PROJETS / SERVICES

# Interfaces d'accès au système

# de Messageries Sécurisées de Santé (MSSanté)

Dossier des Spécifications Fonctionnelles et Techniques - **V1.0.0** - Mars 2014

*Opérateurs de messagerie*

| **Identification du document** | |
|---|---|
| Référence ASIP Santé | **MSS_FON_DSFT_Opérateurs_MSSanté_v1_0_0.PDF** |
| Date de dernière mise à jour | **19/03/2014** |
| Classification | **Non sensible public** |
| Nombre de pages | **155** |

| **Historique du document** | | |
|---|---|---|
| Version | Date | Commentaires |
| V0.0.x | 2013 | Versions de travail successives du document |
| V0.9.0 | 06/05/2013 | Version de travail soumise pour avis aux acteurs de terrain |
| V0.9.1 à V0.9.4 | 05/09/2013 | Versions de travail du DSFT MSSanté opérateurs de messagerie |
| V0.9.5 | 12/09/2013 | Version diffusée du DSFT opérateurs de messagerie |
| V1.0.0 | 19/03/2014 | Version diffusée du DSFT opérateurs de messagerie |

# Sommaire

# 1 Introduction

## 1.1 Objet du document

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

Ce document propose donc de :

- Rappeler le contexte du système de Messageries Sécurisées de Santé au regard des missions et projets de l'ASIP Santé ;
- Exposer les principes généraux du système MSSanté ;
- Décrire le processus organisationnel de mise en œuvre de l'intégration des opérateurs de messagerie à l'espace de confiance MSSanté ;
- Présenter les technologies et protocoles à mettre en œuvre ainsi que les compétences normatives et techniques à maîtriser par les équipes de développement ;
- Définir les spécifications des interfaces pour un service intégré à l'espace de confiance MSSanté ;
- Exposer des exemples d'implémentations de Messageries Sécurisées de Santé afin de fournir des axes de réflexion sur les types de déploiement envisageables ;
- Préciser les modalités d'accès et les types d'interfaces clients éligibles.

## 1.2 Guide de lecture

Ce document est destiné principalement aux décideurs et aux profils techniques des opérateurs de messagerie candidats à l'intégration à l'espace de confiance MSSanté. Selon son profil, le lecteur pourra se concentrer sur certains chapitres spécifiques :

Profil 1 - Décideurs :

Chapitres 2 et 3

Profil 2 - Directeurs techniques, chefs de projets :

Chapitres 2 à 5

Profil 3 - Développeurs, architectes logiciels, consultants techniques :

Chapitres 4 à 7

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

- Les chapitres 2 et 3 retracent le contexte de la MSSanté en général et des interfaces associées ;
- Le chapitre 4 traite du profil Opérateur MSSanté ;
- Le chapitre 5 présente une synthèse des exigences référencées dans ce document ;
- Le chapitre 6 répertorie l'historique des changements entre versions de ce document ;
- Le chapitre 7 regroupe les annexes.

L'annexe « Terminologie, acronymes » au **§ 7.2** référence et définit l'ensemble des acronymes utilisés dans ce document.

## 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.

Certains chapitres portent la marque **[AC]** signifiant qu'ils restent « à compléter » et peuvent faire l'objet d'ajustements.

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 prises en comptes des nouvelles versions du DSFT sont précisées dans le contrat d'intégration à l'espace de confiance « contrat opérateur MSSanté » 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 en s'abonnant à la liste de diffusion MSSanté : msscompatibilite@sante.gouv.fr.

# 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 donnés de santé tout en garantissant aux patients la qualité de la relation soignant/patient qui nécessite de garantir la confidentialité de leurs données de santé.

Des projets de messageries nationales, régionales ou locales, se sont 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.

Les professionnels de santé échangent donc les données de santé traditionnellement par courrier et téléphone, ou via des services de messagerie non sécurisée.

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 de Messageries Sécurisées de Santé (MSSanté) est réalisée en concertation avec les industriels et les organisations représentatives des professionnels de santé.

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 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.

Le service MSSanté est donc destiné à l'ensemble des professionnels susvisés.

**Par convention, le présent DSFT utilise la notion de « professionnel habilité » pour désigner les professionnels de santé et tout professionnel habilité par la loi à collecter et échanger des données de santé à caractère personnel.**

## 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 le « système MSSanté »**

Afin que les professionnels adhèrent à l'utilisation de messageries sécurisées de santé, leur développement doit répondre aux principes suivants :

- Universalité : tous les professionnels habilités, quels que soient leurs modes d'exercice, doivent être en capacité de disposer d'un compte de messagerie sécurisée permettant d'échanger avec tous les professionnels habilités, quels que soient les outils utilisés ;
- Simplicité : l'émission et la consultation des messages sécurisées ne modifient pas les pratiques habituelles des 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 permet :

- D'échanger par voie électronique de façon sécurisée des données de santé à caractère personnel entre professionnels habilités (messagerie inter-professionnelle) ;
- D'alimenter des systèmes d'information (SI) de l'espace de confiance, par exemple à l'occasion d'échanges de messages entre acteurs de santé (messagerie inter-applicative).

Le système MSSanté repose sur un « espace de confiance » qui se caractérise par :

- Un 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 ;
- Un référentiel permettant aux industriels de développer des offres conformes et interopérables entre elles.

## 2.3 Un système de Messageries Sécurisées de Santé respectueux du cadre légal

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 de la loi 78-17 du 6 janvier 1978 modifiées, relative à l'informatique, aux fichiers et aux libertés, dite loi « informatique et libertés ».

Cette loi énumère de façon limitative les cas dans lesquels il est autorisé de traiter des données de santé à caractère personnel (article 8) et impose la réalisation de formalités préalables par le responsable de traitement. Ainsi, tout service de messageries sécurisées de santé doit être autorisé par la Commission Nationale de l'Informatique et des Libertés (CNIL) (cf.infra « focus sur les formalités préalables à accomplir par le responsable de traitement »).

Indépendamment des formalités préalables que doit accomplir chaque responsable d'un traitement de messageries sécurisées de santé, l'ASIP Santé a déposé auprès de la CNIL un dossier de demande d'autorisation pour la mise en œuvre et l'organisation **du système MSSanté** et la fourniture d'un service de messagerie sécurisée de santé de base.

La CNIL a autorisé par sa délibération du 25 avril 2013 (n° 2013-096) la mise en œuvre par l'ASIP Santé du système MSSanté.

En outre, 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 et d'utiliser un moyen d'authentification forte pour l'accès aux données de santé (carte de professionnel de santé ou tout autre dispositif équivalent).

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 et du décret 2006-6 du 4 janvier 2006 relatives à l'hébergement de données de santé à caractère personnel (articles R.1111-9 et suivants du code de la santé publique).

Selon les cas, l'hébergement des données de santé échangées via le service de messagerie sécurisée de santé peut être réalisé **par l'opérateur lui-même ou par un prestataire tiers choisi par l'opérateur.**

En tout état de cause, pour pouvoir héberger un service de messageries sécurisées de santé, **l'hébergeur (opérateur ou prestataire de l'opérateur)** doit être titulaire d'un **agrément** couvrant une telle prestation :

- Soit l'hébergeur est agréé pour l'hébergement d'applications de types messagerie sécurisées de santé et prévoit l'obligation pour le professionnel habilité d'utiliser un moyen d'authentification forte par carte CPS ou tout autre dispositif équivalent pour accéder aux données de santé ;
- Soit l'hébergeur est agréé pour une prestation dite « générique » lui permettant d'héberger des applications contenant des données de santé à caractère personnel et prévoit l'obligation pour le professionnel habilité d'utiliser un moyen d'authentification forte par carte CPS ou tout autre dispositif équivalent pour accéder aux données de santé.

Cet agrément n'est pas requis lorsqu'un opérateur-établissement de santé héberge par ses propres moyens le service de messagerie sécurisée de santé utilisé par les personnes qu'il emploie.

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.

Il convient de rappeler que l'ASIP Santé est chargée d'élaborer la politique générale de sécurité des systèmes d'information de santé (PGSSI-S), en concertation avec les acteurs du monde de la santé concernés, qui doit s'appliquer à tout système d'information de santé dont les services de messagerie sécurisée de santé.

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 incombe.

# 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 d'intégration à l'espace de confiance appelé « contrat opérateur MSSanté» conclu entre l'ASIP Santé et tout opérateur souhaitant intégrer l'espace de confiance MSSanté.
- **Opérateur d'un service sur le domaine pro.mssante.fr et 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.

## 2.4.2 Les opérateurs de messageries sécurisées de santé

Les opérateurs de messageries sécurisées de santé sont toute 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.

L'ASIP Santé est un des opérateurs de l'espace de confiance.

Pour proposer un service de messageries sécurisées de santé raccordé à l'espace de confiance, l'opérateur doit avoir conclu le « contrat opérateur MSSanté » avec l'ASIP Santé, qui a pour objet de déterminer 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.

L'opérateur est tenu d'assurer la sécurité des données échangées via le service MSSanté qu'il propose et doit à cet effet respecter les articles L.1111-8 et R.1111-9 et suivants du code de la santé publique relatives à l'hébergement de données de santé. Lorsque l'hébergement des données de santé requiert l'agrément défini aux articles précités, l'opérateur peut lui-même héberger les données de santé et être titulaire de cet agrément ou recourir à un hébergeur tiers agréé.

La sécurité du service de messagerie mis en œuvre par l'opérateur repose sur des fonctions de sécurité du Proxy Opérateur MSSanté (ou Proxy de messagerie MSSanté) 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.

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 habilités, quel que soit leur mode d'exercice.

Des boîtes aux lettres organisationnelles ou applicatives (rattachées par exemple à des « services » ou « pôles » au sein de structures de soins) peuvent être créées. Leurs modalités de création sont définies au point **§ 4.4** « Publication de BAL MSSanté dans l'annuaire national MSSanté » du présent DSFT. Leur utilisation est en tout état de cause réalisée sous le contrôle et la responsabilité d'un professionnel habilité.

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

***Détermination des formalités préalables à accomplir***

Les traitements de services de messagerie sécurisée de santé poursuivent un intérêt public et relèvent des dispositions des articles 8-IV et 25-I de la loi du 6 janvier 1978 modifiée. Tout service de messagerie sécurisé de santé doit donc faire l'objet d'une demande d'autorisation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) par le responsable du traitement.

Toutefois, pour les traitements de messageries sécurisées de santé raccordés à l'espace de confiance MSSanté proposés par les opérateurs, la CNIL a mis en place un régime d'autorisation unique. Chaque responsable de traitement doit simplement adresser à la CNIL un engagement de conformité à l'autorisation unique, à condition de respecter toutes les exigences fixées par cette autorisation unique.

***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.

#### *2.4.4.1 Cas pratiques*

##### 2.4.4.1.1 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 des formalités préalables à réaliser auprès de la CNIL pour 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[1].

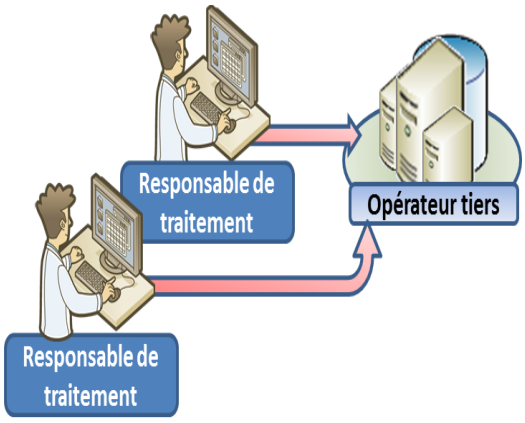


**Figure 1 : PS libéral utilisant le service MSSanté proposé par un opérateur « tiers »**

[1] Dans le cadre du service MSSanté qu'elle propose, l'ASIP Santé est, à titre expérimental, le responsable de ce traitement. Les professionnels de santé ne sont donc pas tenus de réaliser de formalités préalables auprès de la CNIL. Cette répartition des responsabilités entre l'ASIP Santé et les utilisateurs finaux de ce service a été reconnue par la CNIL, en raison du rôle de l'agence en tant qu'opérateur national offrant un service minimal, gratuit et nécessaire à l'amorçage du projet MSSanté.

#### 2.4.4.1.2 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 un service de messagerie sécurisée de santé

**Le service de messagerie sécurisée de santé est développé et fourni par un tiers (industriel, GCS, etc.)**

Dans ce cas,

- **La structure est** :
  - Le responsable du traitement de messagerie sécurisée de santé ;
  - En charge des formalités préalables à réaliser auprès de la CNIL pour le service MSSanté.
- **La structure n'est pas** :
  - Opérateur.

Le tiers dont la structure utilise le service est l'opérateur et est considéré comme un « sous-traitant » au sens de la loi Informatique et libertés.

Cet opérateur doit permettre à la structure de s'assurer du respect du cadre juridique de l'échange de données de santé.

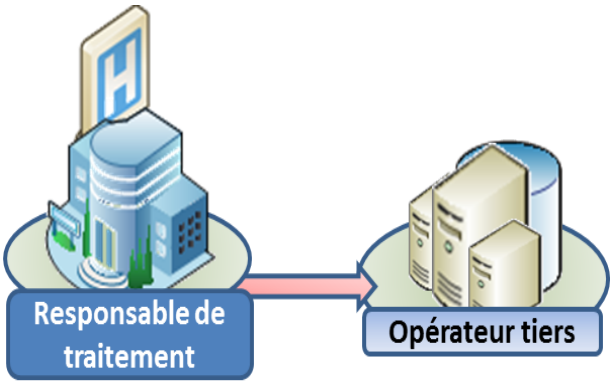


**Figure 2 : Structure utilisant le service MSSanté proposé par un opérateur « tiers »**

**La structure décide de développer son propre service de messagerie sécurisée de santé**

Dans ce cas, **la structure est** :

- Le responsable du traitement de messagerie sécurisée de santé ;
- En charge des formalités préalables à réaliser auprès de la CNIL pour le service MSSanté ;
- Opérateur.

La structure conclut le « contrat opérateur MSSanté » et doit garantir à ses utilisateurs le respect du cadre juridique de l'échange de données de santé.

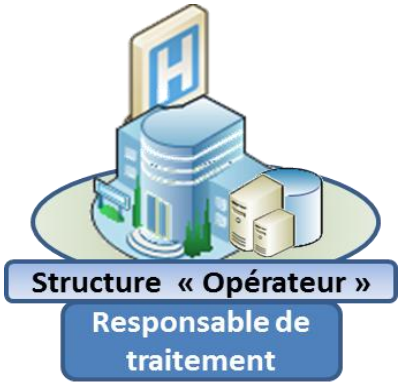


**Figure 3 : Structure utilisant son propre service MSSanté en tant qu'opérateur**

## 2.5 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 ou le destinaire du message fait 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.) publics ou privés 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 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) ;
- Les Ordres professionnels peuvent proposer des boîtes aux lettres sur le modèle xxx@profession.mssante.fr par exemple ;
- L'ASIP Santé propose un service aux professionnels habilités qui le souhaitent sous la forme d'une adresse 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 le nom de domaine « mssante.fr » dont l'ASIP Santé est titulaire.

L'ASIP Santé fournit à l'opérateur qui utilise des certificats avec un domaine rattaché à « mssante.fr » pour ses interfaces clientes d'accès aux BAL (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 à msscompatibilite@sante.gouv.fr.

# 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 « traditionnel » d'émission et de réception de messages électroniques. 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 peuvent être perdus mais qu'ils ne peuvent pas 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 accompagnés ou non de documents (pièce-jointes) entre des domaines de messagerie dédiés spécifiquement à la MSSanté.

## 3.1 Domaine MSSanté et groupe autorisé de domaines

### 3.1.1 Le concept de domaine MSSanté et de liste 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 BAL.

Les échanges de messages ne sont autorisés qu'entre les domaines de messagerie MSSanté répertoriés au sein d'une « liste blanche ». La MSSanté se présente comme une « liste de domaines autorisés de messageries ». Cette 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.

Le schéma ci-dessous illustre le principe des échanges entre les différents types d'opérateurs appartenant à l'espace de confiance MSSanté :

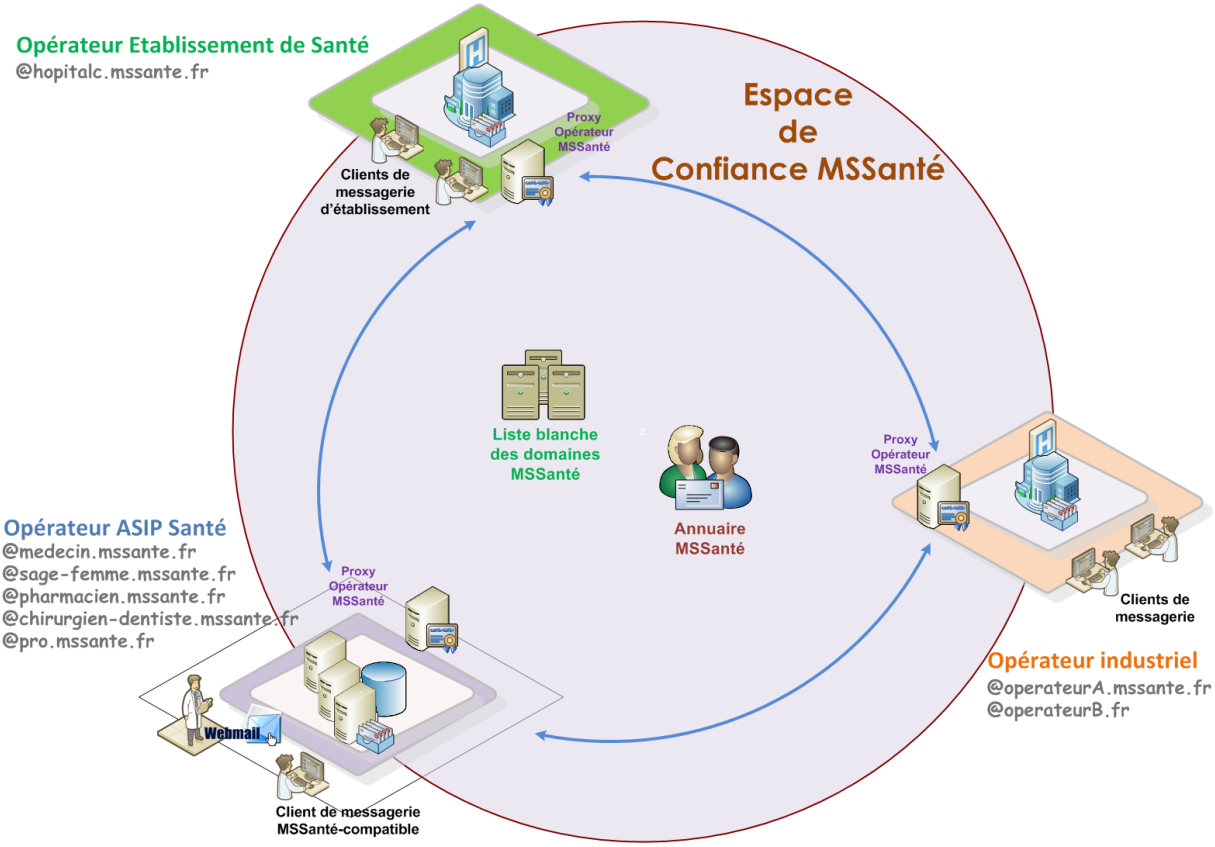


Figure 4 : Echanges au sein du système MSSanté

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 « Proxy Opérateur MSSanté » afin de pouvoir se raccorder techniquement à l'espace de confiance MSSanté.

En outre, ils doivent le cas échéant obtenir l'agrément pour l'hébergement de données de santé[2] ou faire appel à un prestataire agréé à cet effet.

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.**

[2] Rappel : si l'opérateur de messagerie n'est pas un Etablissement de Santé opérant la messagerie pour son propre compte, il est soumis à l'agrément Hébergeur de données de santé.

## 3.2 La boîte aux lettres MSSanté

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

- 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 et @etablissementB-securise.fr ;
- Une boîte aux lettres sur le domaine hébergé par un opérateur du domaine concurrentiel, du type @domaineY.mssante.fr.

Ces différentes adresses seront référencées dans l'annuaire national MSSanté pour cet utilisateur.

## 3.3 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 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 **§ 4.4** « Publication de BAL MSSanté dans l'annuaire national MSSanté » et **§ 4.5.1** « TM2.1.1A et TM2.1.2A - 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 Proxy d'annuaire local leur permettant d'appliquer leur propre niveau de disponibilité. |

# 3.4 Proxy Opérateur MSSanté

Le Proxy Opérateur MSSanté (ou Proxy de messagerie MSSanté) doit être vu comme un relais de messagerie permettant de prendre en charge les échanges de messages entre opérateurs au sein de l'espace de confiance.

Un Proxy Opérateur MSSanté communique uniquement avec un autre Proxy Opérateur MSSanté.

Le Proxy Opérateur MSSanté permet de contrôler l'identité de l'opérateur qui fournit le service de messagerie, de l'expéditeur et du destinataire d'un message. Lors de l'émission d'un message, le contrôle de l'appartenance de l'adresse du destinataire à un domaine de messagerie de la liste blanche est assuré. En cas de contrôle négatif, un avis de non envoi doit être retourné à l'expéditeur.

***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 Proxys Opérateur MSSanté présentent des certificats d'authentification émis par l'ASIP Santé).

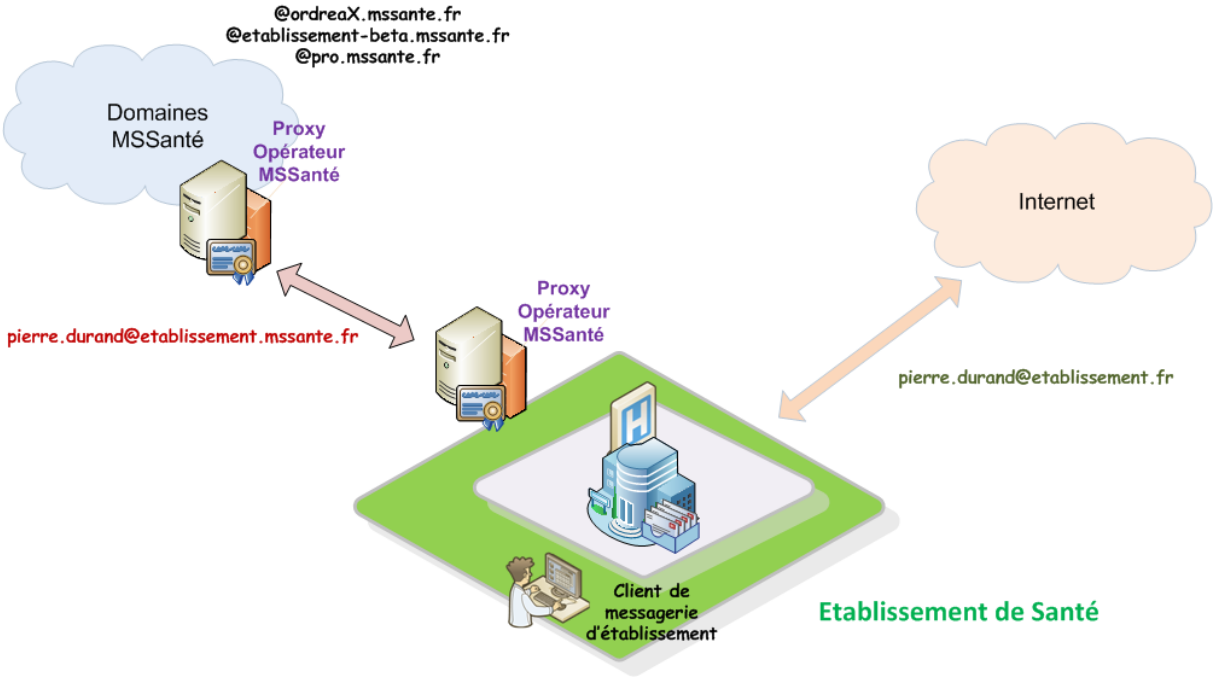


Figure 5 : Principe Proxy Opérateur MSSanté

# 3.5 Proxy d'Annuaire MSSanté

Le Proxy d'annuaire 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 ;
  - Via le client de messagerie ;
  - Par une vue unifiée des adresses MSSanté au sein de l'établissement.

Remarque : des exemples d'implémentations sont disponibles au **§ 3.7** « Exemples de mise en œuvre ».

# 3.6 Les clients de messagerie MSSanté

## 3.6.1 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 les interfaces standards ou propriétaires proposées par cet opérateur.

Les éditeurs de LPS et de clients de messagerie ont aussi l'opportunité d'intégrer les interfaces standards MSSanté (décrites dans le document « Dossier des Spécifications Techniques (DST) Clients de messagerie », disponible sur le site de l'ASIP Santé http://esante.gouv.fr/) qui sont en particulier mises en œuvre dans le cadre du service de messagerie opéré par l'ASIP Santé et les Ordres professionnels.

Remarques :

- Il n'est pas exigé des opérateurs qu'ils offrent nécessairement des interfaces standards 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.

### 3.6.2 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 **§ 7.1.1** « 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 échanges de données structurées entre applicatifs à l'aide du système MSSanté, le volet « Echange de Documents de Santé » ([CI-ECH-DOC]) du CI-SIS, définit les modalités d'échanges de documents de santé via la messagerie électronique sécurisée selon le principe suivant : l'échange de documents de santé est réalisé par attachement du contenu de lots de soumission en pièce jointe de messages électroniques selon la logique développée dans le profil IHE-XDM.

Les clients de messagerie pourront donc échanger des pièces jointes standardisées sur la logique du profil IHE-XDM. En complément de la pièce jointe XDM, les documents pourront également être attachés au format bureautique afin de faciliter la lecture pour les destinataires qui ne seraient pas en capacité d'exploiter le format XDM.

Il est à noter qu'un message ne doit contenir qu'une seule pièce jointe de type XDM, qui peut elle-même contenir plusieurs documents de santé (concept de lot de soumission) concernant le même patient. Dans ce cas, et afin de faciliter la lecture pour les destinataires qui ne seraient pas en capacité d'exploiter le format XDM, le message contiendra plusieurs pièces jointes au format bureautique, mais une seule pièce jointe de type XDM. C'est au client de messagerie émetteur de s'assurer de la cohérence entre les documents contenus dans la pièce jointe XDM et ceux transmis au format bureautique.

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

### 3.6.3 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 classiques (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.

Les interfaces standard décrites dans le DST Client de Messagerie sont brièvement présentées ci-dessous. Elles sont présentées de façon plus détaillées dans le DST Client de Messagerie.

***Client de messagerie – Accès par les protocoles classiques de messagerie***

Cette interface repose sur la mise en place d'une session TLS avec authentification mutuelle par carte CPS préalablement aux échanges par les protocoles standards de messagerie SMTP avec extension STARTTLS (port TCP/587) et IMAP4 avec extension STARTTLS (port TCP/143).

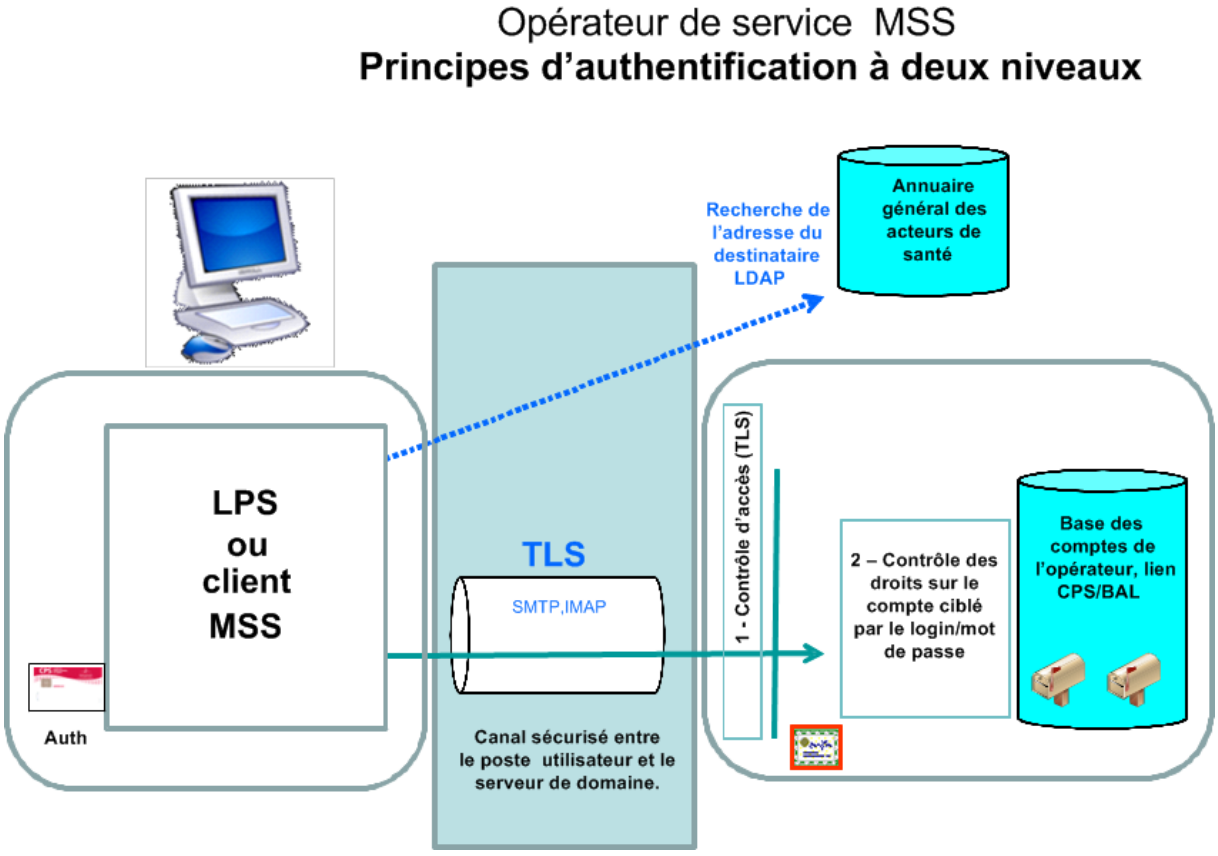


**Figure 6 : Principes d'authentification entre un Client de messagerie et un opérateur MSSanté selon un protocole standard de messagerie**

Le contrôle d'accès par le serveur est assuré sur deux niveaux :

- Un premier niveau d'authentification forte de l'utilisateur via l'établissement d'une session TLS avec présentation du certificat d'authentification CPS ;
- Un second niveau de contrôle des opérations de messagerie autorisées à l'utilisateur, préalablement authentifié au premier niveau, sur un compte de messagerie identifié par l'identifiant (login) présenté par les protocoles IMAP4 ou SMTP (mode de fonctionnement standard d'accès à un compte de messagerie).

***Client de messagerie – Accès par Web Services***

L'accès aux fonctions de messagerie peut également se faire via des Web Services implémentables par tout client de messagerie. Ces Web Services offrent des fonctions équivalentes à celles offertes par les protocoles classiques de messagerie.

L'accès à ces Web Services se fait par une authentification préalable, matérialisée par l'obtention d'un jeton d'authentification qui permet d'établir une session authentifiée sur le service de messagerie cible.

L'obtention de ce jeton peut se baser sur une authentification par carte CPS ou un mécanisme d'authentification équivalent de type OTP, et tout autre protocole y compris propriétaire conforme aux exigences légales. Le mécanisme d'authentification permettant d'obtenir ce jeton d'authentification est donc hors du périmètre du socle de base.

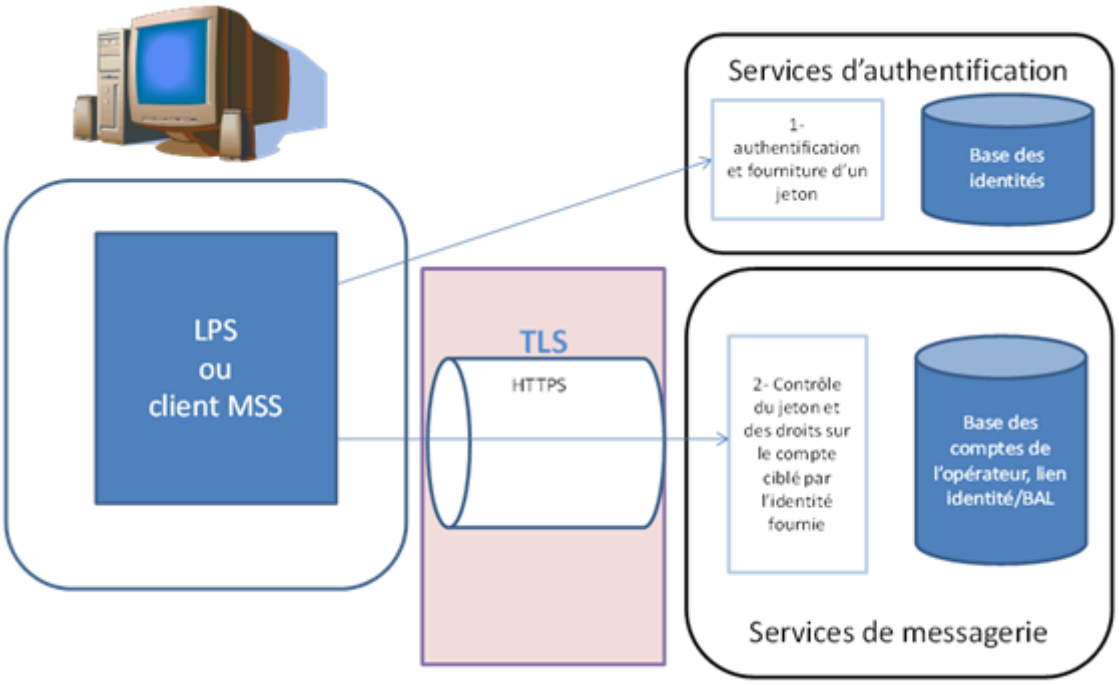


**Figure 7 : Principes d'authentification entre un Client de messagerie et un opérateur MSSanté exposant des Web Services de messagerie**

L'authentification préalable à l'obtention du jeton d'authentification doit permettre de s'assurer de l'identité de l'utilisateur.

L'accès au service de messagerie se fait sur HTTPS, avec l'établissement d'une connexion TLS avec authentification asymétrique, permettant d'assurer la confidentialité des échanges et de permettre la vérification, par le client de messagerie, du certificat présenté par le serveur.

Le service assure le contrôle d'accès aux données en vérifiant l'identité portée par le jeton d'authentification et les droits positionnés au sein du service.

# 3.7 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 Proxys Opérateur MSSanté). Ces exemples ont pour but de fournir des axes de réflexion sur les types d'intégration de la Messagerie Sécurisée de Santé.

## 3.7.1 Accès au service MSSanté via un domaine autorisé

### *3.7.1.1 Services de messagerie distincts*

L'exemple d'implémentation présenté ci-dessous décrit un service de messagerie complètement dédié à la Messagerie Sécurisée de Santé, qui est implémenté directement dans l'environnement d'un Etablissement de Santé ou d'un autre type d'opérateur.

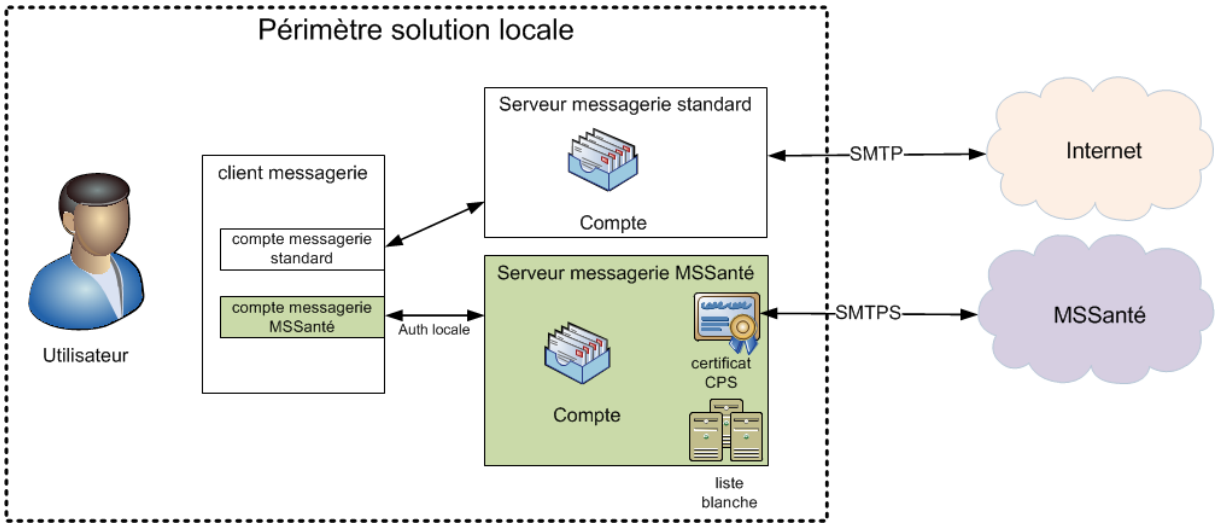


**Figure 8 : Services de messagerie distincts**

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 Proxy Opérateurs MSSanté est intégré au serveur de messagerie.

### *3.7.1.2 Service de messagerie unifié*

L'exemple d'implémentation présenté ci-dessous décrit un service de Messagerie Sécurisée 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.

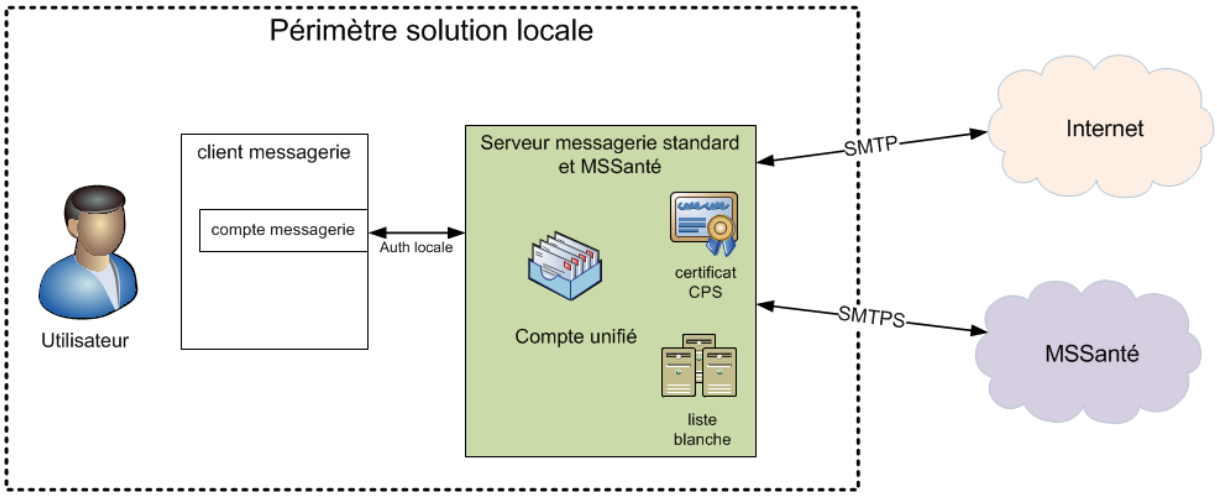


**Figure 9 : Service de messagerie unifié**

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

Remarque : le Proxy Opérateurs MSSanté est intégré au serveur de messagerie.

### *3.7.1.3 Fonction Proxy Opérateur MSSanté non intégré dans le serveur de messagerie*

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

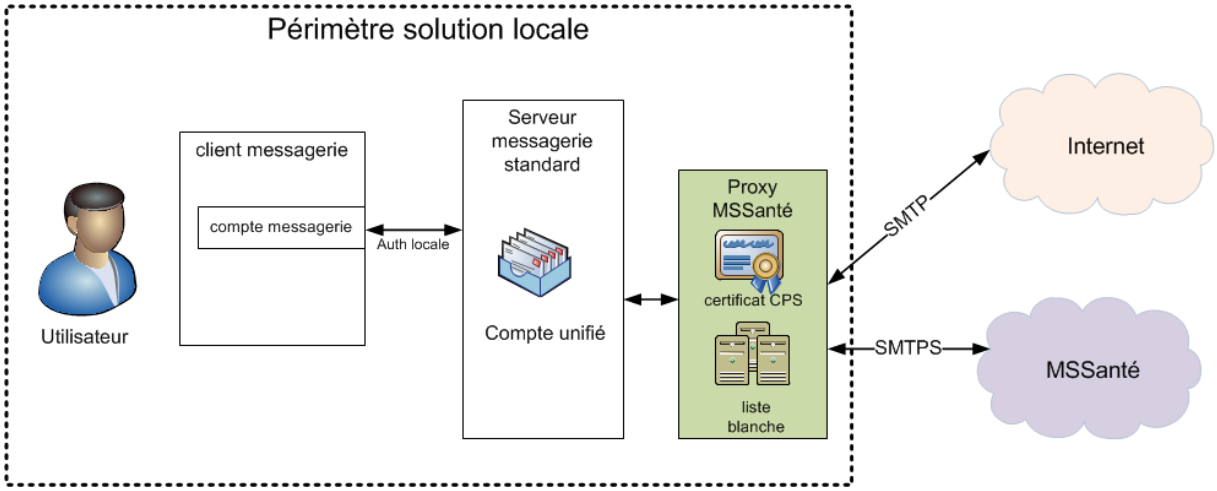


**Figure 10 : Proxy Opérateur MSSanté non intégré au serveur de messagerie**

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

Il gère également la correspondance entre les adresses internes et les adresses MSSanté.

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

#### *3.7.1.4 Echange de messages sécurisés depuis ou vers des applications*

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

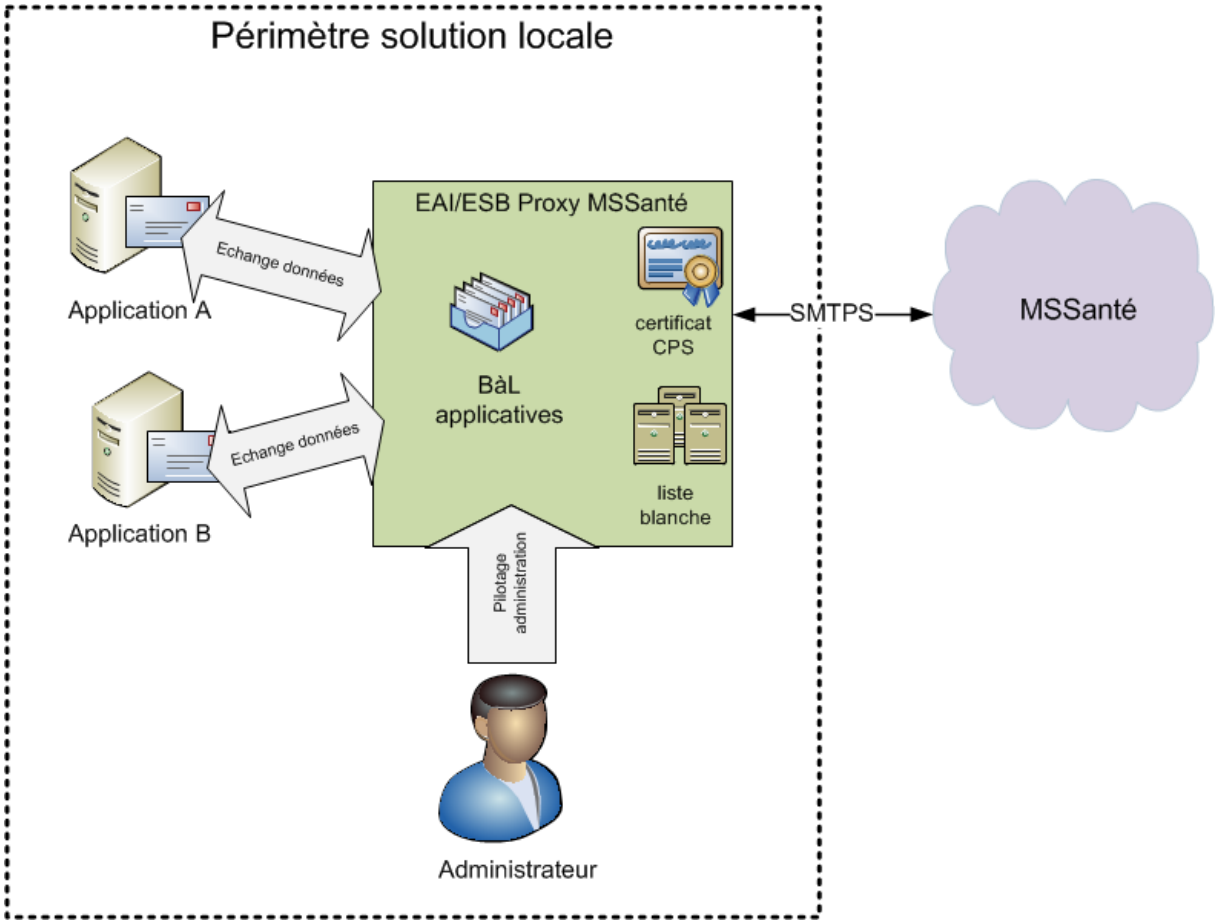


**Figure 11 : Echange de messages sécurisés depuis ou vers des applications**

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

## 3.7.2 Accès à la BAL MSSanté

### *3.7.2.1 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.

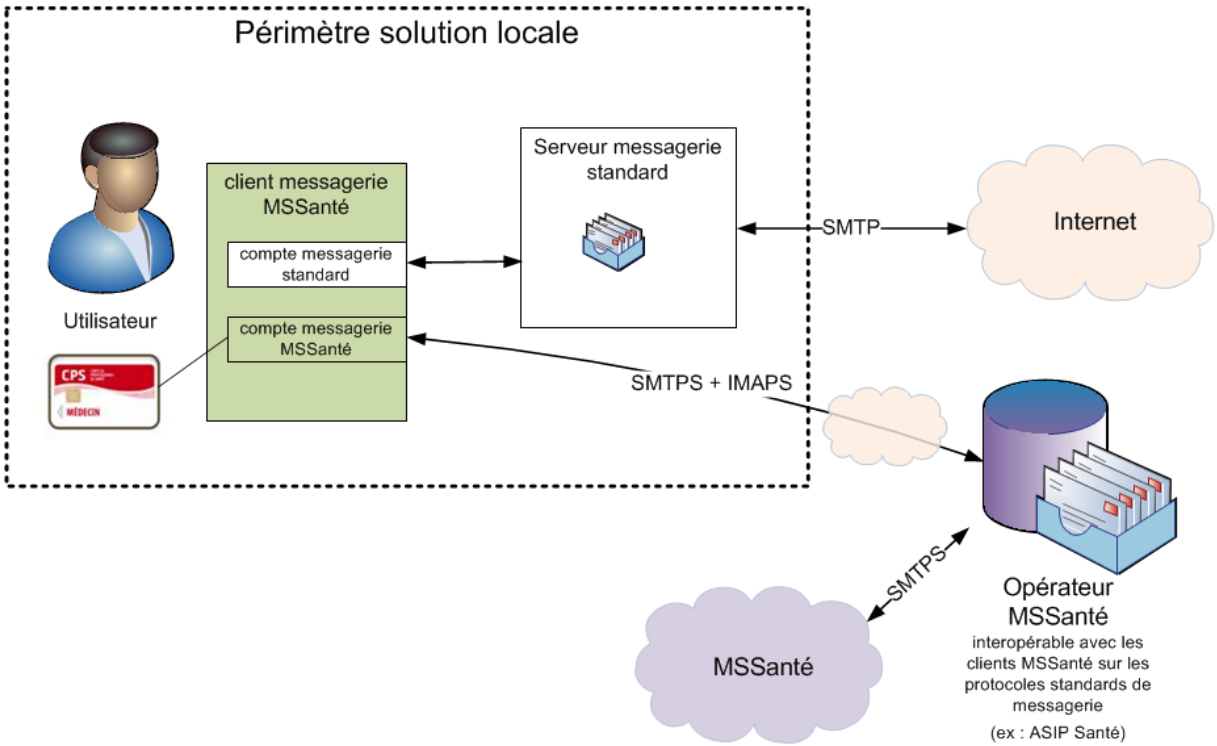


**Figure 12 : Accès MSSanté par client de messagerie et carte CPS**

### *3.7.2.2 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 Passsword = OTP) par SMS sur le terminal de l'utilisateur.

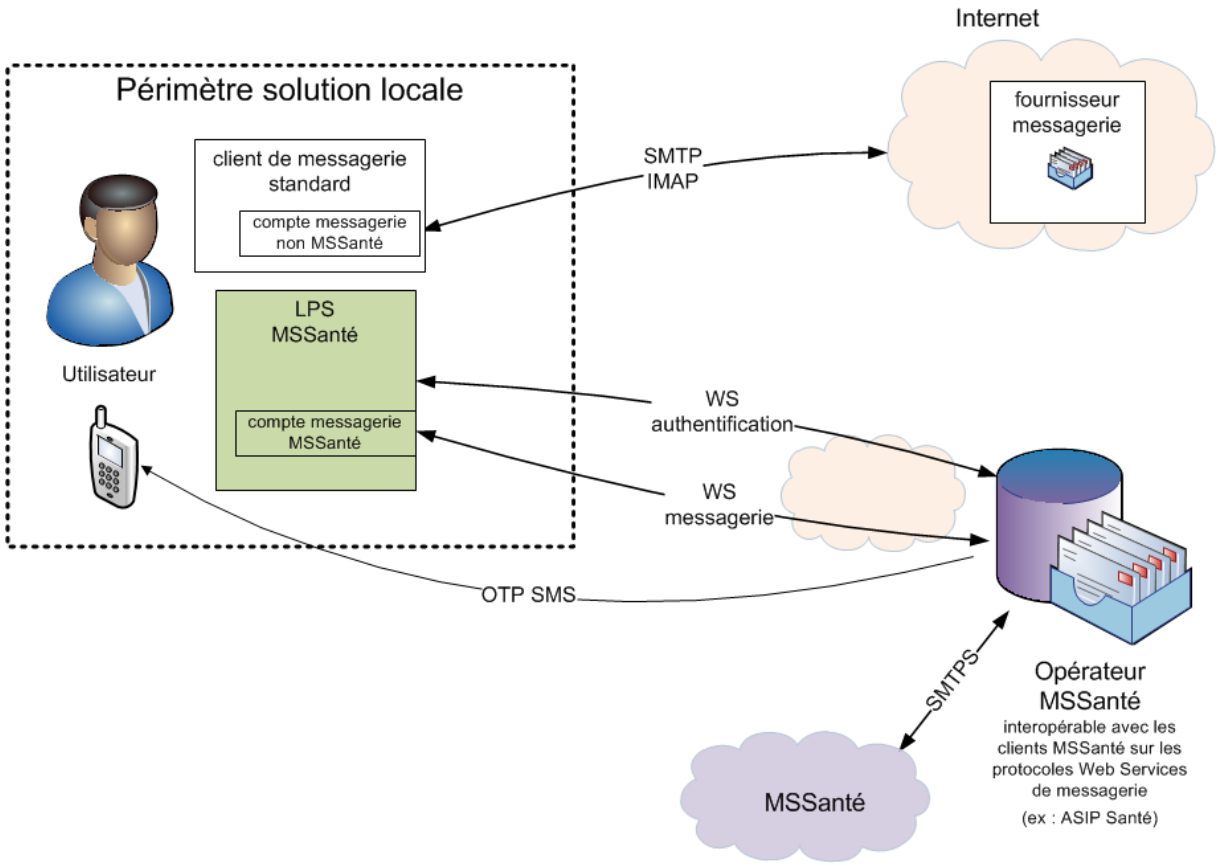


**Figure 13 : Accès MSSanté par LPS et identifiant/mot de passe/OTP**

#### *3.7.2.3 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 internet[3].

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

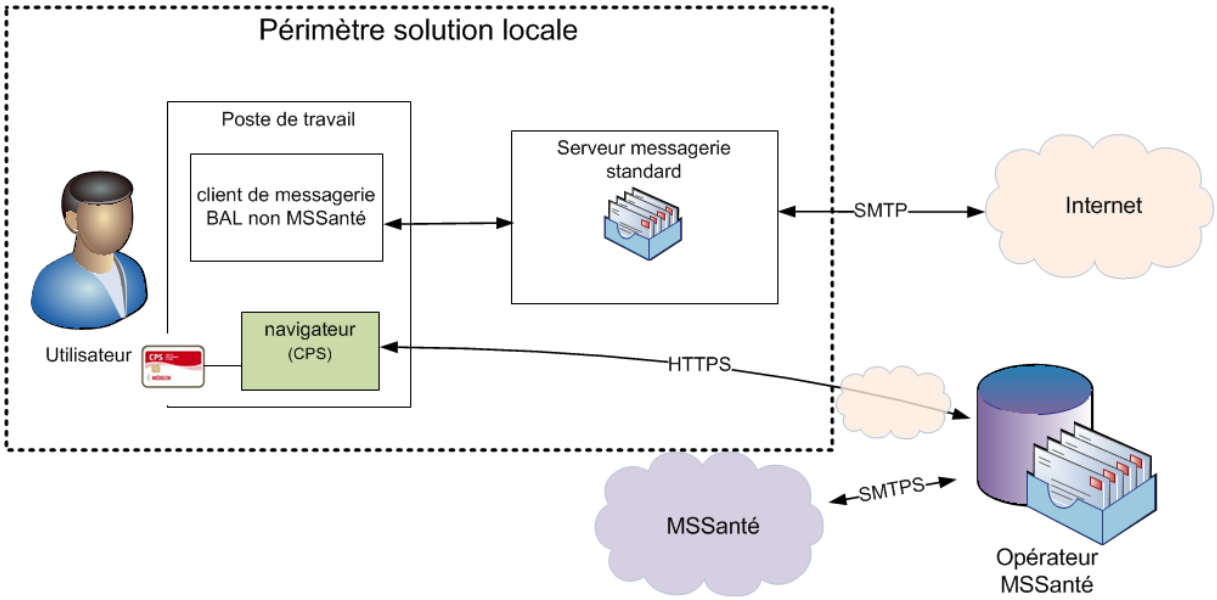


**Figure 14 : Accès MSSanté par Webmail et par carte CPS (plateforme nationale MSSanté)**

[3] L'opérateur ASIP Santé met à disposition un accès en Webmail pour les BAL qu'elle héberge sur les domaines ordinaux (@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).

#### *3.7.2.4 Par Webmail et mode d'authentification équivalent à la 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 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.

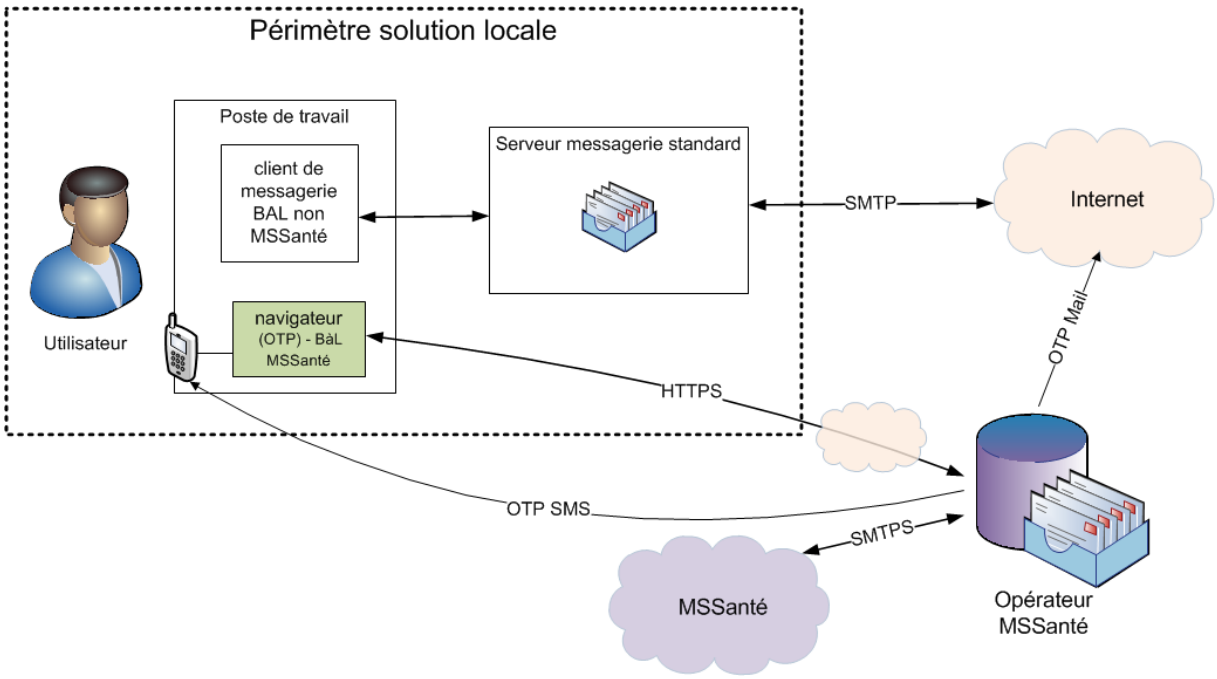


**Figure 15 : Accès MSSanté par Webmail et sans carte CPS (plateforme nationale MSSanté)**

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.

### *3.7.2.5 Exemple des modalités retenues par l'opérateur ASIP Santé pour le domaine générique et ceux des Ordres professionnels*

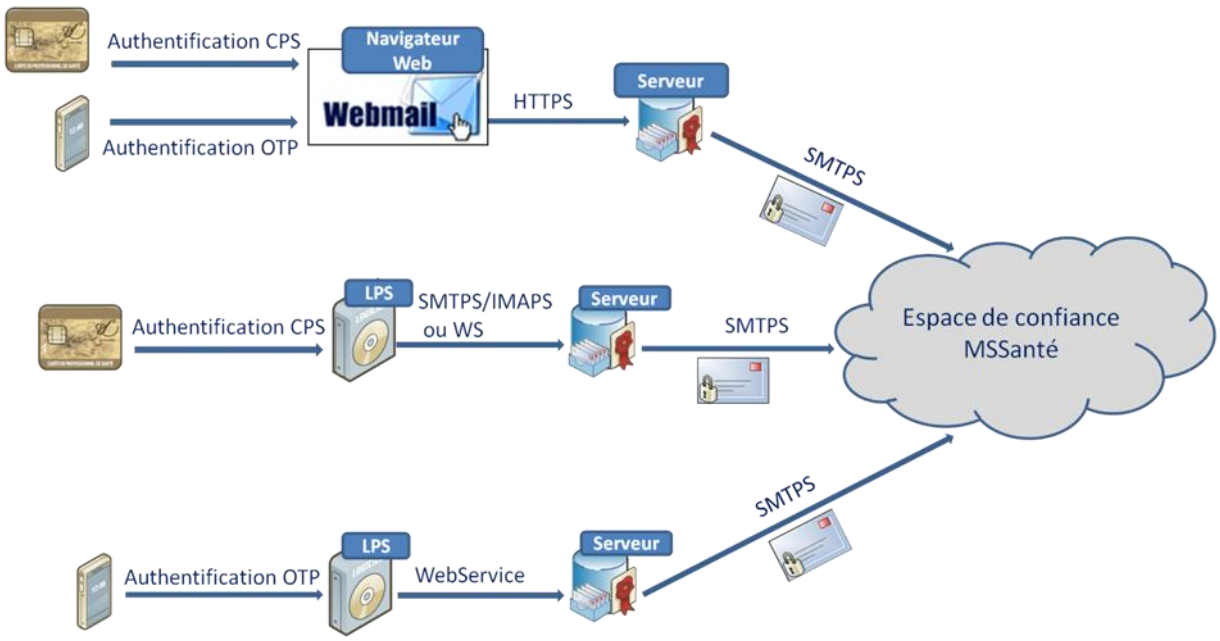


**Figure 16 : Modalités retenues par l'ASIP Santé an tant qu'opérateur de domaines MSSanté**

## 3.7.3 Consultation de l'annuaire national MSSanté

### *3.7.3.1 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.

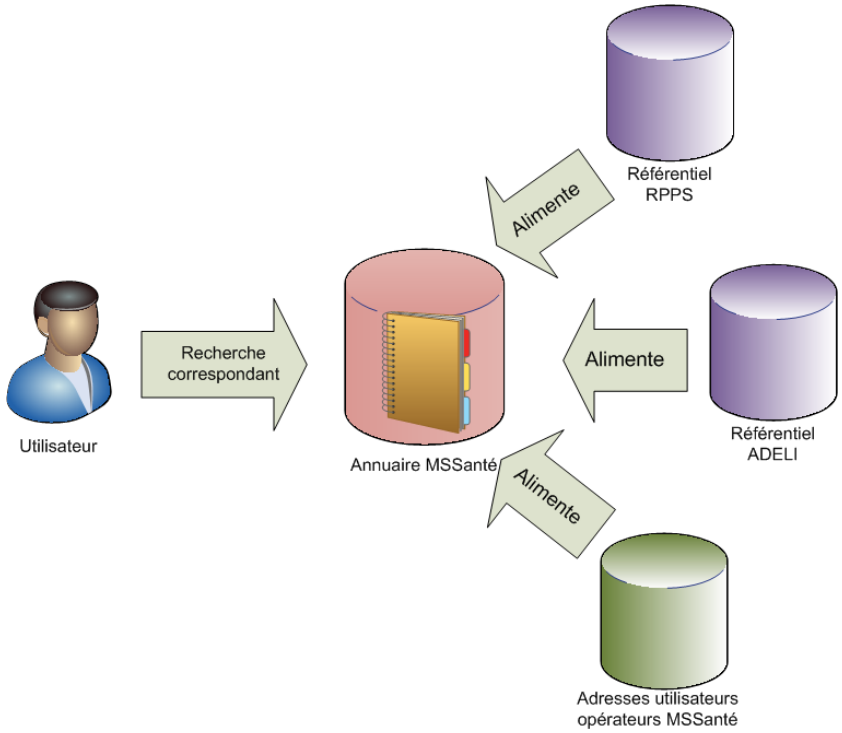


**Figure 17 : Principe d'alimentation de l'annuaire national MSSanté**

### *3.7.3.2 Recherche de correspondants MSSanté*

#### 3.7.3.2.1 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 Proxy d'annuaire 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.

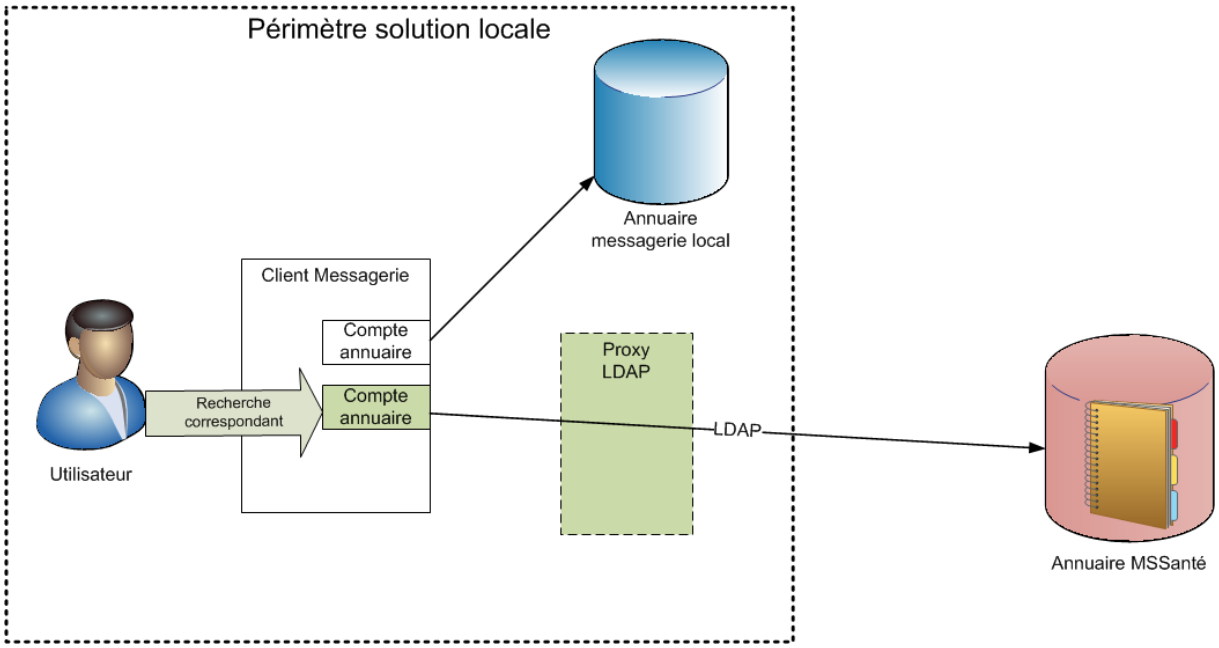


**Figure 18 : Accès direct à l'annuaire national MSSanté via le client de messagerie**

#### 3.7.3.2.2 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.

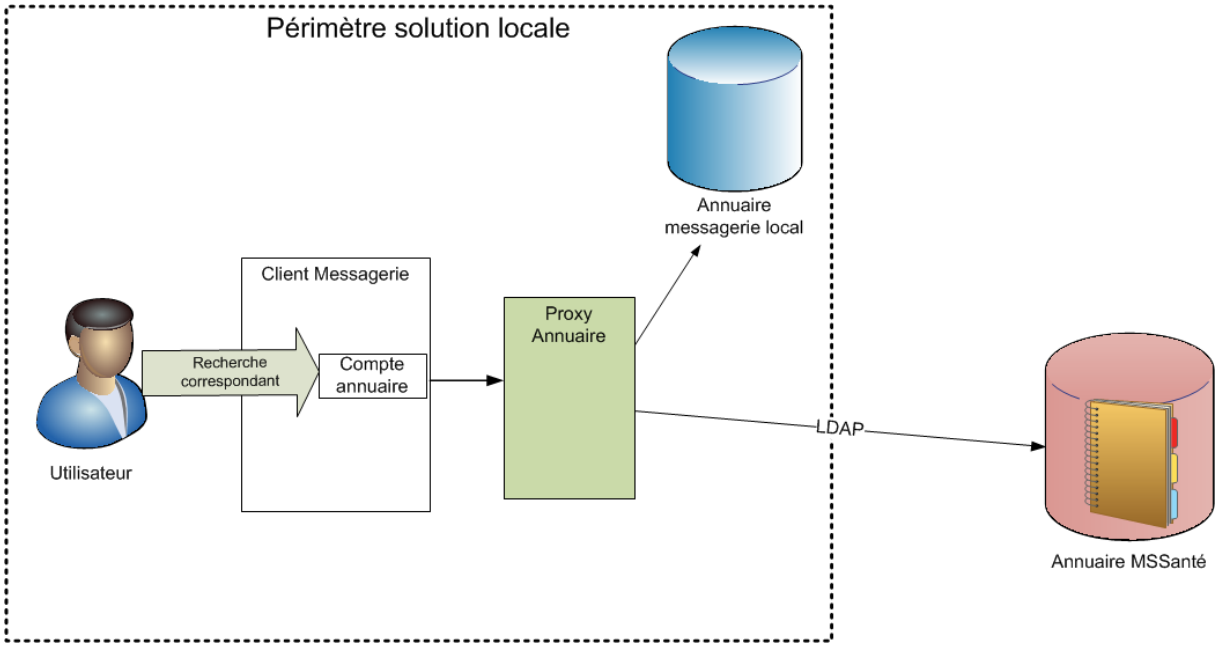


**Figure 19 : Vue unifiée de l'annuaire au sein du domaine MSSanté**

Le Proxy annuaire MSSanté permet alors de proposer une vue unifiée dans les réponses renvoyées à l'utilisateur.

#### 3.7.3.2.3 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.

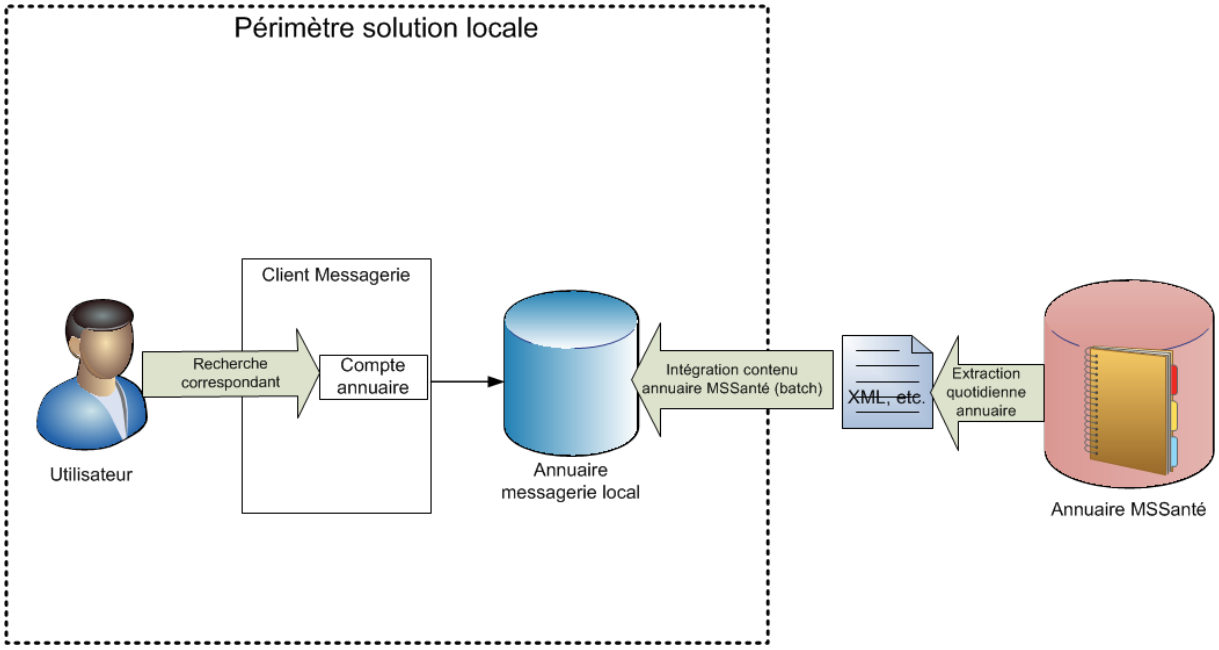


**Figure 20 : Intégration de l'annuaire national MSSanté au sein du domaine MSSanté**

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

### 3.7.4 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.

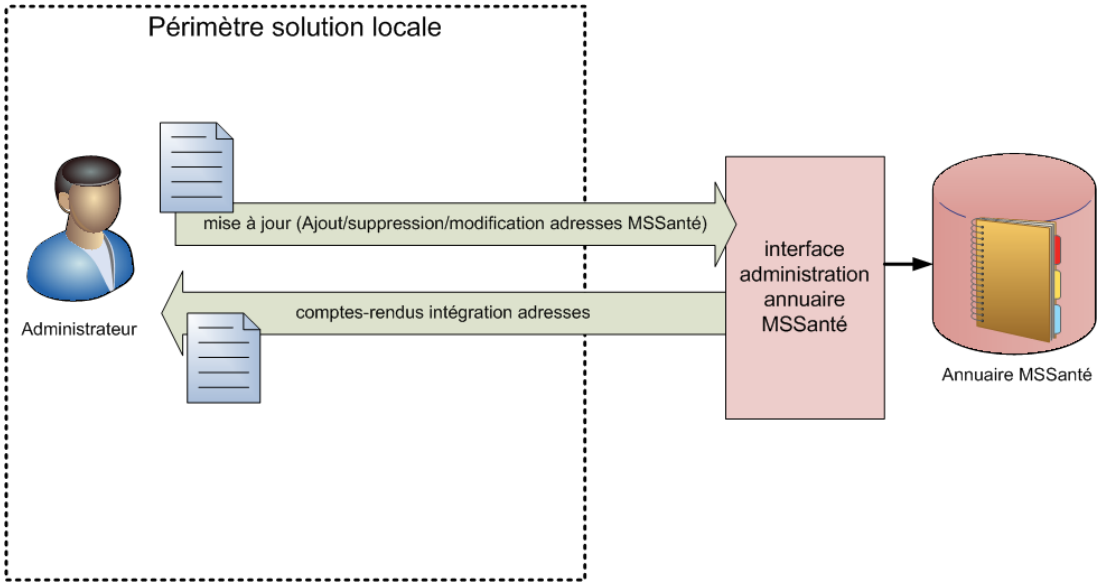


**Figure 21 : Publication dans l'annuaire national MSSanté**

Plusieurs types d'interfaces de mises à jour sont proposés par l'ASIP Santé. Un compte-rendu d'intégration est envoyé à l'administrateur local après chaque demande de mise à jour.

# 4 Exigences fonctionnelles et techniques à respecter par les opérateurs MSSanté

Le « contrat opérateur MSSanté » conditionne l'intégration validée de l'opérateur à l'espace de confiance au respect d'un ensemble de dispositions techniques et fonctionnelles identifiés dans le présent DSFT sous la notion d'« exigences » : « Ⓔ ».

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 »).

L'opérateur doit mettre en œuvre un Proxy de messagerie MSSanté pour le raccordement de son serveur de messagerie à l'espace de confiance MSSanté.

Par Proxy Opérateur MSSanté (ou Proxy de messagerie MSSanté), il faut entendre un logiciel capable d'assurer le raccordement d'un domaine de Messagerie Sécurisée de Santé à l'espace de confiance MSSanté, dans le respect des exigences fonctionnelles et techniques définies par l'ASIP Santé. Ce raccordement consiste essentiellement en la capacité du Proxy de messagerie à émettre et recevoir des messages dans l'espace de confiance MSSanté, ainsi qu'à gérer le cycle de vie des boîtes aux lettres (publication des adresses des BAL du domaine dans l'annuaire national MSSanté au rythme de leur attribution).

L'opérateur candidat peut également mettre en œuvre un Proxy Annuaire MSSanté pour la recherche dans l'annuaire national MSSanté par les utilisateurs de son service de messagerie.

Les opérateurs MSSanté (Etablissements de Santé, fournisseurs de service de messagerie de santé sécurisée du secteur concurrentiel, etc.), fournissent eux-mêmes des BAL MSSanté aux utilisateurs du service qu'ils proposent ; les chapitres suivants traitent exclusivement des cas d'usages et fonctions proposées dans ce cadre.

**Un opérateur MSSanté peut mettre à disposition les boîtes aux lettres de ses utilisateurs de plusieurs manières :**

- **Soit en utilisant un mode d'accès spécifique (exemples : Webmail, client de messagerie standard ou client de messagerie propriétaire à l'opérateur) qui respecte les règles d'intégration dans l'espace de confiance MSSanté (décrites dans le « contrat opérateur MSSanté ») ;**
- **Soit en proposant les interfaces (Web Services et/ou IMAPS/SMTPS) décrites dans le DST Clients de messagerie pour les logiciels respectant ces spécifications.**

Dans le cadre de l'attribution de BAL MSSanté à leurs utilisateurs, les opérateurs MSSanté doivent s'assurer que :

- Les utilisateurs du service MSSanté sont identifiés et authentifiés individuellement, conformément aux exigences légales (CPS ou dispositifs équivalents) ;
- Les utilisateurs n'accèdent qu'aux BAL MSSanté pour lesquelles ils sont explicitement autorisés.

## 4.1 Choix des transactions à implémenter pour un Proxy Opérateur MSSanté

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

Les transactions indiquées comme « 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 | Requis/ Option |
|---|---|---|---|---|
| **Publication des BAL MSSanté** | | | | |
| **TM1.1P** | **TM1.1.1P** | MàJ des BAL dans l'annuaire national MSSanté en Web Service global* et récupération du compte-rendu d'intégration | Transaction de publication des BAL MSSanté d'un domaine de messagerie dans l'annuaire national MSSanté | Requis* |
| | **TM1.1.2P [AC]** | MàJ des BAL dans l'annuaire national MSSanté en Web Service différentiel* **[AC]** | | |
| | **TM1.1.3P [AC]** | MàJ des BAL dans l'annuaire national MSSanté en transfert de fichier * **[AC]** | | |
| **Annuaire national MSSanté** | | | | |
| **TM2.1A** | **TM2.1.1A** | Consultation de l'annuaire national MSSanté en LDAP** | Recherche multicritères de correspondants dans l'annuaire national MSSanté | Option** |
| | **TM2.1.2A [AC]** | Consultation de l'annuaire national MSSanté par Web Service** **[AC]** | | |
| | **TM2.1.3A** | Téléchargement de l'annuaire national MSSanté ** | Récupération d'une copie des données de l'annuaire national MSSanté par téléchargement | |
| **Téléchargement des données d'identités** | | | | |
| **TM2.1.4 A** | 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 |
| **Emission et réception de messages** | | | | |
| **TM3.1P** | Réception de messages | | Fonctions de réception de messages depuis des domaines de l'espace de confiance MSSanté, sous le protocole SMTP avec extension STARTTLS | Requis |
| **TM3.2P** | Emission de messages | | Fonctions d'émission de messages vers des domaines de l'espace de confiance MSSanté, sous le protocole SMTP avec extension STARTTLS | Requis |
| **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 | Requis |

**Tableau 1 : Liste des transactions MSSanté pour les opérateurs MSSanté**

(*) Plusieurs modalités de publication des comptes de messagerie dans l'annuaire national MSSanté sont prévues et détaillées au **§ 4.4** « Publication de BAL MSSanté dans l'annuaire national MSSanté » ; il est exigé que le Proxy de messagerie MSSanté mette en œuvre au moins l'une des modalités proposées.

(**) Plusieurs modalités de consultation ou téléchargement de l'annuaire national MSSanté sont prévues et détaillées au **§ 4.5.1** « TM2.1.1A et TM2.1.2A - Consultation de l'annuaire national MSSanté » et au **§ 4.5.2** « TM2.1.3A - Téléchargement d'une extraction de l'annuaire national MSSanté » ; la mise en œuvre de la transaction (optionnelle) de consultation de l'annuaire national MSSanté nécessite le cas échéant l'implémentation par l'opérateur d'au moins une des modalités proposées.

## 4.2 Modalités techniques pour assurer la sécurisation des échanges

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

### 4.2.1 Principes de raccordement des Proxys Opérateur MSSanté 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 Proxys de messagerie MSSanté 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 Proxys de messagerie MSSanté des opérateurs MSSanté doivent la prendre en compte (voir **§ 4.6.2** « 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 forte 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.

| **EX_OPE_5010** |
| --- |
| La version minimum de TLS qui doit être mise en œuvre est la version 1.0 (cf. RFC 2246 - http://tools.ietf.org/html/rfc2246). |

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.

### 4.2.2 Validation des certificats serveur

| EX_OPE_5020 |
| --- |
| Le Proxy de messagerie 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 le certificat utilisé par les serveurs des opérateurs MSSanté sont disponibles aux adresses suivantes : http://annuaire.asipsante.fr/ (onglet : « Informations ») et http://esante.gouv.fr/services/espace-cps/telechargement.

***Gestion de plusieurs chaînes de certification***

| RE_OPE_5010 |
| --- |
| Il est recommandé que les Proxys de messagerie MSSanté des opérateurs MSSanté soient en mesure de gérer plusieurs chaînes de certification afin de pouvoir prendre en compte, le cas échéant, de nouvelles offres de produits de certification. |

***Certificats racine***

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 des fils de l'AC nommée "AC-classe-4" elle-même fille de l'AC "GIP-CPS". Les ressources liées à ces deux AC sont donc nécessaires pour valider les certificats. Les fichiers (certificats) des AC "GIP-CPS" et "AC-classe-4" doivent être récupérés par l'intermédiaire du site http://annuaire.asipsante.fr/ (onglet : « Autorités de Certification »), et déployés avec le Proxy Opérateur MSSanté.<br>Lorsque la vérification de l'intégrité de la chaine de confiance des certificats échoue, la 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). Cependant, les CRLs des certificats serveurs de classe 4 peuvent être téléchargées par le Proxy Opérateur MSSanté (éventuellement par tâche planifiée : les CRLs « ASIP Santé » sont mises à jour en totalité une fois par jour mais des deltas CRLs existent néanmoins permettant ainsi d'optimiser la mise à jour des CRLs si besoin), puis utilisées de manière programmatique lors de la validation (en général en installant ou en passant en paramètre les CRLs dans le composant technique de validation de certificat).

Les informations et ressources (fichiers) sur les AC et les listes de révocation (CRLs) "ASIP Santé" sont disponibles sur le site http://annuaire.asipsante.fr/ dans les onglets « Autorités de Certification » et « CRL ».

***Vérification des certificats des AC Classe 4 et racine GIP-CPS installés***

| **RE_OPE_5040** |
| --- |
| Pour assurer la sécurité des applications intégrant des certificats d'AC, il est recommandé de comparer l'empreinte numérique des certificats utilisés avec la source de confiance (http://integrateurs-cps.asipsante.fr/pages/Certificats-Racines-CPS). |

La validation (comparaison de l'empreinte) peut être réalisée :

- Automatiquement (dans la majorité des cas) par la librairie ou le composant logiciel de gestion des connexions TLS :
  - Ce contrôle est réalisé de base par les navigateurs du marché ;
  - Soit en passant ces fichiers en paramètre de ce composant lors de l'établissement de la connexion TLS (cas de librairies se basant sur OpenSSL par exemple) ;
  - Soit en intégrant ces fichiers dans un magasin de certificats (autorités de confiance) propre au composant de connexion (cas de Java par exemple) ;
  - Soit en intégrant ces fichiers dans le magasin des autorités de confiance de l'OS, utilisé par le composant (cas de Microsoft .Net par exemple).
- Manuellement, en comparant les empreintes ; pour les calculer :
  - Cette information est calculée automatiquement par la visionneuse de certificat Windows (onglet "Détail", "<tout>", dernière ligne) ;
  - En utilisant la commande "openssl X509 -fingerprint" sur le fichier certificat ;
  - En utilisant les commandes "sha1sum" ou "sha256sum" sur le certificat dans sa forme DER.

Remarque : pour effectuer ce contrôle, le simple téléchargement des certificats des serveurs constitue une mauvaise pratique : il est demandé de bien valider le certificat à l'aide de l'autorité émettrice AC-Classe-4 subordonnée à l'autorité racine « GIP-CPS »; en effet, l'ajout du certificat des serveurs des opérateurs MSSanté comme autorité de confiance dans le Proxy Opérateur MSSanté (ou dans le système d'exploitation) n'est pas adapté car, à terme, lors du renouvellement du certificat des opérateurs MSSanté (tous les 3 ans), cette mesure obligerait à mettre à jour tous les Proxys déployés.

## 4.3 Modalités techniques spécifiques aux Web Services d'annuaire

| **EX_WSA_5010** |
| --- |
| L'authentification mutuelle du Proxy de messagerie MSSanté avec le serveur d'annuaire national MSSanté constitue un pré-requis 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 utilisé pour l'authentification TLS mutuelle : il est donc nécessaire que celui-ci l'ait obtenu au préalable pour le domaine (certificat serveur « classe 4 ») auprès de l'ASIP Santé pour l'authentification pour personne morale (certificat X509, de type « SSL »).

Remarque : 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). |

Remarque : les abréviations utilisées dans les descriptions des attributs et des règles sont définies au **§ 7.2.3** « Légendes et abréviations utilisées dans les descriptions des attributs et règles ».

#### *4.3.1.1 Web Services de l'annuaire national MSSanté en SOAP*

##### 4.3.1.1.1 Encodage et espace de nommage

| **EX_WSA_5030** |
|---|
| Les spécifications du **§ 4.3.1.1.1** 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://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"*

##### 4.3.1.1.2 Sécurité et intégrité

| **EX_WSA_5040** |
|---|
| Les spécifications du **§ 4.3.1.1.2** 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 le document [CI-TR-CLI-LRD].

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

Le contrôle d'accès est réalisé par rapport au DN du certificat d'authentification utilisé par le système initiateur. Pour qu'un système soit autorisé à utiliser les Web Services de l'annuaire 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.

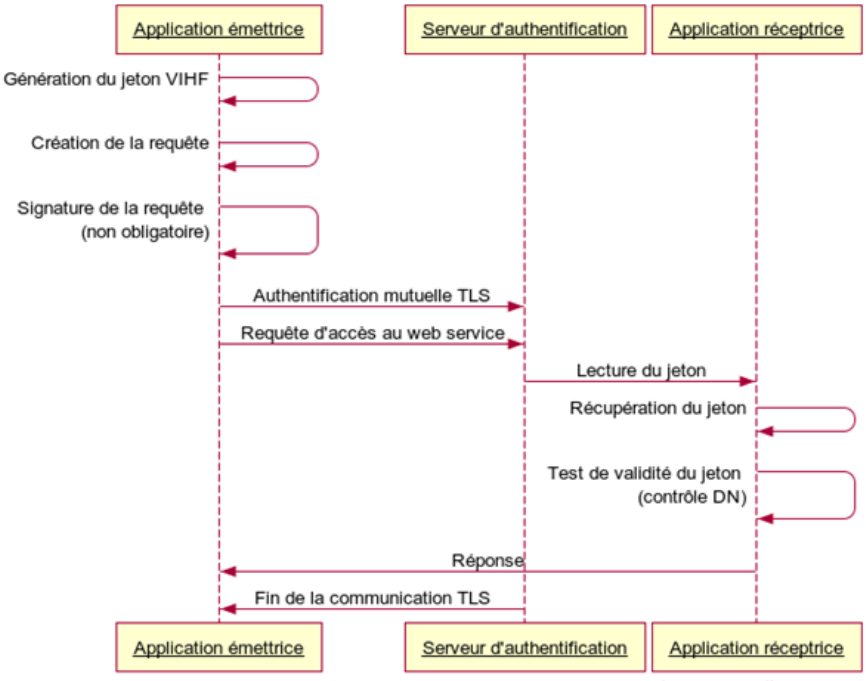


**Figure 22 : Principe d'identification et d'authentification**

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.

#### 4.3.1.1.3 Description des échanges

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

##### *4.3.1.1.3.1 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 peut ensuite utiliser pour interroger le Web Service de suivi de l'avancement de l'alimentation (ou « Web Service de rapport d'alimentation »).

##### *4.3.1.1.3.2 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.

La version courante d'un Web Service est la **V1011**.

##### *4.3.1.1.3.3 Principe de construction des messages*

| **EX_WSA_5050** |
| --- |
| Les spécifications du **§ 4.3.1.1.3.3** (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).

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

##### *4.3.1.1.3.3.1 En-tête du message*

Dans le cadre de l'annuaire national MSSanté, l'élément `Header` du message contient le jeton VIHF et les informations sur le message (WS-Adressing).

Eléments spécifiques de l'en-tête :

- 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 ;
- Le jeton VIHF, intégré dans l'en-tête, permet d'identifier le système initiateur ;
- Le message SOAP proposé est étendu avec la spécification WS-Addressing 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.

Elle contient une entrée WS-Adressing obligatoire qui étend les spécifications du protocole SOAP 1.2 et le jeton VIHF.

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 : Eléments du WS-Addressing**

### *Contenu du jeton VIHF*

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

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

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

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE |
|---|---|---|---|---|
| **CHAMPS STANDARDS** | | | | |
| //Assertion/@xmlns:saml2 | *namespace XML SAML* | Oui | Alpha numérique | **Constante** :"urn:oasis:names:tc:SAML:2.0:assertion" |
| //Assertion/@Version | *Version utilisée* | Oui | Alpha numérique | **Constante** : "2.0" |
| //Assertion/@ID | *Identifiant unique de l'assertion* | Oui | Alpha numérique | Id de l'assertion |
| //Assertion/@IssueInstant | *Date et heure d'émission de l'assertion SAML* | Oui | xs: dateTime | Contrôle de validité à l'instant I : T < I < T+1h contrôlée par le système cible et doit être antérieure à l'heure d'arrivée |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE |
|---|---|---|---|---|
| | | | | de l'assertion sur le système cible et inférieure à la durée maximum acceptable |
| //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.<br>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.<br>**Cet attribut est utilisé pour l'authentification de l'utilisateur.** |
| //Assertion/Issuer/@Format | *Type de valeur utilisée pour renseigner le champ Issuer (X509)* | Oui | Alpha numérique | **Constante** : urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName |
| //Assertion/ds:Signature | *Emplacement réservé à la signature* | Oui pour les jetons signés | Alpha numérique | Eléments de la signature |
| //Assertion/Subject/NameID | *L'identifiant de l'utilisateur final envoyé par le système initiateur* | Oui | Alpha numérique | **En authentification indirecte** (authent serveur) : information déclarative - pas de contrôle. |
| //Assertion/AuthnStatement/AuthnContext/AuthnContextClassRef | *La méthode d'authentification de l'utilisateur* | Oui | Alpha numérique | **En authentification indirecte**, la valeur est laissée au choix de l'émetteur de l'assertion dès lors qu'elle est sélectionnée dans le document http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf |
| //Assertion/AuthnStatement/@AuthnInstant | *La date et l'heure exprimée en UTC à laquelle l'authentification a été réalisée par le système initiateur* | Oui | xs: dateTime | Date/heure d'authentification SI |
| //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 | Date/heure de début de l'assertion<br>Contrôle de validité à l'instant I : T < (NotBefore) < I < min(T+1h, NotOnOrAfter) |
| //Assertion/Conditions/@NotOnOrAfter | *La date et l'heure UTC de fin de validité de l'assertion* | Oui | xs: dateTime | |
| **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 | Nomenclature Secteur d'activité<br>**code** : code du secteur |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE |
|---|---|---|---|---|
| | | | | d'activité<br>**codeSystem**: 1.2.250.1.71.4.2.4<br>**codeSystemName** : optionnel<br>**displayName :** optionnel<br><br>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 |
| 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 | Non significatif dans le contexte MSSanté.<br><br>Ce paramètre ne sera pas utilisé mais il est demandé de le positionner à « normal » |
| Mode_Acces_Raison | *Explication de la raison de l'usage du bris de glace.* | Non | Alpha numérique | Vide - non significatif dans le contexte MSSanté. |
| urn:oasis:names:tc:xspa:1.0:subject:subject-id | *Identité de l'utilisateur* | Oui | Alpha numérique | Identification explicite de l'utilisateur (ex : nom, prénom, service au sein d'un établissement…) ou identification explicite de la machine (ex. nom du logiciel, nom du modèle, service au sein d'un établissement…).<br><br>Pas de contrôle sur la valeur. |
| Identifiant_Structure | *Identifiant de L'établissement de santé depuis lequel la requête a été émise* | Oui | Alpha Numérique | L'identifiant national de la structure « **Struct_IdNat »** |
| LPS_Nom | *Nom du logiciel utilisé* | Oui | Alpha numérique | Non significatif dans le contexte MSSanté |
| LPS_Version | *Version du logiciel utilisé* | Oui | Alpha numérique | Non significatif dans le contexte MSSanté |
| LPS_ID | *Numéro de série ou identifiant de l'installation du logiciel* | Oui | Alpha numérique | Non significatif dans le contexte MSSanté |
| PROFIL_UTILISATEUR | *Le profil de l'utilisateur* | Oui | OID | Nomenclature Profil d'accès à l'annuaire national MSSanté<br><br>**code** : 'OPER'<br>**codeSystem** : 1.2.250.1.213.1.9.1.1<br><br>**codeSystemName** (attribut optionnel) : 'R84'<br>**displayName** (attribut optionnel) : 'Opérateur |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE |
|---|---|---|---|---|
| | | | | MSSanté ‘ |
| PROFIL_UTILISATEUR_PERIMETRE | *Le contexte métier ou périmètre de l’utilisateur* | Non | OID | Vide - non significatif dans le contexte MSSanté. |
| VIHF_PROFIL | *Le profil VIHF* | Oui | OID | Nomenclature Profil VIHF<br>**code** : profil_annuaire_PS<br><br>**codeSystem**: 1.2.250.1.213.1.1.4.312<br><br>**codeSystemName** (attribut optionnel) : ‘profil VIHF’<br>**displayName** (attribut optionnel) : 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 de jeton VIHF***

Voici un exemple de jeton VIHF pour l'annuaire national MSSanté (authentification indirecte).

```
<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="4df37536-4fc6-4f21-a192-837fb4153bed"
IssueInstant="2013-06-07T15:49:24.669Z" Version="2.0">
 <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:X509SubjectName">CN=Client
WebServices, OU=RASS, O=ASIP, ST=IDF, C=FR</saml2:Issuer>
 <saml2:Subject>
 <saml2:NameID>30B0025920/CDET0001</saml2:NameID>
 </saml2:Subject>
 <saml2:AuthnStatement AuthnInstant="2013-06-07T15:49:24.706Z">
 <saml2:AuthnContext>
<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml2:AuthnContextClassR
ef>
 </saml2:AuthnContext>
 </saml2:AuthnStatement>
 <saml2:AttributeStatement>
 <saml2:Attribute Name="VIHF_Version">
  <saml2:AttributeValue>2.0</saml2:AttributeValue>
 </saml2:Attribute>
 <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 Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
  <saml2:AttributeValue>Jean Dupont </saml2:AttributeValue>
 </saml2:Attribute>
 <saml2:Attribute Name="Identifiant_Structure">
  <saml2:AttributeValue>10B0025920</saml2:AttributeValue>
 </saml2:Attribute>
 <saml2:Attribute Name="LPS_Version">
  <saml2:AttributeValue>1.1</saml2:AttributeValue>
 </saml2:Attribute>
 <saml2:Attribute Name="LPS_ID">
  <saml2:AttributeValue>ID du LPS </saml2:AttributeValue>
 </saml2:Attribute>
 <saml2:Attribute Name="LPS_Nom">
  <saml2:AttributeValue>SUPER_LPS</saml2:AttributeValue>
 </saml2:Attribute>
  <saml2:Attribute Name="Profil_Utilisateur">
  <saml2:AttributeValue>
  <Profil_Utilisateur xmlns="urn:hl7-org:v3" xmlns:xsi="urn:hl7-org:v3" hl7:code="OPER"
hl7:codeSystem="1.2.250.1.213.1.9.1.1" hl7:codeSystemName="R84" hl7:displayName=" Opérateur MSSanté "
xsi:type="CE"/>
  </saml2:AttributeValue>
 </saml2:Attribute>
<saml2:Attribute Name="VIHF_Profil">
  <saml2:AttributeValue>
  <VIHF_Profil xmlns="urn:hl7-org:v3" xmlns:xsi="urn:hl7-org:v3" hl7 :code="profil_annuaire_PS"
hl7:codeSystem="1.2.250.1.213.1.1.4.312" hl7:codeSystemName="profil VIHF" hl7:displayName="Profil pour
annuaire de professionnels de santé du VIHF 2.0" xsi:type="CE"/>
  </saml2:AttributeValue>
 </saml2:Attribute>
 </saml2:AttributeStatement>
</saml2:Assertion>
```

**Figure 23 : Exemple de jeton VIHF pour l'annuaire national MSSanté (authentification indirecte)**

#### *4.3.1.1.3.3.2 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.

#### *4.3.1.1.3.3.3 Description des ressources terminologiques*

Les ressources terminologiques utilisées dans les échanges sont gérées dans le NAS (Nomenclatures des Acteurs 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 :

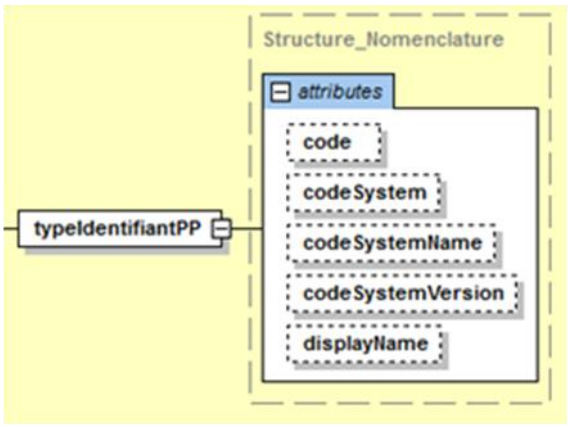


**Figure 24 : Structure de la terminologie de référence type d'identifiant d'une personne physique**

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

Les terminologies de référence (NAS-RES-TERMI) utilisées dans le cadre de MSSanté sont disponibles sur http://esante.gouv.fr/services/referentiels/identification/nomenclature-des-acteurs-de-sante (cf. l'archive ZIP dans le tableau « Documents associés »).

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**<br>**Compétences exclusives**<br>**Qualification PAC** | R38<br>R40<br>R44 | RNR_R38.tab<br>RNR_R40.tab<br>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**

#### *4.3.1.1.3.4 Gestion des erreurs*

**EX_WSA_5060**

Les spécifications du **§ 4.3.1.1.3.4** (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'annuaire national MSSanté en SOAP, doivent être respectées.

##### *4.3.1.1.3.4.1 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 25 : Exemple de SOAP Fault exception**

Les messages d'erreurs de la couche technique et d'échange sont définis au **§ 7.4.1** « Codes d'erreurs pour les Web Services de l'annuaire national MSSanté en SOAP - couche technique et d'échange ».

#### *4.3.1.1.3.4.2 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.

### *4.3.1.2 Web Services de l'annuaire national MSSanté en REST*

#### 4.3.1.2.1 Encodage et espace de nommage

| **EX_WSA_5070** |
|---|
| Les spécifications du **§ 4.3.1.2.1** 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>/<silo>/<version>/<ressource>*
*[/<id_1>/../<id_N>][?<param_1>=<val_1>&…<param_N>=<val_N>]*

- En bleu la 1ère partie du chemin : obligatoire quelle que soit la ressource manipulée et la méthode HTTP utilisée ;
- En rouge la 2ème partie du chemin : utilisée uniquement pour les GET, les PUT et les DELETE (manipulation d'une ressource unique "identifiée") ;
- En vert les paramètres d'URL : utilisables uniquement (et de manière facultative) pour les GET multi-ressources.

La réponse à une opération réussie a les codes de statut HTTP suivants :

| STATUT | CODE | DESCRIPTION |
|---|---|---|
| 200 | OK | Requête effectuée avec succès et retourne un document XML en réponse |
| 201 | Created | Requête effectuée avec succès et nouvelle instance d'entité créée avec succès |

**Tableau 6 : Codes de statuts HTTP pour les Web Services REST**

#### 4.3.1.2.2 Sécurité et intégrité

| **EX_WSA_5080** |
|---|
| Les spécifications du **§ 4.3.1.2.2** concernant la sécurité et l'intégrité, pour les Web Services de l'annuaire national MSSanté en REST, doivent être respectées. |

La sécurité des échanges entre l'annuaire national MSSanté et les autres applications 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 le document [CI-TR-CLI-LRD].

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

Le contrôle d'accès est réalisé par rapport au DN du certificat d'authentification utilisé par le système initiateur. Pour qu'un système soit autorisé à utiliser les Web Services REST de l'annuaire 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 peuvent reposer 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.

#### 4.3.1.2.3 Description des échanges

Les services permettant d'effectuer des opérations de consultation, création, mise à jour ou suppression sur les ressources sont exposés de la façon suivante :

| VERBE HTTP | CONTEXTE | DESCRIPTION |
|---|---|---|
| **GET** | Multi-ressources | Récupération d'une liste de ressources en fonction des critères de recherche |
| **GET** | Mono-ressource | Récupération d'une ressource unique identifiée |
| **PUT** | Mono-ressource | Mise à jour d'une ressource identifiée |
| **POST** | Mono-ressource | Création d'une nouvelle resource |
| **DELETE** | Mono-ressource | Suppression d'une ressource identifiée |

**Tableau 7 : Exposition des services de consultation, création, mise à jour et suppression de ressources sur l'annuaire national MSSanté**

##### *4.3.1.2.3.1 Principes d'échanges*

| **EX_WSA_5090** |
|---|
| Les spécifications du **§ 4.3.1.2.3.1** (et sous-chapitres) concernant les échanges, pour les Web Services de l'annuaire national MSSanté en REST, doivent être respectées. |

###### *4.3.1.2.3.1.1 Récupération d'une liste de ressources*

***Requête***

Un Web Service REST permettant la récupération d'une liste de ressources doit implémenter la méthode `GET` ou `POST` de l'une des manières suivantes :

- Implémentation A (recherches *simples*), `GET` utilisant les querystrings ; dans ce cas, qui ne doit être réservé qu'aux recherches simples, la syntaxe est la suivante :

*https://<host>/<silo>/<version>/<ressource>[<id_element1>/id_element2>/.../<id_element_N]*
*[?<param1>=<valeur1>&<param2>=<valeur2>...&<paramn>=<valeurn>]*

Le body de la requête est vide ; les paramètres sont facultatifs ;

- Implémentation B (recherches *complexes*), `POST` utilisant un formulaire d'échange : dans ce cas, le fournisseur des ressources propose un formulaire à remplir par l'appelant.

***Réponse***

En cas de succès, la réponse est la suivante :

| STATUT | CODE | DESCRIPTION | ENTÊTE | BODY |
|---|---|---|---|---|
| **200** | OK | La recherche a été effectuée avec succès | | 1 retour contenant 0 à N entrées, chaque entrée contenant une ressource unique |

**Tableau 8 : Réponse du Web Service REST de récupération d'une liste de ressources**

En cas d'échec de l'opération, les codes d'erreur définis au **§ 7.4.2** « Codes d'erreurs pour les Web Services de l'annuaire national MSSanté en REST - couche technique et d'échange » doivent être utilisés.

#### *4.3.1.2.3.1.2 Récupération d'une ressource unique*

***Requête***

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

*https://<host>/<silo>/<version>/<ressource>[<id_element1>/id_element2>/.../<id_element_N]*

Où `id_element1 … id_elementN` sont les éléments permettant de composer l'identifiant unique de la ressource à récupérer.

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 9 : Réponse du Web Service REST de récupération d'une ressource unique**

En cas d'échec de l'opération, les codes d'erreur définis au **§ 7.4.2** « Codes d'erreurs pour les Web Services de l'annuaire national MSSanté en REST - couche technique et d'échange » doivent être utilisés.

#### *4.3.1.2.3.1.3 Mise à jour d'une ressource*

***Requête***

Un Web Service REST permettant la mise à jour d'une ressource doit implémenter la méthode `PUT` de la manière suivante :

*https://<host>/<silo>/<version>/<ressource>[<id_element1>/id_element2>/.../<id_element_N]*

Où `id_element1 … id_elementN` sont les éléments permettant de composer l'identifiant unique de la ressource à mettre à jour.

Le body doit contenir une entry correspondant à la ressource complète à mettre à jour.

Remarque : pour mettre à jour une ressource, une représentation complète est à utiliser, il ne faut pas utiliser un message contenant uniquement les champs à mettre à jour.

***Réponse***

En cas de succès, la réponse est la suivante :

| STATUT | CODE | DESCRIPTION | ENTÊTE | BODY |
|---|---|---|---|---|
| **201** | OK | La ressource a été mise à jour avec succès | Location:URL de la ressource modifiée | |

**Tableau 10 : Réponse du Web Service REST de mise à jour d'une ressource**

En cas d'échec de l'opération, les codes d'erreur définis au **§ 7.4.2** « Codes d'erreurs pour les Web Services de l'annuaire national MSSanté en REST - couche technique et d'échange » doivent être utilisés.

#### *4.3.1.2.3.1.4 Création d'une ressource*

***Requête***

Un Web Service REST permettant la création d'une ressource doit implémenter la méthode `POST` de la manière suivante :

*https://<host>/<silo>/<version>/<ressource>*

Le body doit contenir une entry correspondant à la ressource complète à créer.

***Réponse***

En cas de succès, la réponse est la suivante :

| STATUT | CODE | DESCRIPTION | ENTÊTE | BODY |
|---|---|---|---|---|
| **201** | OK | La ressource a été créée avec succès | Location:URL de la ressource créée | |

**Tableau 11 : Réponse du Web Service REST de création d'une ressource**

En cas d'échec de l'opération, les codes d'erreur définis au **§ 7.4.2** « Codes d'erreurs pour les Web Services de l'annuaire national MSSanté en REST - couche technique et d'échange » doivent être utilisés.

#### *4.3.1.2.3.1.5 Suppression d'une ressource*

***Requête***

Un Web Service REST permettant la suppression d'une ressource doit implémenter la méthode `DELETE` de la manière suivante :

*https://<host>/<silo>/<version>/<ressource>[<id_element1>/id_element2>/.../<id_element_N]*

Où `id_element1 … id_elementN` sont les éléments permettant de composer l'identifiant unique de la ressource à supprimer.

Le body est vide.

***Réponse***

En cas de succès, la réponse est la suivante :

| STATUT | CODE | DESCRIPTION | ENTÊTE | BODY |
|---|---|---|---|---|
| **204** | OK | La ressource a été supprimée avec succès | Location:URL de la ressource supprimée | |

**Tableau 12 : Réponse du Web Service REST de suppression d'une ressource**

En cas d'échec de l'opération, les codes d'erreur définis au **§ 7.4.2** « Codes d'erreurs pour les Web Services de l'annuaire national MSSanté en REST - couche technique et d'échange » doivent être utilisés.

#### *4.3.1.2.3.2 Gestion des erreurs*

**EX_WSA_5100**

Les spécifications du **§ 4.3.1.2.3.2** (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 **§ 7.4.2** « 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 13 : Structure du message d'erreur des Web Services REST**

## 4.4 Publication de BAL MSSanté dans l'annuaire national MSSanté

Remarque : dans cette version du document, seule la transaction TM1.1.P est décrite de manière détaillée.

### 4.4.1 Description fonctionnelle

**EX_PBA_5010**

L'opérateur MSSanté doit obligatoirement implémenter au moins une des trois solutions proposées (TM1.1.1P, TM1.1.2P ou TM1.1.3P) 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 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.

**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.

**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).

Remarque : les opérateurs ont la possibilité de définir les offres qui leur semblent pertinentes, par exemple, en termes de capacité de BAL, de nombre et de taille des pièces jointes, dès lors que celles-ci respectent les exigences définies dans ce DSFT.

***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.

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

***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 du « 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 du « zéro papier » (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) du « zéro papier » ;
- Le numéro de téléphone de l'utilisateur (le cas échéant).

**RE_PBA_5030**

La RFC 5321 précise les bonnes pratiques de notification du statut de remise de message (voir **§ 4.7.1.1** « Cinématique »).

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, détection de virus, etc.), de faire en sorte que cette notification soit facilement interprétable pour l'utilisateur final (habillage spécifique, traduction, etc.).

***Cycle de vie des comptes de messagerie***

**EX_PBA_5060**

Afin de garantir la fiabilité des données publiées dans l'annuaire national MSSanté vis-à-vis des utilisateurs des autres domaines, l'opérateur MSSanté doit être en mesure de gérer le cycle de vie des comptes de messagerie MSSanté des utilisateurs de son domaine, par l'intermédiaire de processus organisationnels et techniques au sein de l'organisation en charge du domaine de messagerie.

**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.

**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 professionnels de santé dûment identifiés dans une base des utilisateurs.

| 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. |

| EX_PBA_5140 |
| --- |
| L'opérateur doit s'assurer que les BAL MSSanté liées à son service de messagerie MSSanté fermées ou supprimées ne soient plus publiées dans l'annuaire national MSSanté. |

| 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. |

| 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). |

| EX_PBA_5070 |
| --- |
| Le format des adresses de messagerie MSSanté doit respecter la RFC 5321 (http://tools.ietf.org/html/rfc5321).<br>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). |

| 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.<br><br>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.<br><br>Voici quelques exemples de règles de nommage :<br><br>• Pour les BAL personnelles :<br>○ prenom.nom@domaine-securise.fr<br>○ prenom.nomn°d'ordre@domaine-securise.fr<br>• Pour les BAL organisationnelles :<br>○ service-nom_du_service@domaine-securise.fr<br>○ service-cardiologie@domaine-securise.fr<br>○ cabinet-dr-martin@domaine-securise.fr<br>○ service-pr-dupont@domaine-securise.fr<br>○ institut-pasteur.secretariat@domaine-securise.fr<br>• Pour les BAL applicatives (pour des BAL rattachées à des applications ou des machines) :<br>○ automate_biologie_14@domaine-securise.fr<br>○ dispositif_médical_XYZ@domaine-securise.fr<br>○ notification_SIH_ABC@domaine-securise.fr |

®

#### *4.4.1.1 BAL rattachées à des personnes physiques*

Dans le cas des BAL rattachées à des personnes physiques, les données de description suivantes doivent être fournies par l'opérateur (la spécification détaillée du flux d'alimentation est décrite au **§ 4.4.2.2.3** « Principe de construction du flux d'alimentation de l'annuaire national MSSanté ») :

- Type de BAL ;
- Adresse BAL MSSanté ;
- Type d'identifiant personne physique ;
- Identifiant personne physique ;
- Type d'identifiant de la structure d'activité (à renseigner dans le cas des BAL personnelles avec identifiant interne à la structure d'activité) ;
- Identifiant de la structure d'activité (à renseigner dans le cas des BAL personnelles avec identifiant interne à la structure d'activité) ;
- Service de rattachement de l'utilisateur dans l'organisation ;
- Civilité d'exercice (à renseigner dans le cas des BAL personnelles avec identifiant interne à la structure d'activité et uniquement pour les professions de médecin, pharmacien, chirurgien-dentiste) ;
- Nom d'exercice ;
- Prénom d'exercice ;
- Profession (à renseigner dans le cas des BAL personnelles avec identifiant interne à la structure d'activité) ;
- Spécialité (à renseigner, le cas échéant, dans le cas des BAL personnelles avec identifiant interne à la structure d'activité) ;
- N° de téléphone ;
- Acceptation de la dématérialisation (zéro papier) ;
- Présence en liste rouge.

**EX_PBA_5090**

L'identifiant du titulaire d'une BAL MSSanté transmis par l'opérateur lors de l'alimentation de l'annuaire national MSSanté doit 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.

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).

Dans le cas d'un professionnel de santé ne disposant pas de numéro d'identification national (en particulier professionnel de santé en formation), 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 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.

Remarques :

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

**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.

#### *4.4.1.2 BAL applicatives et organisationnelles*

Dans le cas des BAL applicatives ou organisationnelles, les données de description suivantes doivent être fournies par l'opérateur (la spécification détaillée du flux d'alimentation est décrite au **§ 4.4.2.2.3** « Principe de construction du flux d'alimentation de l'annuaire national MSSanté ») :

- Type de BAL ;
- Adresse BAL MSSanté ;
- Type d'identifiant de la structure d'activité gérant la BAL ;
- Identifiant de la structure d'activité ;
- Service de rattachement de la BAL dans l'organisation ;
- Responsable au niveau opérationnel de la BAL ;
- Description de la BAL ;
- N° de téléphone ;
- Acceptation de la dématérialisation (zéro papier) ;
- Présence en liste rouge.

Remarque : 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.

| **EX_PBA_5080** |
| --- |
| L'opérateur doit s'assurer que les destinataires « machines » sont en mesure d'exploiter des messages de type « indicateur d'absence » ou « message de saturation de BAL » afin de pouvoir déclencher à leur suite les actions appropriées. |

| **EX_PBA_5160** |
| --- |
| Le ou les professionnels indiqués en tant que responsables au niveau opérationnel d'une BAL Organisationnelle ou Applicative doivent être des professionnels habilités à échanger des données de santé personnelles. |

### 4.4.2 TM1.1.xP - Mise à jour des BAL dans l'annuaire national MSSanté

#### *4.4.2.1 Interfaces techniques de mise à jour de l'annuaire national MSSanté*

Deux types d'interfaces de mise à jour de l'annuaire national MSSanté sont proposés :

- Web Service, avec authentification par certificat logiciel de personne morale délivré par l'ASIP Santé, qui permet les mises à jour en mode :
  - Global sur le domaine : de type « annule et remplace » ;
  - Différentiel : de type ajout et suppression d'enregistrements ;
- Transfert de fichiers XML et CSV par interface Web, avec authentification nominative par carte de la famille CPS, qui permet les mises à jour en mode global sur le domaine (« annule et remplace ») ; dans ce cas de figure, les utilisateurs habilités sont enregistrés (par l'ASIP Santé) dans le système MSSanté et un contrôle d'accès applicatif est mis en place au niveau de l'annuaire national MSSanté.

**EX_1.1_5010**

Plusieurs modalités de mise à jour des comptes de messagerie dans l'annuaire national MSSanté sont prévues et détaillées dans les chapitres suivants. Il est exigé que le Proxy de messagerie MSSanté mette en œuvre au moins l'une des modalités proposées.

#### *4.4.2.2 TM1.1.1P - Web Service en mode global*

**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 **§ 4.4.2.2** (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 la structure.

| RE_1.1.1_5010 |
| --- |
| Il est recommandé d'utiliser le Web Service en mode global pour les volumes de données importants et de recourir au Web Service en mode différentiel pour les petits volumes. |

| RE_1.1.1_5020 |
| --- |
| Il est recommandé que l'envoi des BAL soit effectué :<br>• Si au moins une modification (ajout, mise à jour, suppression) de compte est identifiée dans l'annuaire interne de la structure ;<br>• Pas plus d'une fois par jour. |

#### 4.4.2.2.1 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.

#### 4.4.2.2.2 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 la demande |
| **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 14 : 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.<br>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<br>SA6<br>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<br>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 :<br>• Génère un ticket horodaté qu'il attribue au flux ;<br>• Dépose le fichier d'alimentation dans un sas de stockage en l'horodatant. sans contrôle de cohérence des informations transmises ; le batch d'alimentation traitera les fichiers dans l'ordre de cet horodatage ; le nom du fichier d'alimentation contient le DN du certificat de l'opérateur et la date de dépôt du fichier (*aaaammjjhhmmss)* ;<br>• Envoie en réponse au système initiateur le numéro de ticket généré pour le suivi des demandes d'alimentation. | SA5 |

**Tableau 15 : 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 16 : Scénarios alternatifs d'utilisation du Web service global**

#### 4.4.2.2.3 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 **§ 7.3.2** « Documents de référence pour les services ».

##### *4.4.2.2.3.1 Présentation du flux d'alimentation – en entrée de l'annuaire national MSSanté*

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

- Une structure d'en-tête qui contient des informations d'identification et d'authentification (voir **§ 4.3.1.1.3.3.1** « En-tête du message ») ;
- 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 – `COMPTEMSS`.

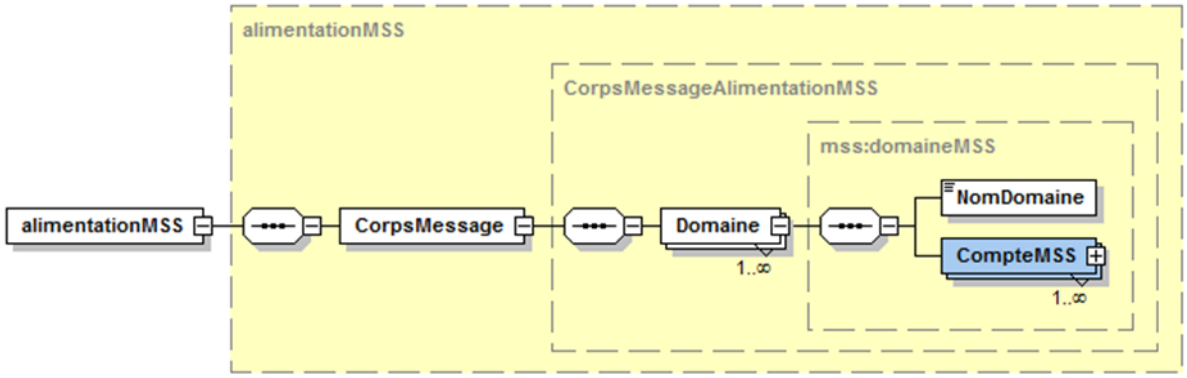


**Figure 26 : Corps du message d'alimentation des comptes MSSanté d'un domaine**

#### *4.4.2.2.3.2 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 17 : Structure du domaine des BAL MSSanté**

#### *4.4.2.2.3.3 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 :<br>• ORG pour BAL Organisationnelle<br>• APP pour BAL Applicative<br>• PER pour BAL Personnelle | Oui | X(3) | Une BAL de type PER est rattachée à une personne physique.<br>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<br>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<br>RG_CTR_004<br>RG_CTR_044<br>RG_CTR_046 |
| TypeIdentifiantPP | Identifiant RPPS, identifiant ADELI, identifiant interne.<br>Valeurs possibles :<br>• 0 si ADELI<br>• 8 si RPPS<br>• 10 si identifiant interne | Oui pour un type de BAL PER<br>Non pour les autres types | | Nomenclature :<br>**CodeSystemName =** G08<br>**CodeSystem =** 1.2.250.1.71.1.2.15 | RG_CTR_005<br>RG_CTR_006<br>RG_CTR_037 |
| IdentifiantPP | Identifiant RPPS, identifiant ADELI ou identifiant interne (si type 10) | Oui pour un type de BAL PER<br>Non pour les autres types | ADELI :X(9)<br>RPPS : X(11)<br>Interne : X(256) | Dans le cas d'un identifiant interne, il s'agira de l'adresse de la BAL | RG_CTR_007<br>RG_CTR_008<br>RG_CTR_035<br>RG_CTR_045 |
| TypeIdentifiantPM | Type de structure à laquelle la BAL est associée.<br>Valeurs possibles :<br>• 1 si FINESS<br>• 2 si SIREN<br>• 3 si SIRET | Oui pour un type de BAL APP ou ORG et pour type de BAL PER avec un identifiant interne (type 10) | | Nomenclature : TypeIdentifiantPM<br>**CodeSystemName =** G07<br>**CodeSystem =** 1.2.250.1.71.1.2.14<br><br>Cet attribut est facultatif pour les BAL de type PP (RPPS/ADELI) 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<br>RG_CTR_011<br>RG_CTR_012<br>RG_CTR_015<br>RG_CTR_038<br>RG_CTR_039 |
| IdentifiantPM | Numéro FINESS EJ ou EG ou le numéro SIREN ou le numéro SIRET | Oui pour un type de BAL APP et ORG et pour type de BAL PER avec un identifiant interne (type 10) | X(32) | L'identifiant de structure ne correspond pas obligatoirement à une structure associée à une situation d'exercice.<br><br>Cet attribut est facultatif pour les BAL de type PP (RPPS/ADELI) mais il est possible de le fournir afin de pouvoir associer la BAL spécifiquement à | RG_CTR_013<br>RG_CTR_014<br>RG_CTR_016<br>RG_CTR_033<br>RG_CTR_034 |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE | REGLES DE CONTROLE |
|---|---|---|---|---|---|
| | | | | une structure donnée lors des recherches sur l'annuaire. | |
| ServiceRattachement | Nom et description du service de rattachement de l'utilisateur dans l'organisation | Non | X(160) | Texte libre<br><br>Cet attribut permet de renseigner le service de rattachement de l'utilisateur (PP) ou de la BAL (PM) dans l'organisation.<br><br>Pour les BAL de type PP RPPS/ADELI, 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 - uniquement pour le type de BAL PER avec un identifiant interne (type 10) | | Nomenclature : CiviliteExercice<br>**CodeSystemName =** R11<br>**CodeSystem =** 1.2.250.1.213.1.6.1.11<br><br>Attribut non renseigné pour les BAL autres que BAL PER avec un identifiant interne (type 10).<br><br>La civilité d'exercice ne concerne que les professions de médecin, pharmacien, chirurgien-dentiste.<br><br>La liste des civilités d'exercice autorisées pour les professions médecin, pharmacien, et chirurgien-dentiste sont les suivantes :<br><br>Médecin : PR (Professeur) / MG (Médecin Général) / MC (Médecin chef) / DR (Docteur)<br><br>Pharmacien : PR (Professeur) / PC (Pharmacien Chef) / PG (Pharmacien Général) / DR (Docteur)<br><br>Chirurgien-dentiste : PR (Professeur) / DR (Docteur) | RG_CTR_017<br>RG_CTR_018<br>RG_CTR_040 |
| NomExercice | Nom de la situation d'exercice de l'utilisateur | Oui pour le type de BAL PER | X(80) | Attribut non renseigné pour les BAL de type ORG ou APP | RG_CTR_019<br>RG_CTR_021 |
| PrenomExercice | Prénom de la situation d'exercice de l'utilisateur | Oui pour le type de BAL PER | X(50) | Attribut non renseigné pour les BAL de type ORG ou APP | RG_CTR_020<br>RG_CTR_021 |
| CategorieProfession | Catégorie de professions de l'utilisateur | Oui - uniquement pour le | | Nomenclature : CatégorieDeProfessions | RG_CTR_022 |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE | REGLES DE CONTROLE |
|---|---|---|---|---|---|
| s | | type de BAL PER avec un identifiant interne (type 10) | | **CodeSystemName =** R37<br>**CodeSystem =** 1.2.250.1.213.1.6.1.3<br><br>Attribut non renseigné pour les BAL autres que BAL PER avec un identifiant interne (type 10). | RG_CTR_023<br>RG_CTR_024<br>RG_CTR_041 |
| Profession | Profession de l'utilisateur | Oui - uniquement pour le type de BAL PER avec un identifiant interne (type 10) | | Nomenclature : Profession<br>**CodeSystemName =** G15<br>**CodeSystem =** 1.2.250.1.71.1.2.7<br><br>Attribut non renseigné pour les BAL autres que BAL PER avec un identifiant interne (type 10). | RG_CTR_025<br>RG_CTR_026<br>RG_CTR_042 |
| Specialite | Spécialité de l'utilisateur | Facultatif - uniquement pour les PP médecin et chirurgien-dentiste pour le type de BAL PER avec un identifiant interne (type 10) | | Nomenclature : Jeux de valeurs Spécialité<br>CodeSystemName **=** R38<br>**CodeSystem =** 1.2.250.1.213.2.28<br>ou<br>CodeSystemName **=** R40<br>**CodeSystem =** 1.2.250.1.213.2.30<br>ou<br>CodeSystemName **=** R44<br>**CodeSystem =** 1.2.250.1.213.2.34<br><br>Attribut non renseigné pour les BAL autres que BAL PER avec un identifiant interne (type 10).<br><br>Cet attribut correspond à la spécialité ordinale et est dépendant de la profession ("médecin" ou "chirurgien-dentiste"), la compétence exclusive ou qualification PAC le cas échéant. | RG_CTR_027<br>RG_CTR_028<br>RG_CTR_043 |
| Responsable | Texte libre donnant les coordonnées de la (ou des) personne(s) responsable(s) au niveau opérationnel de la BAL.<br><br>Exemples : le chef de service, l'administrateur de l'application | Oui pour la BAL de type ORG ou APP | X(160) | Attribut obligatoire pour les BAL de type ORG et APP ; non renseigné pour les BAL de type PER | RG_CTR_029 |
| Description | Description fonctionnelle de la BAL | Oui pour la BAL de type ORG ou APP | X(160) | Attribut obligatoire pour les BAL de type ORG et APP ; non renseigné pour les BAL de type PER | RG_CTR_030 |
| Telephone | Téléphone (de type fixe ou mobile) lié aux BAL (PER, ORG ou APP) | Non | X(20) | Attribut facultatif pour tout type de BAL (PER, ORG ou APP) | |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE | REGLES DE CONTROLE |
|---|---|---|---|---|---|
| Dematerialisation | Indicateur d'acceptation de la dématérialisation.<br>Valeurs possibles :<br>O – dématérialisation acceptée<br>N – dématérialisation refusée | Oui | X(1) | Attribut obligatoire pour tout type de BAL (PER, ORG ou APP) | RG_CTR_031 |
| ListeRouge | Indicateur liste rouge<br>Valeurs possibles :<br>O – le PP/PM a demandé l'intégration de l'adresse MSSanté dans la liste rouge, dans ce cas l'adresse MSSanté n'est pas publiée<br>N – L'adresse MSSanté peut être publiée | Oui | X(1) | Attribut obligatoire pour tout type de BAL (PER, ORG ou APP) | RG_CTR_032 |

**Tableau 18 : Structure des comptes de messagerie MSSanté**

#### *4.4.2.2.3.4 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 **§ 4.3.1.1.3.4** « Gestion des erreurs ») – `FAULT`.

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


**Figure 27 : Message d'accusé de réception ou SOAP Fault**

### 4.4.2.2.4 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.

#### 4.4.2.2.5 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 comptes-rendus sont produits au fil de l'eau dans l'ordre de traitement des messages.

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

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

Le fichier ZIP contient deux fichiers :

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

Le fichier XML contient les données du compte-rendu.

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

| **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. |

| | |
|---|---|
| **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 :<br>• Un fichier XML comportant le compte-rendu d'alimentation ;<br>• 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** | 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 19 : 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 :<br>• En établissant une session TLS avec authentification mutuelle ;<br>• En passant en paramètre le numéro du ticket attribué par l'annuaire national MSSanté.<br>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 :<br>• Récupère le fichier XML de compte-rendu rattaché au ticket (ainsi que le fichier TXT contenant l'empreinte du fichier XML) ;<br>• 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 20 : 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 21 : Scénarios alternatifs d'utilisation du Web Service de récupération de compte-rendu de traitement**

#### *4.4.2.2.5.1 Principe de construction du flux*

##### *4.4.2.2.5.1.1 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`.

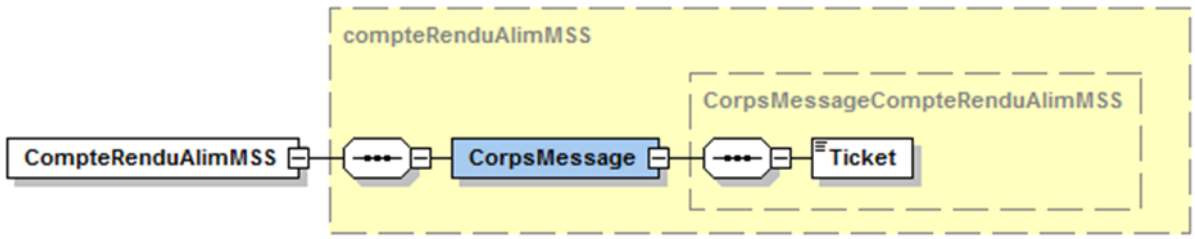


**Figure 28 : Corps du message pour la recherche de compte-rendu de traitement**

##### *4.4.2.2.5.1.2 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`.

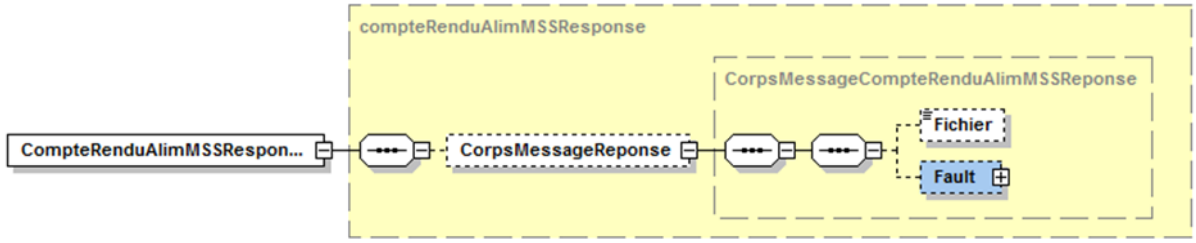


**Figure 29 : Corps du message pour la réponse du Web Service de recherche d'un compte-rendu**

#### *4.4.2.2.5.1.3 Description du fichier de compte-rendu d'alimentation*

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

Ce fichier est structuré en :

- Un bloc d'en-tête qui comporte :
  - Le numéro de ticket (pour rappel) ;
  - La liste des règles de contrôle appliquées (pour les règles de contrôle pouvant être modifiées) ;
- 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 22 : 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<br>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 23 : Bloc d'en-tête, structure de la liste des contrôles**

Remarque : seule la règle RG_CTR_021 (MSS020) est intégrée au compte-rendu d'alimentation dans la version actuelle de l'annuaire national MSSanté.

### *Structure – Domaine*

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

**Tableau 24 : 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 25 : 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 :<br>• ORG pour la BAL Organisationnelle<br>• APP pour la BAL Applicative<br>• PER pour la BAL Personnelle | Non | X(3) | La BAL de type PER est rattachée à une personne physique<br>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) |
| TypeIdentifiantPP | Identifiant RPPS, ADELI, interne | Non | X(2) | Nomenclature : |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE |
|---|---|---|---|---|
| | à la structure d'activité.<br>Valeurs possibles :<br>• 0 si ADELI<br>• 8 si RPPS<br>• 10 si identifiant interne | | | TypeIdentifiantPP<br>**CodeSystemName =** G08<br>**CodeSystem =** 1.2.250.1.71.1.2.15 |
| IdentifiantPP | Identifiant RPPS ou ADELI du titulaire de la BAL ou identifiant interne (si type 10) | Non | X(256) | Les attributs « IdentifiantPP » et « TypeIdentifiantPP) sont renseignés avec les valeurs indiquées dans le fichier d'alimentation transmis par l'opérateur. |
| TypeIdentifiantPM | Type de structure à laquelle la BAL est associée.<br>Valeurs possibles :<br>• 1 si FINESS<br>• 2 si SIREN<br>• 3 si SIRET | Non | X(2) | Nomenclature :<br>TypeIdentifiantPM<br>**CodeSystemName =** G07<br>**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<br>Sinon n'est pas renseigné | X(80) | Remarque : 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<br>Sinon n'est pas renseigné | X(50) | |
| TypeIdentifiantPPAnnuaire | 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<br>Sinon n'est pas renseigné | X(2) | Nomenclature :<br>TypeIdentifiantPP<br>**CodeSystemName** = G08<br>**CodeSystem** = 1.2.250.1.71.1.2.15 |
| IdentifiantPPAnnuaire | Identifiant national connu dans l'annuaire national MSSanté | | X(256) | |

**Tableau 26 : Bloc de détail, structure des anomalies détectées**

La liste des contrôles effectués, des codes d'erreurs et des messages associés est définie au **§ 7.4.3** « 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 **§ 7.3.2** « Documents de référence pour les services ».

#### *4.4.2.3 TM1.1.2P - Web Service en mode différentiel [AC]*

Le Web Service en mode différentiel permet d'envoyer à l'annuaire national MSSanté une liste de BAL MSSanté avec pour chacune d'elle le type d'action à réaliser : ajout ou suppression.

#### *4.4.2.4 TM1.1.3P - Transfert de fichier en mode Web [AC]*

Le chargement complet de la liste des BAL MSSanté d'un domaine dans l'annuaire national MSSanté est proposé également sous la forme d'un transfert de fichier en mode Web.

Dans ce cas d'usage, l'opérateur (en pratique : un intervenant avec un rôle de gestionnaire de BAL du domaine) envoie à l'annuaire national MSSanté un fichier, au format XML ou CSV, comprenant la liste exhaustive des BAL MSSanté. Le traitement de ces informations entraîne dans l'annuaire national MSSanté :

1) Une suppression des BAL MSSanté tels qu'elles étaient connues pour le domaine ;
2) Un remplacement par les nouvelles données contenues dans le fichier.

Dans ce mode de fonctionnement, le gestionnaire des BAL du domaine MSSanté 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 la structure.

## 4.5 Consultation de l'annuaire national MSSanté

| **EX_2.1_5010** |
| --- |
| L'opérateur MSSanté doit obligatoirement implémenter au moins une des trois solutions disponibles (TM2.1.1A, TM2.1.2A ou TM2.1.3A) afin que les utilisateurs du système MSSanté puissent sélectionner de manière sûre et aisée les destinataires de leurs messages. |

### 4.5.1 TM2.1.1A et TM2.1.2A - Consultation de l'annuaire national MSSanté

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 Proxy Annuaire 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 Proxy annuaire 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. |

#### *4.5.1.1 Modalités prévues d'interrogation de l'annuaire national MSSanté*

La recherche de correspondants dans l'annuaire national MSSanté peut être exécutée selon plusieurs modalités techniques, en utilisant au choix :

- Le protocole LDAP ;
- Un Web Service de recherche spécifique.

#### 4.5.1.2 TM2.1.1A - Interrogation de l'annuaire national MSSanté par le protocole LDAP

Les spécifications liées à l'interrogation de l'annuaire national MSSanté pour le protocole LDAP sont définies dans le DST clients de messagerie.

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. |

#### 4.5.1.3 TM2.1.2A - Interrogation de l'annuaire national MSSanté par Web Service *[AC]*

L'interrogation de l'annuaire national MSSanté peut-être réalisée par Web Service.

### 4.5.2 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 **§ 4.5.2** (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.

#### 4.5.2.1 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 **§ 7.3.2** « 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 : date de clôture non renseignée. | Règle de sélection |
| Les informations extraites sont triées dans l'ordre suivant : par domaine, par identifiant de personne physique, par identifiant de personne morale, par BAL. | Tri |
| Les extractions sont transmises sous forme d'un fichier compressé d'extension .zip basé sur l'algorithme « deflate ».<br>Le fichier zip contient deux fichiers :<br>• Un fichier nommé « ExtractionMSSGlobale_AAAAMMJJHHmmss.xml » ;<br>• Un fichier nommé « ExtractionMSSGlobale_AAAAMMJJHHmmss_checksum.txt ».<br>Le fichier XML contient les données extraites.<br>Le fichier TXT contient l'empreinte du fichier XML calculé avec l'algorithme SHA256. Il permet de vérifier l'intégrité du fichier XML avant utilisation. Cette vérification est optionnelle. | Format du fichier |
| Les fichiers d'extraction sont libellés *« ExtractionMSSGlobale_AAAAMMJJHHmmss»,* où *AAAAMMJJHHmmss* est la date et heure de création des fichiers. | Nom du fichier |
| L'identifiant PM (type et valeur) extrait est en priorité le n° FINESS, s'il existe ; sinon, il s'agit du n° SIRET pour une entité géographique ou du n° SIREN pour une entité juridique. | Identifiant PM |
| Données relatives aux structures extraites pour les BAL personnelles :<br>• 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 ;<br>• 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.<br>Remarques :<br>• Dans le cas où la personne aurait plusieurs activités ouvertes dans une même structure, cette structure ne serait extraite qu'une fois ;<br>• Une BAL peut être extraite sans aucune donnée sur la structure (cas où la personne n'aurait aucune activité ouverte). | Structures extraites pour des BAL personnelles |
| Les données extraites relatives à l'exercice professionnel (nom et prénom d'exercice, civilité d'exercice, catégorie de profession, profession) sont celles de l'exercice professionnel le plus récemment ouvert ou le plus récemment fermé (si aucun exercice n'est ouvert à la date de l'extraction). | Données de l'exercice professionnel |
| Pour des personnes possédant plusieurs savoir-faire :<br>• Pour les médecins, le seul savoir-faire extrait est celui de type S, CEX ou PAC (spécialité, compétence exclusive, qualification PAC) ;<br>• Pour les chirurgiens-dentistes, le savoir-faire extrait est celui de type S, s'il existe (sinon aucun savoir-faire n'est extrait).<br>Pour les autres professions aucun savoir-faire n'est extrait. | Données du savoir-faire |
| Les adresses (postales) extraites sont celles des structures | Adresse |

**Tableau 27 : Règles d'extraction du fichier des BAL MSSanté**

#### 4.5.2.2 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 :<br>• Un fichier XML comportant une extraction globale de l'ensemble des BAL MSSanté publiables ;<br>• 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. |
| **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 28 : Cas d'utilisation du Web Service de téléchargement des BAL MSSanté**

#### *Scénario principal*

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

**Tableau 29 : 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 :<br>401 Access Denied | |

**Tableau 30 : Scénarios alternatifs d'utilisation du Web Service de téléchargement des BAL MSSanté**

### *4.5.2.3 Principe de construction du flux d'extraction de l'annuaire national MSSanté*

#### 4.5.2.3.1 Présentation du flux d'entrée

L'appel se fait via URL :

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

#### 4.5.2.3.2 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 31 : 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 :

| ELÉMENT | DESCRIPTION | TYPE | OBLIGATOIRE |
|---|---|---|---|
| Extraction | L'extraction au format demandé encodé en base 64 | xsd:base64Binary | Oui |

**Tableau 32 : Corps de la réponse du Web Service de demande de téléchargement de l'extraction de l'annuaire national MSSanté en cas de succès**

#### 4.5.2.3.3 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<br>Le format n'est pas valide (csv, xml, ldif, 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<br>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 33 : Réponse du Web Service de demande de téléchargement de l'extraction de l'annuaire national MSSanté en cas d'erreur**

#### 4.5.2.3.4 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 :<br>• ORG pour une BAL Organisationnelle<br>• APP pour une BAL Applicative<br>• PER pour une BAL Personnelle | Oui | X(3) | |
| ADRESSEBAL | Adresse unique de messagerie dans un domaine de messagerie MSSanté | Oui | X(256) | |
| TYPEIDENTIFANTPP | Identifiant RPPS, ADELI, interne à la structure d'activité.<br>Valeurs possibles :<br>• 0 si ADELI<br>• 8 si RPPS<br>• 10 si identifiant interne | Oui pour une BAL de type PER<br>Non pour les autres types | | Nomenclature : TypeIdentifiantPP<br>**CodeSystemName =** G08<br>**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) | Oui pour une BAL de type PER<br>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.<br>Valeurs possibles :<br>• 1 si FINESS<br>• 2 si SIREN<br>• 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<br>**CodeSystemName =** G07<br>**CodeSystem =** 1.2.250.1.71.1.2.14 |
| IDENTIFIANTPM | Numéro FINESS EJ ou EG, ou le numéro SIREN, ou le numéro SIRET | Oui pour une BAL de type ORG ou APP et pour type de BAL PER avec un identifiant interne (type 10) | X(32) | |
| SERVICERATTACHEMENT | Nom et description du service de rattachement de l'utilisateur dans | Non | X(160) | Il s'agit du service de rattachement de l'utilisateur (PP) ou de la BAL (PM) dans l'organisation. |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE |
|---|---|---|---|---|
| | l'organisation | | | |
| NCIVILITEEXERCICE | Civilité de la situation d'exercice de l'utilisateur | Non | | Nomenclature : CiviliteExercice<br>**CodeSystemName =** R11<br>**CodeSystem =** 1.2.250.1.213.1.6.1.11<br><br>La civilité d'exercice ne concerne que les professions de médecin, pharmacien, chirurgien-dentiste. |
| NOMEXERCICE | Nom de la situation d'exercice de l'utilisateur | Oui pour une BAL de type PER | X(80) | |
| PRENOMEXERCICE | Prénom de la situation d'exercice de l'utilisateur | 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<br>**CodeSystemName =** R37<br>**CodeSystem =** 1.2.250.1.213.1.6.1.3 |
| NPROFESSION | Profession de l'utilisateur | Oui pour une BAL de type PER | | Nomenclature : Profession<br>**CodeSystemName =** G15<br>**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<br>**CodeSystemName =** R38<br>**CodeSystem =** 1.2.250.1.213.2.28<br>Ou<br>**CodeSystemName =** R40<br>**CodeSystem =** 1.2.250.1.213.2.30<br>Ou<br>**CodeSystemName =** R44<br>**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) | |
| DEMATERIALISATION | Indicateur d'acceptation de la dématérialisation.<br>Valeurs possibles :<br>O – dématérialisation acceptée<br>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) | |
| L2COMPLEMENTLOCALISATION | Ligne 2 de l'adresse<br>Complément d'identification du destinataire ou du point de remise : personne, N° d'appartement, escalier… | Non | X(38) | |
| L3COMPLEMENTDISTRIBUTION | Ligne 3 de l'adresse<br>Complément d'identification du point géographique : entrée, Tour, Résidence, Zone industrielle… | Non | X(38) | |
| L4NUMEROVOIE | Ligne 4 de l'adresse | Non | X(4) | |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE |
|---|---|---|---|---|
| | N° de la voie | | | |
| L4COMPLEMENTNUMEROVOIE | Ligne 4 de l'adresse<br>Indice de répétition du n° dans la voie : bis, ter… | Non | X(3) | |
| NL4TYPEVOIE | Type de voie | Non | | Nomenclature : TypeVoie<br>**CodeSystemName =** R35<br>**CodeSystem =** 1.2.250.1.213.2.44 |
| L4LIBELLEVOIE | Ligne 4 de l'adresse<br>Libellé de la voie : Nom de la rue, de l'avenue | Non | X(38) | |
| L5LIEUDITMENTION | Ligne 5 de l'adresse<br>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 | | Nomenclature : CodePostal<br>**CodeSystemName =** R76<br>**CodeSystem =** 1.2.250.1.213.2.45 |
| NCOMMUNE | Commune | Non | | Nomenclature : Commune<br>**CodeSystemName =** R13<br>**CodeSystem =** 1.2.250.1.213.2.23 |
| NDEPARTEMENT | Département | Non | | Nomenclature : Département<br>**CodeSystemName =** G09<br>**CodeSystem =** 1.2.250.1.71.1.2.16 |
| NPAYS | Pays | Non | | Nomenclature : Pays<br>**CodeSystemName =** R20<br>**CodeSystem =** 1.2.250.1.213.2.24 |

**Tableau 34 : Liste des attributs présents dans le fichier d'extraction des comptes MSSanté**

### 4.5.3 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 **§ 4.5.3** (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.

#### *4.5.3.1 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 |
| <u>Professionnels de Santé RPPS</u> :<br>Pour les professionnels de santé civils de profession : Sage-femme, médecin, chirurgien-dentiste, sont extraits uniquement les PS inscrits à l'Ordre.<br>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).<br>Pour les professionnels de santé militaires, sont extraits les PS ayant au moins un exercice professionnel.<br><br><u>Professionnels de Santé non RPPS</u> :<br>Ensemble des professionnels de santé non RPPS porteurs ou non porteurs d'une carte CPS ayant une situation d'exercice active. | Règle de sélection |
| Les données extraites, liées aux personnes physiques, sont les données qui se rapportent à une situation d'exercice active. | Données de l'exercice professionnel |
| Pour un PS ayant plusieurs situations d'exercice actives, l'extraction comporte autant de lignes que de situations d'exercice : 1 ligne par situation d'exercice. | Tri |
| Un PS sans structure d'activité (PS remplaçant par ex) ou sans activité sera extrait sans identifiant de structure, ni adresse. | Tri |
| Seuls sont restitués les identifiants de structure de type 1, 2 et 3 (FINESS, SIRET ou SIREN). | Données liées aux Structures |

| Description | Concerne |
|---|---|
| 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). | |
| L'identifiant PM (type et valeur) extrait est en priorité le n° FINESS, s'il existe ; sinon, il s'agit du n° SIRET pour une entité géographique ou du n° SIREN pour une entité juridique. | Identifiant PM |
| Pour des personnes possédant plusieurs savoir-faire :<br>• Pour les médecins, le seul savoir-faire extrait est celui de type S (Spécialité), CEX (compétence exclusive) ou PAC (qualification PAC) ;<br>• Pour les chirurgiens-dentistes, le savoir-faire extrait est celui de type S (Spécialité) s'il existe (sinon aucun savoir-faire n'est extrait).<br><br>Pour les autres professions aucun savoir-faire n'est extrait. | Données du savoir-faire |
| Les adresses (postales) extraites sont celles des structures. | Adresse |
| Le fichier d'extraction des données des personnes physiques **porteuses de carte CPS** est nommé :<br>• « extraction_identites_Avec_CPS_aaaammjjhhmm.csv ».<br><br>Le fichier d'extraction des données des personnes physiques **non porteuses de carte CPS** est nommé :<br>• « extraction_identites_Sans_CPS_ aaaammjjhhmm.csv ».<br><br>Où aaaammjjhhmm est la date et heure de création du fichier. | Nom des fichiers |
| Les fichiers sont mis à disposition sous forme d'un fichier compressé d'extension .zip basé sur l'algorithme « deflate ».<br>Le fichier ZIP est nommé « extraction_identites_ aaaammjjhhmm.zip ».<br><br>Le fichier ZIP contient quatre fichiers :<br>• « extraction_identites_Avec_CPS_aaaammjjhhmm.csv » ;<br>• « extraction_identites_Sans_CPS_aaaammjjhhmm.csv » ;<br>• « extraction_identites_Avec_CPS_aaaammjjhhmm_checksum.txt » ;<br>• « extraction_identites_Sans_CPS_aaaammjjhhmm_checksum.txt ».<br><br>Les fichiers CSV contiennent les données d'identités définies précédemment.<br>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.<br><br>Remarque : l'ensemble des fichiers sont donc disponible via une seule transaction qui récupère en sortie le fichier zip. | Format du fichier |
| Les données sont séparées par le caractère « ; » | Séparateur de données |
| La restitution des données est réalisée en colonne et l'ordre de présentation des attributs dans les fichiers est identique à l'ordre du tableau « Liste des attributs présents dans les fichiers des données d'identités ». | Ordre de présentation des données |
| La première ligne du fichier contient le nom des attributs. | Ligne d'en-tête |
| Le fichier d'extraction des données des personnes physiques est généré chaque jour. | Fréquence de mise à disposition |

**Tableau 35 : Règles d'extraction des fichiers des données d'identités des futurs utilisateurs finaux**

### 4.5.3.2 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 :<br>• « extraction_identites_Avec_CPS_aaaammjjhhmm.csv » ;<br>• « extraction_identites_Sans_CPS_aaaammjjhhmm.csv » ;<br>• « extraction_identites_Avec_CPS_aaaammjjhhmm_checksum.txt » ;<br>• « 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 36 : Cas d'utilisation du Web Service de récupération des fichiers des données d'identités**

### Scénario principal

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

**Tableau 37 : 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 :<br>401 Access Denied | |

**Tableau 38 : Scénarios alternatifs d'utilisation du Web Service de récupération des fichiers des données d'identités**

#### *4.5.3.3 Principe de construction du flux d'extraction de l'annuaire national MSSanté*

##### 4.5.3.3.1 Présentation du flux d'entrée

L'appel se fait via URL :

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

##### 4.5.3.3.2 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 39 : Réponse du Web Service de récupération des fichiers des données d'identités en cas de succès**

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

| ELÉMENT | DESCRIPTION | TYPE | OBLIGATOIRE |
|---|---|---|---|
| Extraction | L'extraction au format demandé encodé en base 64 | xsd:base64Binary | Oui |

**Tableau 40 : Corps de la réponse du Web Service de récupération des fichiers des données d'identités en cas de succès**

#### 4.5.3.3.3 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<br>Le format n'est pas valide (csv, xml, ldif, 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 41 : Réponse du Web Service de récupération des fichiers des données d'identités en cas d'erreur**

#### 4.5.3.3.4 Format du fichier d'extraction

Les fichiers d'extraction sont libellés :

- extraction_identites_Avec_CPS_aaaammjjhhmm.csv ;
- extraction_identites_Sans_CPS_aaaammjjhhmm.csv.

Remarques :

- La restitution des données est réalisée en colonne et l'ordre de présentation des attributs dans les fichiers est identique à l'ordre du tableau ci-dessous ;
- La première ligne du fichier contient le nom des attributs.

Le tableau ci-dessous liste les attributs extraits :

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE |
|---|---|---|---|---|
| TYPEIDENTIFANTPP | Identifiant RPPS, ADELI<br>Valeurs possibles :<br>• 0 si ADELI<br>• 8 si RPPS | Oui | | Nomenclature : TypeIdentifiantPP<br>**CodeSystemName =** G08<br>**CodeSystem =** 1.2.250.1.71.1.2.15 |
| LIB_TYPEIDENTIFANTPP | Libellé du type d'identifiant | Oui | X(256) | « FullySpecifiedName » associé au code dans la terminologie source (G08) |
| IDENTIFIANTPP | Identifiant RPPS ou ADELI du PP | Oui | X(11) | |
| NCIVILITEEXERCICE | Civilité de la situation d'exercice du PS | Non | | Nomenclature : CiviliteExercice<br>**CodeSystemName =** R11<br>**CodeSystem =** 1.2.250.1.213.1.6.1.11<br>La civilité d'exercice ne concerne que les professions de médecin, pharmacien, chirurgien-dentiste. |
| NOMEXERCICE | Nom de la situation d'exercice du PS | Oui | X(80) | |
| PRENOMEXERCICE | Prénom de la situation d'exercice du PS | Oui | X(50) | |
| NCATEGORIEPROFESSION | Catégorie de profession du PS | Oui | | Nomenclature : CatégorieDeProfessions<br>**CodeSystemName =** R37<br>**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) |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE |
|---|---|---|---|---|
| NPROFESSION | Profession du PS | Oui | | Nomenclature : Profession<br>**CodeSystemName =** G15<br>**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<br>**CodeSystemName =** R38<br>**CodeSystem =** 1.2.250.1.213.2.28<br>ou<br>**CodeSystemName =** R40<br>**CodeSystem =** 1.2.250.1.213.2.30<br>ou<br>**CodeSystemName =** R44<br>**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<br>Valeurs possibles :<br>• 1 si FINESS<br>• 2 si SIREN<br>• 3 si SIRET | Non | | Nomenclature : TypeIdentifiantPM<br>**CodeSystemName =** G07<br>**CodeSystem =** 1.2.250.1.71.1.2.14 |
| LIB_TYPEIDENTIFANTPM | Libellé du type de structure dans laquelle exerce le PS | Non | X(256) | « FullySpecifiedName » associé au code dans la terminologie source (G07) |
| IDENTIFIANTPM | Numéro FINESS EJ ou EG, ou le numéro SIREN, ou le numéro SIRET | Non | X(32) | |
| RAISONSOCIALE | Raison sociale de la Structure d'activité | Non | X (164) | |
| ENSEIGNECOMMERCIALE | Enseigne commerciale de la<br>Structure d'activité | Non | X(50) | |
| L2COMPLEMENTLOCALISATION | Ligne 2 de l'adresse<br>Complément d'identification du destinataire ou du point de remise : personne, N° d'appartement, escalier… | Non | X(38) | |
| L3COMPLEMENTDISTRIBUTION | Ligne 3 de l'adresse<br>Complément d'identification du point géographique : entrée, Tour, Résidence, Zone industrielle… | Non | X(38) | |

| ATTRIBUT | DEFINITION | REQUIS | TYPE | COMMENTAIRE |
|---|---|---|---|---|
| L4NUMEROVOIE | Ligne 4 de l'adresse<br>N° de la voie | Non | X(4) | |
| L4COMPLEMENTNUMEROVOIE | Ligne 4 de l'adresse<br>Indice de répétition du n° dans la voie : bis, ter… | Non | X(3) | |
| NL4TYPEVOIE | Type de voie | Non | | Nomenclature : TypeVoie<br>**CodeSystemName =** R35<br>**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<br>Libellé de la voie : Nom de la rue, de l'avenue | Non | X(38) | |
| L5LIEUDITMENTION | Ligne 5 de l'adresse<br>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 | | Nomenclature : CodePostal<br>**CodeSystemName =** R76<br>**CodeSystem =** 1.2.250.1.213.2.45 |
| NCOMMUNE | Commune | Non | | Nomenclature : Commune<br>**CodeSystemName =** R13<br>**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<br>**CodeSystemName =** G09<br>**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<br>**CodeSystemName =** R20<br>**CodeSystem =** 1.2.250.1.213.2.24 |
| LIB_NPAYS | Nom du pays | Non | X(256) | « FullySpecifiedName » associé au code dans la terminologie source (R20) |

**Tableau 42 : Liste des attributs présents dans les fichiers des données d'identités**

# 4.6 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. **§ 4.7.2** « 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.

## 4.6.1 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.

L'accès à la liste blanche ne nécessite pas d'authentification préalable du Proxy Opérateur MSSanté.

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<br>[-]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 | XMLDSIG | Sans Objet | XMLDSIG |

**Tableau 43 : 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.<br>Exemples:<br>ch-xyz.mssante.fr<br>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 |
| ResponsableContact | Coordonnées de contact de l'opérateur MSSanté | Alphanumérique | 255 | Sans Objet |
| SupportContact | Coordonnées de contact en cas de demande de support auprès de l'opérateur | Alphanumérique | 255 | Sans Objet |
| DateMAJ | Date de mise à jour du domaine dans la liste blanche | DateTime | Sans Objet | xsd:DateTime<br>[-]CCYY-MM-DDThh:mm:ss[Z\|(+\|-)hh:mm]) |

**Tableau 44 : Liste des paramètres du champ « ListeDomaines » de la liste blanche des domaines MSSanté**

**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.

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 **§ 7.3.2** « Documents de référence pour les services ») ;
- Les champs de la liste blanche sont alimentés sur la base des éléments communiqués par l'opérateur dans son contrat d'intégration à l'espace de confiance MSSanté ;
- Si l'opérateur indique une adresse de messagerie pour les champs «SupportContact » ou « ResponsableContact », celle-ci ne doit pas être une adresse MSSanté ;
- Les informations du champ « SupportContact » sont destinées à être publiées sur un portail d'information spécifique de l'ASIP Santé.

### 4.6.2 TM4.1P - Interrogation de la liste blanche des domaines de messagerie MSSanté

| **EX_2.2_5010** |
| --- |
| Le Proxy de messagerie MSSanté doit récupérer **quotidiennement** la dernière version de la liste blanche à l'adresse suivante : https://listeblanche.mssante.fr/listeblanchemssante.xml. |

| **EX_2.2_5030** |
| --- |
| L'exploitation par le Proxy de messagerie 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 Proxys Opérateur MSSanté (par exemple, lors de l'envoi de messages dans l'espace de confiance MSSanté) de la liste blanche. |

### 4.6.3 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/xmldsig-core/) par le schéma XML suivant : http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd.

Le tableau ci-dessous présente les caractéristiques de la signature de la liste blanche des domaines MSSanté :

| Paramètre | Valeur |
|---|---|
| Suite cryptographique utilisée pour calculer la signature | rsa-sha256 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha256) |
| Algorithme de transformation sous forme canonique du contenu à signer | xml-exc-c14n (http://www.w3.org/2001/10/xml-exc-c14n#) |
| Type de signature | Enveloppé (http://www.w3.org/2000/09/xmldsig#enveloped) |
| Algorithme de hachage du contenu à signer | SHA256 (http://www.w3.org/2001/04/xmlenc#sha256) |

**Tableau 45 : Liste des caractéristiques de la signature de la liste blanche des domaines MSSanté**

**EX_2.2_5040**

La vérification de la signature doit se faire systématiquement à l'issue du téléchargement de la liste blanche dans le respect des bonnes pratiques définies par le W3C : http://www.w3.org/TR/xmldsig-bestpractices/#bp-validate-signing-key.

**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 **§ 7.3.2** « Documents de référence pour les services »).

## 4.7 Réception et émission de messages

### 4.7.1 TM3.1P – Réception de messages

| EX_3.1_5010 |
| --- |
| Le Proxy de messagerie MSSanté doit permettre la réception de messages provenant d'émetteurs propriétaires de BAL sur des domaines de messagerie MSSanté. |

| EX_3.1_5020 |
| --- |
| La réception de messages est effectuée sur le protocole SMTP, dans une session TLS mutuelle avec le Proxy de messagerie MSSanté du domaine émetteur (SMTPS). |

| EX_3.1_5030 |
| --- |
| Le Proxy de messagerie MSSanté mis en œuvre par l'opérateur doit respecter la cinématique décrite dans le **§ 4.7.1.1** pour recevoir une requête en provenance d'un autre Proxy Opérateur MSSanté. |

#### *4.7.1.1 Cinématique*

Les étapes de connexion pour un Proxy de messagerie MSSanté destinataire d'une requête en provenance d'un autre Proxy Opérateur MSSanté sont les suivantes :

1) Vérification que le nom DNS du serveur émetteur possède bien un enregistrement PTR 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 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) ;
3) 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 Proxy de messagerie MSSanté destinataire ne doit accepter que ce type de connexion) ;
4) Vérification du certificat serveur présenté par le Proxy de messagerie MSSanté émetteur comme défini dans la RFC 2246 (http ://tools.ietf.org/html/rfc2246) (voir **§ 4.2** « Modalités techniques pour assurer la sécurisation des échanges ») et vérification que le certificat présenté par le serveur SMTP de l'émetteur est dans la liste blanche des domaines autorisés ;
5) 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) ; le nom de domaine de l'adresse mail de l'expéditeur (« MAIL FROM ») doit à la fois :

- Etre renseigné dans l'enveloppe SMTP du message ;
- Figurer dans la liste blanche des domaines autorisés ;
- Correspondre au DN du certificat utilisé tel que référencé dans la liste blanche pour le domaine de messagerie en question ;

Dans le cas contraire, le Proxy de messagerie MSSanté destinataire doit notifier le Proxy de messagerie 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 Proxy de messagerie 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 Proxys de messagerie MSSanté. Dans ce cas :

- Le Proxy de messagerie 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.

6) 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).

#### *4.7.1.2 Transaction*

| **EX_3.1_5040** |
| --- |
| Les commandes SMTP envoyées par le Proxy de messagerie MSSanté doivent être conformes à la RFC 5321 (voir http ://tools.ietf.org/html/rfc5321). |

### 4.7.2 TM3.2P – Emission de messages

| **EX_3.2_5010** |
| --- |
| Le Proxy de messagerie MSSanté doit permettre l'émission de messages vers des destinataires propriétaires de BAL sur des domaines MSSanté. |

| EX_3.2_5020 |
| --- |
| L'émission de messages est effectuée sur le protocole SMTP, dans une session TLS mutuelle avec le Proxy de messagerie MSSanté destinataire (SMTPS). |

| 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_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 Proxy de messagerie MSSanté mis en œuvre par l'opérateur doit respecter la cinématique décrite dans le **§ 4.7.2.1** pour émettre une requête vers un autre Proxy Opérateur MSSanté. |

#### *4.7.2.1 Cinématique*

| EX_3.2_5060 |
| --- |
| Avant l'envoi d'un message, le Proxy de messagerie 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 Proxy de messagerie MSSanté émettant une requête vers un autre Proxy Opérateur 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 Proxys de messagerie MSSanté destinataires ne doivent accepter que ce type de connexion) ;
4) Vérification des certificats serveurs présentés par les Proxys de messagerie MSSanté destinataires comme défini dans la RFC 2246 (http ://tools.ietf.org/html/rfc2246) et vérification que ces certificats figurent également dans la liste blanche des domaines autorisés ;
5) 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) ;
6) 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).

#### *4.7.2.2 Transaction*

| **EX_3.2_5070** |
| --- |
| Les commandes SMTP envoyées par le Proxy de messagerie MSSanté doivent être conformes à la RFC 5321 (voir http ://tools.ietf.org/html/rfc5321). |

## 4.8 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.

### 4.8.1 Synchronisation du temps

| **EX_SDT_5010** |
| --- |
| La date et l'heure de chaque matériel et système d'exploitation du Proxy Opérateur MSSanté doivent être synchronisées sur une source de temps fiable : le Proxy Opérateur MSSanté doit être en capacité de synchroniser son heure, pour l'horodatage des traces. |

Ce pré-requis 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 Proxy de messagerie 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.

### 4.8.2 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 MSSante.

**EX_GDT_5030**

Des traces fonctionnelles doivent être générées par le Proxy de messagerie 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, 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.

**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, nom, type et taille de(s) pièce(s) jointe(s) du message.

**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 englobent les traces de connexion et de déconnexion au service MSSanté (authentification de l'utilisateur ou de la machine) et les traces des actions réalisées par les opérateurs techniques du système.

***Durée de conservation des traces et des données à caractère personnel échangées par les utilisateurs***

**EX_GDT_5070**

Le service MSSanté proposé par l'opérateur doit prévoir les mécanismes de paramétrages nécessaires pour permettre au responsable de traitement d'être conforme aux durées de conservation des traces et des données à caractère personnel collectées lors des échanges, définies par la CNIL dans son autorisation unique (voir **§ 2.4.4** « Focus sur les formalités préalables à accomplir par le responsable de traitement »).

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, l'ASIP Santé, en sa qualité de responsable de traitement et d'opérateur d'un service de messagerie de sécurité de santé, a défini les règles suivantes pour la conservation des traces :

- En l'absence de règle légale spécifique et eu regard à la finalité du service MSSanté, qui ne doit pas être confondu avec le dossier médical de la personne concernée, les traces fonctionnelles sont conservées pendant une durée de dix ans, durée alignée sur le délai de prescription de l'action en responsabilité médicale ;
- Les traces techniques sont conservées pendant un an[4].

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. Tant que le message n'est pas supprimé par l'utilisateur, celui-ci est conservé pendant toute la durée de vie de la BAL.

### 4.8.3 Production de statistiques d'utilisation

| **EX_PSU_5010** |
| --- |
| L'opérateur MSSanté doit prévoir un dispositif capable d'enregistrer et de restituer des indicateurs de suivi de l'activité MSSanté. |

Ces informations sont consolidées par l'ASIP Santé afin de fournir une vision globale de l'utilisation du système MSSanté.

Remarque : les échanges entre domaines de l'espace de confiance MSSanté sont réalisés directement de domaine à domaine, sans centralisation sur les serveurs de l'opérateur ASIP Santé.

[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.

**EX_PSU_5020**

Les indicateurs demandés portent sur les informations suivantes, calculées du 1er au dernier jour du mois écoulé :

- Activité globale du domaine de messagerie :
  - Nombre total de messages reçus sur le domaine en provenance d'un autre domaine ;
  - Nombre total de messages émis par le domaine vers un autre domaine ;
  - Nombre total de messages émis par les usagers du domaine à l'intérieur du domaine ;

L'indicateur suivant est calculé au dernier jour du mois écoulé :

- Nombre total de BAL MSSanté sur le domaine de messagerie

L'opérateur doit transmettre ces indicateurs à l'ASIP Santé dans le courant du mois qui suit et dans un fichier au format « **CSV** ».

Le nom du fichier doit être de type : « Période concernée (AAAAMM)_SuiviMSSante_NomDomaineMSSante.csv ».

Exemple : 201311_SuiviMSSante_NomdemondomaineMSSante.csv

Ces indicateurs doivent être transmis à l'adresse électronique « mssindicateurs@sante.gouv.fr ».

**EX_PSU_5030**

Dans le cas où un opérateur gère plusieurs domaines de messagerie MSSanté, l'opérateur doit transmettre ces indicateurs pour chacun de ses domaines (1 fichier par domaine de messagerie).

La structure du fichier doit respecter le format défini au **§ 4.8.3.1** « Format du fichier statistiques MSSanté » et doit prendre en compte les règles suivantes :

- Le séparateur à utiliser entre chaque attribut est : « ; »
- La restitution doit être en colonne et l'ordre de présentation des indicateurs dans le fichier doit être respecté ;
- La première ligne du fichier doit contenir les noms des attributs.

#### *4.8.3.1 Format du fichier statistiques MSSanté*

Le tableau ci-dessous liste les attributs et l'ordre attendu :

| Nom | Description | Type | Longueur | Format |
|---|---|---|---|---|
| Date | Date de production des données transmises | Date | 8 | AAAAMMJJ |
| Periode_Concernee | Mois sur lequel porte les indicateurs transmis | Mois | 6 | AAAAMM |
| NomDomaine | Domaine MSSanté correspondant aux données transmises | Alphanumérique | 255 | Sans Objet |
| Nb_Mess_Rec_Inter_D | Nombre total de messages reçus sur le domaine en provenance d'un autre domaine du 1er jour au dernier de la période concernée | Numérique | NA | Sans Objet |
| Nb_Mess_Emi_Inter_D | Nombre total de messages émis par le domaine vers un autre domaine du 1er jour au dernier de la période concernée | Numérique | NA | Sans Objet |
| Nb_Mess_Emi_Intra_D | Nombre total de messages émis par les usagers du domaine à l'intérieur du domaine du 1er jour au dernier de la période concernée | Numérique | NA | Sans Objet |
| Nb_BAL_A_Date | Nombre total de BAL MSSanté sur le domaine au dernier jour de la période concernée | Numérique | NA | Sans Objet |

**Tableau 46 : Liste des attributs pour le fichier de statistiques d'utilisation MSSanté**

Remarque : un exemple de fichier « statistiques MSSanté » que les opérateurs doivent transmettre à l'ASIP Santé est disponible en annexe et correspond au document de référence DR4 défini au **§ 7.3.2** « Documents de référence pour les services ».

### 4.8.4 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 de santé ;
- 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 :
- 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 du « zéro papier ».
- 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.

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'acception de ces conditions par tout utilisateur de son service avant l'usage effectif de celui-ci. |

A titre d'information, les CGU du service MSSanté proposé par l'opérateur ASIP Santé sont accessibles à l'url suivante : https://www.mssante.fr/cgu.

### 4.8.5 Exigences complémentaires de sécurité

#### *4.8.5.1 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.

#### *4.8.5.2 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.<br>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.<br><br>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.<br><br>Le système MSSanté doit également alerter l'utilisateur de la mise en quarantaine d'un message et/ou d'une pièce jointe bloqués lors de l'émission d'un message vers sa BAL. |

***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.<br><br>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. ».<br><br>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. |

***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).<br><br>Les exigences concernant les traces sont définies dans le **§ 4.8.2** « Gestion des traces ». |

***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 **§ 4.3** « Modalités techniques spécifiques aux Web Services d'annuaire ».
Les exigences de sécurité concernant la liste blanche des domaines autorisés sont définies dans le **§ 4.6** « 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). |

***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. |

***Conformité***

| EX_SSI_5170 |
| --- |
| Chaque acteur du projet doit assurer une veille réglementaire en vue d'assurer la conformité du SI tout au long de son cycle de vie. |

### 4.8.6 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.<br><br>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.<br><br>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.<br><br>Le service d'auto-configuration n'est possible que pour les interfaces basées sur les protocoles SMTP/IMAP et permet :<br>• 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) ;<br>• 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).<br><br>A titre d'exemple,les ressources Web suivantes peuvent être consultées respectivement pour les Web Services AutoConfig et AutoDiscover :<br>• https://wiki.mozilla.org/Thunderbird:Autoconfiguration<br>• 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.

# 5 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.

| Fonctionnalité | § DSFT | N° Exigence | Exigence |
|---|---|---|---|
| Emission de messages MSSanté | 4.7.2 | EX_3.2_5010 | Le Proxy de messagerie MSSanté doit permettre l'émission de messages vers des destinataires propriétaires de BAL sur des domaines MSSanté. |
| | 4.7.2 | EX_3.2_5020 | L'émission de messages est effectuée sur le protocole SMTP, dans une session TLS mutuelle avec le Proxy de messagerie MSSanté destinataire (SMTPS). |
| | 4.2.2 | EX_OPE_5020 | Le Proxy de messagerie 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). |
| | 4.7.2 | EX_3.2_5040 | Un opérateur MSSanté ne doit pas utiliser le serveur SMTP d'un autre opérateur MSSanté comme relai de messagerie. |
| | 4.2.1 | EX_OPE_5010 | La version minimum de TLS qui doit être mise en œuvre est la version 1.0 (cf. RFC 2246 - http://tools.ietf.org/html/rfc2246). |
| | 4.7.2.1 | EX_3.2_5060 | Avant l'envoi d'un message, le Proxy de messagerie 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). |
| | 4.7.2 | EX_3.2_5050 | Le Proxy de messagerie MSSanté mis en œuvre par l'opérateur doit respecter la cinématique décrite dans le **§ 4.7.2.1** pour émettre une requête vers un autre Proxy Opérateur MSSanté. |
| | 4.7.2.2 | EX_3.2_5070 | Les commandes SMTP envoyées par le Proxy de messagerie MSSanté doivent être conformes à la RFC 5321 (voir http ://tools.ietf.org/html/rfc5321). |
| | 4.7.2 | 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. |
| Réception de messages MSSanté | 4.7.1 | EX_3.1_5010 | Le Proxy de messagerie MSSanté doit permettre la réception de messages provenant d'émetteurs propriétaires de BAL sur des domaines de messagerie MSSanté. |
| | 4.7.1 | EX_3.1_5020 | La réception de messages est effectuée sur le protocole SMTP, dans une session TLS mutuelle avec le Proxy de messagerie MSSanté du domaine émetteur (SMTPS). |
| | 4.2.2 | EX_OPE_5020 | Le Proxy de messagerie 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 |

| Fonctionnalité | § DSFT | N° Exigence | Exigence |
|---|---|---|---|
| | | | (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). |
| | **4.2.1** | **EX_OPE_5010** | La version minimum de TLS qui doit être mise en œuvre est la version 1.0 (cf. RFC 2246 - http://tools.ietf.org/html/rfc2246). |
| | **4.7.1** | **EX_3.1_5030** | Le Proxy de messagerie MSSanté mis en œuvre par l'opérateur doit respecter la cinématique décrite dans le **§ 4.7.1.1** pour recevoir une requête en provenance d'un autre Proxy Opérateur MSSanté. |
| | **4.7.1.2** | **EX_3.1_5040** | Les commandes SMTP envoyées par le Proxy de messagerie MSSanté doivent être conformes à la RFC 5321 (voir http ://tools.ietf.org/html/rfc5321). |
| **Interrogation liste blanche** | **4.6.1** | **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) :<br>• Un DN de certificat peut être associé à un ou plusieurs domaines de messagerie ;<br>• Un domaine de messagerie peut être associé à un ou plusieurs DN de certificats. |
| | **4.6.2** | **EX_2.2_5010** | Le Proxy de messagerie MSSanté doit récupérer **quotidiennement** la dernière version de la liste blanche à l'adresse suivante : https://listeblanche.mssante.fr/listeblanchemssante.xml. |
| | **4.6.2** | **EX_2.2_5030** | L'exploitation par le Proxy de messagerie MSSanté de la liste blanche doit se faire en local et sans altération du fichier XML récupéré. |
| | **4.6.3** | **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/xmldsig-bestpractices/#bp-validate-signing-key. |
| | **4.6.3** | **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 (Ajout / Modification / Suppression comptes de messagerie de l'opérateur)** | **4.3** | **EX_WSA_5010** | L'authentification mutuelle du Proxy de messagerie MSSanté avec le serveur d'annuaire national MSSanté constitue un pré-requis 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). |
| | **4.3** | **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). |

| Fonctionnalité | § DSFT | N° Exigence | Exigence |
|---|---|---|---|
| | **4.3.1.1.1** | **EX_WSA_5030** | Les spécifications du **§ 4.3.1.1.1** concernant l'encodage et les espaces de nommage, pour les Web Services de l'annuaire national MSSanté en SOAP, doivent être respectées. |
| | **4.3.1.1.2** | **EX_WSA_5040** | Les spécifications du **§ 4.3.1.1.2** concernant la sécurité et l'intégrité, pour les Web Services de l'annuaire national MSSanté en SOAP, doivent être respectées. |
| | **4.3.1.1.3.3** | **EX_WSA_5050** | Les spécifications du **§ 4.3.1.1.3.3** (et sous-chapitres) concernant la construction des messages, pour les Web Services de l'annuaire national MSSanté en SOAP, doivent être respectées. |
| | **4.3.1.1.3.4** | **EX_WSA_5060** | Les spécifications du **§ 4.3.1.1.3.4** (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'annuaire national MSSanté en SOAP, doivent être respectées. |
| | **4.4.1** | **EX_PBA_5010** | L'opérateur MSSanté doit obligatoirement implémenter au moins une des trois solutions proposées (TM1.1.1P, TM1.1.2P ou TM1.1.3P) 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 :<br>• 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) ;<br>• 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) ;<br>• Supprimer de l'annuaire national MSSanté les BAL utilisateurs MSSanté 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). |
| | **4.4.1** | **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 :<br>• service-cardiologie@xyz.mssante.fr ;<br>• cabinet-dr-martin@xyz.mssante.fr ;<br>• service-pr-dupont@xyz.mssantefr ;<br>• institut-pasteur.secretariat@xyz.mssante.fr. |
| | **4.4.1** | **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). |
| | **4.4.1** | **EX_PBA_5040** | L'opérateur doit, par un moyen technique ou organisationnel, permettre à chacun des utilisateurs de son service d'indiquer explicitement :<br>• S'il souhaite être inscrit en liste rouge ;<br>• S'il souhaite la publication de son numéro de téléphone ;<br>• Le cas échéant son acceptation du « zéro papier » (ce choix doit également être indiqué pour les BAL applicatives ou organisationnelles).<br>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 |

| Fonctionnalité | § DSFT | N° Exigence | Exigence |
|---|---|---|---|
| | | | à tout moment par l'utilisateur. |
| | **4.4.1** | **EX_PBA_5050** | L'opérateur doit mettre en œuvre les mécanismes techniques permettant de transmettre à l'annuaire national MSSanté :<br>• Les choix de l'utilisateur concernant : son inscription en liste rouge et son acceptation (ou pas) du « zéro papier » ;<br>• Le numéro de téléphone de l'utilisateur (le cas échéant). |
| | **4.4.1** | **EX_PBA_5060** | Afin de garantir la fiabilité des données publiées dans l'annuaire national MSSanté vis-à-vis des utilisateurs des autres domaines, l'opérateur MSSanté doit être en mesure de gérer le cycle de vie des comptes de messagerie MSSanté des utilisateurs de son domaine, par l'intermédiaire de processus organisationnels et techniques au sein de l'organisation en charge du domaine de messagerie. |
| | **4.4.1** | **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. |
| | **4.4.1** | **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 professionnels de santé dûment identifiés dans une base des utilisateurs. |
| | **4.4.1** | **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. |
| | **4.4.1** | **EX_PBA_5140** | L'opérateur doit s'assurer que les BAL MSSanté liées à son service de messagerie MSSanté fermées ou supprimées ne soient plus publiées dans l'annuaire national MSSanté. |
| | **4.4.1** | **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. |
| | **4.4.1** | **EX_PBA_5070** | Le format des adresses de messagerie MSSanté doit respecter la RFC 5321 (http://tools.ietf.org/html/rfc5321).<br>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). |
| | **4.4.1.2** | **EX_PBA_5080** | L'opérateur doit s'assurer que les destinataires « machines » sont en mesure d'exploiter des messages de type « indicateur d'absence » ou « message de saturation de BAL » afin de pouvoir déclencher à leur suite les actions appropriées. |
| | **4.4.1.2** | **EX_PBA_5160** | Le ou les professionnels indiqués en tant que responsables au niveau opérationnel d'une BAL Organisationnelle ou Applicative doivent être des professionnels habilités à échanger des données de santé personnelles. |
| | **4.4.1.1** | **EX_PBA_5090** | L'identifiant du titulaire d'une BAL MSSanté transmis par l'opérateur lors de l'alimentation de l'annuaire national MSSanté doit être l'identifiant national (RPPS/ADELI) si le titulaire de la BAL en |

| Fonctionnalité | § DSFT | N° Exigence | Exigence |
|---|---|---|---|
| | | | dispose.<br>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. |
| | **4.4.1.1** | **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. |
| | **4.4.2.1** | **EX_1.1_5010** | Plusieurs modalités de mise à jour des comptes de messagerie dans l'annuaire national MSSanté sont prévues et détaillées dans les chapitres suivants. Il est exigé que le Proxy de messagerie MSSanté mette en œuvre au moins l'une des modalités proposées. |
| | **4.4.2.2** | **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 **§ 4.4.2.2** (et sous-chapitres). |
| | **4.4.2.2.5** | **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. |
| **Consultation Annuaire national MSSanté (transaction optionnelle)** | **4.3** | **EX_WSA_5010** | L'authentification mutuelle du Proxy de messagerie MSSanté avec le serveur d'annuaire national MSSanté constitue un pré-requis 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). |
| | **4.3** | **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). |
| | **4.3.1.2.1** | **EX_WSA_5070** | Les spécifications du **§ 4.3.1.2.1** concernant l'encodage et les espaces de nommage, pour les Web Services de l'annuaire national MSSanté en REST, doivent être respectées. |
| | **4.3.1.2.2** | **EX_WSA_5080** | Les spécifications du **§ 4.3.1.2.2** concernant la sécurité et l'intégrité, pour les Web Services de l'annuaire national MSSanté en REST, doivent être respectées. |
| | **4.3.1.2.3.1** | **EX_WSA_5090** | Les spécifications du **§ 4.3.1.2.3.1** (et sous-chapitres) concernant les échanges, pour les Web Services de l'annuaire national MSSanté en REST, doivent être respectées. |
| | **4.3.1.2.3.2** | **EX_WSA_5100** | Les spécifications du **§ 4.3.1.2.3.2** (et sous-chapitres) concernant la gestion des erreurs, pour les Web Services de l'annuaire national MSSanté en REST, doivent être respectées. |
| | **4.5** | **EX_2.1_5010** | L'opérateur MSSanté doit obligatoirement implémenter au moins une des trois solutions disponibles (TM2.1.1A, TM2.1.2A ou TM2.1.3A) afin que les utilisateurs du système MSSanté puissent sélectionner de manière sûre et aisée les destinataires de leurs messages. |

| Fonctionnalité | § DSFT | N° Exigence | Exigence |
|---|---|---|---|
| | **4.5.1.2** | **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. |
| | **4.5.2** | **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 **§ 4.5.2** (et sous-chapitres associés). |
| | **4.5.3** | **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 **§ 4.5.3** (et sous-chapitres associés). |
| **Synchronisation temps** | **4.8.1** | **EX_SDT_5010** | La date et l'heure de chaque matériel et système d'exploitation du Proxy Opérateur MSSanté doivent être synchronisées sur une source de temps fiable : le Proxy Opérateur MSSanté doit être en capacité de synchroniser son heure, pour l'horodatage des traces. |
| **Traces service MSSanté** | **4.8.2** | **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 :<br>• Contribuer à la détection, à l'investigation et au traitement d'incidents de sécurité ;<br>• Contribuer à la résolution de litiges entre le responsable du domaine et des utilisateurs ;<br>• Permettre à une autorité de s'assurer de la conformité du traitement aux dispositions législatives qui l'encadrent. |
| | **4.8.2** | **EX_GDT_5020** | Les utilisateurs et l'exploitant doivent être informés de la génération de traces de leurs actions par le service MSSanté. |
| | **4.8.2** | **EX_GDT_5030** | Des traces fonctionnelles doivent être générées par le Proxy de messagerie MSSanté pour tous les traitements opérés sur les BAL (Personnelles, Applicatives et Organisationnelles) et leur contenu. |
| | **4.8.2** | **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, 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. |
| | **4.8.2** | **EX_GDT_5050** | Pour les traces concernant l'envoi ou la réception d'un message, le champ « type d'action » inclut les informations suivantes :<br>• Identifiant unique interne du message ;<br>• Adresses email de l'émetteur du message et des destinataires du message ;<br>• Objet du message ;<br>• Le cas échéant, nom, type et taille de(s) pièce(s) jointe(s) du message. |
| | **4.8.2** | **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 |

| Fonctionnalité | § DSFT | N° Exigence | Exigence |
|---|---|---|---|
| | | | 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. |
| | **4.8.2** | **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, définies par la CNIL dans son autorisation unique (voir **§ 2.4.4** « Focus sur les formalités préalables à accomplir par le responsable de traitement »).<br><br>Le service de l'opérateur devra donc respecter ces durées. |
| **Statistiques service MSSanté** | **4.8.3** | **EX_PSU_5010** | L'opérateur MSSanté doit prévoir un dispositif capable d'enregistrer et de restituer des indicateurs de suivi de l'activité MSSanté. |
| | **4.8.3** | **EX_PSU_5020** | Les indicateurs demandés portent sur les informations suivantes, calculées du 1er au dernier jour du mois écoulé :<br>• Activité globale du domaine de messagerie :<br>o Nombre total de messages reçus sur le domaine en provenance d'un autre domaine ;<br>o Nombre total de messages émis par le domaine vers un autre domaine ;<br>o Nombre total de messages émis par les usagers du domaine à l'intérieur du domaine ;<br><br>L'indicateur suivant est calculé au dernier jour du mois écoulé :<br>o Nombre total de BAL MSSanté sur le domaine de messagerie<br><br>L'opérateur doit transmettre ces indicateurs à l'ASIP Santé dans le courant du mois qui suit et dans un fichier au format « **CSV** ».<br><br>Le nom du fichier doit être de type : « Période concernée (AAAAMM)_SuiviMSSante_NomDomaineMSSante.csv ».<br><br>Exemple :<br>201311_SuiviMSSante_NomdemondomaineMSSante.csv<br><br>Ces indicateurs doivent être transmis à l'adresse électronique « mssindicateurs@sante.gouv.fr ». |
| | **4.8.3** | **EX_PSU_5030** | Dans le cas où un opérateur gère plusieurs domaines de messagerie MSSanté, l'opérateur doit transmettre ces indicateurs pour chacun de ses domaines (1 fichier par domaine de messagerie).<br><br>La structure du fichier doit respecter le format défini au **§ 4.8.3.1** « Format du fichier statistiques MSSanté » et doit prendre en compte les règles suivantes :<br>• Le séparateur à utiliser entre chaque attribut est : « ; »<br>• La restitution doit être en colonne et l'ordre de présentation des indicateurs dans le fichier doit être respecté ;<br>• La première ligne du fichier doit contenir les noms des attributs. |
| **Sécurité** | **4.8.5** | **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. |
| | **4.8.5** | **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. |

| Fonctionnalité | § DSFT | N° Exigence | Exigence |
|---|---|---|---|
| | **4.8.5** | **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.<br>Des audits de la sécurité du système de messageries MSSanté et de son environnement doivent être réalisés à intervalle régulier. |
| | **4.8.5** | **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. |
| | **4.8.5** | **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. |
| | **4.8.5** | **EX_SSI_5060** | Les locaux hébergeant les plateformes de production et de secours du SI doivent bénéficier d'un contrôle des accès physiques. |
| | **4.8.5** | **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. |
| | **4.8.5** | **EX_SSI_5080** | La capacité du système mis en œuvre pour le service MSSanté doit être testée, suivie et anticipée. |
| | **4.8.5** | **EX_SSI_5090** | Le système MSSanté doit mettre en œuvre des mécanismes de détection des intrusions.<br>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.<br>Le système MSSanté doit également alerter l'utilisateur de la mise en quarantaine d'un message et/ou d'une pièce jointe bloqués lors de l'émission d'un message vers sa BAL. |
| | **4.8.5** | **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.<br>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. ».<br>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. |
| | **4.8.5** | **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. |

| Fonctionnalité | § DSFT | N° Exigence | Exigence |
|---|---|---|---|
| | **4.8.5** | **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).<br>Les exigences concernant les traces sont définies dans le **§ 4.8.2** « Gestion des traces ». |
| | **4.8.5** | **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. |
| | **4.8.5** | **EX_SSI_5140** | Les pare-feux protégeant l'infrastructure du SI doivent bénéficier des mécanismes de protection conformes à l'état de l'art. |
| | **4.8.5** | **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). |
| | **4.8.5** | **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. |
| | **4.8.5** | **EX_SSI_5170** | Chaque acteur du projet doit assurer une veille réglementaire en vue d'assurer la conformité du SI tout au long de son cycle de vie. |
| **Définition des CGU à mettre en œuvre par l'opérateur** | **4.8.4** | **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.<br>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) :<br><u>Rappel du contexte juridique</u> :<br>• 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 de santé ;<br>• 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 ;<br>• 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.<br><u>Bon usage de la MSSanté</u> :<br>• Seuls les professionnels habilités à échanger des données de santé personnelles peuvent utiliser le service MSSanté ;<br>• 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 ;<br>• L'utilisateur s'engage à ne pas procéder à l'envoi de messages non sollicités à un ou plusieurs destinataires, considéré comme du spam ;<br>• L'utilisateur s'interdit de transmettre par messagerie sécurisée ou par tout autre moyen des courriels contenant |

| Fonctionnalité | § DSFT | N° Exigence | Exigence |
|---|---|---|---|
| | | | des virus ou plus généralement tout programme visant notamment à détruire ou limiter la fonctionnalité de tout logiciel, ordinateur ou réseau de télécommunication ;<br>• L'utilisateur s'engage à ne pas rediriger son adresse sécurisée vers une adresse de messagerie non MSSanté.<br><br>Publication dans l'annuaire national MSSanté :<br><br>• 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) :<br>o s'il souhaite être inscrit en liste rouge ;<br>o s'il souhaite la publication de son numéro de téléphone ;<br>o le cas échéant son acceptation du « zéro papier ».<br>• 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).<br><br>Information du patient :<br><br>• 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) ;<br>• 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.<br>• 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.<br><br>Valeur probante :<br><br>• 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. |
| | **4.8.4** | **EX_DCU_5030** | L'opérateur doit mettre en œuvre les moyens lui permettant de s'assurer de l'acception de ces conditions par tout utilisateur de son service avant l'usage effectif de celui-ci. |

**Tableau 47 : Liste des exigences applicables aux opérateurs MSSanté**

# 6 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 avec la version 0.9.5 du 12/09/2013.

| Paragraphe | Page | Changement |
|---|---|---|
| **Général** | **-** | Abandon de la notion d'homologation des clients de messagerie MSSanté (le Document de Spécifications Techniques (DST) Clients de messagerie est publié « pour information », afin de favoriser une standardisation des échanges clients/serveurs de messagerie et d'inspirer l'interopérabilité sans la contraindre). |
| **Général** | **-** | Identification et numérotation dans le corps du document, des exigences (applicables aux opérateurs MSSanté) ainsi que des recommandations. |
| **Général** | **-** | Les BAL « Fonctionnelles » ont été renommée « BAL Applicatives ». |
| **Général** | **-** | Les WSDL et XSD ont été mis à jour afin de prendre en compte les modifications apportées sur les attributs de l'annuaire national MSSanté. |
| **Général** | **-** | Les chapitres 1 à 3 ont été mis à jour pour apporter des précisions et compléments. |
| **4.2.1** | **42** | Des compléments et précisions ont été apportés dans le chapitre « Principes de raccordement des Proxys Opérateur MSSanté à l'espace de confiance MSSanté », principalement sur « *Sécurisation des échanges de messages* ». |
| **4.2.2** | **43** | Des précisions ont été apportées sur l'exigence « EX_OPE_5020 ». |
| **4.2.2** | **43** | Des compléments et précisions ont été apportés dans le chapitre «Validation des certificats serveur», principalement sur les recommandations « RE_OPE_5010 », « RE_OPE_5020 », « RE_OPE_5030 » et « RE_OPE_5040 ». |
| **4.2.2** | **43** | L'exigence : « Le Proxy SMTP doit être en capacité de valider le certificat de l'opérateur MSSanté 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). » a été supprimée.<br>Des compléments ont été apportés aux exigences « EX_OPE_5020 », « EX_2.2_5040 » et « EX_2.2_5050 ». |
| **4.3** | **45** | La remarque suivante a été ajoutée : « 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 MSSanté, le DN du certificat serveur utilisé doit être référencé dans la liste blanche des domaines autorisés ». |
| **4.3** | **45** | L'exigence EX_WSA_5020 a été précisée. |
| **4.3** | **45** | Des compléments et précisions ont été apportés dans le chapitre «<br>Web Services de l'annuaire national MSSanté en SOAP », avec principalement :<br>- Définition des URL des Web Services ;<br>- Mise à jour de la version des Web Services ;<br>- Correction apportée sur les actions possibles (suppression de l'action « extraction ») ;<br>- Mise à jour de l'exemple de jeton VIHF « Figure 23 : Exemple de jeton VIHF pour l'annuaire national MSSanté (authentification indirecte) ». |
| **4.3.1.1.3.4.1** | **55** | Mise à jour de l'exemple de SOAP Fault exception. |
| **4.3.1.2.1** | **56** | Suppression de la recommandation « RE_WSA_5010 » : « Il est recommandé que la longueur d'une URI (chemin + paramètre(s)) ne dépasse pas 1024 octets. » |
| **4.3.1.2.3.1.2** | **59** | Correction apportée à la description fonctionnelle de la requête permettant la récupération |

| Paragraphe | Page | Changement |
|---|---|---|
| | | d'une ressource unique. |
| **4.4.1** | **61** | Mise à jour des exigences / recommandations et des descriptions fonctionnelles pour les paragraphes : « BAL personnelles, applicatives ou organisationnelles », présence des utilisateurs en « Liste rouge », publication du numéro de téléphone, Acceptation du « Zéro papier » et Cycle de vie des comptes de messagerie.<br><br>Les principales modifications sont :<br><br>- Ajout des attributs « téléphone » et « dématérialisation » pour les BAL applicatives ou organisationnelles ;<br><br>- Le format des adresses de messagerie MSSanté doit respecter la RFC 5321 (http://tools.ietf.org/html/rfc5321) (en remplacement de la RFC 3696) – voir exigence « EX_PBA_5070 » ;<br><br>- En cohérence avec la RFC 5321 (qui 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), la longueur maximum pour une adresse de messagerie a été modifiée à 256 caractères (en remplacement de 320) – voir exigence « EX_PBA_5070 » ;<br><br>- Dans le paragraphe « Cycle de vie des comptes de messagerie », l'exigence « EX_PBA_5060 » a été précisée en plusieurs exigences : «EX_PBA_5110», «EX_PBA_5120», «EX_PBA_5130», «EX_PBA_5140» et «EX_PBA_5150» ;<br><br>- Modification des recommandations sur le format des adresses de messagerie – voir en particulier l'exigence « EX_PBA_5020 » et la recommandation « RE_PBA_5020 » ;<br><br>- Ajout de la recommandation « RE_PBA_5030 ». |
| **4.4.1.1** | **65** | Le tableau présentant les attributs d'alimentation pour les BAL rattachées à des personnes physiques a été supprimé de ce paragraphe de présentation – voir le **§ 4.4.2.2.3** pour la spécification détaillée des champs composants le fichier d'alimentation. |
| **4.4.1.1** | **65** | La remarque complémentaire suivante a été ajoutée : « 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. » |
| **4.4.1.1** | **65** | Des précisions ont été apportées concernant l'attribution d'un numéro d'identification local pour les professionnels de santé ne disposant pas de numéro d'identification national (en particulier PS en formation). |
| **4.4.1.1** | **65** | Mise à jour de l'exigence « EX_PBA_5090 » :<br><br>« L'identifiant du titulaire d'une BAL MSSanté transmis par l'opérateur lors de l'alimentation de l'annuaire national MSSanté doit être l'identifiant national (RPPS/ADELI) si le titulaire de la BAL en dispose.<br><br>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. » |
| **4.4.1.2** | **67** | Le tableau présentant les attributs d'alimentation pour les BAL applicatives et organisationnelles a été supprimé de ce paragraphe de présentation – voir le **§ 4.4.2.2.3** pour la spécification détaillée des champs composants le fichier d'alimentation. |
| **4.4.1.2** | **67** | Ajout de l'exigence « EX_PBA_5160 » : « Le ou les professionnels indiqués en tant que responsables au niveau opérationnel d'une BAL Organisationnelle ou Applicative doivent être des professionnels habilités à échanger des données de santé personnelles. » |
| **4.4.1.2** | **67** | Suppression de l'exigence concernant la création par les opérateurs MSSanté d'une BAL probleme@nomdomaine.mssante.fr (ou probleme@nomdomaine-securise.fr, etc.). |
| **4.4.2.2.2** | **70** | Ajout des scénarios alternatifs SA6 et SA7 pour le Web Service d'alimentation global de l'annuaire national MSSanté. |

| Paragraphe | Page | Changement |
|---|---|---|
| **4.4.2.2.3.2** | **72** | Dans le tableau présentant la structure du domaine pour le Web Service d'alimentation global de l'annuaire national MSSanté, la règle de contrôle sur l'attribut « domaine » a été modifiée avec RG_CTR_000 (en remplacement de RG_CTR_001). |
| **4.4.2.2.3.3** | **72** | Le tableau présentant la structure des comptes de messagerie pour le Web Service d'alimentation global de l'annuaire national MSSanté a été mis à jour.<br>Les principales modifications portent sur :<br>- L'attribut "TypeBAL" : modification du "type" (maintenant sur 03 caractères) ;<br>- L'attribut "AdresseBAL" : modification du "type" (maintenant sur 256 caractères), du "commentaire" et des "règles de contrôle" (ajout des règles RG_CTR_001/044/046) ;<br>- L'attribut "IdentifiantPP" : modification du "type" (maintenant sur 256 caractères) et des "règles de contrôle" (ajout de la règle RG_CTR_045) ;<br>- L'attribut " CiviliteExercice" : des compléments ont été apportés ;<br>- L'attribut "PrenomExercice" : modification du "type" (maintenant sur 50 caractères) ;<br>- L'attribut "Specialite" : précisions apportées dans "commentaire" ;<br>- L'attribut "Telephone" : modification de "requis" et "commentaire" ;<br>- L'attribut "Dematerialisation" : modification de "requis" et "commentaire". |
| **4.4.2.2.5** | **78** | Web Service de recherche du compte-rendu d'alimentation<br>Des précisions / modification ont été apportées au niveau de la description fonctionnelle ainsi que le scénario principal, par exemple, sur le format du fichier, nom du fichier.<br>Il faut noter en particulier que les comptes-rendus d'alimentation sont transmis sous forme d'un fichier compressé d'extension .zip basé sur l'algorithme « deflate ».<br>Le fichier ZIP contient deux fichiers :<br>• Un fichier nommé « cralimentationmss_numero_de_ticket_ AAAAMMJJHHmmss.xml » ;<br>• Un fichier nommé « cralimentationmss_numero_de_ticket_ AAAAMMJJHHmmss _checksum.txt ». |
| **4.4.2.2.5** | **78** | L'exigence « EX_1.1.1_5020 », concernant les comptes-rendus d'alimentation de l'annuaire national MSSanté, a été ajoutée. |
| **4.4.2.2.5.1.3** | **81** | Modification de la remarque présente dans la description du fichier de compte-rendu d'alimentation : « seule la règle RG_CTR_021 (MSS020) est intégrée au compte-rendu d'alimentation dans la version actuelle de l'annuaire national MSSanté ». |
| **4.4.2.2.5.1.3** | **81** | Mise à jour de la description du fichier de compte-rendu d'alimentation :<br>- Mise à jour du tableau présentant la « structure du domaine » : modification du « type » de l'attribut « domaine » ;<br>- Mise à jour du tableau présentant « Structure – Liste des anomalies » :<br>* modification des caractéristiques ("requis", "type", "commentaire") des attributs : "TypeBAL", "AdresseBAL", "TypeIdentifiantPP", "IdentifiantPP", "TypeIdentifiantPM", "IdentifiantPM", NomExerciceAnnuaire et "PrenomExerciceAnnuaire" ;<br>* ajouts des attributs : « TypeIdentifiantPPAnnuaire » et « IdentifiantPPAnnuaire ». |
| **4.5.1** | **84** | Les résultats fournis par l'annuaire national MSSanté (mode LDAP) ont été précisés. |
| **4.5.1.2** | **86** | Des précisions (dont l'URL d'accès) ont été apportées concernant l'interrogation de l'annuaire national MSSanté par le protocole LDAP. |
| **4.5.2** | **86** | Téléchargement d'une extraction de l'annuaire national MSSanté :<br>- Les règles d'extraction du fichier ont été mises à jour : voir le tableau « Règles d'extraction du fichier des BAL MSSanté », en particulier pour les éléments : règle de |

| Paragraphe | Page | Changement |
|---|---|---|
| | | sélection, format du fichier, nom du fichier, données du savoir-faire.<br>Il faut noter que les extractions sont transmises sous forme d'un fichier compressé d'extension .zip basé sur l'algorithme « deflate ».<br>Le fichier zip contient deux fichiers :<br>• Un fichier nommé « ExtractionMSSGlobale_AAAAMMJJHHmmss.xml » ;<br>• Un fichier nommé « ExtractionMSSGlobale_AAAAMMJJHHmmss_checksum.txt ».<br>- La description fonctionnelle ainsi que le scénario principal ont été mis en cohérence avec les modifications apportées. |
| **4.5.2.3.3** | **90** | Le tableau « Réponse du Web Service de demande de téléchargement de l'extraction de l'annuaire national MSSanté en cas d'erreur » a été mis à jour : ajout de codes et de messages.<br>Le tableau « Corps de la réponse du Web Service de demande de téléchargement de l'extraction de l'annuaire national MSSanté en cas d'erreur » a également été supprimé. |
| **4.5.2.3.4** | **90** | Le tableau présentant la liste des attributs présents dans le fichier d'extraction des comptes MSSanté a été mis à jour.<br>Les principales modifications portent sur :<br>- L'attribut "TYPEBAL" : modification du "type" (maintenant sur 03 caractères) ;<br>- L'attribut "ADRESSEBAL" : modification du "type" (maintenant sur 256 caractères) ;<br>- L'attribut "IDENTIFIANTPP" : modification du "type" (maintenant sur 256 caractères) ainsi que du « commentaire » ;<br>- L'attribut "SERVICERATTACHEMENT" : mise à jour du commentaire ;<br>- L'attribut "PRENOMEXERCICE" : modification du "type" (maintenant sur 50 caractères) ;<br>- L'attribut "NSPECIALITE" : précisions apportées sur "définition" et "commentaire" ;<br>- L'attribut "TELEPHONE" : modification de "requis" ;<br>- L'attribut "DEMATERIALISATION" : modification de "requis" ;<br>- L'attribut "L4NUMEROVOIE" : modification du "type" (maintenant sur 04 caractères) ;<br>- L'attribut "L4COMPLEMENTNUMEROVOIE" : modification du "type" (maintenant sur 03 caractères). |
| **4.5.3** | **93** | Ajout de la transaction « TM2.1.4A - Téléchargement des données d'identités des futurs utilisateurs finaux ». |
| **4.6.1** | **100** | L'exigence « EX_LBL_5010 », concernant la Liste Blanche des domaines autorisés, a été ajoutée. |
| **4.6.3** | **103** | Des précisions ont été apportées sur les exigences : « EX_2.2_5040 » et « EX_2.2_5050 ». |
| **4.7** | **104** | Mise à jour des exigences et cinématiques pour les transactions de réception (TM3.1P) et d'émission (TM3.2P) de messages. |
| **4.8** | **107** | Des modifications et précisions ont été apportées au chapitre « autres exigences applicables aux opérateurs MSSanté » :<br>- Synchronisation du temps : mise à jour des exigences ;<br>- Gestion des traces : mise à jour des exigences, ajout de précisions sur la durée de conservation des traces ;<br>- Production de statistiques d'utilisation : mise à jour des exigences, ajout de précisions sur la liste et le format des indicateurs, ajout de précisions sur le mode de restitution des indicateurs ;<br>- Définition de conditions générales d'utilisation du service MSSanté : mise à jour des |

| Paragraphe | Page | Changement |
|---|---|---|
| | | exigences.<br>De plus, le **§ 5.7.2** « Protection contre les codes malveillants » présent dans le DSFT opérateurs V0.9.5 a été intégré dans le chapitre **4.8.5** « Exigences complémentaires de sécurité » dans le paragraphe « Protection contre les codes malveillants et mobiles ». |
| **4.8.5** | **114** | Le chapitre 5 « Accès sécurisé à la MSSanté » présent dans le DSFT opérateurs V0.9.5 a été intégré en partie dans le **§ 4.8.5** « Exigences complémentaires de sécurité » ainsi qu'en Annexe (**§ 7.5** «Eléments nécessaires à la réalisation d'une analyse de risque »). |
| **4.8.5** | **114** | Les exigences du **§ 4.8.5** « Exigences complémentaires de sécurité » ont été mises à jour. Les principales modifications portent sur les paragraphes : Analyse des risques, Gestion de l'accès utilisateur, Surveillance, Contrôle d'accès réseau et Protection contre les codes malveillants et mobiles. |
| **4.8.6** | **120** | Précisions apportées dans la recommandation « RE_ACC_5020 » concernant le service d'auto-configuration. |
| **5** | **122** | Le tableau de synthèse des exigences référencées dans ce document a été déplacé dans un chapitre spécifique. |
| **7.3** | **144** | Mise à jour du chapitre **§ 7.3** « Web Services et URL pour les transactions ». |
| **7.4.1** | **145** | Les modifications suivantes ont été apportées :<br>- Le message d'erreur lié au code WSMSS 12 est désormais « variable » ;<br>- Le tableau « Liste des contrôles liés à la vérification du schéma XML dans le cas du code WSMSS12 » a été ajouté. Ce tableau 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. |
| **7.4.1** | **145** | Codes d'erreurs pour les Web Services de l'annuaire national MSSanté en SOAP :<br>- Ajout des messages d'erreurs WSMSS18 à WSMSS25 ;<br>- Les codes erreurs associées aux messages 01 à 09 ont été mis à jour : ajout du « 0 » ;<br>- Le format des codes a été modifié pour l'ensemble des messages d'erreurs : suppression de l'espace, les codes sont maintenant de la forme « WSMSS10 ». |
| **7.4.3** | **147** | Des modifications ont été apportées sur les codes d'erreur liés à la mise à jour des comptes de messagerie dans l'annuaire national MSSanté. Les principales modifications sont :<br>- Mise à jour : RG_CTR_000 / RG_CTR_027 / RG_CTR_031 / RG_CTR_041 / RG_CTR_043 ;<br>- Ajout de : RG_CTR_044 / RG_CTR_045 / RG_CTR_046 ;<br>- Des précisions ont été apportées sur l'ordre de passage des contrôles ;<br>- Les contrôles : RG_CTR_002 / RG_CTR_003 / RG_CTR_004 / RG_CTR_006 / RG_CTR_015 / RG_CTR_031 / RG_CTR_032 / RG_CTR_046 initialement présents dans le tableau « Contrôles effectués sur la TM1.1.xP» ont été déplacés dans le tableau : « Liste des contrôles liés à la vérification du schéma XML dans le cas du code WSMSS 12 » du paragraphe précédent. |

**Tableau 48 : Historique des modifications**

# 7 Annexes

## 7.1 Documents externes

### 7.1.1 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 http ://esante.gouv.fr/)** | | |
| 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 http ://esante.gouv.fr/services/referentiels/identification/nomenclature-des-acteurs-de-sante)** | | |
| DA5 | [NAS-RES-TERMI] | **Liste des Identifiants des Ressources Terminologiques utilisées par le RASS** |

**Tableau 49 : Liste des documents applicables**

### 7.1.2 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 ACCES 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

### 7.1.3 Annexes externes

| **Documentation IETF /**<br>**(spécification internationale en libre accès sur http://www.ietf.org/)** | | |
|---|---|---|
| DX1 | MSS-ANX-CRL1 | **Internet X.509 Public Key Infrastructure**<br>Certificate and Certificate Revocation List (CRL) Profile<br>http://tools.ietf.org/html/rfc5280 |
| DX2 | MSS-SMTP1 | **Simple Mail Transfer Protocol**<br>http://tools.ietf.org/html/rfc5321 |
| DX3 | MSS-SMTP2 | **SMTP Service Extension for**<br>Returning Enhanced Error Codes<br>http://tools.ietf.org/html/rfc2034 |
| DX4 | MSS-ANX-SMTPS | **SMTP Service Extension for**<br>Secure SMTP over Transport Layer Security |

| Documentation IETF / (spécification internationale en libre accès sur http://www.ietf.org/) | | |
|---|---|---|
| | | 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 Acces 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** 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- | **The Model Primary Content Type for Multipurpose Internet Mail** |

| Documentation IETF / (spécification internationale en libre accès sur http://www.ietf.org/) | | |
|---|---|---|
| | MIME6 | **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 |

Tableau 50 : Liste des annexes externes IETF

# 7.2 Terminologie, acronymes et abréviations

## 7.2.1 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 ;
- **MIME**[5] (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 ;

[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).

- **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.

### 7.2.2 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 |
| 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 |
| ES | Etablissement de Santé : terme recouvrant les établissements de soins publics et privés, incluant les plateaux techniques en ville et en hôpital |
| 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 |

| Abréviations | Signification |
|---|---|
| LFSS | Loi de Financement de la Sécurité Sociale |
| LGC | Logiciel de Gestion de Cabinet |
| LPS | Logiciel de Professionnel de Santé (abréviation générique désignant 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) |
| NAS | Nomenclature des Acteurs de Santé |
| NDR | Non-Delivery Report |
| OCSP | Online Certifcate Status Protocol |
| ODI | Outil de Diagnostic d'Installation |
| OTP | One Time Password |
| PAERPA | Personnes Agées En Risque de Perte d'Autonomie |
| PM | Personne Morale |
| PS | Professionnel de Santé - Acteur de Santé humain |
| PSSI | Politique de Sécurité des Systèmes d'Information |
| RASS | Référentiel des Acteurs Sanitaires et Sociaux |
| REST | Representational State Transfer |
| RFC | Request For comments<br>Série numérotée de documents officiels publiés par l'IETF |
| 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<br>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 51 : Liste des acronymes et de leur signification**

### 7.2.3 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)<br>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<br>Public (PU) ou Privée (PR) ou Confidentiel (CO) |

**Tableau 52 : Légendes et abréviations utilisées dans les descriptions des attributs et règles**

# 7.3 Web Services et URL pour les transactions

## 7.3.1 URL des services

| Transaction | Description | Opération | URL |
|---|---|---|---|
| TM1.1.1P | WS d'alimentation des comptes MSSanté d'un ou plusieurs domaines de messagerie | WSALIMENTATIONMSS | https://annuaire.mssante.fr/webservices/1011/Alimentation/WSALIMENTATIONMSS |
| TM1.1.1P | WS de récupération du compte-rendu d'alimentation dans l'annuaire national MSSanté | WSCRALIMENTATIONMSS | https://annuaire.mssante.fr/webservices/1011/CR/WSCRALIMENTATIONMSS |
| TM2.1.1A | Consultation de l'annuaire national MSSanté par le protocole LDAP | | ldap://ldap.annuaire.mssante.fr |
| TM2.1.3A | WS de téléchargement de l'annuaire national MSSanté | extractionMSSante | https://annuaire.mssante.fr/webservices/1011/extractionMSSante?format=xml |
| TM2.1.4A | WS de récupération des données d'identités des futurs utilisateurs finaux | extractionIdentitePS | https://annuaire.mssante.fr/webservices/1011 /extractionIdentitePS/?format=csv |
| TM4.1P | Interrogation de la liste blanche des domaines de messagerie MSSanté | | https://listeblanche.mssante.fr/listeblanchemssante.xml |

**Tableau 53 : URL des services**

## 7.3.2 Documents de référence pour les services

| Documents de référence (Documents accessibles sur le site de l'ASIP Santé http://esante.gouv.fr/) | |
|---|---|
| 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 :** exemple de fichier à transmettre à l'ASIP Santé |
| DR5 | **Annuaire :** exemple de feuille de style que les opérateurs peuvent utiliser pour l'affichage du compte-rendu d'alimentation |

**Tableau 54 : Liste des documents de référence pour les services**

## 7.4 Codes d'erreurs

### 7.4.1 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 IssueInstant) est obligatoire dans le jeton VIHF |
| WSMSS04 | La date d'émission de l'assertion SAML (attribut IssueInstant) n'est pas valide, elle doit être antérieure à l'heure d'arrivée de l'assertion et inférieure au délai maximum acceptable |
| WSMSS05 | L'identité de l'émetteur contenue dans le certificat de l'assertion SAML (élément Issuer) est obligatoire dans le jeton VIHF |
| WSMSS06 | Echec d'authentification - L'identité de l'émetteur contenue dans le certificat de l'assertion SAML (élément Issuer) n'est pas présente dans la liste blanche des domaines autorisés |
| WSMSS07 | La date de début de validité de l'assertion SAML (attribut NotBefore de l'élément Conditions) est obligatoire dans le jeton VIHF, si un élément Conditions est présent |
| WSMSS08 | La date de début de validité de l'assertion SAML (attribut NotBefore de l'élément Conditions) n'est pas valide, elle doit être antérieure à l'heure d'arrivée de l'assertion et ultérieure à sa date d'émission |
| WSMSS09 | La date de fin de validité de l'assertion SAML (attribut NotOnOrAfter de l'élément Conditions) est obligatoire dans le jeton VIHF, si un élément Conditions est présent |
| WSMSS10 | La date de fin de validité de l'assertion SAML (attribut NotOnOrAfter de l'élément Conditions) n'est pas valide, elle doit être ultérieure à l'heure d'arrivée de l'assertion |
| WSMSS11 | L'élément Profil_Utilisateur est obligatoire dans le jeton VIHF |
| WSMSS12 | Schéma XML non conforme : message spécifique dépendant de l'erreur rencontré (cf tableau ci-dessous « Liste des contrôles liés à la vérification du schéma XML ») |
| WSMSS13 | La valeur renseignée dans le champ Issuer est différent du DN du certificat d'authentification de l'opérateur |
| WSMSS14 | La valeur renseignée dans le champ Identifiant_structure est différent de l'identifiant structure du certificat d'authentification de l'opérateur |
| WSMSS15 | Le message ne peut pas être déposé dans le SAS de stockage pour être traité |
| WSMSS16 | Le numéro de ticket ne correspond pas au DN du certificat d'authentification de |

| Code erreur | Définition |
|---|---|
| | 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 |
| 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 55 : 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 :<br>1 : FINESS<br>2 : SIREN<br>3 : SIRET |

| Identifiant contrôle | Contrôle appliqué |
|---|---|
| | 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 56 : Liste des contrôles liés à la vérification du schéma XML dans le cas du code WSMSS12

### 7.4.2 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/incorrects, body manquant/incorrect, ...) |
| **401** | Access Denied | L'authentification du client a échoué (dans le cas où une authentification est nécessaire) ou bien le quota d'appel est dépassé |
| **403** | Forbidden | L'authentification du client a réussi mais il n'est pas habilité sur le service ou sur la ressource demandée |
| **404** | Not found | Le service ou la ressource n'a pas été trouvé |
| **405** | Method Not Allowed | La méthode HTTP n'est pas supportée par ce service ou cette ressource |
| **500** | Internal error | Le serveur a rencontré un problème |
| **503** | Service Unavailable | Le service n'est pas disponible pour le moment (ex: serveur surchargé, opération de maintenance, ...) |

Tableau 57 : Liste des messages d'erreurs pour la couche technique des Web Services en REST

### 7.4.3 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 |
| RG_CTR_005 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER », qu'une valeur est présente pour l'attribut « TypeIdentifiantPP » | MSS005 | Le type d'identifiant personne physique est obligatoire pour les BAL MSSanté de type PER - Personnelle | Bloquante |
| RG_CTR_007 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER », qu'une valeur est présente pour l'attribut « IdentifiantPP » | MSS007 | L'identifiant personne physique est obligatoire pour les adresses BAL MSSanté de type PER (Personnelle) | Bloquante |
| RG_CTR_008 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type RPPS ou ADELI (« TypeIdentifiantPP » = « 0 » ou « 8 »), que l'identifiant envoyé est déjà référencé dans la table des Personnes physiques ou de l'historique des identifiants ADELI, s'il s'agit d'un type ADELI. | MSS008 | L'identifiant national du professionnel de santé transmis n'existe pas dans le référentiel des identités PP/PM | Bloquante |
| RG_CTR_009 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP avec identifiant interne (« typeIdentifiantPP »= « 10 »), qu'une valeur est présente pour l'attribut « TypeIdentifiantPM » | MSS009 | Le type d'identifiant de la structure d'activité est obligatoire pour les BAL MSSanté d'un professionnel de santé avec identifiant interne | Bloquante |
| RG_CTR_011 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP », qu'une valeur est présente pour l'attribut « TypeIdentifiantPM » | MSS011 | Le type d'identifiant de la structure d'activité est obligatoire pour les adresses de BAL MSSanté de type Organisationnelle ou Applicative | Bloquante |
| RG_CTR_012 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP », que la valeur envoyée pour l'attribut « TypeIdentifiantPM» fait partie de la nomenclature Type d'identifiant PM | MSS010 | Le type d'identifiant de la structure d'activité transmis n'est pas présent dans la nomenclature de référence utilisée | Bloquante |
| RG_CTR_013 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), qu'une valeur est présente pour l'attribut « IdentifiantPM » | MSS012 | L'identifiant de la structure d'activité est obligatoire pour les adresses de BAL MSSanté d'un professionnel de santé avec identifiant interne | Bloquante |
| RG_CTR_014 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP », qu'une valeur est présente pour l'attribut | 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 ** |
|---|---|---|---|---|
| | « IdentifiantPM » | | 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 (« typeIdentifiantPP »= « 10 »), que la valeur envoyée pour l'attribut « CiviliteExercice » fait partie de la nomenclature Civilité d'exercice | MSS016 | La valeur de la civilité d'exercice n'est pas conforme à la nomenclature utilisée | Bloquante |
| RG_CTR_018 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que la valeur envoyée pour l'attribut « CiviliteExercice » correspond à la profession envoyée | MSS017 | La valeur de la civilité d'exercice n'est pas conforme à la profession transmise pour le professionnel de santé | Bloquante |
| RG_CTR_019 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER », qu'une valeur est présente pour l'attribut « NomExercice » | MSS018 | Le nom d'exercice est obligatoire pour tout professionnel de santé avec ou sans identifiant national | Bloquante |
| RG_CTR_020 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER », qu'une valeur est présente pour l'attribut «PrénomExercice » | MSS019 | Le prénom d'exercice est obligatoire pour tout professionnel de santé avec ou sans identifiant national | Bloquante |
| RG_CTR_021 | Vérification pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type RPPS ou ADELI (TypeidentifiantPP = 0 ou 8) que le contrôle de cohérence entre les valeurs transmises pour Nom/Prénom et les valeurs connues dans l'annuaire national MSSanté est positif.<br>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.<br>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 ** |
|---|---|---|---|---|
| | (« typeIdentifiantPP »= « 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 (« typeIdentifiantPP »= « 10 »), que l'attribut « CategorieProfessions » est référencé dans la table de nomenclature Catégorie de professions | MSS022 | La valeur transmise pour la catégorie de professions n'est pas présente dans la nomenclature de référence utilisée | Bloquante |
| RG_CTR_024 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP avec identifiant interne (« typeIdentifiantPP »= « 10 »), que l'attribut « CategorieProfessions» est alimenté par la catégorie de profession "01" (Professionnel de Santé) | MSS023 | La valeur transmise pour la Catégorie de profession n'est pas autorisée | Bloquante |
| RG_CTR_025 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « Profession» est renseigné | MSS024 | La profession est obligatoire pour la BAL d'un professionnel de santé avec identifiant interne | Bloquante |
| RG_CTR_026 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « Profession » est référencé dans la table de nomenclature Profession | MSS025 | La valeur transmise pour la profession n'est pas présente dans la nomenclature de référence utilisée | Bloquante |
| RG_CTR_027 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 ») que l'attribut « Spécialité » est référencé dans la table de nomenclature Savoir-faire jeux de valeurs Spécialité ou compétence exclusive ou qualification PAC | MSS026 | La valeur transmise pour la spécialité n'est pas présente dans la nomenclature de référence utilisée | Bloquante |
| RG_CTR_028 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « Spécialité » transmis est autorisé pour la Profession envoyée | MSS027 | Cette spécialité n'est pas autorisée pour la profession indiquée | Bloquante |
| 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 | MSS029 | La description est obligatoire pour une BAL de type Applicative ou | Bloquante |

| Identifiant contrôle | Contrôle appliqué | Code erreur | Message d'erreur affiché * | Criticité ** |
|---|---|---|---|---|
| | « Description » est renseigné | | Organisationnelle | |
| RG_CTR_033 | Vérification que si la valeur de « TypeIdentifiantPM » est 2 ou 3, le PM correspondant à « IdentifiantPM » n'a pas de numéro FINESS | MSS032 | L'identification par un SIRET ou SIREN n'est acceptée que si la structure n'a pas de numéro FINESS | Bloquante |
| RG_CTR_034 | Vérification que si l'identifiantPM est renseigné pour un « TypeBAL » = « PER » (de « TypeIdentifiantPP » = « 0 » ou « 8 ») cet identifiant PM correspond bien à une structure associée à la PP du référentiel | MSS033 | L'identifiant de structure fourni ne correspond pas à une structure d'exercice connue de la personne : la BAL est rattachée à la PP et à la structure indiquée dans le flux d'alimentation (et uniquement à cette structure) | Warning |
| RG_CTR_035 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « IdentifiantPP » = attribut « AdresseBAL » | MSS034 | L'identifiant interne pour un professionnel de santé avec identifiant interne doit être identique à la valeur de la BAL MSSanté | Bloquante |
| RG_CTR_036 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type « TypeIdentifiantPP » = « 0 » ou « 8 », que l'attribut « IdentifiantPM » est renseigné avant de prendre en compte la valeur transmise pour l'attribut « ServiceRattachement » | MSS035 | Pour les types de BAL PP RPPS ou ADELI, la valeur indiquée pour le service de rattachement ne peut être prise en compte que si un identifiant de structure est renseigné | Bloquante |
| RG_CTR_037 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER », que la valeur envoyée pour l'attribut « TypeIdentifiantPP » correspond à un code ouvert de la nomenclature Type d'identifiant PP | MSS036 | Le type d'identifiant personne physique transmis est fermé dans la nomenclature de référence utilisée | Warning |
| RG_CTR_038 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que la valeur envoyée pour l'attribut « TypeIdentifiantPM » correspond à un code ouvert de la nomenclature Type d'identifiant PM | MSS037 | Le type d'identifiant de la structure d'activité transmis est fermé dans la nomenclature de référence utilisée | Warning |
| RG_CTR_039 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « ORG » ou « APP », que la valeur envoyée pour l'attribut « TypeIdentifiantPM» correspond à 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 (« typeIdentifiantPP »= « 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 ** |
|---|---|---|---|---|
| | « CiviliteExercice » 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 (« typeIdentifiantPP »= « 10 »), que l'attribut « CategorieProfessions » correspond à un code ouvert de la nomenclature Catégorie de professions | MSS039 | La valeur transmise pour la catégorie de professions est fermée dans la nomenclature de référence utilisée | Warning |
| RG_CTR_042 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 »), que l'attribut « Profession » correspond à un code ouvert de la table de nomenclature Profession | MSS040 | La valeur transmise pour la profession est fermée dans la nomenclature de référence utilisée | Warning |
| RG_CTR_043 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type BAL PP sans identifiant national (« typeIdentifiantPP »= « 10 ») que l'attribut « Spécialité » correspond à un code ouvert de la table de nomenclature Savoir-faire jeux de valeurs Spécialité ou compétence exclusive ou qualification PAC | MSS041 | La valeur transmise pour la spécialité est fermée dans la nomenclature de référence utilisée | Warning |
| RG_CTR_044 | Vérification de l'unicité de l'adresse BAL MSSanté dans le fichier source | MSS042 | L'adresse de la BAL MSSanté doit être unique dans le fichier d'alimentation | Bloquante |
| RG_CTR_045 | Vérification, pour l'enregistrement d'une BAL de « TypeBAL » = « PER » de type ADELI (« TypeIdentifiantPP » = « 0 »), que l'identifiant envoyé est bien l'identifiant national associé au PS au moment de la publication et non un identifiant antérieur (par exemple, l'opérateur doit transmettre le numéro RPPS et plus le numéro ADELI le cas échéant). | MSS043 | L'identifiant national du professionnel de santé transmis n'est plus l'identifiant national valide dans le référentiel des identités PP/PM. | Warning |

**Tableau 58 : 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.

# 7.5 Eléments nécessaires à la réalisation d'une analyse de risque

## 7.5.1 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 illimitées[6]** | **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 | Oui |
| Code malveillant d'origine inconnue | Oui |
| Phénomène naturel | Oui |
| Catastrophe naturelle ou sanitaire | Oui |
| Événement interne | Oui |

**Figure 30 : Types de sources de menaces**

## 7.5.2 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

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

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.

Interfaces d'accès au système de Messageries Sécurisée de Santé (MSSanté) - DSFT - V 1.0.0 - Mars - 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr