENTIFANTPP	Libellé du type d'identifiant	Oui	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (G08)
IDENTIFIANTPP	Identifiant RPPS ou ADELI du PP	Oui	X(11)	
NCIVILITEEXERCICE	Civilité de la situation d'exercice du PS	Non		Nomenclature : CiviliteExercice **CodeSystemName =** R11 **CodeSystem =** 1.2.250.1.213.1.6.1.11 La civilité d'exercice ne concerne que les professions de médecin, pharmacien, chirurgien-dentiste. Remarque : Il ne s'agit pas des valeurs « Monsieur », « Madame », consulter la nomenclature pour plus de

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
				détails.
NOMEXERCICE	Nom d'exercice de l'utilisateur (nom sous lequel il exerce)	Oui	X(80)	
PRENOMEXERCICE	Prénom d'exercice de l'utilisateur (prénom sous lequel il exerce)	Oui	X(50)	
NCATEGORIEPROFESSION	Catégorie de profession du PS	Oui		Nomenclature : CatégorieDeProfessions **CodeSystemName =** R37 **CodeSystem =** 1.2.250.1.213.1.6.1.3
LIB_NCATEGORIEPROFESSION	Libellé de la catégorie de profession du PS	Oui	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (R37)
NPROFESSION	Profession du PS	Oui		Nomenclature : Profession **CodeSystemName =** G15 **CodeSystem =** 1.2.250.1.71.1.2.7
LIB_NPROFESSION	Libellé de la profession du PS	Oui	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (G15)
NSPECIALITE	Spécialité du PS (ou compétence exclusive ou qualification PAC le cas échéant)	Non		Nomenclature : Jeux de valeurs Spécialité **CodeSystemName =** R38 **CodeSystem =** 1.2.250.1.213.2.28 ou **CodeSystemName =** R40 **CodeSystem =** 1.2.250.1.213.2.30 ou **CodeSystemName =** R44 **CodeSystem =** 1.2.250.1.213.2.34
LIB_NSPECIALITE	Libellé de la spécialité	Non	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (R38, R40, R44)
TYPEIDENTIFIANTPM	Type de structure dans laquelle exerce le PS Valeurs possibles : • 1 si FINESS • 2 si SIREN • 3 si SIRET	Non		Nomenclature : TypeIdentifiantPM **CodeSystemName =** G07 **CodeSystem =** 1.2.250.1.71.1.2.14
LIB_TYPEIDENTIFANTPM	Libellé du type de structure dans laquelle exerce le PS	Non	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (G07)
IDENTIFIANTPM	Numéro FINESS EJ ou EG, ou le numéro SIREN, ou le numéro SIRET	Non	X(32)	
RAISONSOCIALE	Raison sociale de la Structure d'activité	Non	X (164)	
ENSEIGNECOMMERCIALE	Enseigne commerciale de la	Non	X(50)	

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
	Structure d'activité			
L2COMPLEMENTLOCALISATION	Ligne 2 de l'adresse Complément d'identification du destinataire ou du point de remise : personne, N° d'appartement, escalier…	Non	X(38)	
L3COMPLEMENTDISTRIBUTION	Ligne 3 de l'adresse Complément d'identification du point géographique : entrée, Tour, Résidence, Zone industrielle…	Non	X(38)	
L4NUMEROVOIE	Ligne 4 de l'adresse N° de la voie	Non	X(4)	
L4COMPLEMENTNUMEROVOIE	Ligne 4 de l'adresse Indice de répétition du n° dans la voie : bis, ter…	Non	X(3)	
NL4TYPEVOIE	Type de voie	Non		Nomenclature : TypeVoie **CodeSystemName =** R35 **CodeSystem =** 1.2.250.1.213.2.44
LIB_NL4TYPEVOIE	Libellé du type de voie	Non	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (R35)
L4LIBELLEVOIE	Ligne 4 de l'adresse Libellé de la voie : Nom de la rue, de l'avenue	Non	X(38)	
L5LIEUDITMENTION	Ligne 5 de l'adresse Permet d'indiquer le lieu-dit ou un service particulier de distribution : BP 28, Bat A …	Non	X(38)	
L6LIGNEACHEMINEMENT	Ligne 6 libellé acheminement	Non	X(38)	
NCODEPOSTAL	Code postal	Non		
NCOMMUNE	Commune	Non		Nomenclature : Commune **CodeSystemName =** R13 **CodeSystem =** 1.2.250.1.213.2.23
LIB_NCOMMUNE	Nom de la commune	Non	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (R13)
NDEPARTEMENT	Département	Non		Nomenclature : Département **CodeSystemName =** G09 **CodeSystem =** 1.2.250.1.71.1.2.16
LIB_NDEPARTEMENT	Nom du département	Non	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (G09)
NPAYS	Pays	Non		Nomenclature : Pays **CodeSystemName =** R20

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
				CodeSystem = 1.2.250.1.213.2.24
LIB_NPAYS	Nom du pays	Non	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (R20)

Tableau 41 : Liste des attributs présents dans les fichiers des données d'identités

6.6 Liste blanche des domaines MSSanté autorisés

Au sein de l'Espace de Confiance MSSanté, les échanges de messages ne sont autorisés qu'entre les domaines MSSanté référencés dans la liste blanche des domaines MSSanté.

Remarque : à l'émission d'un message (cf. **§ 6.**7.2 « TM3.2P – Emission de messages »), l'appartenance des domaines des adresses de messagerie de l'émetteur et du destinataire à la liste blanche des domaines autorisés est contrôlée.

Description et format de la liste blanche

La liste blanche est un fichier XML signé par l'ANS contenant la liste des domaines autorisés au sein de l'Espace de Confiance MSSanté.

Ce fichier est géré par l'ANS et mis à jour régulièrement au gré de l'arrivée ou du retrait des domaines de messagerie MSSanté autorisés à intégrer l'Espace de Confiance.

Remarque : la liste blanche peut contenir des Opérateurs MSSanté qui sont habilités mais qui n'ont pas encore généré leur certificat serveur. Leur certificat n'est donc pas encore présent dans l'annuaire des produits de certificat qui récence l'ensemble des produits de certification.

L'accès à la liste blanche ne nécessite pas d'authentification préalable du Connecteur MSSanté de l'Opérateur.

Le tableau ci-dessous présente les paramètres contenus dans la liste blanche des domaines MSSanté :

Nom	Description	Type	Longueur	Format
versionFormat	Version du format de la liste blanche	Alphanumérique	50	Libre
DateDeGeneration	Date de génération du fichier	DateTime	Sans Objet	xsd:DateTime [-]CCYY-MM-DDThh:mm:ss[Z|(+|-)hh:mm])
ListeDomaines	Liste des domaines de l'Espace de Confiance MSSanté	Liste de Domaines	Sans Objet	Liste de Domaines
Signature	Signature du fichier par l'ANS avec un certificat logiciel serveur de type SERV_S/MIME de l'IGC Santé	XMLDSIG	Sans Objet	XMLDSIG

Tableau 42 : Liste des paramètres de la liste blanche des domaines de messagerie MSSanté

Pour chaque domaine MSSanté référencé dans la liste blanche, le champ « ListeDomaines » contient les informations suivantes :

Nom	Description	Type	Longueur	Format
Nom	Nom du domaine de messagerie. Exemples: ch-xyz.mssante.fr ch-xyz-securise.fr	Alphanumérique	255	Sans Objet
Description	Description du domaine	Alphanumérique	255	Sans Objet
DNCertificatOperateur	DN du certificat d'authentification pour les échanges SMTP (la structure du DN est conforme à la spécification RFC 2253 « UTF-8 String Representation of Distinguished Names » de Décembre 1997.)	Alphanumérique	255	UTF-8 String Representation of Distinguished Names Voir tableau 43.
ResponsableContact	Champs non utilisé	NA	NA	NA
SupportContact	Champs non utilisé	NA	NA	NA
DateMAJ	Date de mise à jour du domaine dans la liste blanche	DateTime	Sans Objet	xsd:DateTime [-]CCYY-MM-DDThh:mm:ss[Z|(+|-)hh:mm])

Tableau 43 : Liste des paramètres du champ « ListeDomaines » de la liste blanche des domaines MSSanté

Ci-dessous un tableau récapitulatif des éléments contenus dans le DN de la liste blanche pour l'IGC Santé. Les champs apparaitront dans l'ordre indiqué dans le tableau.

Eléments contenus dans le champ DNCertificatOperateur du certificat serveur indiqué en liste blanche		Autorité de certification IGC-Santé
CN		< Nom applicatif >
OU		<Prefix_Type>< IdNat_Struct >
O		< Raison sociale Structure >
ST		< Nom département (N°)>
C		FR

Tableau 44: Liste des paramètres à renseigner pour l'information DNCertificatOperateur en fonction du certificat serveur applicatif utilisé

Détails des éléments contenus dans le champ DNCertificatOperateur du certificat serveur indiqué en liste blanche :

- Le « CN » correspond au FQDN du connecteur MSSanté. Il s'agit du champ « nom de domaine d'adresse web URL » du formulaire de commande de certificat n°413.
- Le <Prefix_Type> du champ « OU » correspond au préfix ajouté à l'identifiant national de la structure (< IdNat_Struct >) selon son type (finess, siret, siren).
- Le « O » correspond à la raison sociale de la structure.

EX_LBL_5010
Les Opérateurs MSSanté doivent prendre en compte les cas suivants, qui sont possibles dans la Liste Blanche des domaines autorisés (en fonction des implémentations mises en œuvre sur les différents services de messagerie MSSanté) : • Un DN de certificat peut être associé à un ou plusieurs domaines de messagerie ; • Un domaine de messagerie peut être associé à un ou plusieurs DN de certificats ; • Un DN issu d'un certificat de l'IGC-Santé.

Remarques :

- Le format « xsd :DateTime » est défini dans le schéma XML suivant : http://www.w3.org/2001/XMLSchema.xsd ;
- Le format de la liste blanche est défini dans le schéma XML « listeblanchemssante.xsd » conforme à la spécification W3C XMLSchema 1.0 (http://www.w3.org/XML/Schema) (voir DR1 au **§ 9.5.**

Les champs de la liste blanche sont alimentés sur la base des éléments communiqués par l'Opérateur dans l'Annexe 1 – Déclaration d'un domaine MSSanté de son contrat « Opérateur MSSanté v2 » pour son intégration à l'Espace de Confiance MSSanté.

6.6.1 TM4.1P - Interrogation de la liste blanche des domaines de messagerie MSSanté

EX_2.2_5010
Le Connecteur MSSanté doit récupérer **quotidiennement** la dernière version de la liste blanche à l'adresse suivante : https://espacedeConfiance.mssante.fr/listeblanchemssante.xml

EX_2.2_5030
L'exploitation par le Connecteur MSSanté de la liste blanche doit se faire en local et sans altération du fichier XML récupéré.

RE_2.2_5010
Il est recommandé de contrôler l'intégrité du fichier XML de la liste blanche par vérification de la signature lors de l'interrogation locale par les Connecteurs MSSanté des Opérateurs (par exemple, lors de l'envoi de messages dans l'Espace de Confiance MSSanté) de la liste blanche.

EX_2.2_5035
Le connecteur MSSanté doit disposer d'une copie locale de la dernière version valide de la liste blanche en cas d'indisponibilité ou de corruption de celle-ci.

6.6.2 Vérification de la signature de la liste blanche

La signature du fichier XML de la liste blanche permet de vérifier son authenticité ainsi que son intégrité, c'est-à-dire :

- Qu'il a bien été émis par l'ANS ;
- Qu'il n'a pas été modifié ;
- Qu'il n'a pas été altéré.

La signature de la liste blanche est au format XMLDSig, tel que défini par le W3C (http://www.w3.org/TR/xmldsig-core/) par le schéma XML suivant : http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd.

Le tableau ci-dessous présente les caractéristiques de la signature de la liste blanche des domaines MSSanté :

Paramètre	Valeur
Suite cryptographique utilisée pour calculer la signature	rsa-sha256 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha256)
Algorithme de transformation sous forme canonique du contenu à signer	xml-exc-c14n (http://www.w3.org/2001/10/xml-exc-c14n#)
Type de signature	Enveloppé (http://www.w3.org/2000/09/xmldsig#enveloped)
Algorithme de hachage du contenu à signer	SHA256 (http://www.w3.org/2001/04/xmlenc#sha256)

Tableau 45 : Liste des caractéristiques de la signature de la liste blanche des domaines MSSanté

EX_2.2_5040
La vérification de la signature doit se faire systématiquement à l'issue du téléchargement de la liste blanche dans le respect des bonnes pratiques définies par le W3C : http://www.w3.org/TR/xmldsig-bestpractices/#bp-validate-signing-key.

Lorsque la signature de la liste blanche téléchargée n'a pu être vérifiée, l'Opérateur doit exploiter la dernière liste blanche dont la signature a été vérifiée afin d'éviter tout interruption de service.

EX_2.2_5050
Le certificat à utiliser pour vérifier la signature est intégré dans le tag X509Data. Il doit être validé selon la norme PKIX (voir RFC 5280 (http://tools.ietf.org/html/rfc5280), RFC 5246 (http://tools.ietf.org/html/rfc2246), RFC 3207 (http://tools.ietf.org/html/rfc3207) et RFC 2034 (http://tools.ietf.org/html/rfc2034). Il faut contrôler qu'il a bien été émis par l'ANS et qu'il a été attribué à l'ANS.

Remarque : un exemple de liste blanche signée (valeur du certificat factice) « listeblanchemssanteSigned.xml » conforme à la spécification W3C Extensible Markup Language (XML) 1.0 (http://www.w3.org/TR/2008/REC-xml-20081126/) est disponible (voir DR1 au **§ 9.5)**.

6.7 Echange de messages entre Opérateurs MSSanté

6.7.1 TM3.1P – Réception de messages

EX_3.1_5010
Tout Opérateur accepte, sans restriction, les mails provenant d'émetteurs propriétaires de BAL sur des domaines de messagerie MSSanté. Il ne peut procéder à des filtrages de mails que pour des motifs de sécurité de son système et ce de façon exceptionnelle jusqu'à résolution du problème.

Remarque : il existe une exception sur la nomenclature des domaines de messagerie MSSanté qui est le domaine « interop-mssante.apicrypt.org ». Tout filtrage sur le suffixe « mssante.fr » devra prendre en compte également le suffixe « interop-mssante.apicrypt.org ».

EX_3.1_5015
Tout Opérateur accepte, sans restriction, les mails provenant du domaine '@dgs.mssante.fr'. Ce nom de domaine est rattaché à la Direction Générale de la Santé et lui permet d'adresser aux professionnels de santé dans un but de santé publique, des informations et alertes sanitaires. L'Opérateur doit en particulier permettre la réception de mails émis en masse en provenance de ce domaine.

Remarque :

L'article L. 4001-2 du code de la santé publique introduit par la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, dispose qu'*«à l'occasion de l'inscription au tableau de l'ordre, les professionnels de santé déclarent auprès du conseil de l'ordre compétent une adresse électronique leur permettant d'être informés des messages de sécurité diffusés par les autorités sanitaires. Cette information est régulièrement mise à jour et transmise aux autorités sanitaires à leur demande ».*

EX_3.1_5020
La réception de messages est effectuée sur le protocole SMTP, dans une session TLS mutuelle avec le Connecteur MSSanté du domaine émetteur (SMTPS).

EX_3.1_5030
Le Connecteur MSSanté mis en œuvre par l'Opérateur doit respecter la cinématique décrite dans le **§ 6.7.1.1** pour recevoir une requête en provenance d'un autre Connecteur MSSanté d'un autre Opérateur. En particulier les vérifications spécifiques à MSSanté et décrites dans cette cinématique doivent être mise en œuvre par le Connecteur MSSanté (étapes 3, 4, 5 et 6).

6.7.1.1 Cinématique

Les étapes de connexion pour un Connecteur MSSanté destinataire d'une requête en provenance d'un autre Connecteur MSSanté sont les suivantes :

1) Ouverture d'une session SMTP comme défini dans les RFC 5321 (http ://tools.ietf.org/html/rfc5321) et RFC 2034 (http ://tools.ietf.org/html/rfc2034) ;
2) Ouverture d'une session TLS avec STARTTLS comme défini dans les RFC 3207 (http ://tools.ietf.org/html/rfc3207) et RFC 2246 (http ://tools.ietf.org/html/rfc2246) (le Connecteur MSSanté destinataire ne doit accepter que ce type de connexion) ;
3) Vérification de la chaine de certificats serveurs présentée par le Connecteur MSSanté émetteur comme défini dans la RFC 2246 (http ://tools.ietf.org/html/rfc2246) (voir **§ 6.2 «** Modalités techniques pour assurer la sécurisation des échanges **»**) ;
4) Vérification que le DN du certificat présenté par le Connecteur MSSanté émetteur est référencé dans la liste blanche des domaines autorisés ;
5) Vérification que le DN du certificat présenté par le Connecteur MSSanté émetteur correspond au domaine émetteur ;
6) Vérification que le nom de domaine de l'adresse mail de l'expéditeur (« MAIL FROM ») :
    - Est renseigné dans l'enveloppe SMTP du message et ;
    - Figure dans la liste blanche des domaines autorisés et ;
    - Correspond au DN du certificat utilisé tel que référencé dans la liste blanche pour le domaine de messagerie en question ;

    Dans le cas contraire, le Connecteur MSSanté destinataire doit notifier le Connecteur MSSanté émetteur de la non émission du message en précisant le motif du rejet.

    Remarque : dans le cas des messages de notifications d'erreurs émis par un Connecteur MSSanté (par exemple : BAL du destinataire du message saturée, message automatique d'indication d'absence, information de détection de virus dans le message, etc.) il est nécessaire, afin de respecter la RFC 5321, d'autoriser les messages dont l'expéditeur (MAIL FROM) est vide (voir : http://tools.ietf.org/html/rfc5321#section-3.6.3 et http://tools.ietf.org/html/rfc5321#section-4.5.5) : ceci permet le cas échéant d'éviter les cas de boucles infinies entre Connecteurs MSSanté. Dans ce cas :
    - Le Connecteur MSSanté destinataire doit vérifier que le DN du certificat est présent dans la liste blanche des domaines autorisés ;
    - Le contrôle de la cohérence entre le domaine du «MAIL FROM » et le DN du certificat n'est pas réalisé.
7) Réception du message en respectant les bonnes pratiques de notification du statut de remise du message (pour son domaine) comme défini dans la RFC 5321 (http ://tools.ietf.org/html/rfc5321) ;
8) Fin de la session SMTPS comme défini dans les RFC 5321 (http ://tools.ietf.org/html/rfc5321) et RFC 2034 (http ://tools.ietf.org/html/rfc2034).

6.7.1.2 Transaction

EX_3.1_5040  
Les commandes SMTP envoyées par le Connecteur MSSanté doivent être conformes à la RFC 5321 (voir http ://tools.ietf.org/html/rfc5321).

6.7.2 TM3.2P – Emission de messages

EX_3.2_5010
Le Connecteur MSSanté doit permettre l'émission de messages vers des destinataires propriétaires de BAL sur des domaines MSSanté. Aucune restriction ne doit être appliquée sur ces envois.

EX_3.2_5020
L'émission de messages est effectuée sur le protocole SMTP, dans une session TLS mutuelle avec le Connecteur MSSanté destinataire (SMTPS).

EX_3.2_5040
Un Opérateur MSSanté ne doit pas utiliser le serveur SMTP d'un autre Opérateur MSSanté comme relai de messagerie.

EX_3.2_5050
Le Connecteur MSSanté de messagerie MSSanté mis en œuvre par l'Opérateur doit respecter la cinématique décrite dans le **§ 6.7.2.1** pour émettre une requête vers un autre Connecteur MSSanté d'un autre Opérateur. En particulier les vérifications spécifiques à MSSanté et décrites dans cette cinématique doivent être mise en œuvre par le Connecteur MSSanté (étapes 4, 5 et 6).

6.7.2.1 Cinématique

EX_3.2_5060
Avant l'envoi d'un message, le Connecteur MSSanté émetteur doit avoir vérifié préalablement que l'émetteur et le destinataire sont dans des domaines inclus dans la liste blanche (cette vérification peut être effectuée plus tard dans le processus **mais dans tous les cas *avant* l'envoi du message**) ; si ce n'est pas le cas, l'émetteur doit être notifié de la non émission (avec le motif du rejet).

Les étapes de connexion pour un Connecteur MSSanté émettant une requête vers un autre Connecteur MSSanté destinataire sont les suivantes :

1) Identification du ou des serveurs de destination par recherche des entrées MX correspondantes sur le serveur de nom de domaine (DNS) comme défini dans les RFC 974 et 2317 (http ://tools.ietf.org/html/rfc974 et http://www.ietf.org/rfc/rfc2317.txt) ;
2) Ouverture de la session SMTP comme défini dans les RFC 5321 (http ://tools.ietf.org/html/rfc5321) et RFC 2034 (http ://tools.ietf.org/html/rfc2034) ;

3) Ouverture de la session TLS avec STARTTLS comme défini dans les RFC 3207 (http ://tools.ietf.org/html/rfc3207) et RFC 2246 (http ://tools.ietf.org/html/rfc2246) (les Connecteurs MSSanté destinataires ne doivent accepter que ce type de connexion) ;
4) Vérification de la chaine de certificats serveurs présentée par le Connecteur MSSanté destinataire comme défini dans la RFC 2246 (http ://tools.ietf.org/html/rfc2246) ;
5) Vérification que le DN du certificat serveur présenté par le Connecteur MSSanté destinataire est référencé dans la liste blanche des domaines autorisés ;
6) Vérification que le DN du certificat serveur présenté par le Connecteur MSSanté destinataire correspond au domaine destinataire ;
7) Début de l'envoi du message : MAIL FROM : … ; RCPT TO : … comme défini dans les RFC 5321 (http ://tools.ietf.org/html/rfc5321), RFC 2034 (http ://tools.ietf.org/html/rfc2034) et RFC 2822 (http ://tools.ietf.org/html/rfc2822) ;
8) Fin de la session SMTPS comme défini dans les RFC 5321 (http ://tools.ietf.org/html/rfc5321) et RFC 2034 (http ://tools.ietf.org/html/rfc2034).

6.7.2.2 Transaction

EX_3.2_5070
Les commandes SMTP envoyées par le Connecteur MSSanté doivent être conformes à la RFC 5321 (voir http ://tools.ietf.org/html/rfc5321).

6.8 Services de messagerie à proposer aux logiciels métiers (API LPS)

L'API LPS est une interface standardisée que tous les Opérateurs de l'Espace de Confiance doivent proposer pour permettre à tout logiciel métier qui le souhaite de consulter ou envoyer des messages depuis une BAL MSSanté pour peu qu'il utilise les protocoles SMTP/IMAP, avec STARTTLS, et un Moyen d'Identification Electronique (MIE) spécifiée par l'API LPS.

Cette API LPS doit être proposée à tout éditeur de LPS conforme au référentiel #2 Clients de messagerie. L'ANS met à disposition l'outil MOTCO2 (MSSanté Outil de Test et de Conformité au Ref#2) [MSS-OUTIL-TEST] qui permet d'attester la conformité à l'API LPS des éditeurs. Les preuves qu'il génère sont traitées dans le cadre des dispositifs de financement proposés aux éditeurs de LPS.

EX_LPS_0110
L'opérateur doit proposer aux LPS conformes au Référentiel #2 MSSanté, des accès publics à l'API LPS, cad qu'il ne doit pas appliquer de mécanisme de filtrage des accès de type filtrage IP.

6.8.1 Vue d'ensemble de l'API

La figure suivante présente une vue d'ensemble de l'environnement de l'API LPS.

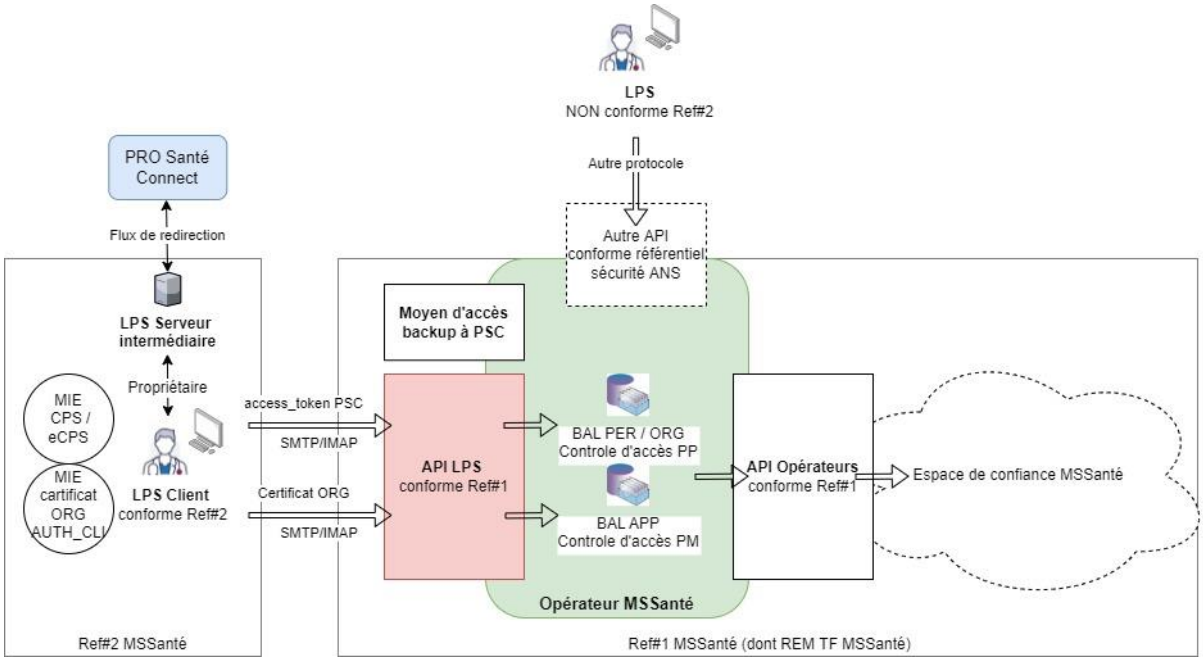


Figure 33 : Environnement général de l'API LPS

Cette API utilise :

- pour la couche transport les protocoles IMAP & SMTP ;
- une identification électronique spécifique à chaque type de BAL :
  - BAL personnelles et organisationnelles :
    - Access Token PRO Santé Connect (PSC) via le mécanisme d'authentification « XOAUTH2 »
  - BAL applicatives :
    - Certificat ORG AUTH-CLI via authentification TLS

Elle présente donc 2 points d'entrée distints en IMAP/SMTP.

Une méthode d'authentification alternative non dépendante de PSC, conforme au référentiel d'identification électronique de la PGSSI-S, peut être proposée par l'Opérateur aux professionnels pour accéder à leurs BAL MSSanté personnelles ou organisationnelle.

6.8.2 Exigences communes de sécurisation de l'API LPS

Afin d'assurer un niveau de sécurité suffisant sur les points d'entrée réseau correspondant à l'API LPS, chaque point d'entrée doit supporter la version 1.2 de TLS (a minima), avec des algorithmes de chiffrement adéquats.

EX_LPS_0100

Sur les interfaces de l'API LPS, le système DOIT impérativement accepter les connexions des clients de messagerie utilisant la version TLS 1.2 (RFC 5246). En complément de la version TLS 1.2, les versions ultérieures (TLS 1.3...) peuvent aussi être acceptées. Dans le cas contraire, la connexion ne doit pas être établie.

EX_LPS_0200

Sur les interfaces de l'API LPS, le système DOIT uniquement utiliser l'une des suites de chiffrement suivantes, lors de la négociation TLS :

- 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

Dans le cas contraire, la connexion ne doit pas être établie.

La longueur du groupe DH doit être >= 2048 bits ou la longueur du groupe elliptique ECDH doit être >= 256 bits.

La confidentialité persistante (PFS - perfect foward secrecy) de DH doit être utilisée (DHE ou ECDHE).

6.8.3 TM5.1P – Autoconfiguration de l'API LPS

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

L'auto-configuration des clients de messagerie (décrite dans le Référentiel #2 MSSanté) s'appuie sur un mécanisme standard proposé par les DNS des Opérateurs.

Cette méthode nécessite que l'Opérateur déclare dans son DNS, pour chacun des domaines de messagerie MSSanté qu'il héberge, les points d'entrée SMTP et IMAP de l'API LPS qu'il expose aux clients de messagerie MSSanté.

Le système MSSanté spécifie que la priorité de l'attribut permet de distinguer les points d'entrée suivants :

- Priorité 10 : Points d'entrée des BAL personnelles ou organsationnelles
- Priorité 20 : Points d'entrée des BAL applicatives

Le Référentiel #2 demande aux clients de messagerie de réaliser les opérations suivantes pour configurer une BAL MSSanté :

1- Extraire le domaine de la BAL à configurer,
2- Interroger le DNS du domaine de la BAL pour récupérer les attributs _submission._tcp & _imap._tcp de type SRV, afin d'obtenir les points d'entrée (hostname + port) SMTP et IMAP conformément aux RFC 2782 & 6186,
3- Suivant le type de BAL à configurer (PER/ORG ou APP), identifier les points d'entrée à utiliser en fonction de la priorité de l'attribut,
Configurer la BAL dans le LPS en utilisant les points d'entrée obtenus.

EX_LPS_0300


Sur les interfaces de l'API LPS, le système DOIT exposer un mécanisme d'auto-configuration à destination des LPS, conforme aux RFC 2782 & 6186, en déclarant sur chacun des noms de domaines déclarés en liste blanche les 4 attributs DNS suivants :

```
_submission._tcp SRV 10 100 587 [front smtp psc de l'opérateur]
_submission._tcp SRV 20 100 587 [front smtp authcli de l'opérateur]

_imap._tcp SRV 10 100 143 [front imap psc de l'opérateur]
_imap._tcp SRV 20 100 143 [front imap authcli de l'opérateur]
```

Le poids de chaque entrée est positionné à la valeur « 100 ». Si besoin, cette valeur peut être modifiée, mais il est impératif de la valeur retenue soit la même pour les 4 entrées.

6.8.4 TM5.2P et TM5.3P – Emission et consultation de messages d'une BAL personnelle ou organisationnelle via l'API LPS

6.8.4.1 Transaction

Le protocole de l'API LPS pour l'envoi de message est SMTP.

EX_LPS_0400

Le système DOIT exposer aux logiciels clients de messagerie respectant le référentiel MSSanté #2 une interface d'envoi de messages utilisant le protocole SMTP avec STARTTLS sur le port 587, conformément à la RFC 5321.

Le protocole l'API LPS pour la consultation des messages est IMAP version 4.

EX_LPS_0500

Le système DOIT exposer aux logiciels clients de messagerie respectant le référentiel MSSanté #2 une interface de consultation de BAL utilisant le protocole IMAP 4 (rev1 ou rev2) avec STARTTLS sur le port 143, conformément à la RFC 3501 ou RFC 9051.

Le moyen utilisé pour s'authentifier via l'API LPS pour une BAL personnelle ou organisationnelle est un Access Token récupéré par le LPS auprès de PRO Santé Connect après identification du PS.

EX_LPS_0600
Le système DOIT permettre à une personne physique identifiée dans l'annuaire santé de se connecter à une BAL personnelle ou organisationnelle en IMAP / SMTP en se basant sur l'Access Token PSC transmis par le LPS.

Ce token doit être transmis à l'établissement initial dès connexion SMTP et IMAP au moyen du mécanisme OAuth 2.0 du framework SASL (Simple Authentication and Security Layer) permettant la différentiation entre le protocole de communication et le moyen d'authentification.

EX_LPS_0700
Le système DOIT exposer le mécanisme SASL d'authentification OAuth 2.0 avec l'implémentation XOAUTH2 en IMAP et SMTP dans le but de permettre le transit de l'Access Token PSC au format JWT (Json Web Token), ainsi que la capability SASL-IR permettant la transmission de l'Access Token en une fois sur IMAP comme défini dans le RFC 4959 (https://tools.ietf.org/html/rfc4959).

Afin de pouvoir satisfaire cette exigence, le serveur de messagerie doit :

- Afficher la capacité d'authentification XOAUTH2 au moment de la connexion initiale du client.
- Afficher la capacité SASL-IR pour permettre la selection du moyen d'authentification et le passage de l'Access Token en une commande

Exemple pour IMAP (C = commande du client, S = réponse du serveur) :

```
C: C01 CAPABILITY
S: * CAPABILITY IMAP4rev1 … SASL-IR AUTH=XOAUTH2 …
S: C01 OK Completed
```

Exemple pour SMTP :

```
C: EHLO sender.example.com
S: 250-mx.exempl.com at your service, [145.87.123.47]
…
S: 250-AUTH LOGIN PLAIN XOAUTH2
…
```

- Supporter le passage de l'access token par le mécanisme d'authentification XOAUTH2 en une commande grâce à SASL-IR

Exemple pour IMAP :

```
C: A01 AUTHENTICATE XOAUTH2 dXNlcj1zb21ldXNlckBleGFtcGxlLmNvb
QFhdXRoPUJlYXJlciB5YTI5LnZGOWRmdDRxbVRjMk52YjNSbGNrQmhkSFJoZG
1semRHRXVZMjl0Q2cBAQ==
S: A01 OK Success
```

Exemple pour SMTP :

```
C: AUTH XOAUTH2 dXNlcj1zb21ldXNlckBleGFtcGxlLmNvbQFhdXRoPUJlY
XJlciB5YTI5LnZGOWRmdDRxbVRjMk52YjNSbGNrQmhkSFJoZG1semRHRXVZMj
l0Q2cBAQ==
S: 235 2.7.0 Accepted
```

En cas d'échec de l'authentification, la gestion des cas d'erreur doit respecter les standards imposés par SMTP et IMAP.

EX_LPS_0710
En cas d'erreur d'authentification, le système DOIT retourner des codes d'erreur conformes aux standard IMAP et SMTP, à savoir : • Pour IMAP : réponse NO Authentication failed, conformément au RFC 5530 (https://datatracker.ietf.org/doc/html/rfc5530#section-3) • Pour SMTP : réponse 535 5.7.8 Authentication credentials invalid code, conforément au RFC 4954 (https://datatracker.ietf.org/doc/html/rfc4954#section-6)

Exemple pour IMAP :

```
C: A01 AUTHENTICATE XOAUTH2 dXNlcj1zb21ldXNlckBleGFtcGxlLmNvb
QFhdXRoPUJlYXJlciB5YTI5LnZGOWRmdDRxbVRjMk52YjNSbGNrQmhkSFJoZG
1semRHRXVZMjl0Q2cBAQ==
S: A01 NO Authentication failed
```

Exemple pour SMTP :

```
C: AUTH XOAUTH2 dXNlcj1zb21ldXNlckBleGFtcGxlLmNvbQFhdXRoPUJlY
XJlciB5YTI5LnZGOWRmdDRxbVRjMk52YjNSbGNrQmhkSFJoZG1semRHRXVZMj
l0Q2cBAQ==
S: 535 5.7.8 Authentication credentials invalid
```

Afin de pouvoir procéder à l'appel du enpoint Userinfo auprès de PSC, il faut que le système ait été précédemment déclaré, enregistré et raccordé à PSC.

EX_LPS_0800
Le système DOIT faire la démarche de raccordement auprès du Fournisseur d'Identité PSC afin d'être autorisé à utiliser ce service. Cf. https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect.

6.8.4.2 Cinématique

Afin d'avoir une vue d'ensemble de l'environnement dans lequel est intégré le serveur de messagerie, la figure suivante présente l'architecture logique autour du serveur lorsqu'un LPS de type client lourd est utilisé.

*

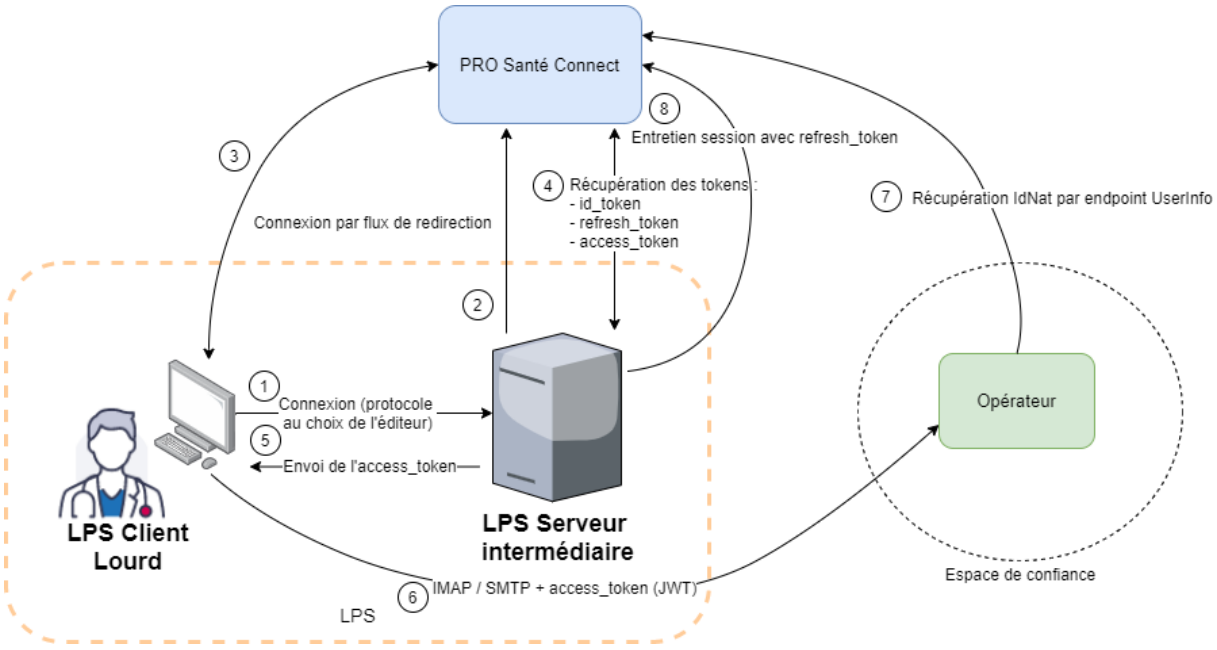


Figure 34 : Environnement de l'API LPS pour le MIE access token PSC avec client lourd LPS

Les différentes étapes sont les suivantes :

1. Connexion du LPS Client au LPS Serveur intermédiaire
2. Le serveur intermédiaire du LPS contacte PSC pour lancer l'authentification
3. Le serveur intermédiaire redirige le PS sur le site de PSC via son navigateur. Ce dernier réalise alors son authentification avec CPS ou e-CPS
4. L'authentification réussie, le serveur intermédiaire récupère 3 tokens de PSC : ID Token, Refresh Token et Access Token
5. Le serveur intermédiaire envoie l'Access Token au LPS Client
6. Lorsque le PS souhaite accéder à sa BAL MSSanté, le LPS Client monte une session IMAP ou SMTP en envoyant l'Access Token à l'Opérateur
7. L'Opérateur contacte PSC sur le endpoint Userinfo pour récupérer à partir de l'Access Token la valeur de l'IdNat présent dans le champ SubjectNameID
8. Le maintien de la connexion auprès de PSC est assuré par le serveur intermédiaire grâce à l'envoi du Refresh Token

Seules les étapes 6 et 7 impliquent directement l'opérateur.

La figure suivante présente l'architecture logique autour du serveur lorsqu'un LPS de type SaaS est utilisé.

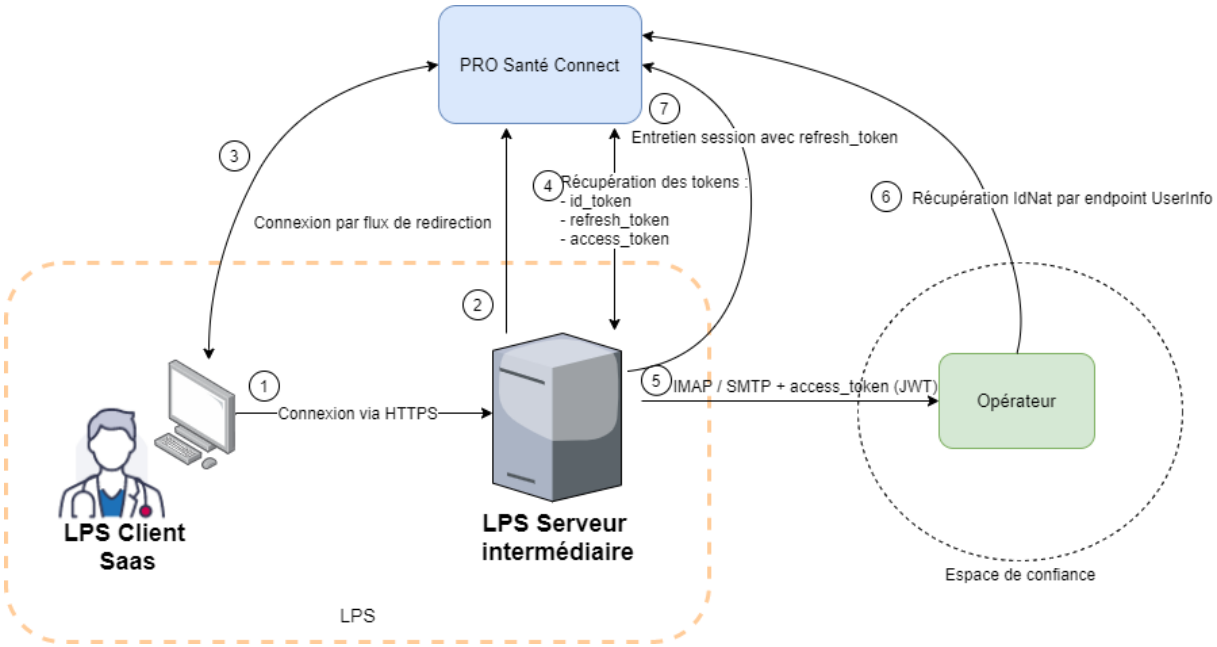


Figure 35 : Environnement de l'API LPS pour le MIE access token PSC avec client LPS type SaaS

Dans ce cas, les différentes étapes sont les suivantes :

1. Connexion du LPS Client au LPS Serveur intermédiaire
2. Le serveur intermédiaire du LPS contacte PSC pour lancer l'authentification
3. Le serveur intermédiaire redirige le PS sur le site de PSC via son navigateur. Ce dernier réalise alors son authentification avec CPS ou e-CPS
4. L'authentification réussie, le serveur intermédiaire récupère 3 tokens de PSC : ID Token, Refresh Token et Access Token
5. Le serveur intermédiaire monte une session IMAP ou SMTP en envoyant l'Access Token à l'Opérateur
6. L'Opérateur contacte PSC sur le endpoint Userinfo pour récupérer à partir de l'Access Token la valeur de l'IdNat présent dans le champ SubjectNameID
7. Le maintien de la connexion auprès de PSC est assuré par le serveur intermédiaire grâce à l'envoi du Refresh Token

Seules les étapes 5 et 6 impliquent directement le serveur de messagerie.

Que le protocole utilisé soit IMAP ou SMTP, une cinématique précise décrite ci-dessous doit être respectée par le système afin que les conditions de sécurité soient réunies et que la logique d'usage de l'Access Token soit correctement appliquée lors de l'authentification du LPS.

EX_LPS_0900

Lors d'une demande d'ouverture de connexion SMTP ou IMAP par un LPS sur l'interface BAL personnelle ou organisationnelle, le système DOIT :

1- Ouvrir la session TLS avec STARTTLS comme défini dans les RFC 3207 et RFC 2246

2- Décoder la chaine de caractères en base64 envoyée par le client à la suite du mot clé AUTHENTICATE XOAUTH2 pour IMAP et AUTH XOAUTH2 pour SMTP

3- Extraire l'adresse de la BAL du champ « user » de la chaine décodée

4- Décoder la chaine de caractères en base64 correspondant à l'Access Token au format Json Web Token récupérée du champ « auth » en supprimant les caractères ^A^A de la chaine décodée à l'étape 2.

5- Vérifier que l'Access Token a bien été signé par PSC grâce à la clé publique exposée par ce dernier (cf [PSC-MOT-FI] : endpoint "jwks_uri").

6- Vérifier que l'Access Token n'a pas expiré grâce aux champs « exp » et « iat »

7 - Interroger le endpoint UserInfo PSC avec l'Access Token pour récupérer l'IdNat au moyen du champ SubjectNameID (cf. [PSC-MOT-FI] : endpoint « UserInfo »)

8- Vérifier que l'idNat récupéré du champ SubjectNameID correspond à l'identité d'une personne physique habilitée à accéder à la BAL

9- Traiter la commande SMTP ou IMAP reçue

Exemple de chaine de caractère reçue à l'étape 2 :

```
user=jean.dupond@medecin.mssante.fr^Aauth=Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJBV19DTUZjaUYtQUMyeGlTdHUtNiIsImF1ZC
I6WyJzZzQ4Q2RBWW9oUlBlUldaOWoxSCJdLCJhdXRoX3R5cGUiOiJwYXNzd29yZCIsIm5ld191c2VyIjp0c
nVlLCJlbWFpbF92ZXJpZmllZCI6ZmFsc2UsInVwZGF0ZWRfYXQiOiIyMDIwLTAxLTIwVDA5OjAyOjI1Ljk1
NVoiLCJjdXN0b21fZmllbGRzIjp7fSwiYXV0aF90aW1lIjoxNTc5NTEwOTQ1LCJpc3MiOiJodHRwczovL2x
vY2FsLXNhbmRib3gub2c0Lm1lIiwiZXhwIjoxNTc5NTk3MzQ1LCJpYXQiOjE1Nzk1MTA5NDUsImVtYWlsIj
oiZ2l2ZXJhbmRvbXRva2VuNEByZWFjaDUuY28ifQ.kR0RRpNi4gFPUEOwuR1Tilx4imYjM1Owrbrtw6liZv
0^A^A
```

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

Exemple d'Access Token décodé à l'étape 4 :


```
{"exp": 1645026147, "iat": 1645026087, "auth_time": 1645026087, "jti": "be31bf33-b8af-42f3-981c-9566922ffa40", "iss": https://auth.bas.esw.esante.gouv.fr/auth/realms/esante-wallet, "sub": "f:550dc1c8-d97b-4b1e-ac8c-8eb4471cf9dd:00B6093351", "typ": "Bearer", "azp": "ans-poc-bas-psc", "nonce": "yYUp49y5xET1cUcEq9MdHNzQkGv_KMqE0IXuXISoSmA", "session_state": "96c91507-4f4c-4aad-9fa6-6f78b466d5c8", "acr": "eidas2", "scope": "openid profile email scope_all", "sid": "96c91507-4f4c-4aad-9fa6-6f78b466d5c8", "email_verified": false, "preferred_username": "00B6093351"}
```


Cette cinématique est illustrée par la figure suivante :

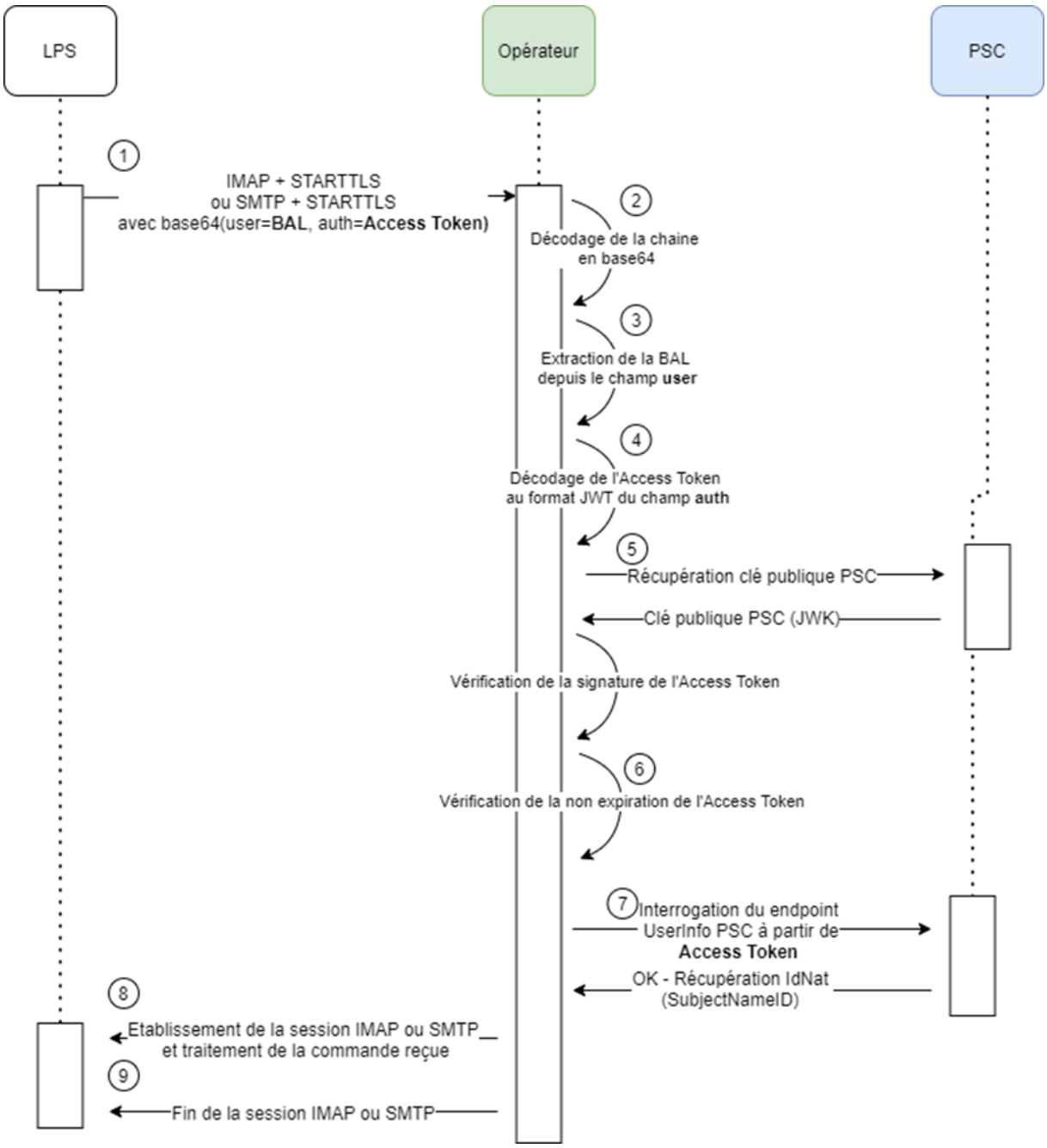


Figure 36 : Cinématique de connexion de l'API LPS avec MIE access token PSC

Comme l'indique cette figure, le système de l'opérateur doit autoriser un flux sortant vers PSC, à la fois pour récupérer la clé publique de PSC nécessaire à la vérification de la signature de l'access token, mais également pour procéder à la récupération de l'IdNat au moyen du endpoint UserInfo.

EX_LPS_910
L'opérateur DOIT autoriser un flux sortant de type Web HTTP sécurisé de son système vers PSC, en paramétrant son infrastructure technique de façon adéquate.

Toujours dans le but de sécuriser la connexion, une durée de vie maximale de la session SMTP / IMAP doit être paramétrée au niveau du serveur de messagerie de l'Opérateur.

EX_LPS_1000
Le système DOIT mettre fin à la session IMAP ou SMTP au bout de : - 15 minutes sur inactivité du LPS (*) - 4 heures sinon

(*) Toute commande IMAP ou SMTP reçue par l'opérateur sur une BAL donnée a pour conséquence de réinitialiser la durée d'inactivité.

Les valeurs de ces durées maximales de session ont été choisies pour correspondre aux durées de vie des sessions Web de PSC (cf. https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/documentation-technique)

Cette session peut bien sûr être interrompue sur demande du LPS lui-même.

Pour garantir une continuité de service, en cas d'indisponibilité de PSC, chaque Opérateur peut fournir un moyen alternatif d'identification permettant aux PS de se connecter à leur BAL.

RE_LPS_0100 
Afin de proposer aux professionnels un accès à sa BAL MSSanté, y compris lors d'une indisponibilité du fournisseur d'identité national (PSC), le système PEUT proposer une méthode d'authentification alternative non dépendante de PSC conforme au référentiel d'identification électronique de la PGSSI-S..

Aucune solution technique n'est précisée de façon à laisser les Opérateurs libres de mettre en place la solution qu'ils souhaitent. A titre indicatif, il est par exemple possible de mettre en œuvre une authentification sur base d'un TOTP (Time-based One–Time Password) sans enrôlement préalable du professionnel.

6.8.5 TM5.4P – Emission et consultation de messages d'une BAL applicative via API LPS

6.8.5.1 Transaction

Les protocoles de l'API LPS sont :

- SMTP pour l'envoi de message,
- IMAP version 4 pour la consultation des messages.

Le moyen utilisé pour s'authentifier via l'API LPS sur une BAL applicative est un certificat de l'IGC Santé permettant d'authentifier une structure (établissement, …). Le DN d'un tel certificat est de la forme :

CN=Authentification MSS, OU=<IdNatStruc>, O=<NomStruc>, ST=<département> (XX), C=FR

Avec CN un libellé informatif, non contrôlé.

Les procédures de commandes de certificats sont disponibles sur le site de l'ANS en fonction du type de structure et sont similaires à celles utilisées pour le DMP : https://esante.gouv.fr/produits-services/certificats-logiciels.

L'opérateur doit s'assurer que le client transmet un certificat AUTH_CLI qui identifie la structure à laquelle est associée la BAL applicative. Cad que l'IdNat contenu dans le champ OU du certificat est bien associé à la BAL contenue dans la commande login IMAP ou SMTP.

Tout certificat identifiant la structure avec cet IdNat peut être utilisé pour accéder aux différentes BAL applicatives de la structure.

E

EX_LPS_1100

Si le système propose des BAL applicatives, ALORS il DOIT permettre à une structure identifiée dans l'annuaire santé de se connecter à une BAL applicative en IMAP et SMTP en présentant un certificat ORG AUTH-CLI issu de l'IGC Santé.

6.8.5.2 Cinématique

Que le protocole utilisé soit IMAP ou SMTP, la cinématique ci-dessous doit être respectée par le système afin que les conditions de sécurité soient réunies et que la logique d'usage du certificat soit correctement appliquée lors de l'authentification.

EX_LPS_1200

Si le système propose des BAL applicatives, ALORS il DOIT, lors d'une demande d'ouverture de connexion SMTP ou IMAP par un LPS sur l'interface BAL applicative :

1- Vérifier le certificat ORG AUTH_CLI présenté par le client de messagerie comme défini dans la RFC 2246 (https://datatracker.ietf.org/doc/html/rfc2246). Dont en particulier la conformité à l'AC, la non expiration et la non révocation.

2- Monter la session TLS

3- Extraire l'adresse de la BAL dans le login de la méthode d'authentification PLAIN comme défini dans la RFC 3501 (https://datatracker.ietf.org/doc/html/rfc3501)

4- Extraire du DN du certificat, le champ OU contenant l'idNat de la structure

5- Vérifier que la BAL applicative, dont l'adresse a été récupérée à l'étape 3, est rattachée à l'IdNat de la structure contenu dans le champ OU du DN du certificat.

6- Traiter la commande SMTP ou IMAP reçue

6.8.6 TM5.5A – Autre interface avec les LPS

Pour la connexion des LPS, l'Opérateur peut proposer une autre interface en complément de l'API LPS. Cette souplesse est introduite pour permettre aux Opérateurs :

- De continuer à proposer des interfaces historiques existantes le temps de la bascule des LPS sur l'API LPS.
- De s'adapter à des contraintes spécifiques où l'API LPS :
  - ne peux pas être supportés par les clients de messageries utilisés (cas dde'Outlook utilisé avec Exchange)
  - n'est pas nécessaire à l'interopérabilité, cad lorsque l'Opérateur maitrise le LPS utilisé.

RE_LPS_0200
Le système PEUT proposer, en complément de l'API LPS, des interfaces avec des LPS qui lui seraient spécifiques afin de s'adapter à des contraintes d'un client particulier qui ne pourrait utiliser l'API LPS commune MSSanté. Dans ce cas, l'Opérateur a la responsabilité de s'assurer que les modalités d'authentification employées sont conformes avec le référentiel d'identification électronique de la PGSSI-S.

6.9 Autres exigences applicables

Au-delà de la mise en œuvre de transactions techniques permettant l'émission, la réception des messages et les actions de publication des BAL, des exigences portant sur les Opérateurs MSSanté peuvent avoir une incidence sur les aménagements à réaliser par les Opérateurs sur leurs services MSSanté.

6.9.1 Synchronisation du temps

EX_SDT_5010  
La date et l'heure de chaque matériel et système d'exploitation du Connecteur MSSanté doivent être synchronisées sur une source de temps fiable : le Connecteur MSSanté doit être en capacité de synchroniser son heure, pour l'horodatage des traces.

Ce prérequis est général pour la mise en œuvre d'un service de messagerie MSSanté, indépendamment des transactions choisies par le candidat.

A titre d'exemple, un pool de serveurs de temps français utilisable est : fr.pool.ntp.org.

Remarque : quel que soit le serveur de temps utilisé par le Connecteur MSSanté, la vigilance du candidat est attirée sur la nécessaire attention à porter aux conditions d'utilisation, aux conditions tarifaires et aux SLA du serveur.

6.9.2 Gestion des traces

EX_GDT_5010


L'Opérateur MSSanté doit prévoir un dispositif capable de tracer les actions d'utilisation et d'exploitation du service MSSanté. Ces traces doivent être conservées afin de pouvoir être rendues accessibles à des personnes autorisées afin de :

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

EX_GDT_5020


Les utilisateurs finaux et les administrateurs de l'Opérateur doivent être informés de la génération de traces de leurs actions par le service MSSanté.

Traces fonctionnelles

Les traces fonctionnelles sont les traces d'utilisation du service MSSanté par les utilisateurs du service mis en œuvre par l'Opérateur. Elles englobent notamment les traces de connexion et de déconnexion au service MSSanté (authentification de l'utilisateur ou de l'application). De plus, tout traitement ayant un impact fonctionnel doit générer des traces fonctionnelles (exp : traitement de fermeture de BAL, etc.). Le traitement de l'INS dans le cadre de ces traces sera conditionné par l'entrée en vigueur des textes venant encadrer MES.

EX_GDT_5030


Des traces fonctionnelles doivent être générées par le Connecteur MSSanté pour tous les traitements opérés sur les BAL (Personnelles, Applicatives et Organisationnelles) et leur contenu.

En particulier, en cas de délégation d'une BAL personnelle ou organisationnelle, les actions de délégation doivent être tracées, de même les actions réalisées par les délégataires (envois de message, etc.) doivent être tracées afin de les identifier.

EX_GDT_5040


Chaque action tracée doit préciser le type d'action, l'identité de son auteur dûment authentifié (ou les informations permettant de la déterminer indirectement), les circonstances attachées à cette action (date et heure précise), les moyens techniques utilisés (nature et version de l'OS, navigateur ou client de messagerie), l'adresse réseau local, le contenu de la demande effectuée au système et la réponse fournie par ce dernier (y compris en cas d'échec) et plus généralement toute information utile à la recherche des causes et des effets d'un incident et à la constitution d'un faisceau de preuve. Le contenu des messages eux-mêmes n'est pas tracé.

EX_GDT_5050
Pour les traces concernant l'envoi ou la réception d'un message, le champ « type d'action » inclut les informations suivantes : • Identifiant unique interne du message ; • Adresses email de l'émetteur du message et des destinataires du message ; • Objet du message ; • Le cas échéant, la taille de l'ensemble encodé du message avec les pièces jointes.

EX_GDT_5060
Pour l'étape connexion à une boîte aux lettres, une trace fonctionnelle contient, une information précisant le type d'authentification mis en œuvre, et les informations relatives au type d'action, à l'identité de son auteur, aux dates et heures, aux moyens techniques utilisés (client de messagerie, web services, etc.), à l'adresse réseau.

Traces fonctionnelles et hébergement des données de santé

Conformément à l'exigence EX_GDT_5050, les traces fonctionnelles contiennent entre autres l'objet du message, et de ce fait, peuvent contenir des données de santé à caractère personnel.
L'Opérateur doit ainsi appliquer aux traces fonctionnelles les mêmes mesures que celles appliquées aux autres données de santé à caractère personnel (mesures organisationnelles, mesures techniques, etc.), pour assurer leur sécurité et leur confidentialité.

Traces techniques

Les traces techniques sont les traces des actions assurées automatiquement par le système (système d'exploitation, équipements réseaux et de sécurité (pare-feu par exemple) et par les composants applicatifs (Jboss, Postfix ou Apache par exemple). Elles comportent aussi les actions réalisées par les Opérateurs techniques du système.

Durée de conservation des traces et des données à caractère personnel échangées par les utilisateurs

EX_GDT_5070
Le service MSSanté proposé par l'Opérateur doit prévoir les mécanismes de paramétrages nécessaires pour permettre au responsable de traitement d'être conforme aux durées de conservation des traces et des données à caractère personnel collectées lors des échanges.

Il appartient au responsable de traitement d'un service de Messageries Sécurisées de Santé de définir les règles de durée de conservation des traces et des données à caractère personnel échangées par les utilisateurs du service.

A titre d'illustration, pour la conservation des traces l'autorisation unique relative aux traitements de messageries sécurisées de santé suscitée précisait les éléments suivants :

- En l'absence de règle légale spécifique et en regard à la finalité du service MSSanté, qui ne doit pas être confondu avec le dossier médical de la personne concernée, les

traces fonctionnelles sont conservées pendant une durée de dix ans, durée alignée sur le délai de prescription de l'action en responsabilité médicale[6] ;
- Les traces techniques sont conservées pendant un an ;

S'agissant de la durée de conservation des données à caractère personnel échangées par les utilisateurs, l'ANS rappelle que le service de Messageries Sécurisées de Santé est un média d'échange qui ne saurait être confondu avec un dossier médical. Chaque utilisateur est donc tenu de reporter dans le dossier médical du patient les données de santé utiles à sa prise en charge.

6.9.3 Production et soumission de statistiques d'utilisation

L'ANS met à disposition des Opérateurs deux webservices :
- Webservice de soumission : permet de déposer les fichiers statistiques.
- Webservice de récupération : permet de récupérer un compte rendu de dépôt

La soumission des fichiers statistiques se fait sous forme d'une archive .ZIP.
Lors de la soumission, l'Opérateur peut indiquer une adresse mail lui permettant de recevoir le compte-rendu de dépôt sans devoir interroger le webservice de récupération.

Le compte rendu permet à l'Opérateur de vérifier la bonne soumission et prise en compte de ses fichiers statistiques.

Les informations statistiques en provenance des Opérateurs sont consolidées par l'ANS, en sa qualité de gestionnaire de l'Espace de Confiance MSSanté, afin de fournir une vision globale de l'utilisation du système MSSanté.

Ces 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. Le traitement est mis en œuvre en application de l'article 5, 5° de la loi n°78-17 du 6 janvier 1978 et du RGPD. L'ANS est responsable du traitement des données réalisé à des fins statistiques. L'Opérateur agit donc en qualité de sous-traitant au sens de l'article 4 du RGPD car il collecte les données sur instruction de l'ANS.

Les données à caractère personnel sont conservées sur 2 années afin de répondre à 2 finalités :
- Construire le rapport indicateur d'usage MSSanté mensuel,
- Pour la gestion des contrôles prévus par la réglementation (usage effectif de la messagerie de santé), lesquels conditionnent l'accès aux financements octroyés ; et d'autre part pour la gestion des recours après l'octroi de ces financements.

Les données à caractère personnel sont ensuite anonymisées. Plus d'information dans la partie 6.9.4 Définition des Conditions Générales d'Utilisation (CGU) du service .

Les Opérateurs ont l'obligation de ne pas transmettre de données personnelles relatives aux utilisateurs usagers dans des fichiers de traces transmis à l'ANS à des fins de production des indicateurs de l'Espace de Confiance MSSanté. Dans l'hypothèse où un Opérateur transmettrait malgré tout (cas d'erreur, incident, anomalie) des matricules INS d'utilisateurs

[6] Pour rappel, l'article L. 1142-28 du Code de la santé publique issu de la loi n° 2002-303 du 4 mars 2002 a unifié le délai de prescription de la responsabilité médicale et hospitalière qui variait suivant les contextes juridiques. Désormais, est appliqué un délai unique de dix ans, courant à compter de la consolidation du dommage.

usagers dans ces fichiers, l'ANS met en mettre en œuvre le mécanisme de contrôle suivant : Dès réception d'un fichier indicateurs par l'ANS, les adresses MSSanté rattachées au domaine patient.mssante.fr sont vérifiées. Celles contenant un INS sont purgées et remplacées par l'adresse générique usager@patient.mssante.fr afin qu'aucune donnée patient ne soit conservée par l'ANS et transmise au système de production des indicateurs de l'Espace de Confiance MSSanté.

Cas particulier du traitement d'indicateurs dans le cadre du programme Ségur numérique :

Conformément aux dispositions prévues par les arrêtés des 11 août 2021 et 2 février 2022 relatifs aux dispositifs de financement à l'équipement logiciel mis en œuvre par l'ANS dans le cadre du programme Ségur numérique, des données relatives au fonctionnement de la messagerie MSSanté des professionnels ou établissements participant au programme de financement sont susceptibles d'être communiquées (identifiant de la boite de messagerie et indicateur d'usage permettant d'identifier l'atteinte du seuil d'envoi de 10 messages) à l'ANS ainsi qu'à son opérateur de paiement, l'Agence des services de paiement (« ASP »), aux seules fins de réaliser les contrôles prévus par la réglementation précitée (usage effectif de la messagerie de santé), lesquels conditionnent l'accès au financement octroyé. Les informations susceptibles d'être communiquées dans ce cadre sont strictement limitées à la réalisation de l'opération de contrôle. Elles sont confidentielles et ne sont accessibles qu'aux agents habilités de l'ANS et de l'ASP.

Remarque : Les échanges de messages se font directement entre Opérateurs MSSanté, sans qu'aucun serveur central ne puisse avoir une vision de l'ensemble des messages.

EX_PSU_5010  
L'Opérateur MSSanté doit prévoir un dispositif capable d'enregistrer et de restituer des indicateurs de suivi de l'activité MSSanté.

Sous réserve des dispositions prévues par décret, les échanges entre les professionnels habilités et les usagers auront pour conséquence la présence du matricule INS dans les traces produites par les Opérateurs. Le traitement et la collecte de l'INS étant strictement encadrés[7], l'Opérateur n'est pas autorisé à transmettre l'INS dans les traces envoyées à l'ANS.

EX_PSU_5020  
L'Opérateur MSSanté, avant soumission des indicateurs à l'ANS, devra retirer toute mention de l'INS dans l'adresse de BAL usager afin de le remplacer par le mot clé « usager ».

Exemple :

[7] L'INS est notamment encadré par 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 de décembre 2019.

La BAL « ***123456789012345@patient.mssante.fr*** » deviendra « ***usager@patient.mssante.fr*** ».

6.9.3.1 Production de statistiques d'utilisation

EX_PSU_5810  
Les informations demandées portent sur le mois écoulé, du 1er au dernier jour du mois (chiffres mensuels). L'Opérateur MSSanté doit déposer des fichiers dans une archive .zip sur un serveur via un webservice de soumission. Ces fichiers sont décrits dans les paragraphes ci-dessous. Les fichiers contenus dans les archives déposées seront validés pour vérifier le nom, le format et le contenu de chacun des fichiers. Une fois validé, ils seront intégrés au système de pilotage MSSanté et un compte rendu de bonne réception sera retourné à l'Opérateur MSSanté. L'Opérateur doit transmettre ces indicateurs à l'ANS **dans les cinq premiers jours du mois qui suit** via le webservice de soumission.

Remarque : Afin que ces indicateurs ne soient pas rejetés, le formalisme du fichier déposé doit respecter de façon précise le format explicité. Par exemple, les noms des colonnes ne doivent en aucun cas être renommés, aucune information complémentaire ou commentaire ne doit être rajouté dans les tableaux, le format des dates doit être respecté (notamment pour le mois en MM).

EX_PSU_5820  
L'Opérateur doit exclure des indicateurs mensuels du mois N : - Toutes boites aux lettres suspendues sauf celles au mois N - Toutes les boites aux lettres supprimées sauf celles au mois N - Les boites aux lettres de tests - Les messages d'erreurs de type serveur

6.9.3.1.1 Format du fichier statistiques MSSanté « Echanges »

EX_PSU_5830  
L'Opérateur doit produire le fichier « Echanges » tel que défini dans le paragraphe suivant : • (AAAAMM)_EchangesMSSante_[Domaine].csv NB : Lors d'un envoi de message à un patient, la trace produite dans le fichier EchangesMSSanté ne doit pas contenir l'INS du patient (voir champ DESTINATAIRE dans le tableau ci-dessous)

Le fichier « Echanges » permet de lister l'ensemble des mails envoyés à partir des BAL d'un Opérateur.

Si l'Opérateur a plusieurs noms de domaines déclarés, il déposera un fichier « Echanges » par domaine émetteur.

Dans un fichier « Echanges », il faut renseigner une ligne par destinataire d'un message. Par exemple, si un mail est adressé à plusieurs destinataires, le fichier « Echanges » comportera pour ce mail autant de lignes que de destinataires.

Dans un fichier « Echanges », tout en respectant la règle des destinataires, il faut renseigner une ligne par message envoyé avec succès. Par exemple, un message rejoué plusieurs fois avant un envoi réussi, le fichier « Echanges » comportera pour ce mail une seule ligne (si un seul destinataire ou plusieurs si plusieurs destinataires).

Dans un fichier « Echanges », il faut renseigner une ligne pour un mail ayant reçu un message d'erreur du serveur de destination (si un seul destinataire ou plusieurs si plusieurs destinataires).

Le tableau ci-dessous liste les attributs et l'ordre attendu pour le fichier (AAAAMM)_EchangesMSSante_[Domaine].csv :

Titre	Description	Type	Longueur	Format
MAIL_ID	Identifiant unique du mail	Alphanumérique	255	Sans Objet
EXPEDITEUR	Adresse mail de l'expéditeur (appartenant à l'un des domaines de l'Opérateur produisant les indicateurs) S'il s'agit d'une BAL patient au format <INS>@patient.mssante.fr Remplacer l'INS par une chaine fixe : « usager@patient.mssante.fr »	Alphanumérique	255	Format mail
DESTINATAIRE	Adresse mail du destinataire. S'il s'agit d'une BAL patient au format <INS>@patient.mssante.fr Remplacer l'INS par une chaine fixe : « usager@patient.mssante.fr »	Alphanumérique	255	Format mail
DATE	Date d'envoi du mail	Date	19	AAAA-MM-JJ HH:mm:SS
TAILLE	Taille totale du mail échangé	Octet	NA	Entier
INS	Valeur issue de l'entête SMTP X-MSS-INS du message ('O', 'N') Indique la présence d'un INS qualifié à l'intérieur du document structuré	Alphanumérique	1	
CODECDA	Valeur issue de l'entête SMTP X-MSS-CODECDA Précise le type du ou des documents structurés véhiculés	Alphanumérique	255	
NIL	Valeur issue de l'entête SMTP X-MSS-NIL Numéro d'identification unique du client de messagerie	Alphanumérique	255	

Tableau 46 : Liste des attributs pour le fichier de statistiques MSSanté « échanges »

Exemple de fichier « echange »

```
MAIL_ID;EXPEDITEUR;DESTINATAIRE;DATE;TAILLE;INS;CODECDA,NIL
1256321;ans@mssante.fr;ans-2@mssante.fr;2020-08-11 14:55:40;21;O;34112-3;<idEditeur/idLogiciel/idVersion>

2257301;ans@mssante.fr;ans-4@mssante.fr;2020-07-12 07:36:12;92;N;34112-3,PRESC-BIO,15508-5;<idEditeur/idLogiciel/idVersion>
```

Les valeurs des colonnes INS, CODECDA et NIL seront respectivement alimentées par les entêtes SMTP *X-MSS-INS*, *X-MSS-CODECDA* et *X-MSS-NIL* du message véhiculé. Ces valeurs étant renseignées par le client de messagerie à l'origine du message.

En cas d'absence d'une ou plusieurs des entêtes précités, la ou les colonnes du fichier « échange » devront être vides.

Aucun traitement n'est exigé sur les valeurs récupérées des LPS via les entêtes SMTP.

Remarque : le Numéro d'Identification Logiciel (NIL) est présent dans les entêtes SMTP des messages MSSanté (hors webmail) afin de renforcer la sécurité de l'Espace de Confiance. Le NIL ouvre la possibilité aux Opérateurs d'identifier le logiciel à l'origine des échanges en cas d'anomalie constatée.

6.9.3.1.2 Format du fichier statistiques MSSanté « Connexions »

EX_PSU_5840 
L'Opérateur doit produire le fichier « Connexions » tel que défini dans le paragraphe suivant : • (AAAAMM)_ConnexionsMSSante_[Domaine].csv

Le fichier « Connexions » permet de lister l'exhaustivité des BAL d'un domaine de l'Opérateur tout en renseignant la date de dernière connexion à cette boite aux lettres.

Si l'Opérateur a plusieurs noms de domaines déclarés, il déposera un fichier « Connexions » par domaine émetteur.

Dans un fichier « Connexions », il faut renseigner une ligne par BAL créée sur le domaine.

Si l'utilisateur ne s'est jamais connecté à sa BAL, une ligne doit être renseignée dans le fichier connexions avec l'attribut « BAL » renseigné et l'attribut « DATE_DERNIERE_CONNEXION » vide.

Le tableau ci-dessous liste les attributs et l'ordre attendu pour le fichier (AAAAMM)_ConnexionsMSSante_[Domaine].csv:

Titre	Description	Type	Longueur	Format
BAL	Adresse mail	Alphanumérique	255	Format mail
DATE_DERNIERE_CONNEXION	Date de dernière connexion	Date	19	AAAA-MM-JJ HH:mm:SS

Tableau 47 : Liste des attributs pour le fichier de statistiques d'utilisation MSSanté « connexion »

Exemple de fichier « connexion »

```
BAL;DATE_DERNIERE_CONNEXION
Ps_user@ch-sud.mssante.fr;2020-08-11 14:55:40
```

EX_SSU_5800

Le fichier Connexion doit contenir l'ensemble des boites aux lettres créées par l'Opérateur.

- Si la boite aux lettres a été créée mais n'a jamais été consultée, le champ « DATE_DERNIERE_CONNEXION » doit être vide. La valeur « null » n'est pas acceptée.
- Si l'information concernant la date de dernière connexion est indisponible, l'Opérateur doit renseigner la valeur 1900-01-01 00:00:00

Remarque : des exemples de fichiers « echanges » « connexions » que les Opérateurs doivent transmettre à l'ANS sont également disponibles en annexe et correspondent au document de référence DR4 défini au § 9.5.

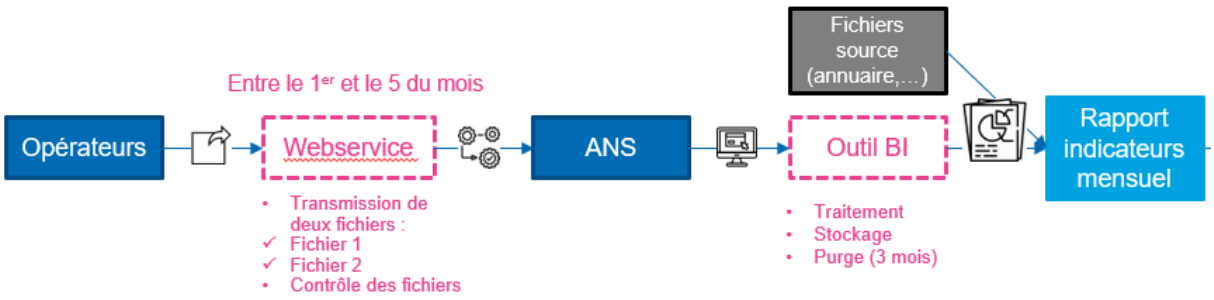
RE_SSU_5800

Pour les BAL applicatives, à défaut de la date de dernière connexion de l'applicatif à la BAL, il est recommandé à l'Opérateur de renseigner la date du dernier échange : envoi ou réception.

6.9.3.2 Soumission des statistiques d'utilisation

L'ANS met à disposition des Opérateurs des webservices permettant de soumettre les fichiers statistiques. Ces webservices permettent le dépôt des fichiers statistiques et la récupération du compte rendu de dépôt.

Ces webservices reprennent les mêmes principes et exigences des webservices Annuaire



Santé décrits dans le § 6.4.2.

EX_SSU_5810
L'authentification mutuelle du Connecteur MSSanté avec le serveur de soumission des statistiques pour les webservices de dépôt et de récupération de compte rendu constitue un prérequis

Le certificat logiciel d'authentification de l'Opérateur MSSanté est aussi utilisé pour l'authentification TLS mutuelle vers le serveur de soumission des statistiques.

Le contrôle d'accès est réalisé par rapport au DN du certificat d'authentification utilisé par le système initiateur. Pour qu'un système soit autorisé à utiliser le Web Service MSSanté avec le serveur de soumission des statistiques, le DN du certificat serveur utilisé doit être référencé dans la liste blanche des domaines autorisés.

Pour soumettre les deux fichiers de statistiques « Echanges » et « Connexions », l'Opérateur MSSanté doit déposer sous forme d'une archive .ZIP sur un serveur via le webservice de dépôt.
Les archives déposées par l'intermédiaire de ce webservice font l'objet d'un traitement qui permet de valider :

- Le nom des fichiers contenus dans l'archive
- Le format des fichiers contenus dans l'archive
- Le contenu de ces fichiers.

Ce traitement génère un compte rendu à disposition de l'Opérateur MSSanté. Ce dernier peut récupérer le compte rendu via un webservice de récupération. Il a également la possibilité de recevoir ce compte rendu par mail. Si l'option de recevoir le compte rendu par mail est choisie (adresse mail renseignée lors de l'appel du webservice de dépôt), la réception du compte rendu est automatique. Il n'est donc pas nécessaire à l'Opérateur d'appeler le webservice de récupération de compte rendu.

Les fichiers validés sont intégrés au système de pilotage de l'ANS à des fins statistiques.

Le tableau ci-dessous présente les webservices de soumission : dépôt et récupération de compte-rendu, et leurs url d'appel en environnement de production.

Webservice	Description	URL
postFile	Nom du webservice pour le dépôt de l'archive	*https://ws-sipil.mssante.fr/sipil/postFile*
getReport	Nom du webservice pour la récupération du compte rendu	*https://ws-sipil.mssante.fr /sipil/getReport*

L'ensemble des codes d'erreurs techniques liés à l'authentification aux webservices, au dépôt des fichiers statistiques ainsi qu'à la récupération du compte rendu par webservice sont listés dans en annexe au paragraphe : $9.7.4 « Codes d'erreurs pour la soumission des fichiers indicateurs »

6.9.3.2.1 Webservice de dépôt de fichiers statistiques

Le webservice de dépôt des fichiers statistiques dispose de deux modes de dépôt :

- Un mode de dépôt pour les archives de moins de 70 Mo, dit « dépôt classique »
- Un mode de dépôt pour les archives dépassant 70 Mo, dit « dépôt de fichiers volumineux »

6.9.3.2.1.1 Dépôt classique de fichiers égaux ou inférieurs à 70 Mo

6.9.3.2.1.1.1 Présentation des flux d'entrée

L'appel du webservice « *postFile* » se fait via l'URL : https://ws-sipil.mssante.fr/sipil/postFile

Exemple :

```
curl [--noproxy "*"] -XPOST --cacert LIST_AC_ELEM_ORG.pem --cert pub.crt --key priv.key -F 'file=@/path/to/file.zip' https://ws-sipil.mssante.fr/sipil/postFile[?email=<email>]
```

Lors de l'appel à ce webservice, la taille maximale de l'archive .ZIP acceptée est de 70Mo.
Il n'existe cependant pas de limite par rapport au nombre de fichiers « echanges » et « connexions » contenus dans l'archive.

Les fichiers contenus dans l'archive doivent tous se trouver à la racine de l'archive et non dans des répertoires.

Lors de l'appel au webservice de dépôt de fichiers statistiques, il est possible de préciser une adresse <email>. Le compte rendu généré par le dépôt sera donc envoyé à l'adresse email indiquée. Cette option pour la réception est préconisée par l'ANS.

6.9.3.2.1.1.2 Présentation du flux en sortie

Le message contient un fichier xml comme l'exemple ci-dessous :

```
<?xml version="1.0" encoding="UTF-8"?>
<Depot xmlns="http://fr/asip/mss/sipil/manager/bean/warehouse">
  <Authentification>
    <Identite>bus.dev.mssante.fr</Identite>
    <Email/>
    <DomainesGeres>
      <Domaine>medecin-dev-mss.svc.meshcore.net</Domaine>
      <Domaine>pharmacien-dev-mss.svc.meshcore.net</Domaine>
      <Domaine>masseur-kinesitherapeute-dev-mss.svc.meshcore.net</Domaine>
      <Domaine>pro-dev-mss.svc.meshcore.net</Domaine>
      <Domaine>sage-femme-dev-mss.svc.meshcore.net</Domaine>
      <Domaine>repondeur-dev-mss.svc.meshcore.net</Domaine>
      <Domaine>infirmier-dev-mss.svc.meshcore.net</Domaine>
    </DomainesGeres>
  </Authentification>
  <Statut>
    <Id>10</Id>
    <NomArchive>10_bus.dev.mssante.fr.zip</NomArchive>
    <CodeRetourGlobal>0</CodeRetourGlobal>
    <Message>Depot de l'archive OK</Message>
  </Statut>
</Depot>
```

Figure 37 : exemple de retour à l'appel du webservice de dépôt de fichier statistique

Si le dépôt est réussi (CodeRetourGlobal = 0), le flux de sortie de l'appel contient un identifiant généré par le service et associé au dépôt.

Cet identifiant se trouve dans l'attribut <*Id*>. Il préfixe également le nom de l'archive .ZIP dans la balise <*NomArchive*>.
Dans l'exemple ci-dessus, l'identifiant est 10. Cet identifiant permettra de récupérer le compte rendu du traitement de l'archive .ZIP par le webservice de récupération. Le fichier compte rendu obtenu sera une archive .ZIP nommée REPORT.ZIP.

6.9.3.2.1.2 Dépôt de fichiers volumineux supérieurs à 70 Mo

Cette méthode de dépôt est à utiliser lors du dépôt d'une archive .ZIP d'une taille supérieure à 70 Mo, sachant que l'archive .ZIP sera rejetée par le mode de dépôt classique.

Elle consiste à segmenter son archive .ZIP en sous-éléments et utiliser un format de requête spécifique pour déposer ses indicateurs, chaque segment représente une division du flux d'octets de l'archive initiale.

6.9.3.2.1.2.1 Présentation du flux d'entrée

L'archive .ZIP doit être segmentée avant d'être déposée, des outils tels que '7zip' ou des scripts peuvent être utilisés pour la segmentation de l'archive .ZIP.

Lors de l'appel au webservice, la taille maximale possible de chaque segment est de 70Mo. Cependant, il est préconisé d'utiliser des segments de 10Mo.

Une fois l'archive .ZIP segmentée, une requête par segment est à effectuer sur l'interface. Ces requêtes doivent elles aussi respecter les contraintes décrites dans le mode de dépôt classique.

L'appel du webservice « *postFile* » se fait via l'URL : https://ws-sipil.mssante.fr/sipil/postFile.

Exemple :

```
curl [--noproxy "*"] -XPOST --header 'File-Part: [NUM_PART]' --header 'Total-File-Parts: [TOTAL]'  --cacert LIST_AC_ELEM_ORG.pem --cert pub.crt --key priv.key -F 'file=@/path/to/file.zip.part1'                                                    https://ws-sipil.mssante.fr/sipil/postFile[?email=<email>]
```

Pour chaque requête envoyée (i.e. chaque segment) les informations suivantes sont nécessaires :

- Un header indiquant le nombre total des segments à déposer :
  - `Total-File-Parts : N`

    **Ce nombre de parties ne peut pas être supérieur à 30.*
- Un header indiquant le numéro du segment envoyé
  - `File-Part : 1..N`

    **Ce nombre de partie ne peut pas être supérieur à la valeur du `Total-File-Parts`.*
- U**ne adresse email**, sur laquelle le compte-rendu de traitement de l'archive est alors communiqué.
  - Cette adresse email est optionnelle.
  - En cas de saisie d'une adresse différente entre deux segments, c'est l'adresse du dernier segment d'archive déposé qui sera prise en compte.

Les dépôts doivent être suffisamment proches dans le temps pour que l'envoi de segments soit considéré comme en cours et que les webservices restent en attente des segments manquants. Au-delà de 12 heures, le dépôt des segments est considéré comme abandonné et est supprimé.

Si le dépôt échoue à une des étapes pour les raisons suivantes :

- Valeur de l'attribut Total-File-Parts dépassant le maximum autorisé (code-retour 6),
- Changement de la valeur de l'attribut Total-File-Parts (code-retour 7),
- Valeur de l'attribut File-Parts supérieure à Total-File-Parts (code-retour 8),
- Délai d'attente dépassé,

Les segments déjà déposés sont supprimés, et l'intégralité du dépôt de l'archive doit être relancé depuis la première requête de dépôt.

Les fichiers contenus dans l'archive .ZIP segmentée doivent tous se trouver à la racine de l'archive et non dans des répertoires.

6.9.3.2.1.2.2 Présentation du flux de sortie

Pour le dépôt d'un segment non final, le message contient un fichier xml comme l'exemple ci-dessous :

```
<?xml version="1.0" encoding="UTF-8"?>
<Depot xmlns="http://fr/asip/mss/sipil/manager/bean/warehouse">
  <Authentification>
    <Identite>bus.dev.mssante.fr</Identite>
    </Email>
    <DomainesGeres>
      <Domaine>infirmier.dev.mssante.fr</Domaine>
      <Domaine>masseur-kine.dev.mssante.fr</Domaine>
      <Domaine>medecin.dev.mssante.fr</Domaine>
      <Domaine>orthophoniste.dev.mssante.fr</Domaine>
      <Domaine>pedicure-podologue.dev.mssante.fr</Domaine>
      <Domaine>pharmacien.dev.mssante.fr</Domaine>
      <Domaine>pro.dev.mssante.fr</Domaine>
      <Domaine>qlf.dev.mssante.fr</Domaine>
      <Domaine>repondeur.dev.mssante.fr</Domaine>
      <Domaine>repondeur2.dev.mssante.fr</Domaine>
      <Domaine>sage-femme.dev.mssante.fr</Domaine>
      <Domaine>social.dev.mssante.fr</Domaine>
    </DomainesGeres>
  </Authentification>
  <Statut>
    <CodeRetourGlobal>4</CodeRetourGlobal>
    <Message>Depot de la partie de l'archive OK : 3</Message>
  </Statut>
</Depot>
```

Figure 38 : exemple de retour à l'appel du webservice de dépôt de fichier statistique

Dans l'exemple ci-dessus, on peut voir que le segment 3 a été déposé avec succès.

Lors du dépôt du dernier segment, le message contient un fichier xml comme l'exemple ci-dessous :

```
<?xml version="1.0" encoding="UTF-8"?>
<Depot xmlns="http://fr/asip/mss/sipil/manager/bean/warehouse">
  <Authentification>
    <Identite>bus.dev.mssante.fr</Identite>
```

```
    </Email>
    <DomainesGeres>
      <Domaine>infirmier.dev.mssante.fr</Domaine>
      <Domaine>masseur-kine.dev.mssante.fr</Domaine>
      <Domaine>medecin.dev.mssante.fr</Domaine>
      <Domaine>orthophoniste.dev.mssante.fr</Domaine>
      <Domaine>pedicure-podologue.dev.mssante.fr</Domaine>
      <Domaine>pharmacien.dev.mssante.fr</Domaine>
      <Domaine>pro.dev.mssante.fr</Domaine>
      <Domaine>qlf.dev.mssante.fr</Domaine>
      <Domaine>repondeur.dev.mssante.fr</Domaine>
      <Domaine>repondeur2.dev.mssante.fr</Domaine>
      <Domaine>sage-femme.dev.mssante.fr</Domaine>
      <Domaine>social.dev.mssante.fr</Domaine>
    </DomainesGeres>
  </Authentification>
  <Statut>
    <Id>31</Id>
    <NomArchive>31_bus.dev.mssante.fr.zip</NomArchive>
    <CodeRetourGlobal>0</CodeRetourGlobal>
    <Message>Depot de l'archive OK</Message>
  </Statut>
</Depot>
```

Si le dépôt du dernier segment est réussi (CodeRetourGlobal = 0), le flux de sortie de l'appel contient un identifiant généré par le service et associé au dépôt.

Cet identifiant se trouve dans l'attribut <Id>. Il préfixe également le nom de l'archive .ZIP dans la balise <NomArchive>.

Dans l'exemple ci-dessus, l'identifiant est 31. Cet identifiant permettra de récupérer le compte rendu du traitement de l'archive .ZIP par le webservice de récupération. Le fichier compte rendu obtenu sera une archive .ZIP nommée REPORT.ZIP

6.9.3.2.2 Webservice de récupération du compte rendu

6.9.3.2.2.1 Présentation du flux d'entrée

L'appel du webservice « *getReport* » se fait via l'URL : https://ws-sipil.mssante.fr /sipil/getReport.

Exemple:

curl [--noproxy ""] -XGET --cacert LIST_AC_ELEM_ORG.pem --cert pub.crt --key priv.key*

https://ws-sipil.mssante.fr /sipil/getReport?id=<id>

Il n'y a pas de délai garanti pour le traitement des fichiers déposés. Le compte rendu est disponible à la fin du traitement de contrôle.
Dans le cas où le compte rendu n'est pas disponible, l'Opérateur MSSanté peut faire une nouvelle tentative 12h après. Si cette nouvelle tentative est en échec, l'Opérateur MSSanté doit contacter l'ANS.
Dans l'appel du webservice de récupération, l'attribut <*id*> correspond à l'identifiant obtenu en sortie du webservice de dépôt. Le fichier compte rendu obtenu sera une archive .ZIP nommée REPORT.ZIP

6.9.3.2.2.2 Présentation du flux de sortie

En sortie, le message contient un fichier compressé d'extension .ZIP contenant un fichier xml « Compte-rendu » avec les balises suivantes :

Balise	**Description**
CompteRendu	
+Authentification	Balise contenant les informations relatives à l'étape d'authentification de l'Opérateur.
++Identite	Nom de l'Opérateur authentifié : CN de l'Opérateur récupéré à sa connexion et sauvegardé en base de données
++Email	Adresse email fournie par l'Opérateur pour l'envoi du CR
++DomainesGeres	Balise contenant l'ensemble des domaines gérés par l'Opérateur authentifié
+++Domaine	Domaine géré par l'Opérateur
+Statut	Cette balise contient le résultat global du traitement de l'archive
++NomArchive	Nom complet de l'archive traitée Il s'agit du nom fourni par l'Opérateur et non du nom préfixé par le traitement.
++Identifiant	Identifiant généré pour l'archive
++CodeRetourGlobal	Code retour global du traitement. Ce code est associé à un référentiel :

	0 = Tous les fichiers de l'archive ont été traités OK ou en Warning 1 = Tous les fichiers de l'archive ont été traités KO 2 = Une partie des fichiers de l'archive sont OK ou en Warning, les autres KO 4 = L'archive n'a pas pu être traitée : Archive vide 5 = L'archive n'a pas pu être traitée : Archive ne pouvant être ouverte 6 = L'archive n'a pas pu être traitée : autre
++Message	Message associé au code retour global du traitement. (*) Cela permet d'indiquer la raison pour laquelle une archive n'a pas pu être traitée : - Archive vide - Archive ne pouvant être ouverte - Autre
+Fichiers	Balise contenant autant de nœud que de fichiers soumis dans l'archive zip soumise.
++Fichier	Balise générique pour l'ensemble des fichiers trouvées. Cette balise peut être présente plusieurs fois
+++InfoTraitement	Informations globales de l'exécution du traitement
++++NomFichier	Nom complet du fichier traité
++++DateDebut	Date de début du traitement Format : dd/MM/AAAA HH:mm:ss
++++DateFin	Date de fin du traitement Format : AAAA-MM-dd HH:mm:ss
++++CodeRetour	Code retour global du traitement. Ce code est associé à un référentiel : 0 = OK 1 = KO 2 = Warning
+++Contrôles	Balise contenant autant de nœud que de contrôles réalisés sur le fichier soumis.
++++Contrôle	Balise générique pour l'ensemble des contrôles réalisés.
+++++CodeContrôle	Code du contrôle réalisé. Ce code est associé à un référentiel. Exemple :

	1 = Contrôle du nom du fichier 2 = Contrôle encodage 4 = Contrôle du séparateur … Le référentiel complet sera fourni dans un document annexe.
+++++CodeRetour	Code retour du contrôle réalisé. Ce code est associé à un référentiel : 0 = OK 1 = KO 2 = Warning
+++++Erreurs	Balise générique pour les erreurs KO ou Warning trouvées. Cette balise peut être présente plusieurs fois.
++++++Message	Message associé au code retour du contrôle réalisé. Il s'agit de la description du problème rencontré de warning ou d'erreur.
++++++LigneErreur	Il s'agit des numéros de ligne sur lesquelles l'erreur ou le warning a été détectée. Le nombre de ligne N remonté en erreur est une limitation ajustable par fichier de configuration. Le séparateur des numéros de ligne en erreur est un espace " ".
+++++DateDebut	Date de début du contrôle réalisé
+++++DateFin	Date de fin du contrôle réalisé

Tableau 48 : structure du fichier xml « Compte rendu »

EX_SSU_5820


L'Opérateur a l'obligation de consulter le compte rendu de soumission. Si le compte rendu indique des erreurs bloquantes, l'Opérateur doit les corriger et soumettre de nouveau les fichiers corrigés dans les délais prévus pour la soumission (les 5 premiers jours du mois).

L'ensemble des contrôles appliqués aux fichiers statistiques sont listés dans en annexe au paragraphe : $9.7.4.4 « Les codes retours appliqués suites aux contrôles des fichiers « Echanges » et « Connexions» »

6.9.3.3 Suppression des fichiers

Les fichiers soumis, traités et générés par le traitement sont conservés trois mois sur le serveur. Tous les fichiers de plus de trois mois sont supprimés quotidiennement.
Sont également supprimés les informations : « identifiant généré x nom de l'Opérateur x adresse email de l'Opérateur » de plus trois mois de la base de données.

6.9.3.4 Arrêt de la soumission des indicateurs d'usage MSSanté au format v1

Il n'est plus nécessaire de soumettre les indicateurs au format v1 à l'ANS par mail. Les indicateurs au format v2 sont désormais adoptés par l'ensemble des Opérateurs présents en Espace de Confiance.

6.9.4 Définition des Conditions Générales d'Utilisation (CGU) du service MSSanté

EX_DCU_5010


L'Opérateur MSSanté doit définir des conditions générales d'utilisation (ou équivalent) pour le service MSSanté qu'il met en œuvre.

A minima, les conditions générales d'utilisation de l'Opérateur doivent contenir les clauses suivantes (dont la forme peut être adaptée aux besoins de l'Opérateur) :

Rappel du contexte juridique :

- Règles de droit commun relatives à l'échange des données de santé à caractère personnel dont les dispositions des articles L 1110-4 et L 1110-12 du code de la santé publique qui précisent les conditions d'échange de données de santé ;
- Règles générales relatives au traitement de données à caractère personnel, et notamment de données de santé, conformément aux dispositions du RGPD et de la loi Informatique et Libertés ;
- L'Opérateur professionnels doit rappeler à l'Utilisateur professionnel qu'il doit respecter le cadre légal qui régit sa profession, en particulier les règles relatives à l'obligation de conserver les données de santé à caractère personnel collectées à l'occasion de l'exercice de sa profession ;
- Préciser que les données de santé à caractère personnel sont couvertes par le secret professionnel dans les conditions prévues à l'article L 1110-4 du code de la santé publique, dont la violation est réprimée par l'article 226-13 du code pénal ;
- L'Utilisateur professionnel est informé qu'il doit traiter l'INS conformément aux dispositions venant encadrer ses conditions d'utilisation et notamment les articles R. 1111-8-1 et suivants du code de la santé publique.

Bon usage de la MSSanté :

- Information des utilisateurs finaux sur les finalités du service MSSanté et les conditions d'utilisation de ses données à caractère personnel ;
- Ajout des mentions d'informations obligatoires conformément aux articles 13 et 14 du RGPD et de la loi Informatique et Libertés ;
- Seuls les professionnels habilités par la loi à échanger des données de santé et, par délégation, les professionnels intervenant dans le système de santé agissant sous leur responsabilité, ainsi que les usagers du système de santé peuvent utiliser le service MSSanté ;
- Le service MSSanté permet les échanges, entre professionnels habilités, de données de santé utiles à la prise en charge d'une personne ainsi que les échanges entre ces professionnels et les usagers du système de santé par le biais de BAL de l'Espace de Confiance MSSanté ;
- Un professionnel habilité à échanger des données de santé peut déléguer l'accès à sa BAL personnelle ou organisationnelle à un professionnel intervenant dans le système de santé agissant sous sa responsabilité (le « Délégataire »), sous réserve du respect des dispositions relatives au secret professionnel et à l'échange et au partage de données de santé.
- Chaque Utilisateur professionnel est responsable des informations qu'il va échanger et partager dans le cadre de son utilisation de la BAL. Il est également responsable des accès qu'il pourrait ouvrir par délégation ou pour toute autre habilitation d'accès à une BAL organisationnelle ou personnelle. Il doit notamment s'assurer que les professionnels qu'il ajoute sont habilités à accéder aux informations relatives aux patients pris en charge.

- L'ouverture de tout nouvel accès à une BAL organisationnelle par un professionnel habilité est conditionnée par l'information, par tout moyen, de l'accord de l'ensemble des professionnels habilités accédant à la BAL.
- Le Délégataire ne peut accéder aux données relatives aux patients que sous la responsabilité d'un professionnel habilité, dans le strict cadre de ses missions et dans le respect des obligations relatives au secret professionnel.
- Toute utilisation abusive par les utilisateurs finaux de la messagerie est interdite (harcèlement, langage abusif, etc.). Dans ce cadre, les utilisateurs finaux s'engagent à ne pas procéder à l'envoi de messages non sollicités à un ou plusieurs destinataires, considéré comme du spam ;
- Les utilisateurs finaux s'interdisent de transmettre par messagerie sécurisée ou par tout autre moyen des courriels contenant des virus ou plus généralement tout programme visant notamment à détruire ou limiter la fonctionnalité de tout logiciel, ordinateur ou réseau de télécommunication ;
- Les utilisateurs finaux s'engagent à ne pas rediriger leur adresse sécurisée vers une adresse de messagerie non MSSanté.
- Les utilisateurs finaux s'engagent à conserver leurs moyens d'authentification dans des conditions garantissant leur sécurité.
- Si l'Opérateur utilise Pro Santé Connect, il doit prévoir qu'en utilisant sa carte CPS ou e-CPS pour se connecter à la messagerie avec Pro Santé Connect l'Utilisateur professionnel s'engage à respecter les obligations qui lui incombent prévues dans les conditions générales d'utilisation des moyens d'identification électroniques (MIE) et de la e-CPS.
- L'Utilisateur professionnel ne doit pas demander la création d'une BAL organisationnelle rattachée à une personne physique s'il exerce dans une structure disposant d'un identifiant FINESS.
- L'Utilisateur professionnel doit veiller à créer des adresses de messagerie avec des dénominations claires, permettant aux autres utilisateurs d'identifier facilement la personne physique ou l'entité titulaire de ces adresses de messagerie.

Publication dans l'Annuaire Santé :

- L'Opérateur professionnels doit annoncer dans ses CGU l'existence de dispositifs permettant à tout Utilisateur professionnel de son service d'indiquer (et de modifier à tout moment) s'il souhaite être inscrit en liste rouge ;
- L'Opérateur professionnels doit également prévoir un moyen permettant à tout Utilisateur professionnel de son service d'être informé que ses données liées à l'usage du système MSSanté sont publiées dans l'Annuaire Santé et consultables par les autres utilisateurs (sauf en cas d'inscription en liste rouge).

Information du patient/usager :

- L'Opérateur professionnels doit préciser qu'en cas d'opposition du patient à l'utilisation du service MSSanté pour échanger des données de santé le concernant, l'utilisateur professionnel devra recourir à un moyen d'échange alternatif (courrier papier par exemple) ;
- L'usager doit être informé sur son droit de s'opposer à l'échange et au partage des données le concernant ;
- L'Opérateur professionnels précise que le service MSSanté ne doit pas être confondu avec le dossier médical de la personne concernée et constitue uniquement un outil d'échange sécurisé de données de santé. Le service MSSanté n'a pas vocation à constituer un espace de stockage sur le long terme ;
- L'Opérateur usagers précise que le service MSSanté ne doit pas être confondu avec le dossier médical de la personne concernée et constitue uniquement un outil d'échange sécurisé de données de santé. Ainsi l'usager s'engage à sauvegarder les documents de santé échangés par le biais du service dans un dispositif de stockage personnel (ex. disque dur, ordinateur, etc.) ou dans son « Dossier médical partagé » ;

- L'Utilisateur professionnel doit reporter dans les dossiers médicaux des patients toute information reçue par messagerie et qu'il jugera utile à la prise en charge de ces derniers ;
- L'Utilisateur usager doit être informé que le service de messagerie sécurisée n'a pas vocation à traiter les situations d'urgence. En cas d'urgence, l'usager doit impérativement composer le numéro 15. En conséquence, la responsabilité du professionnel habilité ne saurait être engagée pour tout préjudice survenu dans le cadre d'une situation d'urgence.

Collecte des données des utilisateurs finaux :

- *Indicateurs d'usage MSSanté*
  L'utilisateur est informé, d'une part, que des données (adresse e-mail, horodatage des échanges, taille des e-mails, présence d'un INS qualifié, présence/type de document structuré, données d'identification, identifiant du logiciel métier utilisé et données relatives à la vie professionnelle) sont collectées, transmises et traitées par l'ANS afin de lui permettre, en tant que gestionnaire de l'Espace de Confiance MSSanté, d'établir des indicateurs anonymes.
  L'ANS est responsable du traitement des données réalisé à des fins statistiques. L'Opérateur agit donc en qualité de sous-traitant au sens de l'article 4 du RGPD. Le traitement est mis en œuvre en application de l'article 5, 5° de la loi n°78-17 du 6 janvier 1978.
  Ce traitement est mis en œuvre dans le cadre de l'exécution d'une mission d'intérêt public dont est investie l'ANS.

- *Transfert d'indicateurs à la Cnam*
  La Cnam est destinataire des données à caractère personnel contenues dans les indicateurs MSSanté aux seules fins d'évaluer l'usage de la MSSanté par les professionnels de santé qui bénéficient de financements conventionnels en faveur de ce déploiement. La Cnam effectuant ledit traitement agit en qualité de Responsable de traitement.
  Ce traitement est mis en œuvre dans le cadre de l'exécution d'une mission d'intérêt public.

- *Indicateurs MSSanté utilisés dans le cadre du Ségur*
  Conformément aux dispositions prévues par les arrêtés relatifs aux dispositifs de financement à l'équipement logiciel mis en œuvre par l'ANS dans le cadre du programme Ségur numérique, des données relatives au fonctionnement de la messagerie MSSanté des professionnels ou établissements participant au programme de financement Ségur sont susceptibles d'être communiquées (identifiant de la boite de messagerie et indicateurs d'usage) à l'ANS ainsi qu'à son opérateur de paiement, l'Agence des services de paiement (« ASP »).

  Ce traitement est réalisé pour la gestion des contrôles prévus par la réglementation précitée (usage effectif de la messagerie de santé), lesquels conditionnent l'accès au financement octroyé.
  Les informations susceptibles d'être communiquées dans ce cadre sont strictement confidentielles et ne sont accessibles qu'aux agents habilités de l'ANS et de l'ASP.
  Ce traitement est mis en œuvre par l'ANS, en qualité de responsable de traitement, dans le cadre de l'exécution d'un contrat.

- *Durée de conservation*
  Les données collectées sont conservées pendant une durée de 2 années, à partir de la date de collecte de la donnée, puis anonymisées.

- *Droit des utilisateurs*

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée et au Règlement européen n°2016/679/UE du 27 avril 2016, l'utilisateur bénéficie d'un droit d'accès, de rectification, d'effacement, d'opposition, portabilité, de limitation, et du droit de définir des directives sur le sort de ses données après sa mort.
Ces droits peuvent être exercés :

- sur demande écrite à l'adresse suivante : GIP Agence du Numérique en Santé - Délégué à la protection des données - 2 - 10 Rue d'Oradour-sur-Glane - 75015 Paris ;
- par messagerie électronique, à l'adresse suivante : dpo@esante.gouv.fr.

L'utilisateur dispose également d'un droit d'introduire une réclamation auprès de la CNIL

Valeur probante :
Prévoir l'acceptation d'une convention de preuve (article 1368 du code civil), par laquelle l'utilisateur final s'engage à ne pas contester la valeur probante des messages électroniques échangés via le système MSSanté sur le fondement de leur nature électronique (article 1366 et suivants du code civil) afin de prévenir d'éventuelles contestations. Cette convention de preuve permettra de s'accorder pour reconnaître la même valeur probante aux écrits électroniques transmis via le système MSSanté qu'aux écrits sur support papier. Les CGU de l'Opérateur MSSanté doivent préciser que leur acceptation a pour conséquence la conclusion d'une convention de preuve.

E

EX_DCU_5030


L'Opérateur doit mettre en œuvre les moyens lui permettant de s'assurer de l'acceptation de ces conditions par tout utilisateur de son service avant l'usage effectif de celui-ci.

A titre d'information, les CGU du service Mailiz proposé par l'Opérateur ANS sont accessibles à l'url suivante : https://mailiz.mssante.fr/cgu.

6.9.5 Exigences complémentaires de sécurité

6.9.5.1 Présentation des orientations de sécurité

L'analyse des obligations réglementaires et des risques SSI à réduire pour le service MSSanté permet de déterminer des orientations pour la sécurité du système qui peuvent être déclinées en objectifs. Ces orientations sont relatives à :

- La protection contre la diffusion abusive des messages et de leur contenu (maîtrise des droits d'échanges entre les abonnés), et contre le détournement de finalité du traitement ;
- La protection du contenu des boîtes aux lettres, messages et pièces jointes, essentiellement en intégrité et en confidentialité, aussi bien dans leur stockage au sein du SI que dans leur transmission sur les réseaux ;
- La sécurité d'accès et d'utilisation du service MSSanté, ce thème concernant le contrôle des accès logiques de l'ensemble des personnes pouvant accéder au service : utilisateurs et personnels de soutien ;
- La protection des ressources techniques et du fonctionnement du service MSSanté, orientée principalement vers la disponibilité et l'intégrité des matériels, des logiciels et des réseaux ;
- La maîtrise de l'organisation globale de la sécurité, au travers d'une politique de sécurité tenue à jour et dont l'application par l'ensemble des acteurs est contrôlée.

6.9.5.2 Présentation des objectifs de sécurité

Les mesures de sécurité mises en place par l'Opérateur doivent répondre aux quatre objectifs suivants :

1. Objectifs de protection contre l'utilisation abusive ou le détournement de finalité de la MSSanté :
   - Respecter les obligations légales et réglementaires ;
   - Responsabiliser les utilisateurs et les exploitants vis-à-vis de la sécurité du contenu des BAL et du service ;
   - Contrôler la diffusion des messages ;
   - Conserver les actions effectuées par les utilisateurs sur leur(s) BAL.
2. Objectifs de sécurité d'accès aux messages et d'utilisation locale du service MSSanté :
   - Contrôler les accès fonctionnels des utilisateurs du service et les accès techniques des exploitants ;
   - Protéger les messages et les pièces jointes en intégrité et en confidentialité durant leur transmission ;
   - Protéger les données stockées par la messagerie contre leur lecture et leur modification ;
   - Contrôler les accès physiques aux machines hébergeant le service MSSanté ;
   - S'assurer que les messages et les pièces jointes ne contiennent pas de codes malveillants (virus, vers, cheval de Troie).
3. Objectifs de protection du fonctionnement de la MSSanté :
   - Protéger le service et les composants logiciels sous-jacents contre les attaques logiques (virus, vers, cheval de Troie) ;
   - Garantir la mise en œuvre et le maintien en condition opérationnelle des composants logiciels sous-jacents ;
   - Surveiller le fonctionnement de la messagerie ;
   - Permettre la poursuite du traitement en cas d'incident majeur.
4. Objectifs de maîtrise de la sécurité du service de messagerie :
   - Faire connaître les engagements de sécurité de la messagerie vis-à-vis d'autres systèmes ;
   - Gérer les incidents de sécurité ;
   - Vérifier régulièrement la conformité et l'efficacité de la sécurité du service MSSanté.

Les exigences ont été triées selon les chapitres de la norme ISO27002. L'ensemble de ces exigences s'applique à tout Opérateur, y compris l'établissement de santé qui devient Opérateur MSSanté pour ses propres utilisateurs.

Analyse des risques :

EX_SSI_5010

Une analyse de risques SSI doit être réalisée lors de la mise en œuvre d'un service MSSanté. Celle-ci doit être actualisée régulièrement et à chaque évolution majeure du **Référentiel #1** pouvant le nécessiter.

EX_SSI_5020

En cas d'incident de sécurité, et en particulier pour ceux liés à une perte d'intégrité ou de confidentialité, l'Opérateur doit informer l'ANS dans les plus brefs délais.

Politique de sécurité :

EX_SSI_5030

La Politique de Sécurité du Système d'Information (PSSI) doit être rédigée pour prendre en compte ce nouveau service. Celle-ci doit être revue à intervalle régulier.
Des audits de la sécurité du système de messageries MSSanté et de son environnement doivent être réalisés à intervalle régulier.

Organisation de la sécurité :

EX_SSI_5040

Les actions de sécurité doivent être coordonnées et pilotées par des responsables désignés. Chaque Opérateur doit désigner un référent de la sécurité qui est l'interlocuteur de l'ANS concernant les questions de sécurité du système.

Sécurité liée aux ressources humaines :

EX_SSI_5050

Les exploitants techniques du service doivent être régulièrement sensibilisés à la confidentialité des informations auxquelles ils accèdent ainsi qu'aux sanctions encourues en cas de divulgation.

Sécurité physique et environnementale :

E

EX_SSI_5060
Les locaux hébergeant les plateformes de production et de secours du SI doivent bénéficier d'un contrôle des accès physiques.

Procédures et responsabilités liées à l'exploitation :

E

EX_SSI_5070
Les opérations d'exploitation importantes sur le SI (migration, restauration de sauvegarde, dans le cadre d'un plan de continuité, etc…) doivent être formalisées dans des procédures dûment explicitées.

Planification et acceptation du système :

E

EX_SSI_5080
La capacité du système mis en œuvre pour le service MSSanté doit être testée, suivie et anticipée.

E

EX_SSI_5085
Tout Opérateur ayant intégré l'Espace de Confiance de production doit mettre en place un mécanisme visant à renouveler avant expiration les certificats IGC Santé exposés dans la liste blanche

Disponibilité du système :

R

RE_SSI_5010
Il est recommandé de mettre en œuvre une infrastructure matérielle qui permet d'assurer la haute disponibilité du service SMTP « entrant », afin de minimiser la perte de messages ou de dysfonctionnements qui pourraient compromettre l'interconnexion avec l'Espace de Confiance MSSanté. Les niveaux de service cibles à atteindre sont les suivants : • Taux de disponibilité : 99,5%, 24x7 • Remise des messages envoyés dans la BAL des destinataires dans un délai maximal de 4 heures

Protection contre les codes malveillants et mobiles :

EX_SSI_5090	 

Le système MSSanté doit mettre en œuvre des mécanismes de détection des intrusions.

Le système MSSanté doit détecter et bloquer les codes malveillants (virus, vers, chevaux de Troie) contenus au sein de tous les flux d'informations entrants (par exemple, messages et pièces jointes) et sortants.

Le système MSSanté doit également alerter les utilisateurs (émetteurs et/ou destinataires) de la mise en quarantaine d'un message et/ou d'une pièce jointe bloqués lors de son envoi ou de sa réception.

Pour plus de précisions concernant le traitement à adopter en cas de messages contenant des pièces jointes infectées, le connecteur MSSanté doit être en capacité de filtrer ces pièces jointes, autant en envoi qu'en réception.

Ainsi, lors de l'envoi ou de la réception d'un message contenant des pièces jointes infectées, le connecteur MSSanté peut au choix :

- Transférer au destinataire le message sans la pièce jointe infectée et informer l'émetteur et le destinataire de la non transmission de cette pièce jointe ;
- Ne pas transférer le message au destinataire et informer l'émetteur que le message ne peut être envoyé pour cause de contenu malveillant détecté dans la pièce jointe.

Gestion de la sécurité des réseaux :

EX_SSI_5100	 

Les serveurs de messagerie doivent s'authentifier mutuellement à l'aide d'un certificat logiciel de personne morale délivré par l'ANS.

L'Opérateur doit suivre les recommandations de sécurité issues des Conditions Générales d'Utilisation (CGU) des moyens d'identification électronique délivrés par l'Agence en Numérique en Santé. Celles-ci sont les suivantes (5.3.2. Engagements des propriétaires de certificat) : « Le propriétaire du certificat garantit, via l'acceptation des présentes CGU et la mise en œuvre d'une politique de sécurité, que des mesures de protection techniques et organisationnelles sont mises en œuvre pour assurer la sécurité des clés privées associées aux certificats émis par l'ANS. Il doit notamment veiller à limiter l'accès à ses clés privées à des personnes dûment autorisées et qu'elles ne puissent pas être dupliquées ni installées dans de multiples équipements ».

Tous les messages électroniques émis et reçus par un Opérateur MSSanté dans l'Espace de Confiance doivent être protégés en confidentialité et en intégrité dans des canaux sécurisés par le protocole TLS.

RE_SSI_5011
Il est recommandé de suivre les guides de bonnes pratiques en matière de sécurisation du service DNS (voir documents [ANSSI-DNS], [ANSSI-NDD] et [ANSSI-GHI]) tant du point de vue du paramétrage que du maintien en condition opérationnelle et de sécurité. Afin de s'assurer de la sécurité des échanges, il est recommandé d'adopter le principe de défense en profondeur (sécuriser les réseaux internes et externes, les équipements, surveiller les systèmes, etc.) en s'appuyant sur le guide d'hygiène établi par l'ANSSI (voir) comme base de départ.

Sauvegarde :

EX_SSI_5110 
Les sauvegardes doivent être testées à intervalle régulier afin de valider l'ensemble du processus de sauvegarde/restauration. Ces tests doivent inclure au moins une restauration de l'ensemble des composants d'un service.

Surveillance :

EX_SSI_5120 
Le service de messagerie doit bénéficier d'un service de supervision configuré pour générer des alertes automatisées sur des événements spécifiés et jugés critiques pour la sécurité du service (disponibilité, intégrité, confidentialité et audibilité). Les exigences concernant les traces sont définies dans le **§ 6.9.2.**

Gestion de l'accès utilisateur :

EX_SSI_5130
Tout Opérateur doit gérer la liste des utilisateurs autorisés à accéder au service et ses évolutions. Chaque utilisateur doit être identifié puis authentifié avec succès, en s'appuyant sur une base des utilisateurs autorisés, avant de pouvoir accéder au service MSSanté.

RE_SSI_5020
Il est recommandé de mettre en œuvre le palier 3 de l'authentification défini dans le Référentiel d'authentification des acteurs de santé de la PGSSI-S.

Les exigences de sécurité concernant la publication de données dans l'Annuaire Santé sont définies dans le **§ 6.3** « Modalités techniques spécifiques aux Web Services de l'Annuaire ». Les exigences de sécurité concernant la liste blanche des domaines autorisés sont définies dans le **§ 6.6** «Liste blanche des domaines MSSanté autorisés »

Contrôle d'accès réseau :

EX_SSI_5140
Les pares-feux protégeant l'infrastructure du SI doivent bénéficier des mécanismes de protection conformes à l'état de l'art.

Contrôle d'accès au système d'exploitation :

EX_SSI_5150
Les outils déployés pour l'administration et/ou l'exploitation du SI doivent mettre en œuvre une authentification des Opérateurs (exploitants, administrateurs).

Remarque : Pour l'administrateur qui accède au système localement ou à partir d'un réseau privé, une authentification par login/mot de passe est acceptable en regard de la PGSSI-S. Des règles pour les interventions à distance sont également précisées dans la PGSSI-S [PG-RG-INT].

Gestion des incidents liés à la sécurité de l'information :

EX_SSI_5160
Le système doit bénéficier d'un dispositif de gestion des incidents de sécurité capable de les détecter, les évaluer et les traiter dans les meilleurs délais.

Obligations légales de signalement

Les incidents graves de sécurité doivent faire l'objet d'un signalement, conformément à l'article L.1111-8-2 du code de la santé publique, sur le portail d'Accompagnement Cybersécurité des Structures de Santé accessible à l'adresse suivante : **https://www.cyberveille-sante.gouv.fr/aide-a-la-declaration-d-un-incident/**.

Remarque : Pour signaler l'incident de sécurité, lors de la première étape, il faut se déclarer en tant que « Professionnel de santé ».

Sont considérés comme graves les incidents de sécurité des systèmes d'information ayant des conséquences :

- potentielles ou avérées sur la sécurité des soins ;
- sur l'intégrité ou la confidentialité des données de santé ;
- sur le fonctionnement normal de l'établissement.

EX_SSI_5165
De plus, conformément aux dispositions des articles 33 et 34 du RGPD, si l'incident de sécurité entraine une violation de données personnelles (divulgation/vol, accès illégitime, altération), l'Opérateur est tenu de notifier l'incident au responsable de traitement et de lui fournir tous les éléments utiles. Ce dernier est dans l'obligation de déposer une déclaration auprès de la CNIL à l'adresse suivante : **https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles**

Conformité :

EX_SSI_5170
Chaque Opérateur doit assurer une veille réglementaire en vue d'assurer la conformité du SI tout au long de son cycle de vie.

6.9.5.3 Gestion des incidents Opérateurs

EX_SSI_5180  
Comme indiqué dans les documents contractuels **les Opérateurs MSSanté présents en Espace de Confiance de production** ont l'obligation de signaler à l'ANS en tant que gestionnaire de l'Espace de Confiance « […] **toute modification, tout dysfonctionnement ou toute anomalie** sur leur service de Messageries Sécurisées de Santé qui aurait un impact sur le bon fonctionnement, la disponibilité ou la sécurité du « système MSSanté » […] dans les vingt-quatre (24) heures qui suivent l'identification du dysfonctionnement ou de l'anomalie.». De même, ils doivent informer l'ANS de tout arrêt temporaire supérieur à 8 jours. Les canaux dédiés pour ces déclarations d'incidents sont : ➢ l'adresse mail : monserviceclient.mssante@esante.gouv.fr ➢ le numéro de téléphone : 0 825 852 000 (Service à 0,06 € / min + prix appel, 24/24 Heures - 7/7 Jours).

<u>Consignes à suivre lors de déclaration d'incidents par les Opérateurs MSSanté</u> :

Les informations utiles sur les démarches à entreprendre auprès de l'ANS par les Opérateurs rencontrant un incident ou une interruption de leur service de messagerie et ce, qu'ils soient en mesure ou non de le résoudre par eux-mêmes, sont indiquée ci-dessous.

Qualifier l'incident **:**
Afin de réduire les délais de traitement, les Opérateurs doivent communiquer des informations précises concernant la qualification de l'incident.

1. La date et heure de détection de l'incident ou d'interruption de service *(programmée ou non)*,

2. La nature de l'incident,
Echec d'émission/réception de messages, téléchargement de la liste blanche, publication / consultation de l'Annuaire Santé, certificats serveur, perte de messages, SPAM / Emetteur non autorisé, téléchargement des extractions de l'Annuaire Santé.

3. Les impacts de l'incident.

Déclarer l'incident :
L'incident doit être déclaré par email ou par téléphone à l'ANS (comme indiqué dans l'exigence ci-dessus).
Lors de sa déclaration, l'Opérateur doit préciser ses coordonnées complètes :
- identifiant de structure *(FINESS Géographique ou SIRET)*,
- raison sociale,
- nom,
- prénom,
- fonction au sein de la structure,
- adresse électronique non sécurisée,
- coordonnées téléphoniques.

7 Vérification de conformité des exigences

7.1 Modalités de vérification de conformité

Comme décrit dans le contrat « Opérateur MSSanté v2 », l'ANS en tant que régulateur de l'Espace de Confiance prévoit 3 dispositifs de contrôle distincts afin de garantir dans les meilleures conditions la conformité des Opérateurs aux exigences du présent référentiel :

EX_MCC_0100


L'Opérateur DOIT se conformer aux modalités de contrôle de conformité définies dans ce paragraphe (§7.1).

	Contrôles de conformité techniques des interfaces	Audit de conformité	Monitoring périodique
Objectif	L'objectif de ces contrôles est de vérifier la conformité des Opérateurs (tests techniques sur les interfaces) aux exigences du Référentiel #1. Cette procédure peut, en fonction du contexte du contrôle, être réalisée sur l'Espace de Confiance de test ou de production.	L'audit de conformité réalisé par l'ANS permet, en complément des contrôles de conformité, d'assurer des vérifications dans l'Espace de Confiance de production qui ne peuvent pas être réalisées via des tests techniques sur les interfaces.	L'ANS réalise un monitoring périodique afin de vérifier régulièrement la bonne configuration et disponibilité des interfaces LPS et Opérateurs de l'ensemble des services de messageries sécurisées de santé présents dans l'Espace de Confiance de production.
Méthodologie / Déroulé	L'ANS peut demander à l'Opérateur de tester la conformité de son service de messageries sécurisées de santé par le biais de l'Outil de tests et de contrôles. L'Opérateur doit se connecter à l'Outil de tests et de contrôles pour jouer l'intégralité des tests techniques sur les interfaces LPS et Opérateurs. L'utilisation de l'Espace de Confiance de test n'implique pas le traitement de données à caractère personnel réelles. Les tests réalisés par l'Opérateur donnent lieu à la production d'un rapport de tests. Le rapport de tests doit être envoyé à l'ANS à l'adresse suivante : monserviceclient.mssante@esante.gouv.fr.	L'audit de conformité s'appuie sur les méthodes suivantes: • Analyse des pièces fournies par l'Opérateur à la demande de l'ANS (et notamment le questionnaire d'audit à renseigner par l'Opérateur); • Visite sur site de l'Opérateur ou de l'hébergeur le cas échéant, donnant lieu à des entretiens avec le personnel de l'Opérateur ; • Tests techniques sur les interfaces de l'Opérateur. L'ANS, dans le cadre de la présente procédure d'audit, n'accède pas aux données de santé des utilisateurs finaux du service de messageries sécurisées de santé de l'Opérateur. Le détail de la méthodologie de l'audit est précisé dans le	L'ANS effectue des requêtes non intrusives (pas de test d'intrusion ou de charge) envoyées sur les interfaces LPS et Opérateurs de production, mais aussi sur les DNS et la liste blanche. Cette action ne nécessite pas d'intervention de l'Opérateur et n'implique pas le traitement de données à caractère personnel des utilisateurs finaux du service de messageries sécurisées de l'Opérateur.

	Contrôles de conformité techniques des interfaces	Audit de conformité	Monitoring périodique
	Pour plus de précisions se reporter à la documentation de l'outil disponible sur le site mssante.fr.	programme d'audit transmis à l'Opérateur lors de la notification adressée par courrier recommandé à l'Opérateur. L'audit donne lieu à la production d'un rapport par l'ANS.	
Fréquence	Ces contrôles sont obligatoires dans les cas suivants : - avant l'entrée dans l'Espace de Confiance de production. L'Opérateur dispose d'un délai de 6 mois à compter de son entrée dans l'Espace de Confiance de test pour produire son rapport de tests et le transmettre à l'ANS ; - à chaque mise à jour majeure du Référentiel #1. L'Opérateur présent dans l'Espace de Confiance de production doit produire le rapport de tests dans le respect du délai de mise en conformité précisé au §1.5. Outre les contrôles obligatoires, l'ANS peut à tout moment demander à l'Opérateur de tester à nouveau la conformité de son service de messageries sécurisées de santé aux exigences du Référentiel #1, notamment en cas de suspicion d'anomalie. L'Opérateur dispose alors après notification par tout moyen, d'un délai de cinq (5) jours ouvrés pour transmettre le rapport à l'ANS.	Non systématique. Leur planification est réalisée à l'initiative de l'ANS. Ces contrôles se déroulent à une date convenue entre l'ANS l'opérateur, sous réserve d'un préavis minimum de quinze (15) jours ouvrés et de la transmission à ce dernier du programme d'audit. .	La fréquence pourra varier en fonction des besoins de l'ANS (pas plus d'une ou deux requêtes par jour).
Conclusion du rapport	L'Outil de tests et contrôles permet de produire un rapport de test qui doit être communiqué à l'ANS. Le rapport de tests fait ensuite l'objet d'un contrôle par l'ANS. Dans le cadre de la procédure d'intégration à l'Espace de Confiance, deux scénarios sont possibles après ce contrôle : o l'ANS valide le rapport de tests, et l'intégration à l'Espace de Confiance de production peut être effectuée ; o l'ANS ne valide pas le rapport de tests, l'Opérateur est alors	Dans un délai maximal de 60 jours à compter de la fin du contrôle, et plus précisément de la réception par l'ANS de l'ensemble des pièces, de la réalisation des entretiens et à l'issue d'un échange contradictoire et de la validation des constats, l'ANS produit un rapport d'audit dont elle adresse une copie par courrier recommandé à l'Opérateur. Il n'est pas rendu public. Il précise les conclusions de l'ANS. Elles peuvent contenir les éléments suivants en fonction de la décision retenue : les points positifs, les non-conformités et les risques	Les rapports de monitoring produits par l'ANS lui permettront de se rapprocher des Opérateurs concernés par les non-conformités et déclencher au besoin des contrôles ou audit de conformité complémentaires. Les non-conformités peuvent conduire au déclenchement des procédures de contrôles décrites au présent chapitre.

	Contrôles de conformité techniques des interfaces	Audit de conformité	Monitoring périodique
	renvoyé vers l'Espace de Confiance de test afin produire un nouveau rapport de tests et le transmettre à l'ANS ; L'ANS notifie sa décision de validation ou d'invalidation à l'Opérateur par courrier électronique. Les non-conformités détectées en Espace de Confiance de production déclenchent le mécanisme de sanction décrit au §7.2	associés, les recommandations de l'ANS et le verdict final de conformité ou non-conformité. Les non-conformités détectées en Espace de Confiance de production déclenchent le mécanisme de sanction décrit au §7.2	

7.2 Sanctions en cas de non-conformité

Tout Opérateur présent dans l'Espace de Confiance de production, s'expose à des sanctions graduées en cas de non-conformités aux exigences du Référentiel #1 applicables constatées dans le cadre de la procédure de contrôle décrite au §7.1.

La procédure de sanction est engagée après mise en demeure préalable, envoyée à l'Opérateur par courrier recommandé avec accusé de réception, de se mettre en conformité avec le Référentiel #1. La mise en demeure précise les non-conformités constatées, les sanctions encourues ainsi que le délai dont dispose l'Opérateur pour se mettre en conformité.

Les sanctions graduées applicables sont les suivantes :

1. La diffusion publique (sur le site mssante.fr et/ou esante.gouv.fr) de la non-conformité au Référentiel #1 constatée par l'ANS à l'issu de la procédure de contrôle ;

2. Interdiction pour l'Opérateur professionnels de déclarer de nouvelles BAL dans l'Annuaire Santé et de déclarer de nouveaux domaines dans l'Espace de Confiance ;

3. La mise en œuvre de la procédure de résiliation prévue à l'article 14 du contrat « Opérateur MSSanté v2 ». L'ANS se réserve le droit de suspendre le service de l'Opérateur professionnels avant résiliation du contrat ;

Ci-dessous la cinématique de la mise en œuvre des sanctions graduées :

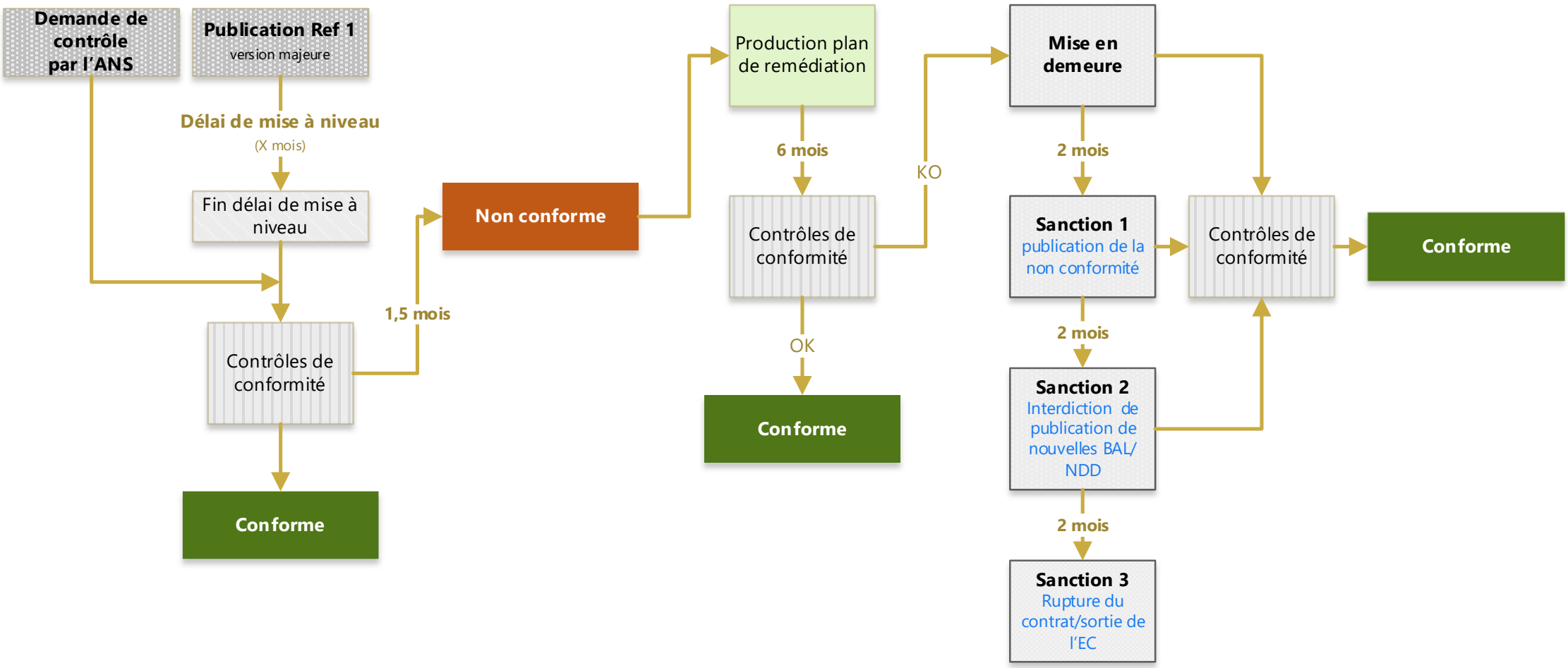


Figure 39 : Etapes et délais processus de mise en conformité et sanctions

Dès la mise en demeure, l'Opérateur peut à tout moment faire parvenir un rapport de test à l'ANS à l'adresse monserviceclient.mssante@esante.gouv.fr . Si validation du rapport, la ou les sanctions en cours seront levées dans un délai maximal de 7 jours.

8 Synthèse des exigences applicables aux Opérateurs MSSanté

Les exigences applicables aux Opérateurs sont définies dans les différents chapitres de ce dossier de spécifications fonctionnelles et techniques.

Les exigences ajoutées ou modifiées dans cette version sont surlignées en jaune ci-dessous.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
Générale	1.6	EX_GEN_0100	Pour chaque nouvelle version majeure du Référentiel #1, tous les Opérateurs présents dans l'Espace de Confiance de production doivent démontrer leur conformité à la dernière version du Référentiel #1 publié, par le biais de l'Outil de tests et de contrôles, dans le respect du délai de mise en conformité précisé dans le Référentiel #1. La mise en conformité de l'Opérateur est vérifiée par l'ANS à travers les résultats de ce rapport de tests conformément à la procédure de contrôle définie à chapitre 7.1
	3	EX_GEN_0200	Tout nouvel Opérateur doit respecter les conditions et modalités d'utilisation de la procédure d'intégration à l'Espace de Confiance MSSanté décrite dans le présent chapitre. L'Opérateur doit intégrer dans un premier temps l'Espace de Confiance de tests qui est dédié à la mise en conformité de son service de Messageries Sécurisées de Santé avec les exigences du Référentiel #1. Suite à un contrôle de conformité, l'Opérateur ayant démontré sa conformité aux exigences du Référentiel #1 en vigueur peut intégrer l'Espace de Confiance de production.
Gestion des boites aux lettres au sein de l'Espace de Confiance MSSanté	5.1.1	EX_GBM_3010	Un Opérateur DOIT proposer à ses utilisateurs finaux des BAL personnelles ou des BAL organisationnelles ou les 2 types de BAL. En complément l'Opérateur peut de façon optionnelle proposer des BAL applicatives.
	5.1.1.2	EX_GBM_3020	Pour une structure disposant d'un FINESS : L'Opérateur doit rattacher dans l'Annuaire Santé la BAL organisationnelle à la structure en renseignant les informations suivantes : typeBAL "ORG" ; TypeIdentifiantPM ; IdentifiantPM. La déclaration par l'Opérateur de la liste des cotitulaires de la BAL dans l'Annuaire Santé n'est pas possible.
	5.1.1.2	EX_GBM_3030	Pour une structure libérale ne disposant pas de FINESS : L'Opérateur doit rattacher dans l'Annuaire Santé la BAL organisationnelle au numéro RPPS du Responsable opérationnel en renseignant les informations suivantes : typeBAL "CAB" ; TypeIdentifiantPP ; IdentifiantPP. Lorsqu'un ou plusieurs Cotitulaires accèdent à la BAL, l'Opérateur a l'obligation de déclarer dans l'Annuaire santé la liste des Cotitulaires de la BAL (limitée à 20 dont le responsable opérationnel).
	5.1.1	EX_GBM_3040	L'Opérateur DOIT communiquer auprès des utilisateurs finaux uniquement via les dénominations des 3 types de BAL du Référentiel #1 : personnelle, organisationnelle, applicative.
	5.1.1	EX_GBM_4000	Les boites aux lettres de test doivent comporter dans leur dénomination la mention « test ». La dénomination d'une boîte aux lettres de tests ne doit pas comporter de données à caractère personnel (nom, prénom, etc.)

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
	5.1.1	**EX_GBM_4010**	Les boites aux lettres de test ne doivent ni émettre ni recevoir des données à caractère personnel et des données de santé. Elles ne sont autorisées à échanger qu'avec : • Les boites aux lettres de test appartenant aux domaines de l'Opérateur • Les boites aux lettres de test des autres domaines
	5.1.1	**EX_GBM_4020**	Chaque Opérateur doit mettre à disposition une boite aux lettres de réponse automatique par nom de domaine qu'il gère dans la liste blanche en respectant le nommage suivant : reponse.automatique-test@<domaineoperateur>.mssante.fr
	5.1.1	**EX_GBM_4030**	Les messages contenus dans la boite aux lettres de réponse automatique doivent être supprimés au maximum un mois après leur réception.
	5.2	**EX_GBM_4200**	L'Opérateur doit s'assurer que les BAL MSSanté personnelles sont exclusivement utilisées sous la responsabilité du professionnel habilité ou de l'utilisateur usager titulaire de cette BAL (ou de son représentant légal)
	5.2	**EX_GBM_4220**	Le professionnel déclaré comme Responsable opérationnel d'une BAL Organisationnelle ou Applicative doit être : - être un professionnel identifié dans l'Annuaire Santé ou par un fournisseur d'identité local ; - lorsqu'il accède au contenu de la BAL, être un professionnel habilité par la loi à échanger des données de santé conformément aux dispositions de l'article L. 1110-4 du code de la santé publique ; - lorsqu'il n'accède pas au contenu de la BAL, être représentant légal de la structure, ou de tout professionnel agissant en son nom et pour son compte.
	5.2	**EX_GBM_4230**	L'Opérateur doit tenir une base interne des utilisateurs finaux de son service MSSanté permettant de faire le lien entre les BAL personnelles et organisationnelles MSSanté de ses domaines et ses utilisateurs finaux.
	5.3	**EX_GBM_4300**	L'Opérateur DOIT utiliser des formats d'adresses de messagerie qui respectent les conditions suivantes : - la RFC 5321 (https://datatracker.ietf.org/doc/html/rfc5321). - les contraintes de l'Annuaire Santé, à savoir que seuls les caractères suivants sont autorisés (ne pas prendre en compte les points-virgules) : caractères alphanumériques ; . ; _ ; - ; +.
	5.3	**EX_GBM_4310**	L'Opérateur ne doit pas décrire une BAL applicative ou organisationnelle avec des informations nominatives relatives à un utilisateur de type personne physique. Il est toutefois possible de recourir à un nom d'organisation ou de structure dans le nommage de la BAL, comme par exemple : • service-cardiologie@xyz.mssante.fr ; • cabinet-dr-martin@xyz.mssante.fr ; • service-pr-dupont@xyz.mssantefr ; • institut-pasteur.secretariat@xyz.mssante.fr.
	5.3	**EX_GBM_4311**	L'Opérateur doit créer les BAL personnelles au format : prenom.nom@<domaineOpérateur>.mssante.fr. Cette exigence

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
			n'est applicable que pour les BAL créées après la mise en conformité au référentiel v1.6. Toutefois l'opérateur peut déroger à cette règle en cas d'homonymie sur un même nom de domaine
	5.4.1	**EX_GBM_4410**	Afin de garantir l'interopérabilité entre systèmes MSSanté, tous les Opérateurs doivent permettre l'échange de messages de taille inférieur ou égale à 10 Mo (pièces jointes encodées comprises). L'Opérateur a la possibilité d'autoriser des échanges de messages de taille supérieure à 10 Mo.
	5.4.1	**EX_GBM_4420**	Afin de minimiser les risques d'émission de messages non sollicités, les Opérateurs doivent limiter le nombre de destinataires d'un message à 40 au maximum.
	5.4.1	**EX_GBM_4430**	L'Opérateur émetteur de messages depuis des BAL applicatives doit s'assurer qu'il est en mesure d'exploiter en réception des messages de type « indicateur d'absence » ou « message de saturation de BAL » afin de pouvoir déclencher les actions appropriées.
	5.6	**EX_GBM_4440**	L'Opérateur doit positionner en liste rouge sur l'Annuaire Santé toute BAL 'personnelle' ou 'organisationnelle' créée depuis plus d'un an et qui n'a pas fait l'objet d'une connexion par un utilisateur final depuis plus de 60 jours consécutifs. Cette action doit être systématiquement précédée, quinze jours avant, d'une information de l'utilisateur par le canal de son choix (hors envoi via l'Espace de Confiance), afin de lui permettre, le cas échéant, de s'opposer à cette dépublication en se connectant de nouveau à sa BAL MSSanté. Les modalités d'envoi de ce message d'alerte, ainsi que le principe de mise en liste rouge, sont portées par tout moyen à la connaissance de l'utilisateur, par exemple dans les conditions générales d'utilisation du service de messagerie sécurisée. La connexion d'un utilisateur final à une BAL mise en liste rouge par ce principe sur l'Annuaire Santé, doit entrainer son retrait de la dite liste rouge, sauf si l'utilisateur avait préalablement explicitement demandé la mise en liste rouge.
	5.4.1	**EX_GBM_5410**	L'Opérateur DOIT mettre à disposition des Cotitulaires d'une BAL organisationnelle, rattachée à un Responsable opérationnel, un dispositif (écran, procédure, ...) lui permettant de modifier les attributs suivants : - d'ajouter / supprimer des Cotitulaires et des Délégataires à la liste des professionnels habilités à accéder à la BAL ; - de modifier le champ "description" de la BAL ; - de changer de « Responsable opérationnel » de la BAL. L'historique de ces actions doit être conservé au titre des traces fonctionnelles (voir §6.9.2).
	5.4.1	**EX_GBM_5411**	L'Opérateur DOIT proposer la fonction de délégation pour toutes les BAL personnelles ou organisationnelles, tel que décrit au §5.4.2 du présent Référentiel #1 Opérateur. Les BAL applicatives ne proposent pas de fonction de délégation.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
	5.4.1	**EX_GBM_5413**	L'Opérateur DOIT proposer aux utilisateurs finaux un dispositif (écran, procédure, ...) de gestion des délégations d'accès (création, consultation, modification, suppression).
	5.4.1	**EX_GBM_5414**	L'Opérateur DOIT permettre aux Délégataires d'accéder aux BAL MSSanté à travers les mêmes interfaces (API LPS, mode d'accès spécifique à l'opérateur, …) que les Responsables opérationnel et Cotitulaires des BAL MSSanté.
	5.7	**EX_GBM_6010**	Le service de Messageries Sécurisées de Santé de l'Opérateur doit comporter un dispositif permettant de supprimer les boîtes aux lettres en cas d'absence d'authentification de l'utilisateur final pendant une période d'un an, conformément aux recommandations de la CNIL. Toute suppression doit être systématiquement précédée, deux mois avant échéance, d'une information de l'utilisateur par le canal de son choix, hors envoi via l'Espace de Confiance, afin de lui permettre, le cas échéant, de s'opposer à cette suppression. Les modalités et le rythme d'envoi de ce message d'alerte sont portés par tout moyen à la connaissance de l'utilisateur, par exemple dans les conditions générales d'utilisation du service de Messageries Sécurisées de Santé.
	5.7	**EX_GBM_6020**	Avant de retirer un nom de domaine de la liste blanche, et donc de l'Espace de Confiance MSSanté, l'Opérateur doit supprimer de l'Annuaire Santé l'ensemble des BAL MSSanté rattachées à ce domaine.
Sécurisation du connecteur Opérateurs MSSanté	**6.2.1**	**EX_OPE_5010**	Le connecteur MSSanté de l'Opérateur DOIT supporter TLS 1.2 (cf. RFC 5246 - http://tools.ietf.org/html/rfc5246)., avec uniquement les suites de chiffrement TLS1.2 suivantes : • 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 Dans le cas contraire, la connexion ne doit pas être établie. Les versions SSLv2, SSLv3 ne doivent pas être activées. La longueur du groupe DH doit être >= 2048 bits ou la longueur du groupe elliptique ECDH doit être >= 256 bits. La confidentialité persistante (PFS - perfect foward secrecy) de DH doit être utilisée (DHE ou ECDHE).
	6.2.2	**EX_OPE_5020**	Le Connecteur MSSanté de l'Opérateur doit initialiser ou accepter les connexions SMTPS uniquement après validation d'un certificat serveur X509 délivré par l'ANS selon la norme PKIX (voir RFC 5280 (http://tools.ietf.org/html/rfc5280), RFC 2246 (http://tools.ietf.org/html/rfc2246), RFC 3207 (http://tools.ietf.org/html/rfc3207) et RFC 2034 (http://tools.ietf.org/html/rfc2034) et ayant une correspondance dans la Liste Blanche (DN du certificat).

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
	6.2.2	**EX_OPE_5030**	Sur l'interface SMTPS, les connecteurs de messagerie MSSanté des Opérateurs doivent gérer la chaîne de certification de l'IGC-Santé gamme Elémentaire.
	6.2.2	**EX_OPE_5040**	Les certificats utilisés par les serveurs de messagerie des Opérateurs MSSanté DOIVENT être issus de la branche gamme Elémentaire / domaine Organisation de l'IGC Santé. Les certificats racines et intermédiaires de cette branche sont donc nécessaires pour valider les certificats serveurs. Ils doivent être récupérés sur le site http://igc-sante.esante.gouv.fr/PC/#ca, et déployés dans le magasin de confiance du Connecteur MSSanté de l'Opérateur.
	6.2.2	**EX_OPE_5050**	Le Connecteur MSSanté de l'Opérateur DOIT faire un contrôle de non révocation des certificats serveurs présentés par les Opérateurs distants de messagerie MSSanté.
Emission de messages MSSanté	**6.7.2**	**EX_3.2_5040**	Un Opérateur MSSanté ne doit pas utiliser le serveur SMTP d'un autre Opérateur MSSanté comme relai de messagerie.
	6.7.2	**EX_3.2_5020**	L'émission de messages est effectuée sur le protocole SMTP, dans une session TLS mutuelle avec le Connecteur MSSanté destinataire (SMTPS).
	6.7.2	**EX_3.2_5040**	Un Opérateur MSSanté ne doit pas utiliser le serveur SMTP d'un autre Opérateur MSSanté comme relai de messagerie.
	6.7.2	**EX_3.2_5050**	Le Connecteur MSSanté mis en œuvre par l'Opérateur doit respecter la cinématique décrite dans le **§** 6.7.2.1 pour émettre une requête vers un autre Connecteur MSSanté d'un autre Opérateur. En particulier les vérifications spécifiques à MSSanté et décrites dans cette cinématique doivent être mise en œuvre par le Connecteur MSSanté (étapes 4, 5 et 6).
	6.7.2.1	**EX_3.2_5060**	Avant l'envoi d'un message, le Connecteur MSSanté émetteur doit avoir vérifié préalablement que l'émetteur et le destinataire sont dans des domaines inclus dans la liste blanche (cette vérification peut être effectuée plus tard dans le processus **mais dans tous les cas avant l'envoi du message**) ; si ce n'est pas le cas, l'émetteur doit être notifié de la non émission (avec le motif du rejet).
	6.7.2.2	**EX_3.2_5070**	Les commandes SMTP envoyées par le Connecteur MSSanté doivent être conformes à la RFC 5321 (voir http ://tools.ietf.org/html/rfc5321).
Réception de messages MSSanté	**6.**7	**EX_3.1_5010**	Tout Opérateur accepte, sans restriction, les mails provenant d'émetteurs propriétaires de BAL sur des domaines de messagerie MSSanté. Il ne peut procéder à des filtrages de mails que pour des motifs de sécurité de son système et ce de façon exceptionnelle jusqu'à résolution du problème.
	6.7	**EX_3.1_5015**	Tout Opérateur accepte, sans restriction, les mails provenant du domaine '@dgs.mssante.fr'. Ce nom de domaine est rattaché à la Direction Générale de la Santé et lui permet d'adresser aux professionnels de santé dans un but de santé publique, des informations et alertes sanitaires. L'Opérateur doit en particulier permettre la réception de mails émis en masse en provenance de ce domaine.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
	6.7	**EX_3.1_5020**	La réception de messages est effectuée sur le protocole SMTP, dans une session TLS mutuelle avec le Connecteur MSSanté du domaine émetteur (SMTPS).
	6.7	**EX_3.1_5030**	Le Connecteur MSSanté mis en œuvre par l'Opérateur doit respecter la cinématique décrite dans le **§ 6.7.1.1** pour recevoir une requête en provenance d'un autre Connecteur MSSanté d'un autre Opérateur. En particulier les vérifications spécifiques à MSSanté et décrites dans cette cinématique doivent être mise en œuvre par le Connecteur MSSanté (étapes 3, 4, 5 et 6).
	6.7.1.2	**EX_3.1_5040**	Les commandes SMTP envoyées par le Connecteur MSSanté doivent être conformes à la RFC 5321 (voir http ://tools.ietf.org/html/rfc5321).
Interrogation liste blanche	**6.6.1**	**EX_LBL_5010**	Les Opérateurs MSSanté doivent prendre en compte les cas suivants, qui sont possibles dans la Liste Blanche des domaines autorisés (en fonction des implémentations mises en œuvre sur les différents services de messagerie MSSanté) : • Un DN de certificat peut être associé à un ou plusieurs domaines de messagerie ; • Un domaine de messagerie peut être associé à un ou plusieurs DN de certificats ; Un DN issu d'un certificat de l'IGC-Santé.
	6.6.1	**EX_2.2_5010**	Le Connecteur MSSanté doit récupérer **quotidiennement** la dernière version de la liste blanche à l'adresse suivante : https://espacedeConfiance.mssante.fr/listeblanchemssante.xml.
	6.6.1	**EX_2.2_5030**	L'exploitation par le Connecteur MSSanté de la liste blanche doit se faire en local et sans altération du fichier XML récupéré.
	6.6.1	**EX_2.2_5035**	Le connecteur MSSanté doit disposer d'une copie locale de la dernière version valide de la liste blanche en cas d'indisponibilité ou de corruption de celle-ci.
	6.6.2	**EX_2.2_5040**	La vérification de la signature doit se faire systématiquement à l'issue du téléchargement de la liste blanche dans le respect des bonnes pratiques définies par le W3C : http://www.w3.org/TR/xmldsig-bestpractices/#bp-validate-signing-key.
	6.6.2	**EX_2.2_5050**	Le certificat à utiliser pour vérifier la signature est intégré dans le tag X509Data. Il doit être validé selon la norme PKIX (voir RFC 5280 (http://tools.ietf.org/html/rfc5280), RFC 5246 (http://tools.ietf.org/html/rfc2246), RFC 3207 (http://tools.ietf.org/html/rfc3207) et RFC 2034 (http://tools.ietf.org/html/rfc2034). Il faut contrôler qu'il a bien été émis par l'ANS et qu'il a été attribué à l'ANS.
	6.3.1	**EX_WSA_5010**	L'authentification mutuelle du Connecteur MSSanté avec le serveur de l'Annuaire Santé constitue un prérequis transverse à l'appel de tout Web Service d'interfaçage avec l'Annuaire Santé (ces fonctions sont définies dans les chapitres suivants de ce document).
Publication dans	**6.3.1**	**EX_WSA_5020**	Cette authentification mutuelle permet d'authentifier la structure d'activité à l'origine de l'appel du Web Service, mais pas l'utilisateur

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
l'Annuaire Santé (Ajout / Modification / Suppression comptes de messagerie de l'Opérateur)			(humain ou machine) à l'initiative de l'action métier. Par conséquent, celui-ci doit être authentifié localement (au sein de la structure d'exercice dans le cas des Opérateurs de type « producteurs de soins », ou sur le service de messagerie dans le cas d'autres types d'Opérateurs), conformément aux exigences légales (CPS ou dispositifs équivalents).
	6.3.2.1	**EX_WSA_5030**	Les spécifications du §6.3.2.1 concernant l'encodage et les espaces de nommage, pour les Web Services de l'Annuaire Santé en SOAP, doivent être respectées.
	6.3.2.2	**EX_WSA_5040**	Les spécifications du §6.3.2.2 concernant la sécurité et l'intégrité, pour les Web Services de l'Annuaire Santé en SOAP, doivent être respectées.
	6.3.2.3.3	**EX_WSA_5050**	Les spécifications du § 6.3.2.3.3 (et sous-chapitres) concernant la construction des messages, pour les Web Services de l'Annuaire Santé en SOAP, doivent être respectées.
	6.3.2.3.4	**EX_WSA_5060**	Les spécifications du § 6.3.2.3.4 (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'Annuaire Santé en SOAP, doivent être respectées.
	6.4.1	**EX_PBA_5010**	Un Opérateur professionnels MSSanté doit obligatoirement implémenter la transaction TM1.1.1P afin d'être en mesure de gérer le cycle de vie des comptes de messagerie des utilisateurs du domaine MSSanté auquel il est rattaché. Cela consiste à être en capacité de : • Publier dans l'Annuaire Santé les BAL créées sur le domaine pour les nouveaux utilisateurs MSSanté (par exemple : à l'occasion de leur arrivée dans l'organisation à laquelle est rattaché le domaine de messagerie) ; • Modifier dans l'Annuaire Santé les données des BAL utilisateurs MSSanté sur le domaine de l'Opérateur (par exemple : à l'occasion d'un changement de service au sein de l'organisation) ; • Supprimer de l'Annuaire Santé les BAL utilisateurs MSSanté suspendues ou supprimées sur le domaine de l'Opérateur (par exemple : à l'occasion de leur départ de l'organisation à laquelle est rattaché le domaine de messagerie) ; • Supprimer la totalité des BAL d'un domaine lorsque celui-ci est retiré de la liste blanche.
	6.4.1	**EX_PBA_5011**	Un Opérateur professionnel MSSanté, qui est immatriculé au FINESS, doit associer un FINESS de type géographique à toutes ses BAL MSSanté déclarées dans l'Annuaire Santé. Le FINESS géographique associé est celui de la structure (site annexe) à laquelle appartient la BAL. Sauf dans le cas où la BAL appartient à une structure (maison mère, siège social, …) doté d'un FINESS juridique et correspond à un usage mutualisé entre plusieurs structures géographiques (sites annexes) : la BAL peut être associée au FINESS juridique du site de rattachement.
	6.4.1	**EX_PBA_5012**	Un Opérateur professionnels MSSanté, non immatriculé au FINESS, doit permettre aux utilisateurs finaux de lier un FINESS géographique à toutes BAL MSSanté déclarées dans l'Annuaire Santé.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
	6.4.1	**EX_PBA_5030**	L'Opérateur ne doit pas publier de BAL fonctionnelles de type « liste de diffusion » dans l'Annuaire Santé (toute adresse MSSanté doit correspondre à une et une seule BAL physique).
	6.4.1	**EX_PBA_5040**	L'Opérateur doit, par un moyen technique ou organisationnel, permettre à chacun des utilisateurs de son service d'indiquer explicitement s'il souhaite être inscrit en liste rouge ; Ce choix, non imposés par défaut, peut être mis en œuvre lors de la création de la BAL MSSanté via un mécanisme technique (case à cocher) ou organisationnel, et doit pouvoir être modifiés à tout moment par l'utilisateur.
	6.4.1	**EX_PBA_5050**	L'Opérateur doit mettre en œuvre les mécanismes techniques permettant de transmettre à l'Annuaire Santé le choix de l'utilisateur concernant : son inscription en liste rouge
	6.4.1	**EX_PBA_5140**	L'Opérateur doit s'assurer que les BAL MSSanté liées à son service de messagerie MSSanté suspendues ou supprimées ne soient plus publiées dans l'Annuaire Santé.
	6.4.1	**EX_PBA_5150**	L'Opérateur doit veiller à ce que les informations de description des BAL liées à son service de messagerie MSSanté publiées dans l'Annuaire Santé soient fiables.
	6.4.1.3	**EX_PBA_5090**	L'identifiant du titulaire d'une BAL personnelle MSSanté transmis par l'Opérateur lors de l'alimentation de l'Annuaire Santé doit impérativement être l'identifiant national (RPPS/ADELI) si le titulaire de la BAL en dispose. Pour le cas particulier des professionnels habilités ne disposant pas d'identifiant national, un identifiant interne (**en pratique : l'adresse de la BAL MSSanté attribuée à l'utilisateur**) à la structure d'activité pourra être transmis.
	6.4.1.3	**EX_PBA_5100**	L'Annuaire Santé peut identifier une erreur sur l'identifiant national du professionnel de santé transmis par l'Opérateur et en retour lui transmettre l'identifiant valide. L'Opérateur MSSanté doit le prendre en compte et le mettre à jour dans son service de messagerie.
	6.4.1.3	**EX_PBA_5220**	Dans le cas de BAL personnelles utilisées par des professionnels exerçant à titre salarié ou libéral dans des structures sanitaires et médico-sociales, l'Opérateur DOIT rattacher explicitement les BAL personnelles au numéro FINESS Géographique de la structure. Cette exigence a pour but d'améliorer la publication dans l'Annuaire Santé en facilitant ainsi l'identification de la « bonne » adresse à utiliser pour les professionnels disposant de plusieurs adresses MSSanté et ayant un exercice mixte (salarié et libéral). Cela permet également de favoriser le pilotage du déploiement des BAL personnelles dites « hospitalières » ainsi que des BAL personnelles dites plutôt « de ville » (l'objectif est de considérer qu'une BAL personnelle est dite « de ville » dans la mesure où aucun numéro FINESS y est rattaché).
	6.4.2	**EX_1.1.1_5010**	Dans le cas où l'Opérateur implémente la transaction « TM1.1.1P – Web Service en mode global », il doit respecter les spécifications d'implémentation décrites dans le chapitre § 6.4.2 (et sous-chapitres).
	6.4.2.5	**EX_1.1.1_5020**	Pour récupérer le compte-rendu d'alimentation, le même certificat d'authentification que celui utilisé lors de l'alimentation correspondante doit être utilisé.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
	6.4.2.5	**EX_1.1.1_5030**	Afin de s'assurer de la bonne publication des BAL MSSanté dans l'Annuaire Santé, les rapports d'alimentation doivent être téléchargés et les erreurs traitées après chaque alimentation.
	6.4.1	**EX_PBA_5230**	L'Opérateur ne doit pas publier dans l'Annuaire Santé les boites aux lettres de tests.
	6.3.1	**EX_WSA_5010**	L'authentification mutuelle du Connecteur MSSanté avec le serveur d'Annuaire Santé constitue un prérequis transverse à l'appel de tout Web Service d'interfaçage avec l'Annuaire Santé (ces fonctions sont définies dans les chapitres suivants de ce document).
Consultation Annuaire Santé (transaction optionnelle)	**6.3.1**	**EX_WSA_5020**	Cette authentification mutuelle permet d'authentifier la structure d'activité à l'origine de l'appel du Web Service, mais pas l'utilisateur (humain ou machine) à l'initiative de l'action métier. Par conséquent, celui-ci doit être authentifié localement (au sein de la structure d'exercice dans le cas des Opérateurs de type « producteurs de soins », ou sur le service de messagerie dans le cas d'autres types d'Opérateurs), conformément aux exigences légales (CPS ou dispositifs équivalents).
	6.3.3.1	**EX_WSA_5070**	Les spécifications du § 6.3.3.1 concernant l'encodage et les espaces de nommage, pour les Web Services de l'Annuaire Santé en REST, doivent être respectées.
	6.3.3.2	**EX_WSA_5080**	Les spécifications du § 6.3.3.2 concernant la sécurité et l'intégrité, pour les Web Services de l'Annuaire Santé en REST, doivent être respectées.
	6.3.3.3.1	**EX_WSA_5090**	Les spécifications du § 6.3.3.3.1 (et sous-chapitres) concernant les échanges, pour les Web Services de l'Annuaire Santé en REST, doivent être respectées.
	6.3.3.3.3	**EX_WSA_5100**	Les spécifications du § 6.3.3.3.3 (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'Annuaire Santé en REST, doivent être respectées.
	6.5	**EX_2.1_5010**	L'Opérateur MSSanté doit intégrer synchroniser les données des utilisateurs de son service avec celles provenant à jour de l'Annuaire Santé.
	6.5.1	**EX_2.1.1_5010**	La transaction « TM2.1.1.A - Interrogation de l'Annuaire Santé par le protocole LDAP » est réservée à la recherche de BAL MSSanté par les utilisateurs finaux et ne doit pas être utilisée pour récupérer l'intégralité du contenu de l'Annuaire Santé de manière automatisée.
	6.5.2	**EX_2.1.3_5010**	Dans le cas où l'Opérateur implémente la transaction « TM2.1.3A - Téléchargement d'une extraction de l'Annuaire Santé », il doit respecter les spécifications d'implémentation décrites dans le chapitre § 6.5.2 (et sous-chapitres associés).
	6.5.2	**EX_2.1.3_5020**	L'Opérateur, qui consomme le téléchargement de l'extraction de l'Annuaire Santé, doit mettre en œuvre un mécanisme permettant d'assurer le fonctionnement de son système de messagerie en cas d'indisponibilité de l'interface fournie par l'ANS. Il pourra s'agir d'un système de cache local.
	6.5.3	**EX_2.1.4_5010**	Dans le cas où l'Opérateur implémente la transaction « TM2.1.4A - Téléchargement des données d'identités des futurs utilisateurs finaux », il doit respecter les spécifications d'implémentation décrites dans le chapitre § 6.5.3 (et sous-chapitres associés).

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
Synchronisation temps	**6.9.1**	**EX_SDT_5010**	La date et l'heure de chaque matériel et système d'exploitation du Connecteur MSSanté doivent être synchronisées sur une source de temps fiable : le Connecteur MSSanté doit être en capacité de synchroniser son heure, pour l'horodatage des traces.
Traces service MSSanté	**6.9.2**	**EX_GDT_5010**	L'Opérateur MSSanté doit prévoir un dispositif capable de tracer les actions d'utilisation et d'exploitation du service MSSanté. Ces traces doivent être conservées afin de pouvoir être rendues accessibles à des personnes autorisées afin de : • Contribuer à la détection, à l'investigation et au traitement d'incidents de sécurité ; • Contribuer à la résolution de litiges entre le responsable du domaine et des utilisateurs ; • Permettre à une autorité de s'assurer de la conformité du traitement aux dispositions législatives qui l'encadrent.
	6.9.2	**EX_GDT_5020**	Les utilisateurs finaux et les administrateurs de l'Opérateur doivent être informés de la génération de traces de leurs actions par le service MSSanté.
	6.9.2	**EX_GDT_5030**	Des traces fonctionnelles doivent être générées par le Connecteur MSSanté pour tous les traitements opérés sur les BAL (Personnelles, Applicatives et Organisationnelles) et leur contenu.
	6.9.2	**EX_GDT_5040**	Chaque action tracée doit préciser le type d'action, l'identité de son auteur dûment authentifié (ou les informations permettant de la déterminer indirectement), les circonstances attachées à cette action (date et heure précise), les moyens techniques utilisés (nature et version de l'OS, navigateur ou client de messagerie), l'adresse réseau local, le contenu de la demande effectuée au système et la réponse fournie par ce dernier (y compris en cas d'échec) et plus généralement toute information utile à la recherche des causes et des effets d'un incident et à la constitution d'un faisceau de preuve. Le contenu des messages eux-mêmes n'est pas tracé.
	6.9.2	**EX_GDT_5050**	Pour les traces concernant l'envoi ou la réception d'un message, le champ « type d'action » inclut les informations suivantes : • Identifiant unique interne du message ; • Adresses email de l'émetteur du message et des destinataires du message ; • Objet du message ; Le cas échéant, la taille de l'ensemble encodé du message avec les pièces jointes.
	6.9.2	**EX_GDT_5060**	• Pour l'étape connexion à une boîte aux lettres, une trace fonctionnelle contient, une information précisant le type d'authentification mis en œuvre, et les informations relatives au type d'action, à l'identité de son auteur, aux dates et heures, aux moyens techniques utilisés (client de messagerie, web services, etc.), à l'adresse réseau.
	6.9.2	**EX_GDT_5070**	Le service MSSanté proposé par l'Opérateur doit prévoir les mécanismes de paramétrages nécessaires pour permettre au responsable de traitement d'être conforme aux durées de conservation des traces et des données à caractère personnel collectées lors des échanges.
	6.9.3	**EX_PSU_5010**	L'Opérateur MSSanté doit prévoir un dispositif capable d'enregistrer et de restituer des indicateurs de suivi de l'activité MSSanté.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
Statistiques service MSSanté	**6.9.3**	**EX_PSU_5020**	L'Opérateur MSSanté, avant soumission des indicateurs à l'ANS, devra retirer toute mention de l'INS dans l'adresse de BAL usager afin de le remplacer par le mot clé « usager ».
	6.9.3	**EX_PSU_5810**	Les informations demandées portent sur le mois écoulé, du 1er au dernier jour du mois (chiffres mensuels). L'Opérateur MSSanté doit déposer des fichiers dans une archive .zip sur un serveur via un webservice de soumission. Ces fichiers sont décrits dans le paragraphe ci-dessous. Les fichiers contenus dans les archives déposées seront parcourus, validés par traitement vérifiant le nom, le format et le contenu de chacun des fichiers. Une fois validé, ils seront intégrés au système de pilotage MSSanté et un compte rendu de bonne réception sera retourné à l'Opérateur MSSanté. L'Opérateur doit transmettre ces indicateurs à l'ANS dans les cinq premiers jours du mois qui suit via le webservice de soumission.
	6.9.3	**EX_PSU_5820**	L'Opérateur doit exclure des indicateurs mensuels du mois N : - les boites aux lettres suspendues au mois N-1 - les boites aux lettres supprimées au mois N-1 - les boites aux lettres de tests
	6.9.3	**EX_PSU_5830**	L'Opérateur doit produire le fichier « Echanges » tel que défini dans le paragraphe suivant : • (AAAAMM)_EchangesMSSante_[Domaine].csv - NB : Lors d'un envoi de message à un patient, la trace produite dans le fichier EchangesMSSanté ne doit pas contenir l'INS du patient (voir champ DESTINATAIRE dans le tableau ci-dessous)
	6.9.3	**EX_PSU_5840**	L'Opérateur doit produire le fichier « Connexions » tel que défini dans le paragraphe suivant : • (AAAAMM)_ConnexionsMSSante_[Domaine].csv
	6.9.3	**EX_SSU_5800**	Le fichier Connexion doit contenir l'ensemble des boites aux lettres créées par l'Opérateur. - Si la boite aux lettres a été créée mais n'a jamais été consultée, le champ « DATE_DERNIERE_CONNEXION » doit être vide. La valeur « null » n'est pas acceptée. - Si l'information concernant la date de dernière connexion est indisponible, l'Opérateur doit renseigner la valeur 1900-01-01 00:00:00
	6.9.3	**EX_SSU_5810**	L'authentification mutuelle du Connecteur MSSanté avec le serveur de soumission des statistiques pour les webservices de dépôt et de récupération de compte rendu constitue un prérequis
	6.9.3	**EX_SSU_5820**	L'Opérateur a l'obligation de consulter le compte rendu de soumission. Si le compte rendu indique des erreurs bloquantes, l'Opérateur doit les corriger et soumettre de nouveau les fichiers corrigés dans les délais prévus pour la soumission (les 5 premiers jours du mois).
	6.9.5.2	**EX_SSI_5010**	Une analyse de risques SSI doit être réalisée lors de la mise en œuvre d'un service MSSanté. Celle-ci doit être actualisée régulièrement et à chaque évolution majeure du Référentiel #1 pouvant le nécessiter.
Sécurité	**6.9.5.2**	**EX_SSI_5020**	En cas d'incident de sécurité, et en particulier pour ceux liés à une perte d'intégrité ou de confidentialité, l'Opérateur doit informer l'ANS

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
			dans les plus brefs délais.
	6.9.5.2	**EX_SSI_5030**	La Politique de Sécurité du Système d'Information (PSSI) doit être rédigée pour prendre en compte ce nouveau service. Celle-ci doit être revue à intervalle régulier. Des audits de la sécurité du système de messageries MSSanté et de son environnement doivent être réalisés à intervalle régulier.
	6.9.5.2	**EX_SSI_5040**	Les actions de sécurité doivent être coordonnées et pilotées par des responsables désignés. Chaque Opérateur doit désigner un référent de la sécurité qui est l'interlocuteur de l'ANS concernant les questions de sécurité du système.
	6.9.5.2	**EX_SSI_5050**	Les exploitants techniques du service doivent être régulièrement sensibilisés à la confidentialité des informations auxquelles ils accèdent ainsi qu'aux sanctions encourues en cas de divulgation.
	6.9.5.2	**EX_SSI_5060**	Les locaux hébergeant les plateformes de production et de secours du SI doivent bénéficier d'un contrôle des accès physiques.
	6.9.5.2	**EX_SSI_5070**	Les opérations d'exploitation importantes sur le SI (migration, restauration de sauvegarde, dans le cadre d'un plan de continuité, etc…) doivent être formalisées dans des procédures dûment explicitées.
	6.9.5.2	**EX_SSI_5080**	La capacité du système mis en œuvre pour le service MSSanté doit être testée, suivie et anticipée.
	6.9.5.2	**EX_SSI_5090**	Le système MSSanté doit mettre en œuvre des mécanismes de détection des intrusions. Le système MSSanté doit détecter et bloquer les codes malveillants (virus, vers, chevaux de Troie) contenus au sein de tous les flux d'informations entrants (par exemple, messages et pièces jointes) et sortants. Le système MSSanté doit également alerter les utilisateurs (émetteurs et/ou destinataires) de la mise en quarantaine d'un message et/ou d'une pièce jointe bloqués lors de son envoi ou de sa réception. Pour plus de précisions concernant le traitement à adopter en cas de messages contenant des pièces jointes infectées, le connecteur MSSanté doit être en capacité de filtrer ces pièces jointes, autant en envoi qu'en réception. Ainsi, lors de l'envoi ou de la réception d'un message contenant des pièces jointes infectées, le connecteur MSSanté peut au choix : Transférer au destinataire le message sans la pièce jointe infectée et informer l'émetteur et le destinataire de la non transmission de cette pièce jointe ; Ne pas transférer le message au destinataire et informer l'émetteur que le message ne peut être envoyé pour cause de contenu malveillant détecté dans la pièce jointe.
	6.9.5.2	**EX_SSI_5100**	Les serveurs de messagerie doivent s'authentifier mutuellement à l'aide d'un certificat logiciel de personne morale délivré par l'ANS. L'Opérateur doit suivre les recommandations de sécurité issues des Conditions Générales d'Utilisation (CGU) des moyens d'identification électronique délivrés par l'Agence en Numérique en Santé. Celles-ci sont les suivantes (5.3.2. Engagements des

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
			propriétaires de certificat) : « Le propriétaire du certificat garantit, via l'acception des présentes CGU et la mise en œuvre d'une politique de sécurité, que des mesures de protection techniques et organisationnelles sont mises en œuvre pour assurer la sécurité des clés privées associées aux certificats émis par l'ANS. Il doit notamment veiller à limiter l'accès à ses clés privées à des personnes dûment autorisées et qu'elles ne puissent pas être dupliquées ni installées dans de multiples équipements ». Tous les messages électroniques émis et reçus par un Opérateur MSSanté dans l'Espace de Confiance doivent être protégés en confidentialité et en intégrité dans des canaux sécurisés par le protocole TLS.
	6.9.5.2	**EX_SSI_5110**	Les sauvegardes doivent être testées à intervalle régulier afin de valider l'ensemble du processus de sauvegarde/restauration. Ces tests doivent inclure au moins une restauration de l'ensemble des composants d'un service.
	6.9.5.2	**EX_SSI_5120**	Le service de messagerie doit bénéficier d'un service de supervision configuré pour générer des alertes automatisées sur des événements spécifiés et jugés critiques pour la sécurité du service (disponibilité, intégrité, confidentialité et auditabilité). Les exigences concernant les traces sont définies dans le § 6.9.2.
	6.9.5.2	**EX_SSI_5130**	Tout Opérateur doit gérer la liste des utilisateurs autorisés à accéder au service et ses évolutions. Chaque utilisateur doit être identifié puis authentifié avec succès, en s'appuyant sur une base des utilisateurs autorisés, avant de pouvoir accéder au service MSSanté.
	6.9.5.2	**EX_SSI_5140**	Les pares-feux protégeant l'infrastructure du SI doivent bénéficier des mécanismes de protection conformes à l'état de l'art.
	6.9.5.2	**EX_SSI_5150**	Les outils déployés pour l'administration et/ou l'exploitation du SI doivent mettre en œuvre une authentification des Opérateurs (exploitants, administrateurs).
	6.9.5.2	**EX_SSI_5160**	Le système doit bénéficier d'un dispositif de gestion des incidents de sécurité capable de les détecter, les évaluer et les traiter dans les meilleurs délais.
	6.9.5.2	**EX_SSI_5170**	Chaque Opérateur doit assurer une veille réglementaire en vue d'assurer la conformité du SI tout au long de son cycle de vie.
	6.9.5.3	**EX_SSI_5180**	Comme indiqué dans les documents contractuels les Opérateurs MSSanté intégrés de façon validés ont l'obligation de signaler à l'ANS en tant que gestionnaire de l'Espace de Confiance « […] toute modification, tout dysfonctionnement ou toute anomalie sur leur service de Messageries Sécurisées de Santé qui aurait un impact sur le bon fonctionnement, la disponibilité ou la sécurité du « système MSSanté » […] dans les vingt-quatre (24) heures qui suivent l'identification du dysfonctionnement ou de l'anomalie.». De même, ils doivent informer l'ANS de tout arrêt temporaire supérieur à 8 jours. Les canaux dédiés pour ces déclarations d'incidents sont : l'adresse mail : monserviceclient.mssante@esante.gouv.fr le numéro de téléphone : 0 825 852 000 (Service à 0,06 € / min + prix appel, 24/24 Heures - 7/7 Jours).

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
	6.9.4	EX_DCU_5010	L'Opérateur MSSanté doit définir des conditions générales d'utilisation (ou équivalent) pour le service MSSanté qu'il met en œuvre. A minima, les conditions générales d'utilisation de l'Opérateur doivent contenir les clauses suivantes (dont la forme peut être adaptée aux besoins de l'Opérateur) : Rappel du contexte juridique : • Règles de droit commun relatives à l'échange des données de santé à caractère personnel dont les dispositions des articles L 1110-4 et L 1110-12 du code de la santé publique qui précisent les conditions d'échange de données de santé ; • Règles générales relatives au traitement de données à caractère personnel, et notamment de données de santé, conformément aux dispositions du RGPD et de la loi Informatique et Libertés ; • L'Opérateur professionnels doit rappeler à l'Utilisateur professionnel qu'il doit respecter le cadre légal qui régit sa profession, en particulier les règles relatives à l'obligation de conserver les données de santé à caractère personnel collectées à l'occasion de l'exercice de sa profession ; • Préciser que les données de santé à caractère personnel sont couvertes par le secret professionnel dans les conditions prévues à l'article L 1110-4 du code de la santé publique, dont la violation est réprimée par l'article 226-13 du code pénal ; • L'Utilisateur professionnel est informé qu'il doit traiter l'INS conformément aux dispositions venant encadrer ses conditions d'utilisation et notamment les articles R. 1111-8-1 et suivants du code de la santé publique. Bon usage de la MSSanté : • Information des utilisateurs finaux sur les finalités du service MSSanté et les conditions d'utilisation de ses données à caractère personnel ; • Ajout des mentions d'informations obligatoires conformément aux articles 13 et 14 du RGPD et de la loi Informatique et Libertés ; • Seuls les professionnels habilités par la loi à échanger des données de santé et, par délégation, les professionnels intervenant dans le système de santé agissant sous leur responsabilité, ainsi que les usagers du système de santé peuvent utiliser le service MSSanté ; • Le service MSSanté permet les échanges, entre professionnels habilités, de données de santé utiles à la prise en charge d'une personne ainsi que les échanges entre ces professionnels et les usagers du système de santé par le biais de BAL de l'Espace de Confiance MSSanté ; • Un professionnel habilité à échanger des données de santé peut déléguer l'accès à sa BAL personnelle ou organisationnelle à un professionnel intervenant dans le système de santé agissant sous sa responsabilité (le « Délégataire »), sous réserve du respect des dispositions relatives au secret professionnel et à l'échange et au partage de données de santé.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
			• Chaque Utilisateur professionnel est responsable des informations qu'il va échanger et partager dans le cadre de son utilisation de la BAL. Il est également responsable des accès qu'il pourrait ouvrir par délégation ou pour toute autre habilitation d'accès à une BAL organisationnelle ou personnelle. Il doit notamment s'assurer que les professionnels qu'il ajoute sont habilités à accéder aux informations relatives aux patients pris en charge. • L'ouverture de tout nouvel accès à une BAL organisationnelle par un professionnel habilité est conditionnée par l'information, par tout moyen, de l'accord de l'ensemble des professionnels habilités accédant à la BAL. • Le Délégataire ne peut accéder aux données relatives aux patients que sous la responsabilité d'un professionnel habilité, dans le strict cadre de ses missions et dans le respect des obligations relatives au secret professionnel. • Toute utilisation abusive par les utilisateurs finaux de la messagerie est interdite (harcèlement, langage abusif, etc.). Dans ce cadre, les utilisateurs finaux s'engagent à ne pas procéder à l'envoi de messages non sollicités à un ou plusieurs destinataires, considéré comme du spam ; • Les utilisateurs finaux s'interdisent de transmettre par messagerie sécurisée ou par tout autre moyen des courriels contenant des virus ou plus généralement tout programme visant notamment à détruire ou limiter la fonctionnalité de tout logiciel, ordinateur ou réseau de télécommunication ; • Les utilisateurs finaux s'engagent à ne pas rediriger leur adresse sécurisée vers une adresse de messagerie non MSSanté. • Les utilisateurs finaux s'engagent à conserver leurs moyens d'authentification dans des conditions garantissant leur sécurité. • Si l'Opérateur utilise Pro Santé Connect, il doit prévoir qu'en utilisant sa carte CPS ou e-CPS pour se connecter à la messagerie avec Pro Santé Connect l'Utilisateur professionnel s'engage à respecter les obligations qui lui incombent prévues dans les conditions générales d'utilisation des moyens d'identification électroniques (MIE) et de la e-CPS. • L'Utilisateur professionnel ne doit pas demander la création d'une BAL organisationnelle rattachée à une personne physique s'il exerce dans une structure disposant d'un identifiant FINESS. • L'Utilisateur professionnel doit veiller à créer des adresses de messagerie avec des dénominations claires, permettant aux autres utilisateurs d'identifier facilement la personne physique ou l'entité titulaire de ces adresses de messagerie. Publication dans l'Annuaire Santé : • L'Opérateur professionnels doit annoncer dans ses CGU l'existence de dispositifs permettant à tout Utilisateur professionnel de son service d'indiquer (et de modifier à tout moment) s'il souhaite être inscrit en liste rouge ; • L'Opérateur professionnels doit également prévoir un moyen permettant à tout Utilisateur professionnel de son service d'être informé que ses données liées à l'usage du système MSSanté sont publiées dans l'Annuaire Santé et consultables par les autres utilisateurs (sauf en cas d'inscription en liste rouge). Information du patient/usager :

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
			• L'Opérateur professionnels doit préciser qu'en cas d'opposition du patient à l'utilisation du service MSSanté pour échanger des données de santé le concernant, l'utilisateur professionnel devra recourir à un moyen d'échange alternatif (courrier papier par exemple) ; • L'usager doit être informé sur son droit de s'opposer à l'échange et au partage des données le concernant ; • L'Opérateur professionnels précise que le service MSSanté ne doit pas être confondu avec le dossier médical de la personne concernée et constitue uniquement un outil d'échange sécurisé de données de santé. Le service MSSanté n'a pas vocation à constituer un espace de stockage sur le long terme ; • L'Opérateur usagers précise que le service MSSanté ne doit pas être confondu avec le dossier médical de la personne concernée et constitue uniquement un outil d'échange sécurisé de données de santé. Ainsi l'usager s'engage à sauvegarder les documents de santé échangés par le biais du service dans un dispositif de stockage personnel (ex. disque dur, ordinateur, etc.) ou dans son « Dossier médical partagé » ; • L'Utilisateur professionnel doit reporter dans les dossiers médicaux des patients toute information reçue par messagerie et qu'il jugera utile à la prise en charge de ces derniers ; • L'Utilisateur usager doit être informé que le service de messagerie sécurisée n'a pas vocation à traiter les situations d'urgence. En cas d'urgence, l'usager doit impérativement composer le numéro 15. En conséquence, la responsabilité du professionnel habilité ne saurait être engagée pour tout préjudice survenu dans le cadre d'une situation d'urgence. Collecte des données des utilisateurs finaux : • Indicateurs d'usage MSSanté L'utilisateur est informé, d'une part, que des données (adresse e-mail, horodatage des échanges, taille des e-mails, présence d'un INS qualifié, présence/type de document structuré, données d'identification, identifiant du logiciel métier utilisé et données relatives à la vie professionnelle) sont collectées, transmises et traitées par l'ANS afin de lui permettre, en tant que gestionnaire de l'Espace de Confiance MSSanté, d'établir des indicateurs anonymes. L'ANS est responsable du traitement des données réalisé à des fins statistiques. L'Opérateur agit donc en qualité de sous-traitant au sens de l'article 4 du RGPD. Le traitement est mis en œuvre en application de l'article 5, 5° de la loi n°78-17 du 6 janvier 1978. Ce traitement est mis en œuvre dans le cadre de l'exécution d'une mission d'intérêt public dont est investie l'ANS. • Transfert d'indicateurs à la Cnam La Cnam est destinataire des données à caractère personnel contenues dans les indicateurs MSSanté aux seules fins d'évaluer l'usage de la MSSanté par les professionnels de santé qui bénéficient de financements conventionnels en faveur de ce déploiement. La Cnam effectuant ledit traitement agit en qualité de Responsable de traitement. Ce traitement est mis en œuvre dans le cadre de l'exécution d'une mission d'intérêt public.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
			• Indicateurs MSSanté utilisés dans le cadre du Ségur Conformément aux dispositions prévues par les arrêtés relatifs aux dispositifs de financement à l'équipement logiciel mis en œuvre par l'ANS dans le cadre du programme Ségur numérique, des données relatives au fonctionnement de la messagerie MSSanté des professionnels ou établissements participant au programme de financement Ségur sont susceptibles d'être communiquées (identifiant de la boite de messagerie et indicateurs d'usage) à l'ANS ainsi qu'à son opérateur de paiement, l'Agence des services de paiement (« ASP »). Ce traitement est réalisé pour la gestion des contrôles prévus par la réglementation précitée (usage effectif de la messagerie de santé), lesquels conditionnent l'accès au financement octroyé. Les informations susceptibles d'être communiquées dans ce cadre sont strictement confidentielles et ne sont accessibles qu'aux agents habilités de l'ANS et de l'ASP. Ce traitement est mis en œuvre par l'ANS, en qualité de responsable de traitement, dans le cadre de l'exécution d'un contrat. • Durée de conservation Les données collectées sont conservées pendant une durée de 2 années, à partir de la date de collecte de la donnée, puis anonymisées. • Droit des utilisateurs Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée et au Règlement européen n°2016/679/UE du 27 avril 2016, l'utilisateur bénéficie d'un droit d'accès, de rectification, d'effacement, d'opposition, portabilité, de limitation, et du droit de définir des directives sur le sort de ses données après sa mort. Ces droits peuvent être exercés : □ sur demande écrite à l'adresse suivante : GIP Agence du Numérique en Santé - Délégué à la protection des données - 2 - 10 Rue d'Oradour-sur-Glane - 75015 Paris ; □ par messagerie électronique, à l'adresse suivante : dpo@esante.gouv.fr. L'utilisateur dispose également d'un droit d'introduire une réclamation auprès de la CNIL Valeur probante : Prévoir l'acceptation d'une convention de preuve (article 1368 du code civil), par laquelle l'utilisateur final s'engage à ne pas contester la valeur probante des messages électroniques échangés via le système MSSanté sur le fondement de leur nature électronique (article 1366 et suivants du code civil) afin de prévenir d'éventuelles contestations. Cette convention de preuve permettra de s'accorder pour reconnaître la même valeur probante aux écrits électroniques transmis via le système MSSanté qu'aux écrits sur support papier. Les CGU de l'Opérateur MSSanté doivent préciser que leur acceptation a pour conséquence la conclusion d'une convention de preuve.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
Définition des CGU à mettre en œuvre par l'Opérateur	**6.9.4**	**EX_DCU_5030**	L'Opérateur doit mettre en œuvre les moyens lui permettant de s'assurer de l'acception de ces conditions par tout utilisateur de son service avant l'usage effectif de celui-ci.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
API LPS	**6.8.2**	**EX_LPS_0100**	Sur les interfaces de l'API LPS, le système DOIT impérativement accepter les connexions des clients de messagerie utilisant la version TLS 1.2 (RFC 5246). En complément de la version TLS 1.2, les versions ultérieures (TLS 1.3...) peuvent aussi être acceptées. Dans le cas contraire, la connexion ne doit pas être établie.
	6.8	**EX_LPS_0110**	L'opérateur doit proposer aux LPS conformes au Référentiel #2 MSSanté, des accès publics à l'API LPS, cad qu'il ne doit pas appliquer de mécanisme de filtrage des accès de type filtrage IP.
	6.8.2	**EX_LPS_0200**	Sur les interfaces de l'API LPS, le système DOIT uniquement utiliser l'une des suites de chiffrement suivantes, lors de la négociation TLS : • 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 Dans le cas contraire, la connexion ne doit pas être établie. La longueur du groupe DH doit être >= 2048 bits ou la longueur du groupe elliptique ECDH doit être >= 256 bits. La confidentialité persistante (PFS - perfect foward secrecy) de DH doit être utilisée (DHE ou ECDHE).
	6.8.3	**EX_LPS_0300**	Sur les interfaces de l'API LPS, le système DOIT exposer un mécanisme d'auto-configuration à destination des LPS, conforme aux RFC 2782 & 6186, en déclarant sur chacun des noms de domaines déclarés en liste blanche les 4 attributs DNS suivants : _submission._tcp SRV 10 100 587 [front smtp psc de l'opérateur] _submission._tcp SRV 20 100 587 [front smtp authcli de l'opérateur] _imap._tcp SRV 10 100 143 [front imap psc de l'opérateur] _imap._tcp SRV 20 100 143 [front imap authcli de l'opérateur]
	6.8.4	**EX_LPS_0400**	Le système DOIT exposer aux logiciels clients de messagerie respectant le référentiel MSSanté #2 une interface d'envoi de messages utilisant le protocole SMTP avec STARTTLS sur le port 587, conformément à la RFC 5321.
	6.8.4	**EX_LPS_0500**	Le système DOIT exposer aux logiciels clients de messagerie respectant le référentiel MSSanté #2 une interface de consultation de BAL utilisant le protocole IMAP 4 (rev1 ou rev2) avec STARTTLS sur le port 143, conformément à la RFC 3501 ou RFC 9051.
	6.8.4	**EX_LPS_0600**	Le système DOIT permettre à une personne physique identifiée dans l'annuaire santé de se connecter à une BAL personnelle ou organisationnelle en IMAP / SMTP en se basant sur l'Access Token PSC transmis par le LPS.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
	6.8.4	**EX_LPS_0700**	Le système DOIT exposer le mécanisme SASL d'authentification OAuth 2.0 avec l'implémentation XOAUTH2 en IMAP et SMTP dans le but de permettre le transit de l'Access Token PSC au format JWT (Json Web Token), ainsi que la capability SASL-IR permettant la transmission de l'Access Token en une fois sur IMAP comme défini dans le RFC 4959 (https://tools.ietf.org/html/rfc4959).
	6.8.4	**EX_LPS_0710**	En cas d'erreur d'authentification, le système DOIT retourner des codes d'erreur conformes aux standard IMAP et SMTP, à savoir : • 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)
	6.8.4	**EX_LPS_0800**	Le système DOIT faire la démarche de raccordement auprès du Fournisseur d'Identité PSC afin d'être autorisé à utiliser ce service. Cf. https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect.
	6.8.4	**EX_LPS_0900**	Lors d'une demande d'ouverture de connexion SMTP ou IMAP par un LPS sur l'interface BAL personnelle ou organisationnelle, le système DOIT : 1- Ouvrir la session TLS avec STARTTLS comme défini dans les RFC 3207 et RFC 2246 2- Décoder la chaine de caractères en base64 envoyée par le client à la suite du mot clé AUTHENTICATE XOAUTH2 pour IMAP et AUTH XOAUTH2 pour SMTP 3- Extraire l'adresse de la BAL du champ « user » de la chaine décodée 4- Décoder la chaine de caractères en base64 correspondant à l'Access Token au format Json Web Token récupérée du champ « auth » en supprimant les caractères ^A^A de la chaine décodée à l'étape 2. 5- Vérifier que l'Access Token a bien été signé par PSC grâce à la clé publique exposée par ce dernier (cf [PSC-MOT-FI] : endpoint "jwks_uri"). 6- Vérifier que l'Access Token n'a pas expiré grâce aux champs « exp » et « iat » 7 - Interroger le endpoint UserInfo PSC avec l'Access Token pour récupérer l'IdNat au moyen du champ SubjectNameID (cf. [PSC-MOT-FI] : endpoint « UserInfo ») 8- Vérifier que l'idNat récupéré du champ SubjectNameID correspond à l'identité d'une personne physique habilitée à accéder à la BAL 9- Traiter la commande SMTP ou IMAP reçue
	6.8.5	**EX_LPS_910**	L'opérateur DOIT autoriser un flux sortant de type Web HTTP sécurisé de son système vers PSC, en paramétrant son infrastructure technique de façon adéquate.

Fonctionnalité	§ Référentiel #1	N° Exigence	Exigence
	6.8.5	**EX_LPS_1000**	Le système DOIT mettre fin à la session IMAP ou SMTP au bout de : - 15 minutes sur inactivité de l'utilisateur - 4 heures sinon
	6.8.5	**EX_LPS_1100**	Le système DOIT permettre à une structure identifiée dans l'annuaire santé de se connecter à une BAL applicative en IMAP et SMTP en présentant un certificat ORG AUTH-CLI issu de l'IGC Santé.
	6.8.6	**EX_LPS_1200**	Lors d'une demande d'ouverture de connexion SMTP ou IMAP par un LPS sur l'interface BAL applicative, le système DOIT : 1- Vérifier le certificat ORG AUTH_CLI présenté par le client de messagerie comme défini dans la RFC 2246 (https://datatracker.ietf.org/doc/html/rfc2246). Dont en particulier la conformité à l'AC, la non expiration et la non révocation. 2- Monter la session TLS 3- Extraire l'adresse de la BAL dans le login de la méthode d'authentification PLAIN comme défini dans la RFC 3501 (https://datatracker.ietf.org/doc/html/rfc3501) 4- Extraire du DN du certificat, le champ OU contenant l'idNat de la structure 5- Réaliser l'habilitation sur la BAL applicative demandée en contrôlant que la structure est bien habilitée à accéder à la BAL identifiée dans le login. 6- Traiter la commande SMTP ou IMAP reçue

Tableau 49 : Liste des exigences applicables aux Opérateurs MSSanté

9 Annexes

9.1 Les environnements Annuaire Santé

9.1.1 L'Annuaire Santé de production

Transaction	Description	Opération	URL
TM1.1.1P	WS d'alimentation des comptes MSSanté d'un ou plusieurs domaines de messagerie	WSALIMENTATIONMSS	https://ws.annuaire.mssante.fr/webservices/V1011/Alimentation/WSALIMENTATIONMSS
TM1.1.1P	WS de récupération du compte-rendu d'alimentation dans l'Annuaire Santé	WSCRALIMENTATIONMSS	https://ws.annuaire.mssante.fr/webservices/V1011/CR/WSCRALIMENTATIONMSS
TM2.1.1A	Consultation de l'Annuaire Santé par le protocole LDAP		Nom DNS de l'Annuaire Santé : ldap.annuaire.mssante.fr URL d'accès : ldap://ldap.annuaire.mssante.fr Port : 389 Base DN au moins égale à « OU=bal, O=mssante, C=fr »
TM2.1.3A NB : décommissionnée courant 2024	WS de téléchargement de l'Annuaire Santé	extractionMSSante	https://ws.annuaire.mssante.fr/webservices/V1011/extractionMSSante?format=xml
TM2.1.4A NB : décommissionnée courant 2025	WS de récupération des données d'identités des futurs utilisateurs finaux	extractionIdentitePS	https://ws.annuaire.mssante.fr/webservices/V1011/extractionIdentitePS/?format=csv
TM4.1P	Interrogation de la liste blanche des domaines de messagerie MSSanté		https://espacedeConfiance.mssante.fr/listeblanchemssante.xml

Tableau 50 : URL des services de l'Annuaire Santé certifiés par l'IGC Santé

Autorité de certification

L'Annuaire Santé présente un certificat issu de l'IGC-Santé de la gamme Elémentaire domaine Organisations de la branche de production.

Il est donc nécessaire de considérer cette AC comme autorité de certification de Confiance dans l'application cliente.

Les certificats racine et intermédiaires de cette AC sont téléchargeables sur http://igc-sante.esante.gouv.fr/PC/#ca

9.1.2 L'Annuaire Santé de tests (dit « partenaires »)

L'ANS met à disposition des Opérateurs un Annuaire Santé de tests (dit "partenaires"). Cet environnement de tests permet aux éditeurs de connecteurs MSSanté et Opérateurs MSSanté qui le souhaitent de vérifier les solutions qu'ils développent. Les traitements de l'alimentation sur cet Annuaire Santé de tests se font à 11h, 15h et la nuit (entre 2h et 4h comme pour l'Annuaire Santé de production).

9.1.2.1 URL des services certifiés par l'IGC-Santé

Transaction	Description	Opération	URL
TM1.1.1P	WS d'alimentation des comptes MSSanté d'un ou plusieurs domaines de messagerie	WSALIMENTATIONMSS	https://ws.partenaires.annuaire.sante.fr/webservices/V1011/Alimentation/WSALIMENTATIONMSS?wsdl
TM1.1.1P	WS de récupération du compte-rendu d'alimentation dans l'Annuaire Santé	WSCRALIMENTATIONMSS	https://ws.partenaires.annuaire.sante.fr/webservices/V1011/CR/WSCRALIMENTATIONMSS?wsdl
TM2.1.1A	Consultation de l'Annuaire Santé par le protocole LDAP		Nom DNS de l'Annuaire Santé : partenaires.annuaire.sante.fr URL d'accès : ldap://partenaires.annuaire.sante.fr Port : 389 Base DN au moins égale à « OU=bal, O=mssante, C=fr »
TM2.1.3A	WS de téléchargement de l'Annuaire Santé	extractionMSSante	https://ws.partenaires.annuaire.sante.fr/webservices/V1011/extractionMSSante?format=xml
TM2.1.4A	WS de récupération des données d'identités des futurs utilisateurs finaux	extractionIdentitePS	https://ws.partenaires.annuaire.sante.fr/webservices/V1011/extractionIdentitePS?format=csv

Tableau 51 : URL des services de l'Annuaire Santé de tests certifiés par l'IGC-Santé

9.1.2.2 L'interface LDAP de l'Annuaire Santé de tests (dit "partenaires")

Les comptes de messagerie sont disponibles dans les extractions LDAP de l'Annuaire Santé de tests le jour qui suit leur création.

9.1.2.3 Autorité de certification de l'Annuaire Santé de tests (dit "partenaires")

L'Annuaire Santé de tests présente un certificat issu de l'IGC-Santé gamme Elémentaire domaine Organisations de la branche de test.

Il est donc nécessaire de considérer cette AC comme autorité de certification de Confiance dans l'application cliente.

Les certificats racine et intermédiaire de cette AC sont téléchargeables sur : http://igc-sante.esante.gouv.fr/PC%20TEST/

9.2 Espace de Confiance MSSanté de tests

L'Espace de Confiance de tests est un environnement mis à disposition des Opérateurs pour réaliser des tests de bout en bout dans un environnement **complètement disjoint de l'environnement de production**. Du point de vue fonctionnel, il reprend les mêmes principes que l'Espace de Confiance de production (liste blanche de tests, Annuaire Santé de tests, webservice de dépôt d'indicateurs d'usage, outil de contrôle) mais ne met pas en œuvre de données de santé à caractère personnel.

Les finalités de cet Espace de Confiance de test sont :

- proposer à tout nouvel Opérateur un moyen de tester son bon fonctionnement vis-à-vis de la liste blanche, de l'Annuaire Santé, de son interface LPS et inter opérateur avant d'intégrer l'Espace de Confiance de production,
- proposer à tout Opérateur existant, un moyen de réaliser des tests de non régression lors d'une montée de version,
- permettre à des éditeurs de LPS qui ont implémentées l'interface API LPS de tester leur implémentation sur différents Opérateurs,
- permettre à des éditeurs et Opérateurs de réaliser de tests de bout en bout dans le cadre de mise en œuvre de projets communs.

NB : Il est interdit d'intégrer un environnement de production à l'Espace de Confiance de test.

9.2.1 Liste blanche de tests

L'url de la liste blanche de test est publique et accessible à l'adresse suivante :

https://espacedeConfiance.test.mssante.fr/listeblanchemssante.xml

L'Opérateur devra gérer un certificat IGC Santé de test que présente le serveur qui abrite la liste blanche de test.

9.2.2 Annuaire Santé de test

L'Opérateur devra gérer le certificat IGC Santé de test que présente l'Annuaire Santé de test (dit partenaires).

Cet annuaire contient les identités de test associées à toutes les cartes CPx de test produites et non expirées. L'Opérateur ne peut déclarer des BAL que sur ces identités. L'Opérateur peut accéder à la liste des identités de test connues de l'Annuaire Santé en utilisant la transaction :TM2.1.4A - Téléchargement des données d'identités des futurs utilisateurs finaux.

Pour plus d'informations, se référer au paragraphe §**9.1.2**.

9.2.3 Boite aux lettres de réponse automatique de test

Tout Opérateur souhaitant réaliser des échanges au sein de l'Espace de Confiance MSSanté de tests devrait se munir d'un connecteur MSSanté.

Le Connecteur MSSanté de tests de l'Opérateur doit initialiser ou accepter les connexions SMTP uniquement après validation d'un certificat serveur X509 délivré par l'ANS selon la norme PKIX (voir RFC 5280 (http://tools.ietf.org/html/rfc5280), RFC 2246 (http://tools.ietf.org/html/rfc2246), RFC 3207 (http://tools.ietf.org/html/rfc3207) et RFC 2034 (http://tools.ietf.org/html/rfc2034) et ayant une correspondance dans la Liste Blanche de tests (DN du certificat de tests).

Chaque Opérateur intégrant l'Espace de Confiance de test, et souhaitant réaliser des échanges doit disposer d'une BAL de réponse automatique de test. Cette BAL permet de faire des échanges inter-Opérateur sans solliciter les équipes d'exploitation et est affichée dans la liste blanche de test (le champ <description>).

Le nom de la BAL de réponse automatique doit être normalisé comme suit :

reponse.automatique@test.<Type d'environnement*>.<*Opérateur*>.mssante.fr

** Type d'environnement* : formation, préproduction, etc.*

Remarque : Il est conseillé aux Opérateurs de choisir un nom de domaine proche de celui déclaré en liste blanche de production pour permettre une faire le rapprochement et reconnaître plus facilement leurs noms de domaines.

9.2.4 Webservice de production et soumission de statistiques d'utilisation

L'Espace de Confiance de test offre aux Opérateurs la possibilité de soumettre des fichiers de statistiques d'utilisation via des webservices à l'instar de ceux de production décrits dans le paragraphe §6.9.3.

Ci-dessous les URL permettant d'accéder aux webservices de soumission de statistiques dans l'Espace de Confiance de test.

Webservice	Description	URL de tests
postFile	Nom du webservice pour le dépôt de l'archive	*https://ws-sipil.formation.mssante.fr/sipil/postFile*
getReport	Nom du webservice pour la récupération du compte rendu	*https://ws-sipil.formation.mssante.fr/sipil/getReport*

Les principes et modalités de soumission sont identiques à ceux de l'Espace de Confiance de production décris au paragraphe §6.9.3. cependant, l'Opérateur devra être présent en liste blanche de test et présenter un certificat de test.

9.3 Canaux de contact

Pour les demandes relatives à l'Espace de Confiance MSSanté (assistance contractuelle, assistance technique sur les composants mis à disposition par l'ANS (Annuaire Santé, liste blanche, référentiels MSSanté…), signalements d'incidents, envoi des indicateurs de suivi d'activité, demandes d'accès à l'Annuaire Santé de tests…) des Opérateurs MSSanté, deux canaux de contact sont disponibles :

- Email : monserviceclient.mssante@esante.gouv.fr,
- Téléphone : 0 825 852 000 (Service à 0,06 € / min + prix appel, de 8h à 20h du lundi au vendredi et de 8h à 14h le samedi).

Les demandes d'inscriptions à la liste de diffusion pour être informé des actualités de l'Espace de Confiance MSSanté se font via ces canaux également.

9.4 Documents externes

Documents applicables

Le tableau ci-dessous récapitule les principaux documents applicables. Dans l'ensemble du document, ils sont désignés par le code apparaissant dans la colonne « Référence ».

Référence	Document
Documents du Cadre d'interopérabilité des Systèmes d'Information de Santé (CI-SIS) (Documents accessibles sur le site de l'ANS **https://esante.gouv.fr/offres-services/ci-sis/espace-publication**)	
[CI-CHAP]	Document Chapeau du CI-SIS
[CI-ECH-DOC]	Volet ECHANGE DE DOCUMENTS DE SANTE
[CI-TR-CLI-LRD]	Couche TRANSPORT VOLET SYNCHRONE
[CI-STRU-ENTETE]	Couche Contenu Volet Structuration Minimale de Documents Médicaux
Nomenclature des Acteurs de Santé (Documents accessibles sur le site de l'ANS **https://mos.esante.gouv.fr/NOS/**)	
[NOS-RES-TERMI]	Liste des Identifiants des Ressources Terminologiques utilisées par le RASS
Documents de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) (Documents accessibles sur le site de l'ANS **https://esante.gouv.fr/offres-services/pgssi-s/espace-de-publication**)	
[PG-IDENT]	Référentiel d'identification des acteurs sanitaires et médico-sociaux
[PG-RG-INT]	Règles pour les interventions à distance sur les systèmes d'information de santé
Documents MSSanté (Documents accessibles sur le site : **https://mssante.fr/is/doc-technique**)	
[MSS-REF2]	Référentiel socle MSSanté #2 – Clients de Messageries Sécurisées de Santé
[CONTRAT-MSSANTE]	Contrat « Opérateur MSSanté v2 » et ses annexes
[MSS-OUTIL-TEST]	MOyen de Test et de Conformité pour le Référentiel #1 (MOTCO 1) MOyen de Test et de Conformité pour le Référentiel #2 (MOTCO 2)
Documents PRO Santé Connect (Documents accessibles sur le site : **https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/documentation-technique**	
[PSC-MOT-FI]	PRO Santé Connect - Mode opératoire technique pour un Fournisseur de Service

Documents ANSSI	
[ANSSI-DNS]	Sécurisation des serveurs DNS https://www.ssi.gouv.fr/uploads/2014/05/guide_dns_fr_anssi_1.3.pdf
[ANSSI-NDD]	Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaines http://www.ssi.gouv.fr/uploads/2014/05/guide_dns_anssi_1.2.pdf
[ANSSI-GHI]	Guide d'hygiène informatique http://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/
Documents Annuaire Santé (Documents accessibles sur le site : **https://esante.gouv.fr/offres-services/annuaire-sante/acceder-aux-donnees**	
[ANN-EXT-PUB]	DSFT des données en libre accès de l'Annuaire Santé
[ANN-EXT-API]	Documentation sur l'API FHIR données publique Annuaire Santé

Tableau 52 : Liste des documents applicables

9.5 Documents de référence pour les services

Documents de référence accessibles sur le site de l'ANS : https://mssante.fr/is/doc-technique#ref1	
DR1	**Liste Blanche** : schéma XML définissant le format de la liste blanche des domaines MSSanté autorisés et exemple de liste blanche des domaines autorisés (signée)
DR2	**Annuaire** : description (WSDL) du Web Service d'alimentation en mode global de l'Annuaire Santé et du Web Service de récupération du compte rendu d'alimentation associé
DR3	**Annuaire** : schémas (XSD) pour les transactions d'alimentation de l'Annuaire Santé et de téléchargement d'une extraction de l'Annuaire Santé
DR4	**Statistiques MSSanté** : exemples de fichiers à transmettre à l'ANS : - Exemple du fichier statistiques MSSanté « Echanges » - Exemple du fichier statistiques MSSanté « Connexions » - Schémas (XSD) et exemples de comptes rendus produits en cas de soumission avec succès et de soumission en échec.
DR5	**Annuaire** : exemple de feuille de style que les Opérateurs peuvent utiliser pour l'affichage du compte-rendu d'alimentation
DR6	**Annuaire : exemples de fichiers d'alimentation et d'extraction**

Tableau 53 : Liste des documents de référence pour les services

9.6 Terminologie, acronymes et abréviations

Termes et abréviations

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
API LPS	Ensemble des transactions proposées par chacun des services MSSanté aux logiciels métiers (LGC, LGO, DPI, DUI, …) intégrant des fonctionnalités MSSanté utilisés par les professionnels. Le terme LPS est utilisé dans sa définition la plus large regroupant l'ensemble des logiciels des domaines sanitaire et médico-social.
API Opérateurs	Ensemble des transactions proposées par chacun des services de messageries permettant aux Opérateurs d'envoyer et de recevoir des messages entre eux
BAL	Boîte aux lettres
Connecteur MSSanté	Ensemble des équipements qui concourent à l'interconnexion à l'Espace de Confiance MSSanté.
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
DSML	Directory Service Markup Language
EAI	Enterprise Application Integration
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EHPAD	Etablissement d'hébergement pour personnes âgées
ES	Etablissement de Santé : terme recouvrant les établissements de soins publics et privés, incluant les plateaux techniques en ville et en hôpital
E-SSC	Dématérialisation des procédures de Soin Sans Consentement
ESB	Enterprise Service Bus
FAQ	Foire Aux Questions
FI	Fournisseur d'identité
IETF	Internet Engineering Task Force
GMSIH	Groupement pour la Modernisation du Système d'Information Hospitalier
HDS	Hébergeur de données de santé
IGC	Infrastructure de Gestion de Clés
INS	Identifiant National de Santé
IMAP	Internet Mail Access Protocol
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format

Abréviations	Signification
LFSS	Loi de Financement de la Sécurité Sociale
LGC	Logiciel de Gestion de Cabinet
LPS	Logiciel de Professionnel de Santé : abréviation générique désignant un . logiciel métier (LGC, LGO, DPI, DUI, …) intégrant des fonctionnalités MSSanté utilisés par les professionnels, dans des situations d'exercice libérale ou en structure. Le terme LPS est utilisé dans ce document dans sa définition la plus large regroupant l'ensemble des logiciels des domaines sanitaire et médico-social, intégrant des fonctionnalités d'échange via MSSanté. On utilise aussi indifféremment le terme client de messagerie MSSanté
MES	Mon Espace Santé
MIE	Moyen d'identification électronique
MIME	Multipurpose Internet Mail Extensions
MSS	Messagerie Sécurisée de Santé
MOA	Maîtrise d'Ouvrage
MTA	Mail Transport Agent
MUA	Mail User Agent (client de messagerie)
NAS	Nomenclature des Acteurs de Santé
NDR	Non-Delivery Report
OCSP	Online Certifcate Status Protocol
ODI	Outil de Diagnostic d'Installation
Opérateur professionnels	Désigne toute personne physique ou morale qui développe et fournit un service de Messageries Sécurisées de Santé au profit d'utilisateurs professionnel. 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…
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 MES.
OTP	One Time Password
Outil de tests et de contrôles de conformité	Désigne la solution logicielle mise à disposition par l'ANS à un l'Opérateur lui permettant : > d'effectuer des itérations de test pour la recette technique de son service de Messageries Sécurisées de Santé ; > de produire un rapport de tests de son service de Messageries Sécurisées de santé ayant pour finalité l'évaluation de son niveau de conformité aux exigences du Référentiel #1. Ce rapport de test est utilisé par l'ANS dans le cadre de sa mission de contrôle.
PAERPA	Personnes Agées En Risque de Perte d'Autonomie
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
RASS	Référentiel des Acteurs Sanitaires et Sociaux
Référentiel des identités PP/PM	Référentiel des identités de personnes et de structures issus du RPPS, FINESS et ADELI
REST	Representational State Transfer
RFC	Request For comments Série numérotée de documents officiels publiés par l'IETF
RGPD	Règlement Général sur la Protection des Données
RPPS	Répertoire Partagé des Professionnels intervenant dans le système de Santé
SAML	Security Assertion Markup Language
Service MSSanté	Service de Messageries Sécurisées de Santé proposé par un Opérateur à des Utilisateurs professionnel ou usager. Il s'agit d'un service standard d'émission et de réception de messages électroniques accompagnés ou non de documents (pièces-jointes) qui intègre des fonctionnalités spécifiques répondant aux besoins de garantir la sécurité et la confidentialité des données de santé échangées.
SI	Système d'Information

Abréviations	Signification
SSI	Sécurité du Système d'Information
SLA	Service Level Agreement
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)
TM	Transaction MSSanté
Utilisateur Usager	Désigne les usagers du système de santé utilisant la MSSanté pour échanger avec des professionnels habilités
VIHF	Vecteur d'Identification et d'Habilitation Formelles
WSDL	Web Services Description Language

Tableau 54 : Liste des acronymes et de leur signification

Légendes et abréviations utilisées dans les descriptions des attributs et règles

Les abréviations utilisées dans les descriptions des attributs et des règles sont définies dans le tableau suivant :

Abréviation		Description
Paragraphe : Description détaillée de l'écran		
Format	X(i)	Champ alphanumérique avec entre parenthèses le nombre de caractères
	N(i) N (i, j)	Champ numérique avec entre parenthèses le nombre de chiffres suivi (i) ou du nombre de décimales si nécessaire (j)
	Binaire (i)	Champ binaire avec entre parenthèse le nombre de bits
	DT(F)	Champ de type date au format F
	DT(AAAAMMJJ)	Champ de type date au format AAAAMMJJ
	DateTime	Horodatage de type AAAAMMJJ:HH:MM:SS
	LV (1,…, n)	Champ appartient à une liste de valeurs de 1 à n
	LD (Oui, Non)	Liste de valeurs avec les valeurs admises Oui et Non
Paragraphe : Traitements métiers et contrôles		
	RAi	Règle d'affichage suivie de son indice
Code	RMi	Règle métier suivie de son indice
	RCi	Règle de contrôle suivie de son indice
Le document en général		
S/O		Sans objet
PU, PR ou CO		Type de donnée Public (PU) ou Privée (PR) ou Confidentiel (CO)

Tableau 55 : Légendes et abréviations utilisées dans les descriptions des attributs et règles

9.7 Codes d’erreurs

9.7.1 Codes d’erreurs pour les Web Services de l’Annuaire Santé en SOAP - couche technique et d'échange

Le tableau ci-dessous liste les messages d’erreurs de la couche technique et d'échange pour les Web Services de l’Annuaire Santé en SOAP :

Code erreur	Définition
WSMSS01	L'en-tête de sécurité n'existe pas dans le message SOAP
WSMSS02	Le jeton SAML n'a pas été trouvé dans l'en-tête du message SOAP
WSMSS03	La date d'émission de l'assertion SAML (attribut IssueInstant) est obligatoire dans le jeton VIHF
WSMSS04	La date d'émission de l'assertion SAML (attribut IssueInstant) n'est pas valide, elle doit être antérieure à l'heure d'arrivée de l'assertion et inférieure au délai maximum acceptable
WSMSS05	L'identité de l'émetteur contenue dans le certificat de l'assertion SAML (élément Issuer) est obligatoire dans le jeton VIHF
WSMSS06	Echec d’authentification - L'identité de l'émetteur contenue dans le certificat de l'assertion SAML (élément Issuer) n’est pas présente dans la liste blanche des domaines autorisés
WSMSS07	La date de début de validité de l'assertion SAML (attribut NotBefore de l'élément Conditions) est obligatoire dans le jeton VIHF, si un élément Conditions est présent
WSMSS08	La date de début de validité de l'assertion SAML (attribut NotBefore de l'élément Conditions) n'est pas valide, elle doit être antérieure à l'heure d'arrivée de l'assertion et ultérieure à sa date d'émission
WSMSS09	La date de fin de validité de l'assertion SAML (attribut NotOnOrAfter de l'élément Conditions) est obligatoire dans le jeton VIHF, si un élément Conditions est présent
WSMSS10	La date de fin de validité de l'assertion SAML (attribut NotOnOrAfter de l'élément Conditions) n'est pas valide, elle doit être ultérieure à l'heure d'arrivée de l'assertion
WSMSS11	L'élément Profil_Utilisateur est obligatoire dans le jeton VIHF
WSMSS12	Schéma XML non conforme : message spécifique dépendant de l’erreur rencontré (cf tableau ci-dessous « Liste des contrôles liés à la vérification du schéma XML »)
WSMSS13	La valeur renseignée dans le champ Issuer est différent du DN du certificat d’authentification de l’Opérateur
WSMSS14	La valeur renseignée dans le champ Identifiant_structure est différent de l’identifiant structure du certificat d’authentification de l’Opérateur
WSMSS15	Le message ne peut pas être déposé dans le SAS de stockage pour être traité
WSMSS16	Le numéro de ticket ne correspond pas au DN du certificat d’authentification de l’Opérateur
WSMSS17	Le traitement n’est pas démarré ou est en cours. Le compte-rendu n’est pas encore disponible
WSMSS18	Le DN du certificat d'authentification de l'Opérateur n'est pas valide

Code erreur	Définition
WSMSS19	L'identifiant de l'utilisateur final (élément Subject NameID) est obligatoire dans le jeton VIHF
WSMSS20	L'identifiant de l'utilisateur final (élément Subject NameID) n'est pas valide, en authentification directe, il doit être renseigné avec le CN contenu dans le DN du certificat d'authentification
WSMSS21	La valeur de l'élément Profil_Utilisateur n'est pas valide
WSMSS22	L'élément Identifiant_structure est obligatoire dans le jeton VIHF
WSMSS23	Le numéro de ticket n'existe pas
WSMSS24	La demande d'alimentation est en échec
WSMSS25	Le fichier du compte-rendu de l'alimentation n'existe pas
WSMSS26	Le fichier du compte-rendu de l'alimentation ne peut être récupéré du SAS de stockage

Tableau 56 : Liste des messages d'erreurs pour la couche technique des Web Services en SOAP

Remarque : le tableau ci-dessous présente les contrôles appliqués spécifiquement par le serveur de l'Annuaire Santé lors de la vérification de conformité du schéma XML et associés au code erreur WSMSS 12 (le libellé décrit supra pour le code WSMSS12 est dans ce cas complété par un libellé spécifique permettant d'identifier l'erreur) :

Identifiant contrôle	Contrôle appliqué
RG_CTR_002	Vérification dans l'enregistrement qu'une valeur est présente pour l'attribut « TypeBal »
RG_CTR_003	Vérification que la valeur envoyée pour l'attribut « TypeBAL » fait partie des valeurs suivantes : PER (Personnelle), APP (Applicative), ORG (Organisationnelle) ou CAB (cabinet)
RG_CTR_004	Vérification, pour l'enregistrement chargé à partir du fichier, qu'une valeur est présente pour l'attribut « AdresseBal »
RG_CTR_006	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » ou « CAB », que la valeur envoyée pour l'attribut « TypeIdentifiantPP » fait partie de la nomenclature Type d'identifiant PP
RG_CTR_015	Vérification, pour l'enregistrement avec un identifiant de structure obligatoire (BAL de type ORG ou APP, ou PER avec identifiant interne), que le type l'identifiant transmis « TypeIdentifiantPM » correspond à : 1 : FINESS 2 : SIREN 3 : SIRET Toute autre type d'identifiant est rejeté.
RG_CTR_032	Vérification pour tout enregistrement que l'attribut « ListeRouge » est renseigné
RG_CTR_046	Vérification que la valeur envoyée pour l'attribut « AdresseBAL » est au maximum de 256 caractères

Tableau 57 : Liste des contrôles liés à la vérification du schéma XML dans le cas du code WSMSS12

9.7.2 Codes d'erreurs pour les Web Services de l'Annuaire Santé en REST - couche technique et d'échange

Le tableau ci-dessous liste les messages d'erreurs de la couche technique et d'échange pour les Web Services de l'Annuaire Santé en REST :

Statut	Code	Description
400	Bad Request	La requête n'est pas valide (paramètres manquants/incorrects, body manquant/incorrect, ...)
401	Access Denied	L'authentification du client a échoué (dans le cas où une authentification est nécessaire) ou bien le quota d'appel est dépassé
403	Forbidden	L'authentification du client a réussi mais il n'est pas habilité sur le service ou sur la ressource demandée
404	Not found	Le service ou la ressource n'a pas été trouvé
405	Method Not Allowed	La méthode HTTP n'est pas supportée par ce service ou cette ressource
500	Internal error	Le serveur a rencontré un problème
503	Service Unavailable	Le service n'est pas disponible pour le moment (ex: serveur surchargé, opération de maintenance, ...)

Tableau 58 : Liste des messages d'erreurs pour la couche technique des Web Services en REST

9.7.3 Codes d'erreurs pour la TM1.1.xP - Mise à jour des comptes de messagerie dans l'Annuaire Santé

Pour chaque enregistrement BAL MSSanté traité, les contrôles sont appliqués dans l'ordre suivant :

- Contrôles de format ;
- Contrôle de présence de données obligatoires ;
- Contrôles d'existence du code dans les nomenclatures.

Ces contrôles s'arrêtent à la première anomalie bloquante trouvée.

Si les enregistrements sont conformes à cette première série de contrôles, alors l'ensemble des contrôles listés ci-dessous sont effectués (même en cas d'erreur).

Le tableau ci-dessous liste les contrôles effectués par le serveur de l'Annuaire Santé lors de l'intégration des BAL publiées par les Opérateurs, les codes d'erreurs et les messages fonctionnels associés :

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
RG_CTR_000	Vérification que le domaine est présent dans la liste blanche des domaines autorisés	MSS000	Le nom de domaine communiqué n'existe pas dans la liste blanche	Bloquante
RG_CTR_001	Vérification que le domaine de la BAL envoyé dans l'entrée du corps du message correspond au domaine de la BAL de la ligne d'adresse MSSanté à alimenter	MSS001	Le domaine de la BAL ne correspond pas au domaine alimenté	Bloquante

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
RG_CTR_005	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » ou « CAB », qu'une valeur est présente pour l'attribut « TypeIdentifiantPP »	MSS005	Le type d'identifiant personne physique est obligatoire pour les BAL MSSanté de type PER - Personnelle	Bloquante
RG_CTR_007	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » ou « CAB », qu'une valeur est présente pour l'attribut « IdentifiantPP »	MSS007	L'identifiant personne physique est obligatoire pour les adresses BAL MSSanté de type PER (Personnelle)	Bloquante
RG_CTR_008	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type RPPS ou ADELI (« TypeIdentifiantPP » = « 0 » ou « 8 »), que l'identifiant envoyé est déjà référencé dans la table des Personnes physiques ou de l'historique des identifiants ADELI, s'il s'agit d'un type ADELI.	MSS008	L'identifiant national du professionnel de santé transmis n'existe pas dans le référentiel des identités PP/PM	Bloquante
RG_CTR_009	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP avec identifiant interne (« typeIdentifiantPP »= « 10 »), qu'une valeur est présente pour l'attribut « TypeIdentifiantPM »	MSS009	Le type d'identifiant de la structure d'activité est obligatoire pour les BAL MSSanté d'un professionnel de santé avec identifiant interne	Bloquante
RG_CTR_010	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que la valeur envoyée pour l'attribut « TypeIdentifiantPM » fait partie de la nomenclature Type d'identifiant PM (N_TYP_ID_PM)	MSS010	Le type d'identifiant de la structure d'activité transmis n'est pas présent dans la nomenclature de référence utilisée	Bloquante
RG_CTR_011	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP », qu'une valeur est présente pour l'attribut « TypeIdentifiantPM »	MSS011	Le type d'identifiant de la structure d'activité est obligatoire pour les adresses de BAL MSSanté de type Organisationnelle ou Applicative	Bloquante
RG_CTR_012	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP », que la valeur envoyée pour l'attribut « TypeIdentifiantPM» fait partie de la nomenclature Type d'identifiant PM	MSS010	Le type d'identifiant de la structure d'activité transmis n'est pas présent dans la nomenclature de référence utilisée	Bloquante
RG_CTR_013	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), qu'une valeur est présente pour l'attribut « IdentifiantPM »	MSS012	L'identifiant de la structure d'activité est obligatoire pour les adresses de BAL MSSanté d'un professionnel de santé avec identifiant interne	Bloquante
RG_CTR_014	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP », qu'une valeur	MSS013	L'identifiant de la structure d'activité est obligatoire pour les	Bloquante

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
	est présente pour l'attribut « IdentifiantPM »		BAL MSSanté de type Organisationnelle ou Applicative	
RG_CTR_016	Vérification, pour l'enregistrement avec un identifiant structure obligatoire (BAL de type ORG ou APP, ou PER avec identifiant interne), que l'identifiant transmis « IdentifiantPM » est référencé dans la table des sites ou des entités juridiques	MSS015	L'identifiant de la structure d'activité transmise n'existe pas dans le référentiel des identités PP/PM	Bloquante
BAL PER avec identifiant type 10				
RG_CTR_017	Vérification, pour l'enregistrement d'une de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que la valeur envoyée pour l'attribut « CiviliteExercice » fait partie de la nomenclature Civilité d'exercice	MSS016	La valeur de la civilité d'exercice n'est pas conforme à la nomenclature utilisée	Bloquante
RG_CTR_018	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que la valeur envoyée pour l'attribut « CiviliteExercice » correspond à la profession envoyée	MSS017	La valeur de la civilité d'exercice n'est pas conforme à la profession transmise pour le professionnel de santé	Bloquante
RG_CTR_019	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER », qu'une valeur est présente pour l'attribut « NomExercice »	MSS018	Le nom d'exercice est obligatoire pour tout professionnel de santé avec ou sans identifiant national	Bloquante
RG_CTR_020	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER », qu'une valeur est présente pour l'attribut «PrénomExercice »	MSS019	Le prénom d'exercice est obligatoire pour tout professionnel de santé avec ou sans identifiant national	Bloquante
RG_CTR_021	Vérification pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type RPPS ou ADELI (TypeidentifiantPP = 0 ou 8) que le contrôle de cohérence entre les valeurs transmises pour Nom/Prénom et les valeurs connues dans l'Annuaire Santé est positif. Ce contrôle est évolutif, par conséquent, le libellé complet du contrôle en vigueur au moment de l'alimentation sera présent dans le compte-rendu d'alimentation. Pour information, le contrôle de cohérence actuel vérifie que la première lettre du prénom et les deux premières lettres du nom - après la normalisation (sans : accents-tirets-apostrophe-espaces) - sont identiques aux valeurs connues dans l'Annuaire Santé.	MSS020	Le nom et/ou le prénom d'exercice du professionnel de santé ne correspondent pas au nom et/ou prénom d'exercice rattachés à l'identifiant national dans l'Annuaire Santé	Warning

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
RG_CTR_022	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « CategorieProfessions» est renseigné	MSS021	La catégorie de profession est obligatoire pour la BAL d'un professionnel de santé avec identifiant interne	Bloquante
RG_CTR_023	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « CategorieProfessions » est référencé dans la table de nomenclature Catégorie de professions	MSS022	La valeur transmise pour la catégorie de professions n'est pas présente dans la nomenclature de référence utilisée	Bloquante
RG_CTR_024	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP avec identifiant interne (« typeIdentifiantPP »= « 10 »), que l'attribut « CategorieProfessions» est alimenté par la catégorie de profession "01" (Professionnel de Santé)	MSS023	La valeur transmise pour la Catégorie de profession n'est pas autorisée	Bloquante
RG_CTR_025	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « Profession» est renseigné	MSS024	La profession est obligatoire pour la BAL d'un professionnel de santé avec identifiant interne	Bloquante
RG_CTR_026	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « Profession » est référencé dans la table de nomenclature Profession	MSS025	La valeur transmise pour la profession n'est pas présente dans la nomenclature de référence utilisée	Bloquante
RG_CTR_027	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 ») que l'attribut « Spécialité » est référencé dans la table de nomenclature Savoir-faire jeux de valeurs Spécialité ou compétence exclusive ou qualification PAC	MSS026	La valeur transmise pour la spécialité n'est pas présente dans la nomenclature de référence utilisée	Bloquante
RG_CTR_028	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « Spécialité » transmis est autorisé pour la Profession envoyée	MSS027	Cette spécialité n'est pas autorisée pour la profession indiquée	Bloquante
BAL ORG & APP				
RG_CTR_029	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP » ou « CAB »,	MSS028	Le responsable est obligatoire pour une BAL de type	Bloquante

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
	que l'attribut « Responsable » est renseigné		Applicative ou Organisationnelle	
RG_CTR_030	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP » ou « CAB », que l'attribut « Description » est renseigné	MSS029	La description est obligatoire pour une BAL de type Applicative ou Organisationnelle	Bloquante
RG_CTR_033	Vérification que si la valeur de « TypeIdentifiantPM » est 2 ou 3, le PM correspondant à « IdentifiantPM » n'a pas de numéro FINESS	MSS032	L'identification par un SIRET ou SIREN n'est acceptée que si la structure n'a pas de numéro FINESS	Bloquante
RG_CTR_034	Vérification que si l'identifiantPM est renseigné pour un « TypeBAL » = « PER » (de « TypeIdentifiantPP » = « 0 » ou « 8 ») cet identifiant PM correspond bien à une structure associée à la PP du référentiel	MSS033	L'identifiant de structure fourni ne correspond pas à une structure d'exercice connue de la personne : la BAL est rattachée à la PP et à la structure indiquée dans le flux d'alimentation (et uniquement à cette structure)	Warning
RG_CTR_035	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « IdentifiantPP » = attribut « AdresseBAL »	MSS034	L'identifiant interne pour un professionnel de santé avec identifiant interne doit être identique à la valeur de la BAL MSSanté	Bloquante
RG_CTR_036	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type « TypeIdentifiantPP » = « 0 » ou « 8 », que l'attribut « IdentifiantPM » est renseigné avant de prendre en compte la valeur transmise pour l'attribut « ServiceRattachement »	MSS035	Pour les types de BAL PP RPPS ou ADELI, la valeur indiquée pour le service de rattachement ne peut être prise en compte que si un identifiant de structure est renseigné	Bloquante
RG_CTR_037	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER », que la valeur envoyée pour l'attribut « TypeIdentifiantPP » correspond à un code ouvert de la nomenclature Type d'identifiant PP	MSS036	Le type d'identifiant personne physique transmis est fermé dans la nomenclature de référence utilisée	Warning
RG_CTR_038	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que la valeur envoyée pour l'attribut « TypeIdentifiantPM » correspond à un code ouvert de la nomenclature Type d'identifiant PM	MSS037	Le type d'identifiant de la structure d'activité transmis est fermé dans la nomenclature de référence utilisée	Warning
RG_CTR_039	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP », que la valeur envoyée pour l'attribut « TypeIdentifiantPM» correspond à	MSS037	Le type d'identifiant de la structure d'activité transmis est fermé dans la nomenclature de référence utilisée	Warning

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
	un code ouvert de la nomenclature Type d'identifiant PM			
RG_CTR_040	Vérification, pour l'enregistrement d'une de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que la valeur envoyée pour l'attribut « CiviliteExercice » correspond à un code ouvert de la nomenclature Civilité d'exercice	MSS038	La valeur de la civilité d'exercice est fermée dans la nomenclature utilisée	Warning
RG_CTR_041	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « CategorieProfessions » correspond à un code ouvert de la nomenclature Catégorie de professions	MSS039	La valeur transmise pour la catégorie de professions est fermée dans la nomenclature de référence utilisée	Warning
RG_CTR_042	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « Profession » correspond à un code ouvert de la table de nomenclature Profession	MSS040	La valeur transmise pour la profession est fermée dans la nomenclature de référence utilisée	Warning
RG_CTR_043	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 ») que l'attribut « Spécialité » correspond à un code ouvert de la table de nomenclature Savoir-faire jeux de valeurs Spécialité ou compétence exclusive ou qualification PAC	MSS041	La valeur transmise pour la spécialité est fermée dans la nomenclature de référence utilisée	Warning
RG_CTR_044	Vérification de l'unicité de l'adresse BAL MSSanté dans le fichier source	MSS042	L'adresse de la BAL MSSanté doit être unique dans le fichier d'alimentation	Bloquante
RG_CTR_045	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type ADELI (« TypeIdentifiantPP » = « 0 »), que l'identifiant envoyé est bien l'identifiant national associé au PS au moment de la publication et non un identifiant antérieur (par exemple, l'Opérateur doit transmettre le numéro RPPS et plus le numéro ADELI le cas échéant).	MSS043	L'identifiant national du professionnel de santé transmis n'est plus l'identifiant national valide dans le référentiel des identités PP/PM.	Warning
RG_CTR_047	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 ») et catégorie de profession "professionnel social" (code = "06),	MSS045	L'identifiant de la structure d'activité est recommandé pour les adresses de BAL MSSanté d'un professionnel social	Warning

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
	qu'une valeur est présente pour l'attribut « IdentifiantPM »			
RG_CTR_048	Vérification, pour l'enregistrement avec un identifiant structure facultatif (BAL de type PER avec identifiant interne (« typeIdentifiantPP »= « 10 ») et catégorie de profession "professionnel social" (code = "06), que l'identifiant transmis « IdentifiantPM » est référencé dans la table des sites ou des entités juridiques (M_SITE : NO_FINESS_ET ou NO_SIRET, M_ENT_JUR : NO_FINESS ou NO_SIREN)	MSS046	L'identifiant de la structure d'activité transmise n'existe pas dans le référentiel des identités PP/PM	Warning
RG_CTR_049	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP avec identifiant national RPPS (« typeIdentifiantPP »= « 8 »), que l'attribut « N_CAT_PROF» d'au moins un exercice professionnel actif de la table RASS « M_EXE_PRO » ne correspond pas à « Etudiant » (code =E)	MSS047	Le numéro RPPS indiqué est attribué à un étudiant.	Bloquante

Tableau 59 : Contrôles effectués sur la TM1.1.xP

(*) Les libellés des messages d'erreur sont fournis à titre d'information et sont susceptibles d'être modifiés par l'ANS.

(**) La criticité est fournie à titre d'information et peut-être modifiée à l'initiative de l'ANS sur le serveur de l'Annuaire Santé :

- Une criticité « bloquante » entraîne le rejet de l'enregistrement ;
- Une criticité « warning » n'entraîne pas de rejet de l'enregistrement mais produit une entrée dans le compte-rendu d'intégration pour indiquer à l'Opérateur une incohérence dans les données.

Remarque sur RG_CTR_034 : si l'IdentifiantPM ne correspond pas à un lieu d'activité du PP (ADELI ou RPPS) connue de l'Annuaire Santé, alors :

- La BAL est créée et rattachée à la PP et à la structure indiquée dans le flux d'alimentation ;
- Les situations d'exercice RPPS (connues de l'Annuaire Santé) ne sont pas impactées.

Dans ce cas de figure, en consultation de l'Annuaire, la BAL de la PP pour cette structure n'est rattachée qu'à cette structure et à elle seule.

9.7.4 Codes d'erreurs pour la soumission des fichiers indicateurs

9.7.4.1 Les codes retours lors de l'authentification aux webservices de dépôt et de récupération

Code	Message	Raison
10	La recuperation de la liste blanche a echoue	La liste blanche n'a pas pu être récupérée pour vérifier que l'Opérateur fait bien parti de l'Espace de Confiance. La connexion de l'Opérateur est donc refusée.
20	Acces refuse. Le certificat n'est pas lisible	Le certificat de l'Opérateur n'est pas lisible, sa connexion est refusée

30	Acces refuse. Le certificat presente n'appartient pas a l'Espace de Confiance	L'Opérateur ne fait pas partie de l'Espace de Confiance, sa connexion est refusée.
100	Une erreur technique est survenue	

Tableau 60 : codes retours lors de l'authentification aux webservices de soumission de fichiers statistiques

9.7.4.2 Les codes retours du webservice de dépôt de l'archive contenant les fichiers statistiques

Code	Message	Raison
0	Depot de l'archive OK	L'archive a été déposée correctement sur les serveurs
1	Depot de l'archive KO - Erreur technique	Suite à une erreur technique l'archive n'a pas pu être déposée sur les serveurs
2	Depot de l'archive KO - Taille trop grande	La taille de l'archive dépasse 70 Mo, le dépôt est refusé
3	Depot de l'archive KO - Type Mime non autorise	Format de l'archive non autorisé (tout autre format que le format zip)
4	Dépôt de la partie de l'archive OK	Le dépôt du segment d'archive a été réalisé avec succès.
5	Partie déjà déposée et écrasée	Le dépôt concerne un segment qui avait déjà été déposé : le nouveau dépôt a donc écrasé l'ancien dépôt de ce segment.
6	Depot de l'archive KO - Le nombre total de parties dépasse le maximum autorisé	Le nombre renseigné dans l'entête Total-File-Parts est supérieur à la limite fixée en Erreur ! S ource du renvoi introuvable. Erreur ! Source du renvoi introuvable.
7	Depot de l'archive KO - Le nombre total de parties a changé	Le nombre renseigné dans l'entête Total-File-Parts est différent de celui précisé dans un dépôt de segment précédent.
8	Depot de l'archive KO - Le numéro de la partie dépasse le total	Le nombre renseigné dans l'entête File-Parts est supérieur à celui indiqué dans l'entête Total-File-Parts.
100	Une erreur technique est survenue	Une erreur technique est survenue lors de la vérification de l'Opérateur dans la liste blanche

Tableau 60 : Codes retours lors du dépôt des fichiers statitisques

9.7.4.3 Les codes retours du webservice de récupération du compte rendu.

Code	Message	Raison
0	Tous les fichiers de l'archive ont été traités OK ou en Warning	Tous les fichiers de l'archive ont été traités OK ou en Warning

1	Une partie des fichiers de l'archive sont OK ou en Warning, les autres KO	Une partie des fichiers de l'archive sont OK ou en Warning, les autres KO
2	Tous les fichiers de l'archive ont été traités KO	Tous les fichiers de l'archive ont été traités KO
4	L'archive n'a pas pu être traitée : Archive vide	L'archive est vide, aucun traitement n'est donc réalisé
5	L'archive n'a pas pu être traitée : - Archive ne pouvant être ouverte	L'archive n'a pas pu être décompressé et les fichiers extraits. Elle n'est donc pas traitée.
6	L'archive est toujours en cours de traitement	Le traitement de l'archive et de l'ensemble de ses fichiers n'est pas terminé. Il faut alors solliciter le service ultérieurement pour obtenir le CR de traitement terminé.
7	L'archive n'a pas pu être traitée : Virus trouve	L'antivirus a détecté un virus dans l'archive et son contenu. L'archive n'est donc pas traitée
8	L'archive n'a pas pu être traitée : autre	
99	L'archive n'existe pas	Aucune archive n'est trouvé pour l'identifiant fourni
100	Une erreur technique est survenue	

Tableau 61 : Codes retours de la récupération du compte rendu

9.7.4.4 Les codes retours appliqués suites aux contrôles des fichiers « Echanges » et « Connexions»

Code	Message	Raison
0	OK	Le contrôle concerné est passant
1	KO	Le contrôle concerné est KO
2	Warning	Le contrôle concerné est passant mais remonte un warning
100	Une erreur technique est survenue	

Tableau 62 : Codes retours des contrôles sur les fichiers « Echanges » et « Connexions »

9.7.4.4.1 Les contrôles appliqués au fichier « Echanges » sont :

N°	Type de contrôle	Contrôle	Description
1	Bloquant	Contrôle du nom du fichier	Contrôle de la syntaxe du nom du fichier de l'archive zip. Le nom doit être : (AAAAMM)_EchangesMSSante_[Domaine].csv
2	Bloquant	Contrôle encodage	Contrôle de l'encodage du fichier en UTF8

3	Bloquant	Contrôle encodage	Contrôle de l'encodage du fichier : retour à la ligne Unix
4	Bloquant	Contrôle du séparateur	Le séparateur doit être le point-virgule.
5	Bloquant	Contrôle du nombre de champ	Le fichier doit contenir 5 champs par ligne
6	Bloquant	Contrôle du nommage des champs dans l'entête	Le nommage des champs doit respecter celui établi dans le **Référentiel #1** Opérateurs. La casse doit être prise en compte.
7	Bloquant	Contrôle de la cohérence des lignes	Le fichier ne contient que des données exploitables cohérentes avec ce qui est défini pour chacun des champs dans le **Référentiel #1**
8	Bloquant	Opérateur habilité pour déposer pour un domaine ?	Vérifier dans la liste blanche si l'Opérateur est gestionnaire du domaine présent dans le nom du fichier
9	Bloquant	Contrôle de la période	La période déclarée doit être celle du mois précédent le traitement. • warning : Si l'écart est de 1 mois : information retournée à l'Opérateur rappelant les conditions de soumission ; • warning : Si l'écart se situe entre 1 et 3 mois : warning indiquant à l'Opérateur que son fichier est susceptible de ne pas être intégré et rappel des conditions de soumission ; • bloquant : Si l'écart est supérieur à 3 mois : warning indiquant à l'Opérateur que son fichier ne sera pas traité et rappel et des conditions de soumission.
10	warning	Fichier déjà reçu avec contrôle OK	Si un fichier OK a déjà été soumis avec le même nom pour cette période alors un warning est remonté

Tableau 63 : Contrôles appliqués au fichier « Echanges »

9.7.4.4.2 Les contrôles appliqués au fichier « Connexions » sont :

N°	Type de contrôle	Contrôle	Description
1	Bloquant	Contrôle du nom du fichier	Contrôle de la syntaxe du nom du fichier de l'archive zip. Le nom doit être : (AAAAMM)_ConnexionsMSSante_[Domaine].csv
2	Bloquant	Contrôle encodage	Contrôle de l'encodage du fichier en UTF8
3	Bloquant	Contrôle encodage	Contrôle de l'encodage du fichier : retour à la ligne Unix
4	Bloquant	Contrôle du séparateur	Le séparateur doit être le point-virgule.
5	Bloquant	Contrôle du nombre de champ	Le fichier doit contenir 2 champs par ligne
6	Bloquant	Contrôle du nommage des champs dans l'entête	Le nommage des champs doit respecter celui établi dans le **Référentiel #1** Opérateurs. La casse doit être prise en compte.
7	Bloquant	Contrôle de la cohérence des lignes	Le fichier ne contient que des données exploitables cohérentes avec ce qui est défini pour chacun des champs dans le **Référentiel #1**
8	Bloquant	Opérateur habilité pour déposer pour un domaine ?	Vérifier dans la liste blanche si l'Opérateur est gestionnaire du domaine présent dans le nom du fichier
9	Bloquant	Contrôle de la période	Pour chaque domaine d'un fichier, vérifier dans la liste blanche si l'opérateur est gestionnaire de ce domaine
10	Bloquant	Contrôle de la période	La période déclarée doit être celle du mois précédent le traitement. • warning : Si l'écart est de 1 mois : information retournée à l'Opérateur rappelant les conditions de soumission ; • warning : Si l'écart se situe entre 1 et 3 mois : warning indiquant à l'Opérateur que son fichier est susceptible de ne pas être intégré et rappel des conditions de soumission ; • bloquant : Si l'écart est supérieur à 3 mois : warning indiquant à l'Opérateur que son fichier ne sera pas traité et rappel et des conditions de soumission.
11	warning	Fichier déjà reçu avec contrôle OK	Si un fichier OK a déjà été soumis avec le même nom pour cette période alors un warning est remonté

Tableau 64 : Contrôles appliqués au fichier « Connexions »

9.8 Eléments nécessaires à la réalisation d'une analyse de risque

Menaces prises en compte

Ce chapitre donne la liste et les caractéristiques des sources de menaces à prendre en compte dans la sécurisation du service de messagerie sécurisée.

Types de sources de menaces	Retenu ou non
Source humaine interne, malveillante, avec de faibles capacités	Oui
Source humaine interne, malveillante, avec des capacités importantes	Oui
Source humaine interne, malveillante, avec des capacités illimitées	Oui
Source humaine externe, malveillante, avec de faibles capacités	Oui
Source humaine externe, malveillante, avec des capacités importantes	Oui
Source humaine externe, malveillante, avec des capacités illimitées[8]	**Non**
Source humaine interne, sans intention de nuire, avec de faibles capacités	Oui
Source humaine interne, sans intention de nuire, avec des capacités importantes	Oui
Source humaine interne, sans intention de nuire, avec des capacités illimitées	Oui
Source humaine externe, sans intention de nuire, avec de faibles capacités	Oui
Source humaine externe, sans intention de nuire, avec des capacités importantes	Oui
Source humaine externe, sans intention de nuire, avec des capacités illimitées	Non
Code malveillant d'origine inconnue	Oui
Phénomène naturel	Oui
Catastrophe naturelle ou sanitaire	Oui
Événement interne	Oui

Tableau 65 : Types de sources de menaces

[8] Organisation criminelle, agence gouvernementale ou organisation sous le contrôle d'un État étranger, espions, organisation terroriste (EBIOS 2010).

9.9 Rappel des principaux scénarios de menaces

Ce chapitre présente les menaces auxquelles le service de MSSanté est exposé. Ces menaces peuvent impacter la sécurité du service et en particulier des messages.

Ces menaces peuvent être classées en trois catégories :

1. Les menaces internes au service MSSanté
   Leur origine provient des vulnérabilités des biens supports du système de Messageries Sécurisées de Santé (système informatique et réseau (matériel, logiciel, etc.), organisation, locaux, etc.). Ces menaces sont donc propres à chaque Opérateur et aux biens supports qu'il mobilise pour mettre en œuvre son service. L'ANSSI met à disposition une base de connaissance des menaces génériques portant sur les biens support des SI dans le cadre de la promotion de sa méthodologie d'analyse des risques EBIOS.

2. Les menaces externes
   Ces menaces sont liées à la gestion des identités et du moyen d'authentification :
   - Suite à des erreurs, des falsifications en entrée ou à des dysfonctionnements de l'annuaire des utilisateurs, ce dernier fournit au système de Messageries Sécurisées de Santé des informations sur les PS qui comportent des défauts d'intégrité (doublons, erreurs, lacunes). Cela permet à une personne non autorisée d'accéder au service ;
   - Une personne accède au service de Messagerie Sécurisée de Santé avec les paramètres d'authentification obtenus auprès de leur détenteur légitime, par vol et observation, ingénierie sociale ou prêt, ou encore par erreur d'attribution.

3. Les menaces fonctionnelles
   Leur origine provient des « vulnérabilités » des utilisateurs du service de Messagerie Sécurisée de Santé et de celles des moyens d'accès que ces personnes utilisent pour bénéficier des informations et des services offerts par le système. Leur prise en compte est nécessaire pour déterminer le traitement des risques SSI résultants au niveau du service délivré.

Les menaces sont les suivantes :

- Un utilisateur commet une erreur ou une négligence lors de son utilisation du service de Messagerie Sécurisée de Santé ;
- Un utilisateur effectue des actions qui lui sont autorisées dans le service de Messagerie Sécurisée de Santé, mais qui vont au-delà de ce qui est lui strictement nécessaire (envoi de messages non sollicités ou envoi de messages avec contenu dangereux par exemple) ou qui portent atteinte aux composants informatiques, aux supports de stockage du moyen d'accès ou aux données accessibles. Il peut s'agir aussi d'un déni d'actions (actions volontairement non effectuées ou retardées) ;
- Une personne malintentionnée accède logiquement au service de Messagerie Sécurisée de Santé sous l'identité d'un utilisateur autorisé ou effectue des actions dans le système à sa place ;
- Une personne malintentionnée installe délibérément ou fait installer fortuitement une fonction matérielle ou logicielle malveillante (cheval de Troie, ver ou virus informatique, bombe logique etc.) dans un matériel, un logiciel ou un élément de réseau constituant le moyen d'accès de l'utilisateur. La fonction empêche cette personne d'utiliser le service de Messagerie Sécurisée de Santé conformément à ce qui est prévu ;
- Une personne malintentionnée introduit des données falsifiées, dans le moyen d'accès, par insertion ou substitution d'un matériel ou d'un support de stockage, par écriture illicite dans l'un de ces éléments, par accès à partir du réseau externe.

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