PROJETS / SERVICES

Interfaces d'accès au système

de Messageries Sécurisées de Santé (MSSanté)

Dossier des Spécifications Techniques - **V0.9.5** - Février 2014

Clients de messagerie

Identification du document	
Référence ASIP Santé	**MSS_FON_DST_ interfaces_Clients_MSSanté_v0.9.5.PDF**
Date de dernière mise à jour	**14/02/2014**
Classification	**Non sensible public**
Nombre de pages	**95**

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

Sommaire

1 Introduction

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

- L'envoi, par une personne certifiée et habilitée, d'un message pouvant contenir des données de santé à caractère personnel, à l'initiative d'un émetteur (ou entité émettrice) et pour un destinataire (ou entité destinataire) ;
- La consultation, par une personne certifiée et habilitée, d'un message reçu pouvant contenir des données de santé à caractère personnel.

Le service d'échange attendu des acteurs fonctionne de manière asynchrone : l'entité destinataire peut récupérer un message à sa propre initiative, dans un laps de temps plus ou moins long après qu'il ait été émis.

Le système MSSanté est un espace de confiance que de nombreux opérateurs de messageries pour les acteurs du monde de la santé ont vocation à intégrer. 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]).

En sa qualité d'opérateur d'un des services de messagerie sécurisée de santé, l'ASIP Santé publie aussi le présent Dossier de Spécifications Techniques (DST), 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 ASIP Santé. Les autres opérateurs peuvent aussi implémenter ces spécifications afin de faciliter l'interfaçage des clients de messagerie à leur propre service MSSanté.

Note :

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

- Relever et envoyer des courriers électroniques pour une BAL MSSanté ;
- Pouvoir réaliser la recherche de boîtes aux lettres (BAL) dans l'annuaire national MSSanté.

1.1 Objet du document

Lorsque l'utilisateur du service de messagerie proposé **par l'opérateur ASIP Santé** souhaite accéder à sa boîte aux lettres en dehors d'un simple accès en Webmail, il doit utiliser un client de messagerie conforme aux présentes spécifications techniques.

L'objectif de ce document est donc de décrire en détail les principes et les spécifications techniques permettant d'interfacer un client de messagerie avec le service de messagerie proposé par l'opérateur ASIP Santé.

Ces spécifications techniques ne s'imposent pas aux autres 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 du DST publié par l'ASIP Santé pour faciliter l'interfaçage des clients de messagerie du marché avec leur service, car les protocoles utilisés sont connus et largement répandus.

Les interfaces techniques proposées dans ce document reposent sur deux solutions libres de droits recourant :

- Soit à des protocoles d'accès standards IMAP et SMTP sur TLS ;

- Soit à des protocoles d'accès conformes aux Web Services définis dans le présent document.

Remarque : les opérateurs et éditeurs sont libres de mettre en œuvre ces protocoles 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.

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

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

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

1.2.1 Rôle du client de messagerie MSSanté

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

- De réaliser les tâches de messagerie classiques (envoyer, recevoir et stocker des courriers électroniques) ;
- De permettre la recherche de PS dans l'annuaire national MSSanté.

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.

Accès au service par les protocoles classiques de messagerie

Le « socle de base », pour les accès par les protocoles de messagerie standards, repose sur la mise en place d'une session TLS avec authentification mutuelle par carte CPS préalablement aux échanges par les protocoles standards de messagerie SMTP avec extension STARTTLS (port TCP/587) et IMAP4 avec extension STARTTLS (port TCP/143).

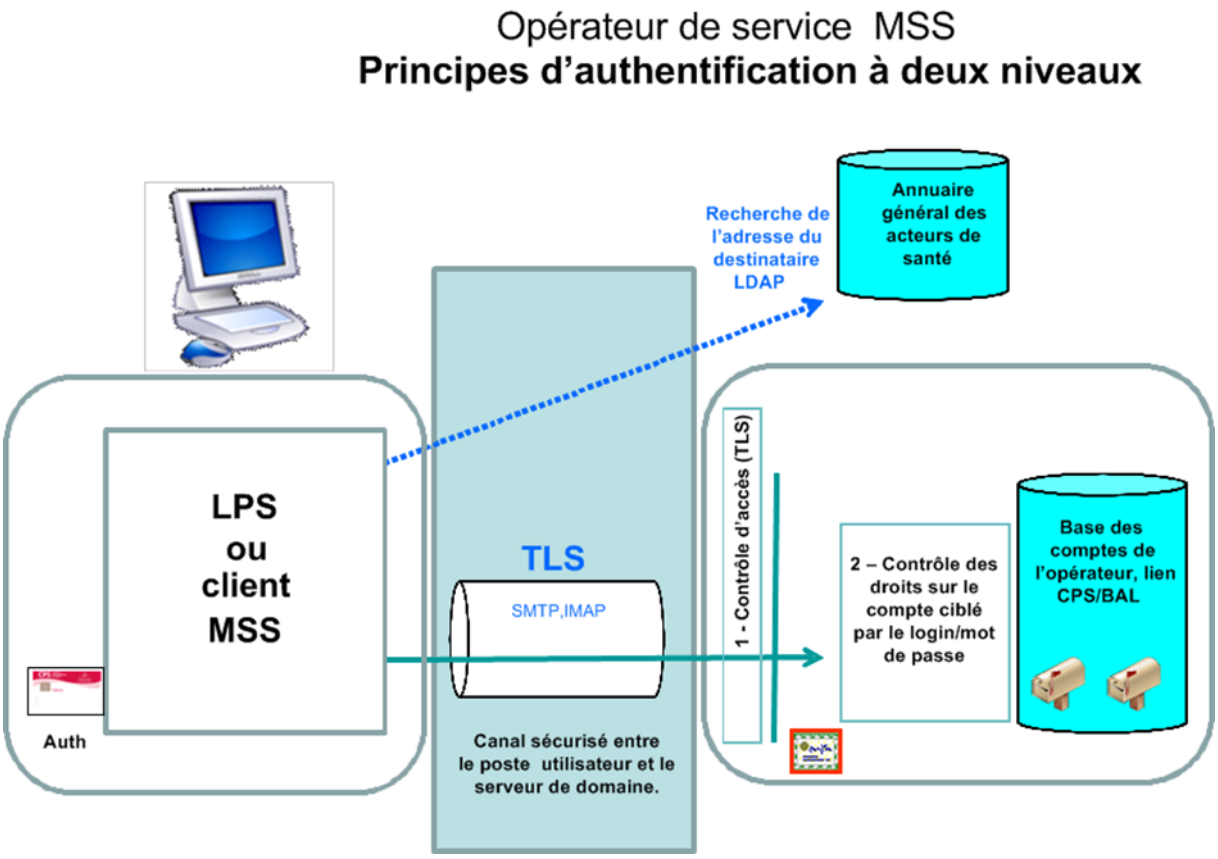

Figure 1 : Principes d'authentification entre un LPS et un opérateur de service MSSanté selon un protocole standard de messagerie

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

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

Accès au service par Web Services

L'accès aux fonctions de messagerie peut également se faire via des Web Services définis dans ce document. Ces Web Services offrent des fonctions équivalentes à celles offertes par les protocoles classiques de messagerie.

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

Pour le service de l'opérateur ASIP Santé, l'obtention de ce jeton se base soit sur une authentification par carte CPS, soit sur un mécanisme d'authentification équivalent par identifiant, pot de passe et code d'accès à usage unique (*One Time Password* – OTP) qui nécessite un enrôlement préalable de l'utilisateur sur le Webmail de l'opérateur ASIP Santé.

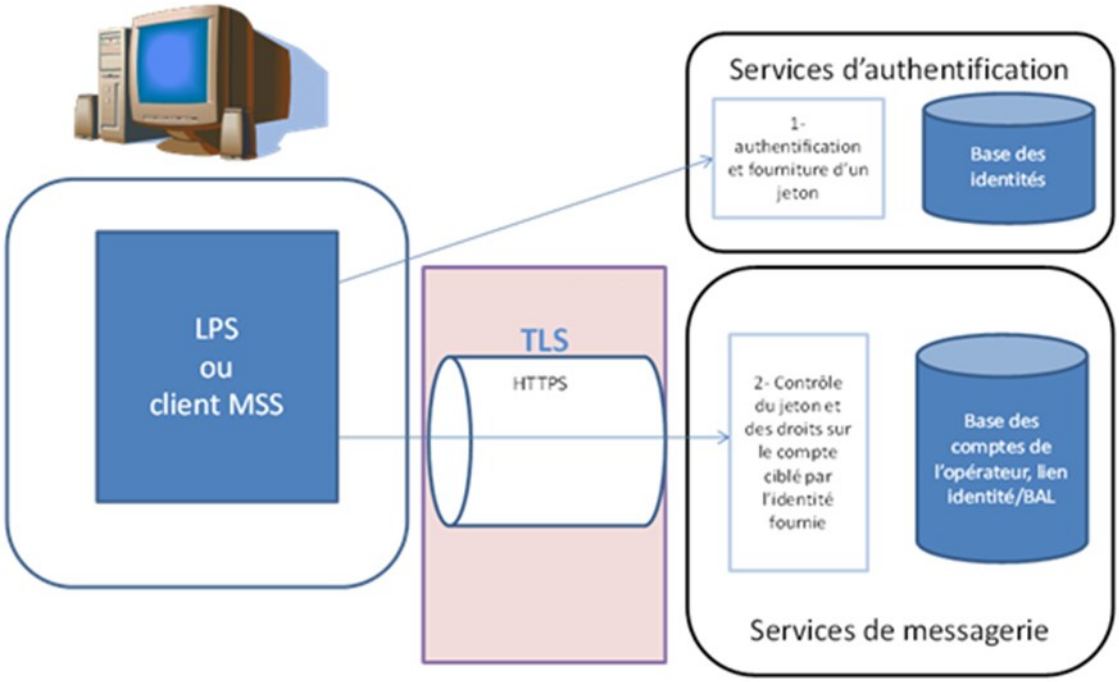

Figure 2 : Principes d'authentification entre un LPS et un opérateur de service MSSanté exposant des Web Services de messagerie

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

En dehors de l'authentification CPS, l'accès aux Web Service de messagerie se fait sur HTTPS, avec l'établissement d'une connexion TLS avec authentification asymétrique, permettant d'assurer la confidentialité des échanges et la vérification, par le client de messagerie, du certificat présenté par le serveur.

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

1.2.2 Interopérabilité des échanges de données de santé structurées

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

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

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

Pour les messages ne contenant que des pièces jointes au format bureautique, il est vivement recommandé de ne pas permettre à un utilisateur du client de messagerie émetteur de joindre dans un même message des documents de plusieurs patients. La bonne pratique est donc qu'un message ne concerne qu'un seul patient.

1.2.3 Implémentation des interfaces de messagerie au sein des LPS

Le choix d'implémenter les interfaces de messagerie décrites dans ce dossier de spécifications techniques est laissé à la libre appréciation des éditeurs de ce type de solution ainsi qu'aux opérateurs MSSanté.

Le respect des présentes spécifications n'est encadré par aucun processus de vérification ou de contrôle de l'ASIP Santé, compte tenu du caractère standard des procédés techniques à mettre en œuvre par les éditeurs.

1.3 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]), disponible sur le site internet de l'ASIP Santé. 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 de spécifications techniques (DST) est destiné principalement aux profils techniques des éditeurs de Clients de messagerie MSSanté.

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

- Le chapitre 2 expose les prérequis et les recommandations pour l'intégration de MSSanté dans les clients de messagerie ;
- Le chapitre 3 décrit les transactions standards MSSanté pouvant être implémentées dans un client de messagerie ;
- Le chapitre 4 décrit les interfaces de messagerie basées sur les échanges en IMAPS et SMTPS ;
- Le chapitre 5 décrit les interfaces de messagerie basées sur des Web Services de messagerie ;
- Le chapitre 6 décrit la consultation de l'annuaire national MSSanté selon le protocole LDAP ;
- Le chapitre 7 décrit la consultation de l'annuaire national MSSanté par Web Service ;
- Le chapitre 8 regroupe les annexes.

Le tableau de l'annexe au **§ 8.1** « Documents externes» récapitule les principaux documents applicables. Dans l'ensemble du document, ils sont désignés par le code apparaissant dans la colonne « Référence » du tableau de l'annexe.

L'annexe « Terminologie et acronymes » du **§ 8.3** référence et définit l'ensemble des acronymes utilisés dans ce document.

1.4 Gestion des versions successives

Le DST 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.

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

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.

Il est possible d'être automatiquement informé des dernières mises à jour de ce dossier en s'abonnant à la liste de diffusion MSSanté Compatibilité : msscompatibilite@sante.gouv.fr.

2 Recommandations

2.1 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 ou un Proxy 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.

2.2 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. Les données de santé personnelles ne doivent être envoyées que dans le cadre de l'utilisation d'une messagerie sécurisée de santé. 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.

3 Présentation des transactions « standards » MSSanté

Le présent chapitre décrit les transactions « standards » MSSanté[1] pouvant être intégrées dans un client de messagerie :

- Les transactions de messagerie basées sur les protocoles standards de messagerie (SMTPS et IMAPS) ;
- Les transactions de messagerie basées sur les Web Services définis dans ce document pour le service de messagerie MSSanté (mais pouvant être implémentés par tout opérateur de messagerie s'il le souhaite) ;
- La transaction de consultation de l'annuaire national MSSanté par le protocole LDAP ;
- La transaction de consultation de l'annuaire national MSSanté par Web Service.

Les clients de messagerie concernés par le présent document sont ceux utilisant des BAL hébergées par tout opérateur MSSanté ayant mis en œuvre les transactions définies dans le présent DST, dont l'Opérateur ASIP Santé.

Les spécifications détaillées de ces transactions MSSanté sont décrites aux chapitres 4 à 7 du présent document.

Un opérateur de messagerie MSSanté peut implémenter l'une, l'autre ou aucune de ces transactions « standards ». Il peut aussi proposer des modes d'accès spécifiques aux BAL MSSanté qu'il héberge (Webmail, client de messagerie propriétaire, interfaces ouvertes selon des protocoles propriétaires).

L'information concernant le type d'interfaces mises à disposition par les opérateurs de messagerie MSSanté est disponible sur le site internet de l'ASIP Santé. L'opérateur ASIP Santé propose toutes les transactions « standards » décrites dans ce document.

Un client de messagerie souhaitant s'interfacer avec un opérateur donné doit mettre en œuvre les transactions compatibles avec celles proposées par cet opérateur. Concernant les BAL MSSanté hébergées par l'opérateur ASIP Santé, le client de messagerie peut donc implémenter les transactions « standards » qu'il souhaite.

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

Transactions « standards » MSSanté pour les clients de messagerie		Description de la transaction
Annuaire		
TM2.1.1C	Consultation de l'annuaire national MSSanté en LDAP	Recherche multicritères de correspondants dans l'annuaire national MSSanté par le protocole LDAP
TM2.1.2C	Consultation de l'annuaire national MSSanté en Web Service	Recherche multicritères de correspondants dans l'annuaire national MSSanté par Web Service
Emission et réception de messages sur les protocoles standards de messagerie		
TM3.1C	Gestion des messages de la BAL MSSanté par IMAPS	Consultation et gestion des messages MSSanté et des dossiers de classement sous le protocole IMAPS
TM3.2C	Emission de messages par SMTPS	Emission de messages sous le protocole SMTPS
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 sur un service MSSanté par carte CPS	Gestion de l'authentification préalable à l'appel des Web Services MSSanté
TM4.1.2C	Authentification sur un service MSSanté par identifiant/mot de passe/OTP	Gestion de l'authentification préalable à l'appel des Web Services MSSanté
TM4.1.3C	Filtre de contrôle d'accès aux Web Services	Validation du jeton d'authentification fourni dans la requête lors de l'appel du service
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 de 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

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

3.1 La sécurisation des échanges

3.1.1 Les moyens d'authentification d'accès

L'accès à ces interfaces nécessite l'utilisation d'une authentification forte de l'utilisateur :

- Pour les transactions utilisant les protocoles SMTPS et IMAPS, le seul moyen d'authentification possible est la carte CPS ;
- Pour les Web Services de messagerie, d'autres moyens d'authentification peuvent être utilisés 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 concerné : le mécanisme d'authentification est donc distinct des Web Services de messagerie.

Pour l'accès par Web Service, les mécanismes d'authentification proposés dans cette version par l'opérateur ASIP Santé sont les suivants :

- Carte CPS ;
- Identifiant/ mot de passe/ OTP (SMS ou mail) ; dans le cas du service de messagerie mis en œuvre par l'ASIP Santé, ce deuxième moyen s'adosse à la carte CPS et ne peut être mis en œuvre qu'une fois la BAL créée (l'opération d'autocréation de BAL nécessitant une authentification par carte CPS).

Ces mécanismes d'authentification sont décrits dans ce document, afin de permettre une compatibilité des clients MSSanté avec tout opérateur de messagerie qui les met en œuvre.

Les opérateurs de messagerie sont libres d'utiliser les Web Services MSSanté, tout en offrant des modes 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).

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.

3.1.2 Etablissement d'un 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).

3.1.2.1 Pour les transactions de messagerie basées sur les protocoles standards de messagerie (SMTPS et IMAPS)

La connexion à un service MSSanté depuis un client utilisant les protocoles standards de messagerie (SMTPS, IMAPS) est assurée par l'établissement d'un **canal TLS avec authentification mutuelle** entre le client de messagerie et le serveur de l'opérateur MSSanté.

Côté client de messagerie, l'établissement de ce canal TLS nécessite l'utilisation de la carte CPS.

Les protocoles SMTPS et IMAPS permettent d'assurer l'identification et l'authentification réciproque du client et des serveurs et d'assurer la confidentialité des échanges.

3.1.2.2 Pour les transactions de messagerie basées sur les Web Services MSSanté

La connexion à un service MSSanté depuis un client utilisant les Web Services de messagerie définis dans le présent document est assurée par l'établissement d'un **canal TLS** entre le client de messagerie et le serveur de l'opérateur MSSanté.

Côté client de messagerie, **l'authentification** peut être réalisée :

- Avec une carte CPS (établissement d'un canal TLS avec authentification mutuelle) ;
- Avec une solution alternative à la carte CPS (établissement d'un canal TLS asymétrique).

Les mécanismes d'obtention du jeton d'authentification auprès du service d'authentification de l'opérateur ASIP Santé sont décrits dans le §5.1 «TM4.1.xC - Authentification préalable pour les appels de Web Services ».

En dehors de l'authentification, **l'appel des Web Services de messagerie** est réalisé en TLS asymétrique quel que soit le mode d'authentification (CPS ou solution alternative) utilisé.

3.1.2.3 Bonnes pratiques pour l'accès à sa messagerie 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 ASIP Santé : « ASIP-PTS-PSCE_Guide-implementation-detection-arrachage-CPS_v1.0.3.pdf » disponible à l'adresse suivante : http://integrateurs-cps.asipsante.fr/documents/Guide-impl-arrachage-CPS (accès réservé aux titulaires d'un compte Editeurs CPS - pour les modalités de création d'un compte : http://integrateurs-cps.asipsante.fr/services-cps/contrat-editeurs-cps).

3.1.3 Vérification des certificats serveurs

3.1.3.1 Principe général

Le certificat serveur MSSanté des interfaces pour les clients de messagerie est émis par l'IGC-CPS. Des précisions sur le certificat utilisé par les serveurs des opérateurs MSSanté sont disponibles aux adresses suivantes : http://annuaire.asipsante.fr/ (onglet : « Informations ») et http://esante.gouv.fr/services/espace-cps/telechargement.

Gestion de plusieurs chaînes de certification

Il est recommandé que le client de messagerie soit en mesure de gérer plusieurs chaînes de certification afin de pouvoir prendre en compte, le cas échéant, de nouvelles offres de produits de certification.

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 la RFC 3501 (voir http://tools.ietf.org/html/rfc3501).

Certificats racine

Dans le cadre de l'IGC-CPS, l'ASIP Santé assure le rôle d'autorité de certification (AC).

Le certificat utilisé par le serveur de messagerie de l'opérateur ASIP Santé est un fils de l'AC nommée "AC-classe-4" elle-même fille de l'AC "GIP-CPS". Les ressources liées à ces deux AC sont donc nécessaires pour valider le certificat. Les fichiers (certificats) des AC "GIP-CPS" et "AC-classe-4" doivent être récupérés par l'intermédiaire du site http://annuaire.asipsante.fr/ (onglet : « Autorités de Certification »), et déployés avec le client de messagerie.

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 : pour effectuer ce contrôle, le simple téléchargement du certificat du serveur de messagerie de l'opérateur MSSanté constitue une mauvaise pratique : il est demandé de bien valider le certificat à l'aide de l'autorité émettrice AC-Classe-4 subordonnée à l'autorité racine GIP-CPS. En effet, l'ajout du certificat du serveur de l'opérateur MSSanté comme autorité de confiance dans le client de messagerie (ou dans le système d'exploitation) 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.

3.1.3.2 Bonnes pratiques pour la vérification des certificats serveurs

Contrôle de non révocation

L'ASIP Santé, en sa qualité d'autorité de certification ne dispose pas encore d'un service OCSP (Online Certificate Status Protocol). Cependant, les CRLs des certificats serveurs de classe 4 peuvent être téléchargées par le client (éventuellement par tâche planifiée : les CRLs « ASIP Santé » sont mises à jour en totalité une fois par jour mais des deltas CRLs existent néanmoins permettant ainsi d'optimiser la mise à jour des CRLs si besoin), puis utilisées de manière programmatique lors de la validation (en général en installant ou en passant en paramètre les CRLs dans le composant technique de validation de certificat).

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

La vérification de non révocation du certificat serveur de l'opérateur de messagerie constitue une bonne pratique en termes de sécurisation des échanges.

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

Pour assurer la sécurité des applications intégrant des certificats d'AC, il est recommandé de comparer l'empreinte numérique des certificats utilisés avec la source de confiance (http://integrateurs-cps.asipsante.fr/pages/Certificats-Racines-CPS).
La validation (comparaison de l'empreinte) peut être réalisée[2] :

- Automatiquement (dans la majorité des cas) par la librairie ou le composant logiciel de gestion des connexions TLS :
  - Ce contrôle est réalisé de base par les navigateurs du marché ;
  - Soit en passant ces fichiers en paramètre de ce composant lors de l'établissement de la connexion TLS (cas de librairies se basant sur OpenSSL par exemple) ;
  - Soit en intégrant ces fichiers dans un magasin de certificats (autorités de confiance) propre au composant de connexion (cas de Java par exemple) ;
  - Soit en intégrant ces fichiers dans le magasin des autorités de confiance de l'OS, utilisé par le composant (cas de Microsoft .Net par exemple).

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

- Manuellement, en comparant les empreintes ; pour les calculer :
    - Cette information est calculée automatiquement par la visionneuse de certificat Windows (onglet "Détail", "<tout>", dernière ligne) ;
    - En utilisant la commande "openssl X509 -fingerprint" sur le fichier certificat ;
    - En utilisant les commandes "sha1sum" ou "sha256sum" sur le certificat dans sa forme DER.

4 Transactions basées sur les protocoles standards de messagerie

4.1 TM3.1C – Gestion des messages de la BAL par IMAPS

Le client de messagerie permet à l'utilisateur, via le protocole IMAPS, 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 mutuelle avec le serveur IMAPS de l'opérateur MSSanté. Avec le protocole IMAP les messages et les dossiers peuvent être gérés directement sur le serveur.

4.1.1 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[3] 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 IMAPS comme défini dans la RFC 3501 (voir http://tools.ietf.org/html/rfc3501).

4.1.2 Transaction

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

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

4.2 TM3.2C - Emission de messages par SMTPS

Le client de messagerie permet à l'utilisateur, via le protocole SMTPS, 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 SMTPS de l'opérateur MSSanté.

Information sur la 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, limitent le nombre de destinataires d'un message à 40 au maximum.

4.2.1 Cinématique

Les étapes de « connexion / envoi du message / fin de session » pour un client de messagerie émettant une requête vers 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 SMTPS comme défini dans les RFC 5321 (http ://tools.ietf.org/html/rfc5321) et RFC 2034 (http ://tools.ietf.org/html/rfc2034).

4.2.2 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).

4.3 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 ») et « AutoDiscover ».

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

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

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

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

Les cinématiques d'utilisation par un client de messagerie des services « AutoConfig » et « AutoDiscover » qui peuvent être mis en œuvre par les opérateurs MSSanté sont décrites dans les sous-chapitres suivants.

4.3.1 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 les URLs suivantes : http://autoconfig.«emailaddressdomain»/mail/config-v1.1.xml?emailaddress=«emailaddress» et/ou http://«emailaddressdomain»/.well-known/autoconfig/mail/config-v1.1.xml ;
    - 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.

4.3.2 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.

4.3.3 Cinématique AutoDiscover

Les étapes d'auto-configuration d'un client de messagerie utilisant le service « AutoDiscover » 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 les URLs suivantes : https://«emailaddressdomain»/autodiscover/autodiscover.xml et/ou https://autodiscover.«emailaddressdomain»/autodiscover/autodiscover.xml ;
    - 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.

4.3.4 Transaction AutoDiscover

Les commandes envoyées par le client de messagerie doivent être conformes aux spécifications fournies par l'éditeur à l'adresse suivante : http://msdn.microsoft.com/en-us/library/ee332364%28v=exchg.140%29.aspx.

5 Transactions de messagerie basées sur les Web Services

Le client de messagerie mettant en œuvre les Web Services permet à l'utilisateur :

- 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.

Ces fonctionnalités sont basées sur plusieurs transactions de Web Services qui composent un « catalogue de services ». Ce catalogue de services permet de mettre à disposition des fonctionnalités comparables à celles proposées par les protocoles IMAP et SMTP.

Le catalogue est composé de plusieurs transactions de Web Services SOAP, regroupées en 5 grands domaines et définis dans les paragraphes suivants :

- **§5.2** « TM4.2.xC - Services de consultation et gestion des dossiers » ;
- **§5.3** « TM4.3.xC - Services envoi et gestion de messages » ;
- **§5.4** « TM4.4.xC - Services envoi et consultation des pièces jointes » ;
- **§5.5** « TM4.5.xC - Services consultation et recherche de messages » ;
- **§5.6** « TM4.6C - Service de recherche de BAL correspondant à un Professionnel de Santé ».

L'accès à ces Web Services repose sur la mise en œuvre d'une authentification forte de l'utilisateur ; cette authentification est matérialisée par l'usage d'un jeton fourni par un service d'authentification dédié mis en œuvre par l'opérateur de messagerie.

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

5.1.1 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.

Chaque opérateur MSSanté exposant des interfaces standards de Web Services de messagerie fournit également un service d'authentification basé sur des mécanismes d'authentification qui garantissent la sécurité et la confidentialité des accès aux données contenues dans le système MSSanté. Les mécanismes d'authentification sont spécifiques à chaque opérateur. En revanche, le format du jeton d'authentification est standardisé. Le service d'authentification d'un client de messagerie pour accéder à un service de messagerie s'appuie sur le profil SAML 2.0 ECP.

Ce chapitre décrit spécifiquement, et à titre d'exemple, les mécanismes d'obtention du jeton d'authentification auprès du service d'authentification de l'opérateur ASIP Santé dont le service de messagerie propose deux mécanismes d'authentification : par identifiant/mot de passe/OTP et par carte CPS.

Il comporte les étapes suivantes :

1) Client de messagerie : tentative de connexion au service de *messagerie* ;
2) Service de messagerie : redirection vers le service d'*authentification* si la session n'est pas active ou que la session est expirée ;
3) Client de messagerie : connexion au service d'*authentification* pour récupérer un jeton d'authentification (assertion SAML 2.0) ; ce service d'authentification est spécifique au moyen d'authentification utilisé par l'utilisateur :

a. Authentification par carte CPS ;
b. Authentification par Identifiant / mot de passe / OTP ;

4) Client de messagerie : connexion au service de *messagerie* avec le jeton d'authentification récupéré précédemment et qui permet la récupération du jeton de session (sous la forme d'un cookie de session) ;
5) Client de messagerie : accès aux services de *messagerie* en réutilisant le jeton de session durant sa période de validité.

La figure ci-dessous présente la cinématique générale d'accès aux services de messagerie :

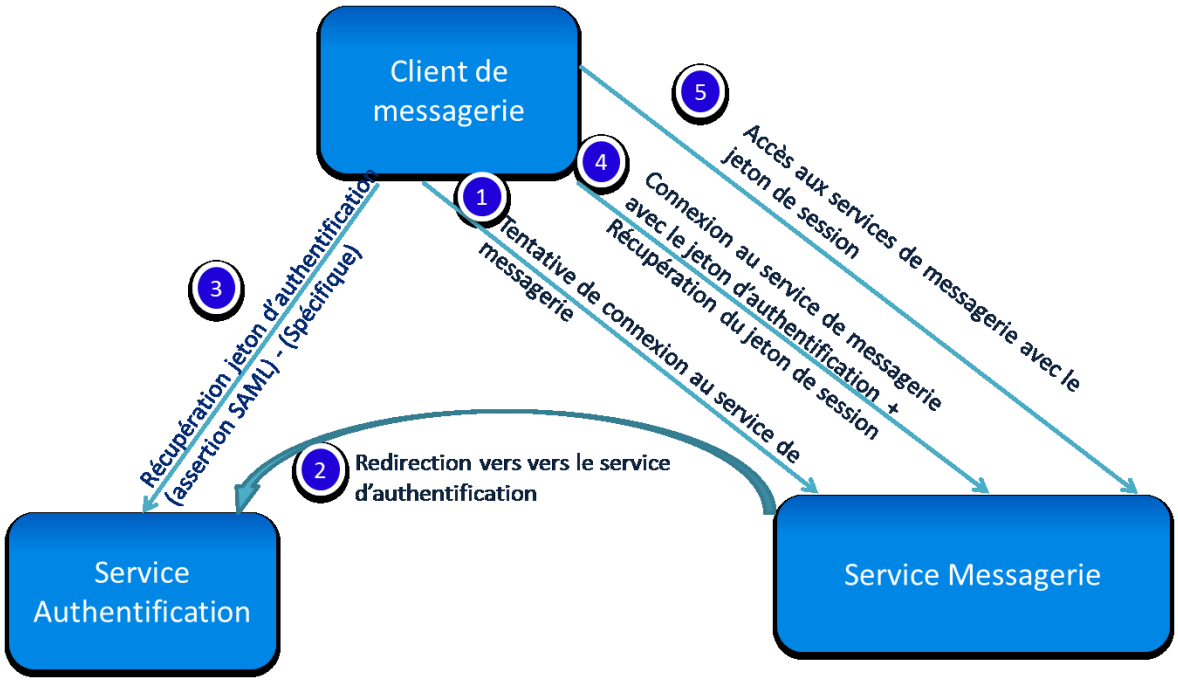

Figure 3 : Présentation de la cinématique d'accès aux services de messagerie

5.1.2 Structure de l'Assertion SAML V2.0

La structure de l'élément assertion est normée ; la référence en ligne explicitant le format d'une assertion SAML v2 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.

Remarque :

- 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'ASIP Santé ;
- 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 ; un opérateur peut enrichir ces attributs en fonction de ses besoins le cas échéant ;
- Le champ « profession » doit être alimenté.

5.1.3 TM4.1.1C - Authentification par carte CPS

5.1.3.1 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 :

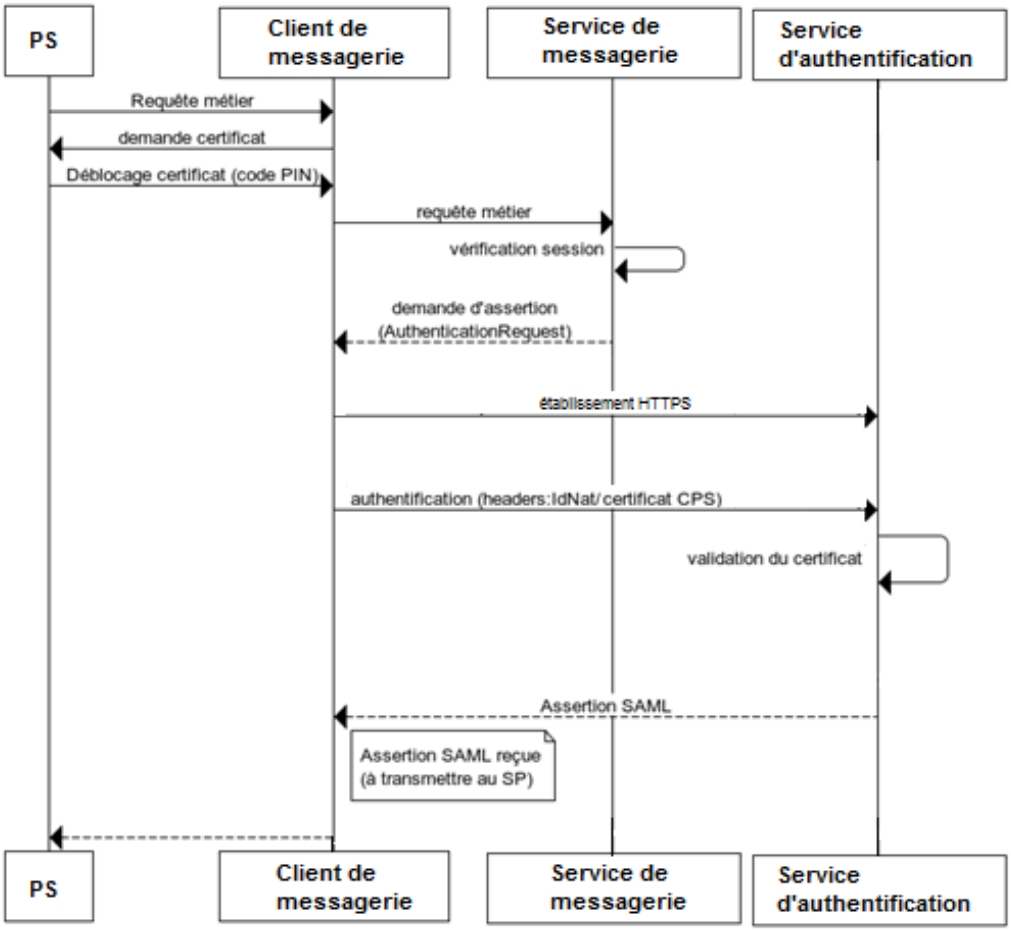

Figure 4 : Cinématique d'authentification par carte CPS

5.1.3.2 Description détaillée d'une authentification par carte CPS

Les 5 étapes décrites ci-après correspondent aux étapes 1 à 5 listées au § 5.1.1.

5.1.3.2.1 Tentative de connexion au service de messagerie

Lorsqu'un client de messagerie tente d'accéder à un service de messagerie, la première étape consiste à détecter si une authentification est requise pour accéder au service demandé (c'est le cas si l'utilisateur n'est pas authentifié ou que la session est expirée).

Cette étape nécessite une communication standardisée avec le service de messagerie, c'est pourquoi tous les messages vers le service de messagerie doivent contenir les entêtes (HTTP headers) suivants :

```
"Accept" => "application/vnd.paos+xml"
"PAOS"                    =>                    "ver='urn:liberty:paos:2003-
08';'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'"
```

Ces entêtes indiquent un support de l'authentification SAML en reverse SOAP.

5.1.3.2.2 Redirection vers le service d'authentification s'il n'existe pas de session active

Dans le cas où le service de messagerie requiert une authentification préalable, la réponse à la requête contient alors un élément XML de type « AuthnRequest » indiquant le besoin de fournir une assertion.

Cet élément « AuthnRequest » est standardisé par SAML 2.0 et contient plusieurs sous-éléments non présentés ici, tels que le certificat X509 du service de messagerie qui sera transmis au service d'authentification.

Exemple de balise « AuthnRequest » :

```
<saml2p:AuthnRequest    xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="http://exemple.com/mss-
msg/saml/SSO/alias/defaultAlias"                          ForceAuthn="false"
ID="a2j8b2fba6jdd8gd21gi6632e80ce11"  IsPassive="false"  IssueInstant="2013-
07-12T12:43:33.538Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Version="2.0">
```

Lors de cette première phase d'échanges entre le client de messagerie et le service de messagerie de l'opérateur MSSanté, plusieurs éléments sont disponibles :

- Un cookie de session (« JSESSIONID ») ;
- L'URL de retour (où l'assertion SAML devra être déposée sur le service de messagerie) : « AssertionConsumerServiceURL ».

Il est nécessaire de conserver ces éléments :

- Le cookie de session, émis par le service de messagerie permet de poursuivre l'authentification (fourniture de l'assertion SAML) et le maintien du statut authentifié lors des futurs échanges ;
- L'URL de retour, indiquant l'adresse où l'assertion SAML devra être déposée sur le service de messagerie : « AssertionConsumerServiceURL ».

Le nom de domaine du service d'authentification n'est pas fourni dans la réponse, le client de messagerie doit donc s'assurer de l'avoir à disposition.

Avec l'opérateur ASIP Santé
Le nom de domaine du service d'authentification de l'opérateur ASIP Santé est : **[AC]**

La réponse du service de messagerie (format SOAP) doit ensuite être acheminée vers le service d'authentification et nécessite au préalable la suppression de ses headers (balises `<soap11:Header>`).

5.1.3.2.3 Connexion au service d'authentification

Cinématique :

Le mécanisme permettant à un client de messagerie d'obtenir un jeton d'authentification en cas d'usage de la CPS est le suivant :

1) [Client] 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 Auth.] Le service d'authentification vérifie la validité du certificat client présenté (non expiré, non révoqué) ;
3) [Client] Le client vérifie la validité du certificat du serveur (non expiré, non révoqué) ;
4) [Client] Une fois la connexion HTTPS validée, le client envoie par Web Service une demande de jeton d'authentification au service d'authentification ;
5) [Service Auth.] Le service d'authentification vérifie la validité de la demande de jeton en fonction de l'identité présentée par le certificat de l'utilisateur et renvoie au client un jeton matérialisant l'authentification réalisée sur la base de l'identité contenue dans le certificat de la carte CPS.

Description détaillée :

A l'étape 4 : la requête d'authentification est enrichie avec des headers spécifiques puis transmise au service d'authentification, sinon la requête est rejetée (au niveau de l'établissement de la connexion HTTPS).

Dans le cadre du service mis en place par l'opérateur ASIP Santé, le header spécifique CPS ajouté par le service d'authentification est le suivant :

- CPSIDNAT => l'identifiant national du PS extrait du certificat.

A l'étape 5 : le service d'authentification réceptionne alors la requête 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), puis l'acceptation ou le rejet de l'authentification.

En réponse à cette requête, le service d'authentification retourne soit :

- Un rejet ;
- Un « body » contenant l'assertion SAML « <saml:Assertion> dans une enveloppe SOAP.

5.1.3.2.4 Connexion au service de messagerie avec le jeton d'authentification

Toujours sur le principe de reverse SOAP, le contenu SOAP de la requête précédente doit être extrait (ce contenu contient entre autre l'assertion SAML) tout en lui retirant les entêtes <SoapHeaders>.

Le contenu obtenu doit ensuite être transmis à l'url de validation de l'assertion « AssertionConsumerServiceURL » (obtenue lors de la première phase d'échanges entre le client de messagerie et le service de messagerie).

La session (cookie JSESSIONID issu de la première requête) doit être maintenue.

En réponse à cette validation, on obtient soit :

- Un retour en « redirect » (HTTP 302) vers l'url initiale (le service « métier » du service de messagerie) indiquant que l'assertion a été validée ;
- Un retour HTTP 200 contenant un « AuthnRequest » (réponse standard initiant le processus d'authentification) indiquant que l'assertion n'a pas été validée.

5.1.3.2.5 Accès aux services de messagerie avec le jeton de session

En dernière étape, le client doit alors faire une redirection (dans la même session) pour consommation du service initialement demandé.

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

5.1.4.1 Cinématique d'une authentification par identifiant / mode de passe / OTP

Le diagramme de séquence ci-dessous présente l'enchainement entre les Web Services de messagerie et les Web Services d'authentification :

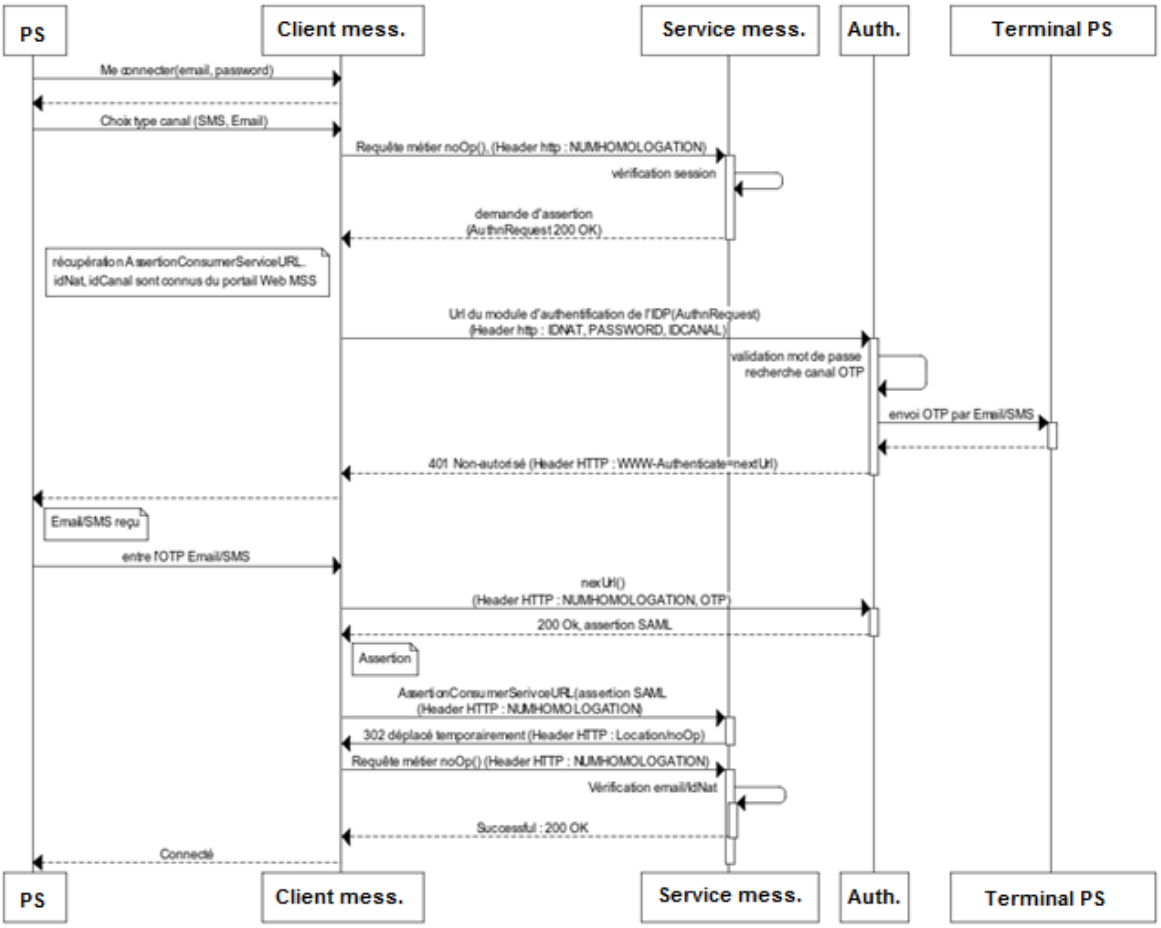

Figure 5 : Cinématique d'authentification par identifiant/mot de passe/OTP

5.1.4.2 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 § 5.1.1.

5.1.4.2.1 Tentative de connexion au service de messagerie

Lorsqu'un client de messagerie tente d'accéder à un service de messagerie, la première étape consiste à détecter si une authentification est requise pour accéder au service demandé (c'est le cas si l'utilisateur n'est pas authentifié ou que la session est expirée).

Cette étape nécessite une communication standardisée avec le service de messagerie, c'est pourquoi, tous les messages vers le service de messagerie doivent contenir les entêtes (HTTP headers) suivants :

```
"Accept" => "application/vnd.paos+xml"
"PAOS"                    =>                    "ver='urn:liberty:paos:2003-
08';'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'"
```

Ces entêtes indiquent un support de l'authentification SAML en reverse SOAP.

5.1.4.2.2 Redirection vers le service d'authentification s'il n'existe pas de session active

Dans le cas où le service de messagerie requiert une authentification préalable, la réponse à la requête contient alors un élément XML de type « AuthnRequest » indiquant le besoin de fournir une assertion.

Cet élément « AuthnRequest » est standardisé par SAML 2.0 et contient plusieurs sous-éléments non présentés ici, tels que le certificat X509 du service de messagerie qui sera transmis au service d'authentification.

Exemple de balise « AuthnRequest » :

```
<saml2p:AuthnRequest    xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="http://exemple.com/mss-
msg/saml/SSO/alias/defaultAlias"                          ForceAuthn="false"
ID="a2j8b2fba6jdd8gd21gi6632e80ce11"  IsPassive="false"  IssueInstant="2013-
07-12T12:43:33.538Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Version="2.0">
```

Lors de cette première phase d'échanges entre le client de messagerie et le service de messagerie de l'opérateur MSSanté, plusieurs éléments sont disponibles :

- Un cookie de session (« JSESSIONID ») ;
- L'URL de retour (où l'assertion SAML devra être déposée sur le service de messagerie) : « AssertionConsumerServiceURL ».

Il est nécessaire de conserver ces éléments :

- Le cookie de session, émis par le service de messagerie, permet de poursuivre l'authentification (fourniture de l'assertion SAML) et le maintien du statut authentifié lors des futurs échanges ;
- L'URL de retour, indiquant l'adresse où l'assertion SAML devra être déposée sur le service de messagerie : « AssertionConsumerServiceURL ».

Le nom de domaine du service d'authentification n'est pas fourni dans la réponse, le client de messagerie doit donc s'assurer de l'avoir à disposition.

Avec l'opérateur ASIP Santé
Le nom de domaine du service d'authentification de l'opérateur ASIP Santé est : **[AC]**

La réponse du service de messagerie (format SOAP) doit ensuite être acheminée vers le service d'authentification (nécessite au préalable la suppression de ses headers (balises `<soap11:Header>`).

5.1.4.2.3 Connexion au service d'authentification

Cinématique :

Le mécanisme permettant à un client de messagerie d'obtenir un jeton d'authentification en cas d'usage de l'authentification par identifiant/mot de passe/OTP est le suivant :

1) [Client] Connexion en HTTPS du client de messagerie sur le portail d'authentification de l'opérateur MSSanté ;
2) [Client] Le client vérifie la validité du certificat du service d'authentification (non expiré, non révoqué) ;
3) [Client] Une fois la connexion HTTPS validée, le client envoie par Web Service une demande initiale au service d'authentification indiquant l'identifiant, le mot de passe et le canal OTP choisi par l'utilisateur ;
4) [Service Auth.] Le service d'authentification vérifie la validité de la demande initiale en fonction de l'identité présentée, du mot de passe fourni et du canal OTP sélectionné ; le cas échéant, le service d'authentification renvoie au client un jeton

initial matérialisant la prise en compte de la demande, et envoie par le canal OTP sélectionné le mot de passe à usage unique ;
5) [Utilisateur] Réception de l'OTP via le canal sélectionné et saisie du mot de passe dans son client de messagerie ;
6) [Client] Envoi par Web Service de l'OTP avec le jeton initial ;
7) [Service Auth.] Vérification de la validité de l'OTP et le cas échéant renvoi au client d'un jeton matérialisant l'authentification réalisée.

Description détaillée :

A l'étape 3 : la première requête vers le service d'authentification consiste à retransmettre en HTTPS les éléments SOAP reçus du service de messagerie (requête précédente) vers le point d'entrée du service d'authentification.

A cette requête, on ajoute les entêtes HTTP spécifiques à l'authentification.

Pour l'opérateur ASIP Santé les éléments sont :

- "IDNAT" : valeur de l'identifiant national du PS ;
- "PASSWORD" : mot de passe du canal sélectionné par le PS ;
- "IDCANAL" : identifiant unique du canal sélectionné par le PS ;
- "NUMHOMOLOGATION" : numéro d'homologation du logiciel client utilisé (non utilisé dans cette version du service - valeur fixée à « 0 »).

Remarque : le champ « IDCANAL » permet au serveur d'authentification d'identifier de façon unique un canal d'authentification. Cette valeur est fixée par le serveur d'authentification lors de l'enrôlement de l'utilisateur (non décrit dans ce document), il est donc nécessaire d'obtenir au préalable cette valeur qui est un élément attendu par le service d'authentification.

Avec l'opérateur ASIP Santé
Dans le cadre du service mis en place par l'opérateur ASIP Santé, l'identifiant unique du canal sélectionné par le PS détenteur d'un compte de messagerie sera disponible par l'intermédiaire du portail Web (page « gestion de mon compte » après authentification) du service ASIP Santé : https://www.mssante.fr/.

A l'étape 4 : en réponse à cette requête, le service d'authentification retourne soit :
- Une erreur d'authentification (HTTP 200 et un message HTML « authentication failed ») ;
- Un retour HTTP 401 contenant l'URL vers laquelle renvoyer l'OTP (« WWW-Authorization : OTP nextUrl= »).

En cas de retour HTTP 401, un OTP a été transmis à l'utilisateur (en fonction des préférences du canal de réception qu'il a déclarées : email ou SMS).
Cet OTP doit alors être renvoyé au service d'authentification, à l'adresse extraite de la requête (OTP nextURL).

Aux étapes 5 + 6 : transmission de l'OTP :

La seconde requête vers le service d'authentification consiste à transmettre l'OTP reçu.

Cette étape nécessite de construire un flux HTTP « POST » contenant en entête les headers HTTP spécifiques suivants :

- « OTP » : valeur de l'OTP reçu ;
- « AMAuthCookie » et « amlbcookie » : les cookies servant à la continuité de la requête et à la gestion de l'équilibre de charge du service d'authentification.

Cette requête doit être transmise à l'adresse « OTP next url » (obtenue lors du premier échange avec le service d'authentification).

Le contenu (body) de la requête suit les mêmes règles que les requêtes précédentes, le message SOAP (sans la partie <SoapHeaders>) issu du service précédent doit être retourné.

A l'étape 7 : en réponse à cette requête, l'OTP est soit :
- Invalide (code HTTP 200 + message HTML « authentication failed ») ;
- Valide (code HTTP 200 + body contenant l'assertion SAML « <saml:Assertion> dans une enveloppe SOAP).

5.1.4.2.4 Connexion au service de messagerie avec le jeton d'authentification

Toujours sur le principe de reverse SOAP (communiquer le message SOAP en réponse vers le endpoint suivant), le contenu SOAP de la requête validant l'OTP doit être extrait (ce contenu contient entre autres l'assertion SAML) tout en lui retirant les entêtes <SoapHeaders>.

Le contenu obtenu doit ensuite être transmis à l'URL de validation de l'assertion « AssertionConsumerServiceURL » (obtenue lors de la première phase d'échanges entre le client de messagerie et le service de messagerie).

La session (cookie JSESSIONID issu de la première requête) doit être maintenue.

En réponse à cette validation, on obtient soit :
- Un retour en « redirect » (HTTP 302) vers l'URL initiale (le service « métier » du service de messagerie) indiquant que l'assertion a été validée ;
- Un retour HTTP 200 contenant un « AuthnRequest » (réponse standard initiant le processus d'authentification), indiquant que l'assertion n'a pas été validée.

5.1.4.2.5 Accès aux services de messagerie avec le jeton de session

En dernière étape, le client doit alors faire une redirection (dans la même session) pour consommation du service initialement demandé.

5.1.5 TM4.1.3C - Fonction de filtre de contrôle d'accès

5.1.5.1 Validation du jeton d'authentification

Le filtre de contrôle d'accès est appliqué lors de chaque appel de Web Service requérant une authentification préalable.

Ce filtre a pour objectif de valider le 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 ». Si le jeton d'authentification n'est pas fourni, alors l'utilisateur est renvoyé sur les services d'authentification.

5.1.5.2 Informations nécessaires (dans le header de la requête)

5.1.5.2.1 Dans le cas d'un appel avec une assertion SAML

Elément	Type	Cardinalité	Description
assertionSAML	STRING	0..1	Assertion SAML
numHomologation	STRING(50)	1	Numéro d'homologation du logiciel (variable NUMHOMOLOGATION dans l'entête HTTP)

Tableau 2

Avec l'opérateur ASIP Santé
L'ASIP Santé ne mettant pas en œuvre une homologation des clients de messagerie pour l'accès à son service de messagerie, la valeur du champ 'numHomologation' est fixée par défaut à la valeur '0'.

5.1.5.2.2 Dans le cas d'un appel avec un cookie de session

Elément	Type	Cardinalité	Description
idSession	STRING Taille max 4ko	0…1	Cookie de session
numHomologation	STRING(50)	1	Numéro d'homologation du logiciel (variable NUMHOMOLOGATION dans l'entête HTTP)

Tableau 3

Avec l'opérateur ASIP Santé
L'ASIP Santé ne mettant pas en œuvre une homologation des clients de messagerie pour l'accès à son service de messagerie, la valeur du champ 'numHomologation' est fixée par défaut à la valeur '0'.

5.1.5.3 Algorithme

1. Si le jeton d'authentification est vide, le service répond une erreur : « 27 » ;
2. Si le jeton d'authentification contient une Assertion SAML, le service valide l'Assertion SAML :
    - Si l'Assertion SAML est valide techniquement et que l'utilisateur identifié dans le jeton est connu par le système, alors le service crée une session utilisateur sur le système de messagerie et retourne au client le cookie de session permettant de faire le lien avec cette session ;
    - Si l'Assertion SAML est invalide, le service répond une erreur : « 25 ».
3. Si le jeton d'authentification contient un cookie de session, le service valide le cookie de session :
    - Si le cookie est valide le service procède au traitement de la requête ;
    - Si le cookie est invalide le service répond une erreur : « 26 ».

5.1.5.4 Erreur

Code http	Code d'erreur	Libellé Erreur	Description
302	**27**	Jeton d'authentification vide, assertion SAML ou Cookie de session est nécessaire	Affiché lorsque le jeton d'authentification n'est pas fourni
403	**25**	L'assertion SAML est invalide	Affiché lorsque l'assertion SAML n'est pas/plus valide
403	**26**	Le cookie de session est invalide	Affiché lorsque le cookie de session n'est pas/plus valide
503	**2**	Le service est temporairement indisponible, merci de réessayer ultérieurement	Survient quand le service de messagerie n'est pas accessible

Tableau 4

5.2 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 5 : Liste des Web Services de consultation et gestion des dossiers

La WSDL associée à ce service est : FolderService.wsdl (voir DR1 au **§ 8.4.2** « Documents de référence pour les services »).

5.2.1 TM4.2.1C - Service listFolders

5.2.1.1 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.

5.2.1.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
folderId	INT	0..1	ID du dossier. Si folderId vide, retourne tous les dossiers. Si folderId non vide, retourne tous les sous-dossiers de ce dossier.

Tableau 6

5.2.1.3 Flux sortants

Elément	Type	Cardinalité	Description
folders	ARRAY	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
|- folderId	INT	1	ID du dossier
|- folderName	STRING	1	Nom du dossier
|- folderNbUnread	INT	1	Nombre de messages non lus
|- folders	ARRAY	0…1	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 7

5.2.1.4 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	
403	**41**	Le dossier n'existe pas	Le dossier en entrée du service est inexistant
403	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue

Tableau 8

5.2.1.5 Exposition SOAP

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

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

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « listFolders » de l'opérateur ASIP Santé est : **[AC]**

5.2.2 TM4.2.2C - Service createFolder

5.2.2.1 Description

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

5.2.2.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
folderName	STRING Taille max dépend du serveur de messagerie	1	Nom du dossier à créer
folderParentId	INT	1	ID du dossier parent

Tableau 9

5.2.2.3 Flux sortants

Elément	Type	Cardinalité	Description
folder			
|- folderId	INT	1	ID du dossier
|- folderName	STRING	1	Nom de dossier

Tableau 10

5.2.2.4 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	
403	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue
403	**41**	Le dossier parent n'existe pas	Le dossier en entrée du service est inexistant

Tableau 11

5.2.2.5 Exposition SOAP

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

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

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « createFolder » de l'opérateur ASIP Santé est : **[AC]**

5.2.3 TM4.2.3C - Service deleteFolder

5.2.3.1 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).

5.2.3.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
folderId	INT	0..1	ID du dossier à supprimer. Si l'identifiant du dossier n'existe pas, alors retour vide (http 200).

Tableau 12

5.2.3.3 Flux sortants

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

5.2.3.4 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	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue
403	**36**	Un des champs a un format invalide	

Tableau 13

5.2.3.5 Exposition SOAP

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

```
https://server/mss-msg-services/services/Folder/soap/vX/deleteFolder
```

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « deleteFolder » de l'opérateur ASIP Santé est : **[AC]**

5.2.4 TM4.2.4C - Service emptyFolder

5.2.4.1 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).

5.2.4.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : #^[a-z0-9._-]+@[a-z0-9._-]{2,}\.[a-z]{2,4}$#
folderId	INT	0..1	ID du dossier à vider. Si l'identifiant du dossier n'existe pas, alors retour vide (http 200).

Tableau 14

5.2.4.3 Flux sortants

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

5.2.4.4 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	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue
403	**36**	Un des champs a un format invalide	

Tableau 15

5.2.4.5 Exposition SOAP

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

```
https://server/mss-msg-services/services/Folder/soap/vX/emptyFolder
```

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « emptyFolder » de l'opérateur ASIP Santé est : **[AC]**

5.2.5 TM4.2.5C - Service trashFolder

5.2.5.1 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.

5.2.5.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
folderId	INT	0..1	ID du dossier à mettre à la corbeille. Si l'identifiant du dossier n'existe pas, alors retour vide (http 200).

Tableau 16

5.2.5.3 Flux sortants

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

5.2.5.4 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	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue
403	**36**	Un des champs a un format invalide	

Tableau 17

5.2.5.5 Exposition SOAP

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

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

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « trashFolder » de l'opérateur ASIP Santé est : **[AC]**

5.2.6 TM4.2.6C - Service renameFolder

5.2.6.1 Description

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

5.2.6.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
folderId	INT	0..1	ID du dossier existant. Si non renseigné, le service ne renvoie rien.
newFolderName	STRING Taille max dépend du serveur de messagerie	1	Nouveau nom du dossier.

Tableau 18

5.2.6.3 Flux sortants

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

5.2.6.4 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	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue
403	**36**	Un des champs a un format invalide	

Tableau 19

5.2.6.5 Exposition SOAP

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

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

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « renameFolder» de l'opérateur ASIP Santé est : **[AC]**

5.2.7 TM4.2.7C - Service moveFolder

5.2.7.1 Description

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

5.2.7.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
folderId	INT	1	ID du dossier existant
destinationFolderId	INT	1	ID du dossier de destination

Tableau 20

5.2.7.3 Flux sortants

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

5.2.7.4 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	
403	**41**	Le dossier n'existe pas	Le dossier en entrée du service est inexistant.
403	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue.
403	**47**	Déplacement de dossier impossible	Par exemple : si l'on tente de déplacer un dossier dans un de ses sous-dossiers.

Tableau 21

5.2.7.5 Exposition SOAP

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

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

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « moveFolder » de l'opérateur ASIP Santé est : **[AC]**

5.3 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 22 : Liste des Web Services d'envoi et de gestion de messages

La WSDL associée à ce service est : ItemService.wsdl (voir DR2 au **§ 8.4.2** « Documents de référence pour les services »).

5.3.1 TM4.3.1C - Service updateMessages

5.3.1.1 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.

5.3.1.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
messageIds	ARRAY[INT]	0…1	Liste de messages ID. Si aucun message, le service ne fait rien.
operation	STRING(10)	1	Opération à exécuter sur le message

Tableau 23

Les opérations disponibles sont :

Code
DELETE
READ
UNREAD
FLAGGED
UNFLAGGED
SPAM
UNSPAM
TRASH

Tableau 24

5.3.1.3 Flux sortants

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

5.3.1.4 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	
403	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue.
403	**45**	Le message n'existe pas	

Tableau 25

5.3.1.5 Exposition SOAP

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

```
https://server/mss-msg-services/services/Item/soap/vX/updateMessages
```

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « updateMessages » de l'opérateur ASIP Santé est : **[AC]**

5.3.2 TM4.3.2C - Service draftMessage

5.3.2.1 Description

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

5.3.2.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
messages	ARRAY	1	Liste de messages. Si pas de message renseigné, le service ne fait rien.
|- messageId	INT	0..1	ID du brouillon à mettre à jour.
|- addresses	ARRAY	0..1	Liste des adresses de messagerie (la liste peut être vide).
|- email	STRING(256)	1	Adresse de messagerie de la personne Respecte l'expression régulière : #^[a-z0-9._-]+@[a-z0-9._-]{2,}\.[a-z]{2,4}$#
|- type	STRING(5)	1	Type d'adresse de messagerie.
|- subject	STRING(50)	0..1	Sujet du message.
|- replyType	STRING(9)	0..1	Type de renvoi.
|- priority	STRING(6)	0..1	Priorité du message, « NORMAL » si non renseignée et sinon « HAUTE ».
|- isHtml	BOOLEAN	0..1	Si non renseigné ou false, le format du message est TEXT, sinon il est HTML.
|- isAccuse	BOOLEAN	0..1	Indique si un accusé de lecture est souhaité, FALSE si non renseigné.
|- messageTransferedId	INT	0…1	ID de message transféré.
|- body	STRING La taille max dépend du serveur de messagerie	0..1	Corps du message.
|- attachments	ARRAY	0..1	Liste des pièces jointes.
|- 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.
|- file	Array[byte]	0..1	Contenu du fichier à uploader en UTF-8.

Elément	Type	Cardinalité	Description
			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 26

La liste des types d'adresses de messagerie est la suivante :

Type
FROM
TO
CC
BCC

Tableau 27

La liste des types de renvoi est la suivante :

Type
REPLIED
FORWARDED

Tableau 28

La liste des priorités est la suivante :

Type
NORMAL
HAUTE

Tableau 29

5.3.2.3 Flux sortants

Elément	Type	Cardinalité	Description
message		1	Message enregistré.
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.
attachments	ARRAY	0..1	Liste des pièces jointes.
|- part	INT	1	Numéro de la pièce jointe.
|- contentType	STRING	1	Type de fichier.
|- size	LONG	1	Taille de fichier en octets.
|- fileName	STRING	1	Nom de fichier.

Tableau 30

5.3.2.4 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	
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	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue.
403	**45**	Le message 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 31

5.3.2.5 Exposition SOAP

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

https://server/mss-msg-services/services/Item/soap/vX/draftMessage

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé

L'URL permettant d'accéder au service « draftMessage » de l'opérateur ASIP Santé est : **[AC]**

5.3.3 TM4.3.3C - Service moveMessages

5.3.3.1 Description

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

5.3.3.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
messageIds	ARRAY[INT]	0…1	Liste des identifiants de messages. Si aucun message n'est fourni, le service ne fait rien.
destinationFolderId	INT	1	ID du dossier de destination.

Tableau 32

5.3.3.3 Flux sortants

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

5.3.3.4 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	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue.
403	**36**	Un des champs a un format invalide	
403	**41**	Le dossier n'existe pas	
403	**45**	Le message n'existe pas	

Tableau 33

5.3.3.5 Exposition SOAP

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

```
https://server/mss-msg-services/services/Item/soap/vX/moveMessages
```

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « moveMessages » de l'opérateur ASIP Santé est : **[AC]**

5.3.4 TM4.3.4C - Service sendMessage

5.3.4.1 Description

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

5.3.4.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
message		1	
|- messageId	INT	0…1	ID du message : à renseigner uniquement dans le cas de l'envoi d'un brouillon.
|- messageTransferedId	INT	0…1	ID de message transféré.
|- addresses	ARRAY	1	Liste des adresses de messagerie (destinataires, copie cachée, etc).
|- email	STRING(256)	1	Adresse de messagerie du destinataire.
|- type	STRING(5)	1	Type d'adresse de messagerie.
|- subject	STRING(50)	0..1	Sujet du message.
|- body	STRING La taille max dépend du serveur de messagerie	0…1	Corps du message.
|- replyType	STRING(9)	0..1	Type de renvoi.
|- priority	STRING(6)	0..1	Priorité du message ; « NORMAL » si non renseigné.
|- isHtml	BOOLEAN	0..1	Si non renseigné ou false, le format du message est « TEXT », sinon il est « HTML ».
|- isAccuse	BOOLEAN	0..1	Indique si un accusé de lecture est souhaité.
|- attachments	ARRAY	0..1	Liste des pièces jointes.
|- part	INT	0…1	Numéro de la pièce jointe.
|- 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
|- file	Array[byte]	0..1	Contenu du fichier à uploader en UTF-8.
|- messageId	INT	0..1	Identifiant du message lié au part (dans le cas du transfert de pièce jointe).

Tableau 34

La liste des types d'adresses de messagerie est la suivante :

Type
FROM
TO
CC
BCC

Tableau 35

La liste des types de renvoi est la suivante :

Type
REPLIED
FORWARDED

Tableau 36

La liste des priorités est la suivante :

Type
NORMAL
HAUTE

Tableau 37

5.3.4.3 Flux sortants

Elément	Type	Cardinalité	Description
message		1	Message.
|-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.
|-attachments	ARRAY	0..1	Liste des pièces jointes.
|- part	INT	1	Numéro de la pièce jointe.
|- contentType	STRING	1	Type de fichier (cf. RFC 2045, 2045 à 2048).
|- size	LONG	1	Taille de fichier en octets.
|- fileName	STRING	1	Nom de fichier.

Tableau 38

5.3.4.4 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	
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	L'adresse de messagerie est inconnue.
403	**45**	Le message n'existe pas	Le message d'une des pièces jointes n'existe pas.

Tableau 39

5.3.4.5 Exposition SOAP

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

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

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « sendMessage » de l'opérateur ASIP Santé est : **[AC]**

5.3.5 TM4.3.5C - Service syncMessages

5.3.5.1 Description

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

5.3.5.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
folderId	INT	0..1	ID du dossier à synchroniser. S'il n'est pas renseigné, cela synchronise tous les dossiers.
token	STRING(60)	0..1	Jeton obtenu lors de la dernière synchronisation. Si ce jeton est vide, cela retourne un jeton.

Tableau 40

5.3.5.3 Flux sortants

Elément	Type	Cardinalité	Description
deletedMessageIds	ARRAY[INT]	0…1	Liste des ID des messages supprimés.
modifiedMessages	ARRAY[Message]	0..1	Liste des messages créés et modifiés.
token	STRING	1	Token qui permettra de rappeler la synchronisation.

Tableau 41

Avec l'élément **Message** constitué des attributs suivants :

Elément	Type	Cardinalité	Description
|- messageId	INT	1	ID du message.
|- date	LONG	1	Date de réception du message.
|- size	LONG	1	Taille du message en octets.
|- flags	ARRAY[STRING]	0…1	Flags associés au message.
|- folderId	INT	1	ID du dossier.
|- addresses	ARRAY	1	Liste des adresses de messagerie.
|- email	STRING	1	Adresse de messagerie de la personne.
|- name	STRING	0..1	Alias.
|- type	STRING	1	Type d'adresse de messagerie.
|- subject	STRING	1	Sujet du message.
|- 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.
|- fragment	STRING	0…1	Fragment du corps du message (utilisé pour l'affichage du contenu sur le détail du message dans la liste des messages).
|- body	STRING	0…1	Corps du message.
|- attachments	ARRAY	1	Liste des pièces jointes.
|- part	INT	1	Numéro de la pièce jointe.
|- contentType	STRING	1	Type de fichier.
|- size	LONG	1	Taille de fichier en octets.
|- fileName	STRING	1	Nom de fichier.

Tableau 42

5.3.5.4 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	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue.
403	**36**	Un des champs a un format invalide	

Tableau 43

La liste des flags est la suivante :

Code
UNREAD
FLAGGED
ATTACHMENT
REPLIED
SENT_BY_ME
DELETED
DRAFT
FORWARDED
URGENT
LOW_PRIORITY
PRIORITY

Tableau 44

La liste des types d'adresses de messagerie est la suivante :

Type
FROM
TO
CC
BCC

Tableau 45

5.3.5.5 Exposition SOAP

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

```
https://server/mss-msg-services/services/Item/soap/vX/syncMessages
```

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « syncMessages » de l'opérateur ASIP Santé est : **[AC]**

5.4 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 46 : Liste des Web Services d'envoi et consultation des pièces jointes

La WSDL associée à ce service est : AttachmentService.wsdl (voir DR3 au **§ 8.4.2** « Documents de référence pour les services »).

5.4.1 TM4.4.1C - Service uploadAttachment

5.4.1.1 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.

5.4.1.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
file	ARRAY[Byte]	1	Ficher 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 47

5.4.1.3 Flux sortants

Elément	Type	Cardinalité	Description
attachmentId	String	1	ID du ficher.

Tableau 48

5.4.1.4 Erreurs

Elément	Type	Cardinalité	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	
403	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue

Tableau 49

5.4.1.5 Exposition SOAP

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

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

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « uploadAttachment » de l'opérateur ASIP Santé est : **[AC]**

5.4.2 TM4.4.2C - Service removeAttachment

5.4.2.1 Description

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

5.4.2.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
messageId	INT	1	Identifiant du message sur lequel on souhaite supprimer un fichier.
part	INT	1	Numéro de la pièce jointe à supprimer.

Tableau 50

5.4.2.3 Flux sortants

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

5.4.2.4 Erreurs

Elément	Type	Cardinalité	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	
403	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue.
403	**45**	Le message n'existe pas	
403	**46**	La pièce jointe n'existe pas	

Tableau 51

5.4.2.5 Exposition SOAP

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

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

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « removeAttachment » de l'opérateur ASIP Santé est : **[AC]**

5.4.3 TM4.4.3C - Service downloadAttachment

5.4.3.1 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.

5.4.3.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
messageId	INT	1	ID du message.
part	INT	1	Numéro de la pièce jointe dans le message.

Tableau 52

5.4.3.3 Flux sortants

Elément	Type	Cardinalité	Description
file	ARRAY[Byte]	0..1	Ficher à envoyer vers le client.

Tableau 53

5.4.3.4 Erreurs

Elément	Type	Cardinalité	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	
403	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue.
403	**45**	Le message n'existe pas	
403	**46**	La pièce jointe n'existe pas	

Tableau 54

5.4.3.5 Exposition SOAP

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

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

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « downloadAttachment » de l'opérateur ASIP Santé est : **[AC]**

5.5 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 55 : Liste des Web Services de consultation et recherche de messages

La WSDL associée à ce service est : ItemService.wsdl (voir DR2 au **§ 8.4.2** « Documents de référence pour les services »).

5.5.1 TM4.5.1C - Service searchMessages

5.5.1.1 Description

Le service « searchMessages » permet d'effectuer des recherches multicritères de messages.

5.5.1.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
searchCriteria		0..1	Paramètres de recherche.
| - html	BOOLEAN	0..1	Si « true », le service retourne le message au format TEXT/HTML ; sinon au format TEXT/PLAIN.
|- 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	STRING	0…1	Type de tri. Si valeur vide ou type inexistant, le tri par défaut est par ordre de date décroissante.
|- query		0…1	
|- content	STRING(80)	0…1	Messages contenant la chaîne spécifiée dans le corps du message.
|- subject	STRING(80)	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.

Elément	Type	Cardinalité	Description
|- 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 56

5.5.1.3 Flux sortants

Elément	Type	Cardinalité	Description
messages	Message	0..1	Liste de messages.
|- messageId	INT	1	ID du message.
|- date	STRING	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	ARRAY[STRING]	0…1	Flags associés au message.
|- folderId	INT	1	ID du dossier.
|- addresses	ARRAY	1	Liste des adresses de messagerie.
|- email	STRING	1	Adresse de messagerie de la personne.
|- name	STRING	0…1	Nom de personne.
|- type	STRING	1	Type d'adresse 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	1	Sujet du message.
|- fragment	STRING	0…1	Fragment du contenu de message (à afficher lors du détail du message dans la liste de message).
|- body	STRING	0…1	Corps du message.
|- attachments	ARRAY	0..1	Liste des pièces jointes.
|- part	INT	1	Numéro de la pièce jointe.
|- contentType	STRING	1	Type de fichier.

Elément	Type	Cardinalité	Description
|- size	LONG	1	Taille de fichier en octets.
|- fileName	STRING	1	Nom de fichier.
|- subject	STRING	1	Sujet du message.

Tableau 57

La liste des types d'adresses de messagerie est la suivante :

Type
FROM
TO
CC
BCC

Tableau 58

La liste des flags est la suivante :

Code
UNREAD
FLAGGED
ATTACHMENT
REPLIED
SENT_BY_ME
DELETED
DRAFT
FORWARDED
URGENT
LOW_PRIORITY
PRIOIRTY

Tableau 59

La liste des types de tri est la suivante :

Code
dateAsc
dateDesc
subjAsc
subjDesc
nameAsc
nameDesc
rcptAsc
rcptDesc
attachAsc
attachDesc
flagAsc
flagDesc
priorityAsc
priorityDesc
sizeAsc
sizeDesc

Tableau 60

5.5.1.4 Erreurs

Elément	Type	Cardinalité	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	
403	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue.

Tableau 61

5.5.1.5 Exposition SOAP

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

https://server/mss-msg-services/services/Item/soap/vX/searchMessages

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « searchMessages » de l'opérateur ASIP Santé est : **[AC]**

5.5.2 TM4.5.2C - Service fullTextSearchMessages

5.5.2.1 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.

5.5.2.2 Flux entrants

Elément	Type	Cardinalité	Description
email	STRING(256)	1	Identifiant de l'utilisateur : adresse de messagerie. Respecte l'expression régulière : ^[_A-Za-z0-9-\\+]+(\\.[_A-Za-z0-9-]+)*@[a-zA-Z0-9][a-zA-Z0-9-]{1,61}[a-zA-Z0-9]\\.[a-zA-Z]{2,}
searchCriteria		1	Paramètres de recherche.
| - html	BOOL	0..1	Si « true », le service retourne le message au format TEXT/HTML ; sinon au format TEXT/PLAIN.
|- 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		0…1	Requête.
|- 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(80)	1	Texte libre.

Tableau 62

5.5.2.3 Flux sortants

Elément	Code d'erreur	Libellé Erreur	Description
messages	Message	0..1	Liste de messages.
|- messageId	INT	1	ID du message.
|- date	STRING	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	ARRAY[STRING]	0…1	Flags associés au message.
|- folderId	INT	1	ID du dossier.
|- addresses	ARRAY	1	Liste des adresses de messagerie.
|- email	STRING	1	Adresse de messagerie de la personne.
|- name	STRING	0…1	Nom de personne.
|- type	STRING	1	Type d'adresse de messagerie.
|- isBodyLarger	BOOLEAN	0..1	Si ce champ est à « true », le contenu du message est trop volumineux (> 50 000 caractères). Le contenu du message a donc été tronqué à 50 000 caractères.
|- subject	STRING	1	Sujet du message.
|- fragment	STRING	0…1	Fragment du contenu de message (à afficher lors du détail du message dans la liste de message).
|- body	STRING	0…1	Corps du message.
|- attachments	ARRAY	0..1	Liste des pièces jointes.
|- part	INT	1	Numéro de la pièce jointe.
|- contentType	STRING	1	Type de fichier.
|- size	LONG	1	Taille de fichier en octets.
|- fileName	STRING	1	Nom de fichier.
|- subject	STRING	1	Sujet du message.

Tableau 63

5.5.2.4 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	
403	**42**	L'adresse de messagerie est inconnue	L'adresse de messagerie est inconnue.

Tableau 64

5.5.2.5 Exposition SOAP

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

https://server/mss-msg-services/services/Item/soap/vX/fullTextSeachMessages

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « fullTextSearchMessages » de l'opérateur ASIP Santé est : **[AC]**

5.6 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.

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 65 : 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 **§ 8.4.2** « Documents de référence pour les services »).

5.6.1 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.

5.6.2 Flux entrants

Elément	Type	Cardinalité	Description
userId	STRING(256)	1	Identifiant de l'utilisateur.

Tableau 66

5.6.3 Flux sortants

Elément	Type	Cardinalité	Description
emails	ARRAY[STRING]	0…1	Liste d'adresses de messagerie d'un utilisateur.

Tableau 67

5.6.4 Erreurs

Elément	Type	Cardinalité	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

Tableau 68

5.6.5 Exposition SOAP

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

https://server/mss-msg-services/services/Annuaire/soap/vX/listEmails

Avec X : version majeure du service.

Avec l'opérateur ASIP Santé
L'URL permettant d'accéder au service « listEmails » de l'opérateur ASIP Santé est : **[AC]**

6 Transaction de consultation de l'annuaire national MSSanté 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 national MSSanté permet de rechercher un correspondant sur la base de multiples critères et de récupérer en retour de la requête les informations d'identité, l'adresse de messagerie et les coordonnées de contact des destinataires potentiels répondant aux critères de recherche utilisés.

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 national MSSanté 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 national MSSanté, lorsque, après récupération d'une première liste de résultats l'utilisateur souhaite affiner ses critères de recherche.

6.1 Cinématique

La cinématique de recherche dans l'annuaire national MSSanté 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 national MSSanté ;
- [Client] Le client de messagerie appelle la transaction TM2.1.1C de recherche dans l'annuaire national MSSanté ;
- [Annuaire national MSSanté] L'annuaire national MSSanté 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.

6.2 TM2.1.1C - Interrogation de l'annuaire national MSSanté par le protocole LDAP

L'interrogation de l'annuaire national MSSanté 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.

6.2.1 Prérequis

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

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

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).

6.2.2 DIT et types d'entrées de l'annuaire national MSSanté

6.2.2.1 DIT de l'annuaire national MSSanté

La figure suivante présente le schéma et l'arborescence (DIT pour Directory Information Tree) de l'annuaire national MSSanté :

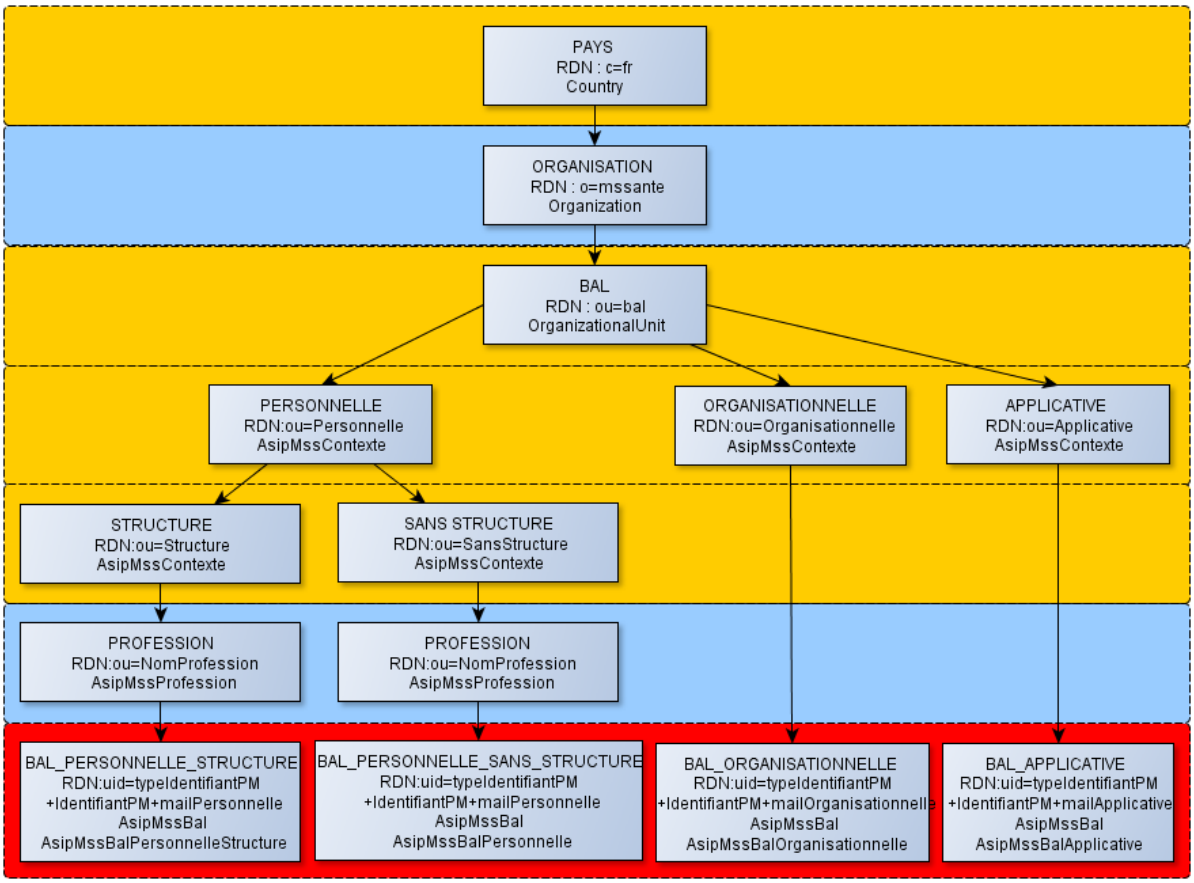

Figure 6 : Représentation du DIT de l'annuaire national MSSanté

Avec :

- Nœuds statiques
- Nœuds dynamiques
- Feuilles

6.2.2.2 Types d'entrées de l'annuaire national MSSanté

L'annuaire national MSSanté 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[4] :** nœud se trouvant sous le nœud BAL. Les entrées de ce type regroupent les BAL organisationnelles ;
- **APPLICATIVE[5] :** nœud se trouvant sous le nœud BAL. Les entrées de ce type regroupent les BAL applicatives ;

[4] BAL Organisationnelle : attachée à une structure (BAL d'un service dans un Etablissement de Santé par exemple).

[5] BAL Applicative : attachée à un système d'information (BAL émettant des compte-rendus par exemple).

- **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 organisationnelle ;
- **BAL_APPLICATIVE :** feuille se trouvant sous le nœud APPLICATIVE. Les entrées de ce type représentent les BAL applicative.

6.2.2.3 Objectclass

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

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

Les objectclasses vides servent à marquer des entrées et 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.

6.2.3 Liste des attributs LDAP standards utilisés

Les attributs standards utilisés sont :

Attribut	Description	Objectclass	Syntaxe	Multi-valué	Sens. Casse	Taille Max
cn (CommonName)	Identifiant national pour les porteurs de cartes, nom du rôle pour les rôles-fonctions, nom du domaine complètement qualifié pour les serveurs, nom de l'autorité de certification pour les autorités de certification intermédiaires.	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 69 : Liste des attributs LDAP standards utilisés

6.2.4 Liste des attributs LDAP spécifiques à l'annuaire national MSSanté

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 70 : Liste des attributs LDAP spécifiques

6.2.5 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 national MSSanté, 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 national MSSanté, voir le chapitre « TM2.1.3A – Téléchargement d'une extraction de l'annuaire national MSSanté » 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 : xxxxxxxxxxxxx Responsable de la BAL : xxxxxxxxxxxxx Zéro papier : oui
givenname :	PRENOMEXERCICE	s/o

Attribut LDAP	Cas BAL Personnelle	Cas BAL Applicative ou Organisationnelle
l :	NCOMMUNE	NCOMMUNE
mail :	ADRESSEBAL	ADRESSEBAL
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)
objectclass : inetOrgPerson		
objectclass : top		
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	Concaténation des données : • Si RAISONSOCIALE n'est pas vide, RAISONSOCIALE (CODE_POSTAL) • Si RAISONSOCIALE est vide, ENSEIGNECOMMERCIALE (CODE_POSTAL) *Exemple* : HOPITAL LA PITIE

Attribut LDAP	Cas BAL Personnelle	Cas BAL Applicative ou Organisationnelle
	SALPETRIERE (75013)	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 concaténation de TYPEIDENTIFIANTPP et IDENTIFIANTPP (sans espace de séparation) • Sinon aucune information. Civilité d'exercice • Si NCIVILITEEXERCICE n'est pas vide, alors concaténation de : « Civilité d'exercice : « et NCIVILITEEXERCICE • Sinon aucune information. Type de BAL Concaténation de « Type de BAL : « et libellé fonctionnel de TYPEBAL Dématérialisation • 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) Type de BAL Concaténation de « Type de BAL : « et libellé fonctionnel de TYPEBAL Description de la BAL Concaténation de « Description de la BAL : « et DESCRIPTION Responsable de la BAL Concaténation de « Responsable de la BAL : « et RESPONSABLE Dématérialisation • 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,	s/o

Attribut LDAP	Cas BAL Personnelle	Cas BAL Applicative ou Organisationnelle
	alors concaténation de : "Identifiant national du PS :" et Concaténation de TYPEIDENTIFIANTPP et IDENTIFIANTPP (sans espace de séparation) • Sinon aucune information. Exemple : 811111111111	
departement	NDEPARTEMENT	NDEPARTEMENT
specOrdRPPS	NSPECIALITE (code spécialité)	s/o
codeProfession	NPROFESSION (code profession)	s/o
codeCategorieProfession	NCATEGORIEPROFESSION (code catégorie de professions)	s/o
libelleCategorieProfession	NCATEGORIEPROFESSION (libellé catégorie de professions)	s/o

Tableau 71 : contenu des attributs de l'annuaire LDAP

6.2.6 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 72 : 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 »).

6.2.7 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.

6.2.8 Résultats fournis par l'annuaire national MSSanté

Un nombre maximum de résultats est prévu : au-delà, l'annuaire national MSSanté renvoie un code d'erreur que le 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 national MSSanté
Pour information, les valeurs configurées par défaut sur l'annuaire national MSSanté sont : • TimeLimitExceeded : 1 minute ; • SizeLimitExceeded : 100 entrées.

7 Transaction de consultation de l'annuaire national MSSanté par Web Service

7.1 TM2.1.2C – Interrogation de l'annuaire national MSSanté par Web Service

L'interrogation de l'annuaire national MSSanté par Web Service est prévue (la spécification correspondante est en cours de définition à la date de rédaction de ce document). **[AC]**

8 Annexes

8.1 Documents externes

8.1.1 Documents applicables

Le tableau ci-dessous récapitule les principaux documents applicables. Dans l'ensemble du document, ils sont désignés par le code apparaissant dans la colonne « Référence ».

N°	Référence	Document
Documents du Cadre d'interopérabilité des Systèmes d'Information de Santé (CI-SIS) (Documents accessibles sur le site de l'ASIP Santé http://esante.gouv.fr/)		
DA1	[CI-CHAP]	**Document Chapeau du CI-SIS**
DA2	[CI-ECH-DOC]	**Volet ECHANGE DE DOCUMENTS DE SANTE**
DA3	[CI-TR-CLI-LRD]	**Couche TRANSPORT VOLET SYNCHRONE**
DA4	[CI-STRU-ENTETE]	**Couche Contenu Volet Structuration Minimale de Documents Médicaux**
Nomenclature des Acteurs de Santé (Documents accessibles sur le site de l'ASIP Santé http://esante.gouv.fr/services/referentiels/identification/nomenclature-des-acteurs-de-sante)		
DA5	[NAS-RES-TERMI]	**Liste des Identifiants des Ressources Terminologiques utilisées par le RASS**
Autres documents (Documents accessibles sur le site de l'ASIP Santé http://esante.gouv.fr/)		
DA6	[DSFT-MSSANTE]	**Dossier des Spécifications Fonctionnelles et Techniques des Interfaces d'accès au système de Messageries Sécurisées de Santé (MSSanté)**

Tableau 73 : Liste des documents applicables

8.1.2 Documents de référence

Documents de référence	

Tableau 74 : Liste des documents de référence

8.1.3 Requests For Comments (RFC)

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

- MSS-ANX-CRL1 : INTERNET X.509 PUBLIC KEY INFRASTRUCTURE – CERTIFICATE AND CERTIFICATE REVOCATION LIST (CRL) PROFILE
- MSS-ANX-SMTPS: SMTP SERVICE EXTENSION FOR – SECURE SMTP OVER TRANSPORT LAYER SECURITY
- MSS-ANX-IMAPS: USING TLS WITH IMAP, POP3 AND ACAP
- MSS-SMTP1 : SIMPLE MAIL TRANSFER PROTOCOL
- MSS-SMTP2: SMTP SERVICE EXTENSION FOR RETURNING ENHANCED ERROR CODES
- MSS-ANX-SMTPS: SMTP SERVICE EXTENSION FOR SECURE SMTP OVER TRANSPORT LAYER SECURITY
- MSS-ANX-TLS1: USING TLS WITH IMAP, POP3 AND ACAP
- MSS-ANX-TLS2: THE TLS PROTOCOL VERSION 1

- MSS-ANX-LDAP1: LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP): TECHNICAL SPECIFICATION ROAD MAP
- MSS-ANX-LDAP2: LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP): THE PROTOCOL
- MSS-ANX-LDAP3: LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP): DIRECTORY INFORMATION MODELS
- MSS-ANX-LDAP4: LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP): AUTHENTICATION METHODS AND SECURITY MECHANISMS
- MSS-ANX-IMAP : INTERNET MESSAGE 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

8.1.4 Annexes externes

Documentation IETF **(spécification internationale en libre accès sur http ://www.ietf.org/)**		
DX1	MSS-ANX-CRL1	**Internet X.509 Public Key Infrastructure** Certificate and Certificate Revocation List (CRL) Profile http ://tools.ietf.org/html/rfc5280
DX2	MSS-SMTP1	**Simple Mail Transfer Protocol** http ://tools.ietf.org/html/rfc5321
DX3	MSS-SMTP2	**SMTP Service Extension for**

Documentation IETF (spécification internationale en libre accès sur http ://www.ietf.org/)		
		Returning Enhanced Error Codes http://tools.ietf.org/html/rfc2034
DX4	MSS-ANX-SMTPS	**SMTP Service Extension for** Secure SMTP over Transport Layer Security http://www.ietf.org/rfc/rfc3207.txt
DX5	MSS-ANX-TLS1	**Using TLS with IMAP, POP3 and ACAP** http://www.ietf.org/rfc/rfc2595.txt
DX6	MSS-ANX-TLS2	**The TLS Protocol Version 1.0** http://tools.ietf.org/html/rfc2246
DX7	MSS-ANX-LDAP1	**Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map** http://tools.ietf.org/html/rfc4510
DX8	MSS-ANX-LDAP2	**Lightweight Directory Access Protocol (LDAP): The Protocol** http://tools.ietf.org/html/rfc4511
DX9	MSS-ANX-LDAP3	**Lightweight Directory Access Protocol (LDAP): Directory Information Models** http://tools.ietf.org/html/rfc4512
DX10	MSS-ANX-LDAP4	**Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms** http://tools.ietf.org/html/rfc4513
DX11	MSS-ANX-IMAP	**Internet Message Acces Protocol – Version 4rev1** http ://tools.ietf.org/html/rfc3501
DX12	MSS-ANX-DKIM1	**Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)** http://tools.ietf.org/html/rfc4686
DX13	MSS-ANX-DKIM2	**DomainKeys Identified Mail (DKIM) Signatures** http://tools.ietf.org/html/rfc4871
DX14	MSS-ANX-DKIM3	**DomainKeys Identified Mail (DKIM) Signatures** http://tools.ietf.org/html/rfc6376
DX15	MSS-ANX-MAIL	**Application Techniques for Checking and Transformation of Names** http://tools.ietf.org/html/rfc3696
DX16	MSS-ANX-MIME1	**Multipurpose Internet Mail Extensions (MIME) Part One : Format of Internet Message Bodies** http://tools.ietf.org/html/rfc2045
DX17	MSS-ANX-MIME2	**Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types** http://tools.ietf.org/html/rfc2046
DX18	MSS-ANX-MIME3	**MIME (Multipurpose Internet Mail Extensions) Part Three : Message Header Extensions for Non-ASCII Text** http://tools.ietf.org/html/rfc2047
DX19	MSS-ANX-MIME4	**Media Type Specifications and Registration Procedures**

Documentation IETF (spécification internationale en libre accès sur http ://www.ietf.org/)		
		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 75 : Liste des annexes externes IETF

8.2 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 ;

[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).

- **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.

8.3 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
ASIP	Agence des Systèmes d'Information Partagés (cf. ASIP Santé)
BAL	Boîte aux lettres
CAH	Comité d'Agrément des Hébergeurs
CI-SIS	Cadre d'interopérabilité des Systèmes d'Information de Santé de l'ASIP Santé
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

Abréviations	Signification
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

Tableau 76 : Liste des acronymes et de leurs significations

8.4 Web Services et URL pour les transactions

8.4.1 URL des services [AC]

Transaction	Description	Opération	URL

Tableau 77 : URL des services

8.4.2 Documents de référence pour les services

Documents de référence (Documents accessibles sur le site de l'ASIP Santé http://esante.gouv.fr/)	
DR1	WSDL des services de consultation et gestion des dossiers description : FolderService.wsdl
DR2	WSDL des services envoi et gestion de messages & des services consultation et recherche de messages : ItemService.wsdl
DR3	WSDL des services envoi et consultation des pièces jointes: AttachmentService.wsdl
DR4	WSDL du service de recherche de BAL correspondant à un Professionnel de Santé : AnnuaireService.wsdl

Tableau 78 : Liste des documents de référence pour les services

8.5 Exemple de flux HTTP d'appel au service d'authentification

```
--------------------------------------------------------------------------------
-                                                    AUTHENTIFICATION  MSSante
                                                                          -
```

```
--------------------------------------------------------------------------------
------------------
POST /mss-msg-services/services/Annuaire/rest/v1/listEmails HTTP/1.1
Host: ns202477.ovh.net:444
PAOS:                                                ver='urn:liberty:paos:2003-08';
'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'
Accept: application/json, application/vnd.paos+xml
Content-Type: application/json; charset=utf-8
Accept-Language: fr;q=1, en;q=0.9, de;q=0.8, ja;q=0.7, nl;q=0.6, it;q=0.5
Connection: keep-alive
Accept-Encoding: gzip, deflate
Content-Length: 43
NUMHOMOLOGATION: APPMOBILE
User-Agent: MSSante/1.0 (iPhone; iOS 6.1.4; Scale/2.00)
Request HTTP Body
{
       "listEmailsInput":
       {
              "userId":"1827364559"
       }
}

HTTP/1.1 200 OK
Set-Cookie:   JSESSIONID=42CE4C4B825BA68CAC765772ED9D9866;   Path=/mss-msg-services;
Secure
Cache-control: no-cache, no-store
Pragma: no-cache
SOAPAction: http://www.oasis-open.org/committees/security
Content-Type: application/vnd.paos+xml;charset=UTF-8
Content-Length: 4262
Connection: close
Response String:
<?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://ns202477.ovh.net:444/mss-msg-
services/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</saml2:Issuer>
         <saml2p:IDPList xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
            <saml2p:IDPEntry ProviderID="https://ns202477.ovh.net:443/openam" />
         </saml2p:IDPList>
      </ecp:Request>
   </soap11:Header>
   <soap11:Body>
      <saml2p:AuthnRequest       xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://ns202477.ovh.net:444/mss-msg-
services/saml/SSO/alias/defaultAlias"                              ForceAuthn="false"
ID="a3c88b0h1j8jg15f16e6a141he2ffi5"    IsPassive="false"    IssueInstant="2013-09-
24T09:12:48.312Z"        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</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="#a3c88b0h1j8jg15f16e6a141he2ffi5">
                  <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>J37BBfJCv8dboisErskgPB6Y+Qc=</ds:DigestValue>
              </ds:Reference>
           </ds:SignedInfo>
           <ds:SignatureValue>

      CwrFzuVbBX++V3zKYFiCE5/kd7Z51HeVo42Pk3lY0xlP6kkABoCjqMRRJyk0tgh0JMuTzUaEZOAO

      CmIRseF6e2PiT2Nf4X3rRK3WFvYKTa/ByHMPVS+WgRS99luk7wjCU/TJTnsBJAGPCnF8dIoKSbri

      oDAdufgoAP8RGAJraGs0AmhYP2AbthLbELMOjtK1fI1RB6ooFLtn7756drDyaQSLutkGXOE1YdFS

      mHWTZtIjbXN6/0P7NqeiXbw3lR9S1hBiI5QWWH1PkicIul6dQbvfFCgsVaWtsyl6+wrB8JdBK07E
                        Aw23SQMNu/dCUbpK5BpH3heUuJotfLC81e5lSw==
                 </ds:SignatureValue>
           <ds:KeyInfo>
              <ds:X509Data>
                 <ds:X509Certificate>

      MIIEnjCCAoagAwIBAgIBBTANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJGUjEPMA0GA1UECAwG

      RnJhbmNlMQ4wDAYDVQQHDAVQQXJpczESMBAGA1UECgwJQ2FwZ2VtaW5pMRcwFQYDVQQDDA5DYXBn

      ZW1pbmkgRGVtbzAeFw0xMzA4MDkxMjI2MjNaFw0xNDA4MDkxMjI2MjNaME0xCzAJBgNVBAYTAkZS

      MQ8wDQYDVQQIDAZGcmFuY2UxEjAQBgNVBAoMCUNhcGdlbWluaTEZMBcGA1UEAwwQbnMyMDI0Nzcu

      b3ZoLm5ldDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMeNH2F8A2r3kwiwXdWMmR+/

      0vFCSQqb29RbSONDM7rtyUmMT5NlpLnVKQkEJfKQubG3HPMVLkaCT3rdOuV5tujZGR56Ew/jHGFi

      /p+6bJz4Lm229nRe85SPzvcerYaD2VwPE5k6CwLMifQv1eDcI/2J+LRGKhgD7H2A54zIyUKcRN5D

      RE7nlviMQr4NS8DPLWJjkZjNnXJUR3ZhLgLmLAbg+ElkNfRxOQo45EQgw7GMeqMbzXaewHVGVGt/

      TY3AQhD2laaO5vtlAsdI/k2nex9QPBjb29E0rbRFm6SUklGgGlgT65dF+J2zbeN5War7zHbsTJUX

      MkWuxcJvorUYKfECAwEAAaN7MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBH

      ZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFB8h9PzL5h7bbfO0deUxlLGDoY4GMB8GA1Ud

      IwQYMBaAFCymCnuDqdBd7cLl+XM46VwEi6hAMA0GCSqGSIb3DQEBBQUAA4ICAQCcpejiBjmzqaYl

      rJwS1FvTDpY7sweyYofMYI1HEqZhKKn/WNNEHw4cs/i0NCEmGSbj3nTJmptnziIkpE2Kjfh2jU+0

      UYnpTKYGeDdbc8f7KiAcyGpPDzy4PBHx2KAC+grWqVq3voodNUesfgrl3kbiE64Vlz7G1GQLlTFB

      EVfwQnEFSnpQMLtODWuTfg6RnMpQJYXIHUD6wIl8uNgehGpdJhLG/athXfKf3MVAfx2xV1KeylEj

      lMauBFZ+fwjtNEbbqkDtlWnah2+bJUmN26ZvrNI0cO4enP6b/XomYHMPE1NC2zsBCBHFkBnGN3YI

      YkPsMarrXgHE7TEUWRnkbUP0/Y6vqgzPL3PgESpL8o5DHLWSZE1iwvJzf22CEzkQOAbGxkfzswas

      JX195bYrx4a2WmRua6BErN9VwniqvufLMg8ZlFqGPtxQRGISl7pYhmcWtrmOTLjE3js8ezpuMf5j

      /MWElgO3EQoxPBnMJ5zvoCnV205CRiaOKbO78LAudtPdB2rn62avqXnPFrzg8sCNlHuQgpe7qe7c

      M9Qum9oVUSKi3aWhVcvy+/0gUHUQArCzUPkzdLZnpAn7+8qE8U1+j2ny+R4XI8z+cTncY3pzuCTb

      0tDF6qyhiMInFTMoy87DvPRAuRXaqFVIwrWuhrupRVEGwKUoIH6vuhsVcwU9sA==
                        </ds:X509Certificate>
              </ds:X509Data>
           </ds:KeyInfo>
        </ds:Signature>
        <saml2p:Scoping ProxyCount="2">
           <saml2p:IDPList>
```

```
               <saml2p:IDPEntry ProviderID="https://ns202477.ovh.net:443/openam" />
            </saml2p:IDPList>
         </saml2p:Scoping>
      </saml2p:AuthnRequest>
   </soap11:Body>
</soap11:Envelope>
```

```
/!\ ETAPE#1 : Execute Authentifier OTP/!\
POST /openam/SSOSoap/metaAlias/asip/idp HTTP/1.1
Host: ns202477.ovh.net
PASSWORD: aaaa
Accept: */*
IDCANAL: 1518
User-Agent: MSSante/1.0 (iPhone; iOS 6.1.4; Scale/2.00)
Accept-Language: fr;q=1, en;q=0.9, de;q=0.8, ja;q=0.7, nl;q=0.6, it;q=0.5
Content-Type: text/xml
NUMHOMOLOGATION: APPMOBILE
Connection: keep-alive
Content-Length: 3539
IDNAT: 1827364559
Accept-Encoding: gzip, deflate
Request HTTP Body
<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
   <soap11:Header />
   <soap11:Body>
      <saml2p:AuthnRequest       xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://ns202477.ovh.net:444/mss-msg-
services/saml/SSO/alias/defaultAlias"                              ForceAuthn="false"
ID="a3c88b0h1j8jg15f16e6a141he2ffi5"    IsPassive="false"    IssueInstant="2013-09-
24T09:12:48.312Z"        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</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="#a3c88b0h1j8jg15f16e6a141he2ffi5">
                  <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>J37BBfJCv8dboisErskgPB6Y+Qc=</ds:DigestValue>
               </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>

      CwrFzuVbBX++V3zKYFiCE5/kd7Z51HeVo42Pk3lY0xlP6kkABoCjqMRRJyk0tgh0JMuTzUaEZOAO

      CmIRseF6e2PiT2Nf4X3rRK3WFvYKTa/ByHMPVS+WgRS99luk7wjCU/TJTnsBJAGPCnF8dIoKSbri

      oDAdufgoAP8RGAJraGs0AmhYP2AbthLbELMOjtK1fI1RB6ooFLtn7756drDyaQSLutkGXOE1YdFS

      mHWTZtIjbXN6/0P7NqeiXbw3lR9S1hBiI5QWWH1PkicIul6dQbvfFCgsVaWtsyl6+wrB8JdBK07E
                        Aw23SQMNu/dCUbpK5BpH3heUuJotfLC81e5lSw==
                  </ds:SignatureValue>
            <ds:KeyInfo>
               <ds:X509Data>
                  <ds:X509Certificate>

      MIIEnjCCAoagAwIBAgIBBTANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJGUjEPMA0GA1UECAwG
```

```
        RnJhbmNlMQ4wDAYDVQQHDAVQQXJpczESMBAGA1UECgwJQ2FwZ2VtaW5pMRcwFQYDVQQDDA5DYXBn
        ZW1pbmkgRGVtbzAeFw0xMzA4MDkxMjI2MjNaFw0xNDA4MDkxMjI2MjNaME0xCzAJBgNVBAYTAkZS
        MQ8wDQYDVQQIDAZGcmFuY2UxEjAQBgNVBAoMCUNhcGdlbWluaTEZMBcGA1UEAwwQbnMyMDI0Nzcu
        b3ZoLm5ldDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMeNH2F8A2r3kwiwXdWMmR+/
        0vFCSQqb29RbSONDM7rtyUmMT5NlpLnVKQkEJfKQubG3HPMVLkaCT3rdOuV5tujZGR56Ew/jHGFi
        /p+6bJz4Lm229nRe85SPzvcerYaD2VwPE5k6CwLMifQv1eDcI/2J+LRGKhgD7H2A54zIyUKcRN5D
        RE7nlviMQr4NS8DPLWJjkZjNnXJUR3ZhLgLmLAbg+ElkNfRxOQo45EQgw7GMeqMbzXaewHVGVGt/
        TY3AQhD2laaO5vtlAsdI/k2nex9QPBjb29E0rbRFm6SUklGgGlgT65dF+J2zbeN5War7zHbsTJUX
        MkWuxcJvorUYKfECAwEAAaN7MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBH
        ZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFB8h9PzL5h7bbfO0deUxlLGDoY4GMB8GA1Ud
        IwQYMBaAFCymCnuDqdBd7cLl+XM46VwEi6hAMA0GCSqGSIb3DQEBBQUAA4ICAQCcpejiBjmzqaYl
        rJwS1FvTDpY7sweyYofMYI1HEqZhKKn/WNNEHw4cs/i0NCEmGSbj3nTJmptnziIkpE2Kjfh2jU+0
        UYnpTKYGeDdbc8f7KiAcyGpPDzy4PBHx2KAC+grWqVq3voodNUesfgrl3kbiE64Vlz7G1GQLlTFB
        EVfwQnEFSnpQMLtODWuTfg6RnMpQJYXIHUD6wIl8uNgehGpdJhLG/athXfKf3MVAfx2xV1KeylEj
        lMauBFZ+fwjtNEbbqkDtlWnah2+bJUmN26ZvrNI0cO4enP6b/XomYHMPE1NC2zsBCBHFkBnGN3YI
        YkPsMarrXgHE7TEUWRnkbUP0/Y6vqgzPL3PgESpL8o5DHLWSZE1iwvJzf22CEzkQOAbGxkfzswas
        JX195bYrx4a2WmRua6BErN9VwniqvufLMg8ZlFqGPtxQRGISl7pYhmcWtrmOTLjE3js8ezpuMf5j
        /MWElgO3EQoxPBnMJ5zvoCnV205CRiaOKbO78LAudtPdB2rn62avqXnPFrzg8sCNlHuQgpe7qe7c
        M9Qum9oVUSKi3aWhVcvy+/0gUHUQArCzUPkzdLZnpAn7+8qE8U1+j2ny+R4XI8z+cTncY3pzuCTb
        0tDF6qyhiMInFTMoy87DvPRAuRXaqFVIwrWuhrupRVEGwKUoIH6vuhsVcwU9sA==
                        </ds:X509Certificate>
                </ds:X509Data>
             </ds:KeyInfo>
          </ds:Signature>
          <saml2p:Scoping ProxyCount="2">
             <saml2p:IDPList>
                <saml2p:IDPEntry ProviderID="https://ns202477.ovh.net:443/openam" />
             </saml2p:IDPList>
          </saml2p:Scoping>
       </saml2p:AuthnRequest>
    </soap11:Body>
</soap11:Envelope>

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.*AAJTSQACMDEAAlNLABQtM
zIyOTg3MDg1MjUwMjE3MzU5NQ..*; Domain=.ovh.net; Path=/
Set-Cookie: amlbcookie=01; Domain=.ovh.net; Path=/
WWW-Authenticate:                    DEBUG_OTP=[34653835]                    OTP
nextUrl=/openam/UI/Login?forward=true&realm=%2Fasip&goto=%2FSSOSoap%2FmetaAlias%2Fa
sip%2Fidp%3FReqID%3Da3c88b0h1j8jg15f16e6a141he2ffi5&spEntityID=mss-msg-services
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>


/!\ ETAPE#2 : En attente de la reception de l'OTP par push notification /!\
Received notification: {

    aps =     {

    };

    otp = 34653835;

}


/!\ ETAPE#3 : Execute Valider OTP /!\
POST
/openam/UI/Login?forward=true&realm=%2Fasip&goto=%2FSSOSoap%2FmetaAlias%2Fasip%2Fid
p%3FReqID%3Da3c88b0h1j8jg15f16e6a141he2ffi5&spEntityID=mss-msg-services HTTP/1.1
Host: ns202477.ovh.net
OTP: 34653835
Content-Type: text/xml
Accept: */*
Cookie:
AMAuthCookie=AQIC5wM2LY4SfcyQn5K2wvViX1K61npjcQ3OIy6ZufCPPRE.*AAJTSQACMDEAAlNLABQtM
zIyOTg3MDg1MjUwMjE3MzU5NQ..*; amlbcookie=01;
Accept-Language: fr;q=1, en;q=0.9, de;q=0.8, ja;q=0.7, nl;q=0.6, it;q=0.5
Connection: keep-alive
Accept-Encoding: gzip, deflate
Content-Length: 2
NUMHOMOLOGATION: APPMOBILE
User-Agent: MSSante/1.0 (iPhone; iOS 6.1.4; Scale/2.00)
Request                                                                    URL
https://ns202477.ovh.net/openam/UI/Login?forward=true&realm=%2Fasip&goto=%2FSSOSoap
%2FmetaAlias%2Fasip%2Fidp%3FReqID%3Da3c88b0h1j8jg15f16e6a141he2ffi5&spEntityID=mss-
msg-services
Request HTTP Body {}

HTTP/1.1 200 OK
Cache-Control: private
Pragma: no-cache
Expires: 0
X-DSAMEVersion: OpenAM 10.1.0-Xpress (2013-February-07 15:45)
AM_CLIENT_TYPE: genericHTML
X-AuthErrorCode: 0
Set-Cookie:
iPlanetDirectoryPro=AQIC5wM2LY4SfcyQn5K2wvViX1K61npjcQ3OIy6ZufCPPRE.*AAJTSQACMDEAAl
NLABQtMzIyOTg3MDg1MjUwMjE3MzU5NQ..*; Domain=.ovh.net; Path=/
Set-Cookie: AMAuthCookie=LOGOUT; Domain=.ovh.net; Expires=Thu, 01-Jan-1970 00:00:10
GMT; Path=/
Content-Type: text/xml;charset=utf-8
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 2774
Connection: close
Response String:
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
   <soap-env:Header />
   <soap-env:Body>
      <samlp:Response             xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="s299271fafc0dab6838bf13ef5ddbd3d46a37b8fef"
InResponseTo="a3c88b0h1j8jg15f16e6a141he2ffi5" Version="2.0" IssueInstant="2013-09-
24T09:12:55Z"                    Destination="https://ns202477.ovh.net:444/mss-msg-
services/saml/SSO/alias/defaultAlias">
```

```
         <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://ns202477.ovh.net:443/ope
nam</saml:Issuer>
         <samlp:Status>
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
         </samlp:Status>
         <saml:Assertion          xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="s2903125cdd9f4d397e5093a595fdc2c9c9f5b9ba6"  IssueInstant="2013-09-24T09:12:55Z"
Version="2.0">
            <saml:Issuer>https://ns202477.ovh.net:443/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="#s2903125cdd9f4d397e5093a595fdc2c9c9f5b9ba6">
                     <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>6H/N01pqFsjSK8KPVzzzLqjBSMY=</ds:DigestValue>
                  </ds:Reference>
               </ds:SignedInfo>
               <ds:SignatureValue>

JdrAah7J8IAZjyGnby/LKPfdAeQGqhcnUcALoqolj5oUlfg2StLziqkvU5cZAigMjGNbNVOCRwtx

ayyXKalunquDE2CfwVkKNBdbo7nD12iWrthMXDiNrXWN5nTTla82YnmnBSEcrpVOmnQAET1Bii3V

3fzYtI88TLKu5jXELEiTku+D7eqO8ujluH+dWJN8TJsu3PeJg05/FaVPG2yh8np/ujUehmTkzxjo

Kt5M2T6AuKOv6bq70G8wliPevbz9JeezDb7NNWYm5TPjFgWuWmwg9h++1K/bzG5TOcF5jbw2/8/F
                           FfHQBgdu5OPOCCAXqp+nTbsOoNeQhVYiYEuddg==
                        </ds:SignatureValue>
               <ds:KeyInfo>
                  <ds:X509Data>
                     <ds:X509Certificate>

      MIIEnjCCAoagAwIBAgIBBTANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJGUjEPMA0GA1UECAwG

      RnJhbmNlMQ4wDAYDVQQHDAVQQXJpczESMBAGA1UECgwJQ2FwZ2VtaW5pMRcwFQYDVQQDDA5DYXBn

      ZW1pbmkgRGVtbzAeFw0xMzA4MDkxMjI2MjNaFw0xNDA4MDkxMjI2MjNaME0xCzAJBgNVBAYTAkZS

      MQ8wDQYDVQQIDAZGcmFuY2UxEjAQBgNVBAoMCUNhcGdlbWluaTEZMBcGA1UEAwwQbnMyMDI0Nzcu

      b3ZoLm5ldDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMeNH2F8A2r3kwiwXdWMmR+/

      0vFCSQqb29RbSONDM7rtyUmMT5NlpLnVKQkEJfKQubG3HPMVLkaCT3rdOuV5tujZGR56Ew/jHGFi

      /p+6bJz4Lm229nRe85SPzvcerYaD2VwPE5k6CwLMifQv1eDcI/2J+LRGKhgD7H2A54zIyUKcRN5D

      RE7nlviMQr4NS8DPLWJjkZjNnXJUR3ZhLgLmLAbg+ElkNfRxOQo45EQgw7GMeqMbzXaewHVGVGt/

      TY3AQhD2laaO5vtlAsdI/k2nex9QPBjb29E0rbRFm6SUklGgGlgT65dF+J2zbeN5War7zHbsTJUX

      MkWuxcJvorUYKfECAwEAAaN7MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBH

      ZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFB8h9PzL5h7bbfO0deUxlLGDoY4GMB8GA1Ud

      IwQYMBaAFCymCnuDqdBd7cLl+XM46VwEi6hAMA0GCSqGSIb3DQEBBQUAA4ICAQCcpejiBjmzqaYl

      rJwS1FvTDpY7sweyYofMYI1HEqZhKKn/WNNEHw4cs/i0NCEmGSbj3nTJmptnziIkpE2Kjfh2jU+0

      UYnpTKYGeDdbc8f7KiAcyGpPDzy4PBHx2KAC+grWqVq3voodNUesfgrl3kbiE64Vlz7G1GQLlTFB
```

```
      EVfwQnEFSnpQMLtODWuTfg6RnMpQJYXIHUD6wIl8uNgehGpdJhLG/athXfKf3MVAfx2xV1KeylEj

      lMauBFZ+fwjtNEbbqkDtlWnah2+bJUmN26ZvrNI0cO4enP6b/XomYHMPE1NC2zsBCBHFkBnGN3YI

      YkPsMarrXgHE7TEUWRnkbUP0/Y6vqgzPL3PgESpL8o5DHLWSZE1iwvJzf22CEzkQOAbGxkfzswas

      JX195bYrx4a2WmRua6BErN9VwniqvufLMg8ZlFqGPtxQRGISl7pYhmcWtrmOTLjE3js8ezpuMf5j

      /MWElgO3EQoxPBnMJ5zvoCnV205CRiaOKbO78LAudtPdB2rn62avqXnPFrzg8sCNlHuQgpe7qe7c

      M9Qum9oVUSKi3aWhVcvy+/0gUHUQArCzUPkzdLZnpAn7+8qE8U1+j2ny+R4XI8z+cTncY3pzuCTb

      0tDF6qyhiMInFTMoy87DvPRAuRXaqFVIwrWuhrupRVEGwKUoIH6vuhsVcwU9sA==
                                  </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://ns202477.ovh.net:443/openam">1827364559</saml:NameID>
            <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
               <saml:SubjectConfirmationData
InResponseTo="a3c88b0h1j8jg15f16e6a141he2ffi5"   NotOnOrAfter="2013-09-24T09:22:55Z"
Recipient="https://ns202477.ovh.net:444/mss-msg-
services/saml/SSO/alias/defaultAlias" />
            </saml:SubjectConfirmation>
         </saml:Subject>
         <saml:Conditions  NotBefore="2013-09-24T09:02:55Z"  NotOnOrAfter="2013-
09-24T09:22:55Z">
            <saml:AudienceRestriction>
               <saml:Audience>mss-msg-services</saml:Audience>
            </saml:AudienceRestriction>
         </saml:Conditions>
         <saml:AuthnStatement                AuthnInstant="2013-09-24T09:12:55Z"
SessionIndex="s2a98de75d4f78c01f2537dee3a593c72a7f7e7701">
            <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtected
Transport</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">Jean</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">1827364559</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">Radiologue</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">T1</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">Dupont</saml:AttributeValue>
            </saml:Attribute>
```

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



/!\ ETAPE#4 : Parser AuthRequest /!\
AssertionConsumerServiceURL="https://ns202477.ovh.net:444/mss-msg-
services/saml/SSO/alias/defaultAlias"



/!\ ETAPE#5 : Valider Assertion SAML /!\
POST /mss-msg-services/saml/SSO/alias/defaultAlias HTTP/1.1
Host: ns202477.ovh.net:444
PAOS:                                                ver='urn:liberty:paos:2003-08';
'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'
Content-Type: application/vnd.paos+xml
Accept: application/json, application/vnd.paos+xml
Accept-Language: fr;q=1, en;q=0.9, de;q=0.8, ja;q=0.7, nl;q=0.6, it;q=0.5
Connection: keep-alive
Cookie: JSESSIONID=42CE4C4B825BA68CAC765772ED9D9866; Path=/mss-msg-services;
Accept-Encoding: gzip, deflate
Content-Length: 5946
NUMHOMOLOGATION: APPMOBILE
User-Agent: MSSante/1.0 (iPhone; iOS 6.1.4; Scale/2.00)
Request HTTP Body
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
   <soap-env:Header />
   <soap-env:Body>
      <samlp:Response            xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="s299271fafc0dab6838bf13ef5ddbd3d46a37b8fef"
InResponseTo="a3c88b0h1j8jg15f16e6a141he2ffi5" Version="2.0" IssueInstant="2013-09-
24T09:12:55Z"                    Destination="https://ns202477.ovh.net:444/mss-msg-
services/saml/SSO/alias/defaultAlias">
         <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://ns202477.ovh.net:443/ope
nam</saml:Issuer>
         <samlp:Status>
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
         </samlp:Status>
         <saml:Assertion          xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="s2903125cdd9f4d397e5093a595fdc2c9c9f5b9ba6"  IssueInstant="2013-09-24T09:12:55Z"
Version="2.0">
            <saml:Issuer>https://ns202477.ovh.net:443/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="#s2903125cdd9f4d397e5093a595fdc2c9c9f5b9ba6">
                     <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>6H/N01pqFsjSK8KPVzzzLqjBSMY=</ds:DigestValue>
                  </ds:Reference>
               </ds:SignedInfo>
               <ds:SignatureValue>

JdrAah7J8IAZjyGnby/LKPfdAeQGqhcnUcALoqolj5oUlfg2StLziqkvU5cZAigMjGNbNVOCRwtx
```

```
ayyXKalunquDE2CfwVkKNBdbo7nD12iWrthMXDiNrXWN5nTTla82YnmnBSEcrpVOmnQAET1Bii3V

3fzYtI88TLKu5jXELEiTku+D7eqO8ujluH+dWJN8TJsu3PeJg05/FaVPG2yh8np/ujUehmTkzxjo

Kt5M2T6AuKOv6bq70G8wliPevbz9JeezDb7NNWYm5TPjFgWuWmwg9h++1K/bzG5TOcF5jbw2/8/F
                          FfHQBgdu5OPOCCAXqp+nTbsOoNeQhVYiYEuddg==
                       </ds:SignatureValue>
                <ds:KeyInfo>
                   <ds:X509Data>
                      <ds:X509Certificate>

       MIIEnjCCAoagAwIBAgIBBTANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJGUjEPMA0GA1UECAwG

       RnJhbmNlMQ4wDAYDVQQHDAVQQXJpczESMBAGA1UECgwJQ2FwZ2VtaW5pMRcwFQYDVQQDDA5DYXBn

       ZW1pbmkgRGVtbzAeFw0xMzA4MDkxMjI2MjNaFw0xNDA4MDkxMjI2MjNaME0xCzAJBgNVBAYTAkZS

       MQ8wDQYDVQQIDAZGcmFuY2UxEjAQBgNVBAoMCUNhcGdlbWluaTEZMBcGA1UEAwwQbnMyMDI0Nzcu

       b3ZoLm5ldDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMeNH2F8A2r3kwiwXdWMmR+/

       0vFCSQqb29RbSONDM7rtyUmMT5NlpLnVKQkEJfKQubG3HPMVLkaCT3rdOuV5tujZGR56Ew/jHGFi

       /p+6bJz4Lm229nRe85SPzvcerYaD2VwPE5k6CwLMifQv1eDcI/2J+LRGKhgD7H2A54zIyUKcRN5D

       RE7nlviMQr4NS8DPLWJjkZjNnXJUR3ZhLgLmLAbg+ElkNfRxOQo45EQgw7GMeqMbzXaewHVGVGt/

       TY3AQhD2laaO5vtlAsdI/k2nex9QPBjb29E0rbRFm6SUklGgGlgT65dF+J2zbeN5War7zHbsTJUX

       MkWuxcJvorUYKfECAwEAAaN7MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBH

       ZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFB8h9PzL5h7bbfO0deUxlLGDoY4GMB8GA1Ud

       IwQYMBaAFCymCnuDqdBd7cLl+XM46VwEi6hAMA0GCSqGSIb3DQEBBQUAA4ICAQCcpejiBjmzqaYl

       rJwS1FvTDpY7sweyYofMYI1HEqZhKKn/WNNEHw4cs/i0NCEmGSbj3nTJmptnziIkpE2Kjfh2jU+0

       UYnpTKYGeDdbc8f7KiAcyGpPDzy4PBHx2KAC+grWqVq3voodNUesfgrl3kbiE64Vlz7G1GQLlTFB

       EVfwQnEFSnpQMLtODWuTfg6RnMpQJYXIHUD6wIl8uNgehGpdJhLG/athXfKf3MVAfx2xV1KeylEj

       lMauBFZ+fwjtNEbbqkDtlWnah2+bJUmN26ZvrNI0cO4enP6b/XomYHMPE1NC2zsBCBHFkBnGN3YI

       YkPsMarrXgHE7TEUWRnkbUP0/Y6vqgzPL3PgESpL8o5DHLWSZE1iwvJzf22CEzkQOAbGxkfzswas

       JX195bYrx4a2WmRua6BErN9VwniqvufLMg8ZlFqGPtxQRGISl7pYhmcWtrmOTLjE3js8ezpuMf5j

       /MWElgO3EQoxPBnMJ5zvoCnV205CRiaOKbO78LAudtPdB2rn62avqXnPFrzg8sCNlHuQgpe7qe7c

       M9Qum9oVUSKi3aWhVcvy+/0gUHUQArCzUPkzdLZnpAn7+8qE8U1+j2ny+R4XI8z+cTncY3pzuCTb

       0tDF6qyhiMInFTMoy87DvPRAuRXaqFVIwrWuhrupRVEGwKUoIH6vuhsVcwU9sA==
                                  </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://ns202477.ovh.net:443/openam">1827364559</saml:NameID>
                <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
InResponseTo="a3c88b0h1j8jg15f16e6a141he2ffi5"   NotOnOrAfter="2013-09-24T09:22:55Z"
Recipient="https://ns202477.ovh.net:444/mss-msg-
services/saml/SSO/alias/defaultAlias" />
                </saml:SubjectConfirmation>
             </saml:Subject>
```

```
            <saml:Conditions  NotBefore="2013-09-24T09:02:55Z"  NotOnOrAfter="2013-
09-24T09:22:55Z">
               <saml:AudienceRestriction>
                  <saml:Audience>mss-msg-services</saml:Audience>
               </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:AuthnStatement                AuthnInstant="2013-09-24T09:12:55Z"
SessionIndex="s2a98de75d4f78c01f2537dee3a593c72a7f7e7701">
               <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtected
Transport</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">Jean</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">1827364559</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">Radiologue</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">T1</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">Dupont</saml:AttributeValue>
               </saml:Attribute>
            </saml:AttributeStatement>
         </saml:Assertion>
      </samlp:Response>
   </soap-env:Body>
</soap-env:Envelope>

HTTP/1.1 302 Déplacé Temporairement
Location:                                    https://ns202477.ovh.net:444/mss-msg-
services/services/Annuaire/rest/v1/listEmails
Content-Length: 0
Connection: close



/!\ ETAPE#6 : Appeler le service initial /!\-
POST /mss-msg-services/services/Annuaire/rest/v1/listEmails HTTP/1.1
Host: ns202477.ovh.net:444
PAOS:                                                ver='urn:liberty:paos:2003-08';
'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'
Content-Type: application/json
Accept: application/json, application/vnd.paos+xml
Accept-Language: fr;q=1, en;q=0.9, de;q=0.8, ja;q=0.7, nl;q=0.6, it;q=0.5
Connection: keep-alive
Cookie: JSESSIONID=42CE4C4B825BA68CAC765772ED9D9866; Path=/mss-msg-services;
Accept-Encoding: gzip, deflate
Content-Length: 59
NUMHOMOLOGATION: APPMOBILE
User-Agent: MSSante/1.0 (iPhone; iOS 6.1.4; Scale/2.00)
Request HTTP Body
{
```

```
       "listEmailsInput":
       {
              "userId":"1827364559"
       }
}

--ae34d534-F--
HTTP/1.1 200 OK
Content-Type: application/json;charset=utf-8
Connection: close
Transfer-Encoding: chunked


==========================================================================
```

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté

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