DST
V1.3

Interfaces clients de messagerie / opérateurs

du Système de Messageries Sécurisées de Santé (MSSanté)

Dossier des Spécifications Techniques (DST)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

AGENCE DU NUMÉRIQUE EN SANTÉ

0 825 852 000 Service 0,06 € / min + prix appel
Du lundi au vendredi de 8h00 à 20h00
Et le samedi de 8h00 à 14h00

14/01/2022

Identification du document	
Référence ANS	**MSS_FON_DST_interfaces_Clients_MSSanté_v1.3.pdf**
Date de dernière mise à jour	**14/01/2022**
Classification	**Non sensible public**
Nombre de pages	122

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
V0.9.5	14/02/2014	Version diffusée du DST MSSanté Clients de messagerie
V1.0.0	04/07/2014	Corrections de forme et de mise en page. Suppression du chapitre relatif au mécanisme « AutoDiscover ». Fourniture des URL des Web Services de messagerie du service MSSanté de l'ASIP Santé. Suppression du chapitre relatif à la transaction de consultation de l'Annuaire national MSSanté par Web Services.
V1.0.1	29/05/2015	Précisions et correctifs mineurs.
V1.1	20/12/2017	Les mises à jour sont relatives, principalement, à la mise en conformité du DST avec l'IGC Santé. L'ensemble des différences avec la précédente version sont répertoriées en fin de document au paragraphe **Erreur ! Source du renvoi introuvable.**.
V1.2	15/05/2018	Modifications des coordonnées de contact : la bal msscompatibilite@sante.gouv.fr n'est plus accessible. Toutes les demandes relatives à l'espace de confiance MSSanté doivent désormais être adressées à monserviceclient.mssante@asipsante.fr. Ajout des coordonnées de contact sur la page de garde ainsi qu'au paragraphe « 8.5 Canaux de contact ».
V1.3	14/01/2022	Cas particulier des radiologues exerçant en cabinet individuel : Ajout d'un nouveau mode d'authentification via certificat ORG AUTH_CLI sur les interfaces WS SOAP et IMAP/SMTP (voir §3.1 et §8.1.3). Suppression des références à l'IGC CPS en fin de vie en 2020. Correction documentaire : - mss-msg-igcsante.mssante.fr/mss-msg-services remplacé par https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante - pour l'erreur de code 41 du service listFolders le code de retour HTTP est 500 au lieu de 403

Sommaire

1 Introduction

1.1 Objet du document

Ce document décrit en détail les principes et les spécifications techniques permettant d'interfacer :

- un **client de messagerie** avec :
  - le service de messagerie proposé par l'opérateur Mailiz;
  - l'Annuaire santé géré par l'Agence du Numérique en Santé ;
  - le service de messagerie proposé par d'autres opérateurs MSSanté de l'espace de confiance se conformant au présent DST.
- des **opérateurs MSSanté** (dont l'opérateur Mailiz) se conformant au DST Clients de messagerie avec :
  - les clients de messagerie DST compatibles.

*Par convention, la notion de « **client de messagerie** » utilisée dans le présent document désigne un logiciel de type **client lourd de messagerie** ou **logiciel de professionnel de santé (LPS)** intégrant des fonctions de messagerie.*

Les interfaces techniques décrites dans ce document pour le service de messagerie reposent sur deux solutions libres de droits recourant :

- soit à des protocoles standards de messagerie (IMAP et SMTP sur TLS) ;
- soit à des Web Services spécifiques au système MSSanté.

Les moyens d'authentification décrits dans ce document pour accéder à ces différentes transactions sont :

- La carte CPS
- L'identifiant / mot de passe / code d'accès à usage unique *(One Time Password – OTP).*

L'interface technique proposée dans ce document pour la consultation de l'Annuaire santé repose sur une solution LDAP.

Ces spécifications techniques (interfaces et moyens d'authentifications) ne s'imposent pas à l'ensemble des opérateurs de l'espace de confiance MSSanté pour l'interfaçage de leur propre service de messagerie avec le client de messagerie utilisé par l'utilisateur final.

Cependant, **les opérateurs qui le souhaitent peuvent reprendre les spécifications de ce DST** pour faciliter l'interfaçage des clients de messagerie du marché avec leur service, car les protocoles utilisés et les moyens d'authentifications sont connus et largement répandus. Afin favoriser l'interopérabilité des systèmes d'information, les opérateurs se déclarant compatibles au DST client de messagerie se doivent de présenter **l'une et/ou l'autre des deux interfaces techniques (IMAP et SMTP sur TLS, Web Services) adossées à l'un ou l'autre des deux moyens d'authentification (carte CPS, l'identifiant / mot de passe / code d'accès à usage unique) décrit dans le DST Clients de messagerie**. Ainsi les clients de messagerie ayant développés l'une et/ ou l'autre des interfaces associées aux modes d'authentification cités seront compatibles avec les opérateurs conformes au DST Clients de messagerie.

Les opérateurs et éditeurs sont libres de mettre en œuvre les protocoles décrits dans le présent document ou tout autre protocole de messagerie conforme aux exigences réglementaires, y compris des protocoles propriétaires.

Il appartient donc à chaque utilisateur de s'assurer que le client de messagerie qu'il souhaite utiliser est compatible avec les interfaces proposées par son opérateur de messagerie MSSanté. De même, les opérateurs se doivent de communiquer aux éditeurs de clients de messagerie les interfaces et les modes d'authentification mis en place afin de faciliter les raccordements.

1.2 Guide de lecture

Le contexte de mise en œuvre des Messageries Sécurisées de Santé et la présentation de l'espace de confiance MSSanté sont décrits dans le Dossier des Spécifications Fonctionnelles et Techniques des Interfaces d'accès au système de Messageries Sécurisées de Santé ([DSFT-MSSANTE]). Le lecteur est invité à se reporter en particulier aux chapitres 2 et 3 du document pour appréhender le principe de fonctionnement du système des Messageries Sécurisées de Santé.

Le présent Dossier des Spécifications Techniques (DST) est destiné principalement aux profils techniques des éditeurs de Clients de messagerie MSSanté et des opérateurs MSSanté compatibles.

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

- Le chapitre 2 présente le système MSSanté, les opérateurs et les clients de messagerie ;
- Le chapitre 3 liste les transactions MSSanté pouvant être implémentées dans un client de messagerie ;
- Le chapitre 4 décrit les principes de mise en œuvre pour la sécurisation des échanges ;
- Le chapitre 5 décrit les interfaces de messagerie basées sur les protocoles standards de messagerie (IMAP + StartTLS et SMTP + StartTLS) ;
- Le chapitre 6 décrit les interfaces de messagerie basées sur des Web Services de messagerie ;
- Le chapitre 7 décrit la consultation de l'Annuaire santé selon le protocole LDAP ;
- Le chapitre 8 regroupe les annexes dont les environnements de production § 8.1 et de tests § 8.3 de l'opérateur Mailiz, la liste des principaux documents applicables § 8.9.1 (dans l'ensemble du document, ils sont désignés par le code apparaissant dans la colonne « Référence » du tableau de l'annexe) et les définitions communes à plusieurs transactions de Web Services § 8.11 .

1.3 Gestion des versions successives

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

Plusieurs versions majeures de ces spécifications techniques peuvent coexister en même temps, ceci afin de laisser suffisamment de temps aux opérateurs et aux éditeurs pour adapter leurs produits.

Ce document a vocation à évoluer dans le temps afin de prendre en compte les retours remontés par le terrain.

Il est possible d'être automatiquement informé des dernières mises à jour de ce dossier en s'abonnant à la liste de diffusion (8.5 Canaux de contact).

2 Le système MSSanté

2.1 Le système MSSanté

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

Ce système est dénommé « l'espace de confiance MSSanté »

L'espace de confiance MSSanté est le regroupement de tous les opérateurs de messageries sécurisées de santé respectant les règles du DSFT Opérateurs de messagerie ([DSFT-MSSANTE]) et ayant contractualisé avec l'Agence du Numérique en Santé qui en assure sa régulation. L'espace de confiance garantit la confidentialité, l'intégrité et la traçabilité des données qui sont échangées entre chacun des opérateurs qui le composent.

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

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

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

- D'échanger par voie électronique de façon sécurisée des données de santé à caractère personnel entre professionnels habilités (messagerie interprofessionnelle) ;
- D'échanger des contenus structurés entre applicatifs en s'appuyant sur la messagerie (messagerie inter-applicative) ;
- D'alimenter des systèmes d'information (SI) de l'espace de confiance à l'occasion d'échanges de messages entre acteurs de santé.

Cet espace de confiance se caractérise également par :

- L'Annuaire santé s'appuyant notamment sur le répertoire partagé des professionnels de santé et ayant vocation à référencer l'ensemble des professionnels habilités à échanger des données de santé personnelles ;
- Une liste blanche de domaines qui regroupe l'ensemble des domaines de messageries des opérateurs autorisés à échanger dans l'espace de confiance MSSanté ;
- Des référentiels permettant aux industriels de développer des offres conformes et interopérables entre elles. Ces référentiels comportent les documents de référence : le présent DST Clients de messagerie, le DSFT Opérateurs de messagerie ([DSFT-MSSANTE]**)**, les documents applicables listés au 8.9.1, publiés par l'Agence du Numérique en Santé.

Par convention, le présent DST utilise la notion de « professionnel habilité » pour désigner tout professionnel de santé ou non professionnel de santé des secteurs social et médico-social mentionné à l'article L.1110-4 du code de la santé publique et autorisé à collecter, échanger et partager des données de santé à caractère personnel relatives à un patient pour lequel il intervient dans la prise en charge. La liste de ces professionnels a été définie par le décret n° 2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel : article R.1110-2 2° du code de la santé publique.

2.2 Les acteurs de l'espace de confiance MSSanté

2.2.1 Les opérateurs MSSanté

2.2.1.1 Les opérateurs et l'espace de confiance MSSanté

Un opérateur de messageries sécurisées de santé est 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.

Pour proposer un service de messageries sécurisées de santé, un opérateur MSSanté doit avoir conclu le contrat « opérateur MSSanté » ([CONTRAT-MSSANTE]) avec l'Agence du Numérique en Santé, qui a pour objet de déterminer les conditions d'intégration de l'opérateur à l'espace de confiance MSSanté. Ce contrat précise les droits et obligations de chaque partie, ainsi que les pouvoirs de contrôle de l'ANS en sa qualité de gestionnaire de cet espace.

Les opérateurs sont également tenus d'utiliser une solution technique de « Connecteur MSSanté » afin de pouvoir se raccorder techniquement à l'espace de confiance MSSanté.

Les modalités d'intégration d'un opérateur à l'espace de confiance MSSanté sont décrites dans le Dossier des Spécifications Fonctionnelles et Techniques des Interfaces d'accès au système de Messageries Sécurisées de Santé ([DSFT-MSSANTE]).

Le schéma ci-dessous illustre les échanges au sein de l'espace de confiance MSSanté.

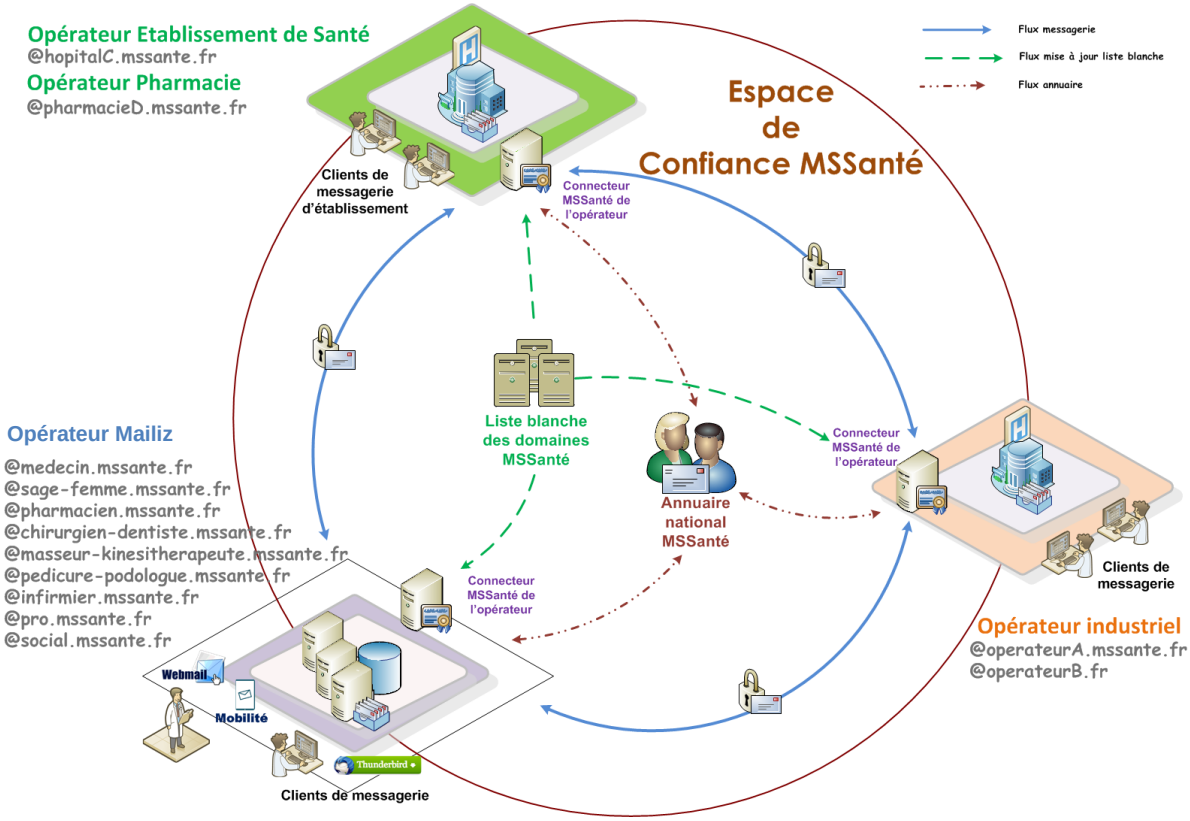

Figure 1 : Echanges au sein de l'espace de confiance MSSanté

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

Les domaines de messagerie MSSanté sont mis en œuvre par les opérateurs MSSanté et permettent d'identifier l'environnement de messagerie sur lequel sont hébergées une ou plusieurs boites aux lettres (BAL) des opérateurs.

Les échanges de messages ne sont autorisés qu'entre les domaines de messagerie MSSanté répertoriés au sein d'une « liste blanche ». La liste blanche est un fichier géré par l'Agence du Numérique en 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 échanges de messages se font donc exclusivement entre utilisateurs (personnes physiques et morales) des services de messagerie mis en œuvre par les opérateurs MSSanté.

2.2.1.2 Les opérateurs et leurs boites aux lettres (BAL) MSSanté

Il existe trois types de boîtes aux lettres sécurisées dans l'espace de confiance MSSanté.
Celles-ci peuvent être affectées à des personnes physiques (boite aux lettres personnelles), à des groupes d'utilisateurs (boite aux lettres organisationnelles) ou à des applications (boite aux lettres applicatives).
Les opérateurs MSSanté sont libres de proposer les types de BAL de leur choix et ont la possibilité de définir les offres qui leur semblent pertinentes (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 le DSFT [DSFT-MSSANTE]).

Ainsi, un 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 proposé par les ordres professionnels, de type @profession.mssante.fr ;
- Une boîte aux lettres au titre de son exercice dans des établissements de santé, de type @etablissementA.mssante.fr ou @etablissementB-securise.mssante.fr ;
- Une boîte aux lettres sur le domaine hébergé par un opérateur industriel, du type @domaineY.mssante.fr.

Ces différentes adresses seront publiées par les différents opérateurs dans l'Annuaire santé pour cet utilisateur.
Pour plus de précisions, se reporter au DSFT Opérateurs de messagerie ([DSFT-MSSANTE]).

2.2.1.2.1 Boîtes aux lettres personnelles

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

Pour plus d'information concernant les BAL personnelles, se reporter au DSFT Opérateurs de messagerie ([DSFT-MSSANTE].

2.2.1.2.2 Boites aux lettres organisationnelles

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

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

Les professionnels habilités seront donc en capacité d'accéder à la même boîte aux lettres et d'émettre des messages au nom du secrétariat/service/pôle (et non pas à titre personnel).
Exemple de mise en œuvre : Ces BAL organisationnelles peuvent être utilisées, par exemple, par les secrétaires médicales, sous la responsabilité d'un professionnel habilité, pour faciliter l'envoi de compte-rendu et la réception de mail dans un établissement de santé. Dans ce cas, c'est à l'établissement de santé de gérer les habilitations et les accès à cette BAL organisationnelle en fonction de la politique de sécurité de son SI.

Pour plus d'information concernant les BAL organisationnelles, se reporter au DSFT Opérateurs de messagerie ([DSFT-MSSANTE]).

2.2.1.2.3 Boites aux lettres applicatives

Elles sont associées à un logiciel métier ou à une machine (dossier patient informatisé, système d'information de laboratoire, serveur de résultats, etc…) et sont accédées directement par le logiciel ou la machine. Elles sont utilisées à des fins d'envois ou de réception automatisés.
Exemple de mise en œuvre: Si un Dossier Patient Informatisé (DPI) dispose du nom du médecin traitant, et son adresse MSSanté, le compte-rendu peut partir directement du Dossier Patient Informatisé vers la BAL du médecin.

Pour plus d'information concernant les BAL applicatives, se reporter au DSFT Opérateurs de messagerie ([DSFT-MSSANTE]).

2.2.2 L'Agence du Numérique en Santé

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

- **Gestionnaire de l'espace de confiance MSSanté** qui inclut la gestion de l'Annuaire santé et l'administration de la liste blanche qui regroupe l'ensemble des domaines de messagerie des opérateurs autorisés à échanger au sein de l'espace de confiance MSSanté. En cette qualité, l'ANS Santé définit les règles d'intégration à l'espace de confiance MSSanté. Ces règles sont énoncées dans le contrat relatif à l'intégration à l'espace de confiance appelé contrat « opérateur MSSanté » [CONTRAT-MSSANTE] conclu entre l'ANS et tout opérateur souhaitant intégrer l'espace de confiance MSSanté.
- **Opérateur pour le compte des ordres professionnels d'un service de messagerie « Mializ » sur les domaines pro.mssante.fr et des Ordres professionnels.** L'ANS offre un service standard de messagerie, mis à disposition des professionnels habilités afin d'amorcer la dynamique du système,

  En tant qu'opérateur, l'ANS met à disposition de ses utilisateurs plusieurs modes d'accès à la messagerie sécurisée :

  - un webmail accessible depuis le site de l'opérateur Mailiz (se reporter au paragraphe 8.1.1.1);
  - un client de messagerie Thunderbird téléchargeable sur le site de l'opérateur Mailiz (se reporter au paragraphe 8.1.2.2) ;
  - une application mobile de l'opérateur Mailiz téléchargeable sur l'Apple Store (iOS) ou Google Play (Android) (se reporter au paragraphe 8.1.2.1) ;
  - des interfaces destinées aux clients de messagerie intégrés à des logiciels de professionnel de santé (voir le présent DST Clients de messagerie).

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

Le présent Dossier des Spécifications Techniques (DST), publié par l'ANS Santé est à destination :

- des éditeurs de logiciels comportant des fonctionnalités de **client de messagerie** et **souhaitant accéder :**
  - **au service de messagerie MSSanté proposé par l'opérateur Mailiz,**
  - **au service de messagerie MSSanté proposé par d'autres opérateurs de l'espace de confiance se conformant au DST**,
  - **à l'Annuaire santé.**
- des opérateurs MSSanté se conformant au DST Clients de messagerie pour l'interfaçage de leur propre service de messagerie avec les clients de messagerie DST compatibles.

Des environnements de tests sont également mis à disposition par l'opérateur Mailiz pour permettre aux éditeurs de logiciels comportant des fonctionnalités de **client de messagerie** et ayant développés les interfaces techniques avec les modes d'authentification décrits dans le DST (et implémentées par l'opérateur Mailiz et les opérateurs compatibles DST) de tester leurs solutions. Pour plus de détail, voir § 8.3 « Les environnements de tests de l'opérateur ».

2.2.3 Les utilisateurs finaux

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

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

2.3 Les clients de messagerie

2.3.1 LPS et clients de messagerie MSSanté

Les fonctions de messageries sécurisées de santé sont accessibles aux professionnels habilités à travers 2 grands types de logiciels :

- Les Logiciels de Professionnels de Santé (LPS)
- Les clients de messagerie

Par convention, la notion de « **client de messagerie** » utilisée dans le présent document désigne un logiciel de type **client lourd de messagerie** ou **logiciel de professionnel de santé (LPS)** intégrant des fonctions de messagerie, en capacité de réaliser :

- les tâches classiques de messagerie (envoyer, recevoir et stocker des courriers électroniques) ;
- la recherche de boîtes aux lettres (BAL) dans l'Annuaire santé.

Ils peuvent en outre effectuer certaines tâches d'administration et de gestion de messagerie, 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.

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'ANS est donc de permettre une intégration aussi harmonieuse que possible entre le LPS et les messageries sécurisées du système MSSanté. Il est donc important que les opérateurs MSSanté se déclarant compatibles au DST Clients de messagerie implémentent les interfaces et les modes d'authentification décrits dans le présent document.

Un même professionnel de santé peut avoir à utiliser un LPS et un client de messagerie, en fonction de sa pratique du moment. Par exemple, un professionnel de santé libéral peut utiliser son LPS lorsqu'il est dans son cabinet et utiliser un client de messagerie lorsqu'il est en déplacement.

Dans les 2 cas, les fonctions de messageries doivent s'intégrer de façon harmonieuse pour offrir aux professionnels de santé des solutions de messagerie simples et souples d'utilisation.

Ainsi, chaque client de messagerie ou LPS MSSanté doit pouvoir permettre à ses clients / utilisateurs de :

- ✓ paramétrer une adresse mail sécurisée,
- ✓ d'intégrer les fonctionnalités d'interrogation de l'Annuaire santé proposées par l'ANS,
- ✓ d'intégrer les fonctionnalités d'émission et de réception de messages proposées par un opérateur MSSanté, en cohérence avec les interfaces DST ou propriétaires proposées par cet opérateur.

Comme indiqué précédemment, pour faciliter l'interfaçage des clients de messagerie du marché avec leur service**, les opérateurs qui le souhaitent peuvent reprendre les spécifications de ce DST (interfaces techniques et moyens d'authentification)**. Le respect des présentes spécifications n'est encadré par **aucun processus de vérification, d'homologation ou de contrôle par l'ANS**, compte tenu du caractère standard des procédés techniques à mettre en œuvre par les éditeurs et les opérateurs MSSanté.

2.3.2 Gestion simultanée des BAL MSSanté et des autres BAL de l'utilisateur

Au-delà de l'accès aux boîtes aux lettres MSSanté, les clients de messagerie peuvent tout à fait gérer simultanément des boîtes aux lettres non MSSanté et proposer à l'utilisateur une réconciliation locale des messages de ses différentes boîtes aux lettres (fonction classique de ces types de logiciels, indépendamment de la problématique MSSanté).

Il n'est cependant pas possible d'envoyer simultanément un même message à des destinataires MSSanté et à des destinataires non MSSanté : il doit alors s'agir de deux messages différents.

Conformément à la réglementation en vigueur, l'échange de données de santé personnelles par messagerie ne doit être fait qu'avec une messagerie « sécurisée ». Il est donc fortement recommandé aux éditeurs de clients de messagerie MSSanté proposant des fonctionnalités de réconciliation locale de plusieurs BAL de mettre en œuvre des messages d'alerte explicites lorsqu'un utilisateur essaie d'associer dans un même message des destinataires MSSanté et des destinataires non MSSanté.

Pour plus d'information concernant ce point, il est conseillé de se reporter au Dossier des Spécifications Fonctionnelles et Techniques des Interfaces d'accès au système de Messageries Sécurisées de Santé ([DSFT-MSSANTE]).

2.3.3 Gestion des paramètres fonctionnels du client de messagerie

Tout service MSSanté proposé par un opérateur dispose de paramètres de fonctionnement susceptibles d'évoluer (nom du serveur SMTP, nom du serveur de boîte aux lettres, etc.). Le changement d'un de ces paramètres par l'opérateur peut affecter le client de messagerie MSSanté.

Il est recommandé que la récupération et la gestion de ces paramètres par un client de messagerie MSSanté soit dynamique, afin que la mise à jour de ces paramètres ne nécessite pas le déploiement d'une nouvelle version ou d'action manuelle de la part des utilisateurs.

2.3.4 Interopérabilité des échanges de données de santé structurées

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

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

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

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

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

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

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

Remarque : Pour plus de détails, un guide concernant l'échange de documents de santé structurés par la MSSanté [ECHANGES-STRUCTURES-MSSANTE] est disponible en téléchargement via le lien suivant https://www.mssante.fr/is/doc-technique.

3 Présentation des transactions MSSanté

3.1 Liste des transactions MSSanté

Les transactions MSSanté[1] décrites dans ce document et pouvant être mises en œuvre dans un client de messagerie et chez un opérateur MSSanté compatibles au présent document sont :

- **Les transactions de messagerie basées sur les protocoles standards de messagerie** (SMTP + StartTLS et IMAP + StartTLS) ;
- **Les transactions de messagerie basées sur les Web Services spécifiques au système MSSanté définis dans ce document.**

La transaction de consultation de l'Annuaire santé par le protocole LDAP peut également être mise en place par les éditeurs de clients de messagerie.

Les spécifications détaillées de ces transactions MSSanté sont décrites aux chapitres 5 à 7 du présent document.

Un client de messagerie souhaitant s'interfacer avec un opérateur de messagerie MSSanté doit mettre en œuvre les transactions compatibles avec celles proposées par cet opérateur.

Cas de l'opérateur Maiiz
L'opérateur Malliz propose toutes les transactions et moyens d'authentification décrits dans ce document. Un client de messagerie souhaitant s'interfacer avec l'opérateur Mailiz doit donc implémenter : ▪ Les transactions de messagerie basées sur les protocoles standards de messagerie (SMTP + StartTLS et IMAP + StartTLS) avec **authentification en CPS uniquement,** ▪ Et/ou Les transactions de messagerie basées sur les Web Services avec **authentification par CPS ou identifiant / mot de passe / code d'accès à usage unique *(One Time Password – OTP)***. Dans le cas particulier des cabinets individuels de radiologie disposant d'un identifiant dit « RPPS Rang », Mailiz permet l'authentification via des certificats ORG AUTH_CLI sur les interfaces Web Services et sur les interfaces IMAP/SMTP. Pour plus de détails se reporter au §8.1.3.

[1] Les transactions MSSanté sont abrégées dans le document sous la forme « TM » (Transaction MSSanté).

Les opérateurs de messagerie MSSanté peuvent proposer les transactions et les moyens d'authentification décrits dans ce document mais ils peuvent également proposer d'autres transactions s'appuyant sur des protocoles différents et d'autres modes d'accès spécifiques aux BAL MSSanté qu'ils hébergent (Webmail, client de messagerie propriétaire).

Transactions MSSanté		Description de la transaction
Emission et réception de messages sur les protocoles standards de messagerie		
TM3.1C	Gestion des messages de la BAL MSSanté par IMAP + StartTLS	Consultation et gestion des messages MSSanté et des dossiers de classement sous le protocole IMAP + StartTLS
TM3.2C	Emission de messages par SMTP + StartTLS	Emission de messages sous le protocole SMTP + StartTLS
TM3.3C	Auto configuration du client de messagerie	Auto configuration du client de messagerie utilisant les protocoles standards de messagerie
Emission et réception de messages par Web Services		
TM4.1.1C	Authentification par carte CPS	Gestion de l'authentification préalable à l'appel des Web Services MSSanté
TM4.1.2C	Authentification par identifiant / mot de passe / OTP	Gestion de l'authentification préalable à l'appel des Web Services MSSanté
TM4.2.xC	Consultation et gestion des dossiers	7 transactions Web Services sont associées à cette transaction
TM4.3.xC	Envoi et gestion de messages	5 transactions Web Services sont associées à cette transaction
TM4.4.xC	Envoi et consultation des pièces jointes	3 transactions Web Services sont associées à cette transaction
TM4.5.xC	Consultation et recherche de messages	2 transactions Web Services sont associées à cette transaction
TM4.6C	Recherche de boîtes aux lettres	Permet de retrouver la liste des boîtes aux lettres associées à un utilisateur
Annuaire santé		
TM2.1.1C	Consultation de l'Annuaire santé en LDAP	Recherche multicritères de correspondants dans l'Annuaire santé par le protocole LDAP

Tableau 1 : Liste des transactions MSSanté pour les clients de messagerie

3.2 Exemple d'enchainement d'appels de transactions MSSanté

3.2.1 Récupération des messages par les Web Services lors de la première connexion

La cinématique globale pour récupérer l'ensemble des messages lors de la première connexion peut être la suivante :

1. Appel du Web Service « listFolders » (**TM4.2.1C**) pour avoir la liste des dossiers et le nombre de messages non lus associés à chaque dossier.
2. Si besoin, appel du Web Service « syncMessages » (**TM4.3.5C**) pour récupérer le token de synchronisation (qui servira pour les rafraichissements).
3. Appel du Web Service « searchMessages » (**TM4.5.1C**) avec les critères souhaités. Par défaut, ce service renvoie tous les messages de la boite de réception.

4 La sécurisation des échanges

Quels que soient les transactions et protocoles utilisés, la sécurisation des échanges des services de messagerie sécurisée MSSanté reposent sur :

- l'établissement d'un **canal TLS** entre le client de messagerie et le serveur de l'opérateur MSSanté,
- une **authentification forte** de l'utilisateur.

4.1 Accès par les protocoles standards de messagerie

Dans ce cas, la sécurisation des échanges repose sur l'établissement d'un **canal TLS avec authentification mutuelle** entre le client de messagerie et le serveur de l'opérateur MSSanté.

Pour les clients de messagerie conformes au DST Clients de messagerie, l'établissement de ce canal TLS nécessite obligatoirement l'utilisation de la carte CPS.

Les protocoles SMTP + StartTLS et IMAP + StartTLS permettent d'assurer l'identification et l'authentification réciproque du client et des serveurs et d'assurer la confidentialité des échanges.

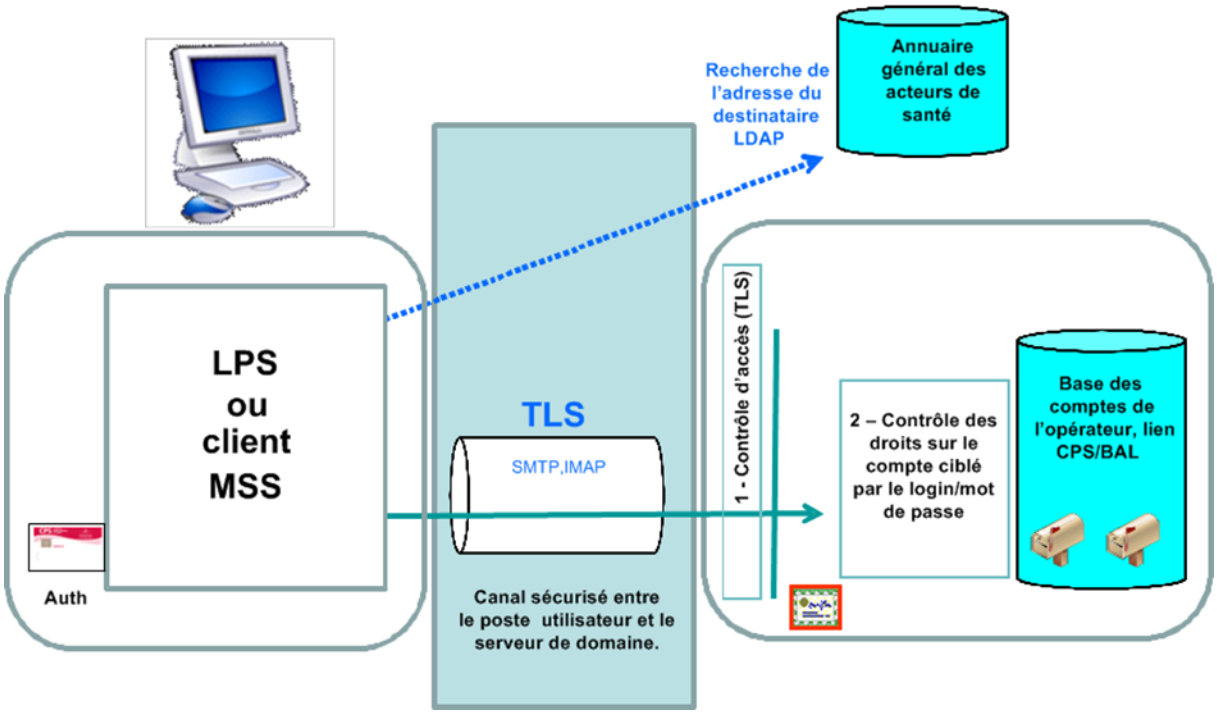

Figure 2 : Sécurisation des échanges entre un client de messagerie et un opérateur de service MSSanté avec un protocole standard de messagerie

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 émis l'IGC Santé ;
- 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).

Tous opérateurs MSSanté
Sur le service des opérateurs MSSanté compatibles avec le présent DST (dont l'opérateur Mailiz), le seul moyen d'authentification pour les transactions de messagerie basées sur les protocoles standards de messagerie (SMTP + StartTLS et IMAP + StartTLS) est **la carte CPS**.

4.2 Accès par Web Services

Dans ce cas, la sécurisation des échanges repose sur l'établissement d'un **canal TLS** entre le client de messagerie et le serveur de l'opérateur MSSanté et sur une **authentification préalable**, matérialisée par l'obtention d'un **jeton d'authentification** qui permet de s'assurer de l'identité de l'utilisateur et d'établir une session authentifiée sur le service de messagerie cible.

L'obtention du jeton d'authentification se base :

- soit sur une authentification par carte CPS (établissement d'un canal TLS avec authentification mutuelle),
- soit sur un mécanisme d'authentification équivalent (établissement d'un canal TLS asymétrique) dès lors que cette authentification est matérialisée par l'usage d'un jeton d'authentification SAML 2.0, fourni par un service d'authentification dédié mis en œuvre par l'opérateur de messagerie (le mécanisme d'authentification est donc distinct des Web Services de messagerie).

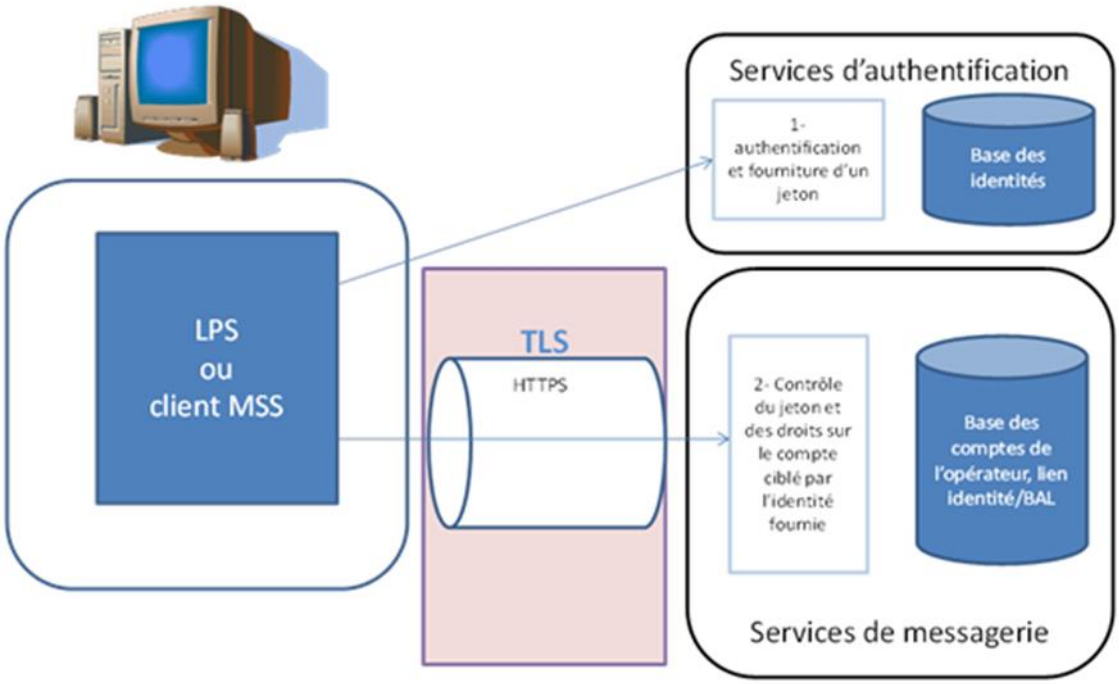

Figure 3 : Sécurisation des échanges entre un client de messagerie et un opérateur MSSanté exposant des Web Services de messagerie

Les opérateurs de messagerie sont libres d'utiliser les Web Services MSSanté, tout en offrant des moyens d'authentification forte, par carte CPS ou tout autre dispositif équivalent, conformes aux exigences réglementaires et permettant d'attribuer à tout utilisateur son numéro d'identification nationale de professionnel de santé s'il en possède un (numéro RPPS ou numéro ADELI). Cependant afin de favoriser l'interopérabilité, les opérateurs se déclarant conformes au DST doivent mettre en place un des deux modes d'authentification décrits ci-dessus (CPS ou identifiant/mdp/OTP).

Remarque : Les moyens d'authentification doivent garantir la sécurité et la confidentialité des accès aux données contenues dans le système MSSanté et doivent être choisis notamment en fonction des résultats de l'analyse de risques et en conformité avec le référentiel d'authentification des acteurs de santé de la PGSSI-S.
Ces moyens seront notamment appréciés par la Commission Nationale de l'Informatique et des Libertés (CNIL) et le Comité d'Agrément des Hébergeurs (CAH), le cas échéant.

Tous opérateurs MSSanté
Pour les opérateurs MSSanté compatibles avec le présent DST (dont l'opérateur Mailiz), les moyens d'authentification permettant l'obtention du jeton d'authentification sont : ▪ soit la carte CPS, ▪ soit l'identifiant / mot de passe / code d'accès à usage unique (*One Time Password* – OTP). Pour l'authentification par identifiant / mot de passe / OTP : ▪ pour l'opérateur Mailiz, un enrôlement préalable du professionnel de santé sur le Webmail est nécessaire. En effet, cette authentification ne peut être mise en œuvre qu'une fois la BAL créée (l'opération d'autocréation de BAL nécessitant une authentification par carte CPS) ; ▪ l'OTP peut être récupéré par l'utilisateur par SMS ou par mail ;

L'accès aux services, après obtention du jeton d'authentification :

En dehors de l'authentification, l'accès aux Web Service de messagerie se fait sur HTTPS, avec l'établissement d'une connexion TLS avec authentification asymétrique quel que soit le moyen d'authentification utilisé (CPS ou OTP).

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.

4.3 Canal TLS

Quels que soient les transactions et protocoles utilisés, un canal TLS doit être établi entre le client de messagerie et le serveur de l'opérateur MSSanté.

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). Il est par ailleurs fortement recommandé de supporter la version TLS 1.2.

4.4 Bonnes pratiques pour l'accès par CPS

Dans le cas où la carte CPS est utilisée pour sécuriser les échanges, la mise en œuvre d'un mécanisme de détection d'arrachage de carte, qui le cas échéant déconnectera l'utilisateur du service MSSanté (en invalidant sa session TLS et en coupant ses sockets TCP/IP par exemple ou, à discrétion, en bloquant le logiciel ou en le fermant), constitue une bonne pratique pour réduire le risque d'accès illégitime à sa BAL.

Des préconisations techniques et des exemples d'implémentation sont disponibles dans la documentation ANS: « ASIP-PTS-PSCE_Guide-implementation-detection-arrachage-CPS_v1.0.3.pdf » **Erreur ! Source du renvoi introuvable.** disponible à l'adresse suivante : http://integrateurs-cps.asipsante.fr/documents/Guide-impl-arrachage-CPS (accès réservé aux titulaires d'un compte Editeurs CPS).

4.5 Vérification des certificats serveurs

4.5.1 Principe général

Le certificat présenté par le serveur d'un opérateur MSSanté sur les interfaces clients de messagerie doit avoir été émis par l'IGC Santé gamme Elémentaire domaine Organisation.

Des précisions sur le certificat utilisé par les serveurs des opérateurs MSSanté sont disponibles à l'adresse suivante :

- IGC Santé : http://igc-sante.esante.gouv.fr/PC/#ca et http://integrateurs-cps.asipsante.fr/IGC-Santé,

Gestion de plusieurs chaînes de certification

Le client de messagerie doit être en mesure de gérer la chaine de certification IGC Santé gamme Elémentaire domaine Organisation.

Le client de messagerie doit être en capacité de valider le certificat serveur 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), RFC 2034 (http://tools.ietf.org/html/rfc2034) et RFC 3501 (voir http://tools.ietf.org/html/rfc3501).

Certificats d'autorité

L'ANS assure le rôle d'autorité de certification (AC) pour les certificats IGC Santé et IGC CPS. Les certificats d'autorité de ces deux AC doivent être déployés sur le client de messagerie afin d'accepter les certificats présentés par les opérateurs MSSanté.

Les certificats IGC Santé sont issus de l'AC intermédiaire IGC Santé « domaine Organisation » subordonnée à l'AC racine IGC Santé « gamme Elémentaire ». Les certificats d'autorité (racine et intermédiaire) sont disponibles à l'adresse suivante : http://igc-sante.esante.gouv.fr/PC/#ca

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).

Remarque : il est demandé de bien valider le certificat serveur à l'aide de l' autorité émettrice IGC Santé. En effet, l'ajout du certificat du serveur de l'opérateur MSSanté comme autorité de confiance dans le client de messagerie n'est pas adapté car, à terme, lors du renouvellement du certificat du serveur de l'opérateur MSSanté (tous les 3 ans), cette mesure obligerait à mettre à jour tous les clients de messagerie MSSanté déployés sur le poste des PS.

4.5.2 Bonnes pratiques pour la vérification des certificats serveurs et des cartes CPS

Contrôle de non révocation

Le contrôle de révocation des certificats du serveur de l'opérateur MSSanté et de la carte CPS constitue une bonne pratique en termes de sécurisation des échanges.

Le contrôle de révocation de ces certificats peut se faire par téléchargement des CRL. Les CRL des AC GIP-CPS et IGC Santé sont mises à jour quotidiennement, des delta-CRL sont également publiées permettant ainsi d'optimiser la mise à jour des CRL si besoin.

Les CRL IGC Santé sont disponibles sur le site : http://igc-sante.esante.gouv.fr/PC/#ca.

Ces CRL sont également disponibles sur un serveur LDAP aux adresses suivantes:

- IGC Santé : ldap://annuaire-igc.esante.gouv.fr

Un guide [PSCE-GUIDE-CRL] est disponible en téléchargement à l'adresse suivante : http://integrateurs-cps.asipsante.fr/node/179. Celui-ci détaille les bonnes pratiques pour la récupération des CRL.

L'IGC Santé dispose également d'un répondeur OCSP (Online Certificate Status Protocol) à l'adresse suivante : http://ocsp.esante.gouv.fr. Il est conforme à la RFC 6960 (https://tools.ietf.org/html/rfc6960).

Vérification des certificats d'autorité stockés dans les magasins de confiance

Pour assurer la sécurité des applications intégrant des certificats d'autorité, il est recommandé avant installation de ces certificats dans les magasins de confiance du serveur de l'opérateur MSSanté ou du client de messagerie de comparer leur empreinte numérique avec celle de la source de confiance :

- IGC Santé: http://igc-sante.esante.gouv.fr/PC/#ca,
-

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

- 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.

Il est également recommandé d'effectuer cette vérification de manière périodique afin de s'assurer qu'aucune modification (involontaire ou volontaire) n'a eu lieu sur les certificats d'autorité stockés dans les magasins de confiance.

5 Transactions basées sur les protocoles standards de messagerie

Tous opérateurs MSSanté
Sur le service des opérateurs MSSanté compatibles avec le présent DST (dont l'opérateur Mailiz), le seul moyen d'authentification pour les transactions de messagerie basées sur les protocoles standards de messagerie (SMTP + StartTLS et IMAP + StartTLS) est **la carte CPS**.

Les transactions suivantes s'exécutent entre l'opérateur MSSanté et le client de messagerie qui s'authentifient mutuellement lors de l'établissement de la session TLS.

L'opérateur MSSanté s'authentifie à l'aide d'un certificat issu de l'IGC Santé gamme Elémentaire domaine Organisation.

Le client de messagerie présente à l'opérateur MSSanté le certificat de la carte CPS issu de l'IGC Santé gamme Forte domaine Personne Physique.

5.1 TM3.1C – Gestion des messages de la BAL par IMAP + StartTLS

Le client de messagerie permet à l'utilisateur, via le protocole IMAP + StartTLS, de relever ses messages et de gérer les dossiers de sa BAL MSSanté hébergée par un opérateur MSSanté.

La gestion des messages et des dossiers (consultation, suppression, déplacement, …) est effectuée sur le protocole IMAP4, dans une session TLS avec le serveur IMAP de l'opérateur MSSanté. Avec le protocole IMAP les messages et les dossiers peuvent être gérés directement sur le serveur.

5.1.1 Cinématique

Les étapes de « connexion / gestion des messages de la BAL / fin de session » d'un client de messagerie sur le serveur IMAP d'un opérateur MSSanté sont les suivantes :

1) Le client de messagerie se connecte au serveur de l'opérateur MSSanté en IMAP et STARTTLS[2] comme défini dans les RFC 3501 et RFC 2246 (voir http://tools.ietf.org/html/rfc3501 et http://tools.ietf.org/html/rfc2246) ;
2) Le serveur IMAP vérifie le certificat TLS du client comme défini dans la RFC 2246 (voir http://tools.ietf.org/html/rfc2246) ;
3) Le client de messagerie réalise une authentification PLAIN comme défini dans la RFC 3501 (voir http://tools.ietf.org/html/rfc3501) : cette méthode permet d'ajouter une information de connexion portant sur l'adresse mail de la BAL à laquelle le client de messagerie veut accéder ;
4) Le serveur s'assure que le certificat utilisé pour la connexion correspond bien à l'adresse mail utilisée dans l'identifiant de connexion ;
5) Le client de messagerie envoie les commandes IMAP au serveur dans la session TLS, conformément au protocole IMAP4, en fonction des actions exécutées par l'utilisateur comme défini dans la RFC 3501 (voir http://tools.ietf.org/html/rfc3501) ;
6) Fin de la session IMAP comme défini dans la RFC 3501 (voir http://tools.ietf.org/html/rfc3501).

[2] Lors de la connexion en STARTTLS, le serveur envoie un certificat au client et le client doit valider ce certificat.

5.1.2 Transaction

Les commandes IMAP envoyées par le client de messagerie doivent être conformes à la RFC 3501 (voir http://tools.ietf.org/html/rfc3501).

5.2 TM3.2C - Emission de messages par SMTP + StartTLS

Le client de messagerie permet à l'utilisateur, via le protocole SMTP + StartTLS, d'émettre des messages vers des destinataires titulaires de BAL sur des domaines MSSanté hébergés par un opérateur MSSanté.

L'émission de messages est effectuée sur le protocole SMTP, dans une session TLS mutuelle avec le serveur SMTP de l'opérateur MSSanté.

Limitation du nombre de destinataires mise en œuvre par les opérateurs MSSanté :

Afin de réduire les risques d'émission de messages non sollicités, les opérateurs MSSanté, conformément à l'exigence correspondante du DSFT Opérateurs [DSFT-MSSANTE], limitent le nombre de destinataires d'un message à 40 au maximum.

5.2.1 Cinématique

Les étapes de « connexion / envoi du message / fin de session » pour un client de messagerie émettant une requête vers un serveur de messagerie MSSanté sont les suivantes :

1) 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) ;
2) 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) ;
3) Vérification du certificat serveur présenté par le serveur de messagerie de l'opérateur comme défini dans la RFC 2246 (http ://tools.ietf.org/html/rfc2246) ;
4) 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) ;
5) Fin 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).

5.2.2 Transaction

Les commandes SMTP envoyées par le client de messagerie doivent être conformes à la RFC 5321 (voir http://tools.ietf.org/html/rfc5321).

Implémentation d'un User-Agent :

Il est recommandé que les clients de messagerie implémentent un « User-Agent » afin de permettre de les identifier, comme défini au paragraphe 3.2.13 de la RFC 5336 (voir http://tools.ietf.org/html/rfc5536#section-3.2.13).

5.3 TM3.3C - Auto configuration du client de messagerie

Un client de messagerie peut utiliser des Web Services d'auto-configuration proposés par les opérateurs MSSanté.

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

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 MSSanté se charge donc de mettre à disposition ces Web Services pour chacun des domaines et des clients de messagerie pour lesquels il souhaite proposer un service d'auto-configuration.

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

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

Les clients de messagerie les plus utilisés implémentent nativement l'interrogation d'un service d'auto-configuration.

Tous opérateurs MSSanté
Les opérateurs MSSanté compatibles avec le présent DST (dont l'opérateur Mailiz), mettent à disposition ces WebServices d'auto-configuration pour chacun de leurs domaines de messagerie MSSanté.

5.3.1 Cinématique AutoConfig

Les étapes d'auto-configuration d'un client de messagerie utilisant le service « AutoConfig » sur une BAL hébergée par un opérateur MSSanté sont les suivantes :

- [Utilisateur] L'utilisateur saisit l'adresse de messagerie MSSanté à configurer via les IHM prévues dans le client de messagerie ;
- [Client] Le client de messagerie identifie le domaine de messagerie MSSanté concerné ;
- [Client] Le client de messagerie :
    - Identifie ou non la disponibilité du Web Service sur ce domaine en recherchant sa présence sur l'URL suivante accessible en http (mais pas en https) : **Erreur ! Référence de lien hypertexte non valide.**>

Cas de l'opérateur Mailiz
par exemple, dans le cas d'un médecin sur le service de l'opérateur Mailiz: https://autoconfig.medecin.mssante.fr/mail/config-v1.1.xml?emailaddress=prenom.nom@medecin.mssante.fr)

    - Définit, le cas échéant, les paramètres du compte de messagerie pour l'adresse de messagerie renseignée par l'utilisateur ;
- [Utilisateur] L'utilisateur valide les paramètres de messagerie proposés par le service via l'IHM du client de messagerie ;
- [Client] Le client de messagerie se connecte à la BAL MSSanté et synchronise ses données ;
- Fin du processus.

5.3.2 Transaction AutoConfig

Les commandes envoyées par le client de messagerie doivent être conformes aux spécifications fournies par l'éditeur à l'adresse suivante : https://wiki.mozilla.org/Thunderbird:Autoconfiguration.

6 Transactions de messagerie basées sur les Web Services

Plusieurs transactions de Web Services SOAP permettant de mettre à disposition des fonctionnalités comparables à celles offertes par les protocoles standards IMAP et SMTP sont proposées et décrites dans les paragraphes suivants :

Elles permettent à l'utilisateur :

- De s'authentifier (authentification forte matérialisée par la récupération d'un jeton fourni par un service d'authentification dédié mis en œuvre par l'opérateur de messagerie) ;
- De relever ses messages et de gérer les dossiers de sa BAL MSSanté hébergée par un opérateur MSSanté ;
- D'émettre des messages vers des destinataires titulaires de BAL sur des domaines hébergés par un opérateur MSSanté.

Les types de données et les énumérations communes à plusieurs transactions sont définis en annexe au paragraphe 8.11.

Les transactions suivantes s'exécutent entre l'opérateur MSSanté et le client de messagerie qui s'authentifient mutuellement lors de l'établissement de la session TLS.

L'opérateur MSSanté s'authentifie à l'aide d'un certificat issu de l'IGC Santé gamme Elémentaire domaine Organisation.

En cas d'authentification par carte CPS, le client de messagerie présente à l'opérateur MSSanté le certificat de la carte CPS issu de l'IGC Santé gamme Forte domaine Personne Physique.

6.1 TM4.1.xC - Authentification préalable pour les appels de Web Services

6.1.1 Principe général

Les Web Services de messagerie décrits dans les chapitres suivants s'appuient sur l'usage de jetons d'authentification (assertions SAML) obtenus auprès d'un *Service d'authentification*.

Ce mécanisme d'**authentification préalable** comporte 5 étapes :

1) **Tentative de connexion du client de messagerie au Service de messagerie.**
2) **Réponse du Service de messagerie au client de messagerie.**
   Si la session n'est pas active ou que la session est expirée, le Service de messagerie :
   - fourni un cookie de session (« JSESSIONID ») et
   - demande au client de messagerie de s'authentifier sur le *Service d'authentification* (présence d'un élément « AuthnRequest »).
3) **Requête du client de messagerie au Service d'authentification** (avec l'élément « AuthnRequest » fourni par le Service de messagerie) **pour récupérer un jeton d'authentification**.
4) **Réponse du Service d'authentification au client de messagerie** avec :
   - le jeton d'authentification (assertion SAML 2.0).
5) **Connexion du client de messagerie au Service de messagerie** avec :
   - le cookie de session (« JSESSIONID ») récupéré en 2);
   - le jeton d'authentification (assertion SAML 2.0) récupéré en 4) ;

La figure ci-dessous présente la cinématique générale de l'authentification préalable en 5 étapes :

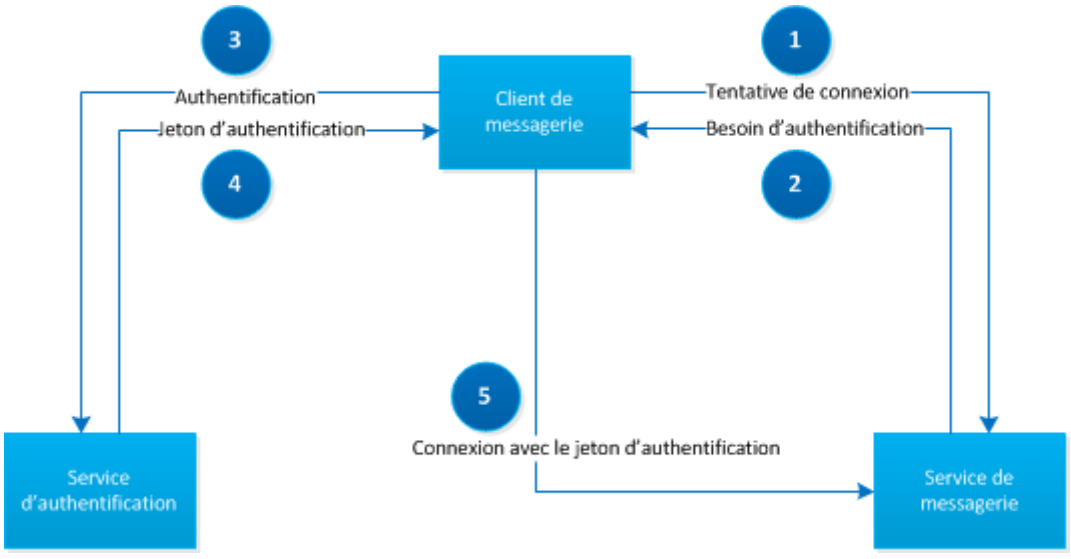

Figure 4 : Cinématique de l'authentification préalable

Ensuite, après l'authentification préalable, le client de messagerie doit alors faire une redirection (dans la même session) vers le service initialement demandé au Service de messagerie en réutilisant le cookie de session (« JSESSIONID ») durant sa période de validité.

Tous opérateurs MSSanté
Les opérateurs MSSanté compatibles avec le présent DST (dont l'opérateur Mailiz), accepte deux moyens d'authentification (et d'obtention du jeton d'authentification) auprès de leur *Service d'authentification* : - Authentification par carte CPS, - Authentification par identifiant/mot de passe/OTP.

Par ailleurs, le format du jeton d'authentification est standardisé, ainsi le service d'authentification d'un client de messagerie s'appuie sur le profil SAML 2.0 ECP pour accéder à un service de messagerie.

Remarque : Les opérateurs MSSanté, exposant des interfaces de Web Services de messagerie non conformes au DST doivent fournir un service d'authentification basé sur des moyens d'authentification qui garantissent la sécurité et la confidentialité des accès aux données contenues dans le système MSSanté.

6.1.2 Structure du jeton d'authentification (Assertion SAML V2.0)

La structure de l'élément assertion est normée ; la référence en ligne explicitant le format d'une assertion SAML V2.0 est disponible à l'adresse suivante: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

Une assertion est un élément XML structuré autour d'une balise telle que la suivante :

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="s2cc47aae81dfcd1d00fa1ab573032ed14a27bc28f" IssueInstant="2013-07-12T07:46:17Z" Version="2.0">
```

L'assertion générée par le Service d'authentification et attendue par le Service de messagerie contient principalement les éléments suivants :

- **Issuer** : référence du service d'authentification :
  « <saml:Issuer>http://example.com/openam</saml:Issuer> » ;
- **Signature** : éléments relatifs à la méthode de signature de l'assertion, au certificat du signataire et au résultat de cette signature :
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ;
- **Subject** : identité à laquelle se réfère cette assertion (éléments imbriqués) : <saml:Subject> ;
- **Conditions** : critères de validité de cette assertion (par exemple la plage de date durant laquelle elle est valide) ; éléments imbriqués autour de la balise suivante : <saml:Conditions NotBefore="2013-07-12T07:36:17Z" NotOnOrAfter="2013-07-12T07:56:17Z"> ;
- **Authorisation statement** : éléments imbriqués de type <saml:AuthnStatement> relatifs à l'acte d'authentification ;
- **<saml:AttributeStatement>** : élément contenant les éléments métier : <saml:Attribute> les attributs à renseigner sont :
  - <saml:Attribute Name="nom "> : contient le nom d'exercice du PS ;
  - <saml:Attribute Name="prenom"> : contient le prénom du PS ;
  - <saml:Attribute Name="idNat"> : contient l'identifiant de l'utilisateur (attribut obligatoire pour s'identifier sur le service de messagerie) ;
  - <saml:Attribute Name="typeUtilisateur"> : contient la valeur 'PS' pour professionnel de santé ;
  - <saml:Attribute Name="profession"> : profession du PS.

Remarques :

- Si l'utilisateur est un professionnel de santé, le champ IdNat peut contenir un identifiant RPPS ou ADELI avec le préfixe correspondant au type d'identifiant (respectivement 0 ou 8), tel qu'il est enregistré dans les certificats émis par l'ANS ;
- Les attributs de l'assertion SAML doivent être en mesure d'identifier de façon unique l'utilisateur pour l'utilisation des Web Services de messagerie ;
- Le champ « profession » doit être alimenté.

6.1.3 Contrôles d'accès aux serveurs MSSanté

Un « filtre de contrôle d'accès » est appliqué lors de chaque appel de Web Service. Il vérifie :

6.1.3.1 La version du service appelée :

Dans l'url (par exemple :https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/listFolders), si la version installée sur le serveur n'est pas la bonne, une erreur http 404 est retournée.

6.1.3.2 La présence et la validité d'un jeton d'authentification :

Ce filtre vérifie la présence et la validité du jeton d'authentification fourni dans la requête pour continuer l'appel du service.

Un jeton d'authentification peut être « une Assertion SAML » ou « un Cookie de Session » (taille max 4k). Si le jeton d'authentification n'est pas fourni, alors l'utilisateur est renvoyé sur les services d'authentification.

6.1.3.3 L'identifiant :

Pour les éditeurs de clients de messagerie implémentant les interfaces décrites dans le DST Clients de messagerie, il leur est demandé de renseigner (en production et en test) le champ 'NUMHOMOLOGATION' présent dans l'entête http avec à minima :

- le nom de l'éditeur de logiciel,
- le nom du logiciel (maximum de 50 caractères).

Afin de faciliter les investigations ce champ doit être communiqué à l'opérateur MSSanté lors de demandes de support.

6.1.4 TM4.1.1C - Authentification par carte CPS

6.1.4.1 Cinématique d'une authentification par carte CPS

Ce diagramme de séquence présente l'enchainement entre les Web Services de messagerie et les Web Services d'authentification :

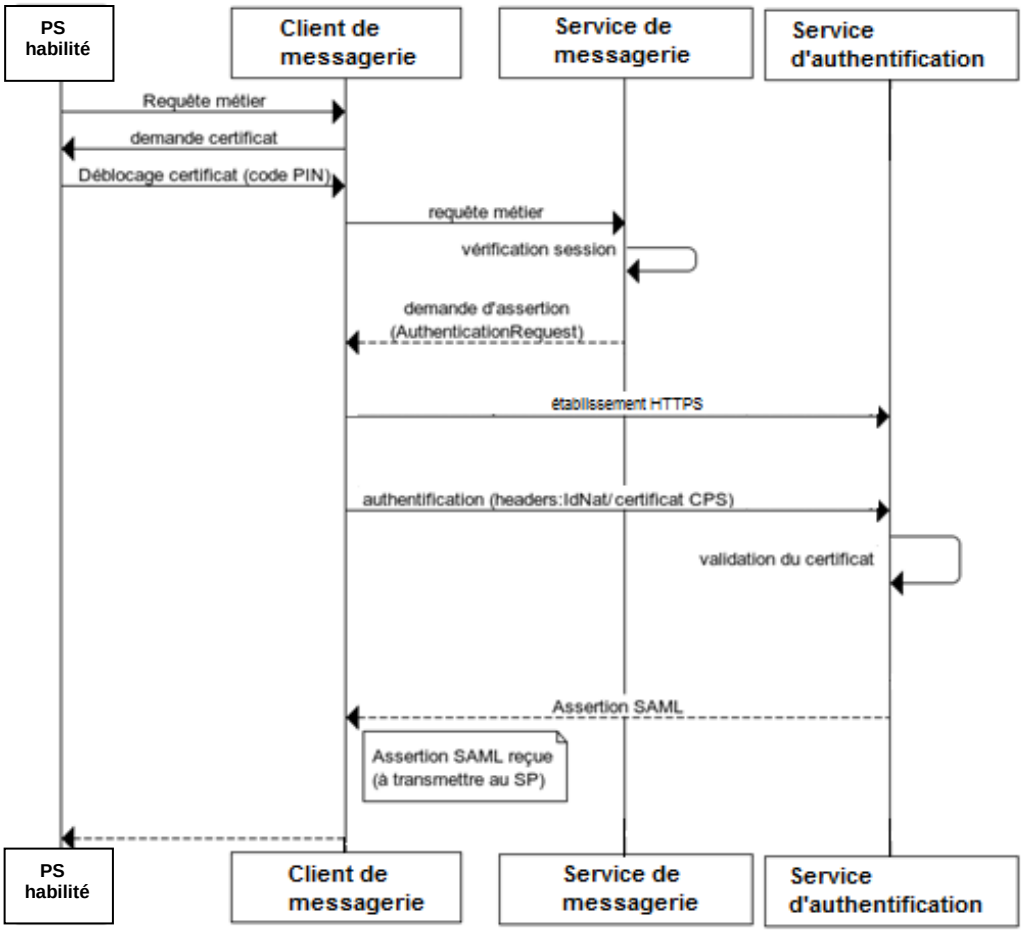

Figure 5 : Cinématique d'authentification par carte CPS

6.1.4.2 Description détaillée d'une authentification par carte CPS

Les 5 étapes décrites ci-après correspondent aux étapes 1 à 5 listées au §6.1.1.

6.1.4.2.1 Etape 1 : Tentative de connexion au service de messagerie

Le client de messagerie tente d'accéder au service de messagerie.

Cette étape nécessite une communication standardisée avec le service de messagerie, avec un en-tête http contenant les paramètres suivants :

```
PAOS:ver='urn:liberty:paos:2003-08'; 'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'
Accept:text/xml, application/vnd.paos+xml
Content-Type:text/xml; charset=utf-8
```

Cet en-tête indique un support de l'authentification SAML en reverse SOAP.

6.1.4.2.2 Etape 2 : Besoin d'une authentification préalable s'il n'existe pas de session active

En réponse à la requête de l'**étape 1**, le service de messagerie envoie au client de messagerie soit :

- **Un code retour HTTP 302** en « redirect » (ce qui signifie que l'utilisateur est déjà authentifié et que la session est toujours active) et l'**url de redirection** (le service de messagerie appelé).

```
HTTP/1.1 302 Moved Temporarily
Date:Thu, 08 Jan 2015 13:21:43 GMT
Content-Length:0
Location:https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1
Content-Type:text/plain; charset=UTF-8
Connection:close
Server:Apache-Coyote/1.1
```

- **Un code retour HTTP 200** et un élément XML de type « **AuthnRequest** », ce qui signifie que l'utilisateur n'est pas authentifié ou que la session est expirée, et qu'il est nécessaire de faire une authentification préalable.

```
HTTP/1.1 200 OK
Cache-control:no-cache, no-store
Date:Thu, 08 Jan 2015 13:22:26 GMT
Content-Length:3644
SOAPAction:http://www.oasis-open.org/committees/security
Set-Cookie:
JSESSIONID=CCC1F35BFA5B308F497D62332617C5F1; [Cookie de session à passer en étape 5]
Path=/mss-msg-services-igcsante; Secure
Connection:close
Content-Type:text/xml;charset=UTF-8
Server:Apache-Coyote/1.1
Pragma:no-cache
<?xml version="1.0" encoding="UTF-8"?>

<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">

<soap11:Header>

<paos:Request
xmlns:paos="urn:liberty:paos:2003-08"
responseConsumerURL="https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias"
service="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
soap11:actor="http://schemas.xmlsoap.org/soap/actor/next" soap11:mustUnderstand="1"/>

<ecp:Request
xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
IsPassive="false"
soap11:actor="http://schemas.xmlsoap.org/soap/actor/next"
soap11:mustUnderstand="1">
<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">mss-msg-services-igcsante</saml2:Issuer>
<saml2p:IDPList xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"><saml2p:IDPEntry ProviderID="https://mss-idp-
igcsante.mssante.fr/openam"/></saml2p:IDPList>
</ecp:Request>

</soap11:Header>

<soap11:Body>

<saml2p:AuthnRequest
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://mss-msg-igcsante.mssante.fr/mss-msg-services-
igcsante/saml/SSO/alias/defaultAlias"
ForceAuthn="false"
ID="a1g097a5ehja6ace47g372670hf542i"
IsPassive="false"
```

```
IssueInstant="2015-01-08T13:22:26.542Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Version="2.0">

<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">mss-msg-services-igcsante</saml2:Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#a1g097a5ehja6ace47g372670hf542i">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Mri1FmRsM4WBYq8iTa06fzZ3LGM=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>RYTDA31U5cBUC01DKgF5xd7mJZVk/HgJCmYZsoaf0A41PDgOo1MheiowCkvj1dzvup3KNkoVCSHkm4VpP
WZzHitWKJ92gzDlgGnSZ9NIAYXUkMB7EW+HdhHg4cC5x6uXfNn2Bw1XN5rnIXNVjadK4h1wrTevSxJi5htfFaLa/s8=</ds:Signat
ureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>
MIIDMDCCApmgAwIBAgIQMDAwMTIwNDIwNj7VHWaLxzANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQG
EwJGUjEVMBMGA1UEChMMR0lQLUNQUy1URVNUMRkwFwYDVQQLExBBQy1DTEFTU0UtNC1URVNUMB4X
DTE0MDkyOTE0MTAwNVoXDTE3MDkyOTE0MTAwNVowcjELMAkGA1UEBhMCRlIxDTALBgNVBAoTBFRF
U1QxEzARBgNVBAcUClBhcmlzICg3NSkxGDAWBgNVBAsTDzMxODc1MTI3NTEwMDAyMDElMCMGA1UE
AxMcbXNzLW1zZy5mb3JtYXRpb24ubXNzYW50ZS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAsJ5mrwVGfiyhQo6dsqfTDh+VJLSoKszeK7PNfp3ffdkKVYCdtKWM1SWi+Do/XDbGr1pzxcch
Y/mvFVY6w/eFfLMF5iwgD9t4NUOeGCizdBFosvLmAq3f2767ij44mDfaCzxAvZjvL48tX+4NCLuu
R3s1tJy83yOQ4K7iP+6y6lkCAwEAAaOB+TCB9jArBgNVHRAEJDAigA8yMDE0MDkyOTE0MTAwNVqB
DzIwMTcwOTI5MTQxMDA1WjAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwQwEQYJ
YIZIAYb4QgEBBAQDAgUgMCcGA1UdEQQgMB6BHG1zcy1tc2dAZm9ybWF0aW9uLm1zc2FudGUuZnIw
FQYDVR0gBA4wDDAKBggqgXoBRwMHBDAPBggqgXoBRwECBQQDBAGCMB0GA1UdDgQWBBTBUaaIE67f
avpGsIB8UGq7gUrxqzAfBgNVHSMEGDAWgBTCVu/vIPJZF7xAbFmzzPibk7toGjANBgkqhkiG9w0B
AQUFAAOBgQCZncjQ1RLfyYajAStMw0svN9wHhs4MTVloNL2nsFQuEBSM6SmMmALVQnD9fDV586B+
sMSiLD3aMGa8Ri0+6hIGrcYgyXiZaCxs/zHO2uVPZWyeiqw0tcFGKTv+GVypVFDNrzQhS9WQws/w
1YpgOHTfeZXJaBHc036ivN1R9SCPFg==
</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
</ds:Signature>

<saml2p:Scoping ProxyCount="2">
<saml2p:IDPList>
<saml2p:IDPEntry ProviderID="https://mss-idp-igcsante.mssante.fr/openam"/>
</saml2p:IDPList>
</saml2p:Scoping>
</saml2p:AuthnRequest>

</soap11:Body>
</soap11:Envelope>
```

L'élément « **AuthnRequest** », standardisé par SAML 2.0, doit être transmis au service d'authentification en **étape 3**.

Le cookie de session « **JSESSIONID** » contenu dans l'en-tête http de la réponse doit être transmis au service d'authentification en **étape 5**.

L'URL « **AssertionConsumerServiceURL** » contenu dans l'élément « AuthnRequest » est utilisée pour la requête vers le service de messagerie en **étape 5**.

6.1.4.2.3 Etape 3 : Authentification sur le service d'authentification

Le mécanisme d'authentification avec la CPS est le suivant :

1) [Client de messagerie] Connexion en HTTPS du client de messagerie, avec le certificat d'authentification de la carte CPS de l'utilisateur, sur le service d'authentification de l'opérateur MSSanté ;
2) [Service d'authentification] Le service d'authentification vérifie la validité du certificat client présenté (non expiré, non révoqué) ;
3) [Client de messagerie] Le client de messagerie vérifie la validité du certificat du serveur (non expiré, non révoqué) ;
4) [Client de messagerie] Une fois la connexion HTTPS validée, le client de messagerie envoie par Web Service une demande de jeton d'authentification au service d'authentification ;

Le nom de domaine du service d'authentification n'est pas fourni dans la réponse du service de messagerie en **étape 2**. Le client de messagerie doit en disposer dans sa configuration.

Cas de l'opérateur Mailiz
Pour l'opérateur Mailiz, le point d'accès du service d'authentification **par CPS** de l'opérateur Mailiz est https://mss-idp-igcsante.mssante.fr/openam/SSOSoap/metaAlias/asip/idp (la liste des url des services MSSanté de l'opérateur Mailiz est donnée en annexe au § 8.1).

Description de la requête de demande de jeton d'authentification :

Tous opérateurs MSSanté
Authentification par carte CPS:
CPSIDNAT:[identifiant national du PS extrait du certificat d'authentification de la carte CPS (exemple :*899700017942)]* Content-Type:text/xml Accept:application/vnd.paos+xml PAOS:ver='urn:liberty:paos:2003-08';'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'

La requête doit reprendre l'enveloppe SOAP de la réponse récupérée en **étape 2** :

- Mais le contenu de l'en-tête SOAP doit être vidé (balises <soap11:Header>)
- Et l'AuthnRequest repris

```
<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">

<soap11:Header></soap11:Header>   [l'entête soap est vide]

<soap11:Body>   [fournir l'AuthnRequest récupéré en étape 2]

<saml2p:AuthnRequest
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://mss-msg-igcsante.mssante.fr/mss-msg-services-
igcsante/saml/SSO/alias/defaultAlias"
ForceAuthn="false"
ID="a1g097a5ehja6ace47g372670hf542i"
IsPassive="false"
IssueInstant="2015-01-08T13:22:26.542Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Version="2.0">

<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">mss-msg-services-igcsante</saml2:Issuer>
```

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#a1g097a5ehja6ace47g372670hf542i">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Mri1FmRsM4WBYq8iTa06fzZ3LGM=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>RYTDA31U5cBUC01DKgF5xd7mJZVk/HgJCmYZsoaf0A41PDgOo1MheiowCkvj1dzvup3KNkoVCSHkm4VpP
WZzHitWKJ92gzDlgGnSZ9NIAYXUkMB7EW+HdhHg4cC5x6uXfNn2Bw1XN5rnIXNVjadK4h1wrTevSxJi5htfFaLa/s8=</ds:Signat
ureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>
MIIDMDCCApmgAwIBAgIQMDAwMTIwNDIwNj7VHWaLxzANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQG
EwJGUjEVMBMGA1UEChMMR0lQLUNQUy1URVNUMRkwFwYDVQQLExBBQy1DTEFTU0UtNC1URVNUMB4X
DTE0MDkyOTE0MTAwNVoXDTE3MDkyOTE0MTAwNVowcjELMAkGA1UEBhMCRlIxDTALBgNVBAoTBFRF
U1QxEzARBgNVBAcUClBhcmlzICg3NSkxGDAWBgNVBAsTDzMxODc1MTI3NTEwMDAyMDElMCMGA1UE
AxMcbXNzLW1zZy5mb3JtYXRpb24ubXNzYW50ZS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAsJ5mrwVGfiyhQo6dsqfTDh+VJLSoKszeK7PNfp3ffdkKVYCdtKWM1SWi+Do/XDbGr1pzxcch
Y/mvFVY6w/eFfLMF5iwgD9t4NUOeGCizdBFosvLmAq3f2767ij44mDfaCzxAvZjvL48tX+4NCLuu
R3s1tJy83yOQ4K7iP+6y6lkCAwEAAaOB+TCB9jArBgNVHRAEJDAigA8yMDE0MDkyOTE0MTAwNVqB
DzIwMTcwOTI5MTQxMDA1WjAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwQwEQYJ
YIZIAYb4QgEBBAQDAgUgMCcGA1UdEQQgMB6BHG1zcy1tc2dAZm9ybWF0aW9uLm1zc2FudGUuZnIw
FQYDVR0gBA4wDDAKBggqgXoBRwMHBDAPBggqgXoBRwECBQQDBAGCMB0GA1UdDgQWBBTBUaalE67f
avpGslB8UGq7gUrxqzAfBgNVHSMEGDAWgBTCVu/vIPJZF7xAbFmzzPibk7toGjANBgkqhkiG9w0B
AQUFAAOBgQCZncjQ1RLfyYajAStMw0svN9wHhs4MTVloNL2nsFQuEBSM6SmMmALVQnD9fDV586B+
sMSiLD3aMGa8Ri0+6hIGrcYgyXiZaCxs/zHO2uVPZWyeiqw0tcFGKTv+GVypVFDNrzQhS9WQws/w
1YpgOHTfeZXJaBHc036ivN1R9SCPFg==
</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
</ds:Signature>

<saml2p:Scoping ProxyCount="2">
<saml2p:IDPList>
<saml2p:IDPEntry ProviderID="https://mss-idp-igcsante.mssante.fr/openam"/>
</saml2p:IDPList>
</saml2p:Scoping>

</saml2p:AuthnRequest>
</soap11:Body>
</soap11:Envelope>

6.1.4.2.4 Etape 4 : Obtention du jeton d'authentification

Le service d'authentification réceptionne la requête décrite en **étape 3** et détecte la présence du header spécifique **CPSIDNAT**. La présence de ce header entraine la vérification de l'autorisation de l'utilisateur (utilisateur au statut actif) sur la base de l'identité contenue dans le certificat de la carte CPS.

Le service d'authentification renvoie au client de messagerie soit :

- un rejet de l'authentification avec
  - un code HTTP 200
  - un message HTML « authentication failed » ;
- une acceptation de l'authentification avec
  - un code HTTP 200
  - une enveloppe SOAP contenant un **jeton d'authentification** (<saml:Assertion>).

```
<soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
<soap-env:Header>
<ecp:Response xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp" xmlns:soap-
env="http://schemas.xmlsoap.org/soap/envelope/" soap-env:mustUnderstand="true" soap-
env:actor="http://schemas.xmlsoap.org/soap/actor/next" AssertionConsumerServiceURL="https://mss-msg-
igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias"></ecp:Response>
</soap-env:Header>
<soap-env:Body>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="s216ac10c4ff55e2d39c0b8249e578eda7e9ba54ca" InResponseTo="a39fc4345120j7ea1ibigf2253hef61" Version="2.0"
IssueInstant="2015-01-08T13:21:38Z" Destination="https://mss-msg-igcsante.mssante.fr/mss-msg-services-
igcsante/saml/SSO/alias/defaultAlias">
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://mss-idp-
igcsante.mssante.fr/openam</saml:Issuer>
<samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<samlp:StatusCode  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Value="urn:oasis:names:tc:SAML:2.0:status:Success">
</samlp:StatusCode>
</samlp:Status>
<saml:Assertion
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="s246daeaa66f92c91428cfef4e331342b291e54f17"
IssueInstant="2015-01-08T13:21:38Z" Version="2.0">
<saml:Issuer>https://mss-idp-igcsante.mssante.fr/openam</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#s246daeaa66f92c91428cfef4e331342b291e54f17">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Gx+I4j9YU2LO1NKZD8lvGxI0JsA=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
Yu+Fhh4O2CaiGkRH115umBkrzAYNnrxB3GHBEH2g83cjaU/G8Y5AM34Z5Gfcqfies4SRNYPul1By
O+D/ZogiZ/5xtq0lEFqQiOsIQBX44tNNF2CybZck5EMpf3p+VF8Ion/q6A15k/YJ7KNPe7UT2hyD
C1aZuhiv5yynPkiySaY=
</ds:SignatureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>
MIIDMDCCApmgAwIBAgIQMDAwMTIwNDIwNj7VHWarwTANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQG
EwJGUjEVMBMGA1UEChMMR0lQLUNQUy1URVNUMRkwFwYDVQQLExBBQy1DTEFTU0UtNC1URVNUMB4X
DTE0MDkyOTE0MTExNVoXDTE3MDkyOTE0MTExNVowcjELMAkGA1UEBhMCRlIxDTALBgNVBAoTBFRF
U1QxEzARBgNVBAcUClBhcmlzICg3NSkxGDAWBgNVBAsTDzMxODc1MTI3NTEwMDAyMDElMCMGA1UE
AxMcbXNzLWlkcC5mb3JtYXRpb24ubXNzYW50ZS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAyKTp2N2PTSiM9OsdE9F4U0JX+NT7J1NWLaVwa0YQRvC25di0vcxetJnlcNJ4rKbp2XPp2qEB
```

P6fMo3rgJIg4+ikJdcOHub/dbHd3WEQ04lE54Ep48Rz1ZEAp1UHy3KkEddnJJeiEY7aBRewVvl+j
hh28FtMCmUoKPw1qFpS870MCAwEAAaOB+TCB9jArBgNVHRAEJDAigA8yMDE0MDkyOTE0MTExNVqB
DzIwMTcwOTI5MTQxMTE1WjAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwQwEQYJ
YIZIAYb4QgEBBAQDAgUgMCcGA1UdEQQgMB6BHG1zcy1pZHBAZm9ybWF0aW9uLm1zc2FudGUuZnIw
FQYDVR0gBA4wDDAKBggqgXoBRwMHBDAPBggqgXoBRwECBQQDBAGCMB0GA1UdDgQWBBSKWIVx3DMK
X/VOcWrfUBbUWFSoSjAfBgNVHSMEGDAWgBTCVu/vIPJZF7xAbFmzzPibk7toGjANBgkqhkiG9w0B
AQUFAAOBgQCNPyJM/tUyfhilhe7a7TeOsD34i6hSP+6tWzomasnnEYWqxsvp0YG1hrO5Q7JdNiws
EXxjW9u6b1u1tQ0XSyxhEqMHBYJXJulCDttejKshQ14WOZObEz5H66OUwV3LggouQt4mC7A9r+sI
Rm6wjElu74OCnuGw/LVERe2ihU/h3Q==
</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" NameQualifier="https://mss-idp-igcsante.mssante.fr/openam">899700017942</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData InResponseTo="a39fc4345120j7ea1ibigf2253hef61" NotOnOrAfter="2015-01-08T13:31:38Z" Recipient="https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias"/>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2015-01-08T13:11:38Z" NotOnOrAfter="2015-01-08T13:31:38Z">
<saml:AudienceRestriction>
<saml:Audience>mss-msg-services-igcsante</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2015-01-08T13:21:38Z" SessionIndex="s2271f0ba691ba8ec3e018e8ec4e8239dc912d9201">
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute Name="prenom">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GERALDINE</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="idNat">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">899700017942</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="profession">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Chirurgien-Dentiste</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="typeUtilisateur">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">PS</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="nom">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">DENTISTE RPPS-ADELI</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
</soap-env:Body>
</soap-env:Envelope>

6.1.4.2.5 Etape 5 : Connexion au service de messagerie avec le jeton d'authentification

Description de la requête :

Elle doit être transmise à l'url de validation de l'assertion « AssertionConsumerServiceURL » récupérée à l'**étape 1**.

Tous opérateurs MSSanté
Cookie:JSESSIONID=9084968B90D9779C378204778F66FB5F [récupéré en étape 2] Content-Type:application/vnd.paos+xml Accept:application/vnd.paos+xml PAOS:ver='urn:liberty:paos:2003-08';'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'

Cette requête doit reprendre l'enveloppe SOAP de la réponse (principe de reverse SOAP) récupérée en **étape 4** :

- Mais le contenu de l'en-tête SOAP doit être vidé (balises <soap11:Header>)
- Et le corps (avec l'assertion SAML) repris

```
<soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">

<soap-env:Header></soap-env:Header>   [l'entête soap est vide]

<soap-env:Body>   [fournir l'assertion SAML  récupérée en étape 4]

<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="s216ac10c4ff55e2d39c0b8249e578eda7e9ba54ca" InResponseTo="a39fc4345120j7ea1ibigf2253hef61" Version="2.0"
IssueInstant="2015-01-08T13:21:38Z" Destination="https://mss-msg-igcsante.mssante.fr/mss-msg-services-
igcsante/saml/SSO/alias/defaultAlias">
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://mss-idp-
igcsante.formation.mssante.fr:443/openam</saml:Issuer>
<samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<samlp:StatusCode  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Value="urn:oasis:names:tc:SAML:2.0:status:Success">
</samlp:StatusCode></samlp:Status>

<saml:Assertion
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="s246daeaa66f92c91428cfef4e331342b291e54f17"
IssueInstant="2015-01-08T13:21:38Z" Version="2.0">
<saml:Issuer>https://mss-idp-igcsante.mssante.fr/openam</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#s246daeaa66f92c91428cfef4e331342b291e54f17">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Gx+I4j9YU2LO1NKZD8lvGxI0JsA=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
Yu+Fhh4O2CaiGkRH115umBkrzAYNnrxB3GHBEH2g83cjaU/G8Y5AM34Z5Gfcqfies4SRNYPul1By
O+D/ZogiZ/5xtq0lEFqQiOsIQBX44tNNF2CybZck5EMpf3p+VF8Ion/q6A15k/YJ7KNPe7UT2hyD
C1aZuhiv5yynPkiySaY=
</ds:SignatureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>
MIIDMDCCApmgAwIBAgIQMDAwMTIwNDIwNj7VHWarwTANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQG
EwJGUjEVMBMGA1UEChMMR0lQLUNQUy1URVNUMRkwFwYDVQQLExBBQy1DTEFTU0UtNC1URVNUMB4X
DTE0MDkyOTE0MTExNVoXDTE3MDkyOTE0MTExNVowcjELMAkGA1UEBhMCRllxDTALBgNVBAoTBFRF
U1QxEzARBgNVBAcUClBhcmlzICg3NSkxGDAWBgNVBAsTDzMxODc1MTI3NTEwMDAyMDElMCMGA1UE
```

AxMcbXNzLWlkcC5mb3JtYXRpb24ubXNzYW50ZS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAyKTp2N2PTSiM9OsdE9F4U0JX+NT7J1NWLaVwa0YQRvC25di0vcxetJnlcNJ4rKbp2XPp2qEB
P6fMo3rgJIg4+ikJdcOHub/dbHd3WEQ04lE54Ep48Rz1ZEAp1UHy3KkEddnJJeiEY7aBRewVvl+j
hh28FtMCmUoKPw1qFpS870MCAwEAAaOB+TCB9jArBgNVHRAEJDAigA8yMDE0MDkyOTE0MTExNVqB
DzIwMTcwOTI5MTQxMTE1WjAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwQwEQYJ
YIZIAYb4QgEBBAQDAgUgMCcGA1UdEQQgMB6BHG1zcy1pZHBAZm9ybWF0aW9uLm1zc2FudGUuZnIw
FQYDVR0gBA4wDDAKBggqgXoBRwMHBDAPBggqgXoBRwECBQQDBAGCMB0GA1UdDgQWBBSKWIVx3DMK
X/VOcWrfUBbUWFSoSjAfBgNVHSMEGDAWgBTCVu/vIPJZF7xAbFmzzPibk7toGjANBgkqhkiG9w0B
AQUFAAOBgQCNPyJM/tUyfhilhe7a7TeOsD34i6hSP+6tWzomasnnEYWqxsvp0YG1hrO5Q7JdNiws
EXxjW9u6b1u1tQ0XSyxhEqMHBYJXJulCDttejKshQ14WOZObEz5H66OUwV3LggouQt4mC7A9r+sI
Rm6wjElu74OCnuGw/LVERe2ihU/h3Q==
</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" NameQualifier="https://mss-idp-igcsante.formation.mssante.fr:443/openam">899700017942</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData InResponseTo="a39fc4345120j7ea1ibigf2253hef61" NotOnOrAfter="2015-01-08T13:31:38Z" Recipient="https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias"/>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2015-01-08T13:11:38Z" NotOnOrAfter="2015-01-08T13:31:38Z">
<saml:AudienceRestriction><saml:Audience>mss-msg-services-igcsante</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2015-01-08T13:21:38Z"
SessionIndex="s2271f0ba691ba8ec3e018e8ec4e8239dc912d9201">
<saml:AuthnContext><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef></saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute Name="prenom">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GERALDINE</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="idNat">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">899700017942</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="profession">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Chirurgien-Dentiste</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="typeUtilisateur">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">PS</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="nom">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">DENTISTE RPPS-ADELI</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>

</samlp:Response>
</soap-env:Body>
</soap-env:Envelope>

Attention : L'assertion SAML doit être transmise sans modification. La moindre altération invalide le message. La vérification de l'assertion SAML renvoie une erreur si des caractères de fin de ligne, des espaces ou des tabulations sont rajoutés lors de la génération du XML en chaine de caractères.

Description de la réponse :

En réponse à cette validation, on obtient soit :

- **Un code retour HTTP 302** « redirect » (ce qui signifie que le jeton d'authentification a été validé) et l'**url de redirection** (le service de messagerie initialement appelé).

```
HTTP/1.1 302 Moved Temporarily
Date:Thu, 08 Jan 2015 13:21:43 GMT
Content-Length:0
Location:https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1
Content-Type:text/plain; charset=UTF-8
Connection:close
Server:Apache-Coyote/1.1
```

Le client doit alors faire une redirection (dans la même session) pour consommation du service initialement demandé.

Remarque développement C# : Pour avoir une authentification qui fonctionne, penser à désactiver le flag autorisant la redirection automatique (mettre AllowRedirect à false sur la dernière requête en C#.net)

- **Un code retour HTTP 200** et un élément XML de type « **AuthnRequest** », ce qui signifie que l'utilisateur n'est pas authentifié ou que la session est expirée, et qu'il est nécessaire de faire une authentification préalable *(Voir § 6.1.4.2.2)*

6.1.5 TM4.1.2C - Authentification par identifiant / mot de passe / OTP

6.1.5.1 Cinématique d'une authentification par identifiant / mot de passe / OTP

Ce diagramme de séquence présente l'enchainement entre les Web Services de messagerie et les Web Services d'authentification :

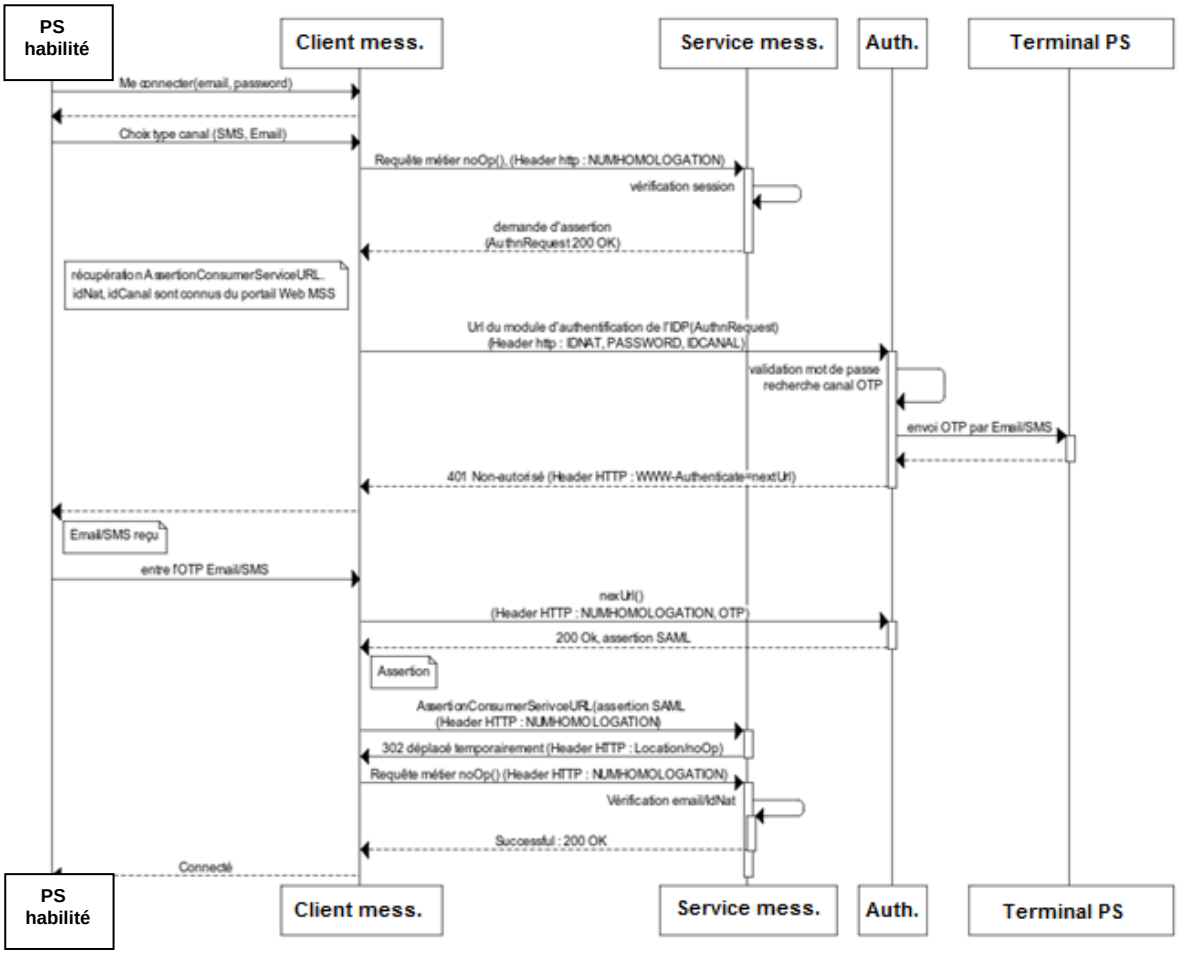

Figure 6 : Cinématique d'authentification par identifiant/mot de passe/OTP

6.1.5.2 Description détaillée d'une authentification par identifiant / mot de passe / OTP

Les 5 étapes décrites ci-après correspondent aux étapes 1 à 5 listées au §6.1.1.

6.1.5.2.1 Etape 1 : Tentative de connexion au service de messagerie

Le client de messagerie tente d'accéder au service de messagerie.

Cette étape nécessite une communication standardisée avec le service de messagerie, avec un en-tête http contenant les paramètres suivants :

```
PAOS:ver='urn:liberty:paos:2003-08'; 'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'
Accept:text/xml, application/vnd.paos+xml
Content-Type:text/xml; charset=utf-8
```

Cet en-tête indique un support de l'authentification SAML en reverse SOAP.

6.1.5.2.2 Etape 2 : Besoin d'une authentification préalable s'il n'existe pas de session active

En réponse à la requête de l'**étape 1**, le service de messagerie envoie au client de messagerie soit :

- **Un code retour HTTP 302** en « redirect » (ce qui signifie que l'utilisateur est déjà authentifié et que la session est toujours active) et l'**url de redirection** (le service de messagerie appelé).

```
HTTP/1.1 302 Moved Temporarily
Date:Thu, 08 Jan 2015 13:21:43 GMT
Content-Length:0
Location:https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1
Content-Type:text/plain; charset=UTF-8
Connection:close
Server:Apache-Coyote/1.1
```

- **Un code retour HTTP 200** et un élément XML de type « **AuthnRequest** », ce qui signifie que l'utilisateur n'est pas authentifié ou que la session est expirée, et qu'il est nécessaire de faire une authentification préalable.

```
HTTP/1.1 200 OK
Cache-control:no-cache, no-store
Date:Thu, 08 Jan 2015 13:22:26 GMT
Content-Length:3644
SOAPAction:http://www.oasis-open.org/committees/security
Set-Cookie:
JSESSIONID=CCC1F35BFA5B308F497D62332617C5F1; [Cookie de session à passer en étape 5]
Path=/mss-msg-services-igcsante; Secure
Connection:close
Content-Type:text/xml;charset=UTF-8
Server:Apache-Coyote/1.1
Pragma:no-cache
<?xml version="1.0" encoding="UTF-8"?>

<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">

<soap11:Header>

<paos:Request
xmlns:paos="urn:liberty:paos:2003-08"
responseConsumerURL="https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias"
service="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
soap11:actor="http://schemas.xmlsoap.org/soap/actor/next" soap11:mustUnderstand="1"/>

<ecp:Request
xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
IsPassive="false"
soap11:actor="http://schemas.xmlsoap.org/soap/actor/next"
soap11:mustUnderstand="1">
<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">mss-msg-services-igcsante</saml2:Issuer>
<saml2p:IDPList xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"><saml2p:IDPEntry ProviderID="https://mss-idp-
igcsante.mssante.fr/openam"/></saml2p:IDPList>
</ecp:Request>

</soap11:Header>

<soap11:Body>

<saml2p:AuthnRequest
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" AssertionConsumerServiceURL="https://mss-msg-
igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias"
ForceAuthn="false"
ID="a1g097a5ehja6ace47g372670hf542i"
IsPassive="false"
IssueInstant="2015-01-08T13:22:26.542Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Version="2.0">
```

```
<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">mss-msg-services-igcsante</saml2:Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#a1g097a5ehja6ace47g372670hf542i">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Mri1FmRsM4WBYq8iTa06fzZ3LGM=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>RYTDA31U5cBUC01DKgF5xd7mJZVk/HgJCmYZsoaf0A41PDgOo1MheiowCkvj1dzvup3KNkoVCSHkm4VpP
WZzHitWKJ92gzDlgGnSZ9NIAYXUkMB7EW+HdhHg4cC5x6uXfNn2Bw1XN5rnIXNVjadK4h1wrTevSxJi5htfFaLa/s8=</ds:Signat
ureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>
MIIDMDCCApmgAwIBAgIQMDAwMTIwNDIwNj7VHWaLxzANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQG
EwJGUjEVMBMGA1UEChMMR0lQLUNQUy1URVNUMRkwFwYDVQQLExBBQy1DTEFTU0UtNC1URVNUMB4X
DTE0MDkyOTE0MTAwNVoXDTE3MDkyOTE0MTAwNVowcjELMAkGA1UEBhMCRlIxDTALBgNVBAoTBFRF
U1QxEzARBgNVBAcUClBhcmlzICg3NSkxGDAWBgNVBAsTDzMxODc1MTI3NTEwMDAyMDElMCMGA1UE
AxMcbXNzLW1zZy5mb3JtYXRpb24ubXNzYW50ZS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAsJ5mrwVGfiyhQo6dsqfTDh+VJLSoKszeK7PNfp3ffdkKVYCdtKWM1SWi+Do/XDbGr1pzxcch
Y/mvFVY6w/eFfLMF5iwgD9t4NUOeGCizdBFosvLmAq3f2767ij44mDfaCzxAvZjvL48tX+4NCLuu
R3s1tJy83yOQ4K7iP+6y6lkCAwEAAaOB+TCB9jArBgNVHRAEJDAigA8yMDE0MDkyOTE0MTAwNVqB
DzIwMTcwOTI5MTQxMDA1WjAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwQwEQYJ
YIZIAYb4QgEBBAQDAgUgMCcGA1UdEQQgMB6BHG1zcy1tc2dAZm9ybWF0aW9uLm1zc2FudGUuZnIw
FQYDVR0gBA4wDDAKBggqgXoBRwMHBDAPBggqgXoBRwECBQQDBAGCMB0GA1UdDgQWBBTBUaalE67f
avpGsIB8UGq7gUrxqzAfBgNVHSMEGDAWgBTCVu/vIPJZF7xAbFmzzPibk7toGjANBgkqhkiG9w0B
AQUFAAOBgQCZncjQ1RLfyYajAStMw0svN9wHhs4MTVloNL2nsFQuEBSM6SmMmALVQnD9fDV586B+
sMSiLD3aMGa8Ri0+6hIGrcYgyXiZaCxs/zHO2uVPZWyeiqw0tcFGKTv+GVypVFDNrzQhS9WQws/w
1YpgOHTfeZXJaBHc036ivN1R9SCPFg==
</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
</ds:Signature>

<saml2p:Scoping ProxyCount="2">
<saml2p:IDPList>
<saml2p:IDPEntry ProviderID="https://mss-idp-igcsante.mssante.fr/openam"/>
</saml2p:IDPList>
</saml2p:Scoping>

</saml2p:AuthnRequest>

</soap11:Body>
</soap11:Envelope>
```

- L'élément « **AuthnRequest** », standardisé par SAML 2.0, doit être transmis au service d'authentification en **étape 3**.
- Le cookie de session « **JSESSIONID** » contenu dans l'en-tête http de la réponse doit être transmis au service d'authentification en **étape 5**.
- L'URL « **AssertionConsumerServiceURL** » contenu dans l'élément « AuthnRequest » est utilisée pour la requête vers le service de messagerie en **étape 5**.

6.1.5.2.3 Etape 3 : Authentification sur le service d'authentification

Le mécanisme d'authentification par identifiant/mot de passe/OTP est le suivant :

1) [Client de messagerie] Connexion en HTTPS du client de messagerie sur le service d'authentification de l'opérateur MSSanté ;
2) [Client de messagerie] Le client de messagerie vérifie la validité du certificat du service d'authentification (non expiré, non révoqué) ;
3) [Client de messagerie] Une fois la connexion HTTPS validée, le client de messagerie envoie par Web Service au service d'authentification une demande d'OTP avec l'identifiant, le mot de passe et le type de canal OTP choisis par l'utilisateur (**voir étape 3.3 ci-après**) ;
4) [Service d'authentification] Le service d'authentification vérifie la validité de la demande d'OTP. Si la demande d'OTP est valide, le service d'authentification envoie l'OTP par le canal OTP sélectionné et une réponse avec l'url vers laquelle renvoyer l'OTP par Web Service au client de messagerie (**voir étape 3.4 ci-après**) ;
5) [Utilisateur] L'utilisateur réceptionne l'OTP via le canal sélectionné et saisit cet OTP dans son client de messagerie (**non décrit dans ce document**) ;
6) [Client de messagerie] Le client de messagerie envoie par Web Service au service d'authentification une demande de jeton d'authentification avec l'OTP et le jeton initial (**voir étape 3.6 ci-après**) ;

Le nom de domaine du service d'authentification n'est pas fourni dans la réponse du service de messagerie en **étape 2**. Le client de messagerie doit donc en disposer dans sa configuration.

Cas de l'opérateur Mailiz
Le point d'accès du service d'authentification par identifiant / mot de passe / OTP de l'opérateur Mailiz est https://mss-idp-igcsante.mssante.fr/openam/SSOSoap/metaAlias/asip/idp (la liste des url des services MSSanté de l'opérateur Mailiz est donnée en annexe au § 8.1).

Etape 3.3 : Demande d'OTP avec l'identifiant, le mot de passe et le type de canal OTP choisi par l'utilisateur

Tous opérateurs MSSanté
IDNAT:899700017942 [valeur de l'identifiant national du PS] PASSWORD:Password01 [mot de passe du PS] TYPECANAL:SMS ["SMS" ou "Mail" : canal sélectionné par le PS] NUMHOMOLOGATION:xxxx;yyy [nom de l'éditeur de logiciel;nom du logiciel, voir paragraphe 6.1.3.3] Content-Type:text/xml Accept:application/vnd.paos+xml PAOS:ver='urn:liberty:paos:2003-08';'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'

Remarque : La solution d'utiliser le paramètre IDCANAL (identifiant unique associé à chaque canal OTP par le serveur d'authentification lors de la saisie par l'utilisateur de ses canaux OTP sur le portail MSSanté) en lieu et place du paramètre TYPECANAL est toujours possible mais est plus complexe à mettre en œuvre. En effet, l'utilisateur doit préalablement renseigner sur son client de messagerie le ou les IDCANAL de son téléphone et/ou de son mail, après les avoir récupérés sur le portail https://www.mssante.fr (page « Gestion de mon compte »).

La requête doit reprendre l'enveloppe SOAP de la réponse récupérée en **étape 2** :

- Mais le contenu de l'en-tête SOAP doit être vidé (balises <soap11:Header>)
- Et l'AuthnRequest repris

```
<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">

<soap11:Header></soap11:Header>  [l'en-tête soap est vide]

<soap11:Body>

<saml2p:AuthnRequest    [fournir l'AuthnRequest récupéré en étape 2]
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" AssertionConsumerServiceURL="https://mss-msg-
igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias"
ForceAuthn="false"
ID="a1g097a5ehja6ace47g372670hf542i"
IsPassive="false"
IssueInstant="2015-01-08T13:22:26.542Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Version="2.0">

<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">mss-msg-services-igcsante</saml2:Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#a1g097a5ehja6ace47g372670hf542i">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Mri1FmRsM4WBYq8iTa06fzZ3LGM=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>RYTDA31U5cBUC01DKgF5xd7mJZVk/HgJCmYZsoaf0A41PDgOo1MheiowCkvj1dzvup3KNkoVCSHkm4VpP
WZzHitWKJ92gzDlgGnSZ9NIAYXUkMB7EW+HdhHg4cC5x6uXfNn2Bw1XN5rnIXNVjadK4h1wrTevSxJi5htfFaLa/s8=</ds:Signat
ureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>
MIIDMDCCApmgAwIBAgIQMDAwMTIwNDIwNj7VHWaLxzANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQG
EwJGUjEVMBMGA1UEChMMR0lQLUNQUy1URVNUMRkwFwYDVQQLExBBQy1DTEFTU0UtNC1URVNUMB4X
DTE0MDkyOTE0MTAwNVoXDTE3MDkyOTE0MTAwNVowcjELMAkGA1UEBhMCRlIxDTALBgNVBAoTBFRF
U1QxEzARBgNVBAcUClBhcmlzICg3NSkxGDAWBgNVBAsTDzMxODc1MTI3NTEwMDAyMDElMCMGA1UE
```

```
AxMcbXNzLW1zZy5mb3JtYXRpb24ubXNzYW50ZS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAsJ5mrwVGfiyhQo6dsqfTDh+VJLSoKszeK7PNfp3ffdkKVYCdtKWM1SWi+Do/XDbGr1pzxcch
Y/mvFVY6w/eFfLMF5iwgD9t4NUOeGCizdBFosvLmAq3f2767ij44mDfaCzxAvZjvL48tX+4NCLuu
R3s1tJy83yOQ4K7iP+6y6lkCAwEAAaOB+TCB9jArBgNVHRAEJDAigA8yMDE0MDkyOTE0MTAwNVqB
DzIwMTcwOTI5MTQxMDA1WjAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwQwEQYJ
YIZIAYb4QgEBBAQDAgUgMCcGA1UdEQQgMB6BHG1zcy1tc2dAZm9ybWF0aW9uLm1zc2FudGUuZnIw
FQYDVR0gBA4wDDAKBggqgXoBRwMHBDAPBggqgXoBRwECBQQDBAGCMB0GA1UdDgQWBBTBUaalE67f
avpGsIB8UGq7gUrxqzAfBgNVHSMEGDAWgBTCVu/vIPJZF7xAbFmzzPibk7toGjANBgkqhkiG9w0B
AQUFAAOBgQCZncjQ1RLfyYajAStMw0svN9wHhs4MTVloNL2nsFQuEBSM6SmMmALVQnD9fDV586B+
sMSiLD3aMGa8Ri0+6hIGrcYgyXiZaCxs/zHO2uVPZWyeiqw0tcFGKTv+GVypVFDNrzQhS9WQws/w
1YpgOHTfeZXJaBHc036ivN1R9SCPFg==
</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
</ds:Signature>

<saml2p:Scoping ProxyCount="2">
<saml2p:IDPList>
<saml2p:IDPEntry ProviderID="https://mss-idp-igcsante.mssante.fr/openam"/>
</saml2p:IDPList>
</saml2p:Scoping>

</saml2p:AuthnRequest>
</soap11:Body>
</soap11:Envelope>
```

Etape 3.4 : Réponse du service d'authentification avec l'url vers laquelle renvoyer l'OTP

Le service d'authentification vérifie la validité de la demande d'OTP.

Si la demande est validée, le service d'authentification renvoie :

- l'OTP à l'utilisateur par le canal OTP (SMS ou MAIL) sélectionné et
- Une réponse avec :
    - Un code retour HTTP 401 ;
    - les cookies « AMAuthCookie » et « amlbcookie » servant à la continuité de la requête et à la gestion de l'équilibre de charge du service d'authentification ;
    - l'URL vers laquelle renvoyer l'OTP (« OTP nextUrl »).

```
HTTP/1.1 401 Non-Autorisé
Cache-Control: private
Pragma: no-cache
Expires: 0
X-DSAMEVersion: OpenAM 10.1.0-Xpress (2013-February-07 15:45)
AM_CLIENT_TYPE: genericHTML
Set-Cookie:
AMAuthCookie=AQIC5wM2LY4SfcyQn5K2wvViX1K61npjcQ3OIy6ZufCPPRE.*AAJTSQACMDEAAlNLABQtMzIyOTg3MDg1MjUwMjE3MzU5NQ..*; Domain=.ovh.net; Path=/
Set-Cookie:
amlbcookie=01; Domain=.ovh.net; Path=/
OTP nextUrl=
/openam/UI/Login?forward=true&realm=%2Fasip&goto=%2FSSOSoap%2FmetaAlias%2Fasip%2Fidp%3FReqID%3Da3c88b0h1j8jg15f16e6a141he2ffi5&spEntityID=mss-msg-services-igcsante
Content-Type: text/html
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 393
Connection: close
Response Error from request URL : <NSMutableURLRequest
https://ns202477.ovh.net/openam/SSOSoap/metaAlias/asip/idp>
```

Si la demande n'est pas validée, le service d'authentification renvoie :

- Une erreur d'authentification (HTTP 200 et un message HTML « authentication failed ») ;

Etape 3.6 : Demande de jeton d'authentification avec l'OTP

Cette requête vise à transmettre l'OTP reçu au service d'authentification et à demander le jeton d'authentification.
Elle doit être envoyée par le client de messagerie au service d'authentification, à l'adresse « OTP nextURL » récupérée dans la réponse de l'**étape 3.4**.

Tous opérateurs MSSanté
Cookie: AMAuthCookie=AQIC5wM2LY4Sfcyo3fSWJtpVXIUbvVl4IiWKBn5GEXodiyg.*AAJTSQACMDEAAlNLABQtNTk1NDY4NzAxOTAwNjI4MDc4Nw..* amlbcookie=01 OTP:89470311 Content-Type:text/xml Accept:application/vnd.paos+xml PAOS:ver='urn:liberty:paos:2003-08';'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'

Cette requête doit reprendre l'enveloppe SOAP de la réponse (principe de reverse SOAP) récupérée en **étape 2** :

- Mais le contenu de len-tête SOAP doit être vidé (balises <soap11:Header>)
- Et le corps (avec l'AuthnRequest) repris

```
<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">

<soap11:Header></soap11:Header>  [l'en-tête soap est vide]

<soap11:Body>
<saml2p:AuthnRequest    [fournir l'AuthnRequest récupéré en étape 2]
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" AssertionConsumerServiceURL="https://mss-msg-
igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias"
ForceAuthn="false"
ID="a1g097a5ehja6ace47g372670hf542i"
IsPassive="false"
IssueInstant="2015-01-08T13:22:26.542Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Version="2.0">

<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">mss-msg-services-igcsante</saml2:Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#a1g097a5ehja6ace47g372670hf542i">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Mri1FmRsM4WBYq8iTa06fzZ3LGM=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>RYTDA31U5cBUC01DKgF5xd7mJZVk/HgJCmYZsoaf0A41PDgOo1MheiowCkvj1dzvup3KNkoVCSHkm4VpP
WZzHitWKJ92gzDlgGnSZ9NIAYXUkMB7EW+HdhHg4cC5x6uXfNn2Bw1XN5rnIXNVjadK4h1wrTevSxJi5htfFaLa/s8=</ds:Signat
ureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>
MIIDMDCCApmgAwIBAgIQMDAwMTIwNDIwNj7VHWaLxzANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQG
EwJGUjEVMBMGA1UEChMMR0lQLUNQUy1URVNUMRkwFwYDVQQLExBBQy1DTEFTU0UtNC1URVNUMB4X
DTE0MDkyOTE0MTAwNVoXDTE3MDkyOTE0MTAwNVowcjELMAkGA1UEBhMCRlIxDTALBgNVBAoTBFRF
U1QxEzARBgNVBAcUClBhcmlzICg3NSkxGDAWBgNVBAsTDzMxODc1MTI3NTEwMDAyMDElMCMGA1UE
AxMcbXNzLW1zZy5mb3JtYXRpb24ubXNzYW50ZS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
```

```
gYEAsJ5mrwVGfiyhQo6dsqfTDh+VJLSoKszeK7PNfp3ffdkKVYCdtKWM1SWi+Do/XDbGr1pzxcch
Y/mvFVY6w/eFfLMF5iwgD9t4NUOeGCizdBFosvLmAq3f2767ij44mDfaCzxAvZjvL48tX+4NCLuu
R3s1tJy83yOQ4K7iP+6y6lkCAwEAAaOB+TCB9jArBgNVHRAEJDAigA8yMDE0MDkyOTE0MTAwNVqB
DzIwMTcwOTI5MTQxMDA1WjAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwQwEQYJ
YIZIAYb4QgEBBAQDAgUgMCcGA1UdEQQgMB6BHG1zcy1tc2dAZm9ybWF0aW9uLm1zc2FudGUuZnIw
FQYDVR0gBA4wDDAKBggqgXoBRwMHBDAPBggqgXoBRwECBQQDBAGCMB0GA1UdDgQWBBTBUaalE67f
avpGsIB8UGq7gUrxqzAfBgNVHSMEGDAWgBTCVu/vIPJZF7xAbFmzzPibk7toGjANBgkqhkiG9w0B
AQUFAAOBgQCZncjQ1RLfyYajAStMw0svN9wHhs4MTVloNL2nsFQuEBSM6SmMmALVQnD9fDV586B+
sMSiLD3aMGa8Ri0+6hIGrcYgyXiZaCxs/zHO2uVPZWyeiqw0tcFGKTv+GVypVFDNrzQhS9WQws/w
1YpgOHTfeZXJaBHc036ivN1R9SCPFg==
</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
</ds:Signature>

<saml2p:Scoping ProxyCount="2">
<saml2p:IDPList>
<saml2p:IDPEntry ProviderID="https://mss-idp-igcsante.mssante.fr/openam"/>
</saml2p:IDPList>
</saml2p:Scoping>

</saml2p:AuthnRequest>
</soap11:Body>
</soap11:Envelope>
```

6.1.5.2.4 Etape 4 : Obtention du jeton d'authentification

Le service d'authentification réceptionne la requête décrite en **étape 3.6** et vérifie la validité de l'OTP.

Le service d'authentification renvoie au client de messagerie soit :

- un rejet de l'authentification avec
  - un code HTTP 200
  - un message HTML « authentication failed » ;
- une acceptation de l'authentification avec
  - un code HTTP 200
  - une enveloppe SOAP contenant un **jeton d'authentification** (<saml:Assertion>).

```
HTTP/1.1 200 OK
X-AuthErrorCode:0
Content-Length:5721
Expires:0
Set-Cookie:AMAuthCookie=LOGOUT; Domain=.mssante.fr; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
iPlanetDirectoryPro=AQIC5wM2LY4Sfcyo3fSWJtpVXIUbvVl4IiWKBn5GEXodiyg.*AAJTSQACMDEAAlNLABQtNTk1NDY4NzAxO
TAwNjI4MDc4Nw..*; Domain=.mssante.fr; Path=/
Connection:close
Server:Apache-Coyote/1.1
Pragma:no-cache
Cache-Control:private
X-DSAMEVersion:OpenAM 10.1.0-Xpress (2013-February-07 15:45)
Date:Thu, 08 Jan 2015 13:22:44 GMT
Vary:Accept-Encoding
AM_CLIENT_TYPE:genericHTML
Via:1.1 mss-idp-igcsante.formation.mssante.fr:443
Content-Type:text/xml;charset=utf-8

<soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
<soap-env:Header>
<ecp:Response xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp" xmlns:soap-
env="http://schemas.xmlsoap.org/soap/envelope/" soap-env:mustUnderstand="true" soap-
env:actor="http://schemas.xmlsoap.org/soap/actor/next" AssertionConsumerServiceURL="https://mss-msg-
igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias">
</ecp:Response>
```

```
</soap-env:Header>

<soap-env:Body>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="s2309eea2bf50cb84be95756c45f22303a278785e3" InResponseTo="a1g097a5ehja6ace47g372670hf542i"
Version="2.0"
IssueInstant="2015-01-08T13:22:44Z"
Destination="https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias">
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://mss-idp-
igcsante.mssante.fr/openam</saml:Issuer>
<samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<samlp:StatusCode  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Value="urn:oasis:names:tc:SAML:2.0:status:Success">
</samlp:StatusCode>
</samlp:Status>
<saml:Assertion
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="s242f819b322daed335ea5065edb7bccdae0046e63"
IssueInstant="2015-01-08T13:22:44Z" Version="2.0">
<saml:Issuer>https://mss-idp-igcsante.mssante.fr/openam</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#s242f819b322daed335ea5065edb7bccdae0046e63">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>IT9GR5DXM5krXgZ5no8ttf8UIyY=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
itKhY7fxXZbbh9MouOvkwnI++KgHlxYFFDCJ6t9FMX3vaXWXcG3HD6Fe9KynAwoi+xlglldQWa/w
pkAeuFsiCAMXgWjm4nZcjc+I90i66NmWjGLh2MmIHd5wWYDKZRMcwCjVsUh2tsnswZWE3evHo5bR
rbwoczk++TYuIfznHPk=
</ds:SignatureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>
MIIDMDCCApmgAwIBAgIQMDAwMTIwNDIwNj7VHWarwTANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQG
EwJGUjEVMBMGA1UEChMMR0lQLUNQUy1URVNUMRkwFwYDVQQLExBBQy1DTEFTU0UtNC1URVNUMB4X
DTE0MDkyOTE0MTExNVoXDTE3MDkyOTE0MTExNVowcjELMAkGA1UEBhMCRlIxDTALBgNVBAoTBFRF
U1QxEzARBgNVBAcUClBhcmlzICg3NSkxGDAWBgNVBAsTDzMxODc1MTI3NTEwMDAyMDElMCMGA1UE
AxMcbXNzLWlkcC5mb3JtYXRpb24ubXNzYW50ZS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAyKTp2N2PTSiM9OsdE9F4U0JX+NT7J1NWLaVwa0YQRvC25di0vcxetJnlcNJ4rKbp2XPp2qEB
P6fMo3rgJIg4+ikJdcOHub/dbHd3WEQ04lE54Ep48Rz1ZEAp1UHy3KkEddnJJeiEY7aBRewVvl+j
hh28FtMCmUoKPw1qFpS870MCAwEAAaOB+TCB9jArBgNVHRAEJDAigA8yMDE0MDkyOTE0MTExNVqB
DzIwMTcwOTI5MTQxMTE1WjAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwQwEQYJ
YIZIAYb4QgEBBAQDAgUgMCcGA1UdEQQgMB6BHG1zcy1pZHBAZm9ybWF0aW9uLm1zc2FudGUuZnIw
FQYDVR0gBA4wDDAKBggqgXoBRwMHBDAPBggqgXoBRwECBQQDBAGCMB0GA1UdDgQWBBSKWIVx3DMK
X/VOcWrfUBbUWFSoSjAfBgNVHSMEGDAWgBTCVu/vIPJZF7xAbFmzzPibk7toGjANBgkqhkiG9w0B
AQUFAAOBgQCNPyJM/tUyfhilhe7a7TeOsD34i6hSP+6tWzomasnnEYWqxsvp0YG1hrO5Q7JdNiws
EXxjW9u6b1u1tQ0XSyxhEqMHBYJXJulCDttejKshQ14WOZObEz5H66OUwV3LggouQt4mC7A9r+sI
Rm6wjElu74OCnuGw/LVERe2ihU/h3Q==
</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" NameQualifier="https://mss-idp-
igcsante.formation.mssante.fr:443/openam">899700017942</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData
InResponseTo="a1g097a5ehja6ace47g372670hf542i"
NotOnOrAfter="2015-01-08T13:32:44Z"
Recipient="https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/saml/SSO/alias/defaultAlias"/>
</saml:SubjectConfirmation>
</saml:Subject>
```

```
<saml:Conditions
NotBefore="2015-01-08T13:12:44Z"
NotOnOrAfter="2015-01-08T13:32:44Z">
<saml:AudienceRestriction>
<saml:Audience>mss-msg-services-igcsante</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement
AuthnInstant="2015-01-08T13:22:44Z"
SessionIndex="s229024c2c760682ce3dfe52c3c0bb6ef8497f3c01">
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextCla
ssRef>
</saml:AuthnContext>
</saml:AuthnStatement>

<saml:AttributeStatement>

<saml:Attribute Name="prenom"><saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">GERALDINE</saml:AttributeValue></saml:Attribute>
<saml:Attribute Name="idNat">

<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:type="xs:string">899700017942</saml:AttributeValue></saml:Attribute>

<saml:Attribute Name="profession"><saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Chirurgien-
Dentiste</saml:AttributeValue></saml:Attribute>

<saml:Attribute Name="typeUtilisateur"><saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">PS</saml:AttributeValue></saml:Attribute>

<saml:Attribute Name="nom"><saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">DENTISTE RPPS-
ADELI</saml:AttributeValue></saml:Attribute>

</saml:AttributeStatement>
</saml:Assertion>

</samlp:Response>
</soap-env:Body>
</soap-env:Envelope>
```

6.1.5.2.5 Etape 5 : Connexion au service de messagerie avec le jeton d'authentification

Description de la requête :

Elle doit être transmise à l'URL de validation de l'assertion « AssertionConsumerServiceURL » récupérée à l'**étape 1**.

Tous opérateurs MSSanté
Cookie:JSESSIONID=CCC1F35BFA5B308F497D62332617C5F1 [récupéré en étape 1] Content-Type:application/vnd.paos+xml Accept:application/vnd.paos+xml PAOS:ver='urn:liberty:paos:2003-08';'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'

Cette requête doit reprendre l'enveloppe SOAP de la réponse (principe de reverse SOAP) récupérée en **étape 4** :

- Mais le contenu de l'en-tête SOAP doit être vidé (balises <soap11:Header>)
- Et le corps (avec l'assertion SAML) repris

```
<soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">

<soap-env:Header></soap-env:Header>  [l'en-tête soap est vide]

<soap-env:Body>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="s2309eea2bf50cb84be95756c45f22303a278785e3" InResponseTo="a1g097a5ehja6ace47g372670hf542i"
Version="2.0" IssueInstant="2015-01-08T13:22:44Z" Destination="https://mss-msg-igcsante.mssante.fr/mss-msg-services-
igcsante/saml/SSO/alias/defaultAlias">
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://mss-idp-
igcsante.mssante.fr/openam</saml:Issuer>
<samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<samlp:StatusCode  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode>
</samlp:Status>

<saml:Assertion   [Assertion saml récupérée en étape 4]
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="s242f819b322daed335ea5065edb7bccdae0046e63"
IssueInstant="2015-01-08T13:22:44Z" Version="2.0">
<saml:Issuer>https://mss-idp-igcsante.mssante.fr/openam</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#s242f819b322daed335ea5065edb7bccdae0046e63">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>IT9GR5DXM5krXgZ5no8ttf8UIyY=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
itKhY7fxXZbbh9MouOvkwnI++KgHlxYFFDCJ6t9FMX3vaXWXcG3HD6Fe9KynAwoi+xlglldQWa/w
pkAeuFsiCAMXgWjm4nZcjc+I90i66NmWjGLh2MmIHd5wWYDKZRMcwCjVsUh2tsnswZWE3evHo5bR
rbwoczk++TYuIfznHPk=
</ds:SignatureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>
MIIDMDCCApmgAwIBAgIQMDAwMTIwNDIwNj7VHWarwTANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQG
EwJGUjEVMBMGA1UEChMMR0lQLUNQUy1URVNUMRkwFwYDVQQLExBBQy1DTEFTU0UtNC1URVNUMB4X
DTE0MDkyOTE0MTExNVoXDTE3MDkyOTE0MTExNVowcjELMAkGA1UEBhMCRllxDTALBgNVBAoTBFRF
U1QxEzARBgNVBAcUClBhcmlzICg3NSkxGDAWBgNVBAsTDzMxODc1MTI3NTEwMDAyMDElMCMGA1UE
AxMcbXNzLWlkcC5mb3JtYXRpb24ubXNzYW50ZS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAyKTp2N2PTSiM9OsdE9F4U0JX+NT7J1NWLaVwa0YQRvC25di0vcxetJnlcNJ4rKbp2XPp2qEB
P6fMo3rgJIg4+ikJdcOHub/dbHd3WEQ04lE54Ep48Rz1ZEAp1UHy3KkEddnJJeiEY7aBRewVvl+j
hh28FtMCmUoKPw1qFpS870MCAwEAAaOB+TCB9jArBgNVHRAEJDAigA8yMDE0MDkyOTE0MTExNVqB
```

```
DzIwMTcwOTI5MTQxMTE1WjAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwQwEQYJ
YIZIAYb4QgEBBAQDAgUgMCcGA1UdEQQgMB6BHG1zcy1pZHBAZm9ybWF0aW9uLm1zc2FudGUuZnIw
FQYDVR0gBA4wDDAKBggqgXoBRwMHBDAPBggqgXoBRwECBQQDBAGCMB0GA1UdDgQWBBSKWIVx3DMK
X/VOcWrfUBbUWFSoSjAfBgNVHSMEGDAWgBTCVu/vIPJZF7xAbFmzzPibk7toGjANBgkqhkiG9w0B
AQUFAAOBgQCNPyJM/tUyfhilhe7a7TeOsD34i6hSP+6tWzomasnnEYWqxsvp0YG1hrO5Q7JdNiws
EXxjW9u6b1u1tQ0XSyxhEqMHBYJXJulCDttejKshQ14WOZObEz5H66OUwV3LggouQt4mC7A9r+sI
Rm6wjElu74OCnuGw/LVERe2ihU/h3Q==
</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
</ds:Signature>

<saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" NameQualifier="https://mss-idp-
igcsante.formation.mssante.fr:443/openam">899700017942</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData InResponseTo="a1g097a5ehja6ace47g372670hf542i" NotOnOrAfter="2015-01-
08T13:32:44Z" Recipient="https://mss-msg-igcsante.mssante.fr/mss-msg-services-
igcsante/saml/SSO/alias/defaultAlias"/></saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions
NotBefore="2015-01-08T13:12:44Z"
NotOnOrAfter="2015-01-08T13:32:44Z">
<saml:AudienceRestriction>
<saml:Audience>mss-msg-services-igcsante</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>

<saml:AuthnStatement AuthnInstant="2015-01-08T13:22:44Z"
SessionIndex="s229024c2c760682ce3dfe52c3c0bb6ef8497f3c01">
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextCla
ssRef>
</saml:AuthnContext>
</saml:AuthnStatement>

<saml:AttributeStatement>
<saml:Attribute Name="prenom"><saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">GERALDINE</saml:AttributeValue></saml:Attribute><saml:Attribute
Name="idNat"><saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">899700017942</saml:AttributeValue></saml:Attribute>

<saml:Attribute Name="profession"><saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Chirurgien-
Dentiste</saml:AttributeValue></saml:Attribute>

<saml:Attribute Name="typeUtilisateur"><saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">PS</saml:AttributeValue></saml:Attribute>

<saml:Attribute Name="nom"><saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">DENTISTE RPPS-
ADELI</saml:AttributeValue></saml:Attribute>

</saml:AttributeStatement>
</saml:Assertion>

</samlp:Response>
</soap-env:Body>
</soap-env:Envelope>
```

Attention : L'assertion SAML doit être transmise sans modification. La moindre altération invalide le message. La vérification de l'assertion SAML renvoie une erreur si des caractères de fin de ligne, des espaces ou des tabulations sont rajoutés lors de la génération du XML en chaine de caractères.

Description de la réponse :

En réponse à cette validation, on obtient soit :

- **Un code retour HTTP 302** « redirect » (ce qui signifie que le jeton d'authentification a été validé) et l'**url de redirection** (le service de messagerie initialement appelé).

```
HTTP/1.1 302 Moved Temporarily
Date:Thu, 08 Jan 2015 13:21:43 GMT
Content-Length:0
Location:https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1
Content-Type:text/plain; charset=UTF-8
Connection:close
Server:Apache-Coyote/1.1
```

Le client doit alors faire une redirection (dans la même session) pour consommation du service initialement demandé.

- **Un code retour HTTP 200** et un élément XML de type « **AuthnRequest** », ce qui signifie que l'utilisateur n'est pas authentifié ou que la session est expirée, et qu'il est nécessaire de faire une authentification préalable *(voir § 6.1.5.2.2)*

6.2 TM4.2.xC - Services de consultation et gestion des dossiers

Les 7 transactions de Web Services décrites ci-dessous permettent de consulter et gérer des dossiers de messagerie.

Web Service	Description	Commande IMAP/SMTP équivalente
listFolders	Récupérer la liste détaillée de tous les dossiers existants, ou une liste détaillée des sous-dossiers d'un dossier spécifique.	LIST (IMAP) STATUS (IMAP)
createFolder	Créer un nouveau dossier pour y ranger des messages.	CREATE (IMAP)
deleteFolder	Supprimer un dossier, ainsi que tous les messages et tous les sous-dossiers dans ce dossier. Cette suppression est définitive (ce n'est pas une suppression dans la corbeille comme la méthode Trash).	DELETE (IMAP)
emptyFolder	Vider tous les messages et tous les sous-dossiers d'un dossier spécifique.	LSUB (IMAP) LIST (IMAP) DELETE (IMAP) STORE (IMAP) EXPUNGE ou CLOSE (IMAP)
trashFolder	Déplacer un dossier et ses sous-dossiers vers la corbeille, marquant tous les contenus comme lus et le renommer si un dossier portant ce nom est déjà existant dans la corbeille.	LIST (IMAP) DELETE (IMAP) STORE flag \Deleted (IMAP) EXPUNGE ou CLOSE (IMAP)
renameFolder	Changer le nom d'un dossier existant.	RENAME (IMAP)
moveFolder	Déplacer un dossier.	MOVE (IMAP)

Tableau 2 : Liste des Web Services de consultation et gestion des dossiers

La WSDL associée à ce service est : FolderService.wsdl (voir DR1 au § 8.6).

Des codes exemples sont fournis en annexe § 8.7.

6.2.1 TM4.2.1C - Service listFolders

6.2.1.1 Description

Le service « listFolders » permet de récupérer la liste détaillée de tous les dossiers existants, ou une liste détaillée des sous-dossiers d'un dossier spécifique.

6.2.1.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
folderId	INT	0..1	ID du dossier. Si folderId n'est pas fourni, retourne tous les dossiers. Si folderId est fourni, retourne tous les sous-dossiers de ce dossier.

Tableau 3

6.2.1.3 Flux sortants

Elément	Type	Card.	Description
folders	**Folder**	0…1	Liste détaillée de tous les dossiers existants (si folderId n'était pas renseigné), ou liste détaillée des sous-dossiers d'un dossier spécifique

Tableau 4

Type : Folder			
Elément	**Type**	**Card.**	**Description**
folderId	INT	1	ID du dossier
folderName	STRING	1	Nom du dossier
folderNbUnread	INT	1	Nombre de messages non lus
Folders	**Folder**	0..*	Liste des sous-dossiers. Le service renvoie une liste de dossiers contenant chacun l'Id du dossier parent (sauf pour le dossier Root). Les informations sont agrégées pour fournir une liste de sous-dossiers contenant Id et Name ; ces sous-dossiers peuvent eux-mêmes contenir une liste de sous-dossiers.

Tableau 5

6.2.1.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prend la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
~~**403**~~ **500**	**41**	Le dossier n'existe pas	Le dossier en entrée du service est inexistant
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 6

6.2.1.5 Exposition SOAP

Opération « listFolders » (cf. WSDL SOAP du composant folder : folder.wsdl).

*https://server/mss-msg-services-igcsante/services/**Folder**/soap/vX/**listFolders***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.2.2 TM4.2.2C - Service createFolder

6.2.2.1 Description

Le service « createFolder » permet de créer un nouveau dossier de messagerie pour y ranger des messages.

6.2.2.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
folderName	STRING Taille max dépend du serveur de messagerie	1	Nom du dossier à créer
folderParentId	INT	1	ID du dossier parent

Tableau 7

6.2.2.3 Flux sortants

Elément	Type	Card.	Description
folder	**FolderValidate**	1	

Tableau 8

Type : FolderValidate			
Elément	**Type**	**Card.**	**Description**
folderId	INT	1	ID du dossier
folderName	STRING	1	Nom de dossier

Tableau 9

6.2.2.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné
403	**30**	Un dossier de même niveau existe déjà avec le même nom	Dans le dossier en cours, un sous-dossier a déjà le même nom.
403	**31**	Le nom du dossier est incorrect	Le nom du dossier a un format invalide : trop long
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**41**	Le dossier parent n'existe pas	Le dossier en entrée du service est inexistant
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 10

6.2.2.5 Exposition SOAP

Opération « createFolder » (cf. : WSDL SOAP du composant folder : folder.wsdl).

*https://server/mss-msg-services-igcsante/services/**Folder**/soap/vX/**createFolder***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.2.3 TM4.2.3C - Service deleteFolder

6.2.3.1 Description

Le service « deleteFolder » permet de supprimer un dossier, ainsi que tous les messages et tous les sous-dossiers dans ce dossier. Cette suppression est définitive (ce n'est pas une suppression dans la corbeille comme la méthode Trash).

6.2.3.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
folderId	INT	0..1	ID du dossier à supprimer. Si l'identifiant du dossier n'existe pas ou si l'identifiant ne correspond à aucun dossier, alors retour vide (http 200).

Tableau 11

6.2.3.3 Flux sortants

Le service ne retourne rien si l'opération est effectuée.

6.2.3.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 12

6.2.3.5 Exposition SOAP

Opération « deleteFolder » (cf. : WSDL SOAP du composant folder : folder.wsdl).

*https://server/mss-msg-services-igcsante/services/**Folder**/soap/v**X**/**deleteFolder***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.2.4 TM4.2.4C - Service emptyFolder

6.2.4.1 Description

Le service « emptyFolder » permet de supprimer définitivement tous les messages et tous les sous-dossiers d'un dossier spécifique (cela ne supprime pas le dossier que l'on vide).

6.2.4.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
folderId	INT	0..1	ID du dossier à vider. Si la cardinalité est 0 (le champ n'est pas fourni) la transaction ne fait rien et retourne un code http 200.

Tableau 13

6.2.4.3 Flux sortants

Le service ne retourne rien si l'opération est effectuée.

6.2.4.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné
403	**41**	Le dossier n'existe pas	Le dossier en entrée du service est inexistant
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 14

6.2.4.5 Exposition SOAP

Opération « emptyFolder » (cf. : WSDL SOAP du composant folder : folder.wsdl).

*https://server/mss-msg-services-igcsante/services/**Folder**/soap/v**X**/**emptyFolder***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.2.5 TM4.2.5C - Service trashFolder

6.2.5.1 Description

Le service « trashFolder » permet de déplacer un dossier et ses sous-dossiers vers la corbeille, marquant tous les contenus comme lus, en le renommant si un dossier portant le même nom est déjà présent dans la corbeille.

6.2.5.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
folderId	INT	0..1	ID du dossier à mettre à la corbeille. Si la cardinalité est 0 (le champ n'est pas fourni) la transaction ne fait rien et retourne un code http 200.

Tableau 15

6.2.5.3 Flux sortants

Le service ne retourne rien si l'opération est effectuée.

6.2.5.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné
403	**41**	Le dossier n'existe pas	Le dossier en entrée du service est inexistant
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 16

6.2.5.5 Exposition SOAP

Opération « trashFolder » (cf. : WSDL SOAP du composant folder : folder.wsdl).

*https://server/mss-msg-services-igcsante/services/**Folder**/soap/vX/**trashFolder***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.2.6 TM4.2.6C - Service renameFolder

6.2.6.1 Description

Le service « renameFolder » permet de changer le nom d'un dossier existant.

6.2.6.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
folderId	INT	0..1	ID du dossier existant. Si la cardinalité est 0 (le champ n'est pas fourni) la transaction ne fait rien et retourne un code http 200.
newFolderName	STRING Taille max dépend du serveur de messagerie	1	Nouveau nom du dossier.

Tableau 17

6.2.6.3 Flux sortants

Le service ne retourne rien si l'opération est effectuée.

6.2.6.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné
403	**30**	Un dossier de même niveau existe déjà avec le même nom	Dans le dossier en cours, un sous-dossier a déjà le même nom.
403	**31**	Le nom du dossier est incorrect	Le nom du dossier est incorrect
403	**41**	Le dossier n'existe pas	Le dossier en entrée du service est inexistant
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 18

6.2.6.5 Exposition SOAP

Opération « renameFolder » (cf. : WSDL SOAP du composant folder : folder.wsdl).

*https://server/mss-msg-services-igcsante/services/**Folder**/soap/vX/**renameFolder***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.2.7 TM4.2.7C - Service moveFolder

6.2.7.1 Description

Le service « moveFolder » permet de déplacer un dossier et ses sous-dossiers vers un autre dossier.

6.2.7.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
folderId	INT	1	ID du dossier existant
destinationFolderId	INT	1	ID du dossier de destination

Tableau 19

6.2.7.3 Flux sortants

Le service ne retourne rien si l'opération est effectuée.

6.2.7.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**30**	Un dossier de même niveau existe déjà avec le même nom	Dans le dossier cible, un sous-dossier a déjà le même nom.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**41**	Le dossier n'existe pas	Le dossier à déplacer ou le dossier de destination indiqué en entrée du service est inexistant.
403	**47**	Déplacement de dossier impossible	Par exemple : si l'on tente de déplacer un dossier dans un de ses sous-dossiers.
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 20

6.2.7.5 Exposition SOAP

Opération « moveFolder » (cf. : WSDL SOAP du composant folder : folder.wsdl).

*https://server/mss-msg-services-igcsante/services/**Folder**/soap/vX/**moveFolder***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.3 TM4.3.xC - Services envoi et gestion de messages

Les 5 transactions de Web Services décrites ci-dessous permettent d'envoyer et de gérer des messages.

Web Service	Description	Commande IMAP/SMTP équivalente
updateMessages	Mettre à jour une liste de messages.	STORE (IMAP)
draftMessage	Enregistrer un message comme un brouillon avec ses pièces jointes.	APPEND (IMAP)
moveMessages	Déplacer une liste de message vers un autre dossier.	COPY (IMAP)
sendMessage	Envoyer un message avec ses pièces jointes.	SMTP Protocol : MAIL FROM, RCPT TO, SIZE, DATA, QUIT …
syncMessages	Obtenir les éléments à synchroniser avec le serveur.	LIST (IMAP)

Tableau 21 : Liste des Web Services d'envoi et de gestion de messages

La WSDL associée à ce service est : ItemService.wsdl (voir DR2 au § 8.6).

6.3.1 TM4.3.1C - Service updateMessages

6.3.1.1 Description

Le service « updateMessages » permet de mettre à jour une liste de messages (la mise à jour est la même pour tous les messages passés en paramètre).

Les différentes mises à jour peuvent être :

- Supprimer ;
- Modifier des flags ;
- Marquer comme lu ou non lu ;
- Marquer comme spam ou non spam ;
- Déplacer vers la corbeille.

6.3.1.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
messageIds	INT	0…*	Liste de messages ID. Si la cardinalité est 0 la transaction ne fait rien et retourne un code http 200
operation	**EnumOperation**	1	Opération à exécuter sur le message

Tableau 22

6.3.1.3 Flux sortants

Le service ne retourne rien si l'opération est effectuée.

6.3.1.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**45**	Le messageId n'existe pas	Le messageId à mettre à jour n'existe pas ou un des identifiants de message des pièces jointes n'existe pas.
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 23

6.3.1.5 Exposition SOAP

Opération « updateMessages » (cf. : WSDL SOAP du composant item : item.wsdl).

*https://server/mss-msg-services-igcsante/services/**Item**/soap/v**X**/**updateMessages***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.3.2 TM4.3.2C - Service draftMessage

6.3.2.1 Description

Le service « draftMessage » permet d'enregistrer un message (y compris ses pièces jointes le cas échéant) comme un brouillon.

6.3.2.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
messages	**messageToSend**	0..1	Liste de messages. Si la cardinalité est 0 (le champ n'est pas fourni) la transaction ne fait rien et retourne un code http 200

Tableau 24

6.3.2.3 Flux sortants

Elément	Type	Card.	Description
message	**MessageValidate**	0..1	Message enregistré.

Tableau 25

6.3.2.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**39**	Le contenu du message est trop volumineux	Si le contenu du message est trop volumineux par rapport à l'acceptation du serveur de messagerie.
403	**45**	Le messageId n'existe pas	Le brouillon à mettre à jour n'existe pas ou un des identifiants de message des pièces jointes n'existe pas.

Tableau 26

6.3.2.5 Exposition SOAP

Opération « draftMessage » (cf. : WSDL SOAP du composant item : item.wsdl).

*https://server/mss-msg-services-igcsante/services/**Item**/soap/v**X**/**draftMessage***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.3.3 TM4.3.3C - Service moveMessages

6.3.3.1 Description

Le service « moveMessages » permet de déplacer une liste de messages vers un autre dossier.

6.3.3.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
messageIds	INT	0…*	Liste des identifiants de messages. Si la cardinalité est 0 (le champ n'est pas fourni) la transaction ne fait rien et retourne un code http 200
destinationFolderId	INT	1	ID du dossier de destination.

Tableau 27

6.3.3.3 Flux sortants

Le service ne retourne rien si l'opération est effectuée.

6.3.3.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**41**	Le dossier n'existe pas	Le dossier en entrée du service est inexistant.
403	**45**	Le messageId n'existe pas	Le messageId à déplacer n'existe pas ou un des identifiants de message des pièces jointes n'existe pas.
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 28

6.3.3.5 Exposition SOAP

Opération « moveMessages » (cf. : WSDL SOAP du composant item : item.wsdl).

*https://server/mss-msg-services-igcsante/services/**Item**/soap/v**X**/**moveMessages***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.3.4 TM4.3.4C - Service sendMessage

6.3.4.1 Description

Le service « sendMessage » permet d'envoyer un message avec ses pièces jointes.

6.3.4.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
message	**messageToSend**	0..1	Liste de messages. Si la cardinalité est 0 (le champ n'est pas fourni) la transaction ne fait rien et retourne un code http 200

Tableau 29

6.3.4.3 Flux sortants

Elément	Type	Card.	Description
message	**MessageValidate**	0..1	Message enregistré.

Tableau 30

6.3.4.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**39**	Le contenu du message est trop volumineux	Le contenu du message est trop volumineux par rapport à l'acceptation du serveur de messagerie.
403	**42**	L'adresse de messagerie est inconnue du serveur de messagerie de l'opérateur MSSanté	L'adresse de messagerie est inconnue.
403	**45**	Le messageId n'existe pas	Le messageId d'une des pièces jointes n'existe pas.
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 31

6.3.4.5 Exposition SOAP

Opération « sendMessage » (cf. : WSDL SOAP du composant item : item.wsdl).

*https://server/mss-msg-services-igcsante/services/**Item**/soap/vX/**sendMessage***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.3.5 TM4.3.5C - Service syncMessages

6.3.5.1 Description

Le service « syncMessages » permet d'obtenir les éléments à synchroniser avec le serveur.

6.3.5.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
folderId	INT	0..1	ID du dossier à synchroniser. S'il n'est pas renseigné, cela synchronise tous les dossiers.
html	BOOLEAN	0..1	Si « true », le body de la réponse contiendra le code html Si « false » (ou non renseigné), le body de la réponse sera du texte brut
token	STRING(60)	0..1	Jeton obtenu lors de la dernière synchronisation. Si ce jeton est vide, cela retourne un jeton.

Tableau 32

L'appel à syncMessages sans spécifier de token, renvoi uniquement un token.

L'appel à syncMessages avec un token, renvoi le différentiel de messages par rapport au moment où le token a été généré et un nouveau token.

Dans le cas d'une boite mail inchangée, syncMessages renvoi le même token qu'en entrée.

Il n'est pas possible de récupérer tous les messages d'une BAL à partir de syncMessages.

6.3.5.3 Flux sortants

Elément	Type	Card.	Description
deletedMessageIds	INT	0..*	Liste des ID des messages supprimés.
modifiedMessages	**Message**	0..*	Liste des messages créés et modifiés.
token	STRING	1	Token qui permettra de rappeler la synchronisation.

Tableau 33

6.3.5.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 34

6.3.5.5 Exposition SOAP

Opération « syncMessages » (cf. : WSDL SOAP du composant item : item.wsdl).

*https://server/mss-msg-services-igcsante/services/**Item**/soap/v**X**/**syncMessages***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.4 TM4.4.xC - Services envoi et consultation des pièces jointes

Les 3 transactions de Web Services décrites ci-dessous permettent d'envoyer et de consulter des pièces jointes.

Web Service	Description	Commande IMAP/SMTP équivalente
uploadAttachment	Envoyer une pièce jointe vers le serveur. Ce service est appelé dans le cadre d'un envoi de message ou d'un enregistrement de brouillon avec pièce jointe.	FETCH (IMAP)
removeAttachment	Supprimer une pièce jointe du serveur.	FETCH (IMAP)
downloadAttachment	Télécharger une pièce jointe d'un message étant donné l'ID du message et le numéro de la pièce jointe à télécharger.	Cette fonction est spécifique à l'utilisation de la messagerie via Web Service, il n'y a donc pas d'équivalent IMAP/SMTP

Tableau 35 : Liste des Web Services d'envoi et consultation des pièces jointes

La WSDL associée à ce service est : AttachmentService.wsdl (voir DR3 au § 8.6).

6.4.1 TM4.4.1C - Service uploadAttachment

6.4.1.1 Description

Le service « uploadAttachment » permet d'envoyer une pièce jointe vers le serveur. Ce service est appelé dans le cadre d'un envoi de message ou d'un enregistrement de brouillon avec pièce jointe.

6.4.1.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
file	base64Binary	0..1	Fichier à envoyer vers le serveur.
contentType	STRING(40)	1	Type de fichier (cf. RFC 2045, 2045 à 2048)*
fileName	STRING La taille max dépend du serveur de messagerie	1	Nom de fichier.

Tableau 36

** Attention : le* **contentType** *doit correspondre au type du fichier transmis (par exemple : "application/pdf" pour un PDF).*

6.4.1.3 Flux sortants

Elément	Type	Card.	Description
attachmentId	String	1	ID du ficher.

Tableau 37

6.4.1.4 Erreurs

Elément	Type	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**32**	La taille des pièces jointes est trop importante	La taille des pièces jointes est trop importante.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 38

6.4.1.5 Exposition SOAP

Opération « uploadAttachment » (cf. : WSDL SOAP du composant Attachement : attachement.wsdl).

*https://server/mss-msg-services-igcsante/services/**Attachment**/soap/vX/**uploadAttachment***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.4.2 TM4.4.2C - Service removeAttachment

6.4.2.1 Description

Le service « removeAttachment » permet de supprimer une pièce jointe du serveur.

6.4.2.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
messageId	INT	1	Identifiant du message sur lequel on souhaite supprimer un fichier.
part	INT	1	Numéro de la pièce jointe à supprimer.

Tableau 39

6.4.2.3 Flux sortants

Le service ne retourne rien si l'opération est effectuée.

6.4.2.4 Erreurs

Elément	Type	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**45**	Le messageId n'existe pas	Le messageId duquel on souhaite supprimer la pièce jointe n'existe pas.
403	**46**	La pièce jointe n'existe pas	
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 40

6.4.2.5 Exposition SOAP

Opération « removeAttachment » (cf. : WSDL SOAP du composant Attachement : attachement.wsdl).

*https://server/mss-msg-services-igcsante/services/**Attachment**/soap/vX/**removeAttachment***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.4.3 TM4.4.3C - Service downloadAttachment

6.4.3.1 Description

Le service « downloadAttachment » permet de télécharger une pièce jointe d'un message étant donné l'ID du message et le numéro de la pièce jointe à télécharger.

6.4.3.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
messageId	INT	1	ID du message.
part	INT	1	Numéro de la pièce jointe dans le message.

Tableau 41

6.4.3.3 Flux sortants

Elément	Type	Card.	Description
file	base64Binary	0..1	Ficher à envoyer vers le client.

Tableau 42

6.4.3.4 Erreurs

Elément	Type	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**45**	Le messageId n'existe pas	Le messageId duquel on souhaite télécharger la pièce jointe n'existe pas.
403	**46**	La pièce jointe n'existe pas	
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 43

6.4.3.5 Exposition SOAP

Opération « downloadAttachment » (cf. : WSDL SOAP du composant Attachement : attachement.wsdl).

*https://server/mss-msg-services-igcsante/services/**Attachment**/soap/vX/**downloadAttachment***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.5 TM4.5.xC - Services consultation et recherche de messages

Les 2 transactions de Web Services décrites ci-dessous permettent de rechercher et consulter des messages.

Web Service	Description	Commande IMAP/SMTP équivalente
searchMessages	Recherche multicritères de messages.	SEARCH (IMAP)
fullTextSearchMessages	Rechercher des messages sur l'objet, les destinataires, les destinataires en copie et l'expéditeur à partir d'un champ texte libre.	SEARCH (IMAP)

Tableau 44 : Liste des Web Services de consultation et recherche de messages

La WSDL associée à ce service est : ItemService.wsdl (voir DR2 au § 8.6).

6.5.1 TM4.5.1C - Service searchMessages

6.5.1.1 *Description*

Le service « searchMessages » permet d'effectuer des recherches multicritères de messages. Il permet également de récupérer la liste des messages d'un répertoire.

6.5.1.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
searchCriteria		0..1	Paramètres de recherche.
| - html	BOOLEAN	0..1	Si « true », le body de la réponse contiendra le code html Si « false » (ou non renseigné), le body de la réponse sera du texte brut
|- offset	INT	0..1	Si offset est renseigné avec la valeur n, alors on retourne les résultats à partir du nième résultat.
|- limit	INT	0..1	Nombre maximal de résultats à retourner.
|- sortBy	**EnumSort**	0..1	Type de tri. Si valeur vide ou type inexistant, le tri par défaut est par ordre de date décroissante.
|- query	Query	0..1	Critères de recherche.
|- content	STRING(80)	0..1	Messages contenant la chaîne spécifiée dans le corps du message.
|- subject	STRING(250)	0..1	Messages contenant la chaîne spécifiée dans l'objet du message.
|- to	STRING(256)	0..1	Messages contenant la chaîne spécifiée dans le champ « To ».
|- from	STRING(256)	0..1	Messages contenant la chaîne spécifiée dans le champ « From ».
|- cc	STRING(256)	0..1	Messages contenant la chaîne spécifiée dans le champ « Cc ».
|- folderId	INT	0..1	Messages dans un dossier spécifique. Si non renseigné, retourne le contenu de la boite de réception.
|- includeSubfolders	BOOLEAN	0..1	Par défaut « false ». Si positionné à « true », retourne également les messages des sous-dossiers.
|- before	STRING(19)	0..1	Messages reçus (ou envoyés si messages de type envoyés) avant la date spécifiée. Date au format « dd/MM/yyyy HH:mm:ss ».
|- after	STRING(19)	0..1	Messages reçus (ou envoyés si messages de type envoyés) après la date spécifiée. Date au format « dd/MM/yyyy HH:mm:ss ».
|- flagged	BOOLEAN	0..1	Messages ayant le flag « Flagged ».
|- draft	BOOLEAN	0..1	Messages ayant le flag « Draft ».
|- seen	BOOLEAN	0..1	Messages ayant le flag « Read ».
|- answered	BOOLEAN	0..1	Messages ayant le flag « Answered ».
|- larger	INT	0..1	Messages ayant une taille plus grande que la taille spécifiée (en octets).
|- smaller	INT	0..1	Messages ayant une taille plus petite que la taille spécifiée (en octets).
|- isSent	BOOLEAN	0..1	Messages envoyés.

Tableau 45

6.5.1.3 Flux sortants

Elément	Type	Card.	Description
messages	Message	0..*	Liste de messages.

Tableau 46

6.5.1.4 Erreurs

Elément	Type	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 47

6.5.1.5 Exposition SOAP

Opération « searchMessages » (cf. : WSDL SOAP du composant item : item.wsdl).

*https://server/mss-msg-services-igcsante/services/**Item**/soap/v**X**/**searchMessages***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.5.2 TM4.5.2C - Service fullTextSearchMessages

6.5.2.1 Description

Le service « fullTextSearchMessages » permet de rechercher des messages sur l'objet, les destinataires, les destinataires en copie et l'expéditeur à partir d'un champ texte libre.

6.5.2.2 Flux entrants

Elément	Type	Card.	Description
email	**EmailAuthent**	1	Identifiant de l'utilisateur : adresse de messagerie.
searchCriteria		1	Paramètres de recherche.
| - html	BOOLEAN	0..1	Si « true », le body de la réponse contiendra le code html, de type <body><html><body>contenu</body></html></body>. Si « false » (ou non renseigné), le body de la réponse sera du texte brut de type <body>contenu</body>. Pour information, dans les deux cas, la première balise <body></body> correspond à un champ du flux récupéré qui contient tout le message. Ce n'est pas une balise HTML.
|- offset	INT	0…1	Si offset est renseigné avec la valeur n, alors on retourne les résultats à partir du nième résultat.
|- limit	INT	0…1	Nombre maximal de résultats à retourner.
|- query	QueryFullText	0…1	Critères de recherche.
|- folderId	INT	0…1	Messages dans un dossier spécifique. Si non renseigné, retourne le contenu de la boite de réception.
|- before	STRING(19)	0…1	Messages reçus avant la date spécifiée. Date au format « dd/MM/yyyy HH:mm:ss ».
|- after	STRING(19)	0…1	Messages reçus après la date spécifiée. Date au format « dd/MM/yyyy HH:mm:ss ».
|- includeSubfolders	BOOLEAN	0..1	Par défaut « false ». Si « true », retourne également les messages des sous-dossiers.
| - searchString	String(256)	1	Texte libre.

Tableau 48

6.5.2.3 Flux sortants

Elément	Type	Card.	Description
messages	**Message**	0..1	Liste de messages.

Tableau 49

6.5.2.4 Erreurs

Code http	Code d'erreur	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**36**	Un des champs a un format invalide	Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).
403	**24**	L'adresse de messagerie est invalide	L'adresse de messagerie ne correspond pas à la session ouverte

Tableau 50

6.5.2.5 Exposition SOAP

Opération « fullTextSearchMessages » (cf. : WSDL SOAP du composant item : item.wsdl).

*https://server/mss-msg-services-igcsante/services/**Item**/soap/v**X**/**fullTextSearchMessages***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

6.6 TM4.6C - Service de recherche de BAL correspondant à un Professionnel de Santé

La transaction de Web Service décrite ci-dessous permet de récupérer la liste des adresses de messagerie valides et actives associées à un compte.

Exemple d'utilisation : On désire savoir si un professionnel de santé possède des adresses de messagerie. On va alors indiquer son identifiant d'utilisateur en format ADELI ou RPPS : on obtiendra en retour, s'il en possède, une liste d'adresses de cet utilisateur.

Web Service	Description	Commande IMAP/SMTP équivalente
listEmails	Récupérer la liste des adresses de messagerie valides et actives associées à un compte.	Cette fonction est spécifique à l'utilisation de la messagerie via Web Service. Il n'y a donc pas d'équivalent IMAP/SMTP.

Tableau 51 : Liste des Web Services de recherche des BAL d'un Professionnel de Santé

La WSDL associée à ce service est : AnnuaireService.wsdl (voir DR4 au § 8.6).

6.6.1 Description

Le service « listEmails » permet de récupérer la liste des adresses de messagerie valides et actives associées à un utilisateur, sur la base de ses données d'authentification.

6.6.2 Flux entrants

Elément	Type	Card.	Description
userId	STRING(32)	1	Identifiant de l'utilisateur en format ADELI ou RPPS.

Tableau 52

6.6.3 Flux sortants

Elément	Type	Card.	Description
emails	STRING	0…*	Liste d'adresses de messagerie d'un utilisateur.

Tableau 53

6.6.4 Erreurs

Elément	Type	Libellé Erreur	Description
400	**28**	Un des champs obligatoires n'est pas renseigné	Un des champs obligatoires (hors ceux servant au contrôle d'accès) n'est pas renseigné.
403	**11**	L'utilisateur n'existe pas	Retourné si l'identifiant de l'utilisateur demandé n'existe pas dans la base.
403	**34**	L'utilisateur n'a pas d'adresse de messagerie	L'utilisateur n'a pas d'adresse de messagerie.
403	**36**	Un des champs a un format invalide	Retourné si userId dépasse 256 caractères. Cas particulier pour un champ de type booléen, ce code d'erreur est retourné uniquement lorsque le champ booléen prends la valeur « T » ou « F » (au lieu des valeurs usuelles "false", "true", "0" ou "1"). Toute autre valeur erronée dans un champ de type booléen entraîne une mauvaise interprétation de ce champ (exception ou booléen à false).

Tableau 54

6.6.5 Exposition SOAP

Opération « listEmails » (cf. : WSDL SOAP du composant annuaire : annuaire.wsdl).

*https://server/mss-msg-services-igcsante/services/**Annuaire**/soap/v**X**/**listEmails***

Avec

- *Server* : url-du-serveur:port
- *X* : version majeure du service.

7 Transaction de consultation de l'Annuaire santé par le protocole LDAP

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

La fonction de consultation de l'Annuaire santé permet de rechercher un correspondant quel que soit l'opérateur qui héberge sa BAL, à l'exception de ceux déclarés en liste rouge. Il s'agit d'une recherche multi-critères qui retourne les informations d'identité, l'adresse de messagerie et les coordonnées de contact des destinataires potentiels.

Attention : le numéro de téléphone du professionnel de santé n'est pas transmis dans le résultat d'une recherche par le protocole LDAP.

Remarque : le renseignement des destinataires de messages peut être directement effectué par la saisie de l'adresse du correspondant, un copier/coller depuis une source d'information externe ou encore la sélection d'une entrée du carnet d'adresses local au client de messagerie. L'utilisation de l'Annuaire santé n'est donc pas systématique.

Utilisation des recherches de type « CONTIENT »

Il est recommandé, 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.

Filtrage des résultats de la recherche par le client de messagerie (en local)

Il est recommandé que le client de messagerie privilégie autant que possible les opérations de filtre des résultats de la recherche en local, sur la base des résultats fournis par l'Annuaire santé, lorsque, après récupération d'une première liste de résultats l'utilisateur souhaite affiner ses critères de recherche.

7.1 Cinématique

La cinématique de recherche dans l'Annuaire santé à partir d'un client de messagerie est la suivante :

- [Utilisateur] L'utilisateur saisit dans l'IHM de recherche du client de messagerie les critères voulus de recherche des correspondants dans l'Annuaire santé ;
- [Client] Le client de messagerie appelle la transaction TM2.1.1C de recherche dans l'Annuaire santé ;
- [Annuaire santé] L'Annuaire santé renvoie en retour la liste des enregistrements correspondants aux critères ;
- [Client] Le client de messagerie affiche les résultats à l'utilisateur avec des possibilités locales de filtres et de tris ; fin du processus.

7.2 TM2.1.1C - Interrogation de l'Annuaire santé par le protocole LDAP

L'interrogation de l'Annuaire santé par le protocole LDAP fait appel à la fonction LDAP Search.

Les champs standards LDAP communément utilisés dans les clients de messagerie du marché sont utilisés pour tous les critères de recherche correspondant aux données de l'Annuaire national MSSanté afin de faciliter son usage dans ce type de logiciel.

7.2.1 Prérequis

Afin de pouvoir accéder à l'Annuaire santé via les interfaces LDAP, les clients de messagerie doivent prendre en compte les paramétrages suivants :

Annuaire santé
• Nom DNS de l'Annuaire santé : ldap.annuaire.mssante.fr ; • URL d'accès : ldap://ldap.annuaire.mssante.fr ; • Base DN au moins égal à : « ou=bal,o=mssante,c=fr » ; • Port : 389.

Les commandes de recherche LDAP envoyées par le client de messagerie doivent être conformes à la RFC 2254 (voir http://tools.ietf.org/html/rfc2254).

7.2.2 DIT et types d'entrées de l'Annuaire santé

7.2.2.1 DIT de l'Annuaire santé

La figure suivante présente le schéma et l'arborescence (DIT pour Directory Information Tree) de l'Annuaire santé :

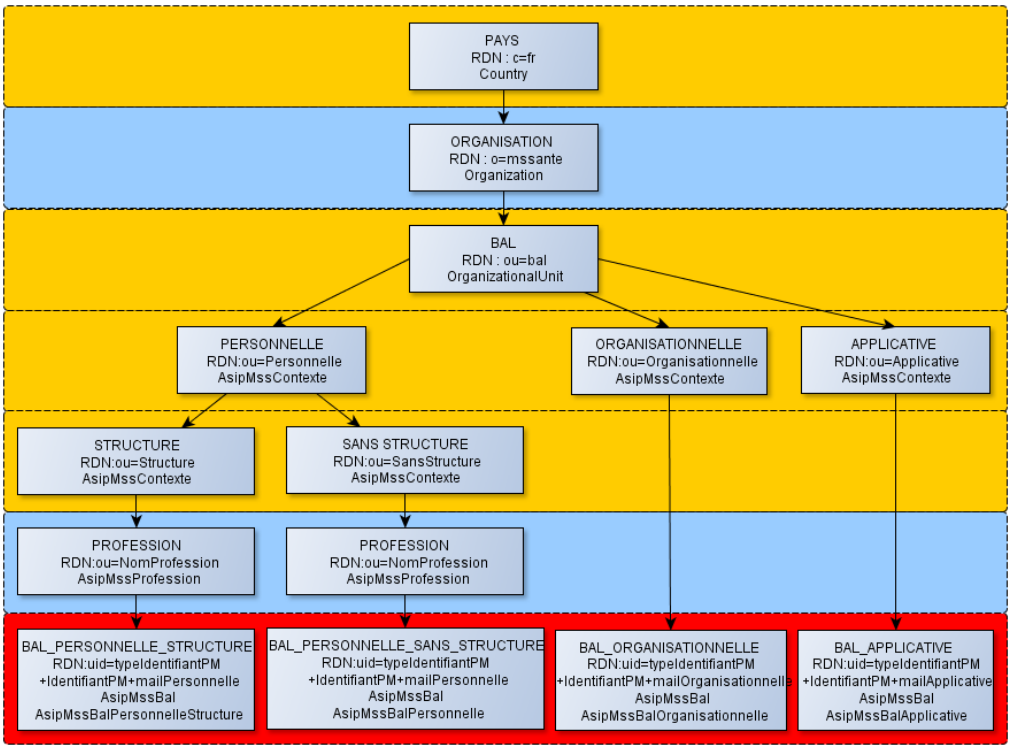

Figure 7 : Représentation du DIT de l'Annuaire santé

7.2.2.2 Types d'entrées de l'Annuaire santé

L'Annuaire santé compte différents types d'entrées :

- **PAYS :** nœud racine ;
- **ORGANISATION :** nœud correspondant à la branche mssante (o=MSSANTE) ;
- **BAL :** nœud se trouvant sous le nœud ORGANISATION. Les entrées de ce type représentent la racine des BAL MSSanté ;
- **PERSONNELLE :** nœud se trouvant sous le nœud BAL. Les entrées de ce type regroupent les entrées associées ou non à une structure **;**
- **ORGANISATIONNELLE[3] :** nœud se trouvant sous le nœud BAL. Les entrées de ce type regroupent les BAL organisationnelles ;
- **APPLICATIVE[4] :** nœud se trouvant sous le nœud BAL. Les entrées de ce type regroupent les BAL applicatives ;
- **STRUCTURE :** nœud se trouvant sous le nœud PERSONNELLE. Les entrées de ce type représentent les entrées associées à une structure ;
- **SANS_STRUCTURE :** nœud se trouvant sous le nœud PERSONNELLE. Les entrées de ce type représentent les entrées non associées à une structure ;
- **PROFESSION :** nœud se trouvant sous les nœuds STRUCTURE et SANS_STRUCTURE. Les entrées de ce type représentent les différentes professions ;
- **BAL_PERSONNELLE_STRUCTURE :** feuille se trouvant sous le nœud PROFESSION. Les entrées de ce type représentent les BAL Personnelles associées à une structure ;
- **BAL_PERSONNELLE_SANS_STRUCTURE :** feuille se trouvant sous le nœud PROFESSION. Les entrées de ce type représentent les BAL Personnelles non associées à une structure ;
- **BAL_ORGANISATIONNELLE :** feuille se trouvant sous le nœud ORGANISATIONNELLE. Les entrées de ce type représentent les BAL organisationnelles ;
- **BAL_APPLICATIVE :** feuille se trouvant sous le nœud APPLICATIVE. Les entrées de ce type représentent les BAL applicatives.

7.2.2.3 Objectclass

Les objectclasses non vides servent à définir des types d'entrées.

- AsipMssContexte : définit le contexte des BAL par exemple Personnelle, PersonnelleStructure, PersonnelleSansStructure, Organisationnelle, Applicative… ;
- AsipMssProfession : définit la profession d'un professionnel de santé ;
- AsipMssBalStd : définit une BAL adaptée aux clients de messagerie standard du marché (se reporter au paragraphe 7.2.3);
- AsipMssBal : définit les informations complémentaires exploitables par les Logiciels de Professionnels de Santé et hérite de l'objectclass « AsipMssBalStd » (se reporter au paragraphe 7.2.3 et 7.2.4).

Les objectclasses vides servent à marquer des entrées et à définir des sous-types d'entrées :

- AsipMssBalPersonnelle : définit une BAL personnelle non associée à une structure ;
- AsipMssBalPersonnelleStructure : définit une BAL personnelle associée à une structure ;
- AsipMssBalOrganisationnelle : définit une BAL organisationnelle ;
- AsipMssBalApplicative : définit une BAL applicative.

[3] BAL Organisationnelle : Se reporter au paragraphe 2.2.1.2.2 du présent document.

[4] BAL Applicative : Se reporter au paragraphe 2.2.1.2.3 du présent document.

7.2.3 Liste des attributs LDAP standards utilisés

Les attributs standards utilisés sont :

Attribut	Description	Objectclass	Syntaxe	Multi-valué	Sens. Casse	Taille Max
cn (CommonName)		asipMssBalStd	Chaîne	Oui	Non	200
description	Notes	asipMssBalStd	Chaîne	Non	Non	1024
gn (givenName)	Prénom usuel	asipMssBalStd	Chaîne	Oui	Non	50
l (localityName)	Nom de la ville	asipMssBalStd	Chaîne	Oui	Non	128
Mail	Adresse MSSanté	asipMssBalStd	Chaîne	Oui	Non	256
o (OrganizationName)	Nom de l'organisation	organization asipMssBalStd	Chaîne	Oui	Non	164
ou (OrganizationalUnitName)	Nom de la racine des BAL, nom du contexte, nom de la profession, nom du service d'attachement	organizationalUnit asipMssContexte asipMssProfession asipMssBalStd	Chaîne	Oui	Non	250
postaladdress	Adresse postale	asipMssBalStd	Chaîne	Oui	Non	250
postalcode	Code postal	asipMssBalStd	Chaîne	Oui	Non	40
sn (surname)	Nom d'exercice	asipMssBalStd	Chaîne	Oui	Non	170
street	Adresse postale	asipMssBalStd	Chaîne	Oui	Non	250
telephonenumber	Numéro de téléphone	asipMssBalStd	Chaîne	Oui	-	20
Title	Profession et spécialité (le cas échéant).	asipMssBalStd	Chaîne	Oui	Non	250
Info	Notes	asipMssBalStd	Chaîne	Oui	Non	1024
c (countryName)	Code du pays sur deux caractères	Country asipMssBal	Chaîne	Non	Non	2
uid	Attribut technique	asipMssBalStd	Chaîne	Oui	Non	320

Tableau 55 : Liste des attributs LDAP standards utilisés

7.2.4 Liste des attributs LDAP spécifiques à l'Annuaire santé

Attribut	Description	Objectclass	Syntaxe	Multi-valué	Sens. Casse	Taille Max
raisonSociale	Raison sociale de la Structure d'activité	asipMssBal	Chaîne	Non	Non	164
specOrdRPPS	Spécialité Ordinale RPPS Code Table R01 – Spécialités RPPS Que pour les Médecins et Chirurgiens-Dentistes	asipMssBal	Chaîne	Non	Non	10
codeProfession	Code de la profession Code Table G15 – Professions Que pour les professionnels de santé.	asipMssBal	Chaîne	Non	Non	10
codeCategorieProfession	Code de la catégorie de profession	asipMssBal	Chaîne	Oui	Non	10
libelleCategorieProfession	Libellé de la catégorie de profession	asipMssBal	Chaîne	Oui	Non	100
typeBal	Type de Bal	asipMssBal	Chaîne	Non	Non	3
dematerialisationBal	Indicateur d'acceptation de la dématérialisation.	asipMssBal	Chaîne	Non	Non	1
descriptionBal	Description fonctionnelle de la BAL	asipMssBal	Chaîne	Non	Non	160
responsableBal	Les coordonnées de la personne responsable au niveau opérationnel de la BAL	asipMssBal	Chaîne	Oui	Non	160
serviceRattachementBAL	Nom et description du service de rattachement de l'utilisateur dans l'organisation	asipMssBal	Chaîne	Oui	Non	160
enseigneCommerciale	Enseigne commerciale de la Structure d'activité	asipMssBal	Chaîne	Oui	Non	64
civiliteExercice	Civilité de la situation d'exercice de l'utilisateur	asipMssBal	Chaîne	Non	Non	64
departement	Département	asipMssBal	Chaîne	Oui	Non	3
pS_IdNat	Identifiant National PS	asipMssBal	Chaîne	Oui	Non	64
struct_IdNat	Identifiant National Structure	asipMssBal	Chaîne	Oui	Non	64
company	Le nom de la société	asipMssBal	Chaîne	Oui	Non	160

Tableau 56 : Liste des attributs LDAP spécifiques

7.2.5 Contenu des attributs

Le tableau suivant décrit le contenu des champs de l'Annuaire LDAP à partir des champs présents dans l'extraction de l'Annuaire santé, en différenciant les cas des BAL de type « PER » et des BAL de type « ORG » ou « APP ».

Ce tableau est réalisé sur la base des champs du fichier d'extraction de l'Annuaire santé, voir le chapitre « TM2.1.3A – Téléchargement d'une extraction de l'Annuaire santé » et plus précisément le sous-chapitre « Format du fichier d'extraction » du DSFT Opérateurs.

Attribut LDAP	Cas BAL Personnelle	Cas BAL Applicative ou Organisationnelle
cn :	Concaténation des données (séparées par un espace) : NOMEXERCICE en majuscules, PRENOMEXERCICE la 1e lettre en majuscule, - (*tiret*) NPROFESSION en majuscules, *Exemple* : DUPONT Jean – MEDECIN	Concaténation des données : • Si RAISONSOCIALE n'est pas vide, RAISONSOCIALE (CODE_POSTAL) • Si RAISONSOCIALE est vide, ENSEIGNECOMMERCIALE (CODE_POSTAL) *Exemple* : HOPITAL LA PITIE SALPETRIERE (75013)
description :	Ce champ peut contenir jusqu'à 4 informations. Identifiant du PS • Si TYPEIDENTIFIANTPP = 0 ou 8, alors concaténation de : « Identifiant national du PS : » et concaténation de TYPEIDENTIFIANTPP et IDENTIFIANTPP (sans espace de séparation) • Sinon aucune information. <u>Civilité d'exercice</u> • Si NCIVILITEEXERCICE n'est pas vide, alors concaténation de : « Civilité d'exercice : » et NCIVILITEEXERCICE • Sinon aucune information. <u>Type de BAL</u> Concaténation de « Type de BAL : » et libellé fonctionnel de TYPEBAL <u>Dématérialisation</u> • Si DEMATERIALISATION = « vrai » ; alors « Zéro papier : oui » • Si DEMATERIALISATION = « faux » ; alors « Zéro papier : non » *Exemple* : Identifiant national du PS : 811111111111 Civilité d'exercice : Professeur Type de BAL : BAL personnelle Zéro papier : oui	Ce champ peut contenir jusqu'à 5 informations. Identifiant structure Concaténation des données « Identifiant structure : » et concaténation de TYPEIDENTIFIANTPM et IDENTIFIANTPM (sans espace de séparation) <u>Type de BAL</u> Concaténation de « Type de BAL : » et libellé fonctionnel de TYPEBAL <u>Description de la BAL</u> Concaténation de « Description de la BAL : » et DESCRIPTION <u>Responsable de la BAL</u> Concaténation de « Responsable de la BAL : » et RESPONSABLE <u>Dématérialisation</u> • Si DEMATERIALISATION = « vrai » ; alors « Zéro papier : oui » • Si DEMATERIALISATION = « faux » ; alors « Zéro papier : non » *Exemple* : Identifiant structure : 12222222222 Type de BAL : BAL organisationnelle Description de la BAL : xxxxxxxxxxxx Responsable de la BAL : xxxxxxxxxxxx Zéro papier : oui
givenname :	PRENOMEXERCICE	s/o
l :	NCOMMUNE	NCOMMUNE
mail :	ADRESSEBAL	ADRESSEBAL

Attribut LDAP	Cas BAL Personnelle	Cas BAL Applicative ou Organisationnelle
o :	Concaténation des données : • Si RAISONSOCIALE n'est pas vide, RAISONSOCIALE (CODE_POSTAL) • Si RAISONSOCIALE est vide, ENSEIGNECOMMERCIALE (CODE_POSTAL) *Exemple* : HOPITAL LA PITIE SALPETRIERE (75013)	Concaténation des données : • Si RAISONSOCIALE n'est pas vide, RAISONSOCIALE (CODE_POSTAL) • Si RAISONSOCIALE est vide, ENSEIGNECOMMERCIALE (CODE_POSTAL) *Exemple* : HOPITAL LA PITIE SALPETRIERE (75013)
ou :	SERVICERATTACHEMENT	SERVICERATTACHEMENT
postaladdress :	L2COMPLEMENTLOCALISATION L3COMPLEMENTDISTRIBUTION L4NUMEROVOIE + L4COMPLEMENTNUMEROVOIE + NL4TYPEVOIE +L4LIBELLEVOIE L5LIEUDITMENTION L6LIGNEACHEMINEMENT	L2COMPLEMENTLOCALISATION L3COMPLEMENTDISTRIBUTION L4NUMEROVOIE + L4COMPLEMENTNUMEROVOIE + NL4TYPEVOIE +L4LIBELLEVOIE L5LIEUDITMENTION L6LIGNEACHEMINEMENT
postalcode :	NCODEPOSTAL	NCODEPOSTAL
sn :	NOMEXERCICE	Concaténation des données : • Si RAISONSOCIALE n'est pas vide, RAISONSOCIALE (CODE_POSTAL) • Si RAISONSOCIALE est vide, ENSEIGNECOMMERCIALE (CODE_POSTAL) *Exemple* : HOPITAL LA PITIE SALPETRIERE (75013)
street :	L2COMPLEMENTLOCALISATION L3COMPLEMENTDISTRIBUTION L4NUMEROVOIE + L4COMPLEMENTNUMEROVOIE + NL4TYPEVOIE +L4LIBELLEVOIE L5LIEUDITMENTION L6LIGNEACHEMINEMENT	L2COMPLEMENTLOCALISATION L3COMPLEMENTDISTRIBUTION L4NUMEROVOIE + L4COMPLEMENTNUMEROVOIE + NL4TYPEVOIE +L4LIBELLEVOIE L5LIEUDITMENTION L6LIGNEACHEMINEMENT
telephonenumber :	s/o	s/o
title :	Concaténation des données (séparées par un espace) : NPROFESSION (libellé court) NSPECIALITE (libellé court) *Exemple* : MEDECIN Pédiatrie	s/o
company :	Concaténation des données : • Si RAISONSOCIALE n'est pas vide, RAISONSOCIALE (CODE_POSTAL) • Si RAISONSOCIALE est vide, ENSEIGNECOMMERCIALE (CODE_POSTAL) *Exemple* : HOPITAL LA PITIE SALPETRIERE (75013)	Concaténation des données : • Si RAISONSOCIALE n'est pas vide, RAISONSOCIALE (CODE_POSTAL) • Si RAISONSOCIALE est vide, ENSEIGNECOMMERCIALE (CODE_POSTAL) *Exemple* : HOPITAL LA PITIE SALPETRIERE (75013)
info :	Ce champ peut contenir jusqu'à 4 informations. Identifiant du PS • Si TYPEIDENTIFIANTPP = 0 ou 8, alors concaténation de : « Identifiant national du PS : » et	Ce champ peut contenir jusqu'à 5 informations. Identifiant structure Concaténation des données « Identifiant structure : » et concaténation de TYPEIDENTIFIANTPM et IDENTIFIANTPM (sans espace de séparation)

Attribut LDAP	Cas BAL Personnelle	Cas BAL Applicative ou Organisationnelle
	concaténation de TYPEIDENTIFIANTPP et IDENTIFIANTPP (sans espace de séparation) • Sinon aucune information. <u>Civilité d'exercice</u> • Si NCIVILITEEXERCICE n'est pas vide, alors concaténation de : « Civilité d'exercice : » et NCIVILITEEXERCICE • Sinon aucune information. <u>Type de BAL</u> Concaténation de « Type de BAL : » et libellé fonctionnel de TYPEBAL <u>Dématérialisation</u> • Si DEMATERIALISATION = « vrai » ; alors « Zéro papier : oui » • Si DEMATERIALISATION = « faux » ; alors « Zéro papier : non » *Exemple* : Identifiant national du PS : 811111111111 Civilité d'exercice : Professeur Type de BAL : BAL personnelle Zéro papier : oui	<u>Type de BAL</u> Concaténation de « Type de BAL : » et libellé fonctionnel de TYPEBAL <u>Description de la BAL</u> Concaténation de « Description de la BAL : » et DESCRIPTION <u>Responsable de la BAL</u> Concaténation de « Responsable de la BAL : » et RESPONSABLE <u>Dématérialisation</u> • Si DEMATERIALISATION = « vrai » ; alors « Zéro papier : oui » • Si DEMATERIALISATION = « faux » ; alors « Zéro papier : non » *Exemple* : Identifiant structure : 12222222222 Type de BAL : BAL organisationnelle Description de la BAL : xxxxxxxxxxxx Responsable de la BAL : xxxxxxxxxxxx Zéro papier : oui
typeBal :	TYPEBAL	TYPEBAL
structIdNat :	s/o	Concaténation de TYPEIDENTIFIANTPM et IDENTIFIANTPM (sans espace de séparation) *Exemple* : 12222222222
dematerialisationBAL :	DEMATERIALISATION	DEMATERIALISATION
descriptionBAL :	s/o	DESCRIPTION
responsableBAL :	s/o	RESPONSABLE
serviceRattachementBAL :	SERVICERATTACHEMENT	SERVICERATTACHEMENT
raisonSociale :	RAISONSOCIALE	RAISONSOCIALE
enseigneCommerciale :	ENSEIGNECOMMERCIALE	ENSEIGNECOMMERCIALE
c :	NPAYS (code ISO)	NPAYS (code ISO)
civiliteExercice	NCIVILITEEXERCICE	s/o
pSIdNat	• Si TYPEIDENTIFIANTPP = 0 ou 8, alors concaténation de : "Identifiant national du PS :" et Concaténation de TYPEIDENTIFIANTPP et IDENTIFIANTPP (sans espace de séparation) • Sinon aucune information. Exemple : 811111111111	s/o
departement	NDEPARTEMENT	NDEPARTEMENT
specOrdRPPS	NSPECIALITE (code spécialité)	s/o

Attribut LDAP	Cas BAL Personnelle	Cas BAL Applicative ou Organisationnelle
codeProfession	NPROFESSION (code profession)	s/o
codeCategorieProfession	NCATEGORIEPROFESSION (code catégorie de professions)	s/o
libelleCategorieProfession	NCATEGORIEPROFESSION (libellé catégorie de professions)	s/o

Tableau 57 : contenu des attributs de l'annuaire LDAP

7.2.6 Critères de recherche

La recherche peut être réalisée selon plusieurs critères correspondant aux attributs et types d'entrées présentés ci-dessus : nom d'exercice, prénom d'exercice, profession, spécialité, lieu d'exercice (raison sociale ou enseigne commerciale, ville, département ou code postal), etc.

Plusieurs critères peuvent être associés entre eux (à l'aide d'opérateurs logiques).

Les opérateurs recommandés pour les filtres de recherche sont les suivants :

Description	Opérateurs
Egalité	=
ET logique	&
OU logique	|
Négation	!

Tableau 58 : Liste des opérateurs recommandés pour les filtres de recherche

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

7.2.7 Données en entrée

Les données en entrée de la fonction LDAP Search doivent être cohérentes avec le schéma de l'annuaire LDAP représenté dans ce chapitre.

7.2.8 Résultats fournis par l'Annuaire santé

Un nombre maximum de résultats est prévu : au-delà, l'Annuaire santé renvoie un code d'erreur que le client de messagerie 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 résultats retourné dépasse le paramètre SIZELIMIT défini côté serveur.

Annuaire santé
Les valeurs configurées par défaut sur l'Annuaire santé sont : • TimeLimitExceeded : 1 minute ; • SizeLimitExceeded : 100 entrées.

8 Annexes

8.1 L'opérateur Mailiz en production

Chaque opérateur se conformant aux interfaces du DST devra communiquer aux clients de messagerie ayant vocation à se connecter à ses services, les paramétrages qui lui sont propres sous une forme équivalente à celle présentée dans ce paragraphe.

8.1.1 Les interfaces clients de messagerie de l'opérateur Mailiz

8.1.1.1 Webmail de l'opérateur Mailiz

Le webmail de l'opérateur Mailiz Santé est accessible à partir du site permettant l'auto-création de BAL personnelles, ainsi que la gestion de leur compte par les utilisateurs. Un lien vers ce site est présent sur le portail de l'espace de confiance MSSante : https://www.mssante.fr/

8.1.1.2 Transactions standards SMTP / IMAP sur TLS

Rappel : Sur le service de l'opérateur Mailiz seule l'authentification par carte CPS est possible pour les transactions SMTP/IMAP sur TLS.

Service	Serveur MSSanté
SMTP	- Nom du serveur : frontsmtp-igcsante.mssante.fr - Port : 587 - Sécurité de la connexion : STARTTLS - Authentification : password-cleartext
IMAP	- Nom du serveur : frontimap-igcsante.mssante.fr - Port : 143 - Sécurité de la connexion : STARTTLS - Authentification : password-cleartext

8.1.1.3 Web Services de messagerie

Rappel : Sur le service de l'opérateur Mailiz seules les authentifications par carte CPS et par identifiant/mot de passe /OTP sont possibles pour les transactions de Web Services de messagerie.

Service	Description	URLs pour l'Opérateur Mailiz
Services d'authentification		
Authentification par CPS	Authentification préalable par CPS au service de messagerie.	https://mss-idp-igcsante.mssante.fr/openam/SSOSoap/metaAlias/asip/idp
Authentification par identifiant / mot de passe / OTP	Authentification préalable par identifiant / mot de passe / OTP au service de messagerie.	https://mss-idp-igcsante.mssante.fr/openam/SSOSoap/metaAlias/asip/idp
Services de consultation et de gestion des dossiers		
listFolders	Récupérer la liste détaillée de tous les dossiers existants, ou une liste détaillée des sous-dossiers d'un dossier spécifique.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/listFolders
createFolder	Créer un nouveau dossier pour y ranger des messages.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/createFolder
deleteFolder	Supprimer un dossier, ainsi que tous les messages et tous les sous-dossiers dans ce dossier. Cette suppression est définitive (ce n'est pas une suppression dans la corbeille comme la méthode Trash).	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/deleteFolder
emptyFolder	Vider tous les messages et tous les sous-dossiers d'un dossier spécifique.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/emptyFolder
trashFolder	Déplacer un dossier et ses sous-dossiers vers la corbeille, marquant tous les contenus comme lus et le renommer si un dossier portant ce nom est déjà existant dans la corbeille.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/trashFolder
renameFolder	Changer le nom d'un dossier existant.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/renameFolder
moveFolder	Déplacer un dossier.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/moveFolder
Services envoi et gestion de messages		
updateMessages	Mettre à jour une liste de	https://mss-msg-igcsante.mssante.fr/mss-msg-services-

Service	Description	URLs pour l'Opérateur Mailiz
	messages.	igcsante/services/Item/soap/v1/updateMessages
draftMessage	Enregistrer un message comme un brouillon avec ses pièces jointes.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/draftMessage
moveMessages	Déplacer une liste de message vers un autre dossier.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/moveMessages
sendMessage	Envoyer un message avec ses pièces jointes.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/sendMessage
syncMessages	Obtenir les éléments à synchroniser avec le serveur.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/syncMessages
Services envoi et consultation des pièces jointes		
uploadAttachment	Envoyer une pièce jointe vers le serveur. Ce service est appelé dans le cadre d'un envoi de message ou d'un enregistrement de brouillon avec pièce jointe.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Attachment/soap/v1/uploadAttachment
removeAttachment	Supprimer une pièce jointe du serveur.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Attachment/soap/v1/removeAttachment
downloadAttachment	Télécharger une pièce jointe d'un message étant donné l'ID du message et le numéro de la pièce jointe à télécharger.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Attachment/soap/v1/downloadAttachment
Services consultation et recherche de messages		
searchMessages	Recherche multicritères de messages.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/searchMessages
fullTextSearchMessages	Rechercher des messages sur l'objet, les destinataires, les destinataires en copie et l'expéditeur à partir d'un champ texte libre.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/fullTextSearchMessages
Services recherche de BAL		
listEmails	Récupérer la liste des adresses de messagerie valides et actives associées à un compte.	https://mss-msg-igcsante.mssante.fr/mss-msg-services-igcsante/services/Annuaire/soap/v1/listEmails

Tableau 59 : URL des services MSSanté de l'opérateur Mailiz en production

8.1.2 Les clients de messagerie de l'opérateur Mailiz

8.1.2.1 Application mobile MSSanté de l'opérateur Mailiz

L'ANS, en tant qu'opérateur MSSanté, a développé une application mobile spécifique pour l'accès en mobilité à son service de messagerie. Cette application est « propriétaire », les spécifications techniques (dont la partie d'authentification des utilisateurs) ne seront donc pas exposées publiquement.

Celle-ci est accessible sur les smartphones et tablettes sous Android et iOS (Apple). Cette application permet aux titulaires d'un compte MSSanté sur le service de l'opérateur Mailiz d'accéder à toutes les fonctionnalités de la messagerie et à l'Annuaire santé. Cette application mobile utilise des Web Services REST et une authentification par un mécanisme de One Time Password en mode push.
Les principes d'identification et d'authentification des utilisateurs qui sont utilisés dans le cadre de cette application mobile développée par l'ANS reposent principalement sur :

- « l'enrôlement » du terminal mobile (par l'intermédiaire du portail web où l'utilisateur a préalablement créé son compte en utilisant sa carte CPS) de l'utilisateur,
- le service d'authentification de l'opérateur Mailiz couplé avec un système d'OTP Push.

Cependant, d'autres opérateurs MSSanté sont libres de mettre en place des systèmes différents en fonction des besoins identifiés et sous réserve de respecter les exigences de la CNIL et de la PGSSI-S.

Des informations complémentaires sont présentes dans le document « Présentation générale des procédures d'enrôlement et d'authentification mises en œuvre par l'opérateur Mailiz pour l'application MSSanté pour terminaux mobiles » [MOBILITE-MSSANTE] disponible en téléchargement via le lien https://www.mssante.fr/is/doc-technique.

8.1.2.2 Thunderbird, logiciel de messagerie compatible avec le service MSSanté de l'opérateur Mailiz

Le logiciel Thunderbird (qui utilise les protocoles SMTP/IMAP), peut être configuré pour permettre à un professionnel de santé disposant d'une carte CPS et d'un compte de messagerie existant sur le service de l'opérateur Mailiz d'accéder à son compte et de gérer dans un seul outil tous ses comptes de messagerie.

Le logiciel Thunderbird, ainsi configuré supporte l'authentification par CPS.

Des informations complémentaires sont disponibles sur le portail Web MSSanté à l'adresse suivante : https://www.mssante.fr/telechargements/thunderbird.

8.1.3 Cas particulier des cabinets de radiologie disposant d'identifiant RPPS Rang

Outre les authentifications de personne physique par carte CPS ou par OTP, Mailiz propose depuis juillet 2021 une authentification par certificat ORG AUTH_CLI présentant un identifiant de type RPPS Rang dans le champ « OU ».

Cette fonctionnalité est réservée au cas d'usage des cabinets de radiologie individuel. Elle permet de se connecter à une BAL personnelle d'un radiologue au moyen d'un certificat ORG AUTH_CLI présentant un identifiant RPPS Rang d'un de ces cabinets. L'objectif est de permettre à un logiciel métier d'envoyer des messages depuis la BAL personnelles du radiologue sans recourir à une authentification interactive du radiologue.

Les différents certificats permettent de se connecter à la même BAL personnelle du radiologue rattachée à l'identifiant RPPS du radiologue.

Exemple :

Un certificat ORG_AUTH_CLI présentant un DN du type :

```
CN=<champ libre>,OU=411111111111222,O=CABINET DU DR RADIO,ST=Somme
                                (80),C=FR
```

Permet de se connecter à la BAL personnelle Mailiz (préalablement créée) rattachée au RPPS :

```
      811111111111
```

Les procédures de commande de certificats ORG AUTH_CLI sont disponibles via les procédures [PSCE-CDE-PM] et [PSCE-CDE-TEST] (voir documents applicables §8.9.1).

8.2 L'Annuaire santé de production

Service	Paramètres
LDAP Annuaire santé	Nom DNS de l'Annuaire santé : ldap.annuaire.mssante.fr URL d'accès : ldap://ldap.annuaire.mssante.fr Port : 389 Base DN au moins égale : «ou=bal,o=mssante,c=fr »

8.3 Les environnements de tests de l'opérateur Mailiz

8.3.1.1 Utilité des environnements de tests

L'ANS met à la disposition des éditeurs qui développent des clients de messagerie devant s'interfacer avec l'opérateur Mailiz ou tous autres opérateurs MSSanté compatibles au DST, un espace de tests composé :

- d'un environnement MSSanté de tests (dit "formation"),
- d'un Annuaire santé de tests (dit "partenaires").

Ces environnements de tests permettent aux éditeurs de vérifier les solutions qu'ils développent. En particulier, ils peuvent par exemple vérifier simplement et rapidement qu'un mail émis par un client de messagerie depuis une BAL 1 de test est bien reçu sur une BAL 2 de test.

Cinématique suggérée :

1) **Création d'un compte de messagerie**

   Se rendre sur le Portail Web MSSanté de test (www.formation.mssante.fr), en utilisant une **CPS de test valide (rappel : seule la CPS de test est autorisée sur l'environnement de tests de l'opérateur Mailiz)**. Cliquer sur « J'active mon compte ! » puis suivre la démarche indiquée de création d'un compte de messagerie. L'éditeur peut créer autant de comptes qu'il le souhaite (avec des CPS de tests différentes) sur les domaines de tests de l'opérateur Mailiz (par exemple : @pharmacien.formation.mssante.fr, @pro.formation.mssante.fr).
   Attention, le poste de travail doit être configuré correctement pour pouvoir utiliser toutes les fonctionnalités du Portail Web MSSanté.

2) **Test des interfaces MSSanté**

   L'éditeur peut tester les interfaces implémentées en utilisant les comptes de tests créés en 1).
   Par exemple, il peut tester l'envoi d'un mail depuis le client de messagerie (utilisant une des interfaces décrites dans le DST avec un des moyens d'authentification implémentés sur le service de l'opérateur Mailiz), puis vérifier la réception de ce mail en utilisant soit le Webmail du Portail Web MSSanté, soit le client Thunderbird MSSanté configuré sur les environnements de tests, soit la version de tests de l'application mobile MSSanté (téléchargeable sur le Portail Web MSSanté de test , une fois connecté : https://www.formation.mssante.fr/mobilite).

3) Test de l'interface LDAP de l'Annuaire santé de tests

   L'éditeur peut tester l'interface LDAP de l'Annuaire santé de test en recherchant les informations relatives aux comptes de messagerie de test qu'il a créé (données d'identité, situation d'exercice, BAL de test, etc.).
   Les comptes de messagerie sont disponibles dans l'Annuaire santé de tests le jour qui suit leur création. Par contre, les nouveaux comptes de messagerie sont immédiatement visibles par le Webmail du Portail Web MSSanté.

4) **Test via la MSSanté de réception de messages contenant des documents structurés (pièces jointes au format IHE-XDM)**

L'éditeur peut réaliser des tests de réception et de bonne intégration de document structurés (tels qu'un Volet de Synthèse Medical ou des comptes rendu d'examens de biologie) au sein de sa solution.
En effet des BAL de type « répondeurs automatiques » sont disponibles sur l'environnement de tests de l'opérateur Mailiz. Dès réception d'un mail par une de ces BAL, celle-ci retourne immédiatement à l'expéditeur un message prédéfini contenant en pièce jointe un ou plusieurs documents structurés dans un fichier IHE_XDM.ZIP.
Pour plus d'information, se reporter à l'adresse suivante : https://www.formation.mssante.fr/aide/editeurs, paragraphe 4) « Utiliser le service répondeur pour tester la réception de documents structurés XDM ».

L'éditeur peut donc envoyer un mail depuis son compte de tests sur une des BAL répondeur automatique de tests et ainsi tester :

- la bonne réception de message contenant des pièces jointes au format IHE_XDM,
- la bonne intégration de documents structurés (tels qu'un Volet de Synthèse Medical ou des comptes rendu d'examens de biologie) au sein de sa solution.

Remarque : Pour plus de détails, un guide concernant l'échange de documents de santé structurés par la MSSanté [ECHANGES-STRUCTURES-MSSANTE] est disponible en téléchargement via le lien suivant https://www.mssante.fr/is/doc-technique.

8.3.1.2 Les données de tests

Sur les environnements de tests, aucune donnée de santé à caractère personnel ne peut être utilisée. Seules sont présentes des données de tests qui ne correspondent à aucun patient réel.
L'environnement MSSanté de tests est chargé et utilisable avec l'ensemble des **cartes CPS de tests** valides (non expirées) sur le périmètre des professions de santé répertoriées dans les référentiels ADELI et RPPS. Les cartes de test de professions intégrées au RPPS (http://esante.gouv.fr/services/referentiels/identification/le-rpps-et-adeli) porteuse d'un numéro Adeli (Type d'identifiant 0) ne sont pas intégrées dans l'environnement de tests. La fréquence de mise à jour des données issues du SI-CPS (nouvelles cartes CPS de tests chargés sur l'environnement MSSanté de tests) est quotidienne.
L'Annuaire santé de tests est alimenté quotidiennement par les comptes de messagerie de tests créés sur l'environnement MSSanté de tests[5].

[5] L'Annuaire national MSSanté de tests est également alimenté en BAL par d'autres environnements MSSanté de tests que celui mis à la disposition des éditeurs de clients de messagerie. Sa consultation peut donc restituer des BAL rattachées à d'autres domaines de messagerie que ceux de l'environnement MSSanté de tests éditeurs (dit « formation »). La tentative d'émission de messages vers ces BAL ne fonctionne pas, dans la mesure où les domaines de messagerie correspondant ne figurent pas dans la liste blanche des domaines de l'environnement MSSanté de tests éditeurs (dit « formation »).

8.3.1.3 Cartes CPS de tests

Pour les tests, les éditeurs doivent :

- utiliser des cartes CPS de tests qui peuvent être obtenu auprès de l'ANS ;
- intégrer éventuellement des middlewares de lecture de carte CPS de tests.

Un espace dédié ayant pour objectif de mettre à disposition des éditeurs les éléments techniques nécessaires à l'intégration du système CPS (cartes CPS, API CPS, …) dans leurs applications est disponible à l'adresse suivante : http://esante.gouv.fr/services/espace-cps/produit-de-certificat-de-test.

8.3.2 Les interfaces clients de messagerie de tests de l'opérateur Mailiz

8.3.2.1 Webmail de tests de l'opérateur Mailiz accessible sur le portail Web MSSanté de tests

https://www.formation.mssante.fr/

8.3.2.2 Transactions standards SMTP / IMAP sur TLS

Rappel : Sur l'environnement de tests de l'opérateur Mailiz seule l'authentification par carte CPS de tests est possible pour les transactions SMTP/IMAP sur TLS.

Service	Serveur MSSanté
SMTP	- Nom du serveur : frontsmtp-igcsante.formation.mssante.fr - Port : 587 - Sécurité de la connexion : STARTTLS - Authentification : password-cleartext
IMAP	- Nom du serveur : frontimap-igcsante.formation.mssante.fr - Port : 143 - Sécurité de la connexion : STARTTLS - Authentification : password-cleartext

8.3.2.3 Web Services de messagerie

Rappel : Sur l'environnement de tests de l'opérateur Mailiz seules les authentifications par carte CPS et par identifiant/mot de passe /OTP sont possibles pour les transactions de Web Services de messagerie.

Service	Description	URL
Services d'authentification		
Authentification par CPS	Authentification préalable par CPS au service de messagerie.	https://mss-idp-igcsante.formation.mssante.fr/openam/SSOSoap/metaAlias/asip/idp
Authentification par identifiant / mot de passe / OTP	Authentification préalable par identifiant / mot de passe / OTP au service de messagerie.	https://mss-idp-igcsante.formation.mssante.fr/openam/SSOSoap/metaAlias/asip/idp
Services de consultation et gestion des dossiers		
listFolders	Récupérer la liste détaillée de tous les dossiers existants, ou une liste détaillée des sous-dossiers d'un dossier spécifique.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/listFolder

Service	Description	URL
createFolder	Créer un nouveau dossier pour y ranger des messages.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/createFolder
deleteFolder	Supprimer un dossier, ainsi que tous les messages et tous les sous-dossiers dans ce dossier. Cette suppression est définitive (ce n'est pas une suppression dans la corbeille comme la méthode Trash).	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/deleteFolder
emptyFolder	Vider tous les messages et tous les sous-dossiers d'un dossier spécifique.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/emptyFolder
trashFolder	Déplacer un dossier et ses sous-dossiers vers la corbeille, marquant tous les contenus comme lus et le renommer si un dossier portant ce nom est déjà existant dans la corbeille.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/trashFolder
renameFolder	Changer le nom d'un dossier existant.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/renameFolder
moveFolder	Déplacer un dossier.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Folder/soap/v1/moveFolder
Services envoi et gestion de messages		
updateMessages	Mettre à jour une liste de messages.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/updateMessages
draftMessage	Enregistrer un message comme un brouillon avec ses pièces jointes.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/draftMessage
moveMessages	Déplacer une liste de message vers un autre dossier.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/moveMessages

Service	Description	URL
sendMessage	Envoyer un message avec ses pièces jointes.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/sendMessage
syncMessages	Obtenir les éléments à synchroniser avec le serveur.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/syncMessages
Services envoi et consultation des pièces jointes		
uploadAttachment	Envoyer une pièce jointe vers le serveur. Ce service est appelé dans le cadre d'un envoi de message ou d'un enregistrement de brouillon avec pièce jointe.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Attachment/soap/v1/uploadAttachment
removeAttachment	Supprimer une pièce jointe du serveur.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/Attachment/soap/v1/removeAttachment
downloadAttachment	Télécharger une pièce jointe d'un message étant donné l'ID du message et le numéro de la pièce jointe à télécharger.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Attachment/soap/v1/downloadAttachment
Services consultation et recherche de messages		
searchMessages	Recherche multicritères de messages.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/searchMessages
fullTextSearchMessages	Rechercher des messages sur l'objet, les destinataires, les destinataires en copie et l'expéditeur à partir d'un champ texte libre.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Item/soap/v1/fullTextSearchMessages
Services recherche de BAL		
listEmails	Récupérer la liste des adresses de messagerie valides et actives associées à un compte.	https://mss-msg-igcsante.formation.mssante.fr/mss-msg-services-igcsante/services/Annuaire/soap/v1/listEmails

Tableau 60 : URL des services de l'opérateur Mailiz en test

Les URLs mentionnées ci-dessus pour l'environnement de tests sont accessibles via le port standard 443. A compter de la date de publication du présent document, les ports 444 et 445,

spécifiés dans la précédente version du DST, seront maintenus un certain temps pour assurer la transition.

8.3.3 Les clients de messagerie de tests de l'opérateur Mailiz

8.3.3.1 Application mobile MSSanté de tests de l'opérateur Mailiz

L'application mobile de l'opérateur Mailiz (voir le paragraphe 8.1.2.1 ci-dessus) est disponible sur l'environnement de tests.
Cette application de tests permet aux titulaires d'un compte MSSanté de tests sur l'environnement de tests de l'opérateur Mailiz d'accéder à toutes les fonctionnalités de la messagerie et à l'Annuaire santé de tests.
Des informations complémentaires sont disponibles à l'adresse suivante, une fois authentifié : https://www.formation.mssante.fr/.

8.3.3.2 Thunderbird, logiciel de messagerie compatible avec le service MSSanté de l'opérateur Mailiz sur l'environnement de tests

Thunderbird peut être configuré pour fonctionner sur l'environnement de tests de l'opérateur Mailiz. Il est accessible aux titulaires d'un compte MSSanté de tests sur l'environnement de tests de l'opérateur Mailiz.
Des informations complémentaires sont disponibles à l'adresse suivante, une fois authentifié : https://www.formation.mssante.fr/.

8.3.4 Niveau de service

Le niveau de service (SLA) assuré par l'ANS pour cet environnement de test / formation est :

- Environnement accessible en 24/7 sans engagement de disponibilité et avec prise en compte des signalements d'incidents (voir 8.5 Canaux de contact) des éditeurs de 9H00 à 18H00, hors weekends et jours fériés ;
- Cet environnement peut être redémarré sans préavis (dans la mesure du possible les plages d'indisponibilité seront communiquées au préalable) ;

Pour les **demandes d'assistance technique auprès de l'opérateur Mailiz** (voir 8.5 Canaux de contact), les éléments à communiquer sont les suivants :

- La transaction testée (SMTPS/IMAPS, WS, Webmail…) et le mode d'authentification,
- Les requêtes complètes entrantes et réponse du serveur vues depuis le client de messagerie (sous forme de 2 fichiers XML (cas des WS) transmis en pièce jointe),
- L'environnement utilisé (tests/formation ou production),
- La version du DST.

8.4 L'Annuaire santé de tests (dit "partenaires")

Service	Paramètres
LDAP Annuaire santé de test	Nom DNS de l'Annuaire santé de tests : partenaires.annuaire.sante.fr URL d'accès : ldap://partenaires.annuaire.sante.fr Port : 389 Base DN au moins égale à «ou=bal,o=mssante,c=fr »

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

8.5 Canaux de contact

Pour les demandes d'assistance et signalements d'incidents des éditeurs de clients de messagerie et des opérateurs compatibles au DST, deux canaux de contact sont disponibles :

- Email : monserviceclient.mssante@asipsante.fr,
- Téléphone : 0 825 852 000 (8h à 20h du lundi au vendredi et de 8h à 14h le samedi – Service à 6 cts/min + prix d'un appel local).

Les demandes d'inscriptions à la liste de diffusion pour être informé des actualités de l'espace de confiance MSSanté se font via ces canaux également.

8.6 WSDL des services MSSanté

Ils sont téléchargeables sur le site :

https://www.mssante.fr/is/doc-technique

WSDL des services MSSanté	
DR1_FolderService	**FolderService.wsdl** : WSDL des services de consultation et gestion des dossiers
DR2_ItemService	**ItemService.wsdl** : WSDL des services envoi et gestion de messages & des services consultation et recherche de messages
DR3_AttachmentService	**AttachmentService.wsdl** : WSDL des services envoi et consultation des pièces jointes
DR4_AnnuaireService	**AnnuaireService.wsdl** : WSDL du service de recherche de BAL correspondant à un Professionnel de Santé

Tableau 61 : Liste des documents de référence pour les services

8.7 Code exemple / exemples de messages SOAP

Du code exemple et des exemples de messages et trames SOAP d'échange avec le service de messagerie MSSanté sont mis à disposition par l'ANS à titre indicatif.

Ils sont téléchargeables sur le site :

https://www.mssante.fr/is/doc-technique

Attention :

- Les code exemples et les exemples et les trames SOAP ne constituent ni une référence, ni une spécification ;

- certaines trames ont été volontairement reformatées (XML indenté) pour plus de lisibilité ;

- la cohérence fonctionnelle des valeurs d'exemples renseignées n'est pas garantie : l'éditeur devra s'assurer que les valeurs produites dans les champs des messages correspondent bien à un cas fonctionnel possible ;

- les valeurs de signatures peuvent être non significatives (trames reformatées) ;

- les balises XML vides dans les requêtes SOAP ne sont pas gérées par les Web Services.

8.8 Terminologie et acronymes

Ce paragraphe 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
ANS	Agence du Numérique en Santé
BAL	Boîte aux lettres
CI-SIS	Cadre d'interopérabilité des Systèmes d'Information de Santé de l'ANS
CNIL	Commission Nationale de l'Informatique et des Libertés
CPS	Carte de Professionnel de Santé
CRL	Certificate Revocation List
DIT	Directory Information Tree
DMP	Dossier Médical Personnel
DN	Distinguished Name
DNS	Domain Name Server
DST	Dossier des Spécifications Techniques
DSFT	Dossier des Spécifications Fonctionnelles et Techniques
DSML	Directory Service Markup Language
ES	Etablissement de Santé : terme recouvrant les établissements de soins publics et privés, incluant les plateaux techniques en ville et en hôpital
IETF	Internet Engineering Task Force
IGC	Infrastructure de Gestion de Clés
IMAP	Internet Mail Access Protocol
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
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
NAS	Nomenclature des Acteurs de Santé
OCSP	Online Certifcate Status Protocol
OTP	One Time Password
PS	Professionnel de Santé - Acteur de Santé humain
RASS	Référentiel des Acteurs Sanitaires et Sociaux
REST	Representational State Transfer
RFC	Request For comments - 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
SMTP	Simple Mail Transport Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security - Norme de sécurisation par chiffrement du transport de l'information au sein des réseaux (anciennement SSL)
TM	Transaction MSSanté
WSDL	Web Services Description Language
RPPS	Répertoire Partagé des Professionnels de Santé

Tableau 62 : Liste des acronymes et de leurs significations

8.9 Documents externes

8.9.1 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'ANS 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'ANS 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**
Autres documents **(Documents accessibles sur le site MSSanté https://www.mssante.fr/is/doc-technique)**		
DA6	[DSFT-MSSANTE]	**Dossier des Spécifications Fonctionnelles et Techniques des Interfaces d'accès au système de Messageries Sécurisées de Santé (MSSanté)**
DA7	[CONTRAT-MSSANTE]	**Contrat « opérateur MSSanté » et ses deux annexes**
DA8	[WSDL-MSSANTE]	**WSDL des services MSSanté**
DA9	[CODE-EX-C#]	**Code exemple WS en langage C#**
DA10	[MOBILITE-MSSANTE]	**Présentation générale des procédures d'enrôlement et d'authentification mises en œuvre par l'opérateur Mailiz pour l'application MSSanté pour terminaux mobiles**
DA11	[ECHANGES-STRUCTURES-MSSANTE]	**Guide sur l'échange de documents de santé structurés par la MSSanté**
Documents de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) **(Documents accessibles sur le site de l'ANS http://esante.gouv.fr/services/politique-generale-de-securite-des-systemes-d-information-de-sante-pgssi-s)**		
DA12	[PG-AUTH]	**Référentiel d'authentification des acteurs de santé**– Décembre 2014 - V2.0
DA13	[PG-IMPUT]	**Référentiel d'imputabilité**– Décembre 2014 – V1.0

DA14	[PG-GR-APPLI]	**Grille d'applicabilité des référentiels de la PGSSI-S**– Mai 2015 – V1.0
Bonne pratique pour la récupération des CRL (**Document accessible sur le site https://tech.esante.gouv.fr/ ou http://esante.gouv.fr)**		
DA16	[PSCE-GUIDE-CRL]	**ANS_Guide_de_bonnes_pratiques_de_verification_de_l%27etat_des_certificats_201707_v3.0.1.pdf**
DA17	[PSCE-CDE-PM]	**Commande de certificats de personne morale pour le DMP - Procédure pour les structures libérales (hors laboratoires de biologie médicale)**
DA18	[PSCE-CDE-TEST]	**Cabinets de radiologie RPPS rang -Fiche pratique pour commander des cartes et certificats ORG de test**

Tableau 63 : Liste des documents applicables

8.9.2 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

8.9.3 Annexes externes

Documentation IETF (spécification internationale en libre accès sur http://www.ietf.org/)		
DX1	MSS-ANX-CRL1	**Internet X.509 Public Key Infrastructure** Certificate and Certificate Revocation List (CRL) Profile http://tools.ietf.org/html/rfc5280
DX2	MSS-SMTP1	**Simple Mail Transfer Protocol** http://tools.ietf.org/html/rfc5321
DX3	MSS-SMTP2	**SMTP Service Extension for** Returning Enhanced Error Codes http://www.ietf.org/rfc/rfc2034.txt
DX4	MSS-ANX-SMTPS	**SMTP Service Extension for** Secure SMTP over Transport Layer Security http://www.ietf.org/rfc/rfc3207.txt
DX5	MSS-ANX-TLS1	**Using TLS with IMAP, POP3 and ACAP** http://www.ietf.org/rfc/rfc2595.txt
DX6	MSS-ANX-TLS2	**The TLS Protocol Version 1.0** http://tools.ietf.org/html/rfc2246
DX7	MSS-ANX-LDAP1	**Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map** http://tools.ietf.org/html/rfc4510
DX8	MSS-ANX-LDAP2	**Lightweight Directory Access Protocol (LDAP): The Protocol** http://tools.ietf.org/html/rfc4511
DX9	MSS-ANX-LDAP3	**Lightweight Directory Access Protocol (LDAP): Directory Information Models** http://tools.ietf.org/html/rfc4512
DX10	MSS-ANX-LDAP4	**Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms** http://tools.ietf.org/html/rfc4513
DX11	MSS-ANX-IMAP	**Internet Message 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

Documentation IETF (spécification internationale en libre accès sur http://www.ietf.org/)		
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-MIME6	**The Model Primary Content Type for Multipurpose Internet Mail Extensions** http://tools.ietf.org/html/rfc2077
DX22	MSS-ANX-MIME7	**Multipurpose Internet Mail Extension (MIME) Part Five : Conformance Criteria and Examples** http://tools.ietf.org/html/rfc2049
DX23	MSS-ANX-MAIL2	**Standard for ARPA Internet Text Messages** http://www.w3.org/Protocols/rfc822
DX24	MSS-ANX-OCSP	**X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP** http://tools.ietf.org/html/rfc2560
DX25	MSS-ANX-MAIL3	**Internet Message Format** http://tools.ietf.org/html/rfc2822
DX26	MSS-ANX-MAIL4	**MAIL ROUTING AND THE DOMAIN SYSTEM** http://tools.ietf.org/html/rfc974
DX27	MSS-ANX-MAIL5	**Classless IN-ADDR.ARPA delegation** http://tools.ietf.org/html/rfc2317

Tableau 64 : Liste des annexes externes IETF

8.10 Standards et protocoles utilisés

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

[6] 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 autres que celui de l'ASCII, ainsi que des contenus non textuels (pièces-jointes). Les messages électroniques sont souvent appelés messages SMTP/MIME (infra ou supra désigné par SMTP).

8.11 Définitions communes à plusieurs transactions Web Services

8.11.1 Les types

Remarque : les champs de type booléen doivent obligatoirement être remplis avec l'une des valeurs conformes (true, false, 1 ou 0). Toute autre valeur entraîne une mauvaise interprétation du champ.

Type : EmailAuthent			
Elément	**Type**	**Card.**	**Description**
email	STRING(256)	1	Respecte l'expression régulière : ^[a-z0-9!#$%&'*+/=?^_`{\|}~-]+(?:\\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*@(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-9])? Attention : l'adresse de messagerie est obligatoirement en minuscules.

Tableau 65

Type : MessageToSend			
Elément	**Type**	**Card.**	**Description**
messageId	**INT**	0..1	ID du message à renseigner uniquement dans le cas de l'envoi d'un brouillon.
addresses	**Address**	0..*	Liste des adresses de messagerie (la liste peut être vide).
subject	STRING(250)	0..1	Sujet du message en UTF-8.
replyType	**EnumReplyType**	0..1	Type de renvoi.
priority	**EnumPriority**	0..1	Priorité du message : NORMAL ou HAUTE. Si non renseigné, la priorité sera considérée comme NORMAL.
isHtml	BOOLEAN	0..1	Si non renseigné ou false, le format du message est TEXT, sinon (si true) le format du message est HTML.
isAccuse	BOOLEAN	0..1	Si un accusé de lecture est souhaité, positionner ce booléen à « true ».
messageTransferedId	INT	0…1	ID de message transféré.
DispositionNotificationTo	STRING	0..1	Facultatif. Lors de la constitution d'un message, le système initiateur peut demander de manière optionnelle au système cible d'envoyer une réponse applicative. Le système cible rapporte alors les résultats de l'importation au système initiateur. Se reporter au volet Echange de documents de Santé du CI-SIS [CI-ECH-DOC]. Remarque : il n'est pas implémenté par les versions actuelles des web-services de messagerie de l'opérateur MSSanté, et ne peut donc pas être positionné. Il est néanmoins bien géré nativement par les interfaces SMTPS / IMAPS. Il doit respecter l'expression régulière : ^[a-z0-9!#$%&'*+/=?^_`{\|}~-]+(?:\\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*@(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-9])?
body	STRING La taille max dépend du serveur de messagerie	0..1	Corps du message en UTF-8. A encapsuler par **<![CDATA[…]]>** si contenu html.
attachments	**AttachmentToSend**	0..*	Liste des pièces jointes.

Tableau 66

Type : Address			
Elément	**Type**	**Card.**	**Description**
email	STRING(256)	1	Adresse de messagerie de la personne
type	**EnumTypeMail**	1	Type d'adresse de messagerie.
name	STRING	0..1	Nom de la personne associée à l'email en UTF-8

Tableau 67

Type : AttachmentToSend			
Elément	**Type**	**Card.**	**Description**
part	INT	0..1	Numéro de la pièce jointe. Ce numéro est renseigné uniquement si la pièce jointe était déjà rattachée à un message (brouillon en cours ou message transféré). Ce numéro ne commence pas forcément à 1 si par exemple une des pièces jointes du brouillon a été supprimée avant le réenregistrement.
contentType	STRING(40)	0..1	Type de fichier (cf. RFC 2045, 2045 à 2048).
fileName	STRING La taille max dépend du serveur de messagerie	0..1	Nom de fichier en UTF-8.
file	base64Binary	0..1	Contenu du fichier à uploader en UTF-8. Ce champ n'est pas à renseigner si part est renseigné. En effet, file est renseigné uniquement si c'est une nouvelle pièce jointe qui n'était pas déjà enregistrée sur le brouillon
messageId	INT	0..1	Identifiant du message lié au part (dans le cas du transfert de pièce jointe) Identifiant du brouillon dans le cas du réenregistrement d'un brouillon où on garde une des pièces jointes.

Tableau 68

Règle : Il y a deux façons d'utiliser le type **AttachmentToSend** :

- La première, pour envoyer une nouvelle pièce jointe, consiste à indiquer *contentType, fileName* ainsi que *file*. Les autres champs ne sont pas à préciser.
- La seconde manière d'utiliser ce type consiste à réutiliser une pièce jointe déjà insérée dans un autre message ou brouillon. Dans ce cas, on renseignera uniquement *part* et *messageId*.

Type : MessageValidate			
Elément	**Type**	**Card.**	**Description**
messageId	INT	1	ID du message.
date	STRING(19)	1	Date de réception du message. Date sous la forme « dd/MM/yyyy HH :mm :ss »
size	LONG	1	Taille du message en octets (comprenant les pièces jointes)
attachments	**attachmentValidate**	0..*	Liste des pièces jointes.

Tableau 69

Type : attachmentValidate			
Elément	**Type**	**Card.**	**Description**
part	INT	0..1	Numéro de la pièce jointe. Ce numéro est renseigné uniquement si la pièce jointe était déjà rattachée à un message (brouillon en cours ou message transféré). Ce numéro ne commence pas forcément à 1 si par exemple une des pièces jointes du brouillon a été supprimée avant le réenregistrement.
contentType	STRING(40)	0..1	Type de fichier (cf. RFC 2045, 2045 à 2048).
fileName	STRING La taille max dépend du serveur de messagerie	0..1	Nom de fichier en UTF-8.
messageId	INT	0..1	Identifiant du message lié au part (dans le cas du transfert de pièce jointe) Identifiant du brouillon dans le cas du réenregistrement d'un brouillon où on garde une des pièces jointes.
size	LONG	0..1	Taille en octets de la pièce jointe

Tableau 70

Type : Message			
Elément	**Type**	**Card.**	**Description**
messageId	INT	1	ID du message.
date	STRING(19)	1	Date de réception (ou d'envoi si le message est de type Envoyé) du message. Date au format « dd/MM/yyyy HH:mm:ss ».
size	LONG	1	Taille du message en octets (comprenant les pièces jointes).
flags	**enumFlag**	0…*	Flags associés au message.
folderId	INT	1	ID du dossier.
origId	INT	0..1	Identifiant du message d'origine
addresses	**Address**	0..*	Liste des adresses de messagerie.
isBodyLarger	BOOLEAN	0..1	Si ce champ est à « true » c'est que le contenu du message est trop volumineux (> 50 000 caractères). Le contenu du message a donc été tronqué à 50 000 caractères.
subject	STRING(250)	1	Sujet du message en UTF-8.
fragment	STRING	0…1	Fragment du contenu de message (à afficher lors du détail du message dans la liste de message) en UTF-8.
body	STRING	0…1	Corps du message en UTF-8.
attachments	**Attachment**	0..*	Liste des pièces jointes.

Tableau 71

Type : **Attachment**			
Elément	**Type**	**Card.**	**Description**
part	INT	0..1	Numéro de la pièce jointe. Ce numéro est renseigné uniquement si la pièce jointe était déjà rattachée à un message (brouillon en cours ou message transféré). Ce numéro ne commence pas forcément à 1 si par exemple une des pièces jointes du brouillon a été supprimée avant le réenregistrement.
contentType	STRING(40)	1	Type de fichier (cf. RFC 2045, 2045 à 2048).
fileName	STRING La taille max dépend du serveur de messagerie	1	Nom de fichier en UTF-8.
file	base64Binary	0..1	Contenu du fichier à uploader en UTF-8. Ce champ n'est pas à renseigner si part est renseigné. En effet, file est renseigné uniquement si c'est une nouvelle pièce jointe qui n'était pas déjà enregistrée sur le brouillon
messageId	INT	0..1	Identifiant du message lié au part (dans le cas du transfert de pièce jointe) Identifiant du brouillon dans le cas du réenregistrement d'un brouillon où on garde une des pièces jointes.
size	LONG	0..1	Taille de la pièce jointe. Ce champ ne doit pas être envoyé, il sert uniquement en retour de transaction.

Tableau 72

8.11.2 Les énumérations

EnumOperation : STRING
DELETE
READ
UNREAD
FLAGGED
UNFLAGGED
SPAM
UNSPAM
TRASH

Tableau 73

EnumTypeMail : STRING
FROM
TO
CC
BCC

Tableau 74

EnumReplyType : STRING
REPLIED
FORWARDED

Tableau 75

EnumPriority : STRING
NORMAL
HAUTE

Tableau 76

EnumFlag : string
UNREAD
FLAGGED
ATTACHMENT
REPLIED
SENT_BY_ME
DELETED
DRAFT
FORWARDED
URGENT
LOW_PRIORITY
PRIORITY

Tableau 77

EnumSort : string
sizeAsc
dateDesc
subjAsc
subjDesc
nameAsc
nameDesc
rcptAsc
rcptDesc
attachAsc
attachDesc
flagAsc
flagDesc
priorityAsc
priorityDesc
sizeAsc
sizeDesc

Tableau 78