VERSION
1.0.0

PROJETS / SERVICES

Guide de mise en œuvre de la MSSanté et de l'alimentation du DMP dans un logiciel de professionnel de santé

Guide à l'attention des éditeurs - **V1.0.0** - mars 2016

AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Classification
Non sensible / Public

Historique du document		
Version	Date	Commentaires
V1.0.0	23/03/2016	Version initiale.

Sommaire

1 Introduction

1.1 Objet du document

Dans le cadre des missions qui lui sont confiées visant à structurer et soutenir le développement de la santé numérique, l'ASIP Santé a développé deux services d'infrastructure, le Dossier Médical Partagé[1] (DMP) et le système des messageries sécurisées de santé (MSSanté), tous deux destinés à fluidifier la coordination des soins.

Le DMP permet la mise en partage de documents de santé et la MSSanté permet l'échange sécurisé d'informations et de documents de santé entre professionnels de santé (PS).

Afin de renforcer la complémentarité de ces deux services, l'ASIP Santé souhaite faciliter au maximum la mise en œuvre de la fonction d'alimentation du DMP lors de l'envoi d'un message MSSanté.

Le présent guide vise à aider les éditeurs de logiciels de professionnel de santé (LPS) à identifier les développements à réaliser pour implémenter les fonctions d'alimentation du DMP lors de l'envoi par un professionnel de santé d'un message MSSanté contenant un document de santé en pièce jointe.

Ce document ne constitue pas une spécification fonctionnelle et technique, mais un guide d'appui à la mise en œuvre de nouvelles fonctionnalités pour les LPS.

1.2 Aide à la lecture

Ce guide est destiné aux décideurs et aux techniciens des éditeurs de logiciels de professionnels de santé afin qu'ils puissent débuter les développements dans leurs logiciels.

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

- le chapitre 2 rappelle les fondamentaux des services DMP et MSSanté ;
- le chapitre 3 introduit les enjeux et les principes d'un logiciel de professionnel de santé ;
- le chapitre 4 présente les mécanismes techniques du système DMP ;
- le chapitre 5 présente les mécanismes techniques du système MSSanté ;
- le chapitre 6 présente les différences entre les mécanismes techniques et les contraintes des deux systèmes ;
- le chapitre 7 présente un exemple d'implémentation de LPS offrant la possibilité de mettre en partage un document dans le DMP lors de son envoi par MSSanté ;
- le chapitre 8 est un glossaire des abréviations utilisées dans ce document ;
- le chapitre 9 regroupe les annexes.

Selon son profil, le lecteur pourra se concentrer sur certains chapitres spécifiques. Les chapitres 2 et 3 sont principalement destinés aux décideurs et directeurs de projet. Les chapitres 4, 5, 6 et 7 sont plutôt destinés aux directeurs techniques, chefs de projets, développeurs et architectes logiciels. Les personnes ayant une bonne connaissance des systèmes DMP et MSSanté peuvent directement consulter les chapitres 6 et 7

[1] La Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé renomme le « dossier médical personnel » en « dossier médical partagé »

2 Rappel sur les fondamentaux des systèmes DMP et MSSanté

URL des sites d'information de référence
[DMP-URL-INFO] http://www.dmp.gouv.fr [MSS-URL-INFO] https://www.msssante.fr

2.1 Le DMP

Améliorer la coordination des soins

Le DMP a été institué par la loi pour :

- faciliter la coordination des soins entre PS et entre les secteurs ville/hôpital ;
- respecter le droit du patient à être informé sur son état de santé.

Face aux défis majeurs que représentent notamment le vieillissement de la population et le développement des maladies chroniques, le Dossier Médical Partagé est un **outil moderne et performant qui permet d'améliorer la coordination, la qualité et la continuité des soins pour tous** grâce à la traçabilité de l'information (l'historique médical est nécessaire au médecin pour la prise en charge du patient), à une meilleure communication médecin/malade, et à la transmission des informations entre professionnels de santé.

Fiabiliser le parcours de soins et les pratiques pluridisciplinaires

Le DMP ne remplace pas le dossier du professionnel de santé. Il contient les informations importantes produites lors du parcours de soins du patient et conservées dans les dossiers des professionnels de santé. A ce titre, le DMP permet de fiabiliser le parcours de soins et les pratiques pluridisciplinaires. Il contribue également à soutenir la décision diagnostique et thérapeutique en garantissant une disponibilité des informations au moment utile et en favorisant une structuration de ces informations pour les rendre plus aisément exploitables.

Interopérabilité

Le DMP contient des documents conformes au cadre d'interopérabilité des systèmes d'information de santé (CI-SIS) qui permet d'assurer l'**interopérabilité** entre les systèmes d'information.

Typologie des documents

Les documents **contenus dans le** DMP sont organisés selon **8 espaces** :

- **synthèses ;**
- **traitements et soins ;**
- **comptes rendus ;**
- **imagerie médicale ;**
- **analyse, biologie ;**
- **prévention ;**
- **certificats, déclarations ;**
- **espace perso, documents ajoutés par le patient.**

Figure 1 : les 8 espaces du DMP

2.2 Le système des messageries sécurisées de santé MSSanté

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

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

- sécurité : l'utilisation d'une messagerie sécurisée de santé doit assurer la confidentialité des données de santé à caractère personnel échangées ;
- universalité : tous les professionnels habilités à échanger des données de santé, quels que soient leurs modes d'exercice, doivent être en capacité de disposer d'un compte de messagerie sécurisée permettant d'échanger avec tous les professionnels habilités, quels que soient les outils utilisés (logiciels métier, webmail, application mobile, client de messagerie standard …) ;
- simplicité : l'émission et la consultation des messages sécurisées ne modifient pas les pratiques habituelles des autres outils de messageries, y compris en mobilité.

MSSanté est le nom donné au système mis en place par les pouvoirs publics avec l'ensemble des Ordres professionnels afin de développer les messageries sécurisées de santé.

Le système MSSanté permet ainsi :

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

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

- un annuaire national MSSanté s'appuyant notamment sur le répertoire partagé des professionnels de santé (RPPS) et ayant vocation à référencer l'ensemble des professionnels habilités à échanger des données de santé personnelles ;
- une liste blanche de domaines qui regroupe l'ensemble des domaines de messageries des opérateurs autorisés à échanger dans l'espace de confiance MSSanté ;
- un référentiel permettant aux industriels de développer des offres conformes et interopérables entre elles.

2.3 L'échange et le partage d'information médicale

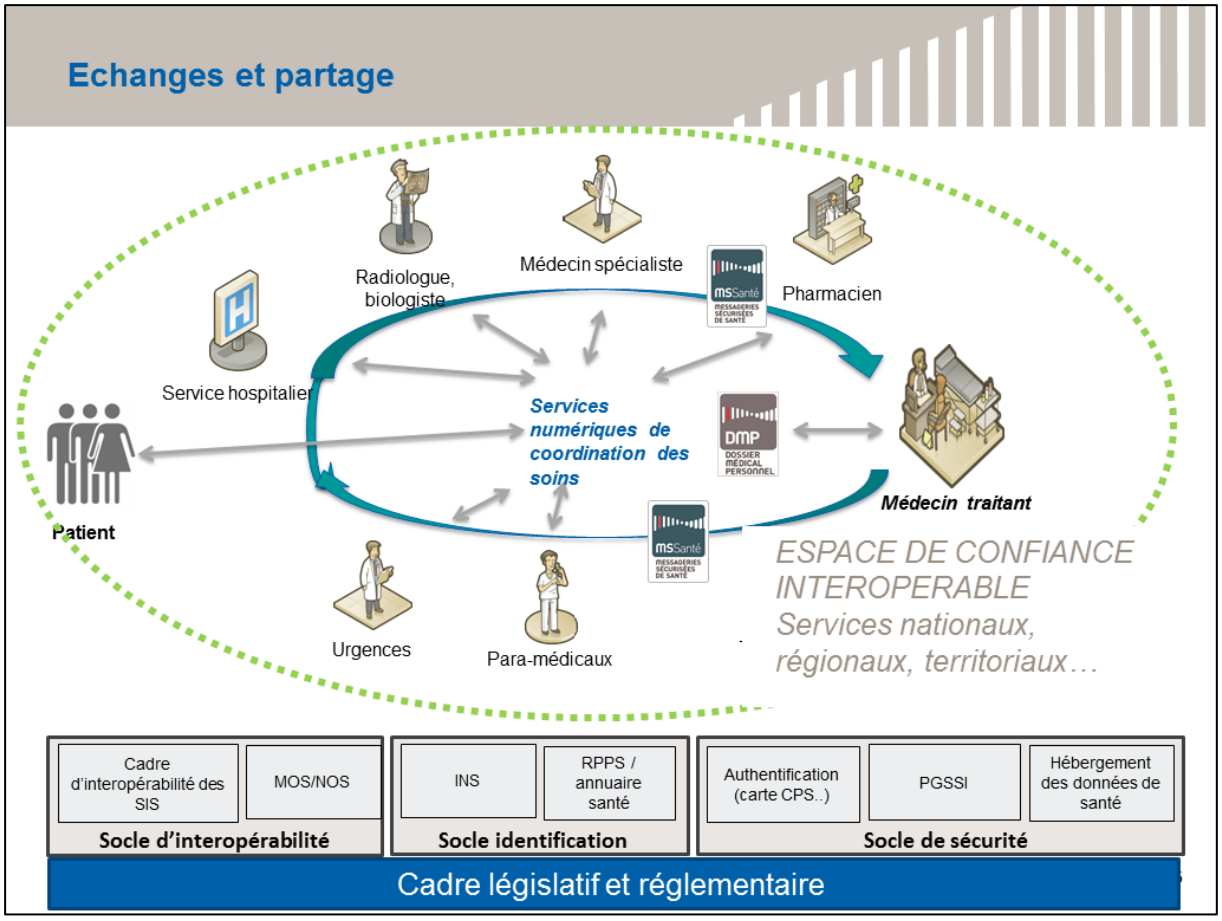

Figure 2 : l'échange et le partage d'information médicale

Selon son usage et son besoin, un PS peut souhaiter :

1. Echanger un message avec un autre PS via un message MSSanté ;
2. Echanger un document de santé avec un autre PS en lui envoyant un message MSSanté contenant en pièce jointe un document de santé ;
3. Partager un document de santé avec les autres PS et le patient en le déposant dans le DMP de son patient ;
4. **Echanger un document de santé avec un autre PS en lui envoyant un message MSSanté contenant en pièce jointe un document de santé et partager ce même document de santé avec les autres PS en le déposant dans le DMP de son patient.**

Ce guide a pour objectif de fournir des indications permettant aux éditeurs d'intégrer au mieux dans leur LPS le 4ème cas d'usage décrit afin que l'ergonomie soit la plus fluide possible pour l'utilisateur.

3 Principes et enjeux des logiciels de professionnels de santé

3.1 De la production de soins au parcours de soins

Les systèmes d'information de santé (SIS) doivent apporter une réponse adaptée aux besoins des professionnels et établissements de santé et du système de santé dans son ensemble, au service de la qualité de prise en charge des patients.

Jusqu'à présent, la première priorité était de mettre à la disposition de chaque acteur un logiciel adapté à son activité médicale ou de soins et supportant sa pratique. Aujourd'hui, l'enjeu est d'outiller efficacement et de manière interopérable la coordination des différents acteurs (structures de soins et professionnels de santé) intervenant dans le parcours de soins des patients, dans un contexte où les maladies chroniques et les pluri-pathologies sont de plus en plus fréquentes.

Les professionnels de santé doivent pouvoir s'appuyer sur des logiciels métier à forte valeur ajoutée, adaptés aux nouveaux contextes d'exercice : mobilité, prise en charge pluridisciplinaire, échanges, etc. Au-delà des fonctionnalités de production de soins (dossier patient, prescriptions, planification des soins…), ces logiciels métiers doivent intégrer de nouvelles fonctionnalités au service du suivi et de la coordination des parcours de soins : recueil des informations cliniques essentielles, communication immédiate avec les autres professionnels de santé, accès direct aux bonnes pratiques selon les situations cliniques via l'exploitation automatique des informations médicales codées dans le dossier patient, programmation multi-acteurs des séquences de prises en charge…

Dans le présent document, le terme LPS (logiciel de professionnel de santé) désigne tout logiciel métier ou système d'information utilisé par un professionnel de santé ou une structure de soins, pour l'assister dans la gestion de la prise en charge de ses patients. Outre les fonctions de gestion, de comptabilité, d'agenda, etc., un LPS produit, gère, reçoit, émet et/ou stocke des données de santé à caractère personnel concernant les patients pris en charge par le PS ou la structure de soins.

Le terme LPS recouvre les logiciels de gestion de cabinet (LGC), les logiciels des structures de soins primaires (maisons et centres de santé – SI-MCS), les systèmes d'information hospitaliers (SIH) et de manière plus générale tout logiciel utilisé par un professionnel de santé.

3.2 Parcours de soins

Pour les éditeurs de LPS, le fait d'améliorer la coordination des soins est une véritable opportunité de créer de la valeur pour leurs clients.

Pour répondre à ce besoin, les LPS doivent être DMP-compatibles et intégrer la MSSanté. Un logiciel DMP compatible et intégrant la MSSanté permet de mobiliser 2 grandes fonctionnalités :

1. **L'échange de documents par messagerie sécurisée de santé** compatible avec le système MSSanté. Ainsi, les documents peuvent être :
    - envoyés de façon simple, rapide et sécurisée à un ou plusieurs PS impliqués dans la prise en charge du patient ;
    - récupérés de façon simple, rapide et sécurisée par les PS impliqués dans la prise en charge du patient.
2. **Le partage des documents dans le DMP**. Grâce au DMP les documents peuvent être :
    - mis à la disposition de tous les PS qui pourraient avoir besoin d'y accéder (notamment en dehors d'une prise en charge programmée), en particulier le médecin traitant ;
    - mis à la disposition du patient.

Pour ces 2 fonctionnalités, les documents de santé doivent (DMP) et peuvent (MSSanté) être conformes à la norme CDA-R2 défini dans le CI-SIS. Si ces documents CDA-R2 sont structurés de niveau 3 (chaque donnée est structurée), ces documents pourront être :

- interprétés par les logiciels de nouvelle génération pour offrir des services à valeur ajoutée au PS (tri, courbes, alertes, etc.) ;
- utilisés pour alimenter automatiquement d'autres documents (par exemple une synthèse médicale ou un document de sortie);
- exploités à des fins de pilotage et d'observation.

4 Le système DMP

Documents de référence
[DMP-DSFT] Dossier de Spécifications Fonctionnelles et Techniques des interfaces DMP des LPS.
[DMP-ARCHI] Urbanisation : Architectures systèmes éligibles aux échanges avec le DMP.
[CI-TR-CLIL-RO] CI-SIS – Transport : Volet Transport Synchrone pour Client Lourd.
[CI-PARTAGE] – Service : Volet Partage de Documents de Santé
[CI-STRU-ENTETE] – Contenu : Volet Structuration Minimale de Documents Médicaux

4.1 Fonctionnement du système DMP

4.1.1 Présentation générale du système DMP

Le système DMP est un service en ligne promu par l'ASIP Santé afin de permettre le partage de données de santé. Il est mis à disposition :

- des patients, via l'accès Web patient accessible par internet
- des professionnels de santé :
    - **via l'accès Web PS** (professionnel de santé) accessible par internet à tout professionnel de santé disposant d'une carte CPS (sous certaines conditions de configuration du poste de travail) **;**
    - **via un accès direct (via Web services) depuis le logiciel métier du professionnel de santé (LPS), à condition qu'il soit « DMP-compatible »** : c'est le mode le plus adapté pour le professionnel de santé car le DMP est intégré dans son logiciel habituel.

Le document [DMP-DSFT] décrit les interfaces proposées par le service DMP que les éditeurs de LPS doivent mettre en œuvre afin que leurs produits puissent accéder au DMP et devenir DMP-compatibles. Un processus d'homologation décrit dans [DMP-DSFT] a été mis en place par l'ASIP Santé pour vérifier la DMP Compatibilité des LPS.

Le présent guide se focalise principalement sur l'interface 'Web services' mise à disposition des LPS.

4.1.2 Les interfaces « Web services »

Le DMP offre des interfaces qui s'appuient sur l'usage de la technologie SOAP, en se basant principalement sur les profils définis dans le cadre d'interopérabilité des systèmes d'information de santé (CI-SIS).

Ce dernier repose principalement sur une adaptation au contexte des SIS français de profils et normes internationales (IHE, HL7, SAML), ce qui permet aux éditeurs de LPS et aux promoteurs de services de capitaliser sur des développements, et de réutiliser ceux-ci en dehors d'un contexte purement DMP.

De plus, le DMP offre quelques services spécifiques, hors CI-SIS (gestion des autorisations sur les dossiers, par exemple).

4.1.3 Les mécanismes d'authentification

Conformément au CI-SIS, l'authentification des utilisateurs repose sur des mécanismes d'échange entre :

- un système initiateur, qui est le LPS (le LPS peut éventuellement être constitué du poste de l'utilisateur final et d'un système tiers) utilisé par l'utilisateur final ;
- un système cible, en l'occurrence le DMP.

L'accès au DMP peut se faire selon deux types de configuration :

- une configuration en authentification directe, qui se fonde sur l'usage des cartes CPS ou CPE délivrées aux utilisateurs finaux ;
- une configuration en authentification indirecte, qui se fonde sur l'usage de certificats logiciels de l'IGC CPS délivrés à une structure de soins, au sein de laquelle les utilisateurs finaux s'authentifient.

Comme les cartes CPx, les certificats logiciels attribués à une structure utilisés en authentification indirecte sont délivrés par l'ASIP Santé et rattachés à l'IGC CPS. Les mécanismes d'identification et d'authentification mis en œuvre reposent pour une configuration en authentification directe ou indirecte, sur :

- l'établissement d'une session TLS avec authentification mutuelle entre le système initiateur et le système cible ;
    - en utilisant le certificat de la carte CPx de l'utilisateur, en authentification directe ;
    - en utilisant un certificat logiciel délivré à l'établissement, en authentification indirecte ;
- l'envoi par le système initiateur d'une assertion SAML 2.0 (nommée jeton VIHF) contenant l'ensemble des éléments d'identification de l'utilisateur et éventuellement de l'établissement, le numéro d'homologation du logiciel ainsi que le mode d'accès retenu (normal, bris de glace, centre de régulation).

Le contrôle d'accès aux différents services offerts par le DMP se fait sur la base :

- du mode d'authentification utilisé ;
- des éléments fournis par le système initiateur (éventuellement par un système tiers) dans le VIHF (identité du PS, de l'établissement ou du système tiers, identité du patient, numéro d'homologation du logiciel) ;
- du consentement du patient concernant l'accès à ses données personnelles, qui est recueilli par l'acteur de santé et enregistré au sein du DMP.

Avec ces éléments, le SI DMP applique des règles de gestion (médecin traitant, matrice d'habilitation selon la profession…) pour déterminer les droits d'accès au DMP et aux documents contenus.

4.1.4 Signature et imputabilité des échanges

La signature électronique est un procédé qui permet de s'assurer de l'intégrité d'un fichier numérique et d'établir un lien avec l'auteur de la signature, sur la base de l'usage d'un certificat X509.

Sur le DMP, la signature du jeton VIHF est requise pour le mode d'authentification indirecte. Elle n'est pas requise pour l'authentification directe, mais est acceptée.

La signature est de type XmlDSig et intégrée au jeton en respectant le standard SAML 2.0.

Pour le mode d'authentification indirecte, la signature du VIHF est faite en utilisant un certificat de signature de personne morale, qui est distinct du certificat utilisé pour l'établissement de l'authentification (dont l'usage est dédié à l'authentification).

Afin d'assurer l'imputabilité du dépôt des documents alimentant le système DMP, il est également requis de signer les lots de soumission, en utilisant une signature de type XAdES quel que soit le mode d'authentification utilisé.

La signature des documents CDA-R2 (voir $4.1.7) alimentant le DMP n'est pas requise, mais les documents signés sont acceptés (signature de type XAdES englobante).

Les certificats de signature utilisés dans ce cadre sont distribués par l'ASIP Santé et rattachés à l'IGC CPS.

4.1.5 Modèles d'architectures possibles pour l'accès au DMP

Le document « Architectures éligibles aux échanges avec le DMP » [DMP-ARCHI] a pour objet de présenter des modèles d'architectures types pour les systèmes accédant au DMP. Ces différents modèles sont présentés avec à chaque fois leurs avantages, contraintes et limitations.

La mise en œuvre de ces architectures doit être accompagnée de mesures de sécurité appropriées. Il faut ainsi assurer la confidentialité des données échangées avec le DMP, et la protection de l'accès aux clés privées des utilisateurs. Ces aspects sécuritaires sont plus particulièrement sensibles pour des architectures en mode SaaS sur internet.

4.1.6 Profil IHE XDS.b

4.1.6.1 Principes

La gestion des documents du DMP et de leurs métadonnées est implémentée par le profil IHE XDS.b, décrit dans le document [CI-PARTAGE]. Dans la version actuelle du DMP, les Classeurs (Folders) ne sont pas supportés.

D'un point de vue IHE, les acteurs entrant en ligne de compte sont :

- repository XDS.b : entrepôt de stockage des documents, utilisé dans l'alimentation et la consultation des documents du DMP ;
- registry XDS.b : registre d'indexation des métadonnées des documents, utilisé dans la recherche et l'extraction des métadonnées des documents du DMP ;
- le LPS : Document Source (émetteur de document), Document Consumer (utilisateur de document), Document Administrator.

Bien qu'ils soient disponibles sur deux endpoints SOAP différents, les deux acteurs repository et registry doivent être vus « groupés » comme un seul acteur technique du point de vue du LPS :

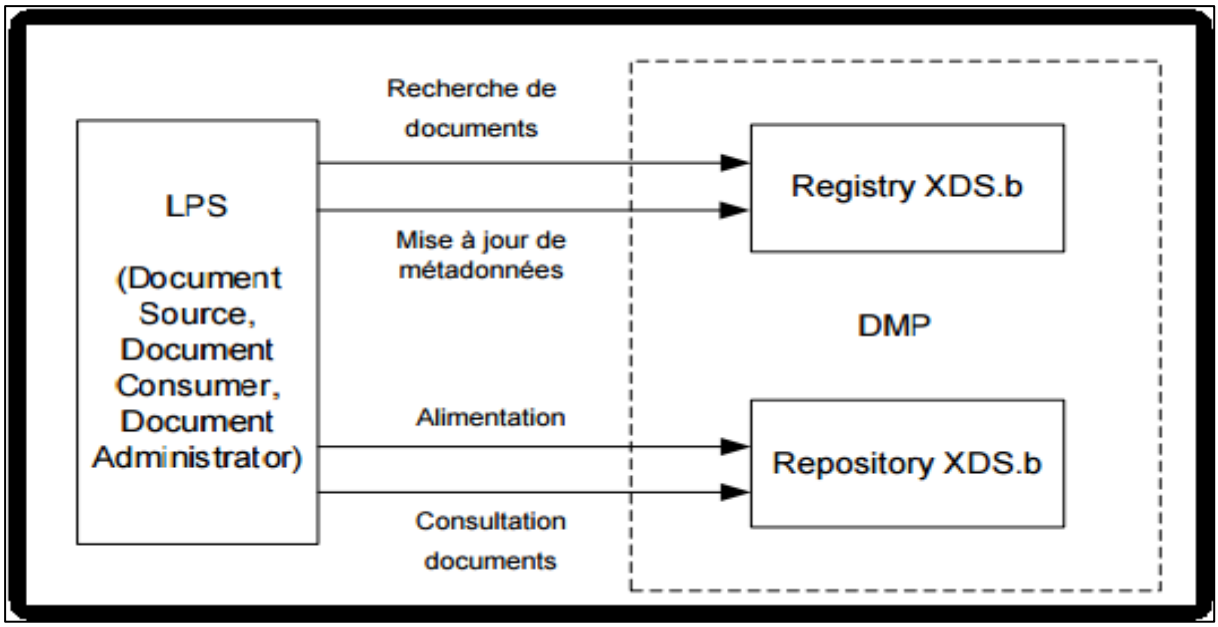

Figure 3 : Schéma de principe des acteurs XDS

4.1.6.2 Métadonnées XDS d'un document

Documents de référence
[CI-PARTAGE] CI-SIS – Couche Service– Volet Partage de documents de santé
[CI-ANX-CDA] CI-SIS – Couche Contenu - annexe **« Liens entre en-tête CDA et métadonnées »**

La mise en partage de ces documents nécessite la gestion de métadonnées (documents et lots de soumission) via le profil IHE XDS.b. Les métadonnées XDS (ebXML) du document et du lot soumis sur l'entrepôt XDS sont indexées dans le registre XDS : elles servent aux opérations de recherche, de sélection et d'extraction de documents par les PS et permettent aussi d'organiser les documents selon différents axes de classement.

Certaines métadonnées sont déductibles :

- du document CDA (profession, spécialité…) : le document [CI-ANX-CDA] définit la correspondance entre le CDA R2 et les métadonnées XDS ;
- de données éventuellement stockées dans le LPS (titre du document, date de l'acte médical documenté, type du document…) ;
- du support d'authentification (carte CPS, certificat logiciel pour personne morale) ;
- **des données saisies par l'utilisateur : la confidentialité du document (masquage aux PS, invisible au patient)[2] via la métadonnée XDS « confidentialityCode » est obligatoire pour la mise en partage dans le DMP.**

[2] Confidentialité du document, 3 possibilités :

1. Document visible par les professionnels de santé autorisés à accéder aux documents du DMP du patient (selon le filtre de la matrice d'habilitation)
2. Document masqué aux professionnels de santé : document visible uniquement par son auteur, les médecins traitants et le patient
3. Document non visible par le patient : document qui nécessite une information préalable du patient par un professionnel de santé (consultation d'annonce)

Le document [CI-PARTAGE] donne une indication sur l'origine possible de chaque métadonnée.

Le LPS doit assurer la cohérence entre les métadonnées XDS du document et celles de l'entête du document HL7 CDA R2.

Auteur d'un document et PS qui dépose le document

L'association d'un document à son ou ses auteurs est assurée par la métadonnée XDS authorPerson ou legalAuthenticator (le responsable légal est assimilé à l'un des auteurs).

Dans le DMP, seul l'un des auteurs d'un document peut ajouter un document ou le mettre à jour avec une nouvelle version (remplacement du document) ; cette règle est appliquée comme suit :

- en authentification directe, le PS authentifié doit faire partie des auteurs (champ NameID du VIHF = composant « identifiant » de authorPerson ou de legalAuthenticator) ;
- en authentification indirecte, la structure authentifiée doit être égale à la métadonnée authorInstitution de l'un des auteurs (champ Identifiant_Structure du VIHF = champ « identifiant » de authorInstitution).

Remplacement d'un document existant dans le DMP

D'un point de vue technique, le « remplacement de document » utilise la même transaction que

l' « alimentation simple », aux différences exposées ci-après.

Pour remplacer un document (fiche métadonnées XDS + document CDA), il faut envoyer la nouvelle version du document à l'entrepôt du DMP (repository XDS) pour remplacer dans le registre (registry XDS) l'ancienne fiche du document par la nouvelle. Il faut également envoyer l'association RPLC qui lie les deux fiches et qui est conservée dans le registre.

Dans la nouvelle fiche, la métadonnée availabilityStatus prend la valeur « approved ».

Dans l'ancienne fiche, la métadonnée availabilityStatus prend la valeur « deprecated ».

Ces deux fiches sont liées par une association de type « RPLC » (replace)

4.1.6.3 Métadonnées XDS d'un lot de soumission

Grouper les documents dans un même lot de soumission XDS

Pour gérer le lien entre plusieurs documents, d'un même « épisode de soins » par exemple, il est possible de les grouper dans un même « lot de soumission ». Cela permettra notamment aux autres médecins de les identifier et d'y accéder beaucoup plus simplement. A noter : un même document peut être référencé dans plusieurs lots de soumission.

4.1.7 Document CDA R2

Documents de référence
[CI-STRU-ENTETE] CI-SIS – Couche Contenu – Volet Structuration Minimale des Documents Médicaux [CI-ANX-CDA] -CI-SIS – Couche Contenu – Annexe **« Liens entre en-tête CDA et métadonnées »**

CDA R2 ou Clinical Document Architecture Release 2 est un «dialecte[3]» XML développé par l'organisation Health Level Seven International (HL7), qui permet de véhiculer des données médicales. CDA.xsd est le schéma XML validant tout document XML conforme au standard CDA R2.

Seuls les documents médicaux au format CDA R2 sont acceptés dans le DMP.

Un document XML commence toujours par un élément racine, appelé **ClinicalDocument** pour le CDA. Un document XML conforme au standard CDA R2 est composé après la racine, d'un en-tête et d'un corps.

L'en-tête structuré contient les informations générales indispensables à l'identification du document ainsi que les données du contexte médical dans lequel il a été produit, par exemple l'identifiant du document, son titre, sa date de création, son auteur, le patient, sa prise en charge, les intervenants etc.

Le corps véhicule la partie médicale du document. Cette partie peut contenir un simple texte, une image ou un son (CDA R2 structuré de niveau 1) ou être organisée en structures de données afin de permettre ou simplifier les traitements informatiques (CDA R2 structuré de niveau 3).

Un document CDA doit comporter au moins un identifiant patient, éventuellement plusieurs.

Un document CDA mis en partage dans le DMP comporte obligatoirement l'INS[4] comme premier identifiant du patient :

<id root=1.2.250.1.213.1.4.2' extension='041188631960571937l016'/>

[3] (1) Un dialecte XML est un langage informatique en syntaxe XML ou acceptant une syntaxe XML. La nature eXtensible d'XML est vérifiée par une très grande famille catégorisée sous ce terme

http://fr.wikipedia.org/wiki/Cat%C3%A9gorie:Dialecte_XML

[4] Pour l'instant l'INS-c mais il est prévu dans la loi de santé 2016 que soit déployé le NIR

4.1.8 Les fonctionnalités

4.1.8.1 Les différents profils de fonctionnalités

Les fonctions offertes par le système DMP sont les suivantes, regroupées par grand profil fonctionnel. Un « profil LPS » est constitué d'un ensemble de transactions fonctionnellement liées entre elles et devant être implémentées conjointement. Trois profils sont définis selon les fonctions couvertes par le LPS :

- création et gestion administrative ;
- alimentation ;
- consultation.

Chacun des 3 profils DMP est constitué de transactions obligatoires et de transactions optionnelles (voir tableau ci-dessous) :

			Profils DMP	
Transactions DMP à implémenter		**CREATION**	**ALIMENTATION**	**CONSULTATION**
ACCES SECURISE AU DMP				
TD0.1	Authentification sur le DMP		Obligatoire	
TD0.2	Test d'existence d'un DMP et vérification de l'autorisation d'accès		Obligatoire	
TD0.3	Mise à jour de l'autorisation d'accès		Obligatoire	
TD0.4	Liste des dossiers autorisés		Optionnelle	
TD0.5	Recherche sans INS du DMP d'un patient			Obligatoire
TD0.9	Accès web-PS contextuel	Optionnelle	Optionnelle	Obligatoire
CREATION ET GESTION ADMINISTRATIVE DU DMP				
TD1.1	Création d'un DMP	Obligatoire		
TD1.2	Réactivation d'un DMP	Optionnelle		
TD1.3	Données administratives d'un DMP	Optionnelle		
TD1.4	Fermeture d'un DMP	Optionnelle		
TD1.5	Accès internet du patient	Obligatoire		
TD1.6	Liste des PS autorisés/bloqués sur un DMP	Optionnelle		
ALIMENTATION DU DMP				
TD2.1	Alimentation en documents d'un DMP		Obligatoire	
TD2.2	Alimentation en documents d'un DMP par CPE pour les secrétaires médicales du secteur libéral		Optionnelle	
CONSULTATION DU DMP				
TD3.1	Recherche de documents dans un DMP			Obligatoire
TD3.2	Consultation d'un document dans un DMP			Obligatoire
TD3.3	Gestion des attributs d'un document		Obligatoire	Optionnelle

Figure 4 : liste des transactions à implémenter par profil

Les LPS n'ont pas l'obligation d'implémenter toutes ces transactions (certaines sont obligatoires et d'autres optionnelles), mais si un profil est retenu, il est recommandé d'implémenter toutes les transactions de ce profil

Dans ce guide nous nous intéressons seulement au profil d'alimentation. Le tableau montre que pour ce profil, 5 TD sont obligatoires et 3 sont optionnelles.

4.1.8.2 Restrictions fonctionnelles par mode d'authentification et profil utilisateur

En fonction de son mode d'accès (authentification directe CPS ou CPE, authentification indirecte) et de son rôle (PS non médecin, médecin traitant –MT, médecin non MT, non PS), l'acteur autorisé disposera de droits fonctionnels spécifiques : tous ces droits sont listés dans le DSFT au paragraphe « Droits fonctionnels par mode d'authentification et par profil utilisateur ».

4.2 Focus sur l'alimentation du DMP

L'alimentation du DMP permet au PS de déposer dans le DMP du patient les documents utiles à la coordination des soins. L'objectif est de permettre un **partage des documents** du patient entre tous les professionnels de santé qui sont amenés à le prendre en charge.

Documents de référence

[DMP-DSFT] Dossier de Spécifications Fonctionnelles et Techniques des interfaces DMP des LPS
[CI-PARTAGE] CI-SIS – Couche Service – Volet Partage de Documents de Santé
[CI-STRU-ENTETE] CI-SIS – Couche Contenu – Volet Structuration Minimale des Documents Médicaux

4.2.1 Profil « Alimentation du DMP »

Pour déposer dans le DMP du patient des documents, le LPS doit être homologué pour le profil « Alimentation du DMP ».

L'alimentation du DMP se fait DMP par DMP avec un « lot de soumission » pouvant comprendre un ou plusieurs documents liés ou non entre eux.

Le [DMP-DSFT] Dossier de spécifications fonctionnelles et techniques des interfaces DMP des LPS décrit en particulier les transactions à mettre en œuvre pour alimenter le DMP d'un patient. Au minimum, les transactions à développer sont :

- TD0.1 Authentification sur le système DMP ;
- TD0.2 Test d'existence d'un DMP;
- TD0.3 Mise à jour de l'autorisation d'accès ;
- TD2.1 Alimentation en documents d'un DMP ;
- TD3.3 Gestion des attributs d'un document

Les transactions TD0.x gèrent les accès au DMP.

La transaction TD2.1 permet de déposer dans le DMP du patient le ou les documents sélectionnés.

La transaction TD3.3 permet de :

- masquer/démasquer un document aux PS ;
- rendre visible un document au patient ;
- archiver/désarchiver un document ;
- supprimer un document.

A noter que pour lier les documents entre eux ultérieurement au dépôt d'au moins l'un d'eux par la notion de lot de soumission, il est aussi nécessaire de mettre en œuvre la transaction TD3.1 « Consultation du DMP ».

4.2.2 Cinématique des appels aux TD

Pour pouvoir alimenter un DMP (c.-à-d. mettre un document en partage dans le DMP d'un patient), il est nécessaire :

- que le PS soit authentifié par le système DMP ;
- que le DMP du patient existe ;
- que le PS ait recueilli l'autorisation d'accès au DMP du patient.

La TD0.1 qui permet d'authentifier le PS est intégré à chaque transaction.

Il est préférable que le LPS vérifie l'existence du DMP et l'autorisation d'accès (TD0.2) et si nécessaire mette à jour l'autorisation d'accès (TD0.3) avant de tenter d'alimenter le DMP (TD2.1). Cela permettra d'éviter un nombre important d'échecs d'alimentation.

Solution non retenue : envoi d'un mail MSSanté avec une archive XDM au système DMP

L'ASIP Santé avait identifié une solution où le LPS alimenterait le DMP en envoyant un mail MSSanté (avec une archive XDM) au système DMP qui l'intégrerait. Cette solution n'a pas été retenue car :

1) Si le LPS ne met pas en œuvre les TD0.x et TD3.3 du DMP, le LPS ne peut pas :

- vérifier que le DMP existe avant l'envoi du document ;
- vérifier l'autorisation d'accès au DMP ni de recueillir l'autorisation d'accès au DMP du patient ;
- supprimer/remplacer un document dans le DMP ;
- gérer la visibilité d'un document.

⇨ Il est donc préférable que le LPS mette en œuvre ces TD

2) Si le LPS met en œuvre les TD0.x et TD3.3 du DMP, il n'y a aucune difficulté pour mettre en œuvre la TD2.1 car l'éditeur aura déjà développé les couches permettant de communiquer avec le DMP (authentification, protocole d'échange)

4.2.3 Focus sur la TD2.1 Alimentation en documents d'un DMP

Après que le PS ait saisi les informations utiles pour la constitution du document **(dont la confidentialité du document dans le DMP)**:

1. Le LPS construit le document CDA à partir des informations saisies par le PS et des informations déduites par le LPS du contexte d'usage ;
2. Le LPS construit le document XDS ;
3. Le LPS réalise la signature du document (non obligatoire) ;
4. Le LPS constitue un lot de soumission XDS ;
5. Le LPS réalise la signature XAdES du lot de soumission ;
6. Le LPS envoie la requête au DMP.

4.2.4 Schéma synthétique de l'alimentation du DMP par un LPS

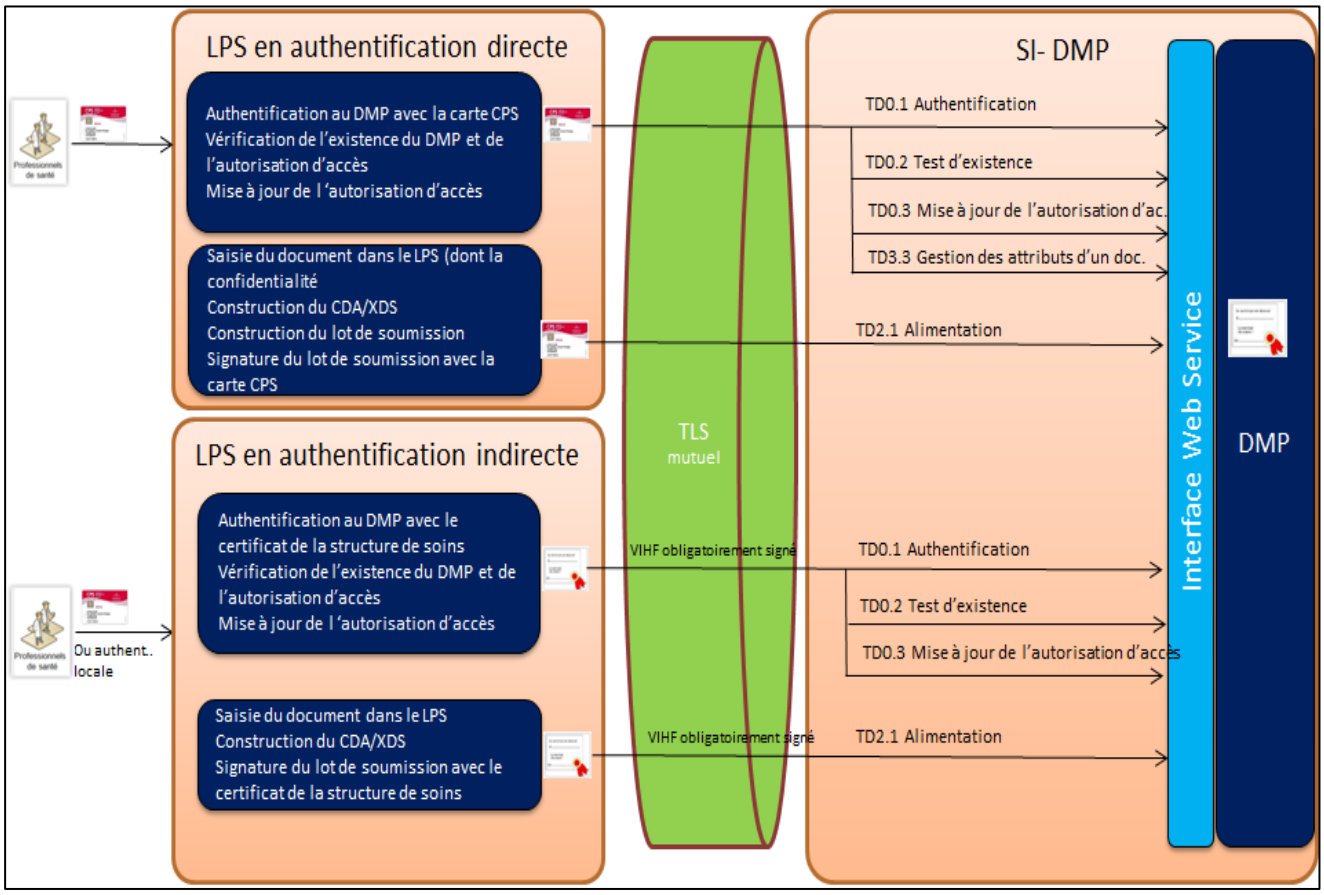

Figure 5 : alimentation du DMP par un LPS

5 Le système MSSanté

5.1 Fonctionnement du système MSSanté

Documents de référence
[MSS-DST-CLIENT] Dossier de Spécifications Techniques Clients de messageries. [MSS-DSFTT-OPERATEUR] Dossier de Spécifications Fonctionnelles et Techniques Opérateurs de messageries MSSanté [CI-ECHANGE] CI-SIS – Service : Volet Echange de documents de santé

5.1.1 Présentation générale du système MSSanté

Le système MSSanté répond aux deux besoins suivants :

- 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 ou plusieurs destinataires (ou entités destinataires) ;
- la consultation, par une personne certifiée et habilitée, d'un message reçu pouvant contenir des données de santé à caractère personnel.

Le système MSSanté est un espace de confiance que de nombreux opérateurs de messageries, adressant des 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 pour les opérateurs MSSanté ».

Les logiciels de type client lourd de messagerie ou logiciel de professionnel de santé (LPS) peuvent s'interfacer avec les opérateurs de l'espace de confiance MSSanté. Cela leur permet d'intégrer les fonctions de messagerie suivantes :

- relever et envoyer des courriers électroniques pour une BAL MSSanté ;
- rechercher des boîtes aux lettres (BAL) dans l'annuaire national MSSanté.

Un LPS souhaitant s'interfacer avec le service de messagerie proposé par l'opérateur ASIP Santé doit se référer au « Dossier des spécifications techniques des interfaces client ». Bien qu'il s'agisse d'une recommandation forte permettant de garantir l'interopérabilité des LPS entre les différents opérateurs, ces spécifications techniques ne s'imposent pas obligatoirement à l'ensemble opérateurs de l'espace de confiance MSSanté. Certains opérateurs peuvent avoir besoin d'utiliser des interfaces propriétaires spécifiques à leurs clients de messagerie.

Les exemples de transactions, de protocoles et de modes d'authentification pris dans la suite de ce document partent de l'hypothèse que les LPS est conforme aux DST.

5.1.2 La sécurisation des échanges

Le DST [MSS-DST-CLIENT] décrit 2 types d'accès possibles entre le client de messagerie et le serveur de l'opérateur MSSanté :

- par protocoles standards de messagerie ;
- par Web services.

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

- pour les transactions utilisant les protocoles SMTP + StartTLS et IMAP + StartTLS, 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.

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

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

5.1.2.1 *Accès par protocoles standards de messagerie*

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

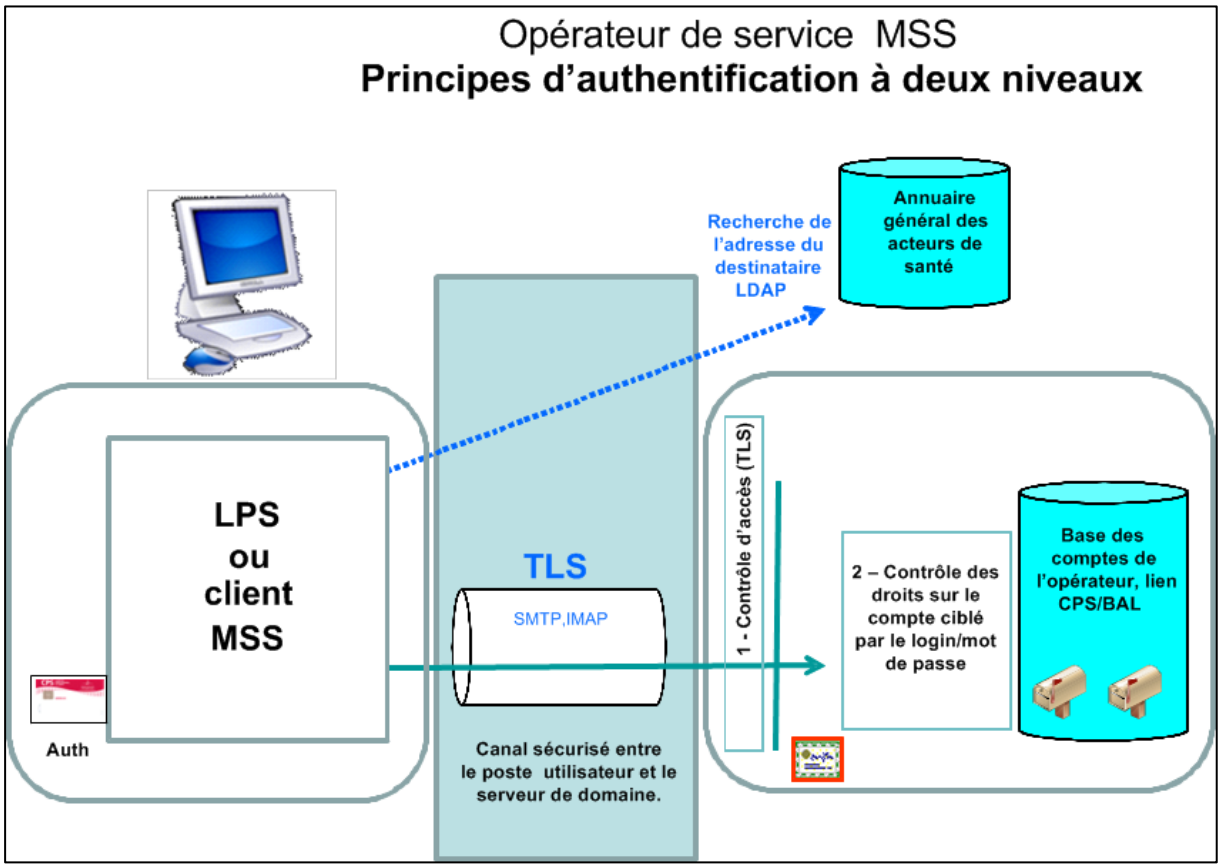

Figure 6 : principes d'authentification entre un client de messagerie et un opérateur MSSanté selon un protocole standard de messagerie

Le contrôle d'accès par le serveur est assuré à 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 pour 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).

5.1.2.1 *Accès par Web service*

Pour l'accès par Web service, les mécanismes d'authentification décrits dans le DST et proposés par l'opérateur ASIP Santé sont les suivants :

- carte CPS ;
- identifiant/ mot de passe/ OTP (SMS ou mail), 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 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.

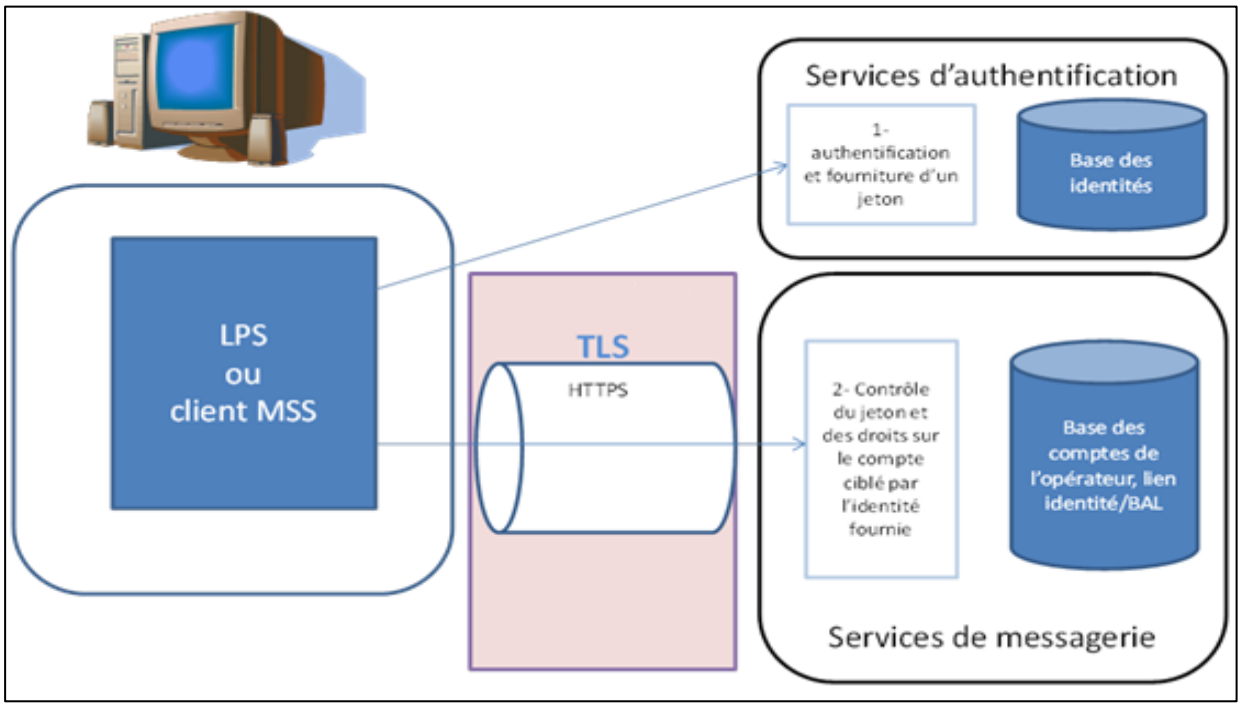

Figure 7 : principes d'authentification entre un Client de messagerie et un opérateur MSSanté exposant des Web Services de messagerie

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

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

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

5.1.3 Les fonctionnalités à implémenter

Le présent chapitre présente les transactions « standards » MSSanté pouvant être intégrées dans un client de messagerie conforme au DST :

- les transactions de messagerie basées sur les protocoles standards de messagerie (SMTP + StartTLS et IMAP + StartTLS) ;
- les transactions de messagerie basées sur les Web Services ;
- la transaction de consultation de l'annuaire national MSSanté par le protocole LDAP.

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

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

5.1.4 Le format d'échange de document (profil IHE XDM)

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-ECHANGE] 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.

Selon les recommandations du profil IHE-XDM et du CI-SIS, le texte de l'objet doit contenir la chaine de caractères non significative " XDM/1.0/DDM", suivi du caractère séparateur "+", lui-même suivi d'une chaîne de caractères significative dont le contenu et la structuration sont à définir par le métier.

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 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.

L'archive XDM permet :

- d'identifier qui envoie le document ;
- de signer le lot de soumission (optionnel) ;
- un meilleur contrôle de l'intégrité des documents (hash et size) ;
- de contenir des documents CDA-R2 ;
- de lier des documents CDA-R2 via les références dans les lots de soumission.

Le volet échanges de documents de santé en référence [CI-ECHANGE] décrit de façon détaillé l'usage et constitution de l'archive XDM.

L'archive XDM contient des métadonnées (que l'on nommera métadonnées XDM) qui correspondent dans leurs structures et leurs valeurs aux métadonnées XDS.

Les métadonnées XDM peuvent donc contenir :

- des liens entre les documents contenus dans le lot ;
- l'information qu'un document remplace une version antérieure de document.

Cas particulier de la métadonnée URI :

La métadonnée URI est requise dans chaque fiche DocumentEntry présente dans la soumission. En effet, URI contient le chemin relatif pointant sur le nom du document de santé dans le sous-répertoire des documents. URI crée ainsi le lien entre la fiche et le document. L'adresse du document de santé dans le répertoire des documents doit toujours être relative, aucune adresse absolue (ex. c:\temp…) ne doit être indiquée.

5.1.5 Document CDA R2

Le document CDA-R2 est identique à celui utilisé pour le DMP (voir §4.1.7) **à l'exception de l'identifiant patient.**

Contrairement au partage de document de santé (DMP), un document CDA échangé via une messagerie sécurisée de santé peut utiliser d'autres identifiants patient que l'INS du moment que les interlocuteurs s'accordent sur les identifiants à utiliser. Par exemple l'IPP attribué par l'établissement de soins impliqué dans la production de ce document peut jouer le rôle d'identifiant commun. Les IPP attribués par un établissement de soins sont associé à un OID détenu par cet établissement, obtenu par exemple auprès de l'AFNOR et qui le représente comme autorité d'affectation de ces IPP.

<id root='1.2.250.1.23.9.4.9' extension='1234567890121' assigningAuthorityName='CHU XYZ' />

En conséquence, un document CDA échangé entre deux professionnels ou organisations de santé via une messagerie sécurisée de santé doit comporter au moins un identifiant du patient, qui n'est pas nécessairement son INS, celui-ci pouvant ne pas être disponible au moment de l'élaboration du document.

Note : Dans le cas d'échange de documents ayant vocation à être mis en partage, il est nécessaire de suivre les spécifications du volet partage de documents de santé dès la constitution initiale des documents pour ne pas avoir à modifier la métadonnée **patientId** avant la mise en partage. En substance, seuls les documents dont le composant 5 de la métadonnée **patientId** est "INS-C" peuvent être mis en partage ultérieurement à leur échange.

5.2 Focus sur l'envoi de documents de santé par MSSanté

Le LPS doit intégrer un client de messagerie qui s'interface avec un opérateur intégré à l'espace de confiance MSSanté pour proposer un service d'échange de messages sécurisés et de gestion de boîte aux lettres aux professionnels de santé.

Pour être en mesure de réaliser une alimentation du DMP en parallèle de l'envoi d'un document via MSSanté, le message et le document envoyés devront nécessairement porter sur un unique patient.

5.2.1 Cinématique d'appel des transactions

Pour envoyer un message contenant un document en pièce jointe, les transactions diffèrent en fonction du protocole implémenté par le LPS. Pour envoyer un message accompagné d'une pièce jointe, un LPS doit a minima implémenter les transactions suivantes :

Protocoles standards de messagerie (IMAP/SMTP) :

- TM3.2C : Emission de message

Web services :

- TM4.1.xC : Authentification par CPS ou OTP ;
- TM4.3.4C : Service sendMessage.

Le [MSS-DSFT-CLIENT] Dossier de spécifications Ttchniques clients de messageries décrit ces transactions.

5.2.2 Préparation de la pièce jointe

Après que le PS a saisi les informations utiles pour la constitution du document :

1. Le LPS construit le document CDA à partir des informations saisies par le PS et des informations déduites par le LPS du contexte d'usage ;
2. Le LPS construit l'archive XDM ;
3. Le LPS ajoute la pièce jointe XDM au message à envoyer ainsi que les documents dans au format lisible par un humain (PDF par exemple).

5.2.3 Schéma synthétique de l'envoi d'un document via MSSanté

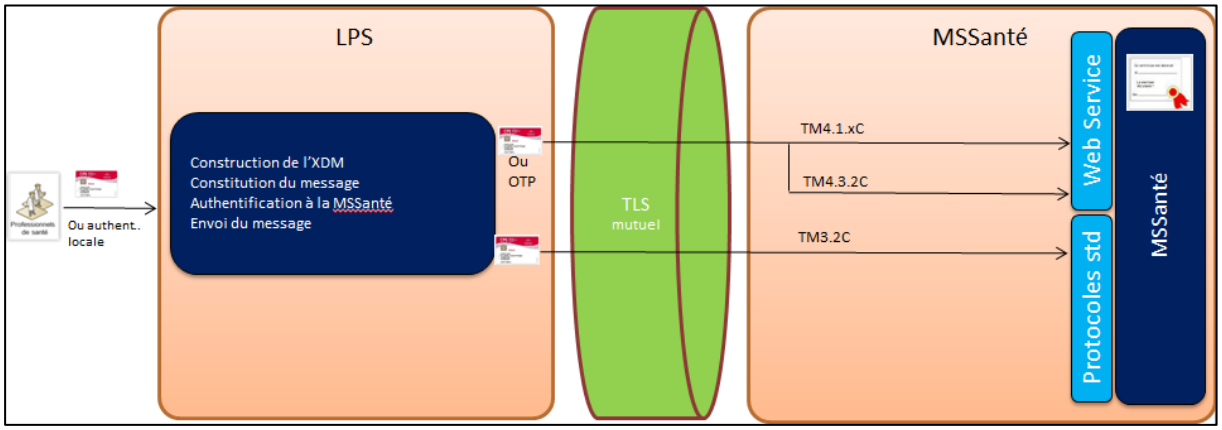

Figure 8 : envoi de document de santé via MSSanté

6 Différences entre les mécanismes techniques et les contraintes des 2 systèmes

6.1 Principe de l'alimentation en Y

Ergonomiquement, il est possible dans un LPS de mettre en partage un document de santé dans le DMP lors de son envoi par MSSanté.

Techniquement, nous avons vu dans les paragraphes précédents que le LPS doit gérer 2 canaux distincts :

- l'envoi d'un document via MSSanté ;
- l'appel aux Web-Services du système DMP pour l'alimentation du DMP.

Une unique action d'un utilisateur dans son LPS peut donc provoquer la sollicitation de 2 systèmes. C'est que nous appelons le principe d'alimentation en Y.

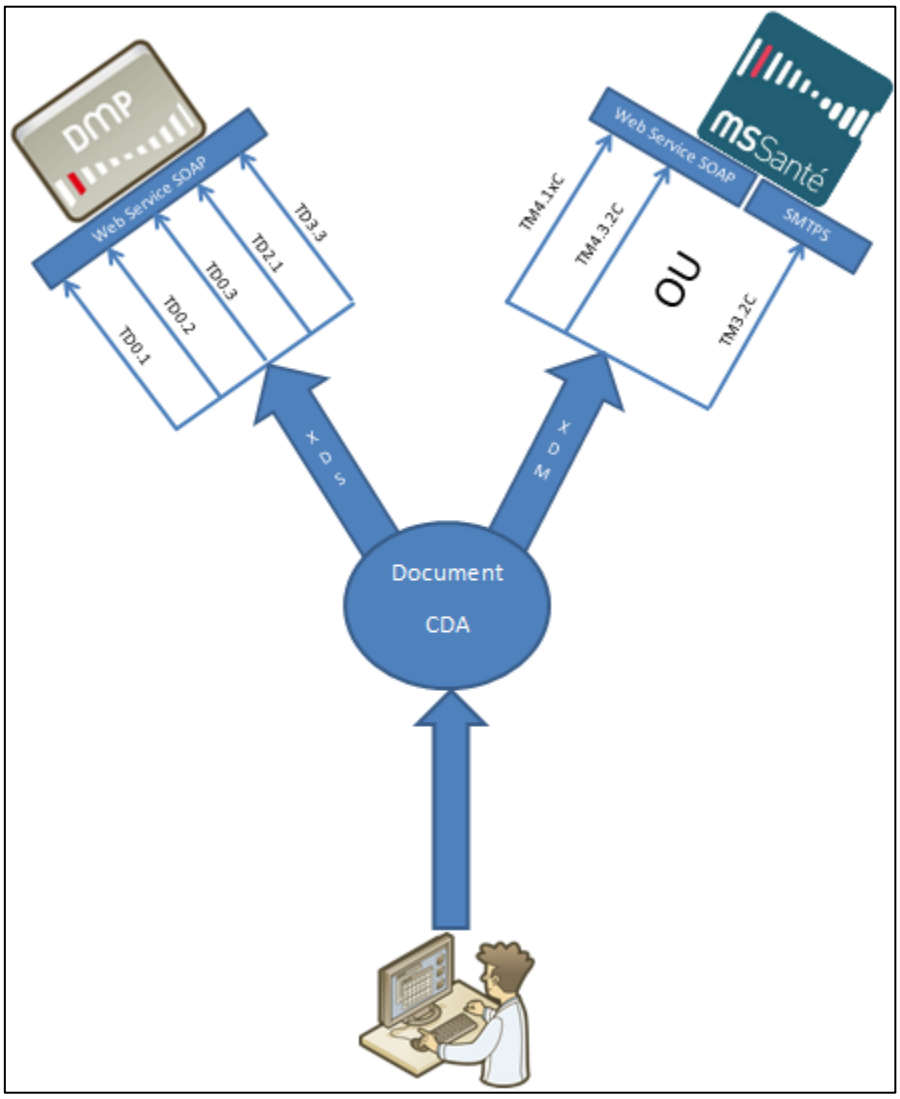

Figure 10 : principe de l'alimentation en Y

6.2 Tableau récapitulatif et comparatif de l'alimentation du DMP et de MSSanté

Ci-dessous un tableau qui récapitule les différences entre les mécanismes techniques ou les contraintes des systèmes DMP et MSSanté. Il est indiqué dans ce tableau la référence du paragraphe de ce guide qui décrit plus précisément le sujet abordé.

	DMP – Mise en partage	Ref.	MSSanté - Echange	Ref.
Authentification et interfaces techniques				
Authentification	Authentification directe via carte CPX ou authentification indirecte via Certificat serveur	4.1.3	Authentification par CPS ou via Login/MdP/OTP	5.1.2
Protocole d'échange	WS soap et VIHF	4.1.2	SMTPS ou WS soap (sans VIHF)	5.1.2
Signatures électroniques				
Signature VIHF	Facultative en authentification directe Obligatoire en authentification indirecte	4.1.4	N/A	
Signature du lot de soumission	Signature du lot de soumission XDS : Obligatoire	4.1.4	Signature du lot de soumission: facultative (en fonction du système cible)	5.1.4
Signature du document	Facultative	4.1.4	Facultative	5.1.5
Profils IHE – Document – Identifiant patient				
Profil IHE	XDS.b. La métadonnée sur la confidentialité du document est **obligatoire**	4.1.6	XDM. Idem que XDS sauf pour la métadonnée URI	5.1.4
Remplacement de document	Oui. Le DMP prend en compte cette information.	4.1.6	Oui mais le traitement de cette information dépend du système cible	5.1.4
Lien possible entre documents	Oui. Le DMP prend en compte cette information.	4.1.6	Oui mais le traitement de cette information dépend du système cible	5.1.4

	DMP – Mise en partage	Ref.	MSSanté - Echange	Ref.
Profils IHE – Document – Identifiant patient				
Document de santé	CDA R2	4.1.7	CDA R2	5.1.5
Identification du Patient dans les métadonnées	INS (actuellement INS-c bientôt NIR)	4.1.7	INS (actuellement INS-c bientôt NIR) ou IPP ou tout autre identifiant que les interlocuteurs se sont préalablement accordés à utiliser	5.1.5
Intégration dans le LPS				
Cinématique des appels du LPS au système cible	TD0.1 Authentification sur le système DMP, TD0.2 Test d'existence d'un DMP, TD0.3 Mise à jour de l'autorisation d'accès, TD2.1 Alimentation en documents d'un DMP,	4.2.2	Protocoles standards de messagerie (IMAP/SMTP) • TM3.2C : Emission de message Web Services : • TM4.1.xC : Authentification par CPS ou OTP • TM4.3.4C : Service sendMessage	5.2.1
Recueil des informations auprès de l'utilisateur en plus des informations permettant de construire un document CDA	Recueil de l'autorisation d'accès au DMP Confidentialité du document (visible, masqué PS, invisible patient)	4.2.2	Aucune	5.2.2
Règles fonctionnelles				
Auteur vs émetteur	Seul l'un des auteurs d'un document peut ajouter un document ou le mettre à jour avec une nouvelle version (remplacement du document)	4.1.6	Un PS peut envoyer un document dont il n'est pas l'auteur	5.1.4

7 Exemple d'ergonomie d'un LPS

L'intégration des fonctionnalités de mise en partage d'un document de santé dans le DMP et de son envoi par MSSanté dans un LPS dépend des cas d'usage et de l'ergonomie du LPS.

Ce chapitre présente un exemple de LPS intégrant ces fonctionnalités dans un cas d'usage donné.

7.1 Contexte

L'exemple concerne un LPS utilisé par un médecin généraliste. Ce médecin s'est authentifié dans son LPS via sa carte CPS.

Le médecin généraliste a réalisé une consultation avec son patient et a renseigné dans le dossier patient de son LPS les informations permettant de réaliser un document VSM (volet de synthèse médicale).

7.2 Etape 1 : le médecin souhaite partager le document VSM

Le médecin clique sur le bouton « Partager le VSM » depuis le dossier patient.

7.3 Etape 2 : le médecin choisit le type de partage

Le médecin a le choix entre 3 cases :

- envoi par MSSanté à un confrère ;
- dépôt dans le DMP du patient ;
- envoi par MSSanté et dépôt dans le DMP du patient.

Il choisit « envoi par MSSanté et dépôt dans le DMP du patient ».

7.4 Etape 3 : vérification de l'accès au DMP

Un écran est proposé au médecin. Cet écran lui indique que :

- le patient possède un DMP ;
- le médecin ne possède pas d'autorisation d'accès à ce DMP (dans l'hypothèse où le médecin ne possède pas encore cette autorisation).

Pour cela le LPS :

- possède ou a calculé l'INS du patient ;
- a appelé la TD0.2 du DMP (test d'existence du DMP).

Ensuite :

- le LPS demande au médecin de confirmer qu'il a recueilli l'autorisation d'accès au DMP du patient ;
- le médecin confirme ;
- le LPS appelle la TD0.3 du DMP (mise à jour de l'autorisation d'accès).

7.5 Etape 4 : Saisie des informations

Sur l'écran affiché, le médecin doit saisir :

- la confidentialité du document dans le DMP (visible, masqué PS, invisible patient). Par défaut, le logiciel propose « visible » ;

- les noms des destinataires MSSanté ;
- l'objet du mail ;
- le corps du mail.

7.6 Etape 5 : Envoi

Le médecin clique sur « envoi ».

Le LPS :

- construit le document CDA à partir des éléments qu'il a déduit (type de document, date, auteur du document, INS-c etc…) et des informations contenus dans le dossier patient du LPS (contenu du VSM) ;
- construit la couche XDS à partir du CDA en ajoutant la confidentialité du document saisit par le médecin ;
- signe le lot de soumission XDS avec la carte CPS du médecin ;
- soumet le lot de soumission au DMP (appel de la TD2.1) ;
- construit la couche XDM à partir de la couche XDS (i.e. ajoute la métadonnée URI) ;
- envoie les mails aux destinataires MSSanté saisis par le médecin avec en pièce jointe l'archive XDM ainsi que le document dans un format lisible par un humain (PDF par exemple).

8 Glossaire

ASIP Santé	Agence des systèmes d'information partagés de santé
CDA	Clinical Document Architecture
CI-SIS	Cadre d'interopérabilité des systèmes d'information de santé (publié par l'ASIP Santé)
CPS	Carte de Professionnel de Santé
DMP	Dossier Médical Partagé
DSFT	Dossier des spécifications fonctionnelles et techniques
DST	Dossier de spécifications techniques
HL7	Health Level Seven International
IGC	Infrastructure de gestion de clés
IMAP	Internet Message Access Protocol
INS	Identifiant National de Santé *du patient*
LGC	Logiciel de gestion de cabinet
LPS	Logiciel de professionnel de santé (abréviation générique désignant une application utilisée par un professionnel de santé, dans ou hors structure de soins)
MSSanté	Système de messagerie sécurisée MSSanté
OID	Object Identifier (identifiant d'objet)
OTP	One Time Password. Code d'accès à usage unique.
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PS	Professionnel de santé
RPPS	Répertoire Partagé des Professionnels de Santé
SAML	Security Assertion Markup Language
SIS	Système d'information de santé
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
SMTPS	Simple Mail Transfer Protocol Secure
TD	Transaction DMP
TLS	Transport Layer Security
SSL	Secure Sockets Layer
VIHF	Vecteur d'Identification et d'habilitation formelles
VSM	Volet de synthèse médicale
WS	Web service
XDM	Cross Enterprise Document Media interchange
XDS	Cross Enterprise Document Sharing

9 Annexe- Documents de références

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/) Version 1.3	
CI-CHAP	**Document Chapeau du CI-SIS et Note de version** CI-SIS_Document_Chapeau_v1.0.1.pdf Ce document est le chapitre introductif du Cadre d'interopérabilité des systèmes d'information de santé(SIS). Il présente : • la définition et le périmètre du cadre d'interopérabilité des SIS, ainsi que sa structure modulaire sous forme de volets ; • la structure générique d'un volet du cadre d'interopérabilité des SIS ; • les règles de nommage d'un volet ; • la trajectoire de ce référentiel ; • une cartographie des volets disponibles dans la version initiale, et de ceux qui viendront compléter le référentiel dans les versions suivantes. • Le glossaire des acronymes utilisés dans le référentiel
CI-PARTAGE	**Couche Service - Volet Partage de Documents de Santé** CI-SIS_SERVICE_VOLET-PARTAGE-DOCUMENTS-SANTE_V1.3.2.1.pdf Ce volet est la version plus récente de CI-PARTAGE, qui précise les valeurs de certains champs (mimeType, size et hash) pour les documents au format « CDA auto-présentable ».
CI-ECHANGE	**Couche Service - Volet Echange de Documents de Santé** CI-SIS_SERVICES_VOLET-ECHANGE-DOCUMENTS-SANTE _v1.3.2.1.pdf Ce volet spécifie la couche Services pour : • un système initiateur qui envoie des documents de santé à un système cible via messagerie électronique ; • un système cible qui reçoit des documents de santé d'un système initiateur via messagerie électronique
CI-TR-CLIL-RD	**Couche Transport - Volet Synchrone pour Client Lourd** CI-SIS_couche_Transport_Volet_Synchrone_client_lourd_v1.3.2.1.pdf Ce volet spécifie la couche Transport pour : • un système cible offrant un service auquel il est possible de se connecter de façon synchrone ; • un système initiateur bénéficiant d'un « client lourd »
CI-STRU-ENTETE	**Couche Contenu - Volet Structuration Minimale de Documents Médicaux** CI-SIS_CONTENU_VOLET-STRUCTURATION-MINIMALE_V1.3.2.1.pdf Ce volet fait partie de la couche « Contenu » du CI-SIS. Il spécifie la structuration minimale des documents médicaux persistants partagés ou échangés dans ce contexte.

CI-ANX-CDA	**Annexe : Liens entre métadonnées et entête CDA** CI-SIS_Annexes_Liens_entête_CDA_Métadonnées_v1.3.1.0.pdf
CI-ANX-NOMENC-DOC	**Annexe : Nomenclatures de Métadonnées Documents** CI-SIS_Annexes_Nomenclatures_Métadonnées_Documents_v1.3.1.pdf
Documents en lien avec le DMP	
DMP-ARCHI	**Urbanisation : Architectures systèmes éligibles aux échanges avec le DMP** asip-_architectures_de_systemes_eligibles_aux_echanges_avec_le_dmp_v1_1_1.pdf http://www.esante.gouv.fr/sites/default/files/asip-_architectures_de_systemes_eligibles_aux_echanges_avec_le_dmp_v1_1_1.pdf
DMP-DSFT	**Dossier de Spécifications Fonctionnelles et Techniques des interfaces DMP des LPS** DSFT_des_interfaces_DMP_des_LPS_v1.0.4_20160315.pdf http://esante.gouv.fr/services/espace-dmp/specifications-fonctionnelles-et-techniques-de-la-dmp-compatibilite-0
Documents en lien avec la MSSanté	
MSS-DST-OPERATEUR	**Dossier de Spécifications Fonctionnelles et Techniques Opérateurs de messageries MSSanté** MSS_FON_DSFT_Opérateurs_MSSanté_v1.0.0.pdf http://esante.gouv.fr/services/mssante/editeurs-operateurs/operateurs
MSS-DSFT-CLIENT	**Dossier de Spécifications Techniques Clients de messagerie** MSS_FON_DST _interfaces_clients_mssante_v1.0.1_150529.pdf http://esante.gouv.fr/services/mssante/editeurs-operateurs/editeurs
URL des sites d'information de référence	
DMP-URL-INFO	**Portail d'information grand public sur le DMP** www.dmp.gouv.fr
MSSANTE-URL-INFO	**Portail d'information pour les professionnels de santé sur la MSSanté** https://www.mssanté.fr

***** FIN DU DOCUMENT *****

Guide de mise en œuvre de la MSSanté et de l'alimentation du DMP dans un logiciel de professionnel de santé - V1.0.0 - mars 2016

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté
esante.gouv.fr

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard
75015 PARIS

Standard : 01 58 45 32 50
du lundi au vendredi (hors jours fériés)
de 8h30 à 13h et de 14h à 17h