



Principes, exigences et interfaces opérateurs

du Système de Messageries Sécurisées de Santé (MSSanté)

Dossier des Spécifications Fonctionnelles et Techniques (DSFT)

Identification du document	
Référence ASIP Santé	MSS_FON_DSFT_Opérateurs_MSSanté_v1.3.1.PDF
Date de dernière mise à jour	11/03/2020
Classification	Non sensible public
Nombre de pages	215

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 : les bals msscompatibilite@sante.gouv.fr, incidentsoperateurs@asipsante.fr, mssindicateurs@sante.gouv.fr ne sont plus accessibles et sont remplacées par monserviceclient.mssante@asipsante.fr.
V1.2.1	21/12/2018	Version apportant des précisions sur certains éléments existants du DSFT et de nouvelles recommandations.
V1.3	14/11/2019	Version introduisant : <ul style="list-style-type: none"> - 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 Cette version majeure nécessite un réengagement dans les six mois suivant la date de publication (envoi du document « Engagement de conformité MSSanté » - Annexe 2 au contrat «opérateur MSSanté ») de la part des opérateurs MSSanté.
V1.3.1	11/03/2020	Version apportant certaines modifications/corrections mineures au document et concernant : <ul style="list-style-type: none"> - 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 La version 1.3 du DSFT est celle à indiquer lors de l'envoi du document « Engagement de conformité MS Santé » - Annexe 2 au contrat «opérateur MSSanté »)

Sommaire

Sommaire	3
1 Introduction.....	6
1.1 Objet du document.....	6
1.2 Guide de lecture.....	7
1.3 Gestion des versions successives.....	8
2 La nécessité de mettre en œuvre un système de Messageries Sécurisées de Santé	9
2.1 Contexte de mise en œuvre du système de Messageries Sécurisées de Santé.....	9
2.2 Définition du système de Messageries Sécurisées de Santé.....	10
2.3 Un système de Messageries Sécurisées de Santé conforme au cadre juridique	12
2.4 Les acteurs de l'espace de confiance MSSanté	14
2.4.1 L'ASIP Santé.....	14
2.4.2 Les opérateurs de messageries sécurisées de santé	14
2.4.3 Les utilisateurs finaux.....	15
2.5 Intégration des opérateurs à l'espace de confiance MSSanté	16
2.6 Focus sur les formalités préalables à accomplir par le responsable de traitement..	18
2.6.1 Cas n°1 – vous fournissez un service de messagerie sécurisée de santé et vos utilisateurs finaux exercent à titre libéral.....	19
2.6.2 Cas n°2 - Une structure de soins (établissement de santé, laboratoire de biologie médicale, EHPAD, etc.) décide de mettre à la disposition de ses professionnels salariés le service de messagerie sécurisée de santé que vous fournissez.....	20
2.6.3 Cas n°3 - Vous êtes une structure de soins et décidez d'opérer votre propre service de messagerie sécurisée de santé	21
2.7 mssante.fr une marque de confiance	22
3 Description du fonctionnement du système de Messageries Sécurisées de Santé	23
3.1 Domaine MSSanté et groupe de domaines autorisés.....	23
3.2 L'Annuaire national MSSanté	25
3.3 Connecteur MSSanté d'un opérateur	26
3.4 Connecteur à l'Annuaire national MSSanté	27
3.5 Les clients de messagerie MSSanté	27
3.5.1 Le LPS au cœur des Systèmes d'Information de Santé	27
3.5.2 Le cadre d'interopérabilité des SIS et interopérabilité des échanges de données de santé structurées	28
3.5.3 Fonctions et interfaces pour les clients de messagerie.....	29
3.6 Exemples de mise en œuvre.....	30
3.6.1 Accès à l'espace de confiance	30
3.6.2 Accès à une BAL MSSanté	34
3.6.3 Consultation de l'Annuaire national MSSanté.....	39
3.6.4 Publication des adresses MSSanté par les opérateurs.....	43
4 Gestion des boîtes aux lettres au sein de l'espace de confiance MSSanté	44
4.1 Les Boîtes Aux Lettres (BAL) MSSanté.....	44
4.1.1 Présentation des types de BAL	45
4.1.2 Les statuts (états) des BAL de l'espace de confiance MSSanté	47
4.2 Les acteurs de l'espace de confiance MSSanté	48
4.2.1 Les rôles dans l'espace de confiance MSSanté	48
4.2.2 Les acteurs éligibles à l'espace de confiance MSSanté	48
4.3 L'ouverture de boîte aux lettres au sein de l'espace de confiance MSSanté.....	51
4.4 Les règles de fonctionnement des boîtes aux lettres au sein de l'espace de confiance MSSanté.....	53
4.4.1 Fonctionnalités relatives aux BAL de l'espace de confiance MSSanté	53
4.4.2 Mesures de sécurité propres aux messageries MSSanté	54
4.5 Suspension d'une boîte aux lettres de l'espace de confiance MSSanté.....	55

4.5.1	Caractéristiques d'une BAL suspendue.....	55
4.5.2	Comment suspendre une boîte aux lettres de l'espace de confiance	55
4.6	Suppression d'une boîte aux lettres de l'espace de confiance MSSanté	56
5	Exigences fonctionnelles et techniques à respecter par les opérateurs MSSanté	57
5.1	Choix des transactions à implémenter pour le Connecteur MSSanté d'un opérateur 58	
5.2	Modalités techniques pour assurer la sécurisation des échanges	60
5.2.1	Principes de raccordement des Connecteurs MSSanté des opérateurs à l'espace de confiance MSSanté	60
5.2.2	Validation des certificats serveur.....	62
5.3	Modalités techniques spécifiques aux Web Services de l'Annuaire national MSSanté.....	65
5.3.1	Sécurisation des échanges	65
5.3.2	Web Services de l'Annuaire national MSSanté en SOAP	66
5.3.3	Web Services de l'Annuaire national MSSanté en REST	77
5.4	Publication de BAL MSSanté dans l'Annuaire national MSSanté	80
5.4.1	Description fonctionnelle	80
5.4.2	TM1.1.1P - Mise à jour des BAL dans l'Annuaire national MSSanté en Web Services en mode global et récupération du compte –rendu d'alimentation	88
5.5	Consultation de l'Annuaire national MSSanté.....	113
5.5.1	TM2.1.1A - Consultation de l'Annuaire national MSSanté par le protocole LDAP 113	
5.5.2	TM2.1.3A - Téléchargement d'une extraction de l'Annuaire national MSSanté 116	
5.5.3	TM2.1.4A - Téléchargement des données d'identités des futurs utilisateurs finaux 123	
5.6	Liste blanche des domaines MSSanté autorisés	131
5.6.1	Description et format de la liste blanche.....	131
5.6.2	TM4.1P - Interrogation de la liste blanche des domaines de messagerie MSSanté	133
5.6.3	Vérification de la signature de la liste blanche.....	134
5.7	Réception et émission de messages	135
5.7.1	TM3.1P – Réception de messages.....	135
5.7.2	TM3.2P – Emission de messages	137
5.8	Autres exigences applicables aux opérateurs MSSanté	139
5.8.1	Synchronisation du temps	139
5.8.2	Gestion des traces	140
5.8.3	Production et soumission de statistiques d'utilisation	143
5.8.4	Définition de Conditions Générales d'Utilisation (CGU) du service MSSanté	152
5.8.5	Exigences complémentaires de sécurité	154
5.8.6	Système d'auto-configuration pour les clients de messagerie	161
6	Synthèse des exigences applicables aux opérateurs MSSanté	162
7	Différences avec les précédentes versions	175
8	Annexes.....	176
8.1	Le service Mailiz de l'opérateur ASIP Santé.....	176
8.2	Détail du processus d'intégration à l'espace de confiance d'un opérateur MSSanté 177	
8.2.1	Le contrat « opérateur MSSanté » et ses annexes.....	177
8.2.2	L'intégration en deux temps d'un opérateur à l'espace de confiance MSSanté 178	
8.2.3	Temps 1 – Intégration provisoire	178
8.2.4	Temps 2 – Intégration validée	181
8.3	Les environnements Annuaire national MSSanté	182
8.3.1	L'Annuaire national MSSanté de production.....	182

8.3.2	L'Annuaire national MSSanté de tests (dit « partenaires »)	183
8.4	Espace de confiance MSSanté de tests	185
8.4.1	Description des composants de l'espace de confiance de test	185
8.4.2	Modalités d'accès à l'espace de confiance MSSanté de tests	187
8.5	Canaux de contact	189
8.6	Documents externes	190
8.6.1	Documents applicables	190
8.6.2	Documents de référence pour les services	191
8.6.3	Requests For Comments (RFC)	192
8.6.4	Annexes externes	193
8.6.5	Bonnes pratiques complémentaires	195
8.7	Terminologie, acronymes et abréviations	196
8.7.1	Termes et abréviations	196
8.7.2	Légendes et abréviations utilisées dans les descriptions des attributs et règles	198
8.7.3	Définition des orientations technologiques retenues pour MSSanté	199
8.8	Codes d'erreurs	200
8.8.1	Codes d'erreurs pour les Web Services de l'Annuaire national MSSanté en SOAP - couche technique et d'échange	200
8.8.2	Codes d'erreurs pour les Web Services de l'Annuaire national MSSanté en REST - couche technique et d'échange	202
8.8.3	Codes d'erreurs pour la TM1.1.xP - Mise à jour des comptes de messagerie dans l'Annuaire national MSSanté	202
8.8.4	Codes d'erreurs pour la soumission des fichiers indicateurs	208
8.9	Éléments nécessaires à la réalisation d'une analyse de risque	213
8.9.1	Menaces prises en compte	213
8.9.2	Rappel des principaux scénarios de menaces	214

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 rattachés à l'espace de confiance MSSanté** 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'ASIP Santé ;
- Le chapitre 3 expose les **principes généraux du système MSSanté** ;
- Le chapitre 4 présente le **cycle de vie des boîtes aux lettres MSSanté** ;
- Le chapitre 5 décrit les **transactions pour les opérateurs MSSanté (exigences fonctionnelles et techniques)** ;
- Le chapitre 6 présente une **synthèse des exigences** référencées dans ce DSFT ;
- Le chapitre 7 liste l'historique des **changements de versions** de ce document ;
- Le chapitre 8 regroupe les **annexes** qui présentent en particulier : le service Mailiz de l'opérateur ASIP Santé, le processus d'intégration des opérateurs à l'espace de confiance, les outils mis à disposition des opérateurs pour les tests, les canaux de contacts ainsi que la liste des documents applicables.

1.2 Guide de lecture

Ce document est destiné aux opérateurs de messagerie candidats à l'intégration à l'espace de confiance MSSanté ainsi qu'aux éditeurs équipant les opérateurs 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 3
Directeurs techniques, Chefs de projets	2, 3, 4, 5 et 6
Développeurs, architectes logiciels, consultants techniques	4, 5, 6 et 7

Exigence / Recommandation

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.

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 DSFT sera mis à jour notamment pour prendre en compte les évolutions fonctionnelles, techniques ou de sécurités apportées au système MSSanté, justifiées dans certains cas par une évolution du cadre juridique qui s'applique au fonctionnement du système MSSanté.

Plusieurs versions majeures des spécifications d'accès du système MSSanté peuvent coexister en même temps, ceci afin de laisser suffisamment de temps aux opérateurs et aux éditeurs pour adapter leurs produits. Les modalités de prise en compte des nouvelles versions du DSFT sont précisées dans le contrat relatif à l'intégration à l'espace de confiance - contrat « opérateur MSSanté » - [\[CONTRAT-MSSANTE\]](#) conclu entre l'ASIP Santé et chaque opérateur.

Les opérateurs seront informés par l'ASIP Santé de la publication des nouvelles versions du DSFT.

En outre, il est également possible pour toute personne d'être automatiquement informée des dernières mises à jour de ce dossier de spécifications fonctionnelles et techniques en s'abonnant (sur simple demande) à la liste de diffusion (8.5 Canaux de contact).

2 La nécessité de mettre en œuvre un système de Messageries Sécurisées de Santé

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

Au cours des dernières années, 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'ASIP Santé 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 données 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.

Des projets de messageries nationales, régionales ou locales, s'étaient développés au cours des dernières années, 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'ASIP Santé 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 et 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'ASIP Santé conduit des travaux pour permettre une ouverture de l'espace de confiance MSSanté à l'ensemble de ces professionnels.

Par convention, le présent DSFT 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 : article R.1110-2 2° du code de la santé publique.

2.2 Définition du système de Messageries Sécurisées de Santé

En définissant les conditions de développement de messageries sécurisées de santé, les pouvoirs publics répondent à une attente des acteurs de faciliter leurs échanges interprofessionnels, indispensables à la prise en charge de leurs patients dans le respect de la loi et de l'éthique professionnelle.

Ce système est dénommé « 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 de ce DSFT et ayant contractualisé avec l'ASIP Santé qui en assure sa régulation. L'espace de confiance garantit la confidentialité, l'intégrité et la traçabilité des données qui sont échangées entre chacun des opérateurs qui le composent.

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 sécurisés 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 des données de santé à caractère personnel entre professionnels habilités (messagerie interprofessionnelle) ;
- 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.

Cet espace de confiance se caractérise également par :

- L'Annuaire national MSSanté s'appuyant notamment sur le répertoire partagé des professionnels de santé et ayant vocation à référencer l'ensemble des professionnels habilités à échanger des données de santé personnelles ;
- Une liste blanche de domaines qui regroupe l'ensemble des domaines de messageries des opérateurs autorisés à échanger dans l'espace de confiance MSSanté ;
- Des référentiels permettant aux industriels de développer des offres conformes et interopérables entre elles. Ces référentiels comportent les documents de référence : le présent DSFT Opérateurs de messagerie, le DST des interfaces clients de messagerie / opérateurs MSSanté [\[DST-MSSANTE\]](#), les documents applicables listés au 8.6.1, publiés par l'ASIP Santé.

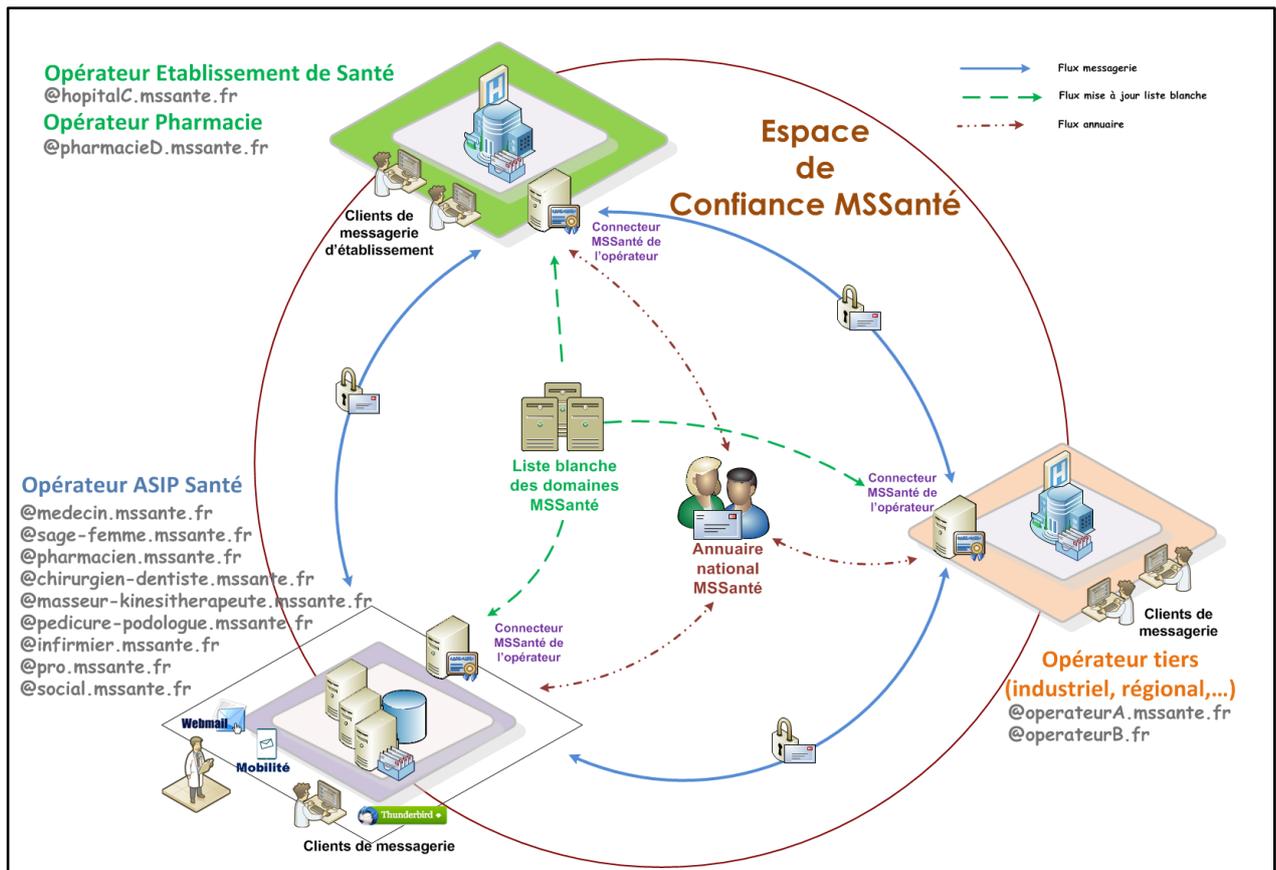


Figure 1 : Echanges au sein du système MSSanté

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 RGPD¹, ainsi que de la loi n°78-17 du 6 janvier 1978 modifiée en dernier lieu par l'ordonnance n°2018-1125 du 12 décembre 2018.

Certaines évolutions liées à l'entrée en vigueur de ces textes seront mises en œuvre au fil de l'eau. Cela concerne notamment les étapes de mise en conformité que chaque responsable de traitement utilisant un service de messagerie sécurisée de santé doit suivre.

En effet, suite à l'entrée en vigueur du RGPD, les responsables de traitement n'ont plus à effectuer d'engagement de conformité à l'autorisation unique n°37 (« AU 37 », disponible à l'adresse suivante : <https://www.cnil.fr/fr/declaration/au-037-traitements-des-donnees-de-sante-par-messagerie-securisee>). La CNIL travaille actuellement à la mise à jour de ce document, afin d'élaborer un référentiel. Dans l'attente de la publication par la CNIL de ce nouveau référentiel, il est recommandé aux responsables de traitement de continuer à se conformer aux dispositions de l'AU 37, dont les dispositions constituent à ce jour les lignes directrices à suivre pour assurer la conformité des traitements de données à caractère personnel (dont les données de santé) dans le cadre d'un service de messagerie sécurisée de santé et pour compléter le registre des traitements.

De plus, afin d'assurer la sécurité et la confidentialité des données de santé et de garantir l'effectivité des droits des personnes concernées par les données, le système MSSanté est développé dans le respect des dispositions du code de la santé publique.

En particulier, les échanges de données de santé entre professionnels habilités doivent être réalisés dans les conditions prévues à l'article L 1110-4 du code précité, qui impose d'informer le patient de l'échange de ses données avec d'autres professionnels participant à sa prise en charge. Ces échanges doivent également respecter l'article L.1110-4-1 relatif 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.

Dans la mesure où un service de messagerie sécurisée 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 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**).

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

Lorsque le fonctionnement du service de messagerie impose de recourir à un hébergeur de données de santé **ce dernier (opérateur ou prestataire de l'opérateur)** doit être titulaire d'un agrément ou d'une **certification** couvrant une telle prestation.

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.

L'opérateur doit se mettre en conformité avec les référentiels publiés de la PGSSI-S. (Art. L. 1110-4-1 du code de la santé publique).

Remarque : le présent DSFT 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 incombent.

2.4 Les acteurs de l'espace de confiance MSSanté

2.4.1 L'ASIP Santé

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

- **Gestionnaire de l'espace de confiance MSSanté** : qui inclut la gestion de l'Annuaire national MSSanté 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'ASIP Santé 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 » [\[CONTRAT-MSSANTE\]](#) conclu entre l'ASIP Santé et tout opérateur souhaitant intégrer l'espace de confiance MSSanté.
- **Opérateur du service Mailiz pour le compte des Ordres professionnels**. L'ASIP Santé 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.
Pour plus d'information concernant le service proposé par l'opérateur ASIP Santé, se reporter au §8.1 « Le service Mailiz de l'opérateur ASIP Santé » du présent DSFT.

2.4.2 Les opérateurs de messageries sécurisées de santé

Un opérateur de messagerie sécurisée de santé est une personne physique ou morale qui développe et fournit un service de messagerie sécurisée de santé au profit d'utilisateurs finaux.

L'opérateur peut être un établissement de santé ou plus largement toute structure de soins, un groupement de coopération sanitaire, un industriel etc.

L'ASIP Santé, comme indiqué ci-dessus est un des opérateurs de l'espace de confiance.

Pour proposer un service de messagerie sécurisée de santé raccordé à l'espace de confiance, un opérateur MSSanté doit avoir conclu le contrat « opérateur MSSanté » [\[CONTRAT-MSSANTE\]](#) avec l'ASIP Santé, 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 DSFT) et respecter les obligations qui y sont définies.

Pour plus d'information concernant l'intégration des opérateurs à l'espace de confiance MSSanté, se reporter au §2.5 «Intégration des opérateurs 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 DSFT et des besoins de sécurité du service.

2.4.3 Les utilisateurs finaux

Les utilisateurs du système MSSanté sont l'ensemble des professionnels quel que soit leur mode d'exercice, habilités par la loi à collecter et échanger des données de santé dans le cadre de leurs missions et à des fins de prise en charge d'un patient ou usager.

Sont notamment concernés les professionnels visés à l'article L.1110-4 du code de la santé publique.

2.5 Intégration des opérateurs à l'espace de confiance MSSanté

On distingue deux modalités d'accès à l'espace de confiance MSSanté :

1) Devenir opérateur MSSanté.

Un opérateur MSSanté opère et propose un service de messagerie sécurisée 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 ces professionnels/utilisateurs. 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 messagerie sécurisée de santé raccordé à l'espace de confiance, un opérateur doit avoir conclu le contrat « opérateur MSSanté » [\[CONTRAT-MSSANTE\]](#) avec l'ASIP Santé qui définit les conditions d'intégration de l'opérateur à l'espace de confiance MSSanté.

L'intégration de l'opérateur à l'espace de confiance s'effectue en deux temps. Le premier, désigné « intégration provisoire », consiste pour l'opérateur à tester et évaluer son service de messagerie sécurisée de santé et le second, appelé « intégration validée », reconnaît la capacité pour l'opérateur de proposer un service de messagerie sécurisée de santé à des utilisateurs finaux.

Pour plus d'information concernant le contrat « opérateur MSSanté » et ses deux annexes ainsi que le processus d'intégration, se reporter au §8.2.

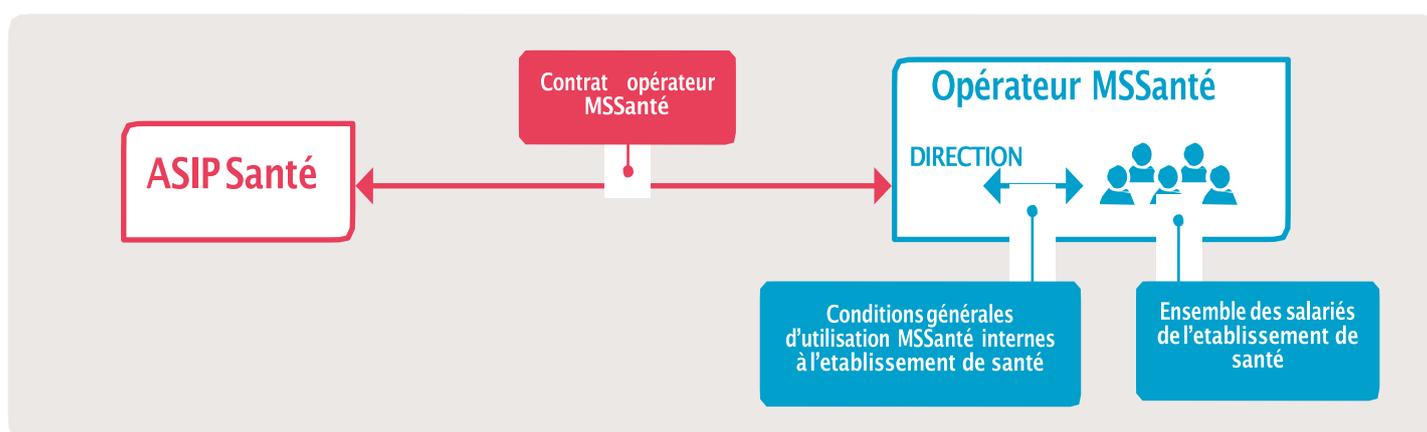


Figure 2 : « Chaîne contractuelle » pour un Etablissement de santé qui est opérateur MSSanté

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 MSSanté qui opère et propose un service de messagerie sécurisée 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 MSSanté peut être par exemple un industriel qui propose des services de messagerie sécurisée à des clients qui peuvent aussi bien être des structures de soins que des professionnels libéraux.

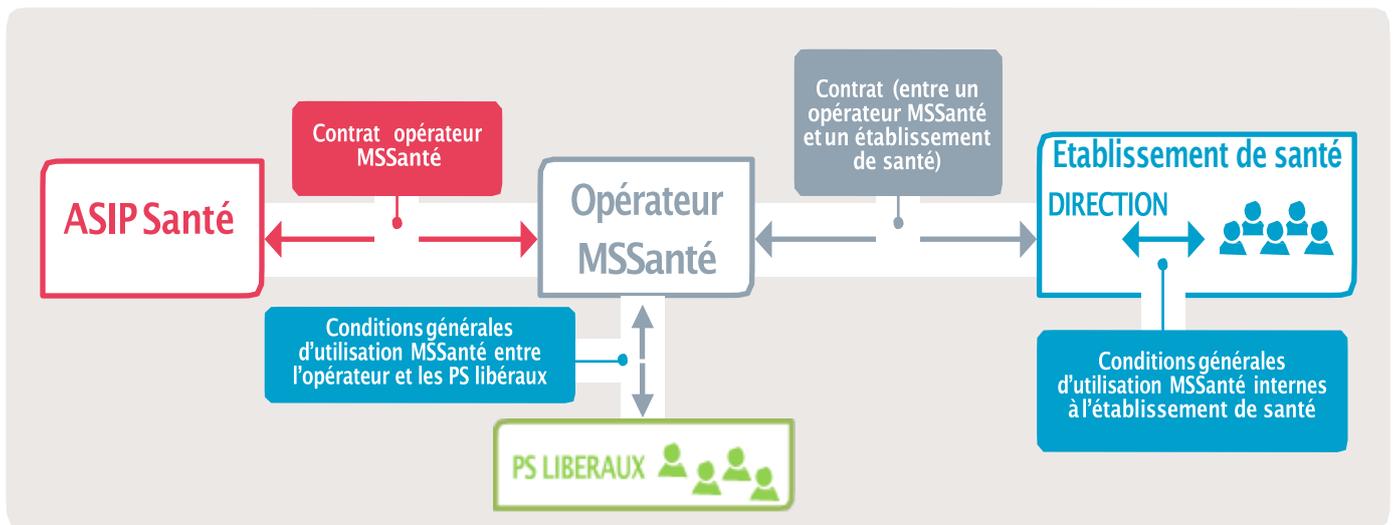


Figure 3 : « Chaîne contractuelle » pour un opérateur MSSanté qui propose un service de messagerie sécurisée de santé à des professionnels de santé libéraux ainsi qu'à un établissement de santé.

2.6 Focus sur les formalités préalables à accomplir par le responsable de traitement

Ce paragraphe sur les formalités préalables à accomplir par le responsable de traitement sera mis à jour à l'issue des travaux menés par la CNIL suite à l'entrée en vigueur du RGPD en mai 2018 : voir le paragraphe 2.3 du DSFT.

Par ailleurs, en attendant l'issue de ces travaux de mise à jour, 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.

Détermination des formalités préalables à accomplir

Avant l'entrée en vigueur du RGPD, pour permettre aux professionnels habilités utilisant une messagerie sécurisée 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 messagerie sécurisée 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 sécurisée².

Après l'entrée en vigueur du RGPD, les professionnels n'ont plus à effectuer d'engagement de conformité à cette autorisation unique, et peuvent se cantonner à documenter leur conformité au RGPD via leur documentation interne (notamment, registre des traitements de données à caractère personnel). L'autorisation unique n°37 demeure cependant un document de référence, dont les dispositions constituent à ce jour les lignes directrices à suivre pour assurer la conformité des traitements de données à caractère personnel (dont les données de santé) dans le cadre d'un service de messagerie sécurisée de santé.

Détermination de la qualité de responsable de traitement

Dans le cadre du système MSSanté, les professionnels habilités utilisant des services de messagerie sécurisée de santé par un opérateur 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.

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

2.6.1 Cas n°1 – vous fournissez un service de messagerie sécurisée de santé et vos utilisateurs finaux exercent à titre libéral

Dans ce cas,

- **Vos utilisateurs sont :**
 - Responsables du traitement de messagerie sécurisée 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.

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 que votre service respecte le cadre juridique applicable aux traitements de messageries sécurisées de santé.

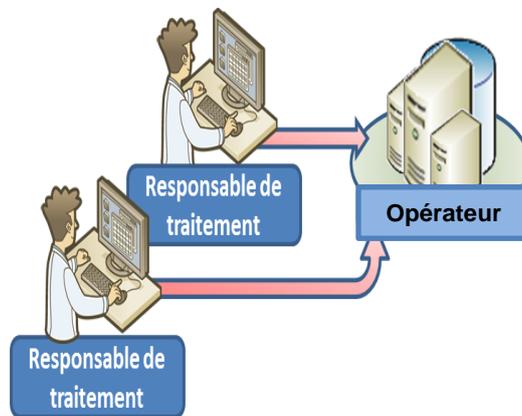


Figure 4 : PS libéral utilisant le service MSSanté proposé par un opérateur

2.6.2 Cas n°2 - Une structure de soins (établissement de santé, laboratoire de biologie médicale, EHPAD, etc.) décide de mettre à la disposition de ses professionnels habilités salariés le service de messagerie sécurisée de santé que vous fournissez

Vous proposez le service de messagerie sécurisée de santé pour cette structure.

Dans ce cas,

- **La structure est :**
 - Le responsable du traitement de messagerie sécurisée 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.

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 de soins, 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...).

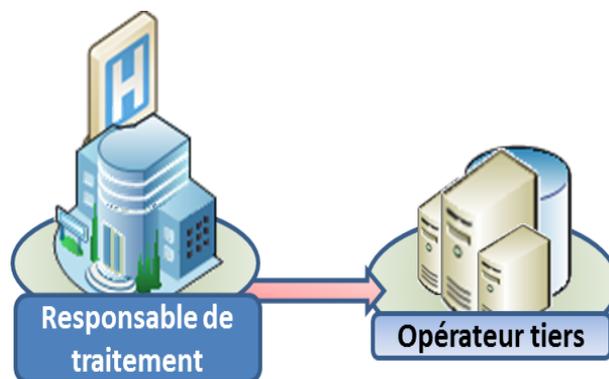


Figure 5 : Structure utilisant le service MSSanté proposé par un opérateur « tiers »

2.6.3 Cas n°3 - Vous êtes une structure de soins et décidez d'opérer votre propre service de messagerie sécurisée de santé

Dans ce cas,

Vous êtes :

- Le responsable du traitement de messagerie sécurisée 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 » [\[CONTRAT-MSSANTE\]](#).

Vous avez la qualité de responsable de traitement des données à caractère personnel échangées au moyen du service de messagerie sécurisée de santé que vous proposez. A ce titre vous devez assurer la conformité du traitement au RGPD.

Vous devez encadrer l'utilisation de votre service de messagerie sécurisée de santé par vos utilisateurs (charte, CGU, etc...).

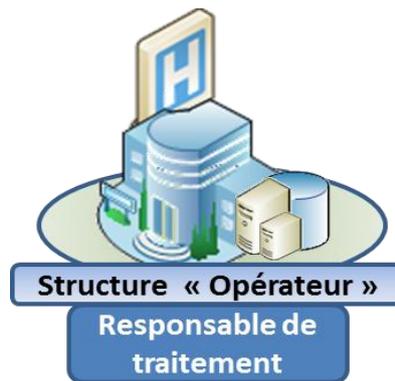


Figure 6 : Structure utilisant son propre service MSSanté en tant qu'opérateur

2.7 mssante.fr une marque de confiance

Le « système MSSanté » permet à tout professionnel habilité, 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 Messagerie Sécurisée de Santé peut être identifié le cas échéant dans les adresses mails par la présence du domaine mssante.fr marque de reconnaissance de cet espace de confiance. Ce domaine peut 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) ou selon leur choix utiliser un autre domaine leur appartenant pour la Messagerie Sécurisée de Santé par exemple xxx@ch-xyz-securise.fr ; ce domaine dédié aux échanges sécurisés devra nécessairement être distinct de leur domaine de messagerie habituel (ch-xyz.fr dans notre exemple) ;
- Le service Mailiz opéré par l'opérateur ASIP Santé pour le compte des Ordres professionnels propose des boîtes aux lettres :
 - sur le domaine de l'ordre du professionnel de santé : xxx@<profession>.mssante.fr
 - ou sur un domaine générique xxx@pro.mssante.fr.

L'usage commun d'une terminaison « mssante.fr » par tous les acteurs de l'espace de confiance 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. Toutefois, les opérateurs sont libres de proposer des services de messagerie sécurisée sans utiliser le nom de domaine « mssante.fr ».

Tout opérateur ayant intégré l'espace de confiance MSSanté est autorisé à utiliser un sous-domaine du domaine mssante.fr dont l'ASIP Santé est titulaire.

L'ASIP Santé peut fournir à l'opérateur qui souhaite produire des certificats utilisant son sous-domaine mssante pour ses interfaces clientes d'accès aux boîtes aux lettres (par exemple : un Webmail), une attestation indiquant que l'ASIP Santé l'y autorise. Cette attestation est exigée des autorités de certification pour la commande de certificats serveurs. L'opérateur doit adresser sa demande d'attestation via les canaux de contacts (8.5).

3 Description du fonctionnement du système de Messageries Sécurisées de Santé

Le système de Messageries Sécurisées de Santé (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. A 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 « La nécessité de mettre en œuvre un 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.

3.1 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 boîtes 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'ASIP Santé 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 :

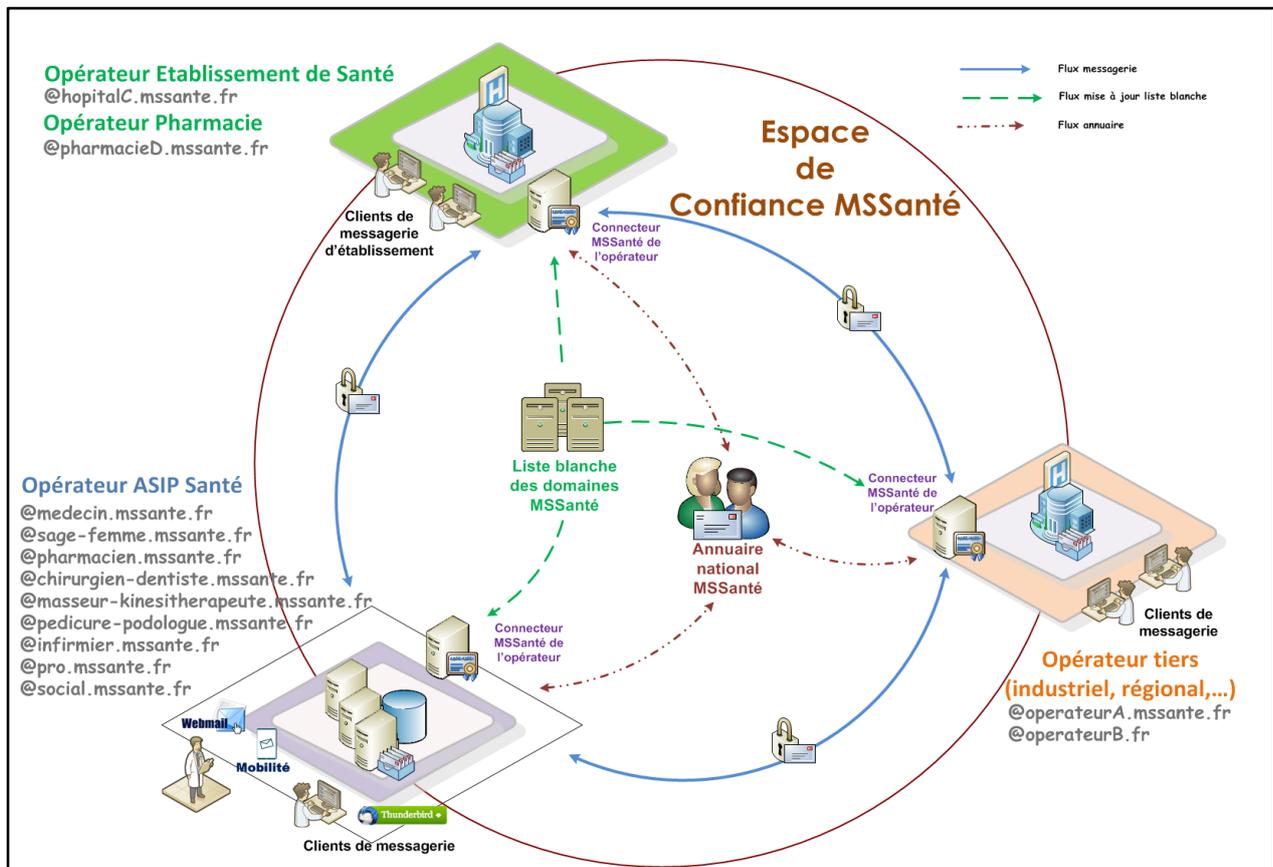


Figure 7 : Echanges au sein du système MSSanté

Les opérateurs de messagerie signent un contrat « opérateur MSSanté » avec l'ASIP Santé 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 exclusivement entre utilisateurs (personnes physiques et morales) des services de messagerie mis en œuvre par les opérateurs MSSanté.

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.

3.2 L'Annuaire national MSSanté

Les utilisateurs du système MSSanté doivent pouvoir sélectionner de manière sûre et aisée les destinataires de leurs messages.

L'ASIP Santé, en sa qualité de gestionnaire de l'espace de confiance MSSanté, met en œuvre et maintient l'Annuaire national MSSanté des utilisateurs du système MSSanté.

La finalité de l'Annuaire national MSSanté est de permettre à tout utilisateur final de retrouver facilement l'adresse d'un autre utilisateur disposant d'une BAL MSSanté afin de lui adresser un message de façon sécurisée.

Pour atteindre cet objectif, l'Annuaire national MSSanté 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.

L'intégration des opérateurs à l'espace de confiance MSSanté nécessite que ceux-ci publient l'ensemble des BAL des utilisateurs de leur(s) domaine(s) dans l'Annuaire national MSSanté.

Les utilisateurs devront être identifiés par leur numéro d'identification national (RPPS ou Adeli). Lorsque l'utilisateur final 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.

La publication des BAL applicatives et organisationnelles nécessite l'utilisation d'un identifiant national de structure de soins.

L'Annuaire national MSSanté contient ainsi des données qui permettent :

- D'identifier les utilisateurs (potentiels ou actifs) du système MSSanté ;
- De rechercher l'adresse de messagerie MSSanté d'un destinataire sur le principe de recherche multicritères ;
- D'afficher les traits d'identité des PS répondants aux critères de recherche.

La gestion des fonctions de l'Annuaire national MSSanté 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 § 5.4 « Publication de BAL MSSanté dans l'Annuaire national MSSanté » et § 5.5.1 « TM2.1.1A - Consultation de l'Annuaire national MSSanté ».

Remarque : l'ASIP Santé gère l'Annuaire national MSSanté dans les conditions de service suivantes :

- Production opérationnelle en 24/7 ;
- Traitement des incidents : bloquant (en moins d'1h), majeur (en moins de 4h), mineur (en moins 8h) ;
- Durée maximale unitaire d'interruption de service : 1 h ;
- Durée maximale mensuelle cumulée d'interruption de service : 4h ;
- Temps de réponse : < 1,5s dans 95% des cas, et < 2s dans les 5% restants.

RE_ANM_5010



Il est fortement recommandé aux opérateurs qui souhaitent assurer de meilleures performances à leurs utilisateurs de mettre en œuvre un Connecteur d'annuaire local leur permettant d'appliquer leur propre niveau de disponibilité.

3.3 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'ASIP Santé.

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 national MSSanté) ;
- de consulter l'Annuaire national MSSanté 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'ASIP Santé).

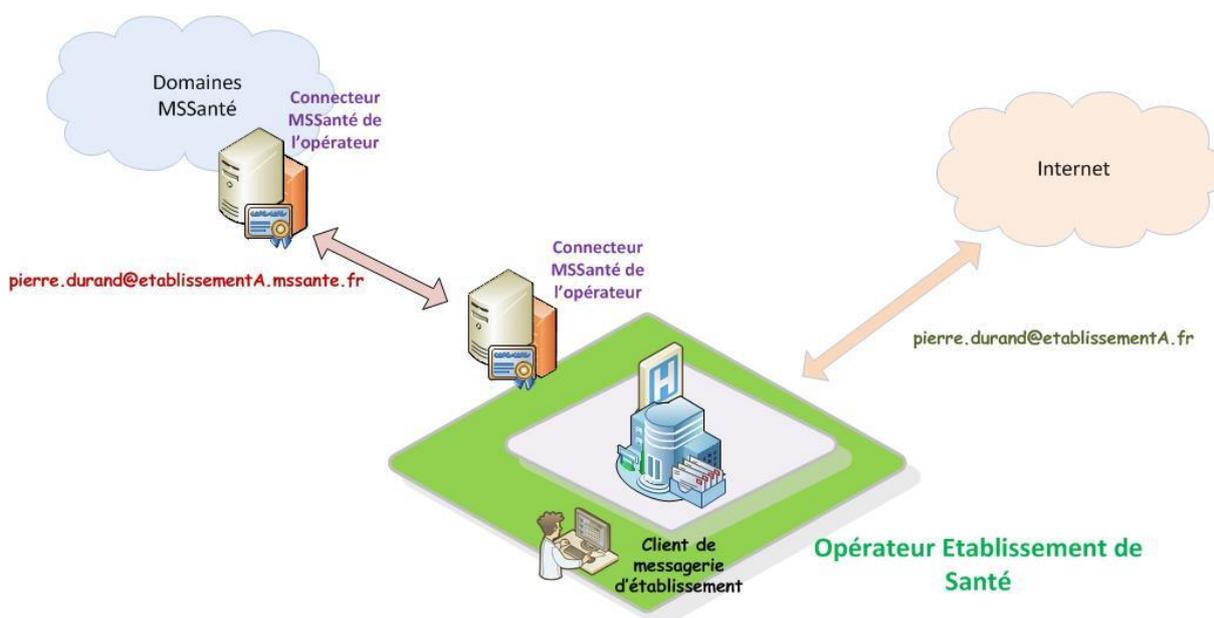


Figure 8 : Connecteur MSSanté de l'opérateur

3.4 Connecteur à l'Annuaire national MSSanté

Le **Connecteur à l'Annuaire national MSSanté** 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 national MSSanté ;
- Réaliser des recherches de correspondants dans l'Annuaire national MSSanté ;
 - Via le client de messagerie ;
 - Par une vue unifiée des adresses MSSanté au sein de l'établissement.

Des exemples d'implémentations sont disponibles au § 3.6 « Exemples de mise en œuvre ».

3.5 Les clients de messagerie MSSanté

3.5.1 Le LPS au cœur des Systèmes d'Information de Santé

Le système MSSanté constitue une étape importante dans la mise en œuvre d'une stratégie de déploiement des systèmes d'information interopérables de santé en France.

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

Ainsi, chaque client de messagerie ou LPS MSSanté doit pouvoir permettre à ses clients / utilisateurs de paramétrer une adresse mail sécurisée ainsi que d'intégrer les fonctionnalités d'interrogation de l'Annuaire national MSSanté proposées par l'ASIP Santé et les fonctionnalités d'émission et de réception de messages proposées par un opérateur MSSanté, en cohérence avec les interfaces standards (voir ci-dessous) ou propriétaires proposées par cet opérateur.

Les éditeurs de LPS et de clients de messagerie ainsi que les opérateurs MSSanté ont aussi l'opportunité d'intégrer les interfaces standards MSSanté (décrites dans le document « Dossier des Spécifications Techniques (DST) des interfaces clients de messagerie / opérateurs MSSanté » [\[DST-MSSANTE\]](#)). Ces interfaces sont par exemple mises en œuvre dans le cadre du service de messagerie Mailiz opéré par l'opérateur ASIP Santé pour le compte des Ordres professionnels. Pour faciliter l'interfaçage des clients de messagerie du marché avec leur service, les opérateurs qui le souhaitent peuvent reprendre les spécifications de ce DST (interfaces techniques et moyens d'authentification).

Les transactions MSSanté décrites dans le DST et pouvant être intégrées dans un client de messagerie sont :

- **Les transactions de messagerie basées sur les protocoles standards de messagerie** (SMTP + StartTLS et IMAP + StartTLS) ;
- **Les transactions de messagerie basées sur les Web Services définis dans le DST ;**
- **La transaction de consultation de l'Annuaire national MSSanté** par le protocole LDAP.

Remarques :

- Bien que ce soit fortement recommandé, afin d'assurer l'interopérabilité des LPS DST compatibles avec un maximum d'opérateurs, il n'est pas exigé des opérateurs qu'ils offrent obligatoirement les interfaces standards du DST vers des clients de messagerie. 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 elles-mêmes propriétaires. 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.
- Par commodité, les LPS et clients de messagerie implémentant ces interfaces standards seront appelés client de messagerie MSSanté dans la suite de ce dossier.

3.5.2 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'ASIP Santé 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 § 8.6.1 « 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 « Echange 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 recommandé de joindre les documents au format bureautique (par exemple le 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.

Pour les messages ne contenant que des pièces jointes au format bureautique, il est vivement recommandé de ne pas permettre à un utilisateur du client de messagerie émetteur de joindre dans un même message des documents de plusieurs patients.

Dans tous les cas, la bonne pratique est toujours : un message ne concerne qu'un seul patient.

3.5.3 Fonctions et interfaces pour les clients de messagerie

Les rôles dévolus au client de messagerie MSSanté sont à minima :

- De réaliser les tâches de messagerie standards (envoyer, recevoir et stocker des courriers électroniques) ;
- De pouvoir réaliser la recherche d'utilisateurs finaux dans l'Annuaire national MSSanté.

Ils peuvent en outre effectuer certaines tâches d'administration et de gestion de messagerie, laissées à l'appréciation des éditeurs, comme par exemple :

- Gestion de dossiers personnels ;
- Filtrage des courriers entrants ;
- Gestion du réacheminement de courrier ;
- Gestion de messages d'absence ;
- Gestion de la carte de visite de l'expéditeur ;
- Et toute fonctionnalité jugée utile par l'éditeur.

Ces interfaces sont décrites dans le DST des interfaces client de Messagerie / opérateurs MSSanté [\[DST-MSSANTE\]](#).

3.6 Exemples de mise en œuvre

Il existe potentiellement de nombreux modèles d'intégration de la messagerie de santé sécurisée au sein du domaine d'un établissement de santé ou d'un autre type d'opérateur.

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

3.6.1 Accès à l'espace de confiance

3.6.1.1 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 Etablissement de Santé ou d'un autre type d'opérateur.

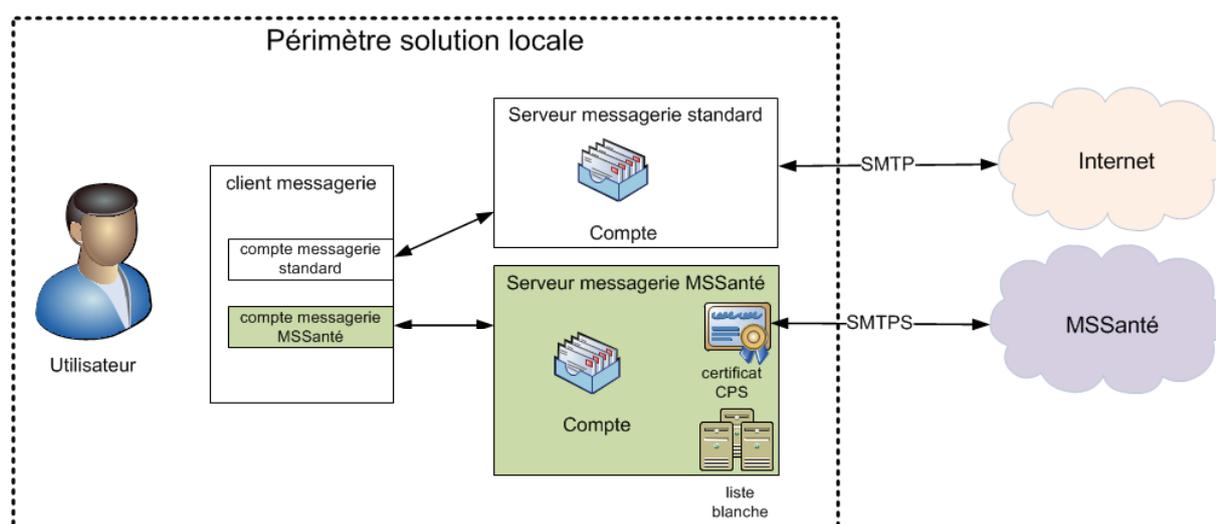


Figure 9 : Services de messagerie distincts

Dans cet exemple, l'utilisateur 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.

3.6.1.2 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 ou à un autre type d'opérateur. 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.

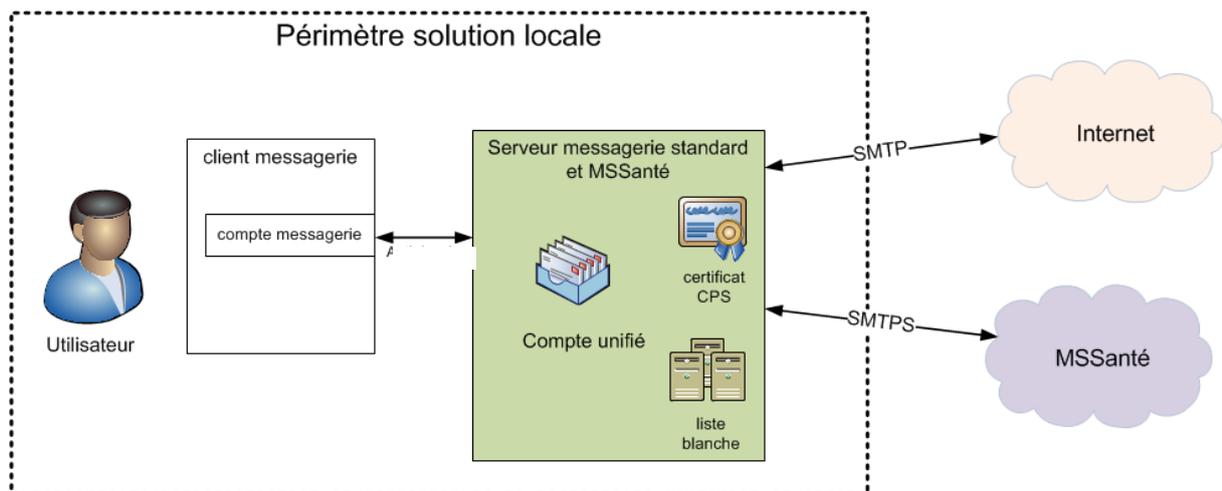


Figure 10 : Service de messagerie unifié

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.

3.6.1.3 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.

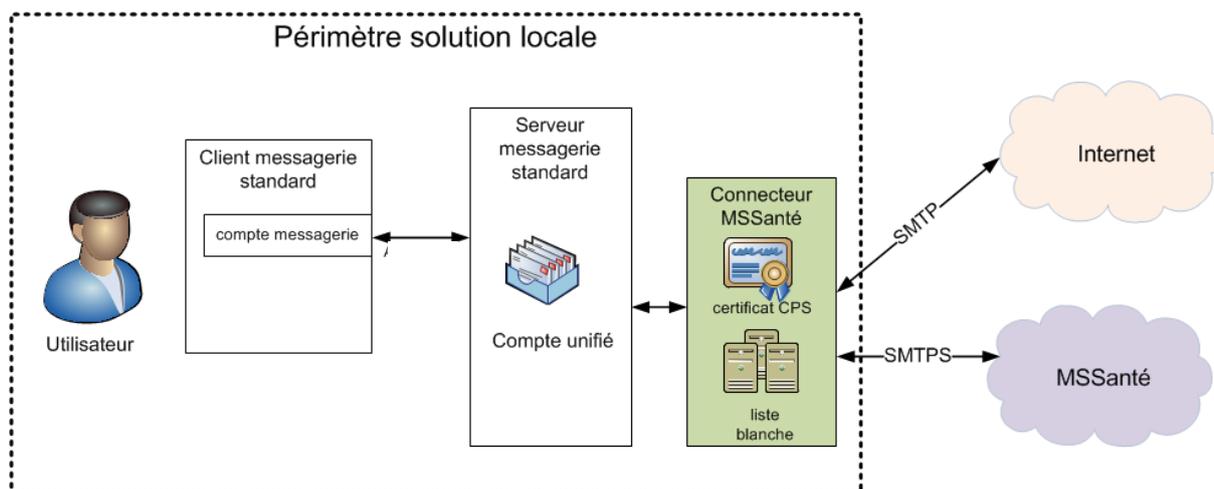


Figure 11 : Connecteur MSSanté d'opérateur non intégré au serveur de messagerie

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.

3.6.1.4 Echange 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.

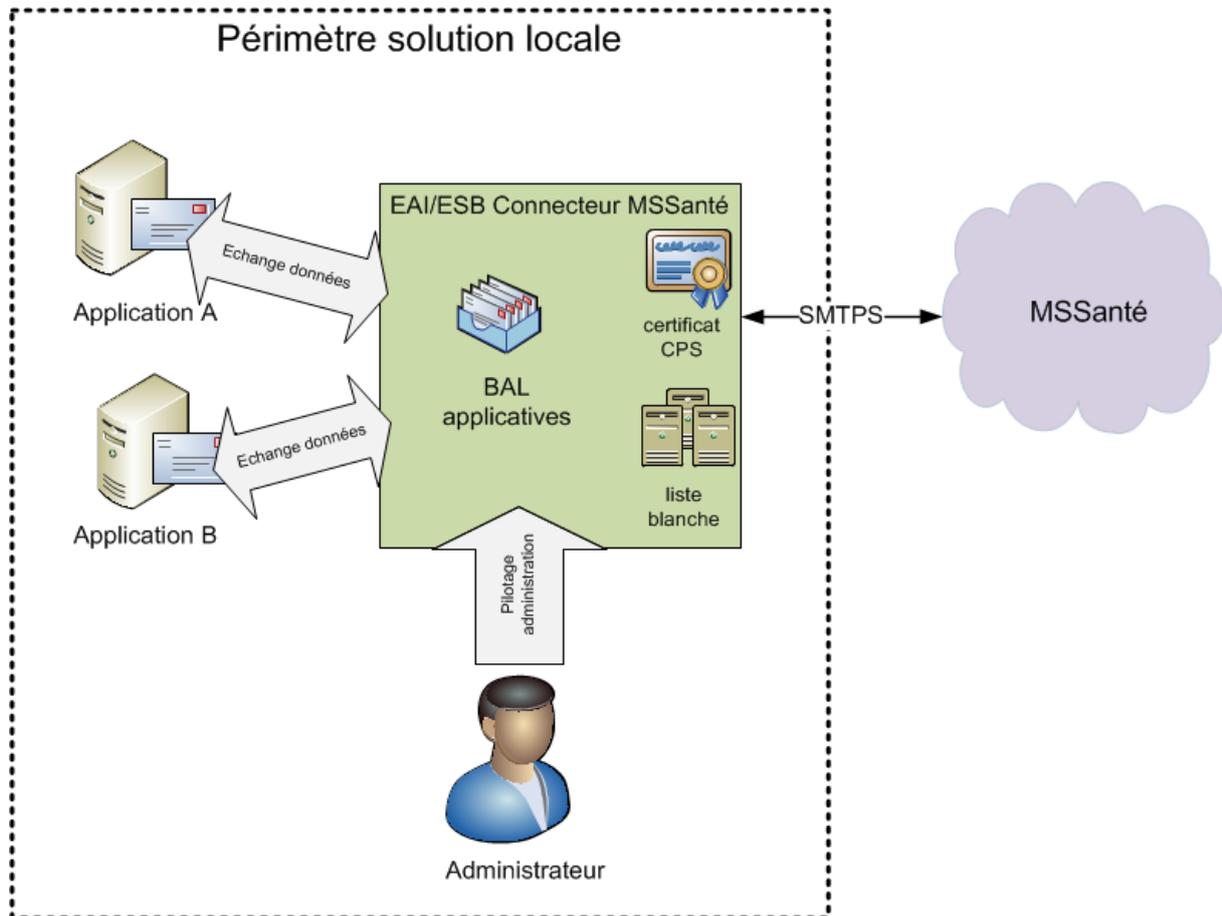


Figure 12 : Echange de messages sécurisés depuis ou vers des applications

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.

3.6.2 Accès à une BAL MSSanté

3.6.2.1 Par client de messagerie et carte CPS

Dans cet exemple, l'utilisateur 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 doit être équipé d'un lecteur de carte CPS pour permettre l'accès à son compte MSSanté.

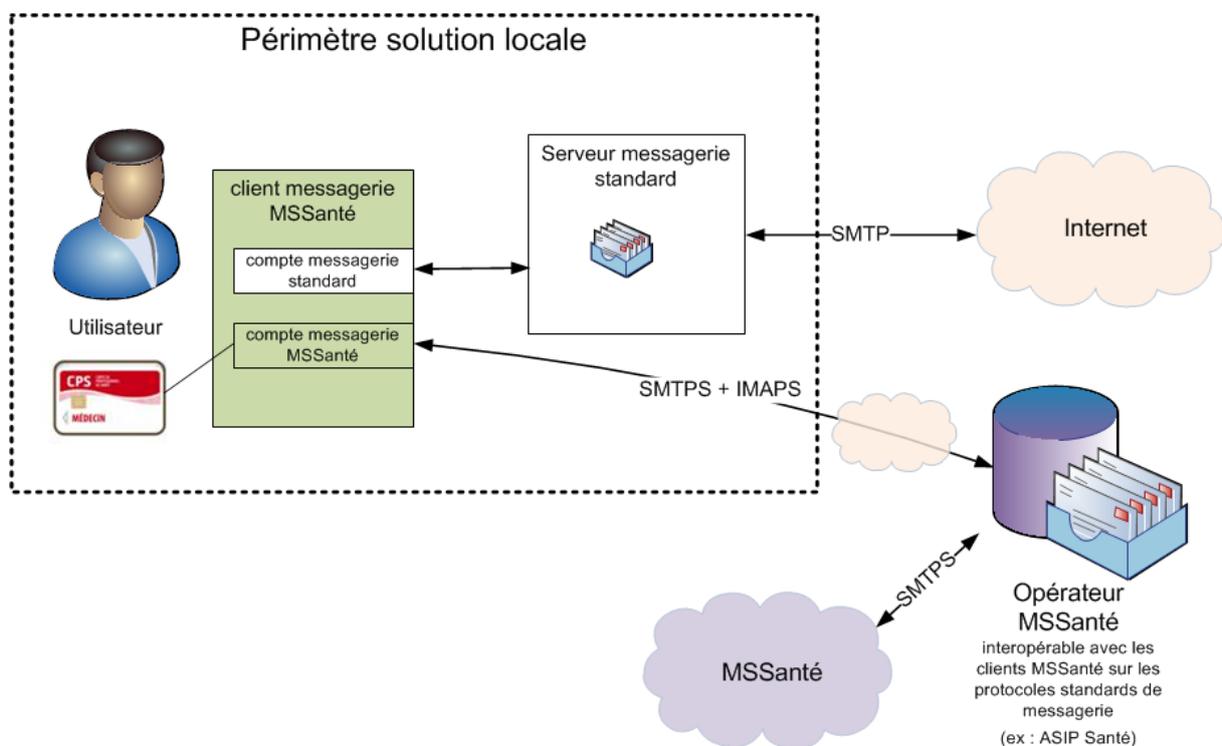


Figure 13 : Accès MSSanté par client de messagerie et carte CPS

3.6.2.2 Par LPS et identifiant/mot de passe/OTP

Dans cet exemple, l'utilisateur utilise spécifiquement deux logiciels :

- Un client de messagerie standard avec un compte de messagerie non-MSSanté ;
- Un LPS utilisant une boîte aux lettres MSSanté accédée par Web Services et configuré pour utiliser l'authentification par identifiant/mot de passe/OTP SMS.

Dans ce cas de figure, le poste de travail de l'utilisateur n'a pas besoin d'être équipé d'un lecteur de carte CPS pour permettre l'accès à son compte MSSanté. Le service de l'opérateur MSSanté doit être configuré pour envoyer le code d'accès à usage unique (ou One Time Password = OTP) par SMS sur le terminal de l'utilisateur.

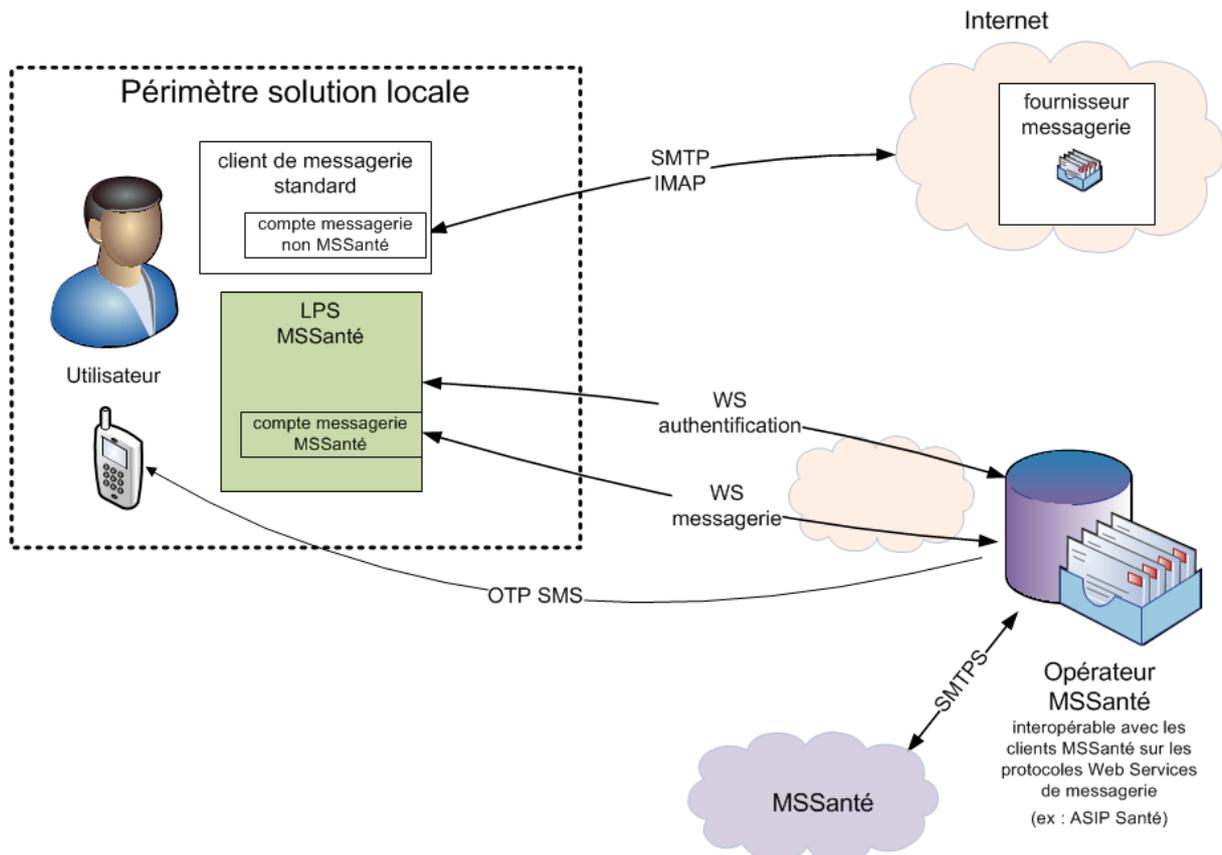


Figure 14 : Accès MSSanté par LPS et identifiant/mot de passe/OTP

Pour plus de précisions, se reporter au document [\[PG-AUTH\]](#) qui détaille les dispositifs d'authentification par OTP.

3.6.2.3 Par Webmail et carte CPS

Dans cet exemple, l'utilisateur 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 internet³.

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

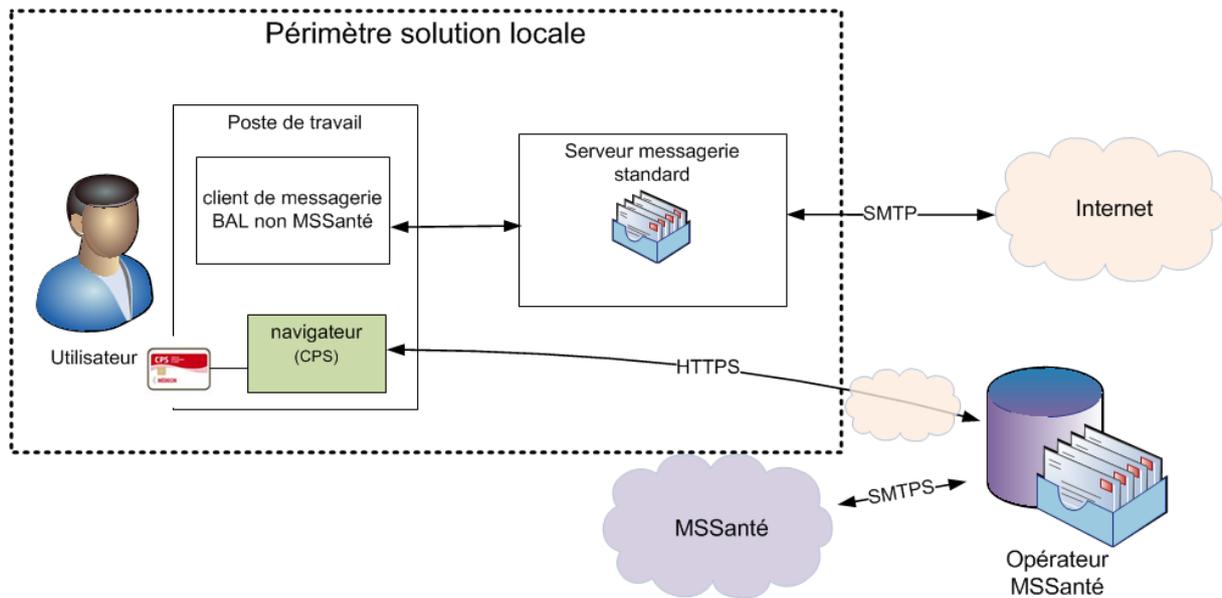


Figure 15 : Accès MSSanté par Webmail et par carte CPS

³ L'opérateur ASIP Santé met à disposition un accès en Webmail (Mailiz) pour les BAL qu'il héberge sur les domaines ordinaires (ex : @profession.mssante.fr) et sur le domaine générique (@pro.mssante.fr). L'accès à la BAL nécessite une authentification préalable par CPS ou par un moyen d'authentification équivalent (identifiant, mot de passe et code d'accès à usage unique délivré par SMS ou sur une adresse de messagerie hors domaine MSSanté).

3.6.2.4 Par Webmail et identifiant/mot de passe/OTP

Dans cet exemple, l'utilisateur 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 dans 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.

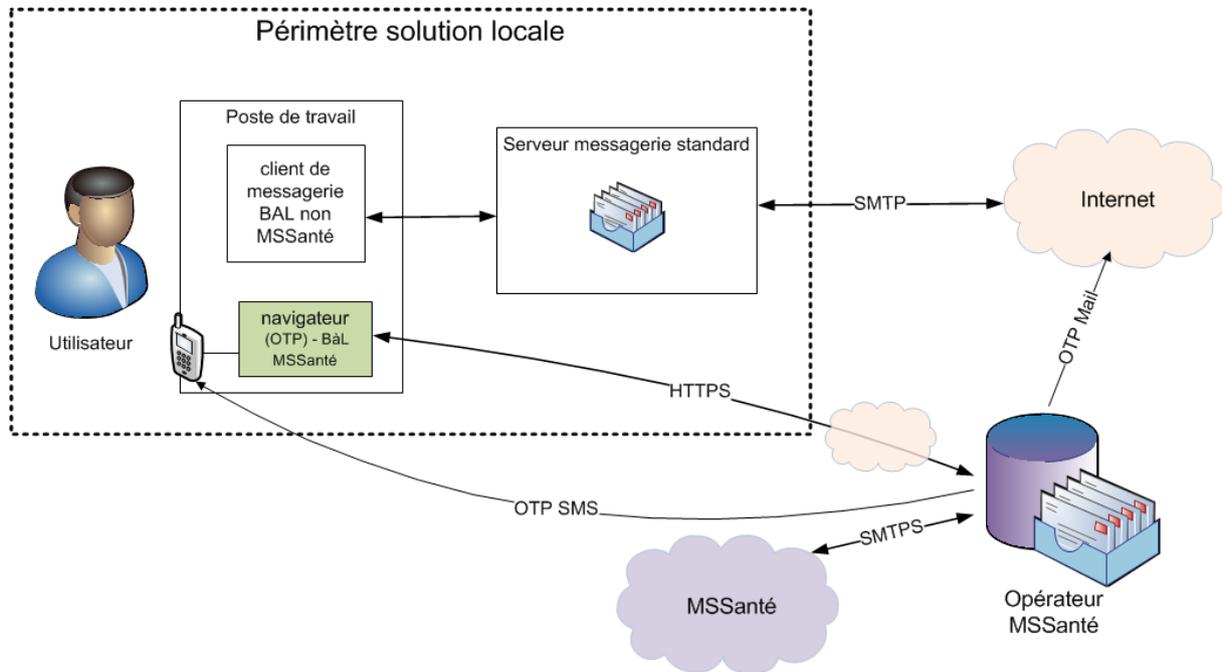


Figure 16 : Accès MSSanté par Webmail et sans carte CPS

Le poste de travail de l'utilisateur n'est pas nécessairement équipé d'un lecteur de carte CPS : l'utilisateur utilise alors un autre moyen d'authentification forte pour l'accès en Webmail, qui s'appuie ici sur la saisie d'un identifiant, d'un mot de passe et d'un code d'accès à usage unique (OTP – *One Time Password*), qui dans notre exemple est transmis par SMS à l'utilisateur.

3.6.2.5 Exemple des modalités retenues par l'opérateur ASIP Santé pour son service de messagerie Mailiz

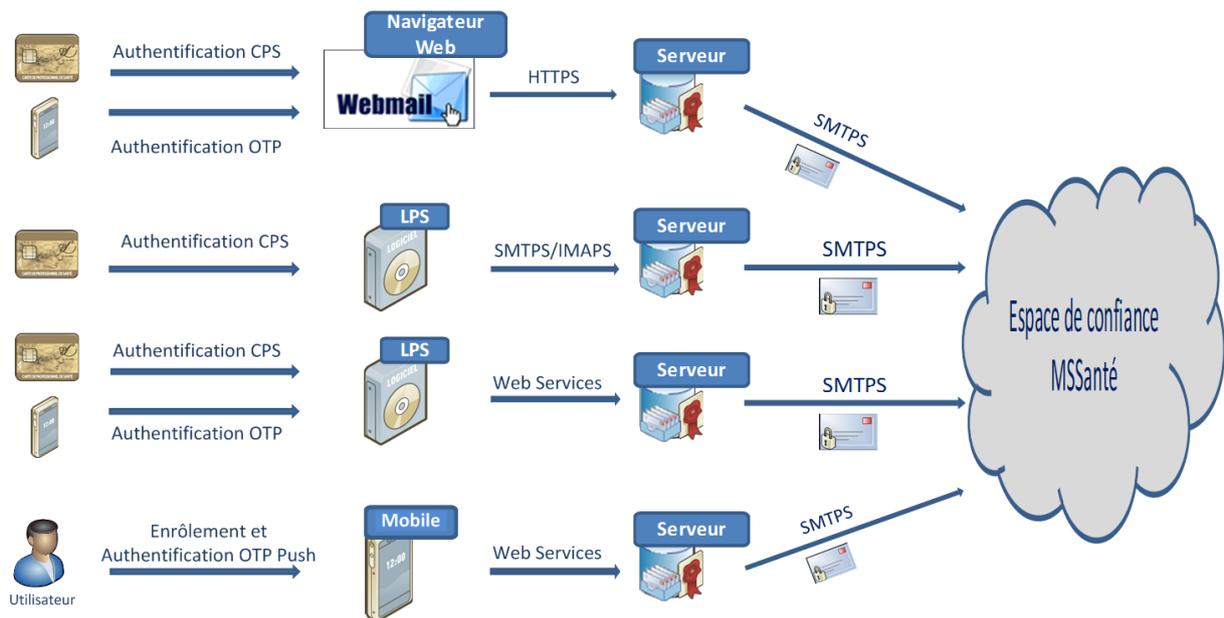


Figure 17 : Modalités retenues par l'ASIP Santé en tant qu'opérateur de domaines MSSanté

3.6.3 Consultation de l'Annuaire national MSSanté

3.6.3.1 Vue d'ensemble de l'Annuaire national MSSanté

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

- 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 national MSSanté permet à l'utilisateur de sélectionner les destinataires de ses messages. Les destinataires doivent être titulaires d'un compte de messagerie attaché à un des domaines MSSanté.

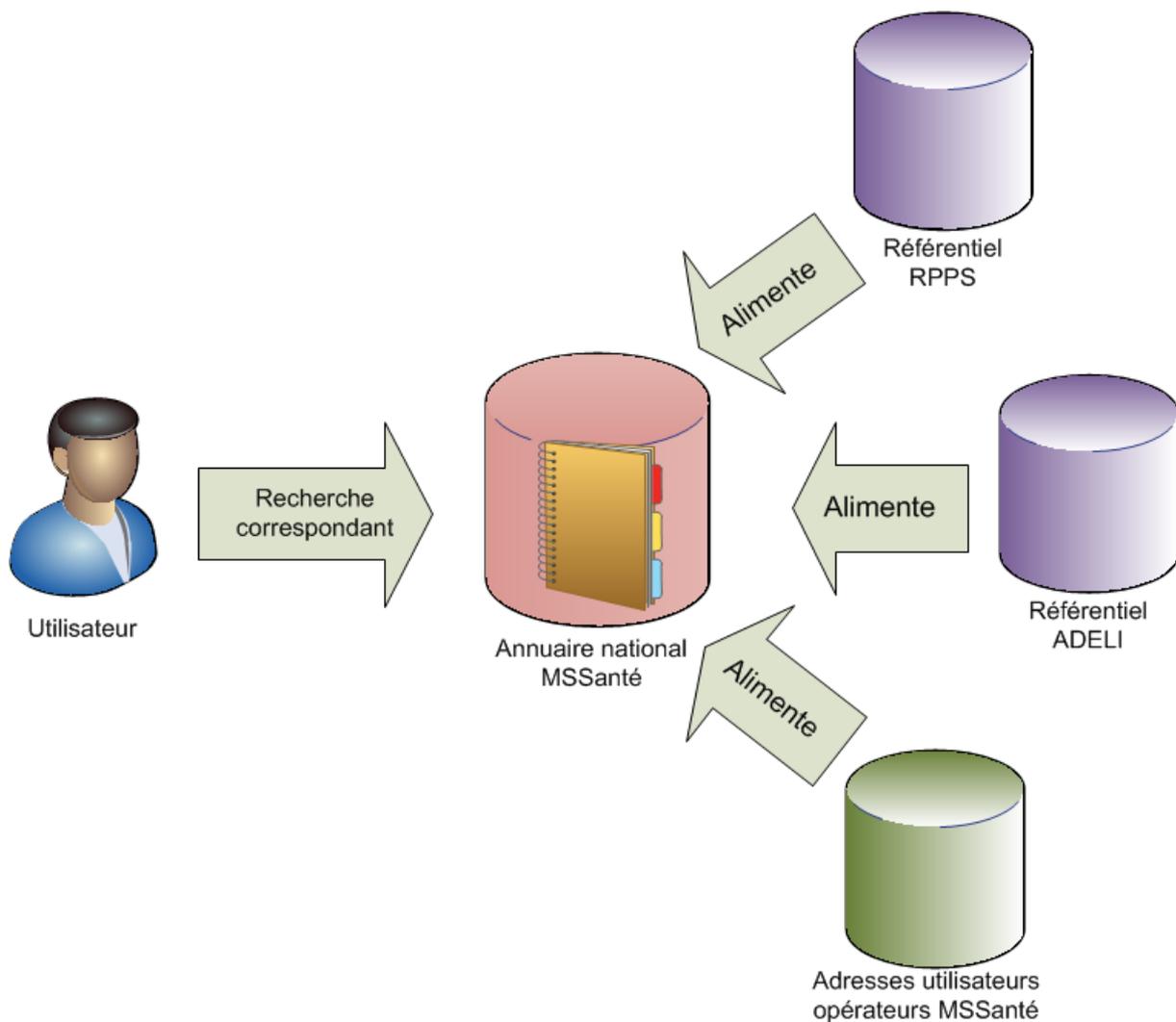


Figure 18 : Principe d'alimentation de l'Annuaire national MSSanté

3.6.3.2 Recherche de correspondants MSSanté

3.6.3.2.1 Accès direct à l'Annuaire national MSSanté via le client de messagerie

Dans cet exemple, l'utilisateur 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 national MSSanté 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.

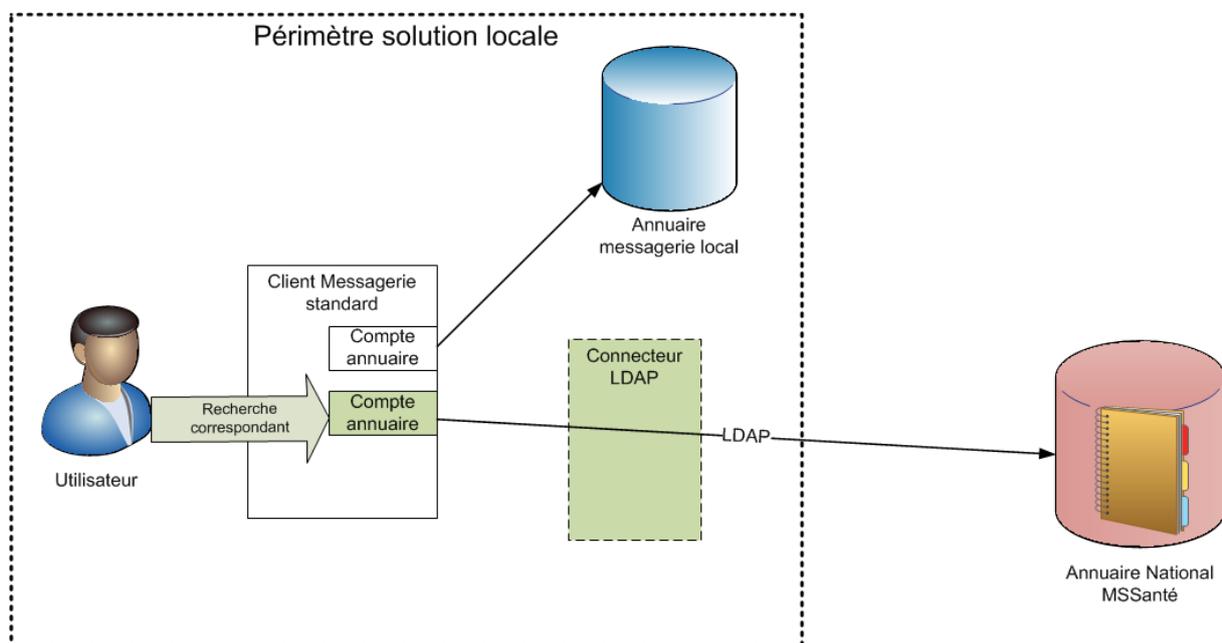


Figure 19 : Accès direct à l'Annuaire national MSSanté via le client de messagerie

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

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

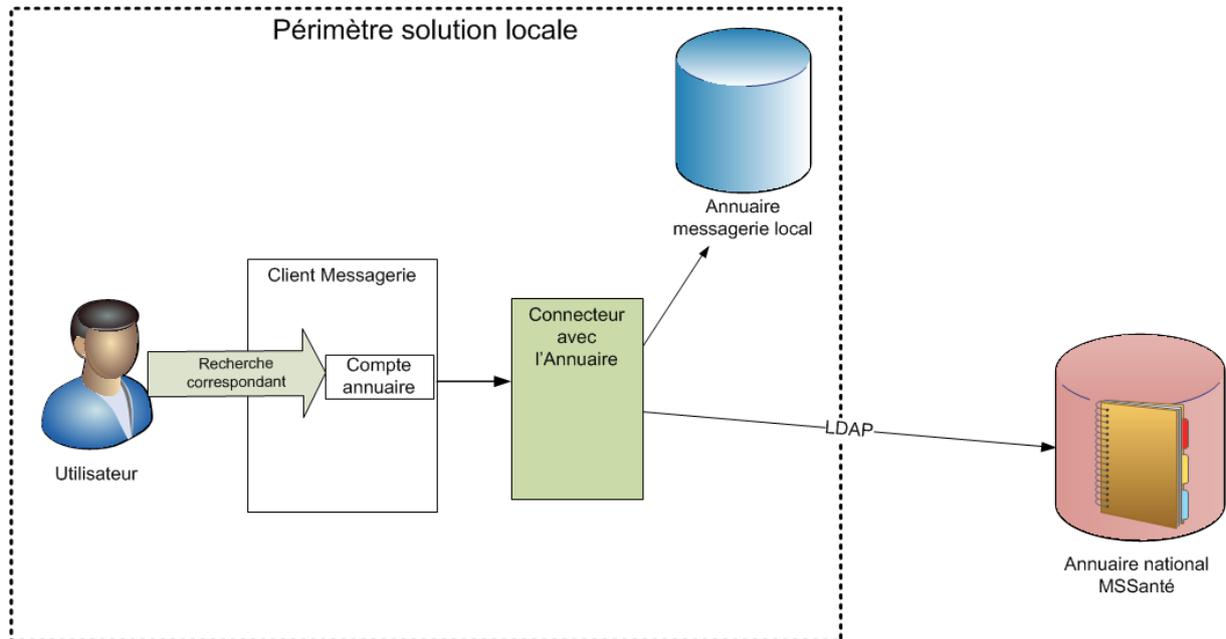


Figure 20 : Vue unifiée de l'annuaire au sein du domaine MSSanté

Le Connecteur avec l'Annuaire national MSSanté permet alors de proposer une vue unifiée dans les réponses renvoyées à l'utilisateur.

3.6.3.2.3 Intégration de l'Annuaire national MSSanté

Dans l'exemple présenté ci-dessous, une extraction quotidienne de l'Annuaire national MSSanté 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 MSSanté sont alors vus comme des contacts.

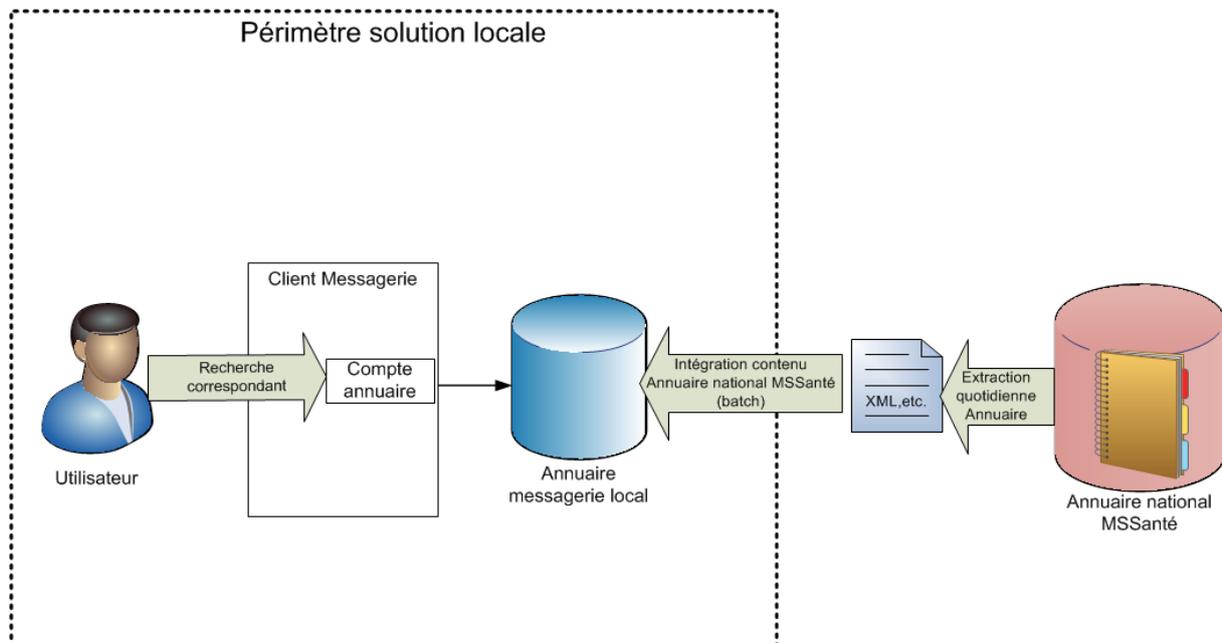


Figure 21 : Intégration de l'Annuaire national MSSanté au sein du domaine MSSanté

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

3.6.4 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 national MSSanté.

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

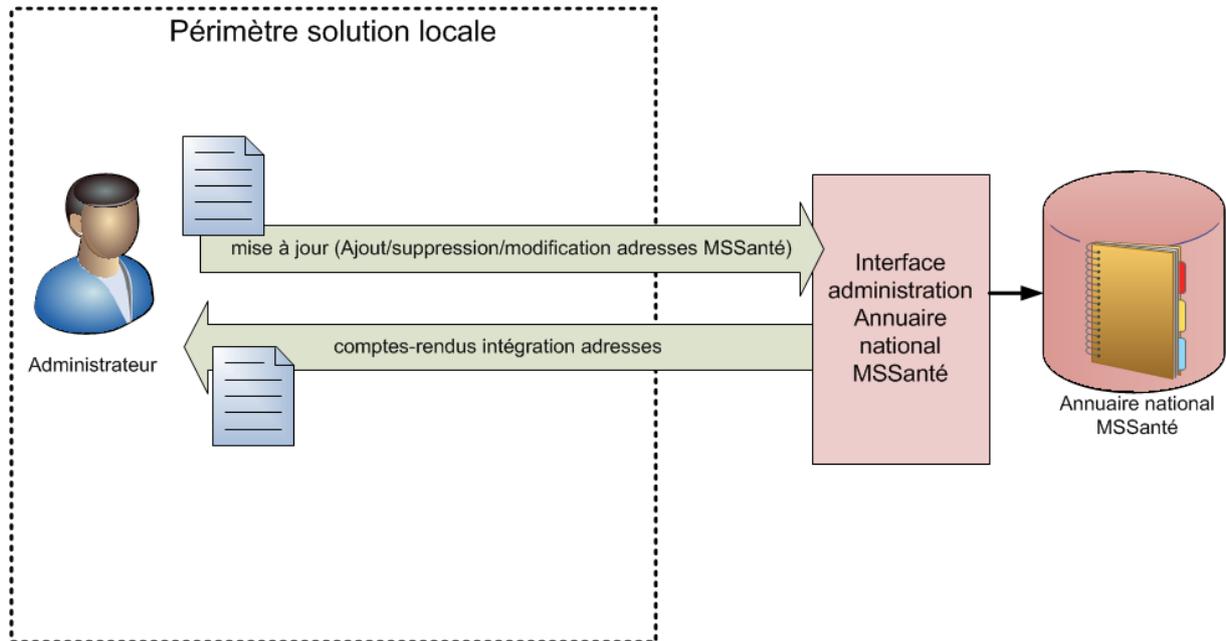


Figure 22 : Publication dans l'Annuaire national MSSanté

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

4 Gestion des boîtes aux lettres au sein de l'espace de confiance MSSanté

4.1 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.

L'utilisateur 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 ou @etablissementB-securise.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 seront référencées dans l'Annuaire national MSSanté.

Un opérateur MSSanté peut proposer à ses utilisateurs d'accéder aux boîtes aux lettres de plusieurs manières :

- Soit en proposant des interfaces décrites dans le DST des interfaces clients de messagerie / opérateurs MSSanté (Web Services et/ou IMAPS/SMTPS) pour les logiciels respectant ces spécifications. Cette solution est à privilégier afin de garantir l'interopérabilité des clients de messagerie MSSanté.
- Soit 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 réglementaires ;

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

- Les utilisateurs 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 n'accèdent qu'aux BAL MSSanté sur lesquelles ils disposent d'une habilitation d'accès.

4.1.1 Présentation des types de 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 (boîte aux lettres personnelles), à des groupes d'utilisateurs (boîte aux lettres organisationnelles) ou à des applications (boîte aux lettres applicatives).

Les opérateurs MSSanté sont libres de proposer les types de BAL de leur choix et ont la possibilité de définir les offres qui leur semblent pertinentes.

4.1.1.1 Boîtes aux lettres personnelles

Ce sont des boîtes aux lettres nominatives, rattachées à des personnes physiques. Elles sont réservées à l'usage d'un professionnel de santé ou de tout professionnel habilité.

4.1.1.2 Boîtes aux lettres organisationnelles

Ce sont des boîtes aux lettres dont l'accès est possible pour un ensemble de professionnels de santé ou de professionnels habilités. Ces boîtes doivent être créées sous la responsabilité d'un professionnel habilité, qui définit ainsi la liste des professionnels qui seront habilités à utiliser la BAL (consultation et envoi de messages). L'opérateur doit être en capacité d'identifier les personnes physiques qui ont utilisé la BAL et de tracer les accès à la BAL.

Ces BAL organisationnelles peuvent, par exemple, être attribuées à un secrétariat, un service, un pôle, etc. et peuvent être utilisées par un groupe d'utilisateurs exerçant au sein d'une même structure (exemple : services de neurologie, de psychiatrie, centre d'imagerie, secrétariat médical, etc...).

Les professionnels habilités seront donc en capacité d'accéder à la même boîte aux lettres et d'émettre des messages au nom du secrétariat/service/pôle (et non pas à titre personnel).

Exemple de mise en œuvre : Ces BAL organisationnelles peuvent être utilisées, par exemple, par les secrétaires médicales, sous la responsabilité d'un professionnel habilité, pour faciliter l'envoi de compte-rendu et la réception de mail dans un établissement de santé. Dans ce cas, c'est à l'établissement de santé de gérer les habilitations et les accès à cette BAL organisationnelle en fonction de la politique de sécurité de son SI.

4.1.1.3 Boîtes aux lettres applicatives

Elles sont associées à un logiciel métier ou à une machine (dossier patient informatisé, système d'information de laboratoire, serveur de résultats, etc...) et sont accédées directement par le logiciel ou la machine. Elles sont utilisées à des fins d'envois ou de réception automatisés.

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.

4.1.1.4 Boites aux lettres de test

Un opérateur peut ouvrir des boites aux lettres de test dans l'espace de confiance MSSanté. 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 bien applicative en fonction de son besoin.

EX_GBM_4000

 Les boites aux lettres de test doivent comporter dans leur dénomination la mention test. Elles ne doivent pas comporter de nomination relative aux noms et prénoms de personnes physiques.

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 de santé à caractère personnel**. Elles ne sont autorisées à échanger qu'avec :

- Les boites aux lettres appartenant aux domaines de l'opérateur
- Les boites aux lettres de test des autres domaines

4.1.1.4.1 Boites aux lettres de réponse automatique

Pour faciliter l'interopérabilité entre les systèmes de messagerie, l'opérateur doit mettre à disposition une boite aux lettres de réponse automatique pour chacun de ces connecteurs de messageries.

Cette boite aux lettres de réponse automatique est considérée comme une boite aux lettres de test, elle doit donc répondre aux mêmes exigences. Elle doit être configurée pour répondre aux messages qu'elle reçoit de manière automatique.

Ces boites aux lettres n'ont pas d'objectif de supervision et ne sont pas destinées à être interrogées par des dispositifs comme des sondes. Elles ne doivent donc pas recevoir de messages automatiques de manière répétée.

EX_GBM_4020

Chaque opérateur doit mettre à disposition au moins une boîte aux lettres de réponse automatique.

Les opérateurs possédant plusieurs domaines dans l'espace de confiance doivent mettre à disposition un domaine de test spécifique et nommer leur boîte aux lettres de réponse automatique de la manière suivante :

Reponse.automatique@domaineoperateur.test.mssante.fr

Les opérateurs ne possédant qu'un seul domaine peuvent utiliser ce même domaine pour mettre à disposition leur boîte aux lettres de tests. Dans ce cas-là, la boîte aux lettres doit se nommer comme ci-dessous ;

Reponse.automatique-test@domaineoperateur.mssante.fr

EX_GBM_4030

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

4.1.2 Les statuts (états) des BAL de l'espace de confiance MSSanté

Le tableau ci-dessous dénomme les états que peut prendre une boîte aux lettres au sein de l'espace de confiance MSSanté.

Etat de BAL	Description
Active	Une boîte aux lettres est active lorsque la dernière date de connexion est inférieure à 30 jours.
Inactive	Une boîte aux lettres est considérée comme inactive lorsque la date de dernière connexion est supérieure à 30 jours. Cette notion est utilisée afin de caractériser l'activité des boîtes 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. A 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 transmis dans l'Annuaire Santé.

4.2 Les acteurs de l'espace de confiance MSSanté

4.2.1 Les rôles dans l'espace de confiance MSSanté

Les comptes de messagerie de l'espace de confiance MSSanté, s'organisent autour des rôles décrits ci-dessous :

Rôle	Entité d'appartenance	Description
Utilisateur final d'une BAL MSSanté	Responsable de traitement	Le ou les personnes physiques qui sont habilités à consulter/envoyer/recevoir des messages depuis une BAL MSSanté
Responsable opérationnel d'une BAL organisationnelle ou applicative	Responsable de traitement	Le responsable opérationnel est un professionnel habilité garant du bon usage d'une boîte aux lettres organisationnelle (gestion des professionnels habilités à y accéder...) ou applicative : respect des règles d'utilisation de l'espace de confiance et des CGU du service de messagerie. Le responsable de traitement s'assure qu'un responsable opérationnel est défini pour chaque BAL organisationnelle ou applicative.
Gestionnaire des BAL MSSanté au sein de la structure	Responsable de traitement	Au sein d'un établissement, personne en charge de gérer la liste des professionnels habilités à disposer d'une BAL MSSanté (nominative ou nom). 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	Opérateur MSSanté	Point de contact de l'opérateur identifié 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	Opérateur MSSanté	Point de contact de l'opérateur identifié 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	Opérateur MSSanté	Personne en charge des tâches 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.

4.2.2 Les acteurs éligibles à l'espace de confiance MSSanté

4.2.2.1 Quels acteurs peuvent s'équiper d'une boîte aux lettres personnelle

Un professionnel est éligible à s'équiper d'une boîte aux lettres 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. Pour les professionnels de santé, l'article R1110-2 du code de santé publique établit une liste des professionnels de santé habilités.

- Les finalités de traitement des données de santé par le professionnel utilisateur de la boîte aux lettres personnelle entrent dans les conditions définies par l'article L1110-4 du code de santé publique.
- Le professionnel est référencé dans l'Annuaire Santé. Ce référencement se fait en concertation avec les organismes représentant ce professionnel et permet d'attester de son identité.

L'ASIP Santé met à disposition des opérateurs une extraction permettant de consulter la liste des professionnels répondant aux trois critères ci-dessus et éligibles à s'équiper de boîtes aux lettres personnelles (cf. chapitre [5.5.3](#)). Cette extraction est mise à jour quotidiennement par les informations transmises par les autorités d'enregistrement qui attestent de l'identité des professionnels habilités.

L'ASIP préconise aux opérateurs d'implémenter un contrôle lors de la création d'une BAL personnelle basé sur cette extraction.

EX_GBM_4200 (anciennement EX_PBA_5110)

L'opérateur doit s'assurer que les BAL MSSanté personnelles sont exclusivement utilisées sous la responsabilité du professionnel titulaire de cette adresse.

4.2.2.2 Quels acteurs peuvent accéder à une boîte aux lettres organisationnelle ou applicative

L'ouverture de boîte aux lettres organisationnelle ou applicative dans l'espace de confiance MSSanté se fait selon les conditions suivantes :

- Les boîtes aux lettres organisationnelles ou applicatives sont ouvertes sur demande du responsable de la structure. Il a pour charge de désigner un responsable opérationnel qui veillera à respecter les conditions d'accès et d'usage de la BAL (les accès se font bien de manière nominative et les données échangées entrent bien dans les finalités de l'espace de confiance MSSanté). Les professionnels accédant à ce type de BAL doivent être des professionnels habilités.
- Les boîtes aux lettres organisationnelles ou applicatives doivent être rattachées à une structure possédant un numéro FINESS ou bien un numéro SIRET/SIREN référencé dans l'Annuaire Santé.

EX_GBM_4210 (anciennement EX_PBA_5120)

L'opérateur doit s'assurer que l'usage des BAL MSSanté organisationnelles ou applicatives s'effectue sous la responsabilité d'un ou plusieurs responsables opérationnels qui sont des professionnels habilités.

EX_GBM_4220 (anciennement EX_PBA_5160)



Le ou les professionnels indiqués en tant que responsables opérationnels d'une BAL Organisationnelle ou Applicative doivent être des professionnels habilités à échanger des données de santé personnelles dûment identifiés dans une base des utilisateurs.

L'opérateur doit être en capacité de tracer l'ensemble des utilisateurs d'une BAL organisationnelle ou bien applicative

EX_GBM_4230 (anciennement EX_PBA_5130)



L'opérateur doit tenir une base des utilisateurs MSSanté interne permettant de faire le lien entre les BAL MSSanté de ses domaines et ses utilisateurs.

4.3 L'ouverture de boîte aux lettres au sein de l'espace de confiance MSSanté

L'opérateur a pour charge de veiller à ce que les boîtes aux lettres créées dans l'espace de confiance MSSanté respectent les exigences de nomenclature suivantes :

EX_GBM_4300 (anciennement EX_PBA_5070)



Le format des adresses de messagerie MSSanté doit respecter la RFC 5321 (<http://tools.ietf.org/html/rfc5321>).

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 en compte « @ » dans les 256 caractères maximum autorisés).

EX_GBM_4310 (anciennement EX_PBA_5020)



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.

RE_GBM_4320 (anciennement RE_PBA_5020)

La RFC 3696 étant très permissive il est recommandé d'être vigilant sur les règles de bon usage en termes de nommage des adresses de messagerie par rapport aux pratiques en vigueur dans les implémentations de messagerie existantes.

Concernant la partie local-part de l'adresse mail (avant l'arobase), l'Annuaire Santé est plus restrictif que la RFC 3696 car il accepte jusqu'à 64 caractères parmi les suivants (ne pas prendre en compte les points-virgules) : _ ; - ; + ; minuscules ; majuscules ; chiffres de 0 à 9.

Il est également recommandé d'utiliser des adresses de messagerie explicites, permettant 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-securise.fr
 - prenom.nomn°d'ordre@domaine-securise.fr
- Pour les BAL organisationnelles :
 - service-nom_du_service@domaine-securise.fr
 - service-cardiologie@domaine-securise.fr
 - cabinet-dr-martin@domaine-securise.fr
 - service-pr-dupont@domaine-securise.fr
 - institut-pasteur.secretariat@domaine-securise.fr
- Pour les BAL applicatives (pour des BAL rattachées à des applications ou des machines) :
 - automate_biologie_14@domaine-securise.fr
 - dispositif_médical_XYZ@domaine-securise.fr
 - notification_SIH_ABC@domaine-securise.fr

L'ensemble des boîtes aux lettres ouvertes dans l'espace de confiance doivent être publiées dans l'Annuaire Santé à l'exception des boîtes aux lettres de test.

RE_GBM_4320 (anciennement RE_PBA_5010)

Il est recommandé d'être vigilant sur la gestion de la réattribution des BAL MSSanté, par exemple, sur la période nécessaire avant de pouvoir réattribuer une BAL à un autre PS (le cas échéant).

4.4 Les règles de fonctionnement des boîtes aux lettres au sein de l'espace de confiance MSSanté

4.4.1 Fonctionnalités relatives aux BAL de l'espace de confiance MSSanté

Les boîtes aux lettres de l'espace de confiance doivent répondre aux exigences suivantes

EX_GBM_4410 (anciennement EX_REM_5010)



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).

Libre choix ensuite à l'opérateur de permettre des échanges de messages de taille supérieure à 10 Mo.

EX_GBM_4420 (anciennement EX_3.2_5030)



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 (anciennement EX_PBA_5080)



L'opérateur émetteur de message 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 à leur suite les actions appropriées.

RE_GBM_4410 (anciennement RE_PBA_5030)



La RFC 5321 précise les bonnes pratiques de notification du statut de remise de message (voir § 5.7.1.1).

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 de messagerie réceptionnant une notification à destination d'un utilisateur 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.).

4.4.2 Mesures de sécurité propres aux messageries MSSanté

De par sa conception basée sur une liste blanche des domaines autorisés, l'Annuaire national MSSanté 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 par la MSSanté, 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 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 DSFT Opérateurs.

4.4.2.1 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 suspects ;
- Installer des outils anti-phishing pour les BAL ou les navigateurs tels que SpamAssassin, ClamAV, etc.

4.4.2.2 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 [§5.8.5](#)

4.5 Suspension d'une boîte aux lettres de l'espace de confiance MSSanté

4.5.1 Caractéristiques d'une BAL suspendue

Lorsqu'une boîte 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 boîte aux lettres suspendue de l'espace de confiance MSSanté n'est plus accessible par son ou ses utilisateurs. Cette boîte aux lettres ne peut plus émettre ni recevoir de messages.

Les boîtes 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 boîtes aux lettres de l'espace de confiance MSSanté.

La suspension d'une boîte 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 boîtes aux lettres suspendues

Pour les opérateurs souhaitant mettre en place le dispositif de suspension des boîtes 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).



4.5.2 Comment suspendre une boîte aux lettres de l'espace de confiance

Un opérateur peut, lorsqu'il constate un mésusage d'une boîte 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 boîte aux lettres. Il doit cependant notifier le responsable de la structure dans un délai prévu par les CGU de la suspension de la boîte aux lettres. Cette notification doit comprendre le motif de la suspension.

L'ASIP Santé, 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 boîtes 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 boîte aux lettres de l'espace de confiance MSSanté doit prévoir un dispositif permettant la réactivation de cette même boîte 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 boîte aux lettres lorsque cette dernière est suspendue.

4.6 Suppression d'une boîte aux lettres de l'espace de confiance MSSanté

Les boîtes aux lettres de l'espace de confiance MSSanté supprimées n'existent plus physiquement.



EX_GBM_6010

Le service de messagerie de l'opérateur doit comporter un dispositif permettant de supprimer les boîtes aux lettres en cas d'absence d'authentification de l'utilisateur 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 messagerie sécurisée.

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 boîtes 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.

5 Exigences fonctionnelles et techniques à respecter par les opérateurs MSSanté

Le contrat « opérateur MSSanté » [\[CONTRAT-MSSANTE\]](#) conditionne l'intégration validée de l'opérateur à l'espace de confiance au respect notamment d'un ensemble de dispositions techniques et fonctionnelles identifiées dans le présent DSFT 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 DSFT (voir § 1.3 « Gestion des versions successives »).

Ces exigences concernent :

- Directement chacune des transactions implémentées par l'opérateur (voir § 5.1 à 5.7)
- La mise en œuvre globale d'un service d'opérateur (voir § 5.8) :
 - Synchronisation du temps (§ 5.8.1),
 - Gestion des traces (§ 5.8.2),
 - Production de statistiques d'utilisation (§ 5.8.3),
 - Définition de Conditions Générales d'Utilisation (CGU) du service MSSanté (§ 5.8.4),
 - Exigences complémentaires de sécurité (§ 5.8.5),
 - Système d'auto-configuration pour les clients de messagerie (§ 5.8.6).

L'opérateur MSSanté doit mettre en œuvre un Connecteur MSSanté (voir § 3.3) pour le raccordement de son serveur de messagerie à l'espace de confiance MSSanté.

L'opérateur MSSanté peut également mettre en œuvre un Connecteur à l'Annuaire national MSSanté (voir § 3.4) pour la recherche dans l'Annuaire national MSSanté par les utilisateurs de son service de messagerie.

L'opérateur MSSanté doit fournir lui-même des BAL MSSanté aux utilisateurs de son service (voir § 4.1).

5.1 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 national MSSanté				
TM1.1.1P	Mise à jour des BAL dans l'Annuaire national MSSanté 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 national MSSanté	Obligatoire	Web Services SOAP
Consultation / Téléchargement d'une extraction de l'Annuaire national MSSanté				
TM2.1.1A	Consultation de l'Annuaire national MSSanté par le protocole LDAP	Recherche multicritères de correspondants dans l'Annuaire national MSSanté	Option	LDAP
TM2.1.3A	Téléchargement d'une extraction de l'Annuaire national MSSanté	Récupération d'une copie des données de l'Annuaire national MSSanté par téléchargement d'une extraction		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.	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
Emission et réception de messages				
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	SMTPS
TM3.2P	Emission de messages	Fonctions d'émission de messages vers des domaines de l'espace de confiance MSSanté, sur le protocole SMTP avec extension STARTTLS	Obligatoire	SMTPS

Tableau 1 : Liste des transactions MSSanté pour les opérateurs MSSanté

5.2 Modalités techniques pour assurer la sécurisation des échanges

Ce chapitre décrit les modalités de raccordement des Connecteurs MSSanté mis en œuvre par les opérateurs pour accéder à l'espace de confiance MSSanté.

5.2.1 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'ASIP Santé et tous les Connecteurs MSSanté des opérateurs doivent la prendre en compte (voir § 5.6.2 « 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 SMTPS, c'est-à-dire le protocole SMTP standard, sécurisé par une connexion TLS mettant en œuvre une authentification mutuelle des deux extrémités par certificats X509 (délivrés par l'ASIP Santé).

Le protocole SMTPS permet d'assurer l'identification et l'authentification réciproque des deux MTA, et d'assurer l'intégrité et la confidentialité des échanges.

Afin d'assurer la compatibilité de l'ensemble des Connecteurs MSSanté, l'espace de confiance utilise la version 1.0 de TLS. La version minimale de ce protocole sera amenée à évoluer dans le futur vers la version 1.2.

EX_OPE_5010

Le Connecteur MSSanté de l'opérateur doit supporter TLS 1.0 (cf. RFC 2246 - <http://tools.ietf.org/html/rfc2246>).

Les versions antérieures SSLv2 et SSLv3 ne doivent pas être activées.



Afin de garantir le haut niveau de sécurité possible tout en assurant l'interopérabilité entre opérateurs, il est recommandé de suivre les préconisations suivantes relatives à la configuration TLS :

Versions du protocole TLS :

- TLS1.2 doit être privilégié afin d'anticiper le retrait progressif de TLS 1.0 (cf. RFC 5246 <https://tools.ietf.org/html/rfc5246>) et d'apporter le meilleur niveau de sécurité.
- Dans le cas où TLS 1.2 est activé, TLS 1.1 devra être activé également.
- Dans tous les cas, le support de TLS 1.0 reste requis conformément à l'exigence EX_OPE_5010.
- SSLv2 et SSLv3 doivent être désactivées (se référer à l'exigence EX_OPE_5010).

Algorithmes obsolètes :

- Les suites de chiffrement considérées comme faibles doivent être désactivées, à minima: DES, 3DES, RC4.
- Les suites de chiffrement 'Export' doivent être désactivées.
- Les protocoles de hachages faibles MD5 et SHA1 doivent être désactivés au profit de la famille SHA-2 (SHA256 ou SHA384).

Chiffrement symétrique :

- L'algorithme AES doit être privilégié du fait de son très large support même si d'autres algorithmes offrent un niveau de sécurité équivalent.
- La longueur des clés AES doit être \geq 256bits (128 bits acceptable).
- Le mode intègre doit être privilégié (par exemple AES_256_GCM_SHA384) ou le mode HMAC couplé à l'extension encrypt_then_mac doit être utilisé en cas d'usage de CBC (AES_256_CBC_SHA384).

Chiffrement asymétrique:

- L'algorithme RSA doit être privilégié du fait de son très large support même si d'autres algorithmes offrent un niveau de sécurité équivalent.

Echange de clés :

- L'échange des clés doit se faire avec l'algorithme DH (Diffie Hellman) et non RSA qui ne permet pas la confidentialité persistante et présente des failles de sécurité (faille ROBOT par exemple).
- La longueur du groupe DH doit être \geq 2048 bits (1024 bits acceptable) ou la longueur du groupe elliptique ECDH doit être \geq 256 bits.
- La confidentialité persistante (PFS - perfect forward secrecy) de DH doit être utilisée (DHE ou ECDHE).

Paramètres déconseillés :

- La compression SSL/TLS doit être désactivée.

Par exemple, les suites de chiffrement ci-dessous sont considérées comme à l'état de l'art :

- 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
- 0xC09F: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- 0xC09E: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- 0xC09F: TLS_DHE_RSA_WITH_AES_256_CCM
- 0xC09E: TLS_DHE_RSA_WITH_AES_128_CCM



- 0xC06B: TLS_DHE_RSA_WITH_AES_256_CBC_SHA384
- 0xC067: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Se référer au guide de l'ANSSI « Recommandations de sécurité relatives à TLS » pour plus d'information et sur les extensions TLS conseillées et proscrites.

Remarque : un opérateur proposant plusieurs domaines de messagerie pour son/ses services MSSanté peut mettre en œuvre un certificat (émis par l'ASIP Santé) par domaine mais cela n'est pas une obligation. Le choix de l'implémentation est laissé à l'appréciation des opérateurs.

5.2.2 Validation des certificats serveur

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'ASIP Santé 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'ASIP Santé. Des précisions sur les certificats IGC-CPS utilisés par les serveurs des opérateurs MSSanté sont disponibles aux adresses suivantes : <http://annuaire.asipsante.fr/> (onglet : « Informations ») et https://esante.gouv.fr/sites/default/files/media_entity/documents/Certificats%20X-509%20pour%20CPS2bis%20et%20certifs%20serveurs%20V2.1.pdf.

Des précisions sur les certificats IGC-Santé sont disponibles aux adresses suivantes : <http://igc-sante.esante.gouv.fr/PC/#ca> et <http://integrateurs-cps.asipsante.fr/IGC-Sante>

Gestion de plusieurs chaînes de certification

EX_OPE_5030

 Sur l'interface SMTPS, les Connecteurs de messagerie MSSanté des opérateurs doivent gérer les chaînes de certification de l'IGC-CPS et de l'IGC-Santé gamme Élémentaire.

Chaines de certification

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

RE_OPE_5020

Les certificats utilisés par les serveurs de messagerie des opérateurs MSSanté sont soit :

- issus de l'AC nommée "AC-classe-4" elle-même issue de l'AC "GIP-CPS". Les certificats de ces deux AC sont donc nécessaires pour valider les certificats serveurs. Ils doivent être récupérés sur le site <http://annuaire.asipsante.fr/> (onglet : « Autorités de Certification »), et déployés avec le Connecteur MSSanté de l'opérateur.
- issus de l'AC du domaine "Organisations" elle-même issue de l'AC de gamme "Elémentaire". Les certificats de ces deux AC sont donc nécessaires pour valider les certificats serveurs. Ils doivent être récupérés sur le site <http://igc-sante.esante.gouv.fr/PC/#ca>, et déployé avec le Connecteur MSSanté de l'opérateur.

Remarque : Les certificats racines et intermédiaires servent à vérifier le certificat serveur présenté par l'opérateur distant. Lorsque la vérification de l'intégrité de la chaîne de confiance des certificats 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

RE_OPE_5030

Il est recommandé de faire un contrôle de non révocation des certificats serveurs de l'opérateur de messagerie MSSanté.

L'ASIP Santé, en sa qualité d'autorité de certification ne dispose pas encore d'un service OCSP (Online Certificate Status Protocol). Les CRL de l'IGC-CPS 2BIS et 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 <http://annuaire.asipsante.fr/> dans les onglets « Autorités de Certification » et « CRL » pour les AC de classe 4 de l'IGC-CPS et 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 GIP-CPS installés sont identiques à ceux de la source de confiance.

Pour les certificats IGC-CPS : <http://annuaire.asipsante.fr/>

Pour les certificats IGC-Santé : <http://iqc-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.

5.3 Modalités techniques spécifiques aux Web Services de l'Annuaire national MSSanté

5.3.1 Sécurisation des échanges

EX_WSA_5010



L'authentification mutuelle du Connecteur MSSanté avec le serveur de l'Annuaire national MSSanté constitue un prérequis transverse à l'appel de tout Web Service d'interfaçage avec l'Annuaire national MSSanté (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 national MSSanté.

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 national MSSanté, 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).

5.3.2 Web Services de l'Annuaire national MSSanté en SOAP

5.3.2.1 Encodage et espace de nommage

EX_WSA_5030

Les spécifications du § 5.3.2.1 concernant l'encodage et les espaces de nommage, pour les Web Services de l'Annuaire national MSSanté 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 national MSSanté

Tableau 2 : Liste des Web Services de l'Annuaire national MSSanté 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"`

5.3.2.2 Sécurité et intégrité

EX_WSA_5040



Les spécifications du §5.3.2.2 concernant la sécurité et l'intégrité, pour les Web Services de l'Annuaire national MSSanté en SOAP, doivent être respectées.

La sécurité des échanges avec l'Annuaire national MSSanté 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 national MSSanté en SOAP. Pour en savoir plus sur les modes d'authentification, voir les documents [\[CI-TR-CLI-LRD\]](#) et [\[PG-AUTH\]](#).

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 national MSSanté, 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.

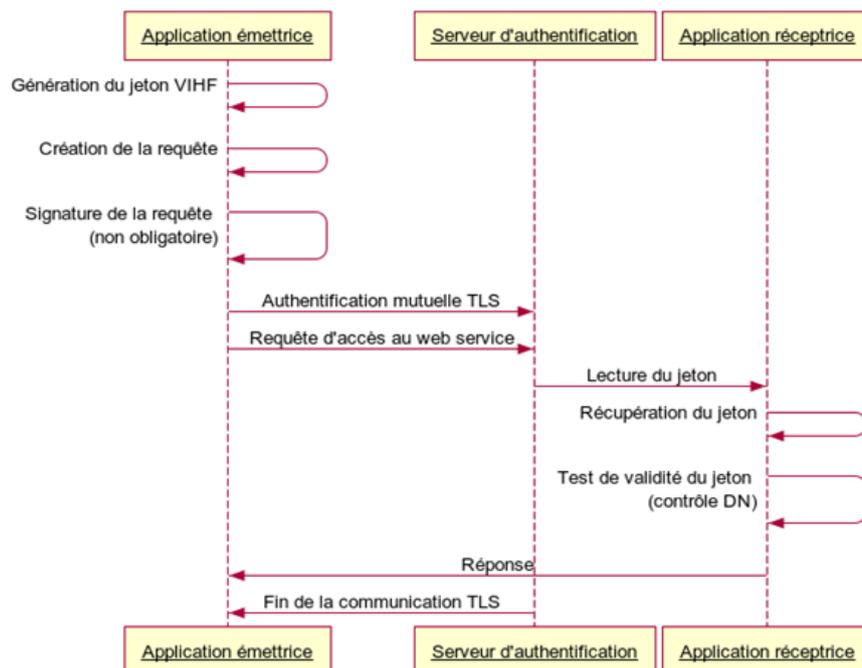


Figure 23 : Principe d'identification et d'authentification

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

- Etablissement d'une session TLS avec authentification mutuelle entre le serveur de l'Annuaire national MSSanté 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 national MSSanté ;
- 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 national MSSanté par rapport à la liste blanche des domaines autorisés ;
- Réponse de l'Annuaire national MSSanté par rapport à l'état du traitement ;
- Fin de la session TLS.

5.3.2.3 Description des échanges

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

5.3.2.3.1 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 »).

5.3.2.3.2 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>.

5.3.2.3.3 Principe de construction des messages

EX_WSA_5050

Les spécifications du § 5.3.2.3.3 (et sous-chapitres) concernant la construction des messages, pour les Web Services de l'Annuaire national MSSanté 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).

5.3.2.3.3.1 *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 national MSSanté, l'élément `Header` du message contient :

- l'extension **WS-Addressing** 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 3 : Éléments 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/@IssuedInstant	Date et heure d'émission de l'assertion SAML	Oui	xs: dateTime	issuedInstant (temps Opérateur) < notBefore (temps Opérateur) < now (temps de réception de la requête par l'Annuaire national MSSanté)) < NotOnOrAfter (issuedInstant (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/AuthenticationContext/AuthenticationContextClassRef	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/AuthenticationInstant	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 réception de la requête par l'Annuaire national MSSanté)) < 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 réception de la requête par l'Annuaire national MSSanté)) < 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	<i>Identité de l'utilisateur</i>	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	<i>Identifiant de L'établissement de santé depuis lequel la requête a été émise</i>	Oui	Alpha Numérique	L'identifiant national de la structure « Struct_IdNat »
LPS_Nom	<i>Nom du logiciel utilisé</i>	Oui	Alpha numérique	Champ technique non vérifié dans ce contexte de requête par un opérateur.
LPS_Version	<i>Version du logiciel utilisé</i>	Oui	Alpha numérique	Champ technique non vérifié dans ce contexte de requête par un opérateur.
LPS_ID	<i>Numéro de série ou identifiant de l'installation du logiciel</i>	Oui	Alpha numérique	Champ technique non vérifié dans ce contexte de requête par un opérateur.
PROFIL_UTILISATEUR	<i>Le profil de l'utilisateur</i>	Oui	OID	code="OPER" codeSystem="1.2.250.1.213.1.9.1.1" codeSystemName="R84" displayName="Opérateur MSSanté"
PROFIL_UTILISATEUR_PERIMETRE	<i>Le contexte métier ou périmètre de l'utilisateur</i>	Non	OID	Vide (car non significatif dans le contexte MSSanté)
VIHF_PROFIL	<i>Le profil VIHF</i>	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 4 : 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 national MSSanté (authentification indirecte).

ws-adressing

```
<soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <wsa:Action>http://annuaire.mssante.fr/webservices/V1011/alimentation/WSAlimentationMSS/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/webservices/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:Password</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
```

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"
h17:code="normal" h17:codeSystem="1.2.250.1.213.1.1.4.248"
h17:codeSystemName="modes accès VIH F 1.0" h17: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"
h17:code="OPER" h17:codeSystem="1.2.250.1.213.1.9.1.1" h17:codeSystemName="R84"
h17: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"
h17:code="profil_annuaire_PS" h17:codeSystem="1.2.250.1.213.1.1.4.312"
h17:codeSystemName="profil VIH F" h17:displayName="Profil pour annuaire de
professionnels de santé du VIH F 2.0" xsi:type="CE"/>
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>

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

```

Figure 24 : Exemple de jeton VIH F pour l'Annuaire national MSSanté (authentification indirecte)

5.3.2.3.3.2 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.

5.3.2.3.3.3 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 :

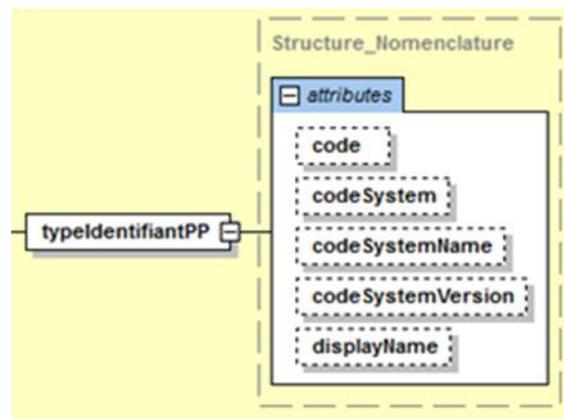


Figure 25 : Structure de la terminologie de référence type d'identifiant d'une personne physique

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

Les terminologies de référence ([\[NOS-RES-TERMII\]](#)) 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	R38	RNR_R38.tab
Compétences exclusives	R40	RNR_R40.tab
Qualification PAC	R44	RNR_R44.tab
Profil_VIHF	Profil VIHF	RNR_Profil_VIHF.tab
Profil d'accès à l'annuaire MSSanté	R84	RNR_R84.tab

Tableau 5 : Terminologies de référence utilisées dans le cadre de MSSanté

5.3.2.3.4 Gestion des erreurs

EX_WSA_5060



Les spécifications du § 5.3.2.3.4 (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'Annuaire national MSSanté en SOAP, doivent être respectées.

5.3.2.3.4.1 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 § 8.8.1 « Codes d'erreurs pour les Web Services de l'Annuaire national MSSanté en SOAP - couche technique et d'échange ».

5.3.2.3.4.2 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.

5.3.3 Web Services de l'Annuaire national MSSanté en REST

5.3.3.1 Encodage et espace de nommage

EX_WSA_5070

Les spécifications du § 5.3.3.1 concernant l'encodage et les espaces de nommage, pour les Web Services de l'Annuaire national MSSanté en REST, doivent être respectées.

Les URIs doivent avoir la forme suivante :

[https://<host>/<silos>/<version>/<ressource>\[?<param_N>=<val_N>\]](https://<host>/<silos>/<version>/<ressource>[?<param_N>=<val_N>])

- En **bleu** la 1^{ère} 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 6 : Codes de statuts HTTP pour les Web Services REST

5.3.3.2 Sécurité et intégrité

EX_WSA_5080

Les spécifications du § 5.3.3.2 concernant la sécurité et l'intégrité, pour les Web Services de l'Annuaire national MSSanté en REST, doivent être respectées.

La sécurité des échanges avec l'Annuaire national MSSanté 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 national MSSanté en REST.

Pour en savoir plus sur les modes d'authentification, voir les documents [\[CI-TR-CLI-LRD\]](#) et [\[PG-AUTH\]](#).

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 national MSSanté, 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 national MSSanté la cinématique est la suivante :

- Etablissement d'une session TLS avec authentification mutuelle entre l'Annuaire national MSSanté 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 national MSSanté ;
- Présentation du certificat d'authentification ;
- Récupération du DN du certificat utilisé ;
- Contrôle de sécurité effectué par l'Annuaire national MSSanté par rapport à la liste blanche des domaines autorisés ;
- Réponse de l'Annuaire national MSSanté par rapport à l'état du traitement ;
- Fin de la session TLS.

5.3.3.3 Description des échanges

5.3.3.3.1 Principes d'échanges

EX_WSA_5090

Les spécifications du § 5.3.3.3.1 (et sous-chapitres) concernant les échanges, pour les Web Services de l'Annuaire national MSSanté en REST, doivent être respectées.



5.3.3.3.2 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>/<silos>/<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 7 : Réponse du Web Service REST de récupération d'une ressource unique

En cas d'échec de l'opération, les codes d'erreur définis au § 8.8.2 « Codes d'erreurs pour les Web Services de l'Annuaire national MSSanté en REST - couche technique et d'échange » doivent être utilisés.

5.3.3.3.3 Gestion des erreurs

EX_WSA_5100

Les spécifications du § 5.3.3.3.3 (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'Annuaire national MSSanté en REST, doivent être respectées.

Les messages d'erreur de la couche technique et d'échange sont définis au § 8.8.2 « Codes d'erreurs pour les Web Services de l'Annuaire national MSSanté 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 8 : Structure du message d'erreur des Web Services REST

5.4 Publication de BAL MSSanté dans l'Annuaire national MSSanté

5.4.1 Description fonctionnelle

EX_PBA_5010

L'opérateur 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 national MSSanté 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 national MSSanté 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 national MSSanté 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).

BAL personnelles, applicatives ou organisationnelles

Les comptes de messagerie peuvent être affectés à des personnes physiques, ou correspondre à des BAL applicatives ou organisationnelles.

L'ensemble des boîtes aux lettres ouvertes dans l'espace de confiance doivent être publiées dans l'Annuaire Santé à l'exception des boîtes aux lettres de test.

EX_PBA_5030

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

Présence des utilisateurs en « Liste rouge »

Les données d'identité des utilisateurs du service de messagerie doivent obligatoirement être transmises par l'opérateur à l'Annuaire national MSSanté.

Si l'utilisateur choisit d'être inscrit en « liste rouge », ses données d'identité ne seront pas affichées lors des recherches dans l'Annuaire national MSSanté. Cela n'empêchera pas pour autant l'utilisateur 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 inscrits en liste rouge est communiquée à la Direction générale de la santé pour l'émission de messages d'alerte sanitaire. Les utilisateurs sont informés et peuvent s'y opposer pour motif légitime.

Publication du numéro de téléphone

Les données d'identité des utilisateurs du service de messagerie de l'opérateur publiées dans l'Annuaire national MSSanté peuvent comprendre le numéro de téléphone de l'utilisateur, à la condition de l'accord explicite de celui-ci. En cas d'acceptation, et sauf inscription en liste rouge, ce numéro de téléphone ne sera accessible qu'aux utilisateurs inscrits auprès d'autres opérateurs MSSanté.

L'opérateur a également la possibilité d'associer un numéro de téléphone aux BAL applicatives ou organisationnelles.

Acceptation de la dématérialisation (ou « Zéro papier »)

Un utilisateur peut porter à la connaissance des autres utilisateurs du système MSSanté, via l'Annuaire national MSSanté son souhait de ne plus recevoir par voie papier des documents d'ores et déjà reçus par voie électronique dans le cadre du système MSSanté.

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

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 ;
- s'il souhaite la publication de son numéro de téléphone ;
- le cas échéant son acceptation de la dématérialisation (ce choix doit également être indiqué pour les BAL applicatives ou organisationnelles).

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

EX_PBA_5050

L'opérateur doit mettre en œuvre les mécanismes techniques permettant de transmettre à l'Annuaire national MSSanté :

- les choix de l'utilisateur concernant : son inscription en liste rouge et son acceptation (ou pas) de la dématérialisation ;
- Le numéro de téléphone de l'utilisateur (le cas échéant).

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 national MSSanté soient fiables.

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 national MSSanté.

EX_PBA_5230



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

5.4.1.1 BAL rattachées à des personnes physiques

Dans le cas des BAL rattachées à des personnes physiques, les données qui doivent être fournies par l'opérateur sont détaillées dans le § 5.4.2.3 « Principe de construction du flux d'alimentation de l'Annuaire national MSSanté ».

EX_PBA_5090

 L'identifiant du titulaire d'une BAL personnelle MSSanté transmis par l'opérateur lors de l'alimentation de l'Annuaire national MSSanté doit impérativement être l'identifiant national (RPPS/ADELI) si le titulaire de la BAL en dispose.

Dans les autres cas, un identifiant interne (**en pratique : l'adresse de la BAL MSSanté attribuée à l'utilisateur**) à la structure d'activité pourra être transmis.

Remarque :

Les professionnels de santé médicaux (Médecin, Sage-Femme, Chirurgien-dentiste) et les pharmaciens disposent d'un numéro RPPS. Les auxiliaires médicaux (infirmiers, ...) disposent d'un numéro Adeli.

Vous pouvez retrouver ce numéro à l'aide de l'extraction décrite en TM2.1.4A ou sur le site annuaire.sante.fr

BAL personnelles avec identifiant national RPPS ou ADELI

Dans le cas de la déclaration d'une BAL MSSanté de personne physique avec identifiant national RPPS ou ADELI dans l'Annuaire national MSSanté, les informations fournies par l'opérateur viennent enrichir les informations d'identité de l'utilisateur déjà présentes dans l'Annuaire national MSSanté (les données pré-chargées dans l'Annuaire national MSSanté 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 national MSSanté 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'ASIP Santé, 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.

La liste suivante présente les 21 professions pour lesquelles la création de BAL personnelles est permise techniquement par l'Annuaire Santé à ce jour. Ces professions rentrent bien entendu dans le cadre légal de l'article R1110-2 du code de la santé publique habilitant certaines professions à échanger des données de santé :

- Professions avec identifiant national RPPS :
 - ✓ Médecin
 - ✓ Pharmacien
 - ✓ Chirurgien-Dentiste
 - ✓ Sage-Femme
 - ✓ Masseur-Kinésithérapeute
 - ✓ Pédicure-Podologue

- Professions avec identifiant national ADELI :
 - ✓ Audioprothésiste
 - ✓ Opticien-Lunetier
 - ✓ Infirmier
 - ✓ Orthoprothésiste
 - ✓ Podo-Orthésiste
 - ✓ Orthopédiste-Orthésiste
 - ✓ Oculariste
 - ✓ Epithésiste
 - ✓ Technicien de laboratoire médical
 - ✓ Orthophoniste
 - ✓ Orthoptiste
 - ✓ Ergothérapeute
 - ✓ Diététicien
 - ✓ Psychomotricien
 - ✓ Manipulateur ERM

Ces professions sont listées dans le jeu de valeurs « JDV_J71-ProfessionFonction-MSSante » qui fait partie des terminologies de référence ([NOS-RES-TERMI]).

Le jeu de valeurs JDV_71 évolue en fonction des professions intégrées dans l'Annuaire Santé et habilitées à disposer d'une boîte aux lettres personnelle MSSanté. Ce document de référence recense la liste exacte des professions pour lesquelles la création de BAL personnelle est techniquement permise par l'Annuaire Santé.

Le jeu de valeurs « JDV_J72-TypeProfessionFonction-MSSante » a également été introduit pour la MSSanté. Il liste les catégories de professions et de fonctions acceptées dans MSSanté. Ce jeu de valeur fait partie des terminologies de référence [NOS-RES-TERMI].

RE_PBA_5120



Afin d'avoir la liste à jour des catégories de professions et des professions pour lesquelles est permise la création de BAL personnelles est permise techniquement par l'Annuaire Santé, l'opérateur devrait consulter régulièrement les dernières mises à jour des tables correspondantes dans le [NOS-RES-TERMI].

D'autres professions habilitées par la loi à échanger des données de santé (article R1110-2 du code de la santé publique) auront par la suite vocation à intégrer l'Annuaire Santé.

BAL personnelles sans identifiant national RPPS ou ADELI

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

L'identifiant d'un professionnel de santé 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 national MSSanté ne l'exonèrent pas du respect des différentes obligations attachées à l'exercice de sa profession.

Rattachement des BAL personnelles dans l'Annuaire national MSSanté avec les situations d'exercice du professionnel de santé

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

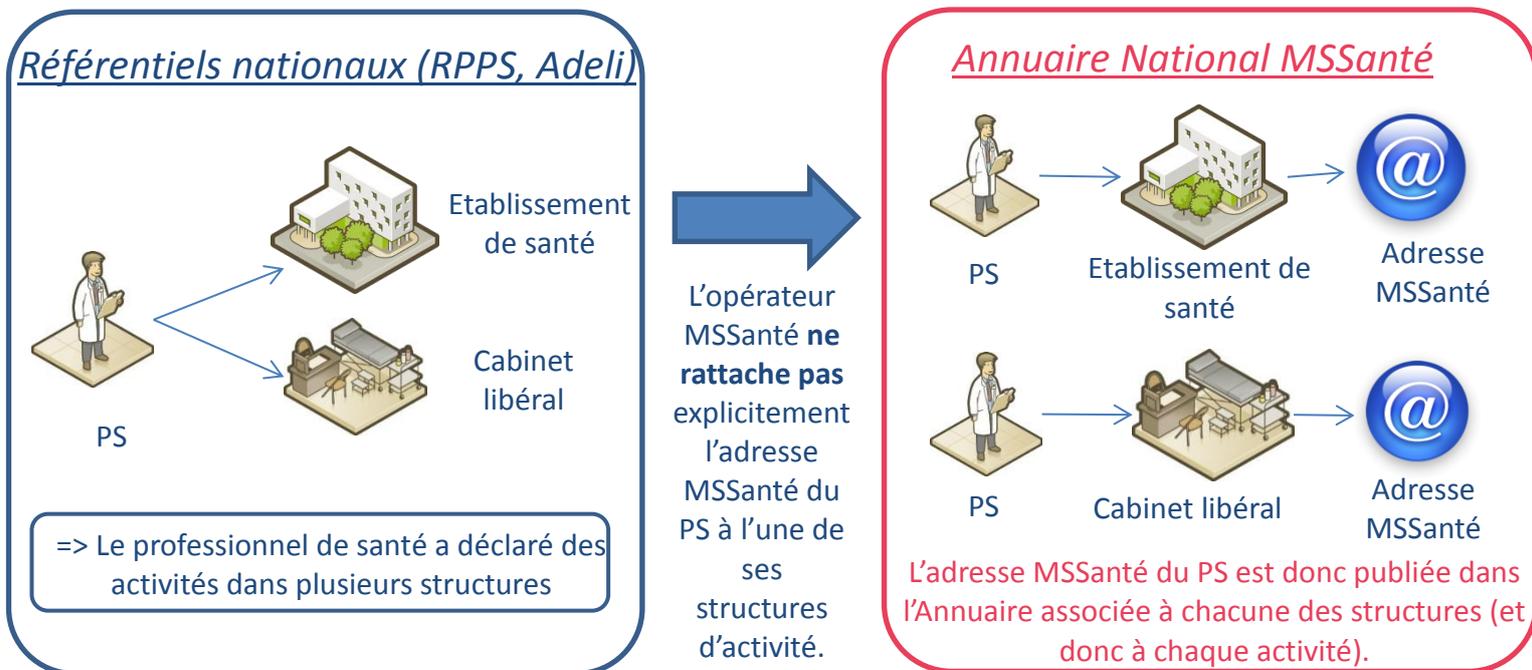


Figure 27 : Publication d'adresses MSSanté dans l'Annuaire national MSSanté dans le cas où l'opérateur MSSanté ne rattache pas explicitement l'adresse MSSanté du PS à l'une de ses structures d'activité

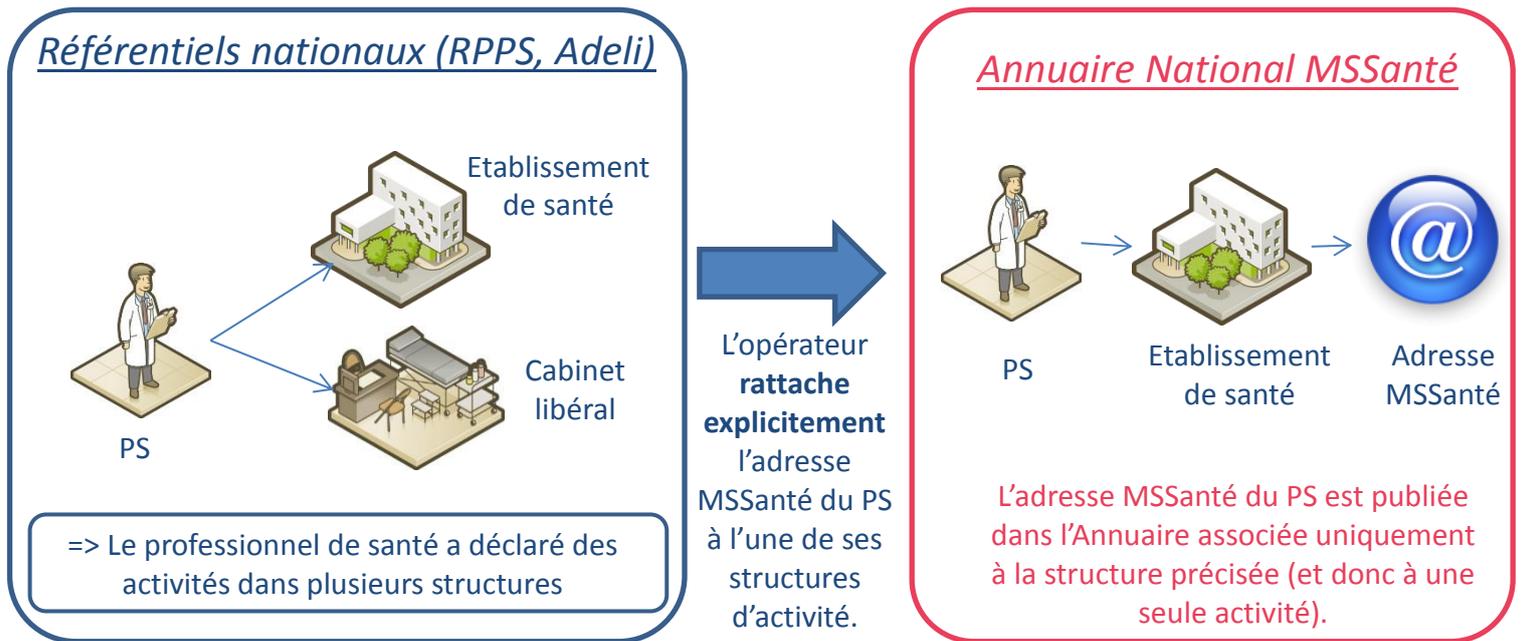


Figure 28 : Publication des adresses MSSanté dans l'Annuaire national MSSanté dans le cas où l'opérateur rattache explicitement l'adresse MSSanté du PS à l'une de ses structures d'activité.

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

- L'adresse MSSanté du PS 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 PS à l'une de ces structures.
- L'adresse MSSanté du PS peut être publiée dans l'Annuaire associée uniquement à une de ses structures d'activité si l'opérateur rattache explicitement l'adresse MSSanté du PS à cette structure.

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

Toutefois, des règles existent pour les cas de figure suivants :

- Dans le cas de BAL personnelles pour professionnels exerçant à titre salarié ou libéral dans des établissements de santé :

EX_PBA_5220



Il est demandé à l'opérateur de rattacher explicitement les BAL personnelles au numéro FINESS (EJ ou EG) de la structure si celle-ci est immatriculée dans le Fichier National des Identifiants Sanitaires et Sociaux.

Cette exigence a pour but d'améliorer la publication dans l'Annuaire national 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 n°FINESS n'y est rattaché).



Pour toute structure non immatriculée dans le Fichier National des Identifiants Sanitaires et Sociaux, il est recommandé à l'opérateur de renseigner l'identifiant issu de la base SIRENE.

5.4.1.2 BAL applicatives et organisationnelles

Dans le cas des BAL applicatives ou organisationnelles, les données qui doivent être fournies par l'opérateur sont détaillées dans le § 5.4.2.3 « Principe de construction du flux d'alimentation de l'Annuaire national MSSanté ».

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

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

La transaction de mise à jour de l'Annuaire national MSSanté 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'ASIP Santé.

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 § 5.4.2 (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 national MSSanté.

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

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

 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 national MSSanté (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 national MSSanté comme indiqué dans l'**EX_WSA_5060**.

5.4.2.1 Cinématique

La cinématique d'alimentation de l'Annuaire national MSSanté 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 national MSSanté 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.

5.4.2.2 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	A 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 9 : Cas d'utilisation du Web Service global d'alimentation de l'Annuaire national MSSanté

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 national MSSanté réceptionne le message et procède à son interprétation.	SA2
3	L'Annuaire national MSSanté identifie l'utilisateur et effectue le contrôle d'accès par rapport à la liste blanche des domaines autorisés.	SA3 SA4
4	L'Annuaire national MSSanté effectue un contrôle syntaxique du contenu du flux (contrôle du respect du schéma XML attendu).	SA2
5	L'Annuaire national MSSanté traite la demande : <ul style="list-style-type: none"> • 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 (<i>aaaammjjhmmss</i>) ; • Envoie en réponse au système initiateur le numéro de ticket généré pour le suivi des demandes d'alimentation. 	SA5

Tableau 10 : 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 national MSSanté.
SA2 : Le message envoyé est mal formaté	
2, 4	L'Annuaire national MSSanté 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 national MSSanté 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 national MSSanté 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 national MSSanté 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 national MSSanté 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 national MSSanté	
5	Si un message ne peut pas être déposé dans le sas de stockage, l'Annuaire national MSSanté envoie un message d'erreur sans traiter la demande (message WSMSS 15).

Tableau 11 : Scénarios alternatifs d'utilisation du Web service global

5.4.2.3 Principe de construction du flux d'alimentation de l'Annuaire national MSSanté

La description WSDL et le schéma XSD du Web Service d'alimentation globale de l'Annuaire national MSSanté (WSDL) associés correspondent respectivement aux documents de référence DR2 et DR3 définis au § 8.6.2 « Documents de référence pour les services ».

5.4.2.3.1 Présentation du flux d'alimentation – en entrée de l'Annuaire national MSSanté

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 § 5.3.2.3.3.1) ;
- **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 pour les PS ou PM du domaine – COMPTESMSS.

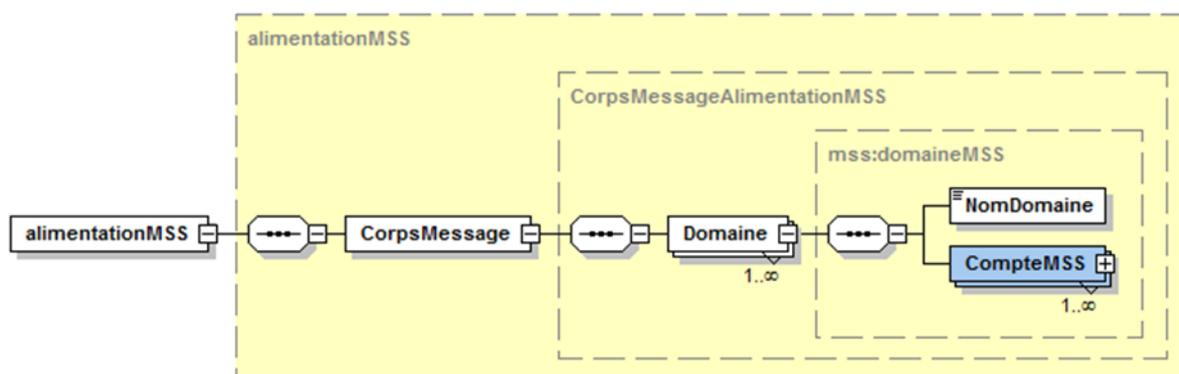


Figure 29 : Corps du message d'alimentation des comptes MSSanté d'un domaine

5.4.2.3.2 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 CONTROLE
Domaine	Domaine de messagerie des BAL MSSanté	Oui	X(255)		RG_CTR_000

Tableau 12 : Structure du domaine des BAL MSSanté

5.4.2.3.3 Structure COMPTESMSS

La structure des BAL (comptes de messagerie) alimentant l'Annuaire national MSSanté est définie dans le tableau suivant :

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
TypeBAL	Valeurs possibles : <ul style="list-style-type: none"> • PER pour BAL Personnelle • ORG pour BAL Organisationnelle • APP pour BAL Applicative 	Oui	X(3)	Une BAL de type PER est rattachée à une personne physique. 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
TypeIdentifiantPP	Valeurs possibles : <ul style="list-style-type: none"> • 0 si identifiant ADELI • 8 si identifiant RPPS • 10 si identifiant interne (adresse de la BAL) 	Oui si typeBAL = PER Non pour les autres types		Nomenclature : 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'Asip Santé	RG_CTR_005 RG_CTR_006 RG_CTR_037
IdentifiantPP	Identifiant ADELI ou Identifiant RPPS ou Identifiant interne (adresse de la BAL)	Oui si typeBAL = PER Non pour les autres types	ADELI :X(9) RPPS : X(11) 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 : <ul style="list-style-type: none"> • 1 si FINESS • 2 si SIREN • 3 si SIRET 	Oui si typeBAL = APP ou ORG Oui si typeBAL = PER avec un identifiant interne Non dans les autres cas		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 CONTROLE
IdentifiantPM	Numéro FINESS (juridique ou géographique) ou Numéro SIREN ou Numéro SIRET	Oui si typeBAL = APP ou ORG Oui si typeBAL = PER avec un identifiant interne Non dans les autres cas	X(32)	L'identifiant de structure ne correspond pas obligatoirement à une structure associée à une situation d'exercice. Cet attribut est facultatif pour les BAL ayant un TypIdentifiantPP = 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_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. Pour les BAL ayant un TypIdentifiantPP = 0 ou 8 (ADELI/RPPS), la valeur fournie ne sera prise en compte que si un identifiant de structure est renseigné.	RG_CTR_036
CiviliteExercice	Civilité de la situation d'exercice de l'utilisateur	Oui si typeBAL = PER avec un identifiant interne Ne pas renseigner dans les autres cas		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 : <ul style="list-style-type: none"> • <u>Médecin</u> : PR (Professeur) / MG (Médecin Général) / MC (Médecin chef) / DR (Docteur) • <u>Pharmacien</u> : PR (Professeur) / PC (Pharmacien Chef) / PG (Pharmacien Général) / DR (Docteur) • <u>Chirurgien-dentiste</u> : PR (Professeur) / DR (Docteur) En cas d'erreur sur la civilité d'exercice par rapport	RG_CTR_017 RG_CTR_018 RG_CTR_040

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
				à la profession saisie, un code erreur MSS017 sera remonté dans le rapport d'alimentation.	
NomExercice	Nom d'exercice de l'utilisateur (nom sous lequel il exerce)	Oui si typeBAL = PER Ne pas renseigner dans les autres cas	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 si typeBAL = PER Ne pas renseigner dans les autres cas	X(50)	Attribut renseigné uniquement si typeBAL = PER.	RG_CTR_020 RG_CTR_021
CategorieProfessions	Catégorie de professions de l'utilisateur Exemple : <ul style="list-style-type: none"> 01 pour les professionnels de santé 06 pour des fonctions dans des expérimentations 	Oui si typeBAL = PER avec un identifiant interne Ne pas renseigner dans les autres cas		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 si typeBAL = PER avec un identifiant interne Ne pas renseigner dans les autres cas		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 <i>Cet attribut correspond à la spécialité ordinale et est dépendant de la profession ou à la compétence exclusive ou à la qualification PAC.</i>	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	RG_CTR_027 RG_CTR_028 RG_CTR_043

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
				<p>CodeSystemName = R44 (qualification PAC) CodeSystem = 1.2.250.1.213.2.34</p> <p>Attribut renseigné uniquement pour les médecins et chirurgiens-dentistes si typeBAL = PER avec un identifiant interne.</p> <p>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.</p> <p>La saisie d'une spécialité est facultative pour un pharmacien, tous ne possédant pas de spécialité. La spécialité est à choisir parmi les 4 codes suivants : SP01, SP02, SP03 et SP04.</p> <p>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.</p> <p>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.</p>	
Responsable	<p>Texte libre donnant les coordonnées de la (ou des) personne(s) responsable(s) au niveau opérationnel de la BAL.</p> <p><i>Exemple : nom, prénom, numéro RPPS...</i></p>	<p>Oui si typeBAL = ORG ou APP</p> <p>Ne pas renseigner si typeBAL = PER</p>	X(160)	<p>Pour faciliter le rattachement de la boîte à un PS, il est recommandé de donner son nom et /ou son numéro RPPS.</p>	RG_CTR_029
Description	Description fonctionnelle de la BAL	<p>Oui si typeBAL = ORG ou APP</p> <p>Ne pas renseigner si typeBAL = PER</p>	X(160)		RG_CTR_030
Telephone	Téléphone (de type fixe ou mobile) lié à la BAL (PER, ORG ou APP)	Non	X(20)		

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
Dematerialisation	Indicateur d'acceptation de la dématérialisation. Valeurs possibles : <ul style="list-style-type: none"> O – dématérialisation acceptée N – dématérialisation refusée 	Oui	X(1)		RG_CTR_031
ListeRouge	Indicateur liste rouge Valeurs possibles : <ul style="list-style-type: none"> 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 national MSSanté.	RG_CTR_032

Tableau 13 : Structure des comptes de messagerie MSSanté

Structure COMPTESS dans le cas de BAL personnelles 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 CONTROLE
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
TypIdentifiantPP	Valeurs possibles : <ul style="list-style-type: none"> 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
TypIdentifiantPM	Type de structure à laquelle la BAL est associée. Valeurs possibles : <ul style="list-style-type: none"> 1 si FINESS 2 si SIREN 3 si SIRET 	Non		Nomenclature : TypIdentifiantPM CodeSystemName = G07 CodeSystem = 1.2.250.1.71.1.2.14 Cet attribut est facultatif pour les BAL ayant un TypIdentifiantPP = 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
IdentifiantPM	Numéro FINESS (juridique ou géographique)	Non	X(32)	Cet attribut est facultatif pour les BAL ayant un TypIdentifiantPP = 0 ou 8 (ADELI/RPPS) mais il	RG_CTR_013 RG_CTR_014

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
	ou Numéro SIREN ou Numéro SIRET			est possible de le fournir afin de pouvoir associer la BAL spécifiquement à une structure donnée lors des recherches sur l'annuaire.	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 : <ul style="list-style-type: none"> • O – dématérialisation acceptée • N – dématérialisation refusée 	Oui	X(1)		RG_CTR_031
ListeRouge	Indicateur liste rouge Valeurs possibles : <ul style="list-style-type: none"> • 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 national MSSanté.	RG_CTR_032

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

Structure COMPTEMSS dans le cas de BAL personnelles sans identifiant national RPPS ou ADELI

Dans le cas de la création d'une BAL personnelle sans identifiant national RPPS ou ADELI, il est nécessaire de fournir l'ensemble des attributs attendus.

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
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
TypIdentifiantPP	Valeurs: <ul style="list-style-type: none"> 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'objet d'une approbation de l'Asip Santé	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
TypIdentifiantPM	Type de structure à laquelle la BAL est associée. Valeurs possibles : <ul style="list-style-type: none"> 1 si FINESS 2 si SIREN 3 si SIRET 	Oui		Nomenclature : TypIdentifiantPM 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 (juridique ou géographique) ou	Oui	X(32)		RG_CTR_013 RG_CTR_014 RG_CTR_016 RG_CTR_033

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
	Numéro SIREN ou Numéro SIRET				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		<p>Nomenclature : CiviliteExercice CodeSystemName = R11 CodeSystem = 1.2.250.1.213.1.6.1.11</p> <p>Attribut renseigné uniquement si typeBAL = PER avec un identifiant interne.</p> <p>La civilité d'exercice ne concerne que les professions de médecin, pharmacien, chirurgien-dentiste et doit être :</p> <ul style="list-style-type: none"> • <u>Médecin</u> : PR (Professeur) / MG (Médecin Général) / MC (Médecin chef) / DR (Docteur) • <u>Pharmacien</u> : PR (Professeur) / PC (Pharmacien Chef) / PG (Pharmacien Général) / DR (Docteur) • <u>Chirurgien-dentiste</u> : PR (Professeur) / DR (Docteur) <p>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.</p>	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
CategorieProfession	Catégorie de professions de l'utilisateur	Oui		CodeSystem = 1.2.250.1.213.1.6.1.3	RG_CTR_022 RG_CTR_023

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
s	Exemple : <ul style="list-style-type: none"> 01 pour les professionnels de santé 06 pour des fonctions dans des expérimentations 			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_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 <i>Cet attribut correspond à la spécialité ordinale et est dépendant de la profession ou à la compétence exclusive ou à la qualification PAC.</i>	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. La spécialité est à choisir parmi les 4 codes suivants : SP01, SP02, SP03 et SP04.	RG_CTR_027 RG_CTR_028 RG_CTR_043

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
				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 : <ul style="list-style-type: none"> • O – dématérialisation acceptée • N – dématérialisation refusée 	Oui	X(1)		RG_CTR_031
ListeRouge	Indicateur liste rouge Valeurs possibles : <ul style="list-style-type: none"> • 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 national MSSanté.	RG_CTR_032

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

Structure COMPTESS dans le cas de BAL applicatives et organisationnelles

Les BAL organisationnelles ou applicatives sont des BAL rattachées à des structures. Dès lors, certains champs ne sont pas nécessaires.

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE	REGLES DE CONTROLE
TypeBAL	Valeurs possibles : <ul style="list-style-type: none"> • 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
TypIdentifiantPM	Type de structure à laquelle la BAL est associée. Valeurs possibles : <ul style="list-style-type: none"> • 1 si FINESS • 2 si SIREN • 3 si SIRET 	Oui		Nomenclature : TypIdentifiantPM 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 (juridique ou géographique) ou Numéro SIREN ou Numéro SIRET	Oui	X(32)	L'identifiant de structure ne correspond pas obligatoirement à une structure associée à une situation d'exercice.	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 CONTROLE
Responsable	Texte libre donnant les coordonnées de la (ou des) personne(s) responsable(s) au niveau opérationnel de la BAL. <i>Exemple : le chef de service....</i>	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 : <ul style="list-style-type: none"> • O – dématérialisation acceptée • N – dématérialisation refusée 	Oui	X(1)		RG_CTR_031
ListeRouge	Indicateur liste rouge Valeurs possibles : <ul style="list-style-type: none"> • 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 national MSSanté.	RG_CTR_032

Tableau 16 : Structure COMPTESMSS dans le cas de BAL applicatives et organisationnelles

5.4.2.3.4 Présentation du flux d'alimentation – en sortie de l'Annuaire national MSSanté

En retour, le serveur de l'Annuaire national MSSanté 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 § 5.3.2.3.4 « Gestion des erreurs ») – FAULT.

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

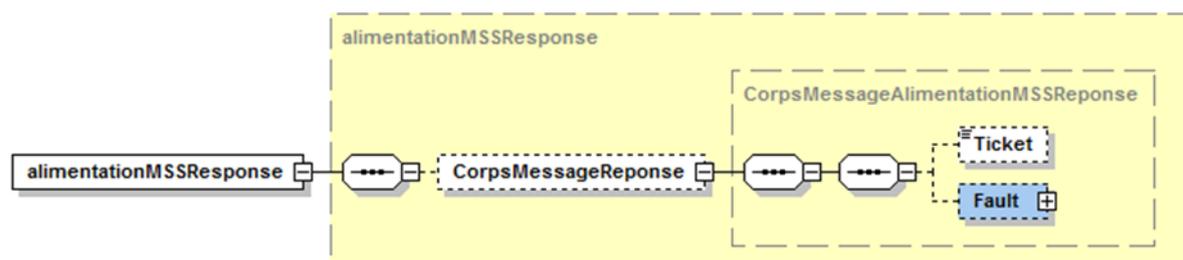


Figure 30 : Message d'accusé de réception ou SOAP Fault

5.4.2.4 Traitement de l'alimentation des messages par le serveur de l'Annuaire national MSSanté

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

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 national MSSanté.

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 :

- A 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 national MSSanté ;
- Production du compte-rendu d'alimentation.

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

En retour d'un message d'alimentation et après traitement, le serveur de l'Annuaire national MSSanté 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 national MSSanté. Le traitement est exécuté **entre 2h et 4h** durant la nuit.

Par conséquent :

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

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_AAAAMMJJHHmss.xml » ;
- Un fichier nommé « cralimentationmss_numero_de_ticket_AAAAMMJJHHmss_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.

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.

EX_1.1.1_5030

 Afin de s'assurer de la bonne publication des BAL MSSanté dans l'Annuaire national MSSanté, 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 : <ul style="list-style-type: none"> • 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 : <ul style="list-style-type: none"> • En établissant une session TLS avec authentification mutuelle ; • En passant en paramètre le numéro du ticket attribué par l'Annuaire national MSSanté. Les comptes rendus d'alimentation disponibles sont les X derniers générés, où X est un nombre paramétrable (de l'Annuaire national MSSanté), dont le maximum est 20.	SA1
2	Le serveur de l'Annuaire national MSSanté réceptionne le message et procède à son interprétation.	SA2
3	Le serveur de l'Annuaire national MSSanté identifie l'utilisateur et effectue le contrôle d'accès par rapport à la liste blanche des domaines autorisés.	SA3, SA4
4	Le système : <ul style="list-style-type: none"> • 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 national MSSanté 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

5.4.2.5.1 Principe de construction du flux

5.4.2.5.1.1 Présentation du flux en entrée du serveur d'Annuaire national MSSanté

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.

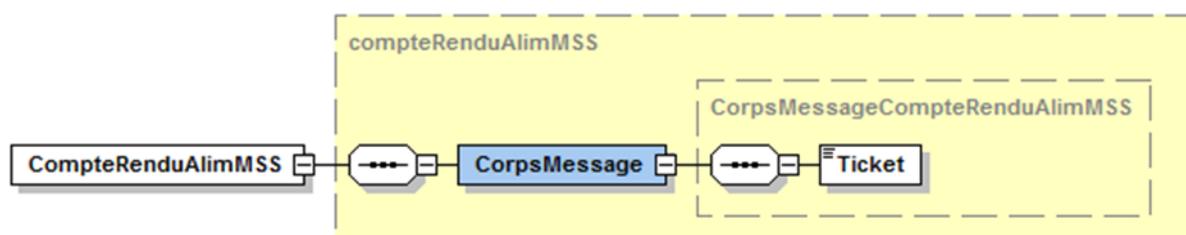


Figure 31 : Corps du message pour la recherche de compte-rendu de traitement

5.4.2.5.1.2 Présentation du flux en sortie du serveur d'Annuaire national MSSanté

En retour le serveur d'Annuaire national MSSanté 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.

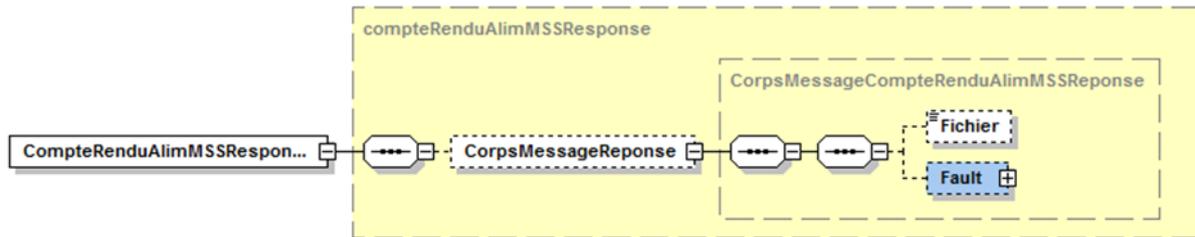


Figure 32 : Corps du message pour la réponse du Web Service de recherche d'un compte-rendu

5.4.2.5.1.3 Description du fichier de compte-rendu d'alimentation

Le fichier de compte-rendu d'alimentation est libellé «cralimentationmss_numero_de_ticket_AAAAMMJJHHmss.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 national MSSanté.
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 – Eléments 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 : <ul style="list-style-type: none"> • 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 en compte « @ » dans les 256 caractères maximum autorisés)

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
TypIdentifiantPP	Identifiant RPPS, ADELI, interne à la structure d'activité. Valeurs possibles : <ul style="list-style-type: none"> • 0 si ADELI • 8 si RPPS • 10 si identifiant interne 	Non	X(2)	Nomenclature : TypIdentifiantPP 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 « TypIdentifiantPP) sont renseignés avec les valeurs indiquées dans le fichier d'alimentation transmis par l'opérateur.
TypIdentifiantPM	Type de structure à laquelle la BAL est associée. Valeurs possibles : <ul style="list-style-type: none"> • 1 si FINESS • 2 si SIREN • 3 si SIRET 	Non	X(2)	Nomenclature : TypIdentifiantPM 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 national MSSanté	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 national MSSanté	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)	
TypIdentifiantPPAnnuaire	Type de l'identifiant national connu dans l'Annuaire national MSSanté	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 : TypIdentifiantPP CodeSystemName = G08 CodeSystem = 1.2.250.1.71.1.2.15
IdentifiantPPAnnuaire	Identifiant national connu dans l'Annuaire national MSSanté		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 § 8.8.3 « Codes d'erreurs pour la TM1.1.xP - Mise à jour des comptes de messagerie dans l'Annuaire national MSSanté ».

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 § 8.6.2 « Documents de référence pour les services ».

5.5 Consultation de l’Annuaire national MSSanté

EX_2.1_5010



L’opérateur MSSanté doit obligatoirement implémenter au moins une des deux solutions disponibles (TM2.1.1A ou TM2.1.3A) afin que les utilisateurs du système MSSanté puissent sélectionner de manière sûre et aisée les destinataires de leurs messages.

RE_2.1_5030



Parmi les deux solutions disponibles, nous recommandons d’utiliser la solution TM2.1.3A correspondant au téléchargement d’une extraction complète de l’Annuaire national MSSanté au moyen de services web. En effet, celle-ci permet une mise en cache locale par l’opérateur de l’Annuaire national MSSanté, dans un objectif d’assurer de meilleures performances et une meilleure résilience, contrairement à la solution TM2.1.1A consistant à consulter l’Annuaire national MSSanté par le protocole LDAP.

5.5.1 TM2.1.1A - Consultation de l’Annuaire national MSSanté par le protocole LDAP

La fonction de consultation de l’Annuaire national MSSanté 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 national MSSanté

Un nombre maximum de résultats est prévu : au-delà, l'Annuaire national MSSanté renvoie un code d'erreur que le **Connecteur à l'Annuaire national MSSanté** 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 national MSSanté sont :

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

RE_2.1_5020



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

Les spécifications liées à l'interrogation de l'Annuaire national MSSanté pour le protocole LDAP sont définies dans le DST des interfaces clients de messagerie / opérateurs MSSanté [\[DST-MSSANTE\]](#).

Remarque :

- Le nom DNS de l'Annuaire national MSSanté 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 national MSSanté 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 national MSSanté de manière automatisée.

5.5.2 TM2.1.3A - Téléchargement d'une extraction de l'Annuaire national MSSanté

EX_2.1.3_5010



Dans le cas où l'opérateur implémente la transaction « TM2.1.3A - Téléchargement d'une extraction de l'Annuaire national MSSanté », il doit respecter les spécifications d'implémentation décrites dans le chapitre § 5.5.2 (et sous-chapitres associés).

L'ASIP Santé met à la disposition des opérateurs une extraction de l'Annuaire national MSSanté, contenant l'ensemble des BAL, tous domaines de messagerie confondus.

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

5.5.2.1 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 § 8.6.2 « Documents de référence pour les services ».

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 national MSSanté avec l'indicateur Liste rouge positionné à « N ».	Informations extraites
Les extractions portent sur les adresses de BAL MSSanté actives.	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
<p>Les extractions sont transmises sous forme d'un fichier compressé d'extension .zip basé sur l'algorithme « deflate ».</p> <p>Le fichier zip contient deux fichiers :</p> <ul style="list-style-type: none"> « ExtractionMSSGlobale_AAAAMMJJHHmss.xml » ; « ExtractionMSSGlobale_AAAAMMJJHHmss_checksum.txt ». <p>Le fichier XML contient les données extraites.</p> <p>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.</p>	Format du fichier
Les fichiers d'extraction sont libellés « <i>ExtractionMSSGlobale_AAAAMMJJHHmss</i> », où AAAAMMJJHHmss 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
<p>Données relatives aux structures extraites pour les BAL personnelles :</p> <ul style="list-style-type: none"> 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. <p><u>Remarques :</u></p> <p>Dans le cas où la personne aurait plusieurs activités ouvertes dans une même structure, cette structure ne serait extraite qu'une fois ;</p> <p>Une BAL peut être extraite sans aucune donnée sur la structure (cas où la personne n'aurait aucune activité ouverte).</p>	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
<p>Pour des personnes possédant plusieurs savoir-faire :</p> <ul style="list-style-type: none"> 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). <p>Pour les autres professions aucun savoir-faire n'est extrait.</p>	Données du savoir-faire
Les adresses (postales) extraites sont celles des structures	Adresse

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

5.5.2.2 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 : <ul style="list-style-type: none"> • 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	A 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, Idif etc.)) Url du type : https://<host>/<silos>/<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 : <ul style="list-style-type: none"> • 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

5.5.2.3 Principe de construction du flux d'extraction de l'Annuaire national MSSanté

5.5.2.3.1 Présentation du flux d'entrée

L'appel se fait via URL :

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

5.5.2.3.2 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 national MSSanté en cas de succès

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

ÉLÉMENT	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 national MSSanté en cas de succès

5.5.2.3.3 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, Idif, dml)
403	Forbidden	Echec d'authentification - L'identité de l'émetteur contenue dans le certificat n'est pas présente dans la liste blanche des domaines autorisés
		Echec 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 national MSSanté en cas d'erreur

5.5.2.3.4 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'Asip Santé
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 FINISS • 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 FINISS 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 : CivileExercice 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. <u>Remarque</u> : 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 ou APP	X(160)	
TELEPHONE	Téléphone (de type fixe ou mobile) lié aux BAL (PER, ORG ou APP)	Non	X(20)	
DEMATERIALIZATION	Indicateur d'acceptation de la dématérialisation. Valeurs possibles : O – dématérialisation acceptée N – dématérialisation refusée	Oui	X(1)	
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

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



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 § 5.5.3 (et sous-chapitres associés).

Afin de permettre aux opérateurs de préparer la publication des BAL MSSanté de leurs utilisateurs finaux dans l'Annuaire national MSSanté, l'ASIP Santé 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.

5.5.3.1 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
<p><u>Professionnels de Santé RPPS :</u></p> <p>Pour les professionnels de santé civils de profession : Sage-femme, médecin, chirurgien-dentiste, sont extraits uniquement les PS inscrits à l'Ordre.</p> <p>Note : Les masseurs-kinésithérapeutes intégreront en 2016 le RPPS</p> <p>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).</p> <p>Pour les professionnels de santé militaires, sont extraits les PS ayant au moins un exercice professionnel.</p> <p>Les professionnels de santé en formation ne sont pas extraits.</p> <p><u>Professionnels de Santé non RPPS :</u></p> <p>Ensemble des professionnels de santé non RPPS porteurs ou non porteurs d'une carte CPS ayant une situation d'exercice active.</p>	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

Description	Concerne
Un PS sans structure d'activité (PS remplaçant par ex) ou sans activité sera extrait sans identifiant de structure, ni adresse.	Tri
<p>Seuls sont restitués les identifiants de structure de type 1, 2 et 3 (FINESS, SIRET ou SIREN).</p> <p>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).</p>	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
<p>Pour des personnes possédant plusieurs savoir-faire :</p> <ul style="list-style-type: none"> • 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). <p>Pour les autres professions aucun savoir-faire n'est extrait.</p>	Données du savoir-faire
Les adresses (postales) extraites sont celles des structures.	Adresse
<p>Le fichier d'extraction des données des personnes physiques porteuses de carte CPS est nommé :</p> <ul style="list-style-type: none"> • « extraction_identites_Avec_CPS_aaaammjjhhmm.csv ». <p>Le fichier d'extraction des données des personnes physiques non porteuses de carte CPS est nommé :</p> <ul style="list-style-type: none"> • « extraction_identites_Sans_CPS_aaaammjjhhmm.csv ». <p>où aaaammjjhhmm est la date et heure de création du fichier.</p>	Nom des fichiers
<p>Les fichiers sont mis à disposition sous forme d'un fichier compressé d'extension .zip basé sur l'algorithme « deflate ».</p> <p>Le fichier ZIP est nommé « extraction_identites_aaaammjjhhmm.zip ».</p> <p>Le fichier ZIP contient quatre fichiers :</p> <ul style="list-style-type: none"> • « 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 ». <p>Les fichiers CSV contiennent les données d'identités définies précédemment.</p> <p>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.</p> <p><u>Remarque</u> : l'ensemble des fichiers sont donc disponible via une seule transaction qui récupère en sortie le fichier zip.</p>	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

Description	Concerne
	disposition

Tableau 33 : Règles d'extraction des fichiers des données d'identités des futurs utilisateurs finaux

5.5.3.2 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 : <ul style="list-style-type: none"> « 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	A 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 34 : 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, Idif etc.)) Url du type : https://<host>/<silos>/<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 : <ul style="list-style-type: none"> 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 35 : 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 36 : Scénarios alternatifs d'utilisation du Web Service de récupération des fichiers des données d'identités

5.5.3.3 Principe de construction du flux d'extraction de l'Annuaire national MSSanté

5.5.3.3.1 Présentation du flux d'entrée

L'appel se fait via URL :

`GET https://ws.annuaire.mssante.fr/webservices/<version>/extractionIdentitePS/?format=csv`

5.5.3.3.2 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 37 : 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 :

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

Tableau 38 : Corps de la réponse du Web Service de récupération des fichiers des données d'identités en cas de succès

5.5.3.3.3 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, Idif, dml)
403	Forbidden	Echec d'authentification - L'identité de l'émetteur contenue dans le certificat n'est pas présente dans la liste blanche des domaines autorisés
		Echec 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 39 : Réponse du Web Service de récupération des fichiers des données d'identités en cas d'erreur

5.5.3.3.4 Format du fichier d'extraction

Les fichiers d'extraction sont libellés :

- extraction_identites_Avec_CPS_aaaammjjhmm.csv ;
- extraction_identites_Sans_CPS_aaaammjjhmm.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_TYPEIDENTIFIANTPP	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 : CivileExercice 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. <u>Remarque</u> : Il ne s'agit pas des valeurs « Monsieur », « Madame », consulter la nomenclature pour plus de détails.

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
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 : <ul style="list-style-type: none"> • 1 si FINISS • 2 si SIREN • 3 si SIRET 	Non		Nomenclature : TypeIdentifiantPM CodeSystemName = G07 CodeSystem = 1.2.250.1.71.1.2.14
LIB_TYPEIDENTIFIANTPM	Libellé du type de structure dans laquelle exerce le PS	Non	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (G07)
IDENTIFIANTPM	Numéro FINISS 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 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
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 CodeSystem = 1.2.250.1.213.2.24

ATTRIBUT	DEFINITION	REQUIS	TYPE	COMMENTAIRE
LIB_NPAYS	Nom du pays	Non	X(256)	« FullySpecifiedName » associé au code dans la terminologie source (R20)

Tableau 40 : Liste des attributs présents dans les fichiers des données d'identités

5.6 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. § 5.7.2 « 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.

5.6.1 Description et format de la liste blanche

La liste blanche est un fichier XML signé par l'ASIP Santé contenant la liste des domaines autorisés au sein de l'espace de confiance MSSanté.

Ce fichier est géré par l'ASIP Santé 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 CPS (<http://annuaire.gip-cps.fr/>) qui recense 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'ASIP Santé avec un certificat logiciel serveur de type SERV_S/MIME de l'IGC Santé	XMLDSIG	Sans Objet	XMLDSIG

Tableau 41 : 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 42 : 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 les 2 IGC. La liste blanche pourra contenir les 2 types de DN. Les champs apparaîtront dans l'ordre indiqué dans le tableau.

Éléments contenus dans le champ DNCertificatOperateur du certificat serveur indiqué en liste blanche	Autorité de certification IGC-CPS	Autorité de certification IGC-Santé
CN	< Nom applicatif >	< Nom applicatif >
OU	<Prefix_Type>< IdNat_Struct >	<Prefix_Type>< IdNat_Struct >
L	< Nom département (N°)>	
O	GIP-CPS	< Raison sociale Structure >
ST		< Nom département (N°)>
C	FR	FR

Tableau 43: 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 (cf. § 8.2.3).
- Le <Prefix_Type> du champ « OU » correspond au prefix 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-CPS ou 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 § 8.6.2 « Documents de référence pour les services ») ;

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 » pour son intégration à l'espace de confiance MSSanté.

5.6.2 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.

5.6.3 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'ASIP Santé ;
- 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/xmlsig-core/>) par le schéma XML suivant : <http://www.w3.org/TR/xmlsig-core/xmlsig-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/xmlsig-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/xmlsig#enveloped)
Algorithme de hachage du contenu à signer	SHA256 (http://www.w3.org/2001/04/xmenc#sha256)

Tableau 44 : 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/xmlsig-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 toute 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 2246 (<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'ASIP Santé et qu'il a été attribué à l'ASIP Santé.

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 § 8.6.2 « Documents de référence pour les services »).

5.7 Réception et émission de messages

5.7.1 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.

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 :

Le nouvel 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 § 5.7.1.1 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).

5.7.1.1 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 chaîne de certificats serveurs présentée par le Connecteur MSSanté émetteur comme défini dans la RFC 2246 (<http://tools.ietf.org/html/rfc2246>) (voir § 5.2 « 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>).

5.7.1.2 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>).



5.7.2 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 § 5.7.2.1 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).

5.7.2.1 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 chaîne 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>).

5.7.2.2 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>).



5.8 Autres exigences applicables aux opérateurs MSSanté

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.

5.8.1 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.

5.8.2 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 et l'exploitant doivent être informés de la génération de traces de leurs actions par le service MSSanté.

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.

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.

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.)

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 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.

Traces fonctionnelles et hébergement des données de santé

Conformément à l'exigence EX_GDT_5050, les traces fonctionnelles contiennent entre autre 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.

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. Des durées recommandées sont définies par la CNIL dans son autorisation unique (voir §2.6).

Le service de l'opérateur devra donc respecter ces durées.

Il appartient au responsable d'un traitement de messagerie sécurisée 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'ASIP Santé a défini les règles suivantes pour permettre aux responsables de traitements utilisateurs de son service, d'être conformes aux recommandations de la CNIL, indiquées dans l'autorisation unique relative aux traitements de messageries sécurisées de santé suscitée :

- 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 médicale⁴. ;
- 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'ASIP Santé rappelle à ses utilisateurs que le service MSSanté 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.

⁴ 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.

5.8.3 Production et soumission de statistiques d'utilisation

L'ASIP Santé met à disposition des opérateurs deux webservice :

- 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'ASIP Santé, 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) sont collectées et transmises à l'ASIP Santé afin de lui permettre d'établir des indicateurs anonymes. Le traitement est mis en oeuvre en application de l'article 5, 5° de la loi n°78-17 du 6 janvier 1978 et du RGPD. Les données sont conservées 3 mois pour construire le rapport d'indicateur mensuel qui exploite et diffuse anonymement les informations des 3 derniers mois. Les données sont ensuite anonymisées. (Plus d'information dans la partie 5.8.4 Définition de Conditions Générales d'Utilisation (CGU) du service MSSanté).

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.

5.8.3.1 Production de statistiques d'utilisation

EX_PSU_5810

Les informations demandées portent sur le mois écoulé, du 1^{er} au dernier jour du mois (chiffres mensuels).

Ces informations sont restituées sous forme de deux fichiers (avec un codage UTF-8) :

- (AAAAMM)_EchangesMSSante_[Domaine].csv
- (AAAAMM)_ConnexionsMSSante_[Domaine].csv

L'opérateur MSSanté doit déposer ces fichiers dans une archive .zip sur un serveur via un webservice de soumission. 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'ASIP Santé **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 boîtes aux lettres suspendues sauf celles au mois N
- Toutes les boîtes aux lettres supprimées sauf celles au mois N
- les boîtes aux lettres de tests



5.8.3.1.1 Format du fichier statistiques MSSanté « Echanges »

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.

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)	Alphanumérique	255	Format mail
DESTINATAIRE	Adresse mail du destinataire	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

Tableau 45 : Liste des attributs pour le fichier de statistiques MSSanté « échanges »

5.8.3.1.2 Format du fichier statistiques MSSanté « Connexions »

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 boîte 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 46 : Liste des attributs pour le fichier de statistiques d'utilisation MSSanté « connexion »

EX_SSU_5800

Le fichier Connexion doit contenir l'ensemble des boîtes aux lettres créées par l'opérateur.

- Si la boîte 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

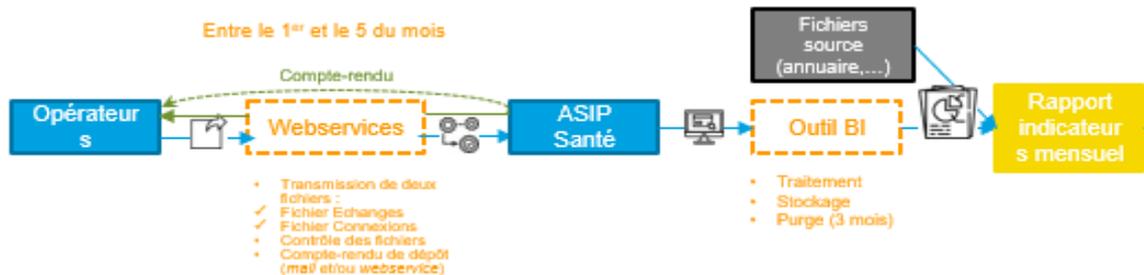
Remarque : des exemples de fichiers « échanges » « connexions » que les opérateurs doivent transmettre à l'ASIP Santé sont également disponibles en annexe et correspondent au document de référence DR4 défini au § 8.6.2 « Documents de référence pour les services ».

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.

5.8.3.2 Soumission des statistiques d'utilisation

L'ASIP Santé met à disposition des opérateurs de nouveaux 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 paragraphe [5.3.1](#).

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 dans 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'ASIP Santé 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	<i>https://ws-sipil.mssante.fr/sipil/postFile</i>
getReport	Nom du webservice pour la récupération du compte rendu	<i>https://ws-sipil.mssante.fr/sipil/getReport</i>

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 : §8.8.4 « Codes d'erreurs pour la soumission des fichiers indicateurs »

5.8.3.2.1 Webservice de dépôt de fichiers statistiques

5.8.3.2.1.1 Présentation du 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 au webservice, la taille maximale de l'archive .ZIP acceptée est de 10Mo. Il n'existe cependant pas de limite par rapport au nombre de fichiers « échanges » 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'ASIP Santé

5.8.3.2.1.2 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">
  <Authentication>
    <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>
    </DomainesGeres>
  </Authentication>
</Depot>
```

```

<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>
</Authentication>
<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 33 : 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.

5.8.3.2.2 Webservice de récupération du compte rendu

5.8.3.2.2.1 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'ASIP Santé.

Dans l'appel du webservice de récupération, l'attribut <id> correspond à l'identifiant obtenu en sortie du webservice de dépôt.

5.8.3.2.2.2 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	
+Authentication	Balise contenant les informations relatives à

	l'étape d'authentification.
++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 lors de l'appel au webservice de dépôt de fichiers statistiques
++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 = 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 3 = L'archive n'a pas pu être traitée : Refus de l'antivirus 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 : <ul style="list-style-type: none"> - Refus de l'antivirus - Archive vide - Archive ne pouvant être ouverte - Autre
+Fichiers	Balise contenant autant de nœud que de fichiers soumis dans l'archive zip soumise.
++InfoTraitement	Informations globales de l'exécution du traitement
+++NomFichier	Nom complet du fichier traité

+++DateDebut	Date de début du traitement
+++DateFin	Date de fin du traitement
+++CodeRetour	Code retour global du traitement. Ce code est associé à un référentiel : 0 = OK 1 = KO 2 = Warning
+++Message	Message associé au code retour global du traitement.
++Controles	Balise contenant autant de nœud que de contrôles réalisés sur le fichier soumis.
+++Controle	Balise générique pour l'ensemble des contrôles réalisés.
++++CodeControle	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 ... L'ensemble des codes sont décrits au chapitre « 8.8.4 Codes d'erreurs pour la soumission des fichiers indicateurs »
++++CodeRetour	Code retour du contrôle réalisé. Ce code est associé à un référentiel : 0 = OK 1 = KO 2 = Warning
++++Message	Message associé au code retour du contrôle réalisé. Dans le cas d'un warning ou d'une erreur, il s'agit de la description du problème rencontré.
++++DateDebut	Date de début du contrôle réalisé
++++DateFin	Date de fin du contrôle réalisé

Tableau 47 : 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 : §8.8.4.4 « Les codes retours appliqués suites aux contrôles des fichiers « Echanges » et « Connexions» »

5.8.3.3 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.

5.8.3.4 Gestion de la phase de transition anciens et nouveaux indicateurs

La procédure de production et soumission des fichiers statistiques décrites dans les paragraphes ci-dessus de l'actuel chapitre 5.8.3 présente une nouvelle procédure différente de celle décrite dans la version v1.2.1 du DSFT Opérateurs. Cette version est accessible à l'adresse suivante : <https://mssante.fr/is/doc-technique>

Les fichiers de statistiques étant différents entre les deux procédures, il est nécessaire d'avoir une cohérence des données soumises par les opérateurs et exploitées par l'ASIP Santé.

EX_SSU_5830



Les opérateurs **doivent continuer à produire** les fichiers de statistiques décrits dans la version v1.2.1 du DSFT Opérateurs pendant au moins 6 mois et ce à partir de la date de publication du présent document. Ces fichiers **doivent envoyés par mail à l'adresse « monserviceclient.mssante@asipsante.fr »**.

L'ASIP Santé informera les opérateurs par communication de l'arrêt du système antérieur de production et soumission des indicateurs. La phase de transition pourrait s'étendre au-delà de 6 mois si la qualité des nouveaux fichiers de statistiques ou leur quantité est jugée insuffisante pour permettre l'élaboration de rapports d'usage de la MSSanté.

5.8.4 Définition de 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 de messagerie 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 de l'article L 1110-4 du code de la santé publique qui précisent les conditions d'échange de données de santé entre deux ou plusieurs professionnels;
- 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 ;
- Information 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.

Bon usage de la MSSanté :

- Information de l'utilisateur sur les finalités de la MSSanté et les conditions d'utilisation de ses données à caractère personnel ;
- Seuls les professionnels habilités à échanger des données de santé personnelles peuvent utiliser le service MSSanté ;
- Le service MSSanté permet l'émission de messages contenant des informations utiles à la prise en charge sanitaire d'une personne, à destination d'un ou plusieurs titulaires d'un compte de messagerie sécurisée de l'espace de confiance MSSanté ;
- L'utilisateur s'engage à ne pas procéder à l'envoi de messages non sollicités à un ou plusieurs destinataires, considéré comme du spam ;
- L'utilisateur s'interdit 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 ;
- L'utilisateur s'engage à ne pas rediriger son adresse sécurisée vers une adresse de messagerie non MSSanté.

Publication dans l'Annuaire national MSSanté :

- L'opérateur doit annoncer dans ses CGU l'existence de dispositifs permettant à tout utilisateur de son service d'indiquer (et de modifier à tout moment) :
 - s'il souhaite être inscrit en liste rouge ;
 - s'il souhaite la publication de son numéro de téléphone ;
 - le cas échéant son acceptation de la dématérialisation.
- L'opérateur doit également prévoir un moyen permettant à tout utilisateur de son service d'être informé que ses données liées à l'usage du système MSSanté sont publiées dans l'Annuaire national MSSanté et consultables par les autres utilisateurs (sauf en cas d'inscription en liste rouge).



Information du patient :

- En cas d'opposition du patient à l'utilisation du service MSSanté pour échanger des données de santé le concernant, l'utilisateur devra recourir à un moyen d'échange alternatif (courrier papier par exemple) ;
- 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.
- L'utilisateur 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.

Collecte des données de l'utilisateur :

- Des données (adresse e-mail, horodatage des échanges, taille des e-mails) sont collectées et transmises à l'ASIP Santé afin de lui permettre, en tant que gestionnaire de l'espace de confiance MSSanté, 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. Les données sont conservées 3 mois, puis anonymisées. 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, de limitation, et du droit de définir des directives sur le sort de ses données après sa mort. L'utilisateur peut, sous réserve de la production d'un justificatif d'identité valide, exercer ses droits sur demande écrite au GIP ASIP Santé (Délégué à la protection des données), 9 rue Georges Pitard, 75015 PARIS ou par messagerie électronique, à l'adresse suivante : dpo.asipsante@sante.gouv.fr. L'utilisateur dispose également d'un droit d'introduire une réclamation auprès de la CNIL.

Valeur probante :

- Afin de prévenir d'éventuelles contestations sur la valeur probante des messages (ou « écrits électroniques ») échangés entre les utilisateurs via le service MSSanté au regard des exigences fixées par la loi 2000-230, l'opérateur MSSanté doit prévoir, dans ses CGU, une clause par laquelle ses utilisateurs s'engagent, en les acceptant, à ne pas contester la force probante des messages sur le fondement de leur nature électronique, et à s'accorder pour reconnaître la même valeur probante aux écrits électroniques transmis via la 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 au sens de l'article 1316-2 du Code civil.

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 ASIP Santé sont accessibles à l'url suivante : <https://mailiz.mssante.fr/cgu>.

5.8.5 Exigences complémentaires de sécurité

5.8.5.1 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.

5.8.5.2 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 DSFT 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'ASIP Santé 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'ASIP Santé 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 :

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 :

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 :

EX_SSI_5080



La capacité du système mis en œuvre pour le service MSSanté doit être testée, suivie et anticipée.

RE_SSI_5010



Il est recommandé de mettre en œuvre une infrastructure matérielle qui permet d'assurer la haute disponibilité du service SMTPS « entrant », afin de minimiser la perte de messages ou de dysfonctionnements qui pourraient compromettre l'interconnexion avec l'espace de confiance MSSanté.

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'ASIP Santé.

L'opérateur doit suivre les recommandations de sécurité issues des Conditions Générales d'Utilisation (CGU) des produits de certification de l'ASIP Santé à destination des établissements de santé. Celles-ci sont les suivantes (Ch 4.1 des CGU – Mesures de sécurité) : « L'Abonné garantit, via sa 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'ASIP Santé. Il devra notamment veiller à limiter l'accès à ces 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 DX27, DX28 et DX29) 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 DX30) 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 auditabilité).

Les exigences concernant les traces sont définies dans le § 5.8.2.

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 national MSSanté sont définies dans le § 5.3 « Modalités techniques spécifiques aux Web Services de l'Annuaire ».

Les exigences de sécurité concernant la liste blanche des domaines autorisés sont définies dans le § 5.6 « Liste blanche des domaines MSSanté autorisés »

Contrôle d'accès réseau :

EX_SSI_5140

Les pare-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.

De plus, si l'incident de sécurité entraîne une violation de données personnelles (divulcation/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.

5.8.5.3 Gestion des incidents opérateurs

EX_SSI_5180

Comme indiqué dans le contrat « opérateur MSSanté » [\[CONTRAT-MSSANTE\]](#), les **opérateurs MSSanté intégrés de façon validés** ont l'obligation de signaler à l'ASIP Santé en tant que gestionnaire de l'espace de confiance « [...] **toute modification, tout dysfonctionnement ou toute anomalie** sur leur service de messagerie sécurisée 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'ASIP Santé de tout arrêt temporaire supérieur à 8 jours.

Les canaux dédiés pour ces déclarations d'incidents sont :

- l'adresse mail : monserviceclient.mssante@asipsante.fr
- le numéro de téléphone : 0 825 852 000 (Service à 0,06 € / min + prix appel, 24/24 Heures - 7/7 Jours).

Consignes à suivre lors de déclaration d'incidents par les opérateurs MSSanté :

Les informations utiles sur les démarches à entreprendre auprès de l'ASIP Santé 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 national MSSanté, certificats serveur, perte de messages, SPAM / Emetteur non autorisé, téléchargement des extractions de l'Annuaire national MSSanté.
3. Les impacts de l'incident.

Déclarer l'incident :

L'incident doit être déclaré par email ou par téléphone à l'ASIP Santé (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.

5.8.6 Système d'auto-configuration pour les clients de messagerie

RE_ACC_5020

Si le contexte d'accès aux BAL de l'opérateur le nécessite, il est recommandé, dans le cas d'une mise en œuvre des interfaces basées sur les protocoles standards de messagerie SMTPS/IMAPS, d'offrir un système d'auto-configuration pour les clients de messagerie.

L'auto-configuration des clients de messagerie s'appuie sur des Web Services spécifiques, par exemple, AutoConfig (également connu sous le nom AutoConfigure) et AutoDiscover.

Ces Web Services sont appelés sur une URL définie en fonction du nom de domaine de l'adresse de messagerie concernée et du client de messagerie utilisé. L'opérateur se charge donc de mettre à disposition ces Web Services pour chacun des domaines et des clients de messagerie pour lesquels il souhaite proposer un service d'auto-configuration.

Le service d'auto-configuration n'est possible que pour les interfaces basées sur les protocoles SMTP/IMAP et permet :

- Aux clients de messagerie de configurer automatiquement les paramètres du compte lors de la configuration initiale de la BAL dans le client de messagerie (en entrant uniquement l'adresse de messagerie) ;
- D'assurer la bonne configuration des clients de messagerie à tout moment via internet, par exemple lorsque le port d'écoute des serveurs SMTP ou IMAP a changé (ce qui permet d'assurer la bonne configuration des clients de messagerie à tout moment via internet).

A titre d'exemple, les ressources Web suivantes peuvent être consultées respectivement pour les Web Services AutoConfig et AutoDiscover :

- <https://wiki.mozilla.org/Thunderbird:Autoconfiguration>
- <http://msdn.microsoft.com/en-us/library/ee332364%28v=exchg.140%29.aspx>.

Remarque : les clients de messagerie les plus populaires implémentent nativement l'interrogation d'un service d'auto-configuration.



6 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	§ DSFT	N° Exigence	Exigence
Gestion des boîtes aux lettres au sein de l'espace de confiance MSSanté	4.1.1	EX_GBM_4000	Les boîtes aux lettres de test doivent comporter dans leur dénomination la mention test. Elles ne doivent pas comporter de nomination relative aux noms et prénoms de personnes physiques.
	4.1.1	EX_GBM_4010	Les boîtes aux lettres de test ne doivent ni émettre ni recevoir des données de santé à caractère personnel . Elles ne sont autorisées à échanger qu'avec : <ul style="list-style-type: none"> • Les boîtes aux lettres appartenant aux domaines de l'opérateur • Les boîtes aux lettres de test des autres domaines
	4.1.1	EX_GBM_4020	Chaque opérateur doit mettre à disposition aux moins une boîte aux lettres de réponse automatique. Les opérateurs possédant plusieurs domaines dans l'espace de confiance doivent mettre à disposition un domaine de test spécifique et nommer leur boîte aux lettres de réponse automatique de la manière suivante : Reponse.automatique@domaineoperateur.test.mssante.fr Les opérateurs ne possédant qu'un seul domaine peuvent utiliser ce même domaine pour mettre à disposition leur boîte aux lettres de tests. Dans ce cas-là, la boîte aux lettres doit se nommer comme ci-dessous ; Reponse.automatique-test@domaineoperateur.mssante.fr
	4.1.1	EX_GBM_4030	Les messages contenus dans la boîte aux lettres de réponse automatique doivent être supprimés au maximum un mois après leur réception.
	4.2.2	EX_GBM_4200 <i>(anciennement EX_PBA_5110)</i>	L'opérateur doit s'assurer que les BAL MSSanté personnelles sont exclusivement utilisés sous la responsabilité du professionnel titulaire de cette adresse.
	4.2.2	EX_GBM_4210 <i>(anciennement EX_PBA_5120)</i>	L'opérateur doit s'assurer que l'usage des BAL MSSanté organisationnelles ou applicatives s'effectue sous la responsabilité d'un ou plusieurs responsables opérationnels qui sont des professionnels habilités.
	4.2.2	EX_GBM_4220 <i>(anciennement EX_PBA_5160)</i>	Le ou les professionnels indiqués en tant que responsables opérationnels d'une BAL Organisationnelle ou Applicative doivent être des professionnels habilités à échanger des données de santé personnelles dûment identifiés dans une base des utilisateurs.
	4.2.2	EX_GBM_4230 <i>(anciennement EX_PBA_5130)</i>	L'opérateur doit tenir une base des utilisateurs MSSanté interne permettant de faire le lien entre les BAL MSSanté de ses domaines et ses utilisateurs.

Fonctionnalité	§ DSFT	N° Exigence	Exigence
	4.3	EX_GBM_4300 <i>(anciennement EX_PBA_5070)</i>	Le format des adresses de messagerie MSSanté doit respecter la RFC 5321 (http://tools.ietf.org/html/rfc5321). 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 en compte « @ » dans les 256 caractères maximum autorisés).
	4.3	EX_GBM_4310 <i>(anciennement EX_PBA_5020)</i>	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 : <ul style="list-style-type: none"> • service-cardiologie@xyz.mssante.fr ; • cabinet-dr-martin@xyz.mssante.fr ; • service-pr-dupont@xyz.mssantefr ; • institut-pasteur.secretariat@xyz.mssante.fr.
	4.4.1	EX_GBM_4410 <i>(anciennement EX_REM_5010)</i>	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). Libre choix ensuite à l'opérateur de permettre des échanges de messages de taille supérieure à 10 Mo.
	4.4.1	EX_GBM_4420 <i>(anciennement EX_3.2_5030)</i>	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.
	4.4.1	EX_GBM_4430 <i>(anciennement EX_PBA_5080)</i>	L'opérateur émetteur de message 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 à leur suite les actions appropriées.
	4.6	EX_GBM_6010	Le service de messagerie de l'opérateur doit comporter un dispositif permettant de supprimer les boîtes aux lettres en cas d'absence d'authentification de l'utilisateur 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 messagerie sécurisée.
	4.6	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.
Emission de messages MSSanté	5.7.2	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
	5.7.2	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).

Fonctionnalité	§ DSFT	N° Exigence	Exigence
	5.2.2	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'ASIP Santé 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).
	5.2.2	EX_OPE_5030	Sur l'interface SMTPS, les Connecteurs de messagerie MSSanté des opérateurs doivent gérer les chaînes de certification de l'IGC-CPS et de l'IGC-Santé gamme Élémentaire.
	5.7.2	EX_3.2_5040	Un opérateur MSSanté ne doit pas utiliser le serveur SMTP d'un autre opérateur MSSanté comme relai de messagerie.
	5.2.1	EX_OPE_5010	Le Connecteur MSSanté de l'opérateur doit supporter TLS 1.0 (cf. RFC 2246 - http://tools.ietf.org/html/rfc2246). Les versions antérieures SSLv2 et SSLv3 ne doivent pas être activées.
	5.7.2.1	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 <u>mais dans tous les cas avant l'envoi du message</u>) ; si ce n'est pas le cas, l'émetteur doit être notifié de la non émission (avec le motif du rejet).
	5.7.2	EX_3.2_5050	Le Connecteur MSSanté mis en œuvre par l'opérateur doit respecter la cinématique décrite dans le § 5.7.2.1 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).
	5.7.2.2	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	5.7.1	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.
	5.7.1	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).
	5.7.1	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.
	5.2.2	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'ASIP Santé 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

Fonctionnalité	§ DSFT	N° Exigence	Exigence
			la Liste Blanche (DN du certificat).
	5.2.2	EX_OPE_5030	Sur l'interface SMTPS, les Connecteurs de messagerie MSSanté des opérateurs doivent gérer les chaînes de certification de l'IGC-CPS et de l'IGC-Santé gamme Elémentaire.
	5.2.1	EX_OPE_5010	Le Connecteur MSSanté de l'opérateur doit supporter TLS 1.0 (cf. RFC 2246 - http://tools.ietf.org/html/rfc2246). Les versions antérieures SSLv2 et SSLv3 ne doivent pas être activées.
	5.7.1	EX_3.1_5030	Le Connecteur MSSanté mis en œuvre par l'opérateur doit respecter la cinématique décrite dans le § 5.7.1.1 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).
	5.7.1.2	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	5.6.1	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) : <ul style="list-style-type: none"> • 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-CPS ou de l'IGC-Santé.
	5.6.2	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 .
	5.6.2	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.
	5.6.3	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/xmlsig-bestpractices/#bp-validate-signing-key .
	5.6.3	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 2246 (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'ASIP Santé et qu'il a été attribué à l'ASIP Santé.
Publication dans l'Annuaire national MSSanté	5.3.1	EX_WSA_5010	L'authentification mutuelle du Connecteur MSSanté avec le serveur de l'Annuaire national MSSanté constitue un prérequis transverse à l'appel de tout Web Service d'interfaçage avec l'Annuaire national MSSanté (ces fonctions sont définies dans les chapitres suivants de ce document).

Fonctionnalité	§ DSFT	N° Exigence	Exigence
(Ajout / Modification / Suppression comptes de messagerie de l'opérateur)	5.3.1	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).
	5.3.2.1	EX_WSA_5030	Les spécifications du § 5.3.2.1 concernant l'encodage et les espaces de nommage, pour les Web Services de l'Annuaire national MSSanté en SOAP, doivent être respectées.
	5.3.2.2	EX_WSA_5040	Les spécifications du §5.3.2.2 concernant la sécurité et l'intégrité, pour les Web Services de l'Annuaire national MSSanté en SOAP, doivent être respectées.
	5.3.2.3.3	EX_WSA_5050	Les spécifications du § 5.3.2.3.3 (et sous-chapitres) concernant la construction des messages, pour les Web Services de l'Annuaire national MSSanté en SOAP, doivent être respectées.
	5.3.2.3.4	EX_WSA_5060	Les spécifications du § 5.3.2.3.4 (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'Annuaire national MSSanté en SOAP, doivent être respectées.
	5.4.1	EX_PBA_5010	L'opérateur 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 : <ul style="list-style-type: none"> • Publier dans l'Annuaire national MSSanté 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 national MSSanté 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 national MSSanté 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).
	5.4.1	EX_PBA_5030	L'opérateur ne doit pas publier de BAL fonctionnelles de type « liste de diffusion » dans l'Annuaire national MSSanté (toute adresse MSSanté doit correspondre à une et une seule BAL physique).
	5.4.1	EX_PBA_5040	L'opérateur doit, par un moyen technique ou organisationnel, permettre à chacun des utilisateurs de son service d'indiquer explicitement : <ul style="list-style-type: none"> • S'il souhaite être inscrit en liste rouge ; • S'il souhaite la publication de son numéro de téléphone ; • Le cas échéant son acceptation de la dématérialisation (ce choix doit également être indiqué pour les BAL applicatives ou organisationnelles). Ces choix, non imposés par défaut, peuvent être mis en œuvre lors de la création de la BAL MSSanté via un mécanisme technique (case à cocher) ou organisationnel, et doivent pouvoir être modifiés à tout moment par l'utilisateur.

Fonctionnalité	§ DSFT	N° Exigence	Exigence
	5.4.1	EX_PBA_5050	L'opérateur doit mettre en œuvre les mécanismes techniques permettant de transmettre à l'Annuaire national MSSanté : <ul style="list-style-type: none"> • Les choix de l'utilisateur concernant : son inscription en liste rouge et son acceptation (ou pas) de la dématérialisation; • Le numéro de téléphone de l'utilisateur (le cas échéant).
	5.4.1	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 national MSSanté.
	5.4.1	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 national MSSanté soient fiables.
	5.4.1.1	EX_PBA_5090	L'identifiant du titulaire d'une BAL personnelle MSSanté transmis par l'opérateur lors de l'alimentation de l'Annuaire national MSSanté doit impérativement être l'identifiant national (RPPS/ADELI) si le titulaire de la BAL en dispose. Dans les autres cas, un identifiant interne (en pratique : l'adresse de la BAL MSSanté attribuée à l'utilisateur) à la structure d'activité pourra être transmis.
	5.4.1.1	EX_PBA_5100	L'Annuaire national MSSanté 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.
	5.4.1.1	EX_PBA_5220	Il est demandé à l'opérateur de rattacher explicitement les BAL personnelles au numéro FINESS (EJ ou EG) de la structure si celle-ci est immatriculée dans le Fichier National des Identifiants Sanitaires et Sociaux. Cette exigence a pour but d'améliorer la publication dans l'Annuaire national 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 n°FINESS n'y est rattaché).
	5.4.2	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 § 5.4.2 (et sous-chapitres).
	5.4.2.5	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.
	5.4.2.5	EX_1.1.1_5030	Afin de s'assurer de la bonne publication des BAL MSSanté dans l'Annuaire national MSSanté, les rapports d'alimentation doivent être téléchargés et les erreurs traitées après chaque alimentation.
	5.4.1	EX_PBA_5230	L'opérateur ne doit pas publier dans l'Annuaire Santé les boîtes aux lettres de tests.
Consultation Annuaire national	5.3.1	EX_WSA_5010	L'authentification mutuelle du Connecteur MSSanté avec le serveur d'Annuaire national MSSanté constitue un prérequis transverse à l'appel de tout Web Service d'interfaçage avec l'Annuaire national

Fonctionnalité	§ DSFT	N° Exigence	Exigence
MSSanté (transaction optionnelle)			MSSanté (ces fonctions sont définies dans les chapitres suivants de ce document).
	5.3.1	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).
	5.3.3.1	EX_WSA_5070	Les spécifications du § 5.3.3.1 concernant l'encodage et les espaces de nommage, pour les Web Services de l'Annuaire national MSSanté en REST, doivent être respectées.
	5.3.3.2	EX_WSA_5080	Les spécifications du § 5.3.3.2 concernant la sécurité et l'intégrité, pour les Web Services de l'Annuaire national MSSanté en REST, doivent être respectées.
	5.3.3.3.1	EX_WSA_5090	Les spécifications du § 5.3.3.3.1 (et sous-chapitres) concernant les échanges, pour les Web Services de l'Annuaire national MSSanté en REST, doivent être respectées.
	5.3.3.3.3	EX_WSA_5100	Les spécifications du § 5.3.3.3.3 (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'Annuaire national MSSanté en REST, doivent être respectées.
	5.5	EX_2.1_5010	L'opérateur MSSanté doit obligatoirement implémenter au moins une des deux solutions disponibles (TM2.1.1A ou TM2.1.3A) afin que les utilisateurs du système MSSanté puissent sélectionner de manière sûre et aisée les destinataires de leurs messages.
	5.5.1	EX_2.1.1_5010	La transaction « TM2.1.1.A - Interrogation de l'Annuaire national MSSanté 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 national MSSanté de manière automatisée.
	5.5.2	EX_2.1.3_5010	Dans le cas où l'opérateur implémente la transaction « TM2.1.3A - Téléchargement d'une extraction de l'Annuaire national MSSanté », il doit respecter les spécifications d'implémentation décrites dans le chapitre § 5.5.2 (et sous-chapitres associés).
	5.5.3	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 § 5.5.3 (et sous-chapitres associés).
Synchronisation temps	5.8.1	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	5.8.2	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 : <ul style="list-style-type: none"> • 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

Fonctionnalité	§ DSFT	N° Exigence	Exigence
			traitement aux dispositions législatives qui l'encadrent.
	5.8.2	EX_GDT_5020	Les utilisateurs et l'exploitant doivent être informés de la génération de traces de leurs actions par le service MSSanté.
	5.8.2	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.
	5.8.2	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.
	5.8.2	EX_GDT_5050	Pour les traces concernant l'envoi ou la réception d'un message, le champ « type d'action » inclut les informations suivantes : <ul style="list-style-type: none"> • 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.
	5.8.2	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.
	5.8.2	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. Des durées recommandées sont définies par la CNIL dans son autorisation unique (voir § 2.6). Le service de l'opérateur devra donc respecter ces durées.
Statistiques service MSSanté	5.8.3	EX_PSU_5010	L'opérateur MSSanté doit prévoir un dispositif capable d'enregistrer et de restituer des indicateurs de suivi de l'activité MSSanté.
	5.8.3	EX_PSU_5810	Les informations demandées portent sur le mois écoulé, du 1 ^{er} au dernier jour du mois (chiffres mensuels). Ces informations sont restituées sous forme de deux fichiers (avec un codage utf-8) : <ul style="list-style-type: none"> • (AAAAMM)_EchangesMSSante_[Domaine].csv • (AAAAMM)_ConnexionsMSSante_[Domaine].csv L'opérateur MSSanté doit déposer ces fichiers dans une archive .zip sur un serveur via un webservice de soumission. Les fichiers contenus dans les archives déposées seront parcourus, validés par

Fonctionnalité	§ DSFT	N° Exigence	Exigence
			<p>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.</p> <p>L'opérateur doit transmettre ces indicateurs à l'ASIP Santé <u>dans les cinq premiers jours du mois qui suit</u> via le webservice de soumission.</p>
	5.8.3	EX_PSU_5820	<p>L'opérateur doit exclure des indicateurs mensuels du mois N:</p> <ul style="list-style-type: none"> - les boites aux lettres suspendues au mois N-1 - les boites aux lettres supprimées au mois N-1 - les boites aux lettres de tests
	5.8.3	EX_SSU_5800	<p>Le fichier Connexion doit contenir l'ensemble des boites aux lettres créées par l'opérateur.</p> <ul style="list-style-type: none"> - 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
	5.8.3	EX_SSU_5810	<p>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</p>
	5.8.3	EX_SSU_5820	<p>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).</p>
	5.8.3	EX_SSU_5830	<p>Les opérateurs doivent continuer à produire les fichiers de statistiques décrits dans la version v1.2.1 du DSFT Opérateurs pendant au moins 6 mois et ce à partir de la date de publication du présent document. Ces fichiers doivent être envoyés par mail à l'adresse « monserviceclient.mssante@asipsante.fr ».</p>
Sécurité	5.8.5.2	EX_SSI_5010	<p>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 DSFT pouvant le nécessiter.</p>
	5.8.5.2	EX_SSI_5020	<p>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'ASIP Santé dans les plus brefs délais.</p>
	5.8.5.2	EX_SSI_5030	<p>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.</p> <p>Des audits de la sécurité du système de messageries MSSanté et de son environnement doivent être réalisés à intervalle régulier.</p>
	5.8.5.2	EX_SSI_5040	<p>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'ASIP Santé concernant les questions de sécurité du système.</p>
	5.8.5.2	EX_SSI_5050	<p>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.</p>

Fonctionnalité	§ DSFT	N° Exigence	Exigence
	5.8.5.2	EX_SSI_5060	Les locaux hébergeant les plateformes de production et de secours du SI doivent bénéficier d'un contrôle des accès physiques.
	5.8.5.2	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.
	5.8.5.2	EX_SSI_5080	La capacité du système mis en œuvre pour le service MSSanté doit être testée, suivie et anticipée.
	5.8.5.2	EX_SSI_5090	<p>Le système MSSanté doit mettre en œuvre des mécanismes de détection des intrusions.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Ainsi, lors de l'envoi ou de la réception d'un message contenant des pièces jointes infectées, le connecteur MSSanté peut au choix :</p> <p>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 ;</p> <p>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.</p>
	5.8.5.2	EX_SSI_5100	<p>Les serveurs de messagerie doivent s'authentifier mutuellement à l'aide d'un certificat logiciel de personne morale délivré par l'ASIP Santé.</p> <p>L'opérateur doit suivre les recommandations de sécurité issues des Conditions Générales d'Utilisation (CGU) des produits de certification de l'ASIP Santé à destination des établissements de santé. Celles-ci sont les suivantes (Ch 4.1 des CGU – Mesures de sécurité) : « L'Abonné garantit, via sa 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'ASIP Santé. Il devra notamment veiller à limiter l'accès à ces clés privées à des personnes dûment autorisées et qu'elles ne puissent pas être dupliquées ni installées dans de multiples équipements. ».</p> <p>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.</p>
	5.8.5.2	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.
	5.8.5.2	EX_SSI_5120	Le service de messagerie doit bénéficier d'un service de supervision configuré pour générer des alertes automatisées sur des

Fonctionnalité	§ DSFT	N° Exigence	Exigence
			<p>événements spécifiés et jugés critiques pour la sécurité du service (disponibilité, intégrité, confidentialité et auditabilité).</p> <p>Les exigences concernant les traces sont définies dans le § 5.8.2.</p>
	5.8.5.2	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.
	5.8.5.2	EX_SSI_5140	Les pare-feux protégeant l'infrastructure du SI doivent bénéficier des mécanismes de protection conformes à l'état de l'art.
	5.8.5.2	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).
	5.8.5.2	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.
	5.8.5.2	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.
	5.8.5.3	EX_SSI_5180	<p>Comme indiqué dans le contrat « opérateur MSSanté » [CONTRAT-MSSANTE], les opérateurs MSSanté intégrés de façon validés ont l'obligation de signaler à l'ASIP Santé en tant que gestionnaire de l'espace de confiance « [...] toute modification, tout dysfonctionnement ou toute anomalie sur leur service de messagerie sécurisée 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.».</p> <p>De même, ils doivent informer l'ASIP Santé de tout arrêt temporaire supérieur à 8 jours.</p> <p>Les canaux dédiés pour ces déclarations d'incidents sont :</p> <ul style="list-style-type: none"> ➤ l'adresse mail : monserviceclient.mssante@asipsante.fr ➤ le numéro de téléphone : 0 825 852 000 (Service à 0,06 € / min + prix appel, 24/24 Heures - 7/7 Jours).
Définition des CGU à mettre en œuvre par l'opérateur	5.8.4	EX_DCU_5010	<p>L'opérateur MSSanté doit définir des conditions générales d'utilisation (ou équivalent) pour le service de messagerie MSSanté qu'il met en œuvre.</p> <p>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) :</p> <p><u>Rappel du contexte juridique :</u></p> <ul style="list-style-type: none"> • Règles de droit commun relatives à l'échange des données de santé à caractère personnel dont les dispositions de l'article L 1110-4 du code de la santé publique qui précisent les conditions d'échange de données de santé entre deux ou plusieurs professionnels; • 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 ; • Information 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

Fonctionnalité	§ DSFT	N° Exigence	Exigence
			<p>226-13 du Code pénal.</p> <p><u>Bon usage de la MSSanté :</u></p> <ul style="list-style-type: none"> • Information de l'utilisateur sur les finalités de la MSSanté et les conditions d'utilisation de ses données à caractère personnel ; • Seuls les professionnels habilités à échanger des données de santé personnelles peuvent utiliser le service MSSanté ; • Le service MSSanté permet l'émission de messages contenant des informations utiles à la prise en charge sanitaire d'une personne, à destination d'un ou plusieurs titulaires d'un compte de messagerie sécurisée de l'espace de confiance MSSanté ; • L'utilisateur s'engage à ne pas procéder à l'envoi de messages non sollicités à un ou plusieurs destinataires, considéré comme du spam ; • L'utilisateur s'interdit 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 ; • L'utilisateur s'engage à ne pas rediriger son adresse sécurisée vers une adresse de messagerie non MSSanté. <p><u>Publication dans l'Annuaire national MSSanté :</u></p> <ul style="list-style-type: none"> • L'opérateur doit annoncer dans ses CGU l'existence de dispositifs permettant à tout utilisateur de son service d'indiquer (et de modifier à tout moment) : <ul style="list-style-type: none"> ○ s'il souhaite être inscrit en liste rouge ; ○ s'il souhaite la publication de son numéro de téléphone ; ○ le cas échéant son acceptation de la dématérialisation. • L'opérateur doit également prévoir un moyen permettant à tout utilisateur de son service d'être informé que ses données liées à l'usage du système MSSanté sont publiées dans l'Annuaire national MSSanté et consultables par les autres utilisateurs (sauf en cas d'inscription en liste rouge). <p><u>Information du patient :</u></p> <ul style="list-style-type: none"> • En cas d'opposition du patient à l'utilisation du service MSSanté pour échanger des données de santé le concernant, l'utilisateur devra recourir à un moyen d'échange alternatif (courrier papier par exemple) ; • 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. • L'utilisateur 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. <p><u>Collecte des données de l'utilisateur</u></p> <ul style="list-style-type: none"> • <u>Des données (adresse e-mail, horodatage des échanges, taille des e-mails) sont collectées et transmises à l'ASIP Santé afin de lui permettre, en tant que gestionnaire de l'espace de confiance MSSanté, 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. Les données sont conservées 3 mois, puis anonymisées. 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,</u>

Fonctionnalité	§ DSFT	N° Exigence	Exigence
			<p><u>de limitation, et du droit de définir des directives sur le sort de ses données après sa mort. L'utilisateur peut, sous réserve de la production d'un justificatif d'identité valide, exercer ses droits sur demande écrite au GIP ASIP Santé (Délégué à la protection des données), 9 rue Georges Pitard, 75015 PARIS ou par messagerie électronique, à l'adresse suivante : dpo.asipsante@sante.gouv.fr. L'utilisateur dispose également d'un droit d'introduire une réclamation auprès de la CNIL.</u></p> <p>Valeur probante :</p> <ul style="list-style-type: none"> Afin de prévenir d'éventuelles contestations sur la valeur probante des messages (ou « écrits électroniques ») échangés entre les utilisateurs via le service MSSanté au regard des exigences fixées par la loi 2000-230, l'opérateur MSSanté doit prévoir, dans ses CGU, une clause par laquelle ses utilisateurs s'engagent, en les acceptant, à ne pas contester la force probante des messages sur le fondement de leur nature électronique, et à s'accorder pour reconnaître la même valeur probante aux écrits électroniques transmis via la 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 au sens de l'article 1316-2 du Code civil.
	5.8.4	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.

Tableau 48 : Liste des exigences applicables aux opérateurs MSSanté

7 Différences avec les précédentes versions

Le tableau suivant référence les différences entre deux versions successives du DSFT MSSanté. Il s'agit ici de la liste des **différences majeures avec la version 1.3 du 14/11/2019**.

La version **v1.3.1** du DSFT opérateur est une **version mineure n'impliquant pas le réengagement** (envoi d'une Annexe 2 - Engagement de conformité) de la part des opérateurs.

La version **v1.3** du DSFT opérateur est une **version majeure** impliquant le réengagement (envoi d'une Annexe 2 - Engagement de conformité) de la part des opérateurs.

Paragraphe DSFT v1.3.1	Page	Changement
4.5	55 à 56	Le chapitre 4.5 concernant la suspension des BAL ne comporte dorénavant que des recommandations. Les trois exigences précédemment publiées dans la v1.3 du DSFT MSSanté ont été réévaluées en recommandations. La recommandation RE_GBM_4430 a été ajoutée.
5.8.3	145	Précision apportée à l'exigence EX_SSU_5800 concernant la valeur à renseigner pour la date de dernière connexion d'une BAL en cas d'indisponibilité de l'information.
5.8.3	145	Ajout d'une recommandation concernant le renseignement de la date de dernière connexion pour les BAL applicatives.
Annexe	DR4	Modification de l'ordre des colonnes Date et Taille: <ul style="list-style-type: none">- Inversion des colonnes Date et Taille dans le fichier exemple « Echanges ». L'ordre des colonnes dans ce fichier, publié dans la version 1.3, était erroné et non conforme aux spécifications. Le fichier modifié se trouve dans l'archive ZIP <i>MSS_OPE_TEC_DSFT_v1.3.1_Annexe_DR4_Statistiques_20200311</i>. L'ordre des colonnes dans le DSFT (paragraphe \$5.8.3) est correct et est celui à implémenter. Il n'y a pas eu de modification apportée dans les spécifications.

Tableau 49 : Historique des modifications

8 Annexes

8.1 Le service Mailiz de l'opérateur ASIP Santé

Comme indiqué au §2.4.1, l'ASIP Santé en plus de son rôle de gestionnaire de l'espace de confiance est un opérateur de l'espace de confiance MSSanté et propose un service de messagerie Mailiz pour les professionnels habilités, pour le compte des Ordres professionnels.

L'opérateur ASIP Santé met à disposition de ses utilisateurs plusieurs modes d'accès à sa messagerie sécurisée Mailiz:

- le webmail Mailiz : <https://mailiz.mssante.fr> ;
- l'application mobile MSSanté téléchargeable sur l'Apple Store (iOS) ou Google Play (Android).
- des interfaces destinées aux clients de messagerie intégrés à des logiciels de professionnel de santé (voir DST des interfaces clients de messagerie / opérateurs MSSanté [\[DST-MSSANTE\]](#)).

Sur son service de messagerie sécurisée Mailiz, l'opérateur ASIP Santé propose des boîtes aux lettres nominatives (de 2 Go max, message de 16 Mo max pouvant contenir 10 Mo max de pièces jointes) pour les professionnels de santé porteurs de CPS (Carte de Professionnel de Santé) uniquement. Le service Mailiz de l'opérateur ASIP Santé propose l'autocréation de BAL MSSanté personnelles par les professionnels de santé disposant d'une carte CPS mais ne permet pas à ces PS de procéder à la création de boîtes aux lettres organisationnelles ou applicatives (se reporter au §4.1 du présent DSFT).

8.2 Détail du processus d'intégration à l'espace de confiance d'un opérateur MSSanté

8.2.1 Le contrat « opérateur MSSanté » et ses annexes

Comme indiqué dans le §2.5 «Intégration des opérateurs à l'espace de confiance MSSanté», pour proposer un service de messagerie sécurisée de santé raccordé à l'espace de confiance, un opérateur doit avoir conclu le contrat « opérateur MSSanté » [\[CONTRAT-MSSANTE\]](#) avec l'ASIP Santé (gestionnaire de l'espace de confiance) qui définit les conditions d'intégration de l'opérateur à l'espace de confiance MSSanté.

Les deux annexes du contrat « opérateur MSSanté » sont :

- **Annexe 1 – Déclaration d'un domaine MSSanté** : cette annexe permet à l'opérateur MSSanté de renseigner les informations techniques nécessaires à son entrée dans l'espace de confiance et d'indiquer le nom de domaine de messagerie qu'il souhaite utiliser. Cette annexe signée est à renvoyer en même temps que le contrat « opérateur MSSanté ». Pour rappel, comme indiqué au paragraphe 2.7 : L'usage commun d'une terminaison « [mssante.fr](#) » par tous les acteurs de l'espace de confiance 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. Toutefois, les opérateurs sont libres de proposer des services de messagerie sécurisée sans utiliser le nom de domaine « [mssante.fr](#) ».

Remarque :

L'ASIP Santé applique pour l'enregistrement des noms de domaines des opérateurs MSSanté dans la liste blanche, la même règle que celle de la Charte de nommage de l'AFNIC : « premier arrivé – premier servi ». Le demandeur (opérateur MSSanté) doit veiller à ce que le nom de domaine dont il sollicite l'enregistrement respecte les droits de propriété intellectuelle des tiers. Cela est notifié dans l'annexe 1 du contrat « opérateur MSSanté » : l'opérateur s'engage « à réaliser les demandes de référencement et de retrait de domaines de bonne foi et 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'ASIP Santé en tant que gestionnaire de l'espace de confiance se réserve le droit de refuser l'enregistrement d'un nom de domaine dans la liste blanche si celui-ci est susceptible de porter atteinte à l'ordre public ou aux bonnes mœurs ou à des droits de propriété intellectuelle.

L'ASIP Santé ne réalise pas de contrôle à proprement parlé pour l'enregistrement des noms de domaine. En cas de contentieux, la personne s'estimant lésée devra rapporter la preuve de sa légitimité à utiliser le nom de domaine en lieu et place de l'autre utilisateur.

- **Annexe 2 – Engagement de conformité MSSanté** : Déclaration de conformité de l'opérateur MSSanté aux exigences de l'espace de confiance MSSanté. En renvoyant cette annexe complète et conforme, l'opérateur déclare être conforme à l'ensemble des exigences de la version du DSFT Opérateurs de messagerie en vigueur au moment de la conclusion du contrat et respecter les dispositions de la loi Informatique et Libertés (et le cas échéant celles relatives à l'hébergement de données de santé caractère personnel).

8.2.2 L'intégration en deux temps d'un opérateur à l'espace de confiance MSSanté

L'intégration de l'opérateur à l'espace de confiance s'effectue en deux temps. Le premier, désigné « **intégration provisoire** », consiste pour l'opérateur à tester et évaluer son service de messagerie sécurisée de santé et le second, appelé « **intégration validée** », reconnaît la capacité pour l'opérateur de proposer un service de messagerie sécurisée de santé à des utilisateurs finaux.

Remarque :

Afin d'être en mesure d'obtenir le certificat serveur SSL qui authentifiera l'opérateur dans l'espace de confiance MSSanté, la procédure d'intégration à l'espace de confiance MSSanté nécessite en outre que :

- l'opérateur ait signé avec l'ASIP Santé un contrat permettant l'obtention de « produits de certification ». Si l'opérateur n'en dispose pas déjà, il est souhaitable d'initier cette démarche dès que possible, en parallèle de la signature du contrat « opérateur MSSanté ».
- 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) soit équipé d'une carte de la famille CPS à jour. L'administrateur technique est la seule personne de confiance de la structure et habilitée à pouvoir générer un certificat serveur et sera en charge des opérations techniques.

Les documents nécessaires pour réaliser cette démarche sont disponibles à l'adresse suivante : <https://esante.gouv.fr/securite/cartes-et-certificats/commandes>, sur l'onglet « Vos commandes ».

8.2.3 Temps 1 – Intégration provisoire

1) L'opérateur envoie son pack opérateur dûment complété, signé et paraphé composé des éléments suivants à l'adresse indiquée sur le contrat « opérateur MSSanté ».

- ✓ **Contrat « opérateur MSSanté »** [\[CONTRAT-MSSANTE\]](#) : *il doit être **paraphé à chaque page et signé en dernière page**. La signature doit être précédée du **nom et prénom du signataire** et accompagné du **cachet de la structure**. Le contrat doit être adressé en **2 exemplaires originaux** par courrier postal à l'adresse indiquée.*
- ✓ **Annexe 1- Déclaration d'un domaine MSSanté** [\[CONTRAT-MSSANTE\]](#) : *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 en **1 exemplaire original** par courrier postal.*
- ✓ **Formulaire de commande de certificat logiciel n°413 – Déclaration des habilitations**
Ce formulaire permet à l'opérateur d'habiliter la CPA d'un administrateur technique de son choix afin de générer le certificat serveur utilisé par le connecteur pour s'authentifier auprès des autres opérateurs. Ce certificat est émis par l'autorité de certification IGC Santé de l'ASIP Santé (sur la branche Elémentaire domaine Organisations). Ce certificat est de type certificat logiciel SERVEUR, usage SSL_SERVEUR. *Il doit être **signé**. La signature doit être précédée du **nom et prénom du signataire** et accompagné du **cachet de la structure**. Il doit être adressé en **1 exemplaire original** par courrier postal.*

Afin de bénéficier d'un accompagnement pour le remplissage du pack opérateur (contrat « opérateur MSSanté » et ses annexes, formulaire de commande de certificat serveur SSL) nous conseillons aux Industriels et aux GRADeS qui souhaitent s'orienter vers une solution d'opérateur MSSanté de prendre contact dans un premier temps avec l'équipe MSSanté via la BAL : monserviceclient.mssante@asipsante.fr (voir §8.5 Canaux de contact).

Les Etablissements de Santé, quant à eux, sont invités à se rendre sur la plateforme de formation en ligne : <https://esante-formation.fr/> où ils trouveront un kit d'accompagnement MSSanté de dix modules qui les guidera dans la mise en place et l'usage de MSSanté au sein de leur structure.

- 2) L'opérateur est intégré provisoirement dans l'espace de confiance MSSanté (en production)

L'opérateur est donc ajouté dans la liste blanche (fichier tenu à jour par l'ASIP Santé) qui contient un enregistrement de l'ensemble des domaines de messagerie des opérateurs autorisés à échanger dans l'espace de confiance.

L'ASIP Santé lui ouvre également les droits pour la génération de son certificat serveur SSL.

- 3) L'opérateur MSSanté est alors en mesure de tester son service et d'évaluer qu'il est en conformité avec l'ensemble des exigences techniques du DSFT Opérateurs de messagerie.

L'opérateur réalise ses tests dans l'espace de confiance **en production**, il est donc tenu durant sa période d'intégration provisoire de respecter certaines règles :

- ✓ interdiction d'émettre des emails contenant des données de santé à caractère personnel ;
- ✓ les échanges sont réalisés exclusivement entre boîtes aux lettres de tests à des seules fins de tests (interdiction d'échanger avec la boîte aux lettres d'un utilisateur final par exemple).
- ✓ créer un nombre limité de boîtes aux lettres (BAL) de test : vingt-cinq (25) maximum. Le nom de la BAL de test doit permettre d'identifier la BAL comme telle (exemple : test1@nomdomaine.mssante.fr).

Outils mis à la disposition de l'opérateur MSSanté pour faciliter ses tests
--

Durant la période d'intégration provisoire, les tests d'échange de mail se font :

1/ Soit dans l'espace de confiance MSSanté de production selon les conditions détaillées dans le contrat « opérateur MSSanté ».

- i. **Le document « Conseils pour une recette réussie des solutions techniques pour rejoindre MSSanté »** est mis à disposition des opérateurs MSSanté (et des éditeurs de Connecteurs MSSanté au besoin) pour les aider dans l'élaboration de leur plan de tests permettant de vérifier la conformité de leur service aux exigences fonctionnelles et techniques du DSFT Opérateurs de messagerie.

Remarque : Ce document de conseil est communiqué par mail aux chefs de projet et aux responsables techniques (identifiés dans l'Annexe 1) des opérateurs lors de leur intégration provisoire à l'espace de confiance MSSanté.

- ii. **Boîtes aux lettres de tests :**
 - a. Un opérateur doit être en capacité de supporter les chaines de certification de l'IGC-CPS et de l'IGC-Santé (voir exigence EX_OPE_5030).
 - b. Deux boîtes aux lettres de tests présentant chacune une des deux IGC sont mises à dispositions des opérateurs sur le domaine de tests de l'opérateur ASIP Santé. Elles sont configurées comme un répondeur automatique et répondent à chaque mail qu'elles reçoivent avec un message prédéfini. Elles permettent donc aux opérateurs de tester de façon autonome leur raccordement à l'espace de confiance et donc leur capacité à envoyer un mail sécurisé et à en recevoir.
 - c. Se reporter au document « **Conseils pour une recette réussie des solutions techniques pour rejoindre MSSanté** » pour plus d'information sur leur usage.

2/ Soit dans l'espace de confiance MSSanté de tests.

Uniquement les opérateurs ayant fait les démarches pour intégrer l'espace de confiance de tests peuvent réaliser leurs tests d'échanges dans cet environnement. Les échanges se basent alors sur une liste blanche de tests. La description de l'espace de confiance de tests et les modalités d'accès sont décrites au §8.4 « L'espace de confiance MSSanté de tests »

- Concernant la mise au point des interfaces avec l'Annuaire national MSSanté, un **Annuaire national MSSanté de tests** est disponible pour aider les opérateurs à mettre au point leur solution technique. Les modalités d'accès à cet annuaire sont décrites au §8.3.2 « L'Annuaire national MSSanté de tests (dit « partenaires ») » du présent DSFT.

8.2.4 Temps 2 – Intégration validée

Dès lors que l'opérateur a pu s'assurer qu'il respecte :

- l'ensemble des exigences du DSFT,
- les recommandations de la CNIL indiquées dans son autorisation unique n°37, le cas échéant,
- les dispositions relatives à l'hébergement de données de santé prévu par l'article L.1111-8 du code de la santé publique, le cas échéant,

Il déclare à l'ASIP Santé qu'il est en conformité.

Pour rappel, se reporter au §2.6.

- 1) Comme indiqué dans le contrat « opérateur MSSanté », l'opérateur MSSanté dispose d'une période de 6 mois (qui peut être renouvelée une fois pour une durée similaire, après accord des deux parties) pour adresser l'élément conditionnant son intégration validée à l'espace de confiance MSSanté :

- ✓ son **Annexe 2-Engagement de conformité MSSanté [CONTRAT-MSSANTE]** : Elle doit être **dument complétée** (avec l'ensemble des cases obligatoire à cocher renseignées), **paraphée et signée**. La signature doit être précédée du **nom et prénom du signataire** et accompagnée du **cachet de la structure**. Elle doit être adressée en **1 exemplaire original** par courrier postal à l'adresse indiquée dans l'Annexe 2.

- 2) Lorsqu'un engagement de conformité, conforme et complet lui est adressé dans les délais précités, l'ASIP Santé notifie par courrier recommandé à l'opérateur son intégration validée à l'espace de confiance. L'opérateur est alors en capacité de proposer un service de messagerie sécurisée de santé à des utilisateurs finaux.

Remarque : La liste des domaines de l'opérateur MSSanté est alors renseignée sur le site <https://www.mssante.fr>.

- 3) Comme indiqué au §5.8.3 « Production et soumission de statistiques d'utilisation », l'opérateur MSSanté doit renvoyer ses indicateurs de suivi d'activité MSSanté.

Remarque : L'opérateur MSSanté peut à tout moment choisir d'ajouter ou de supprimer un nom de domaine de messagerie en renvoyant une nouvelle Annexe 1 au contrat « opérateur MSSanté » à l'adresse indiquée dans l'Annexe 1.

8.3 Les environnements Annuaire national MSSanté

8.3.1 L'Annuaire national MSSanté 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 national MSSanté	WSCRALIMENTATIONMSS	https://ws.annuaire.mssante.fr/webservices/V1011/CR/WSCRALIMENTATIONMSS
TM2.1.1A	Consultation de l'Annuaire national MSSanté par le protocole LDAP		Nom DNS de l'Annuaire national MSSanté : ldap.annuaire.sante.fr URL d'accès : ldap://ldap.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 national MSSanté	extractionMSSante	https://ws.annuaire.mssante.fr/webservices/V1011/extractionMSSante?format=xml
TM2.1.4A	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 national MSSanté certifiés par l'IGC Santé

Autorité de certification

L'Annuaire national MSSanté 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>

8.3.2 L'Annuaire national MSSanté de tests (dit « partenaires »)

L'ASIP Santé met à disposition des opérateurs un Annuaire national MSSanté 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 national MSSanté de tests se font à 11h, 15h et la nuit (entre 2h et 4h comme pour l'Annuaire national MSSanté de production).

8.3.2.1 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/web/services/V1011/Alimentation/WSALIMENTATIONMSS?wsdl
TM1.1.1P	WS de récupération du compte-rendu d'alimentation dans l'Annuaire national MSSanté	WSCRALIMENTATIONMSS	https://ws.partenaires.annuaire.sante.fr/web/services/V1011/CR/WSCRALIMENTATIONMSS?wsdl
TM2.1.1A	Consultation de l'Annuaire national MSSanté par le protocole LDAP		Nom DNS de l'Annuaire national MSSanté : 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 national MSSanté	extractionMSSante	https://ws.partenaires.annuaire.sante.fr/web/services/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/web/services/V1011/extractionIdentitePS?format=csv

Tableau 51 : URL des services de l'Annuaire national MSSanté de tests certifiés par l'IGC-Santé

8.3.2.2 L'interface LDAP de l'Annuaire national MSSanté de tests (dit "partenaires")

Les comptes de messagerie sont disponibles dans les extractions LDAP de l'Annuaire national MSSanté de tests le jour qui suit leur création.

8.3.2.3 Autorité de certification de l'Annuaire national MSSanté de tests (dit "partenaires")

L'Annuaire national MSSanté 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/>

Point d'attention : La recherche de professionnels de santé par LDAP ne retourne pas toujours le même résultat qu'une recherche dans le webmail Mailiz de l'opérateur ASIP Santé. Dans l'environnement de tests, les professionnels de santé migrés RPPS qui ont une carte CPS avec un numéro ADELI (et non un numéro RPPS) ne sont pas retournés dans le résultat d'une recherche LDAP alors qu'ils seront retournés dans le résultat d'une recherche dans le webmail.

Une évolution du SI MSSanté est programmée pour uniformiser le résultat des recherches.

Remarque : L'attribut « l » qui contient la ville (attribut non obligatoire) n'est pas présent dans l'Annuaire national MSSanté de tests (car celui-ci est basé sur les cartes CPS de tests qui ne contiennent pas cet attribut).

8.3.2.4 Modalités d'accès à l'Annuaire National MSSanté de tests (dit "partenaires")

Cet Annuaire national MSSanté de tests / partenaires contient un jeu d'identités de tests qui correspondent aux cartes CPS de tests. La commande d'un certificat serveur SSL de tests est indispensable pour accéder à l'Annuaire national MSSanté de tests. Le formulaire de commande d'un certificat serveur de tests est disponible à l'adresse suivante : <https://esante.gouv.fr/securite/cartes-et-certificats/commandes> , télécharger « Formulaire 414 de commande de produits de certification de test.pdf » en bas de page. Ce formulaire permet également de commander des cartes CPS de tests pour les tests d'alimentation de l'Annuaire national MSSanté de tests.

L'ASIP Santé maintient à jour une liste blanche de tests (fichier XML signé par l'ASIP Santé) contenant l'ensemble des domaines de tests autorisés à accéder à l'Annuaire national MSSanté de tests.

Pour pouvoir accéder aux Web Services exposés par l'Annuaire national MSSanté de tests, les domaines de tests des éditeurs de connecteurs MSSanté et des opérateurs MSSanté doivent être intégrés à cette liste blanche de tests.

Pour se faire, les éléments suivant doivent être transmis aux canaux de contacts décrits au paragraphe 8.5 Canaux de contact :

- le nom de vos domaines de messagerie de tests
- le DN de votre certificat serveur SSL de tests
- les coordonnées du responsable technique (nom, prénom, tél, mail)
- les coordonnées du chef de projet (si différentes du responsable technique)

8.4 Espace de confiance MSSanté de tests

L'espace de confiance MSSanté de tests est un environnement mis à disposition des opérateurs par l'ASIP Santé 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 MSSanté de production (liste blanche de tests, Annuaire national MSSanté de tests, opérateurs de test etc.) mais ne met pas en œuvre de données de santé à caractère personnel.

Les finalités de cet espace de confiance de test sont multiples :

- proposer à tout nouvel opérateur un moyen de tester son bon fonctionnement vis-à-vis de la liste blanche, de l'annuaire national et d'autres opérateurs 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 les interfaces DST de tester leur implémentation sur différents opérateurs présentant ces interfaces DST,
- Permettre à des éditeurs et opérateurs de réaliser de tests de bout en bout dans le cadre de mise en œuvre de projets communs.

Cet environnement permettra aussi de tester des échanges de message entre opérateurs afin de s'assurer de la bonne interopérabilité des opérateurs.

NB : Il est interdit d'intégrer un environnement de production d'un opérateur à l'espace de confiance MSSanté de tests.

8.4.1 Description des composants de l'espace de confiance de test

8.4.1.1 Liste blanche de tests

L'url de la liste blanche de tests est publique et accessible à l'adresse suivante :

<https://espacedecon fiance.test.mssante.fr/listeblanchemssante.xml>

L'opérateur doit pouvoir gérer un certificat IGC Santé de tests que présente le serveur.

La liste blanche de tests est différente de la liste blanche « unifiée » qui permettait à certains opérateurs de réaliser leurs tests d'interfaçage avec l'Annuaire national MSSanté de tests (dit partenaires). Elle la remplace. Les domaines déclarés dans la liste blanche « unifiée » devront faire l'objet d'une demande explicite pour être déclarés dans la liste blanche de tests.

8.4.1.2 Annuaire national MSSanté de tests

L'opérateur doit pouvoir gérer le certificat IGC Santé de tests que présente l'Annuaire national MSSanté de tests (dit partenaires).

Cet annuaire contient les identités de tests associées à toutes les cartes CPx de tests 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 tests 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 §8.3.2.

8.4.1.3 Boîte aux lettres de réponse automatique de tests

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 SMTPS uniquement après validation d'un certificat serveur X509 délivré par l'ASIP Santé 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).

Le certificat serveur présenté par les acteurs techniques de l'échange est émis par l'ASIP Santé, de type IGC Santé de tests.

Chaque opérateur intégrant l'espace de confiance MSSanté de tests, et souhaitant réaliser des échanges au sein de cet espace de confiance doit disposer d'une BAL de réponse automatique de tests. Cette BAL permet de faire des échanges inter-opérateurs sans solliciter les équipes d'exploitation et est affichée dans la liste blanche de tests, dans le champ <description>.

Cette BAL de réponse automatique doit être déclarée sur un nom de domaine de tests dédié. Elle n'a pas vocation à recevoir des messages automatiques de type sonde.

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, preproduction, 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.

8.4.1.4 Webservice de production et soumission de statistiques d'utilisation

L'espace de confiance MSSanté de tests offre aux opérateurs, intégrés dans la liste blanche de tests, la possibilité de soumettre des fichiers de statistiques d'utilisation via des webservices à l'instar de ceux de production décrits dans le paragraphe §5.8.3.

Ci-dessous les URL permettant d'accéder aux webservices de soumission de statistiques dans l'espace de confiance MSSanté de tests.

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

8.4.2 Modalités d'accès à l'espace de confiance MSSanté de tests

8.4.2.1 Les prérequis

Afin de pouvoir accéder à l'espace de confiance de tests, l'opérateur doit vérifier les conditions suivantes :

- 1- Avoir signé un contrat de produits de certification de tests* permettant à l'opérateur de disposer d'un certificat serveur IGC Santé de test
(Pour connaître la démarche, se référer à l'adresse suivante : <https://esante.gouv.fr/securite/cartes-et-certificats/produits-de-developpement>)
- 2- Avoir signé un contrat Opérateur MSSanté avec l'ASIP Santé
- 3- Avoir un **environnement de tests opérateur dédié** ouvert sur internet. Celui-ci doit permettre les échanges SMTP avec les autres opérateurs, mais doit aussi permettre à des éditeurs de LPS qui en feraient la demande d'accéder aux interfaces client de messagerie (webmail, WS, ...) de l'opérateur de test.
- 4- Avoir configuré une BAL de réponse automatique de tests

8.4.2.2 La démarche

Pour intégrer l'espace de confiance de tests, l'opérateur doit envoyer un mail à l'adresse « monserviceclient.mssante@asipsante.fr » en précisant :

- Dans l'objet du mail : le nom de l'opérateur et la demande.
Exemple [*Nom_Opérateur*] Demande d'intégration à l'espace de confiance MSSanté de tests
- Dans le corps du mail :
 - i. Le nom du domaine à inscrire dans la liste blanche de tests
 - ii. Le nom du domaine de tests sur lequel sera définie la BAL automatique de tests
 - iii. Le DN du certificat logiciel de tests associé aux noms de domaines dans la liste blanche.
 - iv. La configuration de la zone DNS (un seul choix possible)
 - Méthode 1 – la délégation : indiquer dans ce cas le nom des serveurs (primaire et secondaire) de l'opérateur
 - Méthode 2 – la redirection : indiquer dans ce cas le nom du serveur de messagerie pour MSSanté de l'opérateur
 - v. Le nom, prénom et coordonnées du chef de projet
 - vi. Le nom, prénom et coordonnées du responsable technique
 - vii. L'adresse de la BAL de réponse automatique de test

Une fois l'inscription en liste blanche et la configuration de la zone DNS réalisées, un mail de confirmation est envoyé à l'opérateur pour l'informer de sa bonne intégration à l'espace de confiance MSSanté de tests.

Pour toute question, assistance technique ou signalement d'incidents sur l'espace de confiance MSSanté de tests, les canaux de contacts sont ceux mentionnés au paragraphe :

§8.5 Canaux de contact. Lors de la prise de contact, l'opérateur doit mentionner clairement l'objet de la demande et l'espace de confiance MSSanté concerné, dans ce cas celui de tests.

8.5 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'ASIP Santé (Annuaire national MSSanté, liste blanche, référentiels MSSanté...), signalements d'incidents, envoi des indicateurs de suivi d'activité, demandes d'accès à l'Annuaire national MSSanté de tests...) des opérateurs MSSanté, deux canaux de contact sont disponibles :

- Email : monserviceclient.mssante@asipsante.fr,
- Téléphone : 0 825 852 000 (Service à 0,06 € / min + prix appel, 24/24 Heures - 7/7 Jours).

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.

8.6 Documents externes

8.6.1 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 ».

N°	Référence	Document
Documents du Cadre d'interopérabilité des Systèmes d'Information de Santé (CI-SIS) (Documents accessibles sur le site de l'ASIP Santé https://esante.gouv.fr/interoperabilite/ci-sis/)		
DA1	[CI-CHAP]	Document Chapeau du CI-SIS
DA2	[CI-ECH-DOC]	Volet ECHANGE DE DOCUMENTS DE SANTE
DA3	[CI-TR-CLI-LRD]	Couche TRANSPORT VOLET SYNCHRONE
DA4	[CI-STRU-ENTETE]	Couche Contenu Volet Structuration Minimale de Documents Médicaux
Nomenclature des Acteurs de Santé (Documents accessibles sur le site de l'ASIP Santé https://esante.gouv.fr/interoperabilite/mos-nos)		
DA5	[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'ASIP Santé https://esante.gouv.fr/secure/pgssi-s/espace-de-publication)		
DA6	[PG-PR-FOND]	Principes fondateurs – Juillet 2013 – V1.0
DA7	[PG-IDENT]	Référentiel d'identification des acteurs sanitaires et médico-sociaux – Décembre 2014 – v1.0
DA8	[PG-AUTH]	Référentiel d'authentification des acteurs de santé– Décembre 2014 - V2.0
DA9	[PG-IMPUT]	Référentiel d'imputabilité– Décembre 2014 – V1.0
DA10	[PG-GR-APPLI]	Grille d'applicabilité des référentiels de la PGSSI-S– Mai 2015 – V1.0
DA11	[PG-RG-INT]	Règles pour les interventions à distance sur les systèmes d'information de santé – Décembre 2014 – V1.0
Autres documents (Documents accessibles sur le site: https://mssante.fr/is/doc-technique)		
DA12	[DST-MSSANTE]	Dossier des Spécifications Techniques des Interfaces d'accès au système de Messageries Sécurisées de Santé (MSSanté) Clients de messagerie
DA13	[CONTRAT-MSSANTE]	Contrat «opérateur MSSanté » et ses deux annexes

Tableau 52 : Liste des documents applicables

8.6.2 Documents de référence pour les services

Documents de référence accessibles sur le site de l'ASIP Santé : https://mssante.fr/is/doc-technique	
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 national MSSanté et du Web Service de récupération du compte rendu d'alimentation associé
DR3	Annuaire : schémas (XSD) pour les transactions : d'alimentation de l'Annuaire national MSSanté et de téléchargement d'une extraction de l'Annuaire national MSSanté
DR4	Statistiques MSSanté : exemples de fichiers à transmettre à l'ASIP Santé : <ul style="list-style-type: none">- 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

Tableau 53 : Liste des documents de référence pour les services

8.6.3 Requests For Comments (RFC)

La liste suivante présente les principales RFC liées à l'usage de la messagerie :

- MSS-ANX-CRL1 : INTERNET X.509 PUBLIC KEY INFRASTRUCTURE – CERTIFICATE AND CERTIFICATE REVOCATION LIST (CRL) PROFILE
- MSS-ANX-SMTPS: SMTP SERVICE EXTENSION FOR – SECURE SMTP OVER TRANSPORT LAYER SECURITY
- MSS-ANX-IMAPS: USING TLS WITH IMAP, POP3 AND ACAP
- MSS-SMTP1 : SIMPLE MAIL TRANSFER PROTOCOL
- MSS-SMTP2: SMTP SERVICE EXTENSION FOR RETURNING ENHANCED ERROR CODES
- MSS-ANX-SMTPS: SMTP SERVICE EXTENSION FOR SECURE SMTP OVER TRANSPORT LAYER SECURITY
- MSS-ANX-TLS1: USING TLS WITH IMAP, POP3 AND ACAP
- MSS-ANX-TLS2: THE TLS PROTOCOL VERSION 1
- MSS-ANX-LDAP1: LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP): TECHNICAL SPECIFICATION ROAD MAP
- MSS-ANX-LDAP2: LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP): THE PROTOCOL
- MSS-ANX-LDAP3: LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP): DIRECTORY INFORMATION MODELS
- MSS-ANX-LDAP4: LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP): AUTHENTICATION METHODS AND SECURITY MECHANISMS
- MSS-ANX-IMAP : INTERNET MESSAGE ACCESS PROTOCOL – VERSION 4REV1
- MSS-ANX-DKIM1: ANALYSIS OF THREATS MOTIVATING DOMAINKEYS IDENTIFIED MAIL (DKIM)
- MSS-ANX-DKIM2: DOMAINKEYS IDENTIFIED MAIL (DKIM) SIGNATURES
- MSS-ANX-DKIM3: DOMAINKEYS IDENTIFIED MAIL (DKIM) SIGNATURES
- MSS-ANX-MAIL: APPLICATION TECHNIQUES FOR CHECKING AND TRANSFORMATION OF NAMES
- MSS-ANX-MIME1: MULTIPURPOSE INTERNET MAIL EXTENSIONS (MIME) PART ONE: FORMAT OF INTERNET MESSAGE BODIES
- MSS-ANX-MIME2: MULTIPURPOSE INTERNET MAIL EXTENSIONS (MIME) PART TWO: MEDIA TYPES
- MSS-ANX-MIME3: MIME (MULTIPURPOSE INTERNET MAIL EXTENSIONS) PART THREE: MESSAGE HEADER EXTENSIONS FOR NON-ASCII TEXT
- MSS-ANX-MIME4: MEDIA TYPE SPECIFICATIONS AND REGISTRATION PROCEDURES
- MSS-ANX-MIME5: MULTIPURPOSE INTERNET MAIL EXTENSIONS (MIME) PART FOUR: REGISTRATION PROCEDURES
- MSS-ANX-MIME6: THE MODEL PRIMARY CONTENT TYPE FOR MULTIPURPOSE INTERNET MAIL EXTENSIONS
- MSS-ANX-MIME7: MULTIPURPOSE INTERNET MAIL EXTENSION (MIME) PART FIVE: CONFORMANCE CRITERIA AND EXAMPLES
- MSS-ANX-MAIL2: STANDARD FOR ARPA INTERNET TEXT MESSAGES
- MSS-ANX-MAIL3 : INTERNET MESSAGE FORMAT
- MSS-ANX-MAIL4: MAIL ROUTING AND THE DOMAIN SYSTEM
- MSS-ANX-MAIL5 : CLASSLESS IN-ADDR.ARPA DELEGATION

8.6.4 Annexes externes

Documentation IETF (spécification internationale en libre accès sur http://www.ietf.org/)		
DX1	MSS-ANX-CRL1	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile http://tools.ietf.org/html/rfc5280
DX2	MSS-SMTP1	Simple Mail Transfer Protocol http://tools.ietf.org/html/rfc5321
DX3	MSS-SMTP2	SMTP Service Extension for Returning Enhanced Error Codes http://tools.ietf.org/html/rfc2034
DX4	MSS-ANX-SMTPS	SMTP Service Extension for Secure SMTP over Transport Layer Security http://www.ietf.org/rfc/rfc3207.txt
DX5	MSS-ANX-TLS1	Using TLS with IMAP, POP3 and ACAP http://www.ietf.org/rfc/rfc2595.txt
DX6	MSS-ANX-TLS2	The TLS Protocol Version 1.0 http://tools.ietf.org/html/rfc2246
DX7	MSS-ANX-LDAP1	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map http://tools.ietf.org/html/rfc4510
DX8	MSS-ANX-LDAP2	Lightweight Directory Access Protocol (LDAP): The Protocol http://tools.ietf.org/html/rfc4511
DX9	MSS-ANX-LDAP3	Lightweight Directory Access Protocol (LDAP): Directory Information Models http://tools.ietf.org/html/rfc4512
DX10	MSS-ANX-LDAP4	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms http://tools.ietf.org/html/rfc4513
DX11	MSS-ANX-IMAP	Internet Message Access Protocol – Version 4rev1 http://tools.ietf.org/html/rfc3501
DX12	MSS-ANX-DKIM1	Analysis of Threats Motivating DomainKeys Identified Mail (DKIM) http://tools.ietf.org/html/rfc4686
DX13	MSS-ANX-DKIM2	DomainKeys Identified Mail (DKIM) Signatures http://tools.ietf.org/html/rfc4871
DX14	MSS-ANX-DKIM3	DomainKeys Identified Mail (DKIM) Signatures http://tools.ietf.org/html/rfc6376
DX15	MSS-ANX-MAIL	Application Techniques for Checking and Transformation of Names http://tools.ietf.org/html/rfc3696
DX16	MSS-ANX-MIME1	Multipurpose Internet Mail Extensions (MIME) Part One : Format of Internet Message Bodies

Documentation IETF (spécification internationale en libre accès sur http://www.ietf.org/)		
		http://tools.ietf.org/html/rfc2045
DX17	MSS-ANX-MIME2	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types http://tools.ietf.org/html/rfc2046
DX18	MSS-ANX-MIME3	MIME (Multipurpose Internet Mail Extensions) Part Three : Message Header Extensions for Non-ASCII Text http://tools.ietf.org/html/rfc2047
DX19	MSS-ANX-MIME4	Media Type Specifications and Registration Procedures http://tools.ietf.org/html/rfc4288
DX20	MSS-ANX-MIME5	Multipurpose Internet Mail Extensions (MIME) Part Four : Registration Procedures http://tools.ietf.org/html/rfc4289
DX21	MSS-ANX-MIME6	The Model Primary Content Type for Multipurpose Internet Mail Extensions http://tools.ietf.org/html/rfc2077
DX22	MSS-ANX- MIME7	Multipurpose Internet Mail Extension (MIME) Part Five : Conformance Criteria and Examples http://tools.ietf.org/html/rfc2049
DX23	MSS-ANX-MAIL2	Standard for ARPA Internet Text Messages http://www.w3.org/Protocols/rfc822
DX24	MSS-ANX-OCSP	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP http://tools.ietf.org/html/rfc2560
DX25	MSS-ANX-MAIL3	Internet Message Format http://tools.ietf.org/html/rfc2822
DX26	MSS-ANX-MAIL4	MAIL ROUTING AND THE DOMAIN SYSTEM http://tools.ietf.org/html/rfc974
DX27	MSS-ANX-MAIL5	Classless IN-ADDR.ARPA delegation http://tools.ietf.org/html/rfc2317
DX28	MSS-ANX-MAIL6	Enhanced Mail System Status Codes https://tools.ietf.org/html/rfc3463

Tableau 54 : Liste des annexes externes IETF

8.6.5 Bonnes pratiques complémentaires

Documentation ANSSI	
DX28	Sécurisation des serveurs DNS http://www.cert.ssi.gouv.fr/site/CERTA-2008-INF-002/
DX29	Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaines http://www.ssi.gouv.fr/uploads/2014/05/guide_dns_ansi_1.2.pdf
DX30	Guide d'hygiène informatique http://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/

Tableau 55 : Documentation ANSSI

8.7 Terminologie, acronymes et abréviations

8.7.1 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
ANSSI	Agence Nationale pour la Sécurité des Systèmes d'Information
ASIP	Agence des Systèmes d'Information Partagés (cf. ASIP Santé)
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'ASIP Santé
CGU	Conditions Générales d'Utilisation
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 Soins Sans Consentement
ESB	Enterprise Service Bus
FAQ	Foire Aux Questions
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
LFSS	Loi de Financement de la Sécurité Sociale
LGC	Logiciel de Gestion de Cabinet
LPS	Logiciel de Professionnel de Santé (abréviation générique désignant une application utilisée par un professionnel de santé, dans ou hors Etablissement de Santé)
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)

Abréviations	Signification
NAS	Nomenclature des Acteurs de Santé
NDR	Non-Delivery Report
OCSP	Online Certificate Status Protocol
ODI	Outil de Diagnostic d'Installation
OTP	One Time Password
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
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 de Santé
SAML	Security Assertion Markup Language
SI	Système d'Information
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
VIHF	Vecteur d'Identification et d'Habilitation Formelles
WSDL	Web Services Description Language

Tableau 56 : Liste des acronymes et de leur signification

8.7.2 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 57 : Légendes et abréviations utilisées dans les descriptions des attributs et règles

8.7.3 Définition des orientations technologiques retenues pour MSSanté

Les orientations technologiques retenues, parmi les principaux protocoles standards ou interfaces d'échanges utilisés, pour la mise en place de la Messagerie Sécurisée de Santé sont les suivantes :

- **SMTP** (Simple Mail Transfer Protocol) : permet l'envoi d'un message et sa réception sur un serveur destinataire par des connexions point à point ;
- **IMAP4** (Internet Message Access Protocol version 4) : permet de gérer plusieurs accès simultanés à une même BAL, de gérer plusieurs dossiers associés à une BAL ou de réaliser des tris sur les messages reçus selon différents critères ;
- **MIME⁵** (Multipurpose Internet Mail Extensions) : étend les possibilités du SMTP en permettant de joindre à des messages des documents variés (pièce-jointe), de taille non bornée, d'utiliser différents jeux de caractères ;
- **TLS** (Transport Layer Security) : assure la confidentialité et l'intégrité des flux échangés entre deux composants ;
- **LDAP** (Lightweight Directory Access Protocol) : protocole standard permettant d'accéder et de gérer des annuaires ;
- **DNS** (Domain Name Server) : permet de traduire un nom de domaine en informations de plusieurs types qui lui sont associées, notamment en adresses IP de la machine portant ce nom (le champ MX – MX record ou *mail exchange record* – définit les serveurs de courriel associés à un nom de domaine) ;
- **DSML** (Directory Service Markup Language) : qui permet de disposer d'une représentation du contenu d'un annuaire LDAP, en utilisant le format XML ;
- **LDIF** (LDAP Data Interchange Format) : format standardisé d'échange de données, qui permet la représentation des données contenues dans un annuaire LDAP ;
- **Web Services** : ensemble de fonctionnalités exposées par des machines ne nécessitant pas d'intervention humaine, et fonctionnant de manière synchrone ou asynchrone ;
- **SOAP** (Simple Object Access Protocol) ;
- **REST** (Representational State Transfer) ;
- **SAML** (Security Assertion Markup Language) : Standard de mise en œuvre de l'authentification retenu pour les Web Services de messagerie.

⁵ Les messages électroniques sont envoyés via le protocole SMTP au format MIME. Ce standard étend le format des données des messages électroniques pour supporter notamment des textes en différents codage de caractères autre que celui de l'ASCII, ainsi que des contenus non textuels (pièces-jointes). Les messages électroniques sont souvent appelés messages SMTP/MIME (infra ou supra désigné par SMTP).

8.8 Codes d'erreurs

8.8.1 Codes d'erreurs pour les Web Services de l'Annuaire national MSSanté 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 national MSSanté 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 IssuedInstant) est obligatoire dans le jeton VIHF
WSMSS04	La date d'émission de l'assertion SAML (attribut IssuedInstant) 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 58 : 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 national MSSanté 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) ou ORG (Organisationnelle)
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 », 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 : FINESSE 2 : SIREN 3 : SIRET Toute autre type d'identifiant est rejeté.
RG_CTR_031	Vérification pour tout enregistrement que l'attribut « Dematerialisation » est renseigné
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 59 : Liste des contrôles liés à la vérification du schéma XML dans le cas du code WSMSS12

8.8.2 Codes d'erreurs pour les Web Services de l'Annuaire national MSSanté 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 national MSSanté en REST :

Statut	Code	Description
400	Bad Request	La requête n'est pas valide (paramètres manquants/incorrecs, body manquant/incorrec, ...)
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 60 : Liste des messages d'erreurs pour la couche technique des Web Services en REST

8.8.3 Codes d'erreurs pour la TM1.1.xP - Mise à jour des comptes de messagerie dans l'Annuaire national MSSanté

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 national MSSanté 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 », qu'une valeur est présente pour l'attribut « TypIdentifiantPP »	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 », 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 (« TypIdentifiantPP » = « 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 (« typIdentifiantPP » = « 10 »), qu'une valeur est présente pour l'attribut « TypIdentifiantPM »	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 (« typIdentifiantPP » = « 10 »), que la valeur envoyée pour l'attribut « TypIdentifiantPM » 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 « TypIdentifiantPM »	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 « TypIdentifiantPM » 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 (« typIdentifiantPP » = « 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 est présente pour l'attribut « IdentifiantPM »	MSS013	L'identifiant de la structure d'activité est obligatoire pour les BAL MSSanté de type Organisationnelle ou	Bloquante

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
			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
RG_CTR_017	Vérification, pour l'enregistrement d'une de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typidentifiantPP »= « 10 »), que la valeur envoyée pour l'attribut « CivilitéExercice » 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 (« typidentifiantPP »= « 10 »), que la valeur envoyée pour l'attribut « CivilitéExercice » 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 national MSSanté 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 national MSSanté.	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 national MSSanté	Warning
RG_CTR_022	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national	MSS021	La catégorie de profession est obligatoire pour la BAL d'un professionnel de	Bloquante

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
	(« typIdentifiantPP »= « 10 »), que l'attribut « CategorieProfessions» est renseigné		santé avec identifiant interne	
RG_CTR_023	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typIdentifiantPP »= « 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 (« typIdentifiantPP »= « 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 (« typIdentifiantPP »= « 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 (« typIdentifiantPP »= « 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 (« typIdentifiantPP »= « 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 (« typIdentifiantPP »= « 10 »), que l'attribut « Spécialité » transmis est autorisé pour la Profession envoyée	MSS027	Cette spécialité n'est pas autorisée pour la profession indiquée	Bloquante
RG_CTR_029	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP », que l'attribut « Responsable » est renseigné	MSS028	Le responsable est obligatoire pour une BAL de type Applicative ou Organisationnelle	Bloquante
RG_CTR_030	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP », que l'attribut « Description » est renseigné	MSS029	La description est obligatoire pour une BAL de type Applicative ou	Bloquante

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
			Organisationnelle	
RG_CTR_033	Vérification que si la valeur de « TypIdentifiantPM » 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 « TypIdentifiantPP » = « 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 (« typIdentifiantPP » = « 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 « TypIdentifiantPP » = « 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 « TypIdentifiantPP » 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 (« typIdentifiantPP » = « 10 »), que la valeur envoyée pour l'attribut « TypIdentifiantPM » 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 « TypIdentifiantPM » 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_040	Vérification, pour l'enregistrement d'une de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typIdentifiantPP » = « 10 »), que la valeur envoyée pour l'attribut	MSS038	La valeur de la civilité d'exercice est fermée dans la nomenclature utilisée	Warning

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
	« CivileExercice » correspond à un code ouvert de la nomenclature Civilité d'exercice			
RG_CTR_041	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typIdentifiantPP » = « 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 (« typIdentifiantPP » = « 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 (« typIdentifiantPP » = « 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 (« TypIdentifiantPP » = « 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 (« typIdentifiantPP » = « 10 ») et catégorie de profession "professionnel social" (code = "06), qu'une valeur est présente pour l'attribut « IdentifiantPM »	MSS045	L'identifiant de la structure d'activité est recommandé pour les adresses de BAL MSSanté d'un professionnel social	Warning
RG_CTR_048	Vérification, pour l'enregistrement avec un identifiant structure facultatif (BAL de type PER avec identifiant interne (« typIdentifiantPP » = « 10 ») et catégorie de profession "professionnel social" (code = "06), que l'identifiant transmis « IdentifiantPM » est référencé dans la table des sites ou des entités	MSS046	L'identifiant de la structure d'activité transmise n'existe pas dans le référentiel des identités PP/PM	Warning

Identifiant contrôle	Contrôle appliqué	Code erreur	Message d'erreur affiché *	Criticité **
	juridiques (M_SITE : NO_FINESS_ET ou NO_SIRET, M_ENT_JUR : NO_FINESS ou NO_SIREN)			
RG_CTR_049	Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP avec identifiant national RPPS (« typIdentifiantPP » = « 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 61 : 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'ASIP Santé.

(**) La criticité est fournie à titre d'information et peut-être modifiée à l'initiative de l'ASIP Santé sur le serveur de l'Annuaire national MSSanté :

- 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 national MSSanté, 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 national MSSanté) 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.

8.8.4 Codes d'erreurs pour la soumission des fichiers indicateurs

8.8.4.1 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 62 : codes retours lors de l'authentification aux webservice de soumission de fichiers statistiques

8.8.4.2 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 la taille de 10 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)
100	Une erreur technique est survenue	

Tableau 63 : Codes retours lors du dépôt des fichiers statistiques

8.8.4.3 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 trouvée pour l'identifiant fourni
100	Une erreur technique est survenue	

Tableau 64 : Codes retours de la récupération du compte rendu

8.8.4.4 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 65 : Codes retours des contrôles sur les fichiers « Echanges » et « Connexions »

8.8.4.4.1 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 DSFT 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 DSFT
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
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 ;

			<ul style="list-style-type: none"> • 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 66 : Contrôles appliqués au fichier « Echanges »

8.8.4.4.2 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 DSFT 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 DSFT
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
10	Bloquant	Contrôle de la période	La période déclarée doit être celle du mois précédent le traitement. <ul style="list-style-type: none"> • 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 67 : Contrôles appliqués au fichier « Connexions »

8.9 Éléments nécessaires à la réalisation d'une analyse de risque

8.9.1 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 illimitées⁶	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

Figure 34 : Types de sources de menaces

⁶ Organisation criminelle, agence gouvernementale ou organisation sous le contrôle d'un État étranger, espions, organisation terroriste (EBIOS 2010).

8.9.2 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.



Pour en savoir plus
www.mssante.fr



Principes, exigences et interfaces opérateurs du Système de Messageries Sécurisées de Santé (MSSanté)