# Service DMP intégré aux LPS

Référence : SEL-MP-037 / Version : 2.9.0 / Date : 05/07/2023
Sécurité : LIBRE

GIE SESAM-Vitale
5, boulevard Marie et Alexandre Oyon – 72 019 LE MANS Cedex 2
www.sesam-vitale.fr

# CONTACTS

Pour toute demande d'évolution, comme pour toute question technique ou fonctionnelle, contactez le Centre de services :

- e-mail : centre-de-service@sesam-vitale.fr
- téléphone : 02 43 57 42 88

# SOMMAIRE

# TABLE DES ANNEXES



# TABLE DES ILLUSTRATIONS

# TABLE DES TABLEAUX

# 1 INTRODUCTION

L'objectif de ce document est de permettre aux éditeurs de rendre les « Logiciels de Professionnel de Santé » (LPS) interopérables avec le système « Dossier Médical Partagé » (système DMP) et de les homologuer « DMP-compatible » par la procédure de vérification mise en œuvre par le CNDA.

NB : ce document est aligné avec les interfaces LPS v2 du système DMP qui intègrent le NIR utilisé comme Identifiant National de Santé.

NB : dans ce document, INS signifie Identifiant National de Santé.

**Évolutions 2.9.0**

Pour un non professionnel équipé d'une CPE (par exemple, une secrétaire médicale), accès à la liste des patients d'un professionnel via la fonctionnalité « Liste des DMP autorisés » (DMP_0.4 / TD0.4).

Prise en compte des CPS remplaçants.

Harmonisation des règles de gestion des notes de vaccination entre le CI-SIS et le DMP (volet 2023). Cf. chapitre 6.1.

La prise en charge de la gestion des notes de vaccination n'est plus obligatoire pour le secteur hospitalier.

Correction d'une coquille et précision au niveau de la donnée VIHF_Version et subject:role.

## 1.1 Documents de référence

Le chapitre 5.1 décrit les standards, normes et référentiels à prendre en compte :

- le cadre d'interopérabilité des SIS (CI-SIS),
- le profil IHE XDS.b et la norme HL7 CDA R2 (alimentation et consultation des documents du DMP du patient),
- la norme HL7 V3 (gestion du DMP du patient),
- le profil IHE PDQ HL7 V3 (recherche de DMP de patient sans identifiant).

L'annexe 4 présente la liste des documents externes auxquels se référer. Cette liste permet de vérifier les versions des normes prises en compte dans le système DMP.

L'annexe 8 présente une synthèse des écarts entre le système DMP et le CI-SIS.

Des documents, fournis à titre informatif, illustrent le fonctionnement du système DMP et indiquent notamment les contrôles effectués par ce système. La liste de ces documents est également disponible dans l'annexe 4.

## 1.2 Abréviations

Les abréviations sont disponibles dans l'annexe2.

## 1.3 Guide de lecture

Ce document s'adresse aux éditeurs qui souhaitent mettre en œuvre ou maintenir les interfaces de leur LPS avec le système DMP.

Selon son profil (décideur, directeur technique, chef de projet, développeur, architecte logiciel, consultant technique), le lecteur pourra se concentrer sur certains chapitres spécifiques.

- Le chapitre 2 offre une vision d'ensemble du périmètre et du contenu fonctionnel du document.
- Le chapitre 3 décrit en détail tous les aspects fonctionnels liés au LPS et aux transactions du système DMP.
- Le chapitre 4 présente les principales données fonctionnelles utilisées pour l'intégration des transactions DMP dans le LPS.

- Le chapitre 5 décrit en détail tous les aspects techniques liés au LPS.
- Le chapitre 6 contient les exigences et recommandations concernant l'intégration de certains documents dans les LPS.

La suite de ce chapitre présente les éléments spécifiques au guide d'intégration DMP. Les autres éléments des guides d'intégration (dont le référencement des données) sont présentés dans l'annexe 1.

### Règles de gestion

La documentation des règles de gestion (y compris les cas particuliers et les cas d'erreur) peut contenir trois types de texte.

- Une exigence est une partie de règle de gestion (fonctionnelle ou technique) obligatoire que l'éditeur doit implémenter. Elle apparaît sous forme d'un encadré avec le symbole Ⓔ dans la marge.
- Une recommandation est un conseil de mise en œuvre visant à guider l'éditeur dans l'élaboration de son LPS. Elle apparaît sous forme d'un encadré avec le symbole Ⓡ dans la marge.
- Les autres textes sont fournis à titre informatif.

La lecture des règles de gestion se fait dans l'ordre d'apparition dans le document.

### Références

Les exigences sont référencées « EX_x.x-yyyy » avec x.x indiquant la transaction concernée et yyyy étant un nombre à quatre chiffres.

Les exigences de portée générale sont référencées « EX_GEN-yyyy » avec yyyy un nombre à quatre chiffres.

Les recommandations sont référencées « REC_x.x-yyyy » avec x.x indiquant la transaction concernée et yyyy étant un nombre à quatre chiffres.

Les recommandations de portée générale sont référencées « REC_GEN-yyyy » avec yyyy un nombre à quatre chiffres.

### Exemples d'IHM

Convention de représentation pour les exemples d'IHM :

[x] : Case à cocher, cochée par défaut.
[ ] : Case à cocher, décochée.
(x) : Bouton radio, coché par défaut.
( ) : Bouton radio, décoché.

### Documents de référence

Les documents de référence sont cités entre crochets, par exemple : [CI-PARTAGE].

# 2 PRESENTATION GENERALE

Le LPS permet à l'utilisateur d'administrer un DMP pour chaque patient. L'utilisateur peut également alimenter le DMP du patient avec des documents de santé et consulter ces documents. Cf. chapitre 2.1 pour plus d'informations.

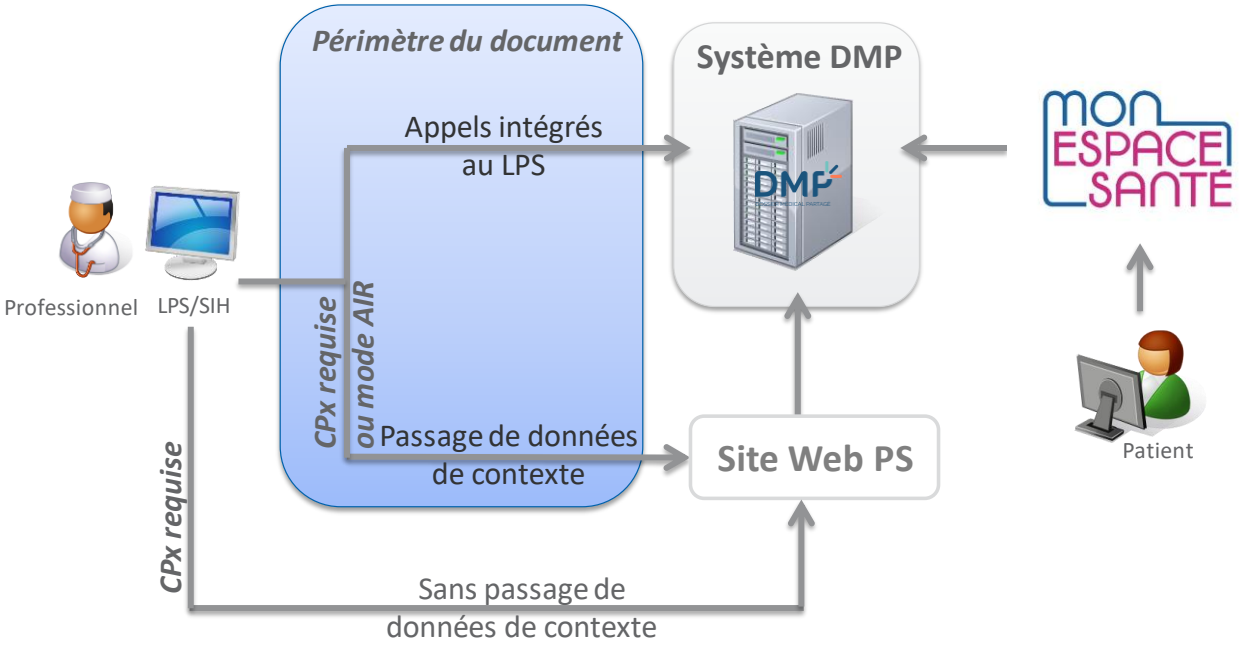



**Figure 1 : vue générale de l'utilisation du service DMP intégré dans le LPS**

L'intégration du service DMP dans le LPS s'appuie sur le cadre d'interopérabilité des systèmes d'information de santé de l'ANS [CI-SIS].

## 2.1 Introduction

### *Mon espace santé*

Dans le cadre de la réforme « Ma santé 2022 », « Mon espace santé » permet au patient d'accéder à différents services dont fait partie le DMP.

### *Le DMP*

**Améliorer la coordination des soins**

Le DMP a été institué par la loi pour faciliter le partage d'informations entre professionnels, éviter les actes redondants et agir contre les interactions médicamenteuses.

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 au partage des informations entre professionnels.

**Fiabiliser le parcours de soins et les pratiques pluridisciplinaires**

Le DMP ne remplace pas le dossier patient du professionnel. Il contient les informations importantes produites lors du parcours de soins du patient et conservées dans les dossiers des professionnels. 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.

### *Le LPS au cœur des Systèmes d'Information de Santé*

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

Le LPS est le premier SIS du Professionnel et il est évidemment l'outil naturel d'accès au système DMP. L'objectif de la Cnam est donc de permettre une intégration aussi harmonieuse que possible entre le LPS et le système DMP. Le DMP doit être une source de valeur ajoutée métier pour les éditeurs et les professionnels qui travaillent avec leurs logiciels.

Par ailleurs, dans un souci de continuité de la prise en charge, une interface d'accès alternative pour les professionnels via un navigateur permet de prendre en compte les situations particulières d'usage ou les restrictions techniques (accès à des fonctions non implémentées dans le LPS par exemple).

#### *Le DMP, système de partage de documents de santé*

L'alimentation du système DMP permet au professionnel[1] de déposer dans le DMP du patient les documents utiles à la coordination des soins. L'objectif est de permettre, avec l'accord du patient (*), un partage des documents du patient entre tous les professionnels qui sont amenés à le prendre en charge.

(*) L'accord du patient se décompose comme suit :

- non opposition à l'alimentation de son DMP,
- consentement à la consultation de son DMP.

#### *Référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP)*

La mise en œuvre et l'utilisation d'un LPS DMP-compatible doivent s'effectuer dans le respect du référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP) [REF-DMP].

### Périmètre

#### *Patients*

Les modalités concernant l'identification des patients sont définies dans le référentiel INS de l'ANS et dans les documents associés : Guide d'implémentation de l'identité INS dans les logiciels, Référentiel National d'IdentitoVigilance, Foire aux questions, … [REF-INS].

#### *Utilisateurs LPS*

Toute personne porteuse d'une carte CPS (titulaire ou remplaçant) ou CPF.

Toute personne exerçant en structure de soins.

Toute personne porteuse d'une carte CPE dans les secteurs d'activité suivants :

- SA01 : Etablissement public de santé,
- SA02 : Hôpital militaire du Service de santé des armées,
- SA03 : Etablissement privé PSPH,
- SA04 : Etablissement privé non PSPH,
- SA05 : Centre de santé,
- SA07 Cabinet individuel,
- SA08 Cabinet de groupe,
- SA09 Exercice en Société,
- SA16 : Etablissement pour personnes handicapées,
- SA17 Etablissement pour personnes âgées,
- SA18 : Etablissement aide à la famille,
- SA20 : Etablissement pour la protection de l'enfance,
- SA25 Laboratoire de Biologie Médicale,
- SA29 Laboratoire d'Analyses et de Biologie Médicale,

[1] L'alimentation est également ouverte aux personnes détentrices d'une carte CPE, exerçant sous la responsabilité d'un ou plusieurs professionnel(s).

- SA30 : Autre établissement sanitaire,
- SA40 Secteur privé PH temps plein,
- SA52 Maison de santé, Pôle de santé.

#### *Documents*

Tout document de santé concernant un patient peut venir alimenter le DMP de ce patient et peut être consulté par tous les professionnels.

D'autres documents peuvent venir alimenter le DMP du patient. Par exemple les documents "Données de remboursement" sont déposés par l'Assurance Maladie et sont consultables par tous les professionnels.

#### *Types de LPS*

Dans le présent document, le terme LPS (Logiciel de Professionnel de Santé) désigne tout système d'information utilisé par un professionnel pour l'assister dans la gestion de la prise en charge de ses patients. Le LPS peut également être utilisé par d'autres personnes, par exemple, les secrétaires médicaux.

Tout type de LPS peut intégrer les transactions du système DMP. La liste est disponible dans les conditions particulières.

L'appel contextuel Web-PS en mode Authentification Indirecte Renforcée (AIR) est soumis à une homologation DMP avec un profil spécifique nommé « Consultation Web-PS en mode AIR ». Cf. chapitre 2.2.5 pour la présentation du profil et le chapitre 5.5 pour une description plus détaillée.

Restriction concernant le mode AIR pour la consultation des DMP intégrée au LPS et pour l'accès Web-PS Contextuel (TD0.10) :

- Dans un premier temps, l'ouverture en généralisation du mode d'authentification AIR ne concernera que les types d'établissements qui avaient été sollicités lors de la phase d'expérimentation (CH, CHU, CHR, HAD et Cliniques).
- L'ouverture des FINESS géographiques en production (après déclaration de conformité au « référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au DMP » sur le portail d'auto-homologation) ne pourra se faire que sur la base des types d'établissements cités ci-dessus.

### Hors périmètre

Les éléments suivants sont hors du périmètre de la DMP-compatibilité des LPS.

- Le site web PS (prérequis au niveau du poste, authentification, navigation…) n'est pas décrit dans ce document. Cf. [DMP-ACCES-WEB]. Exception pour l'accès contextuel Web-PS en mode AIR : cf. chapitre 5.5.
- Le fonctionnement interne du système DMP (contrôle des droits fonctionnels, contrôle des habilitations…) n'est pas décrit dans ce document. Cf. [DMP-MHAB] et [DMP-MDRF]).

Les canaux d'accès dédiés aux patients (accès web, application mobile…) sont également hors périmètre de ce document.

### Principes

#### *L'accès sécurisé au système DMP*

Le partage de données médicales ne peut avoir lieu sans une confiance forte dans le système DMP, rendue possible par la sécurité d'accès et par l'imputabilité des contenus déposés au sein des DMP des patients.

La sécurité est une ligne directrice de la conception du système DMP et se traduit par :

- une authentification forte des acteurs de santé, avec la gestion de certificats et de modes de connexion éprouvés,

- une imputabilité des contenus, avec la gestion de signature électronique des lots de documents déposés dans le DMP du patient,
- le respect de la confidentialité des données de santé, accessibles en fonction de leurs caractéristiques à certains professionnels autorisés par le patient titulaire du DMP,
- la traçabilité de chaque action sur le DMP du patient.

Selon le niveau d'implémentation des fonctions DMP dans son LPS, l'utilisateur peut accéder au DMP de son patient :

- par les fonctions spécifiques DMP intégrées dans son LPS.
  Le LPS est le moyen d'accès privilégié au DMP et est considéré par le système DMP comme l'interface principale.
- par l'accès au site web PS appelé depuis son LPS avec passage de contexte. Cela permet d'accéder à des fonctions non encore proposées en web-services (accès aux traces par exemple) ou d'accéder à des fonctions non encore implémentées dans son LPS. Le passage de contexte permet au professionnel d'accéder directement soit à son tableau de bord DMP (avec la liste des DMP des patients pour lesquels il est autorisé), soit au DMP d'un patient. Cf. §5.4.

L'accès au DMP d'un patient ne peut se faire qu'avec l'identifiant de ce patient. De plus, l'accès n'est possible qu'avec l'accord du patient (non opposition à l'alimentation de son DMP ; consentement à la consultation de son DMP), excepté dans les cas encadrés de l'accès bris de glace et de l'accès par les permanenciers auxiliaires de régulation médicale des centres de réception et de régulation des appels des SAMU-Centres 15. Le patient a la possibilité de s'opposer expressément à l'accès à son DMP en mode « bris de glace » et/ou « centre de régulation ».

### *Accès aux données du DMP d'un patient*

**EX_GEN-1560**

L'accès aux données du DMP d'un patient est réservé aux professionnels expressement autorisés par le patient dans le cadre de sa prise en charge.

Une exploitation par d'autres acteurs, à des fins autres que celles prévues par le décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé, au travers de la solution logicielle n'est pas autorisée, quelle que soit l'architecture sur laquelle elle repose (mode saas par exemple).

### *Identification du patient et de son DMP*

L'INS (Identifiant National de Santé) est l'identifiant du DMP d'un patient (article R1111-33 du code de santé publique) et c'est le NIR du patient (Numéro d'Inscription au Répertoire national d'identification des personnes physiques) qui est utilisé comme INS (article L1111-8-1).

Antérieurement, l'identifiant du DMP d'un patient mis en œuvre était un Identifiant National de Santé dit "Calculé" (INS-C), généré à partir du NIR de l'individu et d'autres éléments d'identification (prénom, date de naissance).

Cet INS-C n'a plus cours mais reste en usage pour les LPS n'ayant pas encore migré vers le nouvel INS. Pour la phase de transition entre l'INS-C et l'INS "NIR", le système DMP gère les deux identifiants pour le DMP de chaque patient.

Le système DMP est construit sur une logique "individu" et s'adresse à toute personne, mineure ou majeure, de tout régime d'assurance maladie, ouvrant droit ou ayant droit.

L'obtention d'un INS et de traits d'identification patient à jour associés à l'INS, notamment à des fins d'identito-vigilance, est un prérequis à toute action sur un DMP patient. L'obtention de ces données doit s'effectuer dans le cadre du référentiel INS de l'ANS et des documents associés [REF-INS].

- En dehors des modalités définies dans le référentiel INS de l'ANS et des documents associés [REF-INS], les NIR fournis par l'Assurance Maladie ne peuvent pas être utilisés directement comme INS dans le cadre du DMP.

- Les transactions TD0.2, TD0.4 et TD0.5 peuvent retourner les deux identifiants (INS-C et NIR utilisé comme INS) pour le DMP de chaque patient.
- Dans la suite du document le NIR utilisé comme INS est appelé INS.

NB : l'INS-C ne peut plus être utilisé en entrée des interfaces LPS v2 du système DMP.

***Patients mineurs***

Le système DMP offre, aux représentants légaux du patient, un accès au DMP du patient.

Dans le cadre de la protection des personnes mineures et des secrets à préserver vis-à-vis de leurs représentants légaux, les LPS doivent permettre à l'occasion du colloque professionnel / patient les actions suivantes :

- Connexion secrète au DMP (traces non visibles aux représentants légaux du patient) ;
- Dépôt de documents « invisibles aux représentants légaux du patient » ;
- Passage des documents « invisibles aux représentants légaux du patient » au statut « visible aux représentants légaux du patient ».

Le chapitre 2.4.4 décrit le cycle de vie de la visibilité d'un document aux patients mineurs et à ses représentants légaux.

Les fonctionnalités permettant ces actions doivent être activables par paramétrage.

Un autre paramètre défini l'âge en dessous duquel un patient est considéré comme mineur.

Ces deux paramétres sont diffusés par le système DMP via un fichier des paramètres. Cf. § 3.1.1 pour l'intégration de ces paramètres dans le LPS.

## 2.2 Acteurs et objectifs d'utilisation du système

L'usage des transactions DMP intégrées au LPS permet :

- l'alimentation du DMP d'un patient avec des documents de santé,
- la consultation des documents de santé du DMP d'un patient.

Chacun de ses objectifs correspond à un profil de DMP-compatibilité. Cf. §2.2.5.

Le LPS peut également fournir les données contextuelles pour l'accès Web-PS. Cette fonctionnalité est décrite dans le chapitre 5.4.

Le LPS (ou tout module logiciel d'un système d'information d'une structure de soins) peut accéder au Web-PS en mode Authentification Indirecte Renforcée (AIR) s'il respecte les restrictions liées au mode AIR décrites dans les types de LPS au chapitre 2.1. Ce type d'accès fait l'objet d'un profil de DMP-compatibilité présenté dans le chapitre 2.2.5. Cette fonctionnalité est décrite dans le chapitre 5.5.

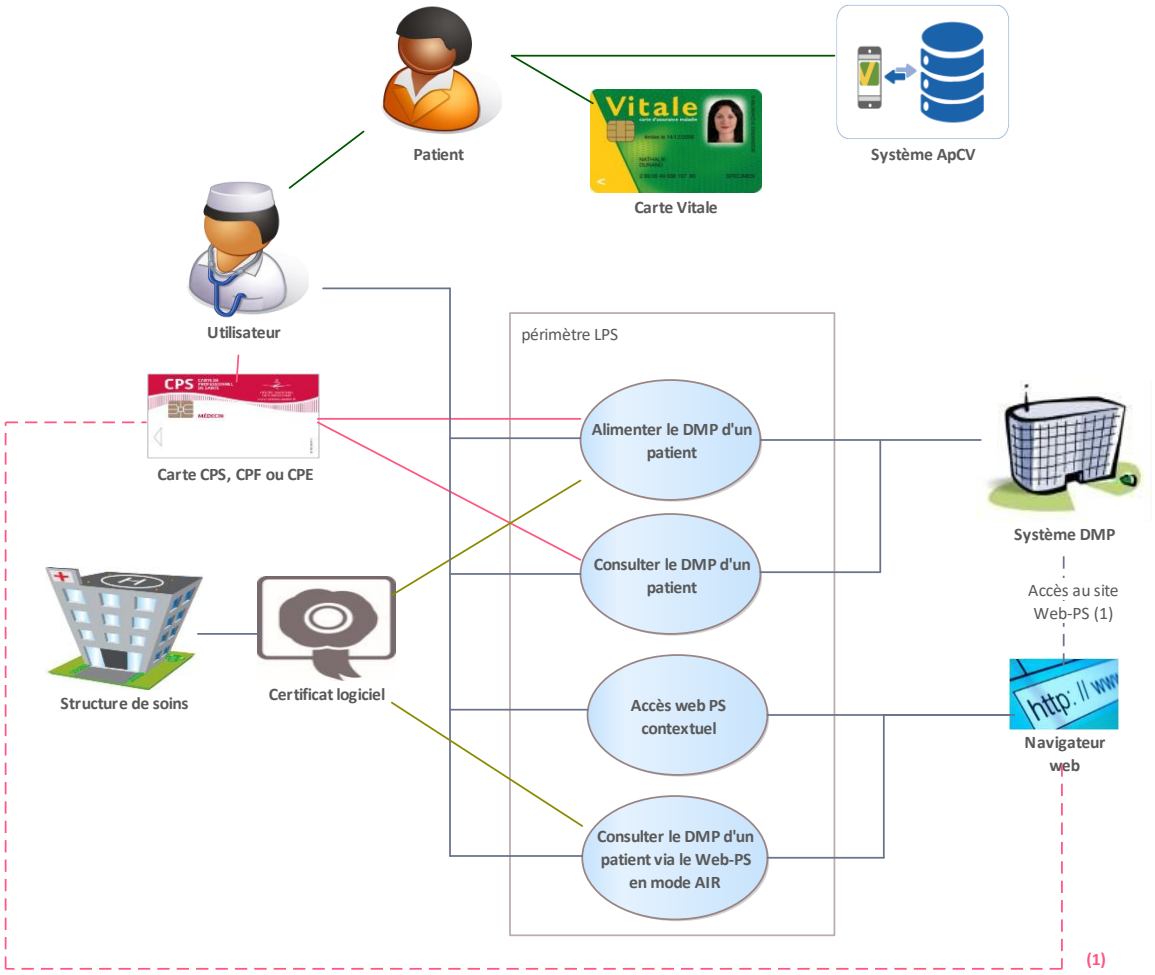



**Figure 2 : acteurs et objectifs métier du service DMP intégré au LPS**

## Acteurs

| | Définition du rôle |
|---|---|
| ***Utilisateur*** | Il s'authentifie auprès du système DMP. Cf. §2.2.1.<br>Il dispose de droits fonctionnels vis-à-vis du système DMP. Cf. §2.2.2.<br>Il est associé à un acteur de santé défini pour chaque type d'authentification. Cf. 2.2.3.<br>Il utilise les transactions DMP intégrés au LPS. Cf. 2.2.4.<br>Note : un composant d'architecture (ex : EAI, SIH…) peut dans certains cas interagir avec le système DMP pour le compte d'un utilisateur ou d'une structure de soins. Il a alors le même rôle que l'utilisateur. |
| ***Carte CPS, CPF ou CPE*** | Elle permet d'authentifier l'utilisateur en authentification directe. Cf. §2.2.1. |
| ***Certificat logiciel*** | Il permet d'authentifier la personne morale (structure de soins) qui réalise l'authentification locale de l'utilisateur. Cf. authentification indirecte et authentification indirecte renforcée (AIR) au §2.2.1. |
| ***Système DMP*** | Il héberge les DMP des patients et contrôle les accès à ces DMP. |
| ***Navigateur web*** | Il permet d'accéder à des fonctionnalités non disponibles via les transactions DMP ou non implémentées par l'éditeur.<br>L'accès au site Web PS (hors mode AIR) est hors périmètre de la DMP-compatibilité des LPS. Cf. (1) dans le schéma ci-dessus. |

**Tableau 1 : acteurs directs**

**Acteurs indirects**

| | Définition du rôle |
|---|---|
| ***Patient, carte Vitale, ApCV*** | Il est identifié selon les modalités définies dans le référentiel INS de l'ANS et des documents associés [REF-INS].<br>Il est également appelé titulaire du DMP. |
| ***Structure de soins*** | Elle définit le contexte d'usage professionnel et juridique (situation d'exercice…) de l'utilisateur. Elle présente le certificat logiciel permettant de l'authentifier. |

**Tableau 2 : acteurs indirects**

### 2.2.1 Mode d'authentification des utilisateurs

Le mode d'authentification a une forte influence sur les règles de gestion. Certaines fonctions sont accessibles ou pas selon le mode d'authentification. Par exemple, la consultation du DMP d'un patient n'est possible qu'en mode d'authentification directe.

La liste détaillée des fonctions accessibles ou pas selon le mode d'authentification est disponible dans le document [DMP-MDRF]. Cf. §2.2.2 pour plus d'informations au sujet des droits fonctionnels des utilisateurs.

Trois modes d'authentification de l'utilisateur sur le système DMP sont possibles pour un LPS. Le tableau ci-dessous indique les usages de chaque mode d'authentification.

| | Alimentation DMP | Consultation DMP |
|---|---|---|
| • authentification directe | X | X |
| • authentification indirecte | X | - |
| • authentification indirecte renforcée (AIR) | - | X |

NB : l'authentification déléguée n'est pas prise en charge par le système DMP.

**Authentification directe**

L'utilisateur utilise sa carte CPS (ou CPF ou CPE) pourvu qu'elle soit rattachée à une structure pour s'authentifier directement auprès du système DMP.

Pour un professionnel remplaçant, le LPS doit gérer l'affectation de ce professionnel remplaçant à une structure (et sa mémorisation pour une durée limitée).

Cf. chapitre 5.3.2 pour plus d'informations sur ce mode d'authentification.

NB : l'usage d'une e-CPS et de Pro Santé Connect n'est pas possible pour le DMP en mode intégré LPS pour l'instant.

**Authentification indirecte**

L'utilisateur utilise un LPS hébergé au sein d'une structure de soins et c'est cette structure qui s'authentifie auprès du système DMP au moyen d'un certificat logiciel d'authentification pour personne morale. Ce mode d'authentification est limité à l'alimentation du DMP.

Cependant, l'accès au système DMP nécessite que chaque utilisateur soit identifié nominativement. Il est donc indispensable que le LPS soit en mesure de fournir au système DMP l'identifiant (éventuellement interne) des utilisateurs à l'origine des transactions. Cf. le référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP) [REF-DMP] pour plus d'information sur ce sujet.

Cf. chapitre 5.3.3 pour plus d'informations sur ce mode d'authentification.

Pour l'alimentation du DMP avec identification FINESS de la structure de soins, trois modes sont identifiés en fonction des FINESS et des certificats utilisés.

| Certificats / FINESS | de l'entité juridique | de l'entité géographique |
|---|---|---|
| de l'entité juridique | Mode EJ [a] | - |
| de l'entité géographique | - | Mode EG [b] |
| de l'entité juridique et de l'entité géographique | Mode EJ/EG [c] | - |

[a] Il est fortement déconseillé de mettre en œuvre ce mode qui sera supprimé à terme.

[b] Le mode EG prévoit l'usage du FINESS de l'entité géographique dans le VIHF, dans les données des lots de soumission, et pour identifier la structure auteur des documents. Le mode EG est le seul disponible pour l'utilisation des certificats d'entité géographique.

[c] Le mode EJ/EG prévoit l'usage :

- du FINESS de l'entité juridique et du FINESS de l'entité géographique dans le VIHF et dans les données des lots de soumission,
- du FINESS de l'entité géographique pour identifier la structure auteur des documents.

Le mode EJ/EG sera, à terme, le seul disponible pour l'utilisation des certificats d'entité juridique.

**Authentification indirecte renforcée (AIR)**

Le mode AIR est un moyen alternatif à la CPS pour la consultation du DMP. Il ne peut pas être utilisé pour l'alimentation du DMP.

La consultation du DMP (avec identification FINESS de la structure de soins) reprend les modes EJ, EG et EJ/EG décrit ci-dessus pour l'authentification indirecte. Cependant, les données NameId et subject:role sont renseignées différemment dans le VIHF.

Cf. chapitre 5.3.4 pour plus d'informations sur ce mode d'authentification.

### 2.2.2 Utilisateurs et droits fonctionnels associés

Les droits fonctionnels des utilisateurs sont contrôlés par le système DMP. Les critères utilisés par celui-ci sont les suivants.

- Mode d'authentification : directe ou indirecte ou indirecte renforcée (AIR).
- Type de carte utilisée pour l'authentification directe : CPS, CPF ou CPE.
- Type d'utilisateur : professionnel ou autre personnel, médecin ou non, médecin traitant DMP ou non (cf. définition dans la suite du texte).
- Mode d'accès au DMP d'un patient : normal, centre de régulation, bris de glace.

Le document de référence concernant la description des droits fonctionnels des utilisateurs est [DMP-MDRF].

Dans la suite de ce chapitre, la description est fournie à titre d'illustration.

**Professionnels**

Parmi les professionnels, on distingue les cas suivants :

- D'une manière générale, une fois authentifiés, les professionnels peuvent alimenter des DMP pour leurs patients.
- Pour consulter les données administratives d'un DMP, les professionnels doivent être autorisés à y accéder par le titulaire du DMP (procédure auto-déclarative par le professionnel), sauf cas particulier (situation d'urgence).
- Les conditions d'accès en lecture aux documents contenus dans le DMP d'un patient (sur lequel ils ont l'autorisation d'accès) dépendent des professions et spécialités des professionnels recueillies à partir de la carte CPx du professionnel. Ces règles sont définies dans la matrice d'habilitation [DMP-MDRF].
- Seuls les médecins (code profession CPS/CPF 10) et l'auteur du document peuvent archiver/désarchiver un document (cf. cycle de vie d'un document au §2.4.3).
- Seul l'un des auteurs du document peut supprimer un document.
- Les médecins traitant DMP ont des droits étendus sur le DMP du patient. Ils peuvent accéder à tous les documents masqués de ce dossier (et si nécessaire démasquer un document masqué). En accès web PS, ils ont accès à l'historique des accès et actions sur un DMP et peuvent débloquer des professionnels bloqués sur un DMP.
- Les permanenciers auxiliaires de régulation médicale (PARM) des centres de réception et de régulation des appels des SAMU-Centres 15 (utilisation d'un LDRM) :
  - sont autorisés à utiliser la fonctionnalité de recherche du DMP d'un patient sans l'INS de ce patient,
  - ont accès aux DMP de tous les patients (mode d'accès « centre de régulation »).

    La consultation du DMP d'un patient reste réservée au médecin régulateur authentifié par sa CPS ou par sa CPF ou en mode AIR.

  Pour information :
  - Ce mode d'accès est indiqué dans le VIHF. Cf. §5.3.2, §5.3.3 et 5.3.4.5 pour l'alimentation du VIHF.
  - Le patient peut s'opposer à ce mode d'accès.
  - En cas de tentative d'accès en mode « centre de régulation » alors que le patient n'a pas autorisé cet usage, le système DMP renvoie une erreur « Accès interdit (le professionnel a été interdit d'accès par le patient) ». (DMPAccessForbidden).
  - L'utilisation de ce mode génère une trace spécifique dans le DMP du patient.
- Le professionnel utilise le mode d'accès « bris de glace » lorsque celui-ci a besoin de consulter le DMP d'un patient en cas d'urgence, sans avoir la possibilité de lui demander son accord.

  Pour information :
  - Ce mode d'accès est indiqué dans le VIHF. Cf. §5.3.2, §5.3.3 et §5.3.4.5 pour l'alimentation du VIHF.
  - Ce mode d'accès est accompagné de restrictions fonctionnelles.
  - Des exigences spécifiques s'appliquent. Cf. §3.2.3.1.
  - Le patient peut s'opposer à ce mode d'accès.
  - L'utilisation de ce mode génère une trace spécifique dans le DMP du patient.
  - L'usage du mode « bris de glace » est suivi par le système de pilotage du DMP pour détecter d'éventuels abus.
  - En cas de tentative d'accès en mode « bris de glace » alors que le patient n'a pas autorisé cet usage, le système DMP renvoie une erreur « Accès interdit (le professionnel a été interdit d'accès par le patient) ». (DMPAccessForbidden).

**Autres personnels**

Il s'agit du personnel d'accueil en structure de soins (via la GAM) ou en cabinet.

En authentification indirecte ou avec certaines CPE (secrétariats médicaux du secteur libéral ou EHPAD), ce personnel peut alimenter le DMP des patients.

L'authentification indirecte ou directe par CPE ne permet pas la consultation du DMP des patients.

### 2.2.3 Acteurs de santé

Pour le contrôle des autorisations d'accès au DMP d'un patient et aux documents qu'il contient, le système DMP utilise la notion d'acteur de santé.

Cette notion est définie comme suit.

- Pour les professionnels authentifiés par leur carte CPS ou CPF, l'acteur de santé est le professionnel.
- Pour les professionnels authentifiés en mode AIR, l'acteur de santé est le professionnel.
- Dans les autres cas, l'acteur de santé est la structure de soins.
  - Pour les utilisateurs authentifiés par leur carte CPE, par exemple les secrétaires médicaux du secteur libéral ou EHPAD, la structure de soins est identifiée dans la carte CPE.
  - Pour les utilisateurs en authentification indirecte (professionnels ou autres personnels), la structure de soins est identifiée dans le certificat logiciel pour personne morale utilisé pour se connecter sur le système DMP.

Exemples d'usage de la notion d'acteur de santé :

- Gestion des autorisations d'accès au DMP d'un patient (cf. DMP_0.3),
- Contrôle lors de l'alimentation du DMP d'un patient avec des documents (cf. EX_2.1-1140 dans le §3.4.1.1.3).

### 2.2.4 Description synthétique des transactions DMP intégrables au LPS

Le tableau ci-dessous décrit succinctement les transactions DMP. Ces transactions peuvent être liées fonctionnellement et certaines d'entre elles doivent être implémentées conjointement.

| | Transactions DMP | Description synthétique |
|---|---|---|
| | **Accès sécurisé au DMP d'un patient** | |
| *TD0.1* | Accès sécurisé au système DMP | Permet l'accès sécurisé aux web-services du système DMP. |
| *TD0.2* | Test d'existence du DMP d'un patient et vérification de l'autorisation d'accès | Permet de vérifier que le DMP d'un patient existe, de récupérer le statut de ce DMP et celui de l'autorisation d'accès de l'acteur de santé sur ce DMP. |
| *TD0.3* | Mise à jour de l'autorisation d'accès | Permet à l'acteur de santé de se déclarer autorisé par le patient à accéder au DMP du patient ou au contraire de se retirer de la liste des acteurs de santé autorisés. |
| *TD0.4* | Liste des DMP autorisés | Permet de récupérer la liste des DMP des patients pour lesquels l'acteur de santé dispose d'une autorisation d'accès. |
| *TD0.5* | Recherche sans INS de patient dans le système DMP | Permet de chercher le DMP d'un patient dans le système DMP, sans INS, à partir de traits d'identité. |
| *TD0.9* | Accès Web-PS Contextuel | Permet d'ouvrir le site web DMP dans un navigateur, avec passage contextuel d'informations. |
| *TD0.10* | Accès Web-PS Contextuel en mode AIR | Permet de déléguer l'authentification de l'utilisateur à la structure de soins pour accéder au Web-PS sans CPx. |
| | **Données administratives du DMP d'un patient** | |
| *TD1.3* | Données administratives du DMP d'un patient | Permet de consulter les données administratives du DMP d'un patient. |
| *TD1.6* | Liste des professionnels autorisés/bloqués sur le DMP d'un patient | Permet d'obtenir, pour le DMP d'un patient, la liste des acteurs de santé autorisés à y accéder, la liste des acteurs de santé bloqués, ou la liste contenant les deux. |
| | **Alimentation du DMP d'un patient** | |
| *TD2.1* | Alimentation en documents du DMP d'un patient | Permet de déposer un (ou des) document(s) dans le DMP d'un patient. Cette transaction gère aussi les mises à jour successives d'un document avec le remplacement d'un document par une nouvelle version. |
| *TD2.2* | Alimentation en documents du DMP d'un patient, par CPE | Transaction identique à TD2.1, mais dédiée aux utilisateurs authentifiés par carte CPE, par exemple les secrétaires médicaux du secteur libéral ou EHPAD. |
| | **Consultation du DMP d'un patient** | |
| *TD3.1* | Recherche de documents dans le DMP d'un patient | Permet de rechercher des documents dans l'index des documents du DMP d'un patient. |
| *TD3.2* | Consultation d'un document dans le DMP d'un patient | Permet de récupérer et consulter un document (à partir de l'identifiant du document récupéré par la TD3.1). |
| *TD3.3* | Gestion des attributs d'un document | Permet de gérer les attributs d'un document : masquer/démasquer aux professionnels, rendre visible au patient ou à ses représentants légaux, archiver / désarchiver et supprimer. |

**Tableau 3 : description des transactions**

L'enchainement des transactions et les restrictions par contexte sont présentés page 33.

### 2.2.5 Choix de profils de DMP-compatibilité à implémenter dans un LPS

Les profils suivants peuvent être implémentés au choix dans les LPS : profil « Alimentation », profil « Consultation » et profil « Consultation Web-PS en mode AIR ». Pour être DMP-compatible, un LPS doit proposer au moins un des trois profils.

Chaque profil de DMP-compatibilité est constitué de transactions obligatoires et de transactions optionnelles (voir tableau ci-dessous).

| | | Profils de DMP-compatibilité | | |
|---|---|---|---|---|
| | **Transactions DMP** | **Alimentation** | **Consultation (1)** | **Consultation Web-PS en mode AIR** |
| | **Accès sécurisé au DMP d'un patient** | | | |
| *TD0.1* | Accès sécurisé au système DMP | **Obligatoire** | | **Obligatoire (5)** |
| *TD0.2* | Test d'existence du DMP d'un patient et vérification de l'autorisation d'accès | **Obligatoire (2)** | | - |
| *TD0.3* | Mise à jour de l'autorisation d'accès | - | **Obligatoire (2)** | - |
| *TD0.4* | Liste des dossiers autorisés | Optionnel (7) | | - |
| *TD0.5* | Recherche sans INS de patient dans le système DMP | Optionnel | Optionnel (2) | - |
| *TD0.9* | Accès Web-PS Contextuel | Optionnel | **Obligatoire (2)** | - |
| *TD0.10* | Accès Web-PS Contextuel en mode AIR | - | Optionnel | **Obligatoire** |
| | **Données administratives du DMP d'un patient** | | | |
| *TD1.3* | Données administratives du DMP d'un patient | - | Optionnel | - |
| *TD1.6* | Liste des professionnels autorisés/bloqués sur le DMP d'un patient | - | Optionnel (1) | - |
| | **Alimentation du DMP d'un patient** | | | |
| *TD2.1* | Alimentation en documents du DMP d'un patient | **Obligatoire** | - | - |
| *TD2.2* | Alimentation en documents du DMP d'un patient, par CPE | **Obligatoire (6)** | - | - |
| | **Consultation du DMP d'un patient** | | | |
| *TD3.1* | Recherche de documents dans le DMP d'un patient | **Obligatoire (4)** | **Obligatoire (1)** | - |
| *TD3.2* | Consultation d'un document dans un DMP | - | **Obligatoire (1)** | - |
| *TD3.3* | Gestion des attributs d'un document | **Obligatoire (3)** | Optionnel (1) | - |

**Tableau 4 : liste des transactions à implémenter par profil**

(1) L'utilisation de la CPS (ou CPF) ou du mode AIR est obligatoire. Les CPE sont exclues.

(2) Sauf pour les LDRM pour lesquels la transaction TD0.5 est obligatoire et les transactions TD0.2, TD0.3, TD0.9 sont optionnelles.

(3) Seule l'implémentation de la suppression d'un document est obligatoire.

(4) Nécessaire pour rechercher l'identifiant technique à des fins de remplacement ou de suppression d'un document.

(5) Uniquement le mode AIR décrit dans le chapitre 5.3.4.

(6) Si le LPS intègre un des secteurs d'activité listés dans le périmètre des utilisateurs (§2.1).

(7) La TD0.4 ne doit pas être sollicitée en authentification indirecte.

**EX_GEN-1110**

L'éditeur doit obligatoirement implémenter les transactions « Obligatoires » du groupe de transactions « Accès sécurisé au système DMP ».

Ensuite, selon ses besoins, l'éditeur sélectionne le(s) profil(s) qu'il souhaite implémenter dans son LPS.

**EX_GEN-1120**

Pour chaque profil qu'il souhaite implémenter, l'éditeur doit obligatoirement implémenter les transactions « Obligatoires » du profil.

L'implémentation des transactions optionnelles relève du choix de l'éditeur.

En implémentant la transaction TD0.9 « Accès Web-PS Contextuel » ou la transaction TD0.10 « Accès Web-PS Contextuel en mode AIR », l'éditeur donne accès à ses utilisateurs, à partir de leur LPS / système d'information, aux fonctionnalités du DMP couvertes par l'Accès Web PS.

### Standards, normes et référentiels

Le tableau ci-dessous indique l'application des standards, normes et référentiels pour chaque profil de DMP-compatibilité.

Une description générale est disponible dans le chapitre 5.1. Cf. indications dans la marge.

Les documents de référence cités dans ce tableau sont décrits dans l'annexe 4.

| | | Profils de DMP-compatibilité | |
|---|---|---|---|
| | **Standards, normes, référentiels** | **Alimentation** | **Consultation (2)** |
| *5.1.1* | Cadre d'interopérabilité des SIS | Obligatoire | |
| | | Cf. [CI-TR-CLI-LRD], [CI-ANX-PS-STRU], [TRANS-ADELI-RPPS]. | |
| | | Cf. [CI-PARTAGE], [CI-STRU-ENTETE]. | |
| | | [CI-ANX-CDA], [TEST-CONTENU-CDA] | - |
| | Norme HL7 V3 (patient topic) | Obligatoire [CI-GESTPAT] (TD0.2) | Obligatoire (1) [CI-GESTPAT] (TD0.2) |
| | IHE PDQ | Optionnel [IHE-PDQV3] (TD0.5) | Optionnel (1) [IHE-PDQV3] (TD0.5) |
| *5.1.2* | Profil IHE XDS.b | Obligatoire [IHE-TF…] [IHE-DSG] (TD2.X) | Obligatoire [IHE-TF…] (TD3.X) |
| | | | |

**Tableau 5 : application des standards, normes et référentiels les profils de DMP-compatibilité Alimentation et Consultation**

(1) Sauf pour les LDRM pour lesquels la transaction TD0.5 est obligatoire et la transaction TD0.2 est optionnelle.

(2) hors profil « Consultation Web-PS en mode AIR ».

### 2.2.6 L'implémentation des profils de DMP-compatibilité dans les LPS

L'implémentation des profils de DMP-compatibilité dans les LPS :

- doit respecter les exigences définies dans le présent document. Elles seront contrôlées lors du processus d'homologation à la DMP-compatibilité,
- doit suivre les règles de bonnes pratiques qui sont de la responsabilité de l'éditeur,
- peut suivre (cela est laissé à l'appréciation de l'éditeur) les conseils et recommandations (par exemple ergonomiques) fournis par le GIE SESAM-Vitale (dans ce document ou lors du processus d'homologation à la DMP-compatibilité).

Les éditeurs doivent porter une attention particulière aux données utilisées dans les transactions.

- L'éditeur doit s'assurer que le LPS dispose de l'ensemble des données « requises » utilisées dans les transactions DMP. Si ce n'est pas le cas, il devra au préalable modifier le LPS pour intégrer les données manquantes. Pour rappel, les données exigées par le DMP sont cohérentes avec le cadre d'interopérabilité des SIS et donc avec l'ensemble des SIS nationaux.
- L'éditeur peut décider, pour le bénéfice de ses utilisateurs et si ce n'était initialement pas le cas, d'intégrer dans le LPS la gestion d'une donnée transmise par une transaction DMP.

**EX_GEN-1140**

Le LPS doit gérer correctement les codes retours et codes d'erreurs retournés par le système DMP qui peuvent déterminer, dans certains cas, les actions possibles ou pas vis-à-vis du DMP.

**EX_GEN-1145**

Les messages affichés doivent être spécifiques à chaque situation (code retour ou d'erreur) et facilement compréhensibles des utilisateurs.

**Recommandations d'ergonomie**

L'interfaçage du LPS avec le DMP nécessite la mise en place de nouvelles IHM dans les LPS DMP-compatibles. Dans ce document, la Cnam fournit aux éditeurs un certain nombre d'éléments de vocabulaire et d'ergonomie en cohérence avec l'Accès Web PS du système DMP.

**REC_GEN-1010**

Il est fortement recommandé d'intégrer au sein du LPS les éléments de vocabulaire et d'ergonomie fournis par la Cnam.

La Cnam met également à disposition une charte graphique à destination des éditeurs de logiciels DMP-compatibles [CHARTE-GRAPHIQUE_DMP-LPS] décrivant les éléments graphiques relatifs au DMP que les éditeurs peuvent intégrer dans leurs logiciels :

- logo indiquant que le logiciel est « DMP-compatible »,
- boutons d'actions pour accéder à l'Accès Web PS du DMP,
- boutons d'actions pour consulter ou alimenter un DMP,
- bouton d'état pour indiquer si le DMP est créé ou pas ou fermé, si le professionnel est autorisé ou pas.

**REC_GEN-1020**

Il est fortement recommandé d'intégrer au sein du LPS les éléments de la charte graphique fournis par la Cnam.

### Recommandations d'intégration

**REC_GEN-1030**

Le niveau d'intégration des transactions dans le LPS doit permettre au professionnel d'accéder au DMP sans rupture ergonomique dans l'utilisation de son LPS.

**REC_GEN-1050**

L'intégration de la fonction d'alimentation du DMP dans le LPS doit se faire avec le minimum d'impact pour le professionnel sur ses habitudes d'utilisation du LPS.

**EX_GEN-1060**

Les règles de déclenchement de l'envoi des documents dans le DMP doivent être claires et paramétrables par le professionnel. Elles doivent s'intégrer dans le processus de validation médicale des documents.

Le LPS alimente le DMP automatiquement.

Le professionnel doit pouvoir retenir un envoi de document par une action manuelle.

L'envoi de documents vides ou n'ayant pas évolué (sans modification du contenu du document ni de ses métadonnées associées conformément au paragraphe 3.5.3.1) est interdit.

**EX_GEN-1070**

Le choix des documents utiles à la coordination des soins à envoyer dans le DMP est défini réglementairement (code de la santé publique, notamment l'article L. 1111-15).

### 2.2.7 Homologation des profils implémentés

Lors du processus d'homologation, la DMP-compatibilité est vérifiée par profil / mode d'authentification.

L'homologation porte sur l'ensemble des transactions requises du profil et sur les transactions optionnelles que l'éditeur a décidé d'intégrer.

L'éditeur peut intégrer les différents profils ou transactions à son rythme, en passant plusieurs homologations pour des profils / transactions / mode d'authentification différents.

A chaque nouvelle homologation, la totalité des transactions fait l'objet de vérifications par le CNDA.

La liste des transactions intégrées par le LPS et validées par le processus de DMP-compatibilité est rattachée au numéro d'homologation fourni par le CNDA.

**EX_GEN-1170**

Le logiciel DMP-compatible doit impérativement proposer aux utilisateurs les transactions obligatoires des profils implémentés.

**EX_GEN-1180**

L'éditeur doit mettre en œuvre dans les LPS homologués un dispositif d'affichage du ou des profils de DMP-compatibilité homologués et de la date d'homologation (menu de type « à propos » par exemple).

Ce dispositif d'affichage doit également faire apparaître le nom de l'éditeur, du LPS et la version du LPS.

- Le nom du LPS doit correspondre à la donnée `LPS_Nom` alimentée dans le VIHF.
- La version du LPS doit correspondre à la donnée `LPS_Version` alimentée dans le VIHF.

Dans le cas d'une famille de produits, chaque produit doit porter un nom qui permette de le distinguer des autres produits de sa famille.

Dans tous les cas, chaque produit doit porter une version qui permette de le distinguer des autres versions de ce produit.

**EX_GEN-1190**

L'éditeur doit préciser dans la documentation de fonctionnement des LPS homologués les fonctions DMP intégrées, ainsi que celles qui ne le sont pas.

### 2.2.8 Spécificités concernant certains documents gérés dans le SI DMP

En règle générale, la DMP-compatibilité est indépendante des documents gérés dans le SI DMP.

Pour les documents créés par d'autres acteurs (patient et Assurance Maladie), l'exigence EX_2.1-1010 indique qu'il n'est pas possible de les créer via l'interface LPS.

Les autres spécificités sont documentées dans le chapitre 6, notamment pour l'évolution « carnet de vaccinations intégré aux LPS » et pour les « données de remboursement ».

## 2.3 Description des processus

Ce chapitre présente un processus pour chaque profil de DMP-compatibilité.

- Profil Alimentation : alimenter le DMP d'un patient,
- Profil Consultation : consulter le DMP d'un patient.

Ce chapitre présente également un processus regroupant les deux profils de DMP-compatibilité Alimentation et Consultation.

Pour le profil Consultation Web-PS en mode AIR, cf. chapitre 5.5.

**Préambule**

Ces processus sont fournis à titre informatif pour présenter une mise en œuvre possible de l'ensemble des transactions DMP intégrées au LPS.

Ces processus à but illustratif ne sont pas imposés pour la DMP-compatibilité.

### 2.3.1 Description générale

Chaque processus est découpé en trois grandes étapes :

- La première étape est commune aux deux processus. Elle permet d'acquérir des données utilisées plusieurs fois dans la suite des processus. Cf. ❶ ci-dessous.
- La deuxième étape est également commune aux deux processus. Elle permet de vérifier l'autorisation d'accès de l'acteur de santé au DMP du patient. Cf. ❷ ci-dessous.
- La dernière étape est spécifique à chaque processus. Cf. ❸, ❹ et ❺ ci-dessous.

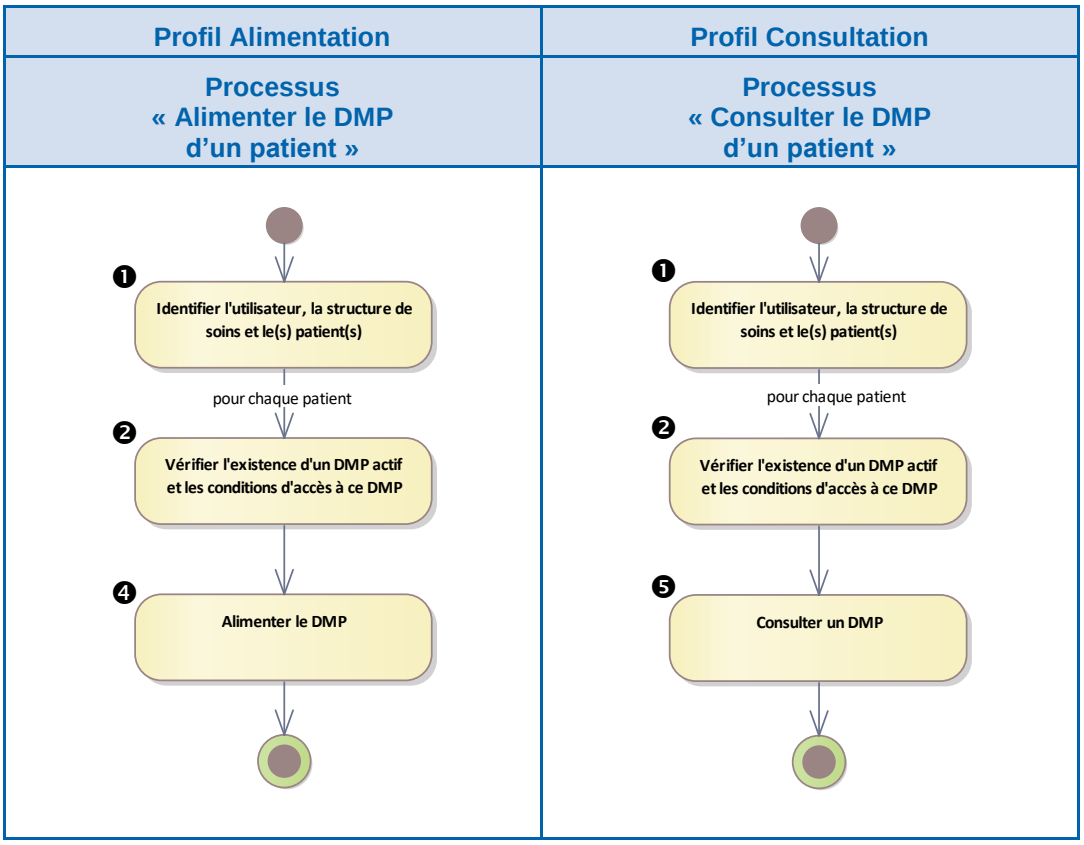



**Figure 3 : présentation synthétique des processus**

Le déroulement de chaque étape est décrit ci-dessous.

❶ Etape « Identifier l'utilisateur, la structure de soins et le(s) patient(s) ».

Le LPS identifie l'utilisateur (professionnel ou autre personnel) et la structure de soins. Cette fonctionnalité est locale au LPS.

Trois possibilités sont offertes pour trouver l'INS et/ou le DMP du ou des patients.

- L'INS du patient est obtenu conformément au référentiel INS [REF-INS]. Cette fonctionnalité n'utilise aucune transaction DMP.
- Le LPS utilise une transaction pour lister des DMP des patients pour lesquels l'acteur de santé a une autorisation d'accès (TD0.4).
- Le LPS utilise une transaction pour rechercher le DMP d'un patient à partir de traits d'identité (TD0.5).

Résultat de cette étape : l'utilisateur, la structure de soins et le(s) patient(s) sont identifiés

Si plusieurs patients sont identifiés (par exemple via TD0.4), la suite du processus se déroule pour chaque patient.

Seuls les INS obtenus conformément au cadre du référentiel INS [REF-INS] peuvent être utilisés pour accéder aux DMP des patients.
La transaction de recherche d'un DMP d'un patient à partir de traits d'identité (TD0.5) ne doit être utilisée qu'en cas d'impossibilité d'obtenir l'INS conformément au référentiel INS et des documents associés [REF-INS].
Dans tous les cas, les mesures à mettre en œuvre pour assurer la bonne identification du patient relèvent de la responsabilité de l'utilisateur. Elles sont décrites dans le Référentiel National d'IdentitoVigilance (RNIV) [REF-INS].

❷ Etape « Vérifier l'existence d'un DMP actif et les conditions d'accès à ce DMP ».

Le LPS utilise la transaction TD0.2 pour vérifier si le DMP d'un patient existe, s'il est actif et si l'acteur de santé dispose d'une autorisation d'accès à ce DMP.

Le LPS gère en local (= hors SI DMP) les conditions d'accès à ce DMP par l'acteur de santé :

- non opposition du patient à l'alimentation de son DMP,
- consentement du patient à la consultation de son DMP.

Dans le cas où le patient n'est pas en capacité de donner son accord, un accès en mode « bris de glace » est possible pour la consultation du DMP.

La vérification de l'autorisation d'accès ne s'applique pas pour le mode d'accès « centre de régulation ». Dans ce mode, l'accès est toujours autorisé (sauf si le patient a déclaré y être opposé).

Cette autorisation d'accès n'est pas à soumettre pour alimenter le DMP avec des documents et pour supprimer des documents si le LPS implémente le profil Alimentation.

Profil Consultation uniquement :

- Si le patient consent à la consultation de son DMP et si l'acteur de santé a une autorisation d'accès à un DMP actif d'un patient, il peut effectuer une action sur ce DMP (cf. étape ❺).
- Il peut ajouter, avec le consentement du patient, une autorisation d'accès si celle-ci est inexistante ou expirée (via TD0.3) ou passer en mode « bris de glace ». L'acteur de santé peut ensuite effectuer une action de consultation sur ce DMP (cf. étape ❺).
- Résultat de cette étape : l'acteur de santé a l'autorisation d'accès au DMP du patient et le consentement du patient pour y accéder.

NB1 : seul « Mon espace santé » permet la réactivation du DMP d'un patient. En cas de DMP inexistant ou fermé pour un patient, les processus s'arrêtent et l'acteur de santé ne peut effectuer aucune action sur le DMP concerné.

NB2 : l'étape ❷ est facultative si le LPS a utilisé la transaction permettant de lister les DMP autorisés (TD0.4) à l'étape ❶.

❹ Etape « Alimenter le DMP d'un patient ».

Les actions possibles sont les suivantes.

- Alimenter ce DMP (via TD2.1 ou TD2.2) avec des nouveaux documents.
- Rechercher un document dans le DMP d'un patient (via TD3.1) puis :
  - remplacer un document par une nouvelle version (via TD2.1 ou TD2.2),
  - archiver un document (via TD3.3),
  - supprimer un document (via TD3.3).

Résultat de cette étape : une action d'alimentation, d'archivage ou de suppression est effectuée.

❺ Etape « Consulter le DMP d'un patient ».

Les actions possibles sont les suivantes.

- Rechercher des documents dans le DMP d'un patient (via TD3.1) puis :
  - consulter un document (via TD3.2),
  - modifier les attributs d'un document (via TD3.3),
  - supprimer un document (via TD3.3).

La modification des attributs d'un document permet les actions suivantes.

- Masquer ou démasquer un document aux autres acteurs de santé.
- Rendre visible un document au patient ou à ses représentants légaux.
- Archiver ou désarchiver un document.

Résultat de cette étape : une action de consultation, de modification ou de suppression est effectuée.

Il est également possible d'effectuer les actions suivantes :

- Supprimer une autorisation d'accès (via TD0.3).
- Consulter les données administratives (via TD1.3).
- Lister les professionnels autorisés / bloqués sur ce DMP (via TD1.6).

***Deux profils***

Pour un LPS implémentant les deux profils de DMP-compatibilité Alimentation et Consultation, les deux processus décrits en amont dans ce chapitre peuvent être fusionnés en un seul comme indiqué ci-dessous.

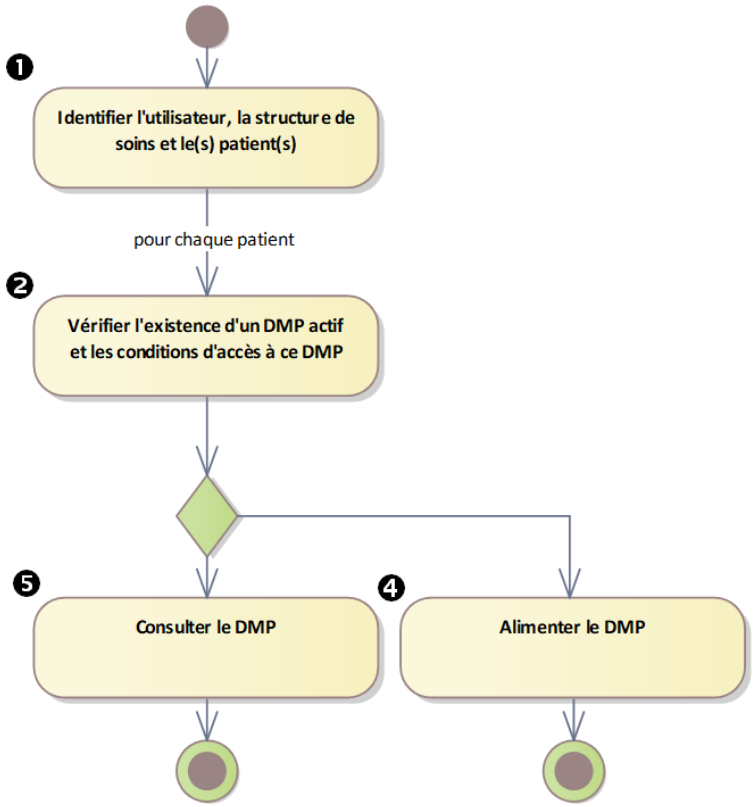



**Figure 4 : présentation synthétique du processus regroupant les deux profils Alimentation et Consultation**

## 2.3.2 Fonctionnalités mises en œuvre

Ce chapitre présente les fonctionnalités du LPS et leur enchaînement dans le cadre des processus décrits dans le chapitre précédent.

Ce chapitre ne présente pas le détail des contrôles des droits des utilisateurs ni l'ensemble des cas d'erreur. Ces éléments sont décrits dans le chapitre 3.

Deux types de fonctionnalités sont identifiés.

- Les fonctionnalités du LPS mettant en œuvre une transaction DMP. Ces fonctionnalités sont référencées DMP_x.y en correspondance avec la référence TDx.y de la transaction utilisée. Par exemple, la fonctionnalité DMP_0.2 met en œuvre la transaction TD0.2.
  NB1 : la transaction TD0.3 est utilisée à différents endroits dans les processus. Dans ce cas, on identifie deux fonctionnalités :
  - DMP_0.3a Ajouter une autorisation d'accès pour la consultation du DMP,
  - DMP_0.3b Supprimer une autorisation d'accès,

  NB2 : les transactions TD2.1 et TD2.2 peuvent être utilisées dans deux fonctionnalités.
  - DMP_2.1a/2.2a Alimenter le DMP d'un patient avec des nouveaux documents.
  - DMP_2.1b/2.2b Remplacer un document existant dans le DMP d'un patient.
- Les fonctionnalités du LPS ne mettant en œuvre aucune transaction DMP. Ces fonctionnalités sont référencées DMP_a et DMP_b.
  Par exemple : DMP_a Acquérir les données concernant l'utilisateur.

Le tableau ci-dessous décrit la correspondance entre les fonctionnalités LPS et les transactions du système DMP.

| Fonctionnalité | Transaction | Commentaire |
|---|---|---|
| DMP_a | - (Fonctionnalité locale au LPS) | Acquisition des données concernant l'utilisateur. |
| DMP_b | - (Fonctionnalité locale au LPS) | Acquisition des données concernant le patient. |
| DMP_0.2 | TD0.2 | Vérifier l'existence d'un DMP actif et les conditions d'accès à ce DMP |
| DMP_0.3a | TD0.3 | La transaction TD0.3 est utilisée dans deux contextes différents :<br>• Ajouter une autorisation pour la consultation du DMP (DMP_0.3a)<br>• Supprimer une autorisation (DMP_0.3b) |
| DMP_0.3b | | |
| DMP_0.4 | TD0.4 [2] | Liste des DMP autorisés. |
| DMP_0.5 | TD0.5 | Recherche d'un DMP sans l'INS du patient. |
| DMP_1.3 | TD1.3a | TD1.3a permet de consulter les données administratives. |
| DMP_1.6 | TD1.6 | Liste des acteurs de santé sur un DMP. |
| DMP_2.1a/2.2a | TD2.1 ou TD2.2 | Alimentation d'un DMP avec des documents.<br>TD2.1 est utilisé en authentification par carte CPS/CPF ou en authentification indirecte.<br>TD2.2 est utilisée en authentification par carte CPE. |
| DMP_2.1b/2.2b | TD2.1 ou TD2.2 | |
| DMP_3.1a | TD3.1 | Recherche d'un document dans un DMP.<br>DMP_3.1a s'applique pour le profil « Consultation » en authentification directe par CPS/CPF ou en mode AIR.<br>DMP_3.1b s'applique dans les autres cas. |
| DMP_3.1b | | |
| DMP_3.2 | TD3.2 | Consultation d'un document dans le DMP. |
| DMP_3.3a/3.3b/3.3d | TD3.3a/ TD3.3b/ TD3.3c/ TD3.3d | DMP_3.3a/3.3b/3.3d permet de modifier les attributs d'un document :<br>• masquer / démasquer aux professionnels (TD3.3a) ;<br>• rendre visible au patient ou à ses représentants légaux (TD3.3b) ;<br>• archiver / désarchiver (TD3.3d).<br>DMP_3.3c permet de supprimer un document (TD3.3c).<br>a, b, c et d représentent des données en entrée différentes pour une même transaction TD3.3. |
| DMP_3.3c | | |

**Tableau 6 : correspondance entre les fonctionnalités LPS et les transactions du système DMP**

L'enchainement des fonctionnalités et les restrictions par contexte sont présentés page 33.

[2] En cas d'absence d'INS dans la réponse de la transaction TD0.4, l'INS doit être obtenu conformément au référentiel INS et aux documents associés [REF-INS].

### Transactions

Les transactions mises en œuvre (TDx.y) sont indiquées dans les processus sous la forme suivante : « (via TDx.y) ». Par exemple :


Les exceptions suivantes sont à noter. Les éléments techniques « Accès sécurisé au système DMP » (TD0.1), « Accès Web-PS Contextuel » (TD0.9) et Accès Web-PS Contextuel en mode AIR (TD0.10) n'apparaissent pas dans les processus. Cf. §5.3 et §5.4 et §5.5 pour plus d'informations.

### Modes d'accès

La prise en compte des modes d'accès « centre de régulation » et « bris de glace » est décrite dans la fonctionnalité DMP_0.2 Vérifier l'existence d'un DMP actif et les conditions d'accès à ce DMP.

### Code couleur

Le tableau ci-dessous indique

- Le code couleur utilisé dans les schémas.
  - Les fonctionnalités n'utilisant aucune transaction DMP sont de couleur beige.
  - Les autres couleurs sont reprises de la description des transactions DMP intégrables au LPS (§2.2.4).
- Les chapitres contenant la description détaillée des fonctionnalités.

| | Groupes de fonctionnalités | Description détaillée |
|---|---|---|
| *DMP_x* | **Fonctionnalités d'acquisition des données de contexte** | **3.1** |
| *DMP_0.x* | **Accès sécurisé au DMP d'un patient (via TD0.x)** | **3.2** |
| *DMP_1.x* | **Données administrative du DMP d'un patient (via TD1.x)** | **3.3** |
| *DMP_2.x* | **Alimentation du DMP d'un patient (via TD2.x)** | **3.4** |
| *DMP_3.x* | **Consultation du DMP d'un patient (via TD3.x)** | **3.5** |

**Tableau 7 : code couleur utilisé dans les schémas**

NB : la création et la réactivation d'un DMP sont prises en charge par « Mon espace santé ». Elles apparaissent sur fond blanc et ne sont plus référencées DMP_1.1 et DMP_1.2.

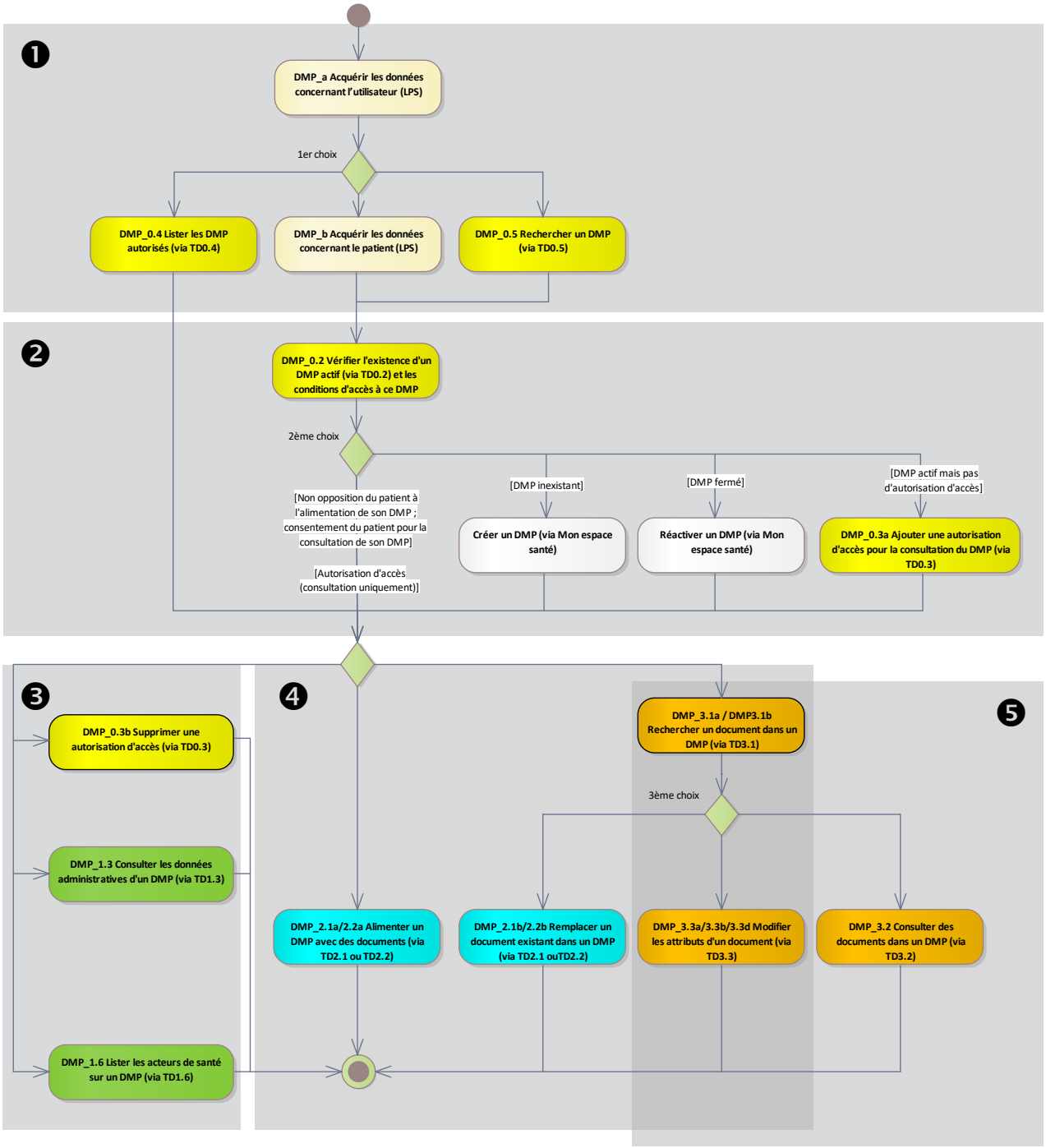



**Figure 5 : processus regroupant les deux profils Alimentation et Consultation**

Dans le schéma ci-dessus, le terme « DMP » fait référence au DMP d'un patient.

Les choix présentés dans le processus sont décrits dans les fonctionnalités suivantes.

- 1er choix : cf. RG_0090 à la fin du chapitre 3.1.2.
- 2ème choix : cf. RG_0330 à la fin du chapitre 3.2.2.1.
- 3ème choix :
  - Pour les LPS donnant accès à la consultation des documents (DMP_3.2), cf. RG_3060 à la fin du chapitre 3.5.1.1 ;
  - Pour les LPS ne donnant pas accès à la consultation des documents (DMP_3.2), cf. RG_3140 à la fin du chapitre 3.5.1.2.

Une déclinaison de ce processus pour les profils de DMP-compatibilité Alimentation et Consultation est disponible en annexe 5.

## 2.4 Description des principales entités fonctionnelles

Les principales entités fonctionnelles manipulées pour l'intégration des transactions DMP dans le LPS sont organisées comme suit.

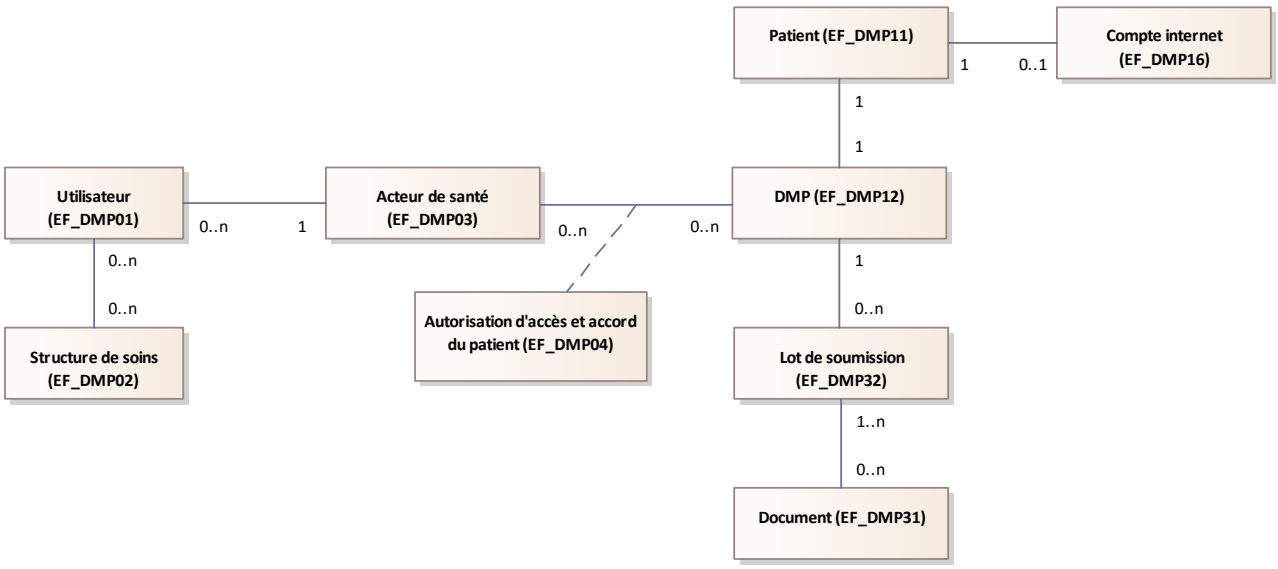



**Figure 6 : présentation des principales entités fonctionnelles**

### Utilisateur et acteur de santé

Pour la description des utilisateurs et des acteurs de santé, cf. §2.2.3.

### Autorisation d'accès et accord du patient

Chaque acteur de santé a accès à un ensemble de DMP.

Un DMP peut être accédé par plusieurs acteurs de santé.

Une autorisation d'accès à un DMP est attribuée à un acteur de santé.

L'accès au DMP par un acteur de santé est soumis à l'accord du patient :

- non opposition du patient à l'alimentation de son DMP,
- consentement du patient à la consultation de son DMP.

NB1 : ces deux notions sont gérées par le LPS en local (= hors SI DMP).

NB2 : la notion d'autorisation d'accès est gérée dans l'interface avec le SI DMP pour le profil Consultation.

### DMP et patient

Chaque DMP correspond à un et un seul patient identifié par son INS.

Le cas d'un patient qui possède plusieurs INS est décrit dans le référentiel INS.

Vis-à-vis du système DMP, chaque DMP n'est associé qu'à un seul patient.

### DMP et document

Chaque DMP contient un ensemble de documents.

Les documents sont transmis au système DMP dans des lots de soumission. Cf. §3.4.1.1.6.

Un document peut être référencé dans plusieurs lots de soumission.
Cf. REC_2.1-1160 § 3.4.1.1.5 et REC_3.2-1080 § 3.5.2.1.

### 2.4.1 Cycle de vie du DMP d'un patient

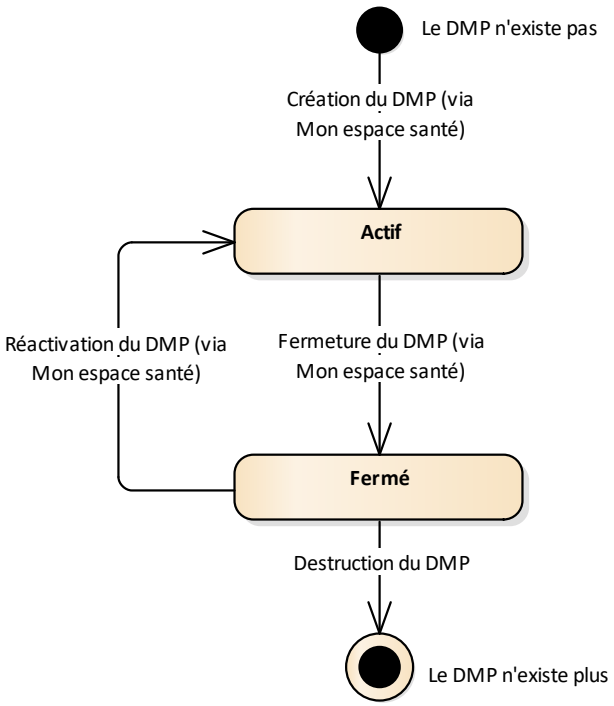



**Figure 7 : cycle de vie du DMP d'un patient**

NB : le cycle de vie du DMP d'un patient est indiqué à titre informatif, car il ne peut pas être géré via les transactions DMP exposées aux LPS.

| Statut | Description |
|---|---|
| Le DMP n'existe pas<br>ou<br>Le DMP n'existe plus | La création des DMP est prise en charge par « Mon espace santé » et n'est plus disponible dans le cadre de la DMP compatibilité des LPS. |
| Actif | Il est possible d'utiliser ce DMP à condition de disposer de l'accord du patient (non opposition pour l'alimentation ; consentement pour la consultation), et selon les règles d'usage du DMP.<br>La fermeture des DMP est prise en charge par « Mon espace santé » et n'est plus disponible dans le cadre de la DMP compatibilité des LPS. |
| Fermé | La réactivation des DMP est prise en charge par « Mon espace santé » et n'est plus disponible dans le cadre de la DMP compatibilité des LPS.<br>Aucune action n'est possible sur ce DMP tant qu'il n'a pas été réactivé. |

### 2.4.2 Cycle de vie d'une autorisation d'accès pour la consultation du DMP

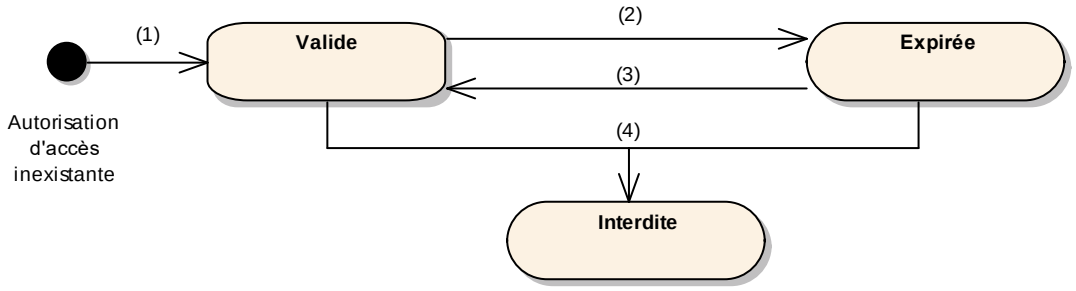



**Figure 8 : cycle de vie d'une autorisation d'accès pour la consultation du DMP**

| | Description des transitions |
|---|---|
| *(1) et (3)* | En pratique, l'autorisation d'accès est déclarée dans le DMP par l'acteur de santé :<br>• qui a créé le DMP avant l'ouverture d'un « Mon espace santé » pour le patient concerné (l'acteur de santé dispose alors d'une autorisation d'accès à ce DMP),<br>• à l'aide de la transaction TD0.3 « Mise à jour de l'autorisation ».<br>Pour information, d'autres possibilités de modification des autorisations d'accès existent via l'accès web PS. |
| *(2)* | Une autorisation peut prendre fin de l'une des façons suivantes :<br>• lorsqu'elle est supprimée par l'acteur de santé lui-même via la transaction TD0.3 « Mise à jour de l'autorisation »,<br>• en cas de non-usage par le professionnel pendant une période donnée (paramétrable au niveau du système DMP et actuellement positionnée à 6 mois). Non applicable aux structures de soins,<br>• lors de la fermeture du DMP. Dans ce cas, toutes les autorisations rattachées prennent fin,<br>• suite à la destruction du DMP du patient (hors périmètre LPS).<br>Pour information, d'autres possibilités existent via l'accès web PS. |
| *(4)* | Une autorisation devient interdite en cas d'inscription du professionnel dans la liste des professionnels bloqués.<br>Pour information, cette modification n'est pas applicable aux structures de soins et n'est disponible que pour le médecin traitant DMP via l'accès web ou pour le patient lui-même. |

| Statut | Description |
|---|---|
| Autorisation inexistante<br>ou<br>Expirée | L'acteur de santé **ne peut pas** accéder au DMP du patient pour le consulter.<br>L'acteur de santé **peut alimenter** le DMP avec des documents **et supprimer** des documents si le LPS implémente le profil Alimentation.<br>L'acteur de santé **peut** se déclarer autorisé à consulter. |
| Valide | L'acteur de santé **peut** accéder au DMP du patient.<br>L'acteur de santé **peut** supprimer une autorisation d'accès. |
| Interdite | L'acteur de santé **ne peut pas** accéder au DMP du patient pour le consulter.<br>L'acteur de santé **peut alimenter** le DMP avec des documents **et supprimer** des documents si le LPS implémente le profil Alimentation.<br>L'acteur de santé **ne peut pas** à nouveau se déclarer autorisé. |

### 2.4.3 Cycle de vie d'un document

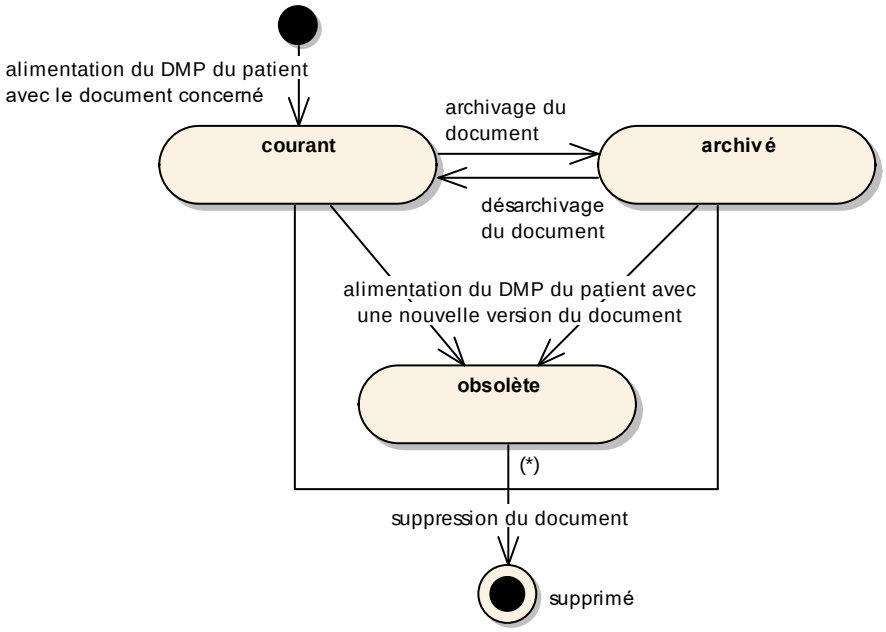



**Figure 9 : cycle de vie d'un document dans le DMP d'un patient**

(*) La suppression d'un document obsolète n'est pas possible directement. Elle est effectuée par le système DMP lors de la suppression du document qui a remplacé ce document obsolète.

| Statut | Description |
|---|---|
| Courant | Statut par défaut lors de l'alimentation du DMP du patient.<br>Si plusieurs versions d'un même document sont stockées dans le DMP du patient, seule la dernière version du document ajoutée est au statut « courant ». |
| Obsolète | Si plusieurs versions d'un même document sont stockées dans le DMP du patient, toutes les versions sauf la dernière sont au statut « obsolète ». |
| Archivé | Ce statut indique que le document n'est plus utile dans la pratique médicale courante du professionnel.<br>Le document reste cependant accessible lors d'une recherche.<br>NB : il s'agit d'un archivage « fonctionnel » et non d'un archivage « physique ». |
| Supprimé | Un document supprimé n'apparaît plus dans les listes de documents (TD3.1) et ne peut plus être consulté (TD3.2), ni déposé avec le même identifiant (TD2.1 ou TD2.2).<br>NB : il s'agit d'une suppression « logique » et non d'une suppression « physique ». |

### 2.4.4 Cycle de vie de la visibilité d'un document

La visibilité d'un document est gérée par rapport à trois populations :

- Les professionnels ;
- Les patients ;
- Les représentants légaux du patient.

Un document peut être visible ou non pour chacune de ces populations.

En fonction du type de population, on parle de :

- Document masqué (= non visible) ou non masqué (= visible) aux professionnels ;
- Document visible ou non visible (ou invisible) aux patients ;
- Document visible ou non visible (ou invisible) aux représentants légaux du patient.

Toutes les combinaisons de visibilité sont possibles. Dans un premier temps le cumul des confidentialités « non visible au patient » et « masqué aux professionnels » n'est pas possible : l'application de cette contrainte est paramêtrable. Cf. paramètre `cumul-invisible_patient-masque_ps`[3] au § 3.1.1.

NB1 : le LPS ne peut demander un changement de visibilité que pour un document courant ou archivé. Ce changement est propagé automatiquement par le système DMP aux versions obsolètes de ce document.

NB2 : le cycle de vie décrit ci-dessous ne concerne pas les documents supprimés.

NB3 : le masquage aux professionnels d'un document s'effectue à la demande du patient.

NB4 : seuls les professionnels en authentification directe par CPS/CPF ou en mode AIR peuvent consulter les documents du DMP d'un patient.

NB5 : la gestion de la visibilité des documents aux représentants légaux d'un patient mineur est une fonctionnalité activable par paramétrage. Cf. paramètre `fonctions-gestion-mineurs` au § 3.1.1.

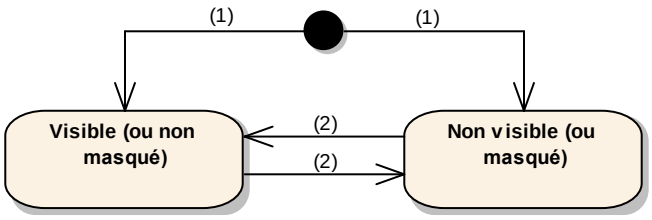



**Figure 10 : cycle de vie de la visibilité d'un document dans le DMP d'un patient (un statut pour chaque population : professionnel, patient, représentants légaux)**

[3] Le nom technique n'évolue pas. Il conserve le terme « PS ».

| | Description des transitions |
|---|---|
| *(1)* | Lors de l'alimentation du DMP du patient avec un document, on peut choisir un statut de visibilité pour chaque population (professionnel, patient, représentants légaux). |
| *(2)* | La transaction TD3.3 permet de modifier le statut de visibilité d'un document pour chaque population (professionnel, patient, représentants légaux).<br>Le masquage d'un document aux professionnels est réversible :<br>• Le patient peut retirer le masquage d'un document aux professionnels ;<br>• Le démasquage peut être réalisé par les médecins traitants DMP pour tous les documents et par les autres professionnels pour les documents dont ils sont l'auteur.<br>Le passage d'un document au statut visible pour le patient ou pour ses représentants légaux est irreversible :<br>• Lorsqu'un document initialement invisible au patient a été rendu visible au patient, il ne peut plus être rendu invisible au patient. De la même manière, un document qui a toujours été visible au patient ne peut pas être rendu invisible au patient.<br>• Lorsqu'un document initialement invisible aux représentants légaux leur a été rendu visible, il ne peut plus leur être rendu invisible. De la même manière, un document qui a toujours été visible aux représentants légaux ne peut pas leur être rendu invisible. |

Le statut de visibilité d'un document est défini pour chaque population :

- Professionnels .

| Statut | Description |
|---|---|
| Non masqué | Le document peut être consulté par les professionnels. |
| Masqué | Le document ne peut pas être consulté par les professionnels sauf par son auteur et par les médecins traitants DMP déclarés dans le DMP du patient (ce filtrage est fait par le système DMP). |

- Patient ;

| Statut | Description |
|---|---|
| Visible | Le document peut être consulté par le patient. |
| Non visible (ou invisible) | Le document ne peut pas être consulté par le patient. |

- Représentants légaux du patient ;

| Statut | Description |
|---|---|
| Visible | Le document et les traces associées peuvent être consultés par les représentants légaux du patient. |
| Non visible (ou invisible) | Le document et les traces associées ne peuvent pas être consultés par les représentants légaux du patient. |

Le patient a la possibilité de masquer des documents aux professionnels. Il peut demander au professionnel de le faire pour lui.

Note 1 : par défaut (paramétrage au niveau du système DMP), les documents masqués aux professionnels sont visibles en mode urgence. Le patient peut néanmoins, via son accès internet DMP uniquement, modifier les modalités d'accès des professionnels aux documents masqués en mode urgence.

Note 2

- Dans la situation actuelle, le SI DMP ne gère qu'un seul compte d'accès au DMP pour un patient et ses représentants légaux. De ce fait, si le document a un statut non visible pour un patient et/ou pour les représentants légaux de ce patient, il ne pourra être consulté ni par le patient, ni par les représentants légaux de ce patient.
- Ce comportement est transitoire et pourra être modifié dans l'avenir. Dans tous les cas, l'acquisition des statuts de visibilité des documents au patient et à ses représentants légaux doit être traitée de manière indépendante par le LPS. Cf. RG_2030, page 86.

# 3 DESCRIPTION DETAILLEE DES FONCTIONNALITES ET DES TRANSACTIONS

Ce chapitre reprend l'organisation des groupes de fonctionnalités présentées dans le chapitre 2.3.

| | Groupes de fonctionnalités | Description détaillée |
|---|---|---|
| *DMP_x* | **Fonctionnalités d'acquisition des données de contexte** | **3.1** |
| *DMP_0.x* | **Accès sécurisé au DMP d'un patient (via TD0.x)** | **3.2** |
| *DMP_1.x* | **Données administrative du DMP d'un patient (via TD1.x)** | **3.3** |
| *DMP_2.x* | **Alimentation du DMP d'un patient (via TD2.x)** | **3.4** |
| *DMP_3.x* | **Consultation du DMP d'un patient (via TD3.x)** | **3.5** |

## 3.1 Fonctionnalités d'acquisition des données de contexte

Ce chapitre décrit des fonctionnalités locales au LPS permettant d'acquérir des données qui sont utilisées plusieurs fois dans les autres fonctionnalités.

### 3.1.1 Pré-requis au processus DMPi

Ce chapitre présente les éléments devant être mis en œuvre avant chaque démarrage du processus DMPi.

**EX_GEN-1540**

Le LPS doit s'actualiser avec les paramètres contenus dans le fichier des paramètres au moins une fois par semaine.

Le fichier des paramètres est disponible en téléchargement sur une URL définie dans [FI-URL].

Le LPS doit savoir gérer les redirections HTTPS 3xx pour le téléchargement de ce fichier.

**EX_GEN-1222**

Il est demandé à un LPS de prendre en compte rapidement le changement de l'URL du fichier des paramètres.

Le délai de mise à jour à respecter sera communiqué par le GIE SESAM-Vitale.

Le fichier des paramètres contient les paramètres suivants.

Le bloc `<parameter-list code="param-si-dmp">` contient les paramètres liés au fonctionnement du système DMP.

| Paramètre | Signification |
|---|---|
| `fonctions-gestion-mineurs` | Ce paramètre indique si le LPS doit activer les fonctionnalités suivantes :<br>• « Connexion secrète ». Cf. balise `confidentiality-code` dans le VIHF (§ 5.3.2, § 5.3.3 et §5.3.4.5).<br>• Gestion de l'invisibilité d'un document aux représentants légaux d'un patient mineur. Cf. définition §2.4.4.<br>Ce paramètre peut prendre les valeurs suivantes : `true` (= activer), `false` (= désactiver). |
| `cumul-invisible_patient-masque_ps`[4] | Ce paramètre indique si le LPS doit activer la possibilité, pour un document, de cumuler les confidentialités « invisible au patient » et « masqué au professionnel ». Cf. définition §2.4.4.<br>Ce paramètre peut prendre les valeurs suivantes : `true` (= activer), `false` (= désactiver). |
| `age-majorite` | Contient l'âge (en années) en dessous duquel le patient doit être considéré comme mineur. Cf. EX_GEN-1550 § 3.1.3. |
| `hr-periode-max-mois` | Ce paramètre indique la durée maximale (en mois) de la période de recherche des données de remboursement par rapport à une date d'acte.<br>Cf. chapitre 6.2 pour plus d'informations. |

**Illustration de la structure du fichier**

```
<?xml version="1.0" encoding="UTF-8" ?>
<dmp-parameters version="1.0">
    <parameter-list code="param-si-dmp">
        <parameter code="fonctions-gestion-mineurs" value="…" />
        <parameter code="cumul-invisible_patient-masque_ps" value="…" />
        <parameter code="age-majorite" value="…">
        <parameter code="hr-periode-max-mois" value="…" />
    </parameter-list>
</dmp-parameters>
```

[4] Le nom technique n'évolue pas. Il conserve le terme « PS ».

### 3.1.2 DMP_a : acquérir les données concernant l'utilisateur

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

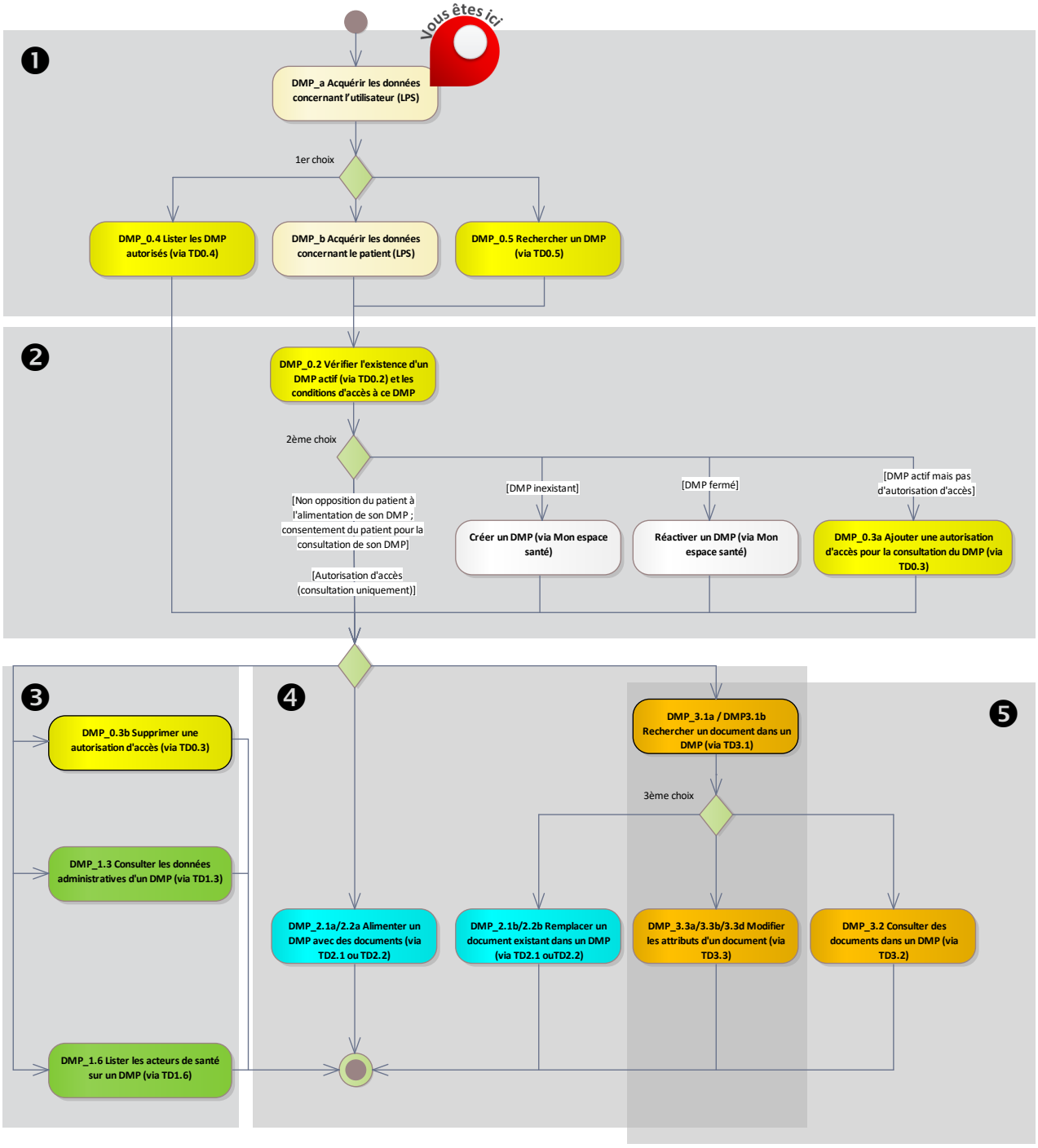



**Figure 11 : localisation de la fonctionnalité DMP_a dans le processus regroupant les deux profils Alimentation et Consultation**

## Vue générale

***Description***

Cette fonctionnalité permet au LPS d'acquérir les données concernant l'utilisateur et la structure de soins. Quel que soit le mode d'authentification, le LPS procède à l'identification de l'utilisateur et à l'identification de la structure de soins.

Le LPS acquiert les données concernant l'utilisateur :

- l'identifiant (cf. RG_0010),
- le mode d'accès (cf. RG_0020),
- la profession et la spécialité (cf. RG_0030),
- le nom (cf. RG_0040),
- le prénom (cf. RG_0050),
- le secteur d'activité (cf. RG_0060),

Le LPS acquiert les données concernant la structure de soins :

- l'identifiant (cf. RG_0070),
- le nom de la structure (cf. RG_0080),

Le LPS détermine les actions possibles pour la suite du processus (cf. RG_0090).

Ces données sont véhiculées dans le VIHF (cf. §5.3.2 et §5.3.3 et §5.3.4.5) et dans certaines données métier, par exemple l'auteur d'un document médical dans le DMP du patient.

Le document [CI-ANX-PS-STRU] fournit les règles de renseignement des données caractérisant les professionnels et structures de santé (source de données CPx ou gestion dans le LPS).

***Entrées et prérequis***

L'utilisateur est identifié par sa CPS, CPF ou CPE ou par le LPS ou par le système d'information de la structure de soins (mode AIR).

***Sorties***

Les données concernant l'utilisateur et la structure de soins.

## Règles de gestion

### *[RG_0010] Acquérir l'identifiant de l'utilisateur (EF_DMP01_01)*

**EX_GEN-1320**

L'accès au DMP nécessite l'identification nominative des utilisateurs telle que décrite au § 5.4 de [CI-ANX-PS-STRU].

Chaque utilisateur doit être identifié :

- en authentification directe ou en mode AIR : par son identifiant national présent dans sa carte CPS/CPF (N°ADELI ou N°RPPS) ou CPE ;
- en authentification indirecte :
  - par son identifiant national (N°ADELI ou N°RPPS) ;
  - à défaut, par l'identifiant de structure + son identifiant interne dans la structure de soins, séparés par un « / ».

NB : tous les identifiants nationaux de professionnel ou de structure sont préfixés par leur type d'identifiant.

### *[RG_0020] Acquérir le mode d'accès (EF_DMP01_02)*

Le mode d'accès « normal » est indiqué dans le VIHF. Cf. §5.3.2, §5.3.3 et §5.3.4.5.

Pour information, le passage en mode « bris de glace » est documenté dans la fonctionnalité DMP_0.2.

#### Cas particuliers

##### [CP1] Mode d'accès « centre de régulation »

Le mode d'accès « centre de régulation » est indiqué dans le VIHF. Cf. §5.3.2, §5.3.3 et §5.3.4.5.

Ce mode d'accès est réservé aux centres de réception et de régulation des appels des SAMU-Centres 15 :

- pour les permanenciers auxiliaires de régulation médicale (PARM) en authentification indirecte avec un certificat logiciel pour personne morale de centre de régulation pour la recherche de DMP sans INS (DMP_0.5),
- pour les médecins régulateurs en authentification directe avec leur CPS/CPF (ou en mode AIR) pour la consultation.

#### [RG_0030] Acquérir le savoir-faire de l'utilisateur (EF_DMP01_03)

Le savoir-faire est déduit :

- de la CPx en authentification directe,
- du LPS en authentification indirecte (dans ce cas, le savoir-faire peut être paramétré à l'avance).

Il s'agit de la profession de l'utilisateur, complétée le cas échéant (en fonction de sa profession) :

- pour un médecin, de sa spécialité
- pour un pharmacien, du tableau des pharmaciens

Cf. §4.3 authorSpecialty dans [CI-ANX-PS-STRU].

Si la spécialité de l'utilisateur est un code de la nomenclature ADELI, il est nécessaire de réaliser, pour les transactions DMP, un transcodage vers un code de la nomenclature RPPS (voir [CI-ANX-PS-STRU]).

Pour information, un médecin du travail (spécialité SM25 ou SCH35, ou activité FON-29 déclarée dans l'annuaire de santé) ne peut pas accéder au DMP en consultation.

#### [RG_0040] Acquérir le nom de l'utilisateur (EF_DMP01_04)

Cf. §5.1 PS_Nom dans [CI-ANX-PS-STRU].

#### [RG_0050] Acquérir le prénom de l'utilisateur (EF_DMP01_05)

Cf. §5.2 PS_Prénom dans [CI-ANX-PS-STRU].

#### [RG_0060] Acquérir le secteur d'activité de l'utilisateur (EF_DMP01_06)

Lorsqu'un utilisateur exerce dans plusieurs secteurs d'activité, ceux-ci correspondent généralement à des lieux d'exercice différents, équipés de LPS différents. A l'inverse, pour un lieu d'exercice donné, le secteur d'activité sera souvent unique.

Pour information :

- En authentification directe et indirecte, le secteur d'activité SA23 est bloqué et ne peut pas accéder au DMP.
- En authentification indirecte seulement, les secteurs d'activité SA11, SA13, SA35, SA44, SA45, SA31, SA55, SA58 sont bloqués et ne peuvent pas accéder au DMP.

L'utilisateur peut cependant travailler dans d'autres secteurs d'activités pour lesquels l'accès au DMP est autorisé (Cabinet individuel par exemple). Il est donc essentiel de définir correctement le secteur d'activité dans lequel l'utilisateur intervient.

En authentification directe, le secteur d'activité est déduit de la CPx.

- Si l'utilisateur a une seule situation d'exercice dans sa CPx, prendre le secteur d'activité de cette situation ;

- Si l'utilisateur a plusieurs situations d'exercice dans sa CPx, prendre le secteur d'activité de la situation sélectionnée par l'utilisateur.

**EX_GEN-1370**

En authentification directe, le LPS doit permettre aux utilisateurs qui possèdent plusieurs situations d'exercice dans leur carte CPx de choisir, à la première lecture de la carte CPx ou à la connexion au DMP, la situation d'exercice qu'il souhaite utiliser pour se connecter au DMP (même si en pratique un LPS sera quasi systématiquement associé à une seule situation d'exercice).

En authentification indirecte le secteur d'activité est paramétré à l'avance dans le LPS.

**EX_GEN-1375**

En authentification indirecte, il est nécessaire d'assurer la cohérence entre le secteur d'activité paramétré dans le LPS et celui connu dans les référentiels nationaux des structures de santé.

**EX_GEN-1377**

Il est nécessaire d'assurer la cohérence entre le secteur d'activité et le cadre d'exercice. Par exemple, on pourra associer un secteur d'activité « cabinet individuel » à un cadre d'exercice « Ambulatoire » et pas à un cadre d'exercice « établissement de santé ».

Les valeurs possibles du secteur d'activité sont celles du jeu de valeurs `healthcareFacilityTypeCode` (voir §4.2 [CI-ANX-PS-STRU] et [FI-JEUX-VALEURS]).

Exemples : Etablissement Public de santé, Hôpital militaire du Service de Santé des Armées, Etablissement Privé PSPH, Cabinet individuel, Cabinet de groupe, …

Si le secteur d'activité est un code de la nomenclature ADELI, il est nécessaire de réaliser, pour les transactions DMP, un transcodage vers un code de la nomenclature RPPS (voir [CI-ANX-PS-STRU]).

***[RG_0070] Acquérir l'identifiant de la structure de soins (EF_DMP02_01)***

**EX_GEN-1330**

Pour un organisme de santé, l'identifiant à utiliser est le numéro d'identifiant de l'organisation précédé d'un chiffre définissant le type d'identifiant utilisé (voir § 5.5 de [CI-ANX-PS-STRU]).

NB : les identifiants de structure sont préfixés par leur type d'identifiant.

***[RG_0080] Acquérir le nom de la structure de soins (EF_DMP02_02)***

Cf. §5.6 Struct_Nom dans [CI-ANX-PS-STRU].

***[RG_0090] Déterminer les actions possibles pour la suite du processus***

Le LPS peut ensuite :

- acquérir les données concernant le patient (cf. DMP_b) ;
- lister les DMP autorisés (cf. DMP_0.4) ;
- rechercher un DMP (cf. DMP_0.5).

### 3.1.3 DMP_b : acquérir les données concernant le patient

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

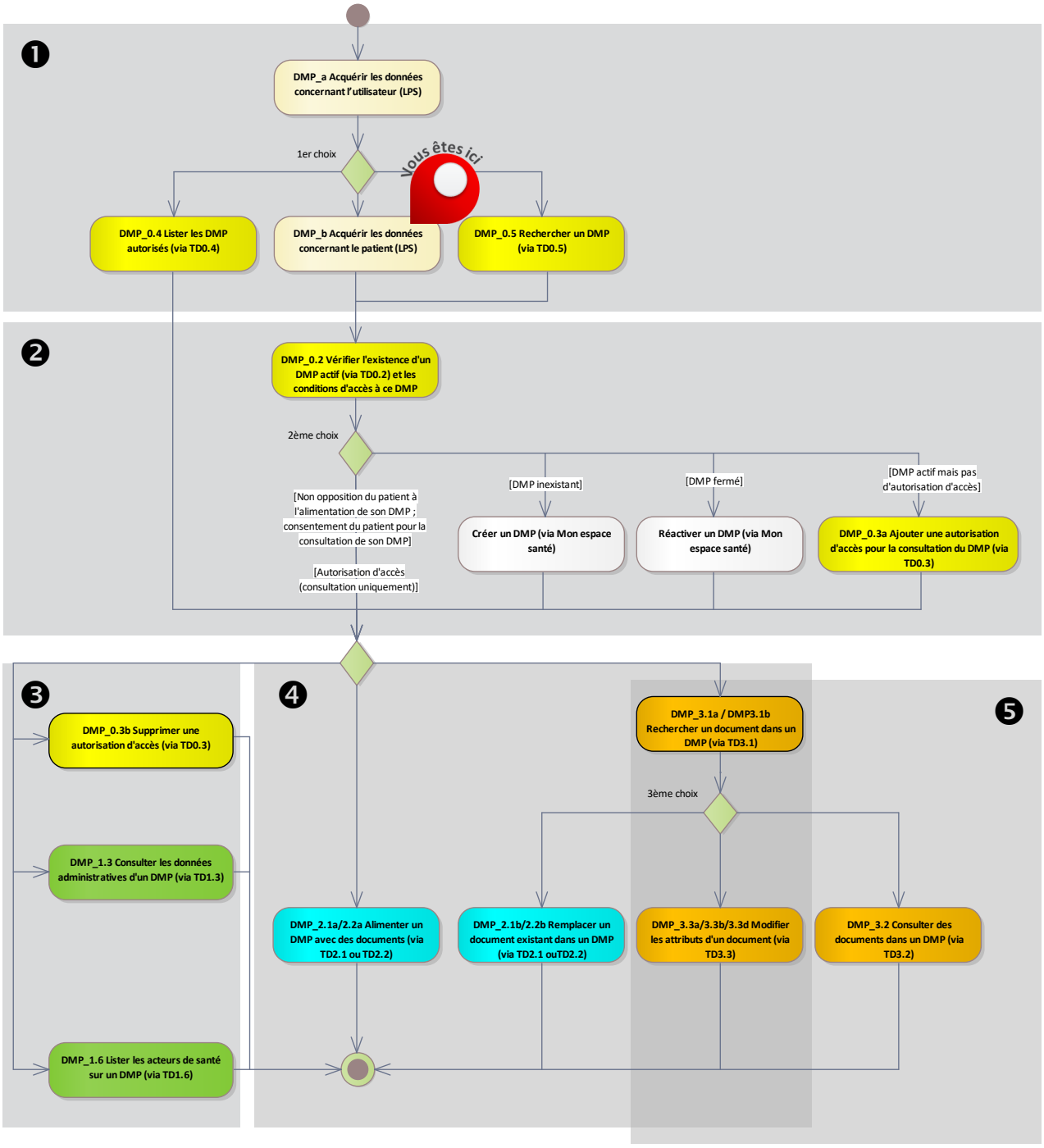



**Figure 12 : localisation de la fonctionnalité DMP_b dans le processus regroupant les deux profils Alimentation et Consultation**

**Vue générale**

***Description*** Cette fonctionnalité permet au LPS d'acquérir l'identité du patient dans le cadre du référentiel INS et des documents associés [REF-INS].

***Entrées et prérequis*** Cf. référentiel INS et les documents associés [REF-INS].

***Sorties*** L'INS du patient.

Les traits d'identité du patient.

**Règles de gestion**

***[RG_0110] Acquérir l'INS (EF_DMP11_01) du patient***

**EX_GEN-1530**

Seuls les INS obtenus dans le respect du référentiel INS et des documents associés [REF-INS] doivent servir pour accéder aux DMP des patients.

L'acquisition de l'INS du patient doit être effectuée sans rupture ergonomique pour l'utilisateur.

**EX_GEN-1550**

Si le paramètre `fonctions-gestion-mineurs` contient la valeur `true`, le LPS doit déterminer si un patient est mineur avant d'accéder à son DMP.

Un patient doit être considéré comme mineur si son âge (en années) est strictement inférieur à l'âge de la majorité défini dans le paramètre `age-majorite`.

Cf. exigence EX_0.1-1100 au § 5.3.1.3 pour la connexion secrète.

Cf. § 3.1.1 pour l'intégration de ces paramètres dans le LPS.

***Cas d'erreur de la règle de gestion RG_0110***

***[CE1] Impossibilité d'obtenir le l'INS du patient***

Le LPS ne doit pas appeler d'autres transactions pour ce DMP (sauf en passant par les transactions TD0.4 et TD0.5).

Pour un patient possédant un DMP référencé dans le LPS via un INS-C, il est toujours possible à l'utilisateur de consulter ce DMP via le site Web-PS (Cf. TD0.9 ou TD0.10).

## 3.2 DMP_0.x : accès sécurisé au DMP d'un patient

Ce chapitre décrit des fonctionnalités permettant d'accéder au DMP d'un patient en tenant compte des autorisations d'accès des acteurs de santé.

La fonctionnalité DMP_0.3 permet de modifier les autorisations d'accès. Cf. §3.2.3.

### 3.2.1 DMP_0.1 : accès sécurisé au système DMP (via TD0.1)

Cette fonctionnalité d'infrastructure, liée à l'appel de chaque transaction DMP, est décrite dans le chapitre 5.3.

## 3.2.2 DMP_0.2 : vérifier l'existence d'un DMP actif (via TD0.2) et les conditions d'accès à ce DMP

### 3.2.2.1 Description de la fonctionnalité

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

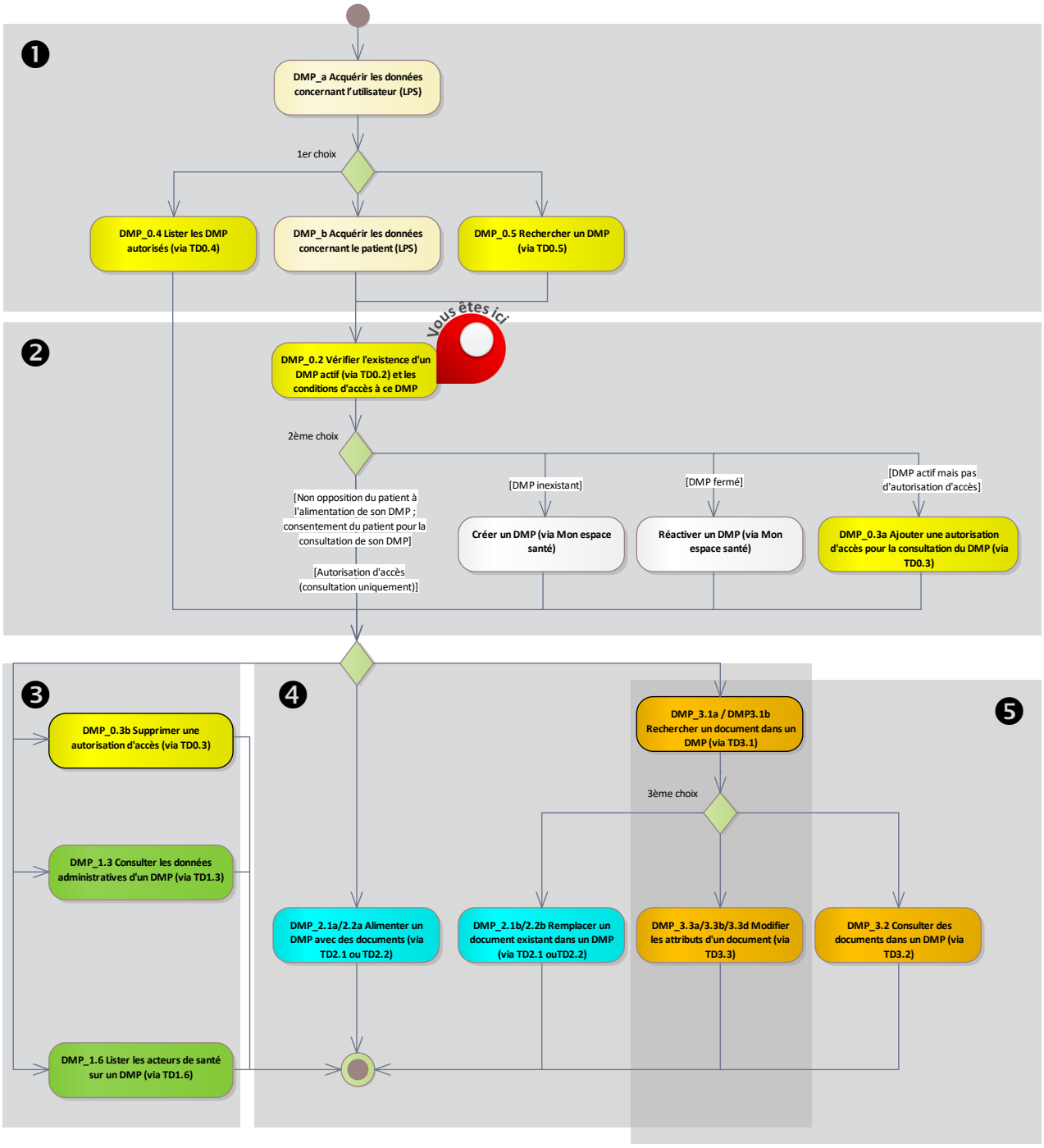



**Figure 13 : localisation de la fonctionnalité DMP_0.2 dans le processus regroupant les deux profils Alimentation et Consultation**

## Vue générale

***Description***

Cette fonctionnalité permet, via la transaction TD0.2, de déterminer si le DMP du patient existe et de récupérer les données suivantes (cf. RG_0310) :

- statut du DMP du patient (EF_DMP12_01),
- si le DMP du patient est fermé, date, motif et raison de la fermeture (cf. EF_DMP12),
- statut de l'autorisation d'accès de consultation de l'acteur de santé (EF_DMP04_01),
- statut « médecin traitant DMP » (EF_DMP01_07).

Ces données permettent au LPS de vérifier :

- si le DMP du patient existe et si celui-ci est actif,
- si l'acteur de santé dispose d'une autorisation d'accès valide pour la consultation de ce DMP.

Le LPS gère en local (= hors SI DMP) les conditions d'accès à ce DMP par l'acteur de santé :

- non opposition du patient à l'alimentation de son DMP,
- consentement du patient à la consultation de son DMP.

En mode d'accès « centre de régulation », le statut de l'autorisation d'accès de l'acteur de santé sur le DMP du patient n'est pas contrôlé par le LPS.

NB1 : un professionnel que le patient a bloqué ne peut pas accéder au DMP de ce patient, que ce soit avec ou sans l'autorisation du patient.

NB2 : les autorisations d'accès ne sont utilisées que pour la consultation des DMP.

Ensuite, le LPS :

- affiche les traits d'identité provenant du DMP (cf. RG_0320),
- détermine les actions possibles sur le DMP du patient (cf. RG_0330).

***Entrées et prérequis***

L'INS du patient (EF_DMP11_01).

***Sorties***

Le LPS a vérifié les conditions d'accès de l'acteur de santé au DMP du patient.

## Règles de gestion

***[RG_0310] Déterminer l'existence du DMP et l'autorisation d'accès de l'acteur de santé pour la consultation de ce DMP***

Le LPS appelle la transaction TD0.2 en passant en entrée l'INS du patient (EF_DMP11_01).

Cf. §3.2.2.2 pour la description de la transaction.

La réponse de la transaction TD0.2 contient notamment le statut du DMP du patient (EF_DMP12_01) et le statut de l'autorisation d'accès de l'acteur de santé pour la consultation de ce DMP (EF_DMP04_01).

***Cas particulier***

***[CP1] DMP fermé à la demande du patient (`statusCode="terminated"`)***

**REC_0.2-1010**

Lors d'un test d'existence, en cas de DMP fermé, il est recommandé que le LPS affiche à l'utilisateur :

- le statut « fermé » du DMP du patient (EF_DMP12_01),
- la date de fermeture (EF_DMP12_02),
- le motif de la fermeture (EF_DMP12_03),
- raison de fermeture (EF_DMP12_04).

***[RG_0320] Afficher les traits d'identité provenant du DMP***

**REC_0.2-1020**

Il est recommandé d'afficher les traits d'identité retournés par la transaction TD0.2.

Si le nom d'usage (EF_DMP11_02) contient la valeur « NON RENSEIGNE » (13 caractères), il est recommandé de ne pas afficher cette valeur.

Il est également recommandé d'alerter l'utilisateur en cas d'écart entre ces traits d'identité provenant du DMP et les traits d'identité liés à l'INS (cf. DMP_b).

***[RG_0325] Acquérir l'accord du patient concernant l'accès à son DMP par l'acteur de santé (EF_DMP04_02 et EF_DMP04_03)***

L'accord du patient est composé :

- du consentement du patient à la consultation de son DMP (EF_DMP04_02),
- de la non opposition du patient à l'alimentation de son DMP (EF_DMP04_03).

L'acquisition de l'accord du patient doit pouvoir être réalisée par :

- le secrétariat pour le professionnel dans le cadre d'un exercice individuel ;
- le secrétariat pour l'équipe de soins dans le cadre d'un exercice coordonné.

**EX_0.2-1100**

Le LPS ne doit pas positionner systématiquement l'accord du patient concernant le consentement pour la consultation de son DMP par l'acteur de santé.

Cette action doit toujours se faire suite à une demande explicite ou à une action spécifique de l'utilisateur.

Pour le recueil du consentement du patient pour la consultation du DMP, le LPS doit afficher le texte suivant : « Le patient (ou son représentant légal), préalablement informé, consent au fait que j'accède à son DMP ».

Le LPS doit permettre de prendre en compte l'opposition du patient à l'alimentation de son DMP et l'absence de consentement pour la consultation de son DMP, si le patient en fait la demande explicite.

Le LPS doit tracer la non opposition du patient pour l'alimentation de son DMP (EF_DMP04_03). La trace doit être gérée en local (= hors SI DMP) pour chaque structure de santé et/ou équipe de soins.

NB : pas d'exigence de tracer le consentement du patient car celui-ci est associé à l'autorisation d'accès (DMP_0.3).

**REC_0.2-1110**

Les éléments de vocabulaire présentés dans les exemples d'IHM ci-dessous peuvent être intégrés au LPS.

Exemple d'IHM en authentification directe pour un seul profil (Consultation) :

( ) Le patient (ou son représentant légal), préalablement informé, consent au fait que j'accède à son DMP

( ) J'accède en urgence au DMP. Le patient est hors d'état d'exprimer sa volonté, et il y a un risque immédiat pour sa santé (accès bris de glace)

Motif de l'accès en mode bris de glace :

[ champ de saisie du motif ]

Exemple d'IHM en authentification directe pour les deux profils (Consultation et Alimentation) :

( ) Le patient (ou son représentant légal), préalablement informé, consent au fait que j'accède à son DMP

(X) Le patient (ou son représentant légal), préalablement informé, n'a pas exprimé d'opposition pour l'alimentation de son DMP

( ) J'accède en urgence au DMP. Le patient est hors d'état d'exprimer sa volonté, et il y a un risque immédiat pour sa santé (accès bris de glace)

Motif de l'accès en mode bris de glace :

[ champ de saisie du motif ]

***Cas particulier de la règle de gestion RG_0410***

***[CP1] Demande de passage en mode d'accès « bris de glace »***

Lorsque l'utilisateur a besoin de consulter le DMP d'un patient en cas d'urgence, sans avoir la possibilité de lui demander son autorisation, au lieu de se déclarer autorisé à accéder au dossier par le patient, il dispose de la possibilité d'accéder au dossier en mode « bris de glace ». Dans ce cas, l'utilisateur doit indiquer la raison de l'utilisation du mode « bris de glace ».

Le mode d'accès « bris de glace » est indiqué dans le VIHF. Cf. §5.3.2, §5.3.3 et §5.3.4.5.

**EX_0.2-1040**

Le mode « bris de glace » ne doit pas être persistant en dehors du temps de la session courante de l'utilisateur dans le LPS et pour le patient actuellement ouvert : il doit être désactivé une fois le dossier local du patient fermé (le LPS ne doit pas continuer à positionner ce champ à la valeur bris de glace).

**EX_0.2-1050**

L'accès au DMP en mode « bris de glace » doit être affiché clairement à l'utilisateur du LPS pendant toute la durée de cet accès.

***[RG_0330] Déterminer les actions possibles sur le DMP du patient***

Les actions possibles sur le DMP du patient dépendent des données indiquées ci-dessous.
NB : les restrictions sur les actions possibles sont cumulatives.

- Le consentement du patient concernant l'accès pour la consultation de son DMP par l'acteur de santé (EF_DMP04_02).

| Choix du patient | Actions possibles |
|---|---|
| Le patient ne consent pas à la consultation de son DMP | Aucune action du profil Consultation n'est possible. |
| Le patient consent à la consultation de son DMP | Toutes les actions du profil Consultation sont possibles et peuvent limitées par les autres données (cf. ci-dessous). |
| (accès au DMP en mode « bris de glace ») | |

- La non opposition du patient concernant l'accès pour l'alimentation de son DMP par l'acteur de santé (EF_DMP04_03).

| Choix du patient | Actions possibles |
|---|---|
| Le patient est opposé à l'alimentation de son DMP | Aucune action du profil Alimentation n'est possible. |
| Le patient n'est pas opposé à l'alimentation de son DMP | Toutes les actions du profil Alimentation sont possibles et peuvent limitées par les autres données (cf. ci-dessous). |

- Le statut de l'autorisation d'accès pour la consultation de ce DMP (EF_DMP04_01).

| Statut de l'autorisation | Actions possibles |
|---|---|
| interdite | Les seules actions possibles sont [5] :<br>• « Alimenter le DMP d'un patient avec des documents » (DMP_2.1/2.2)<br>• « Rechercher l'identifiant technique d'un document » (DMP_3.1b) (si le LPS implémente le profil Alimentation)<br>• « Supprimer un document » (DMP_3.3c) (si le LPS implémente le profil Alimentation). |
| inexistante | Les seules actions possibles sont :<br>• Se déclarer « autorisé ». Cf. « ajouter une autorisation d'accès pour la consultation du DMP » (DMP_0.3a).<br>• « Alimenter le DMP d'un patient avec des documents » (DMP_2.1/2.2)<br>• « Rechercher l'identifiant technique d'un document » (DMP_3.1b) (si le LPS implémente le profil Alimentation)<br>• « Supprimer un document » (DMP_3.3c) (si le LPS implémente le profil Alimentation).<br>En mode d'accès « centre de régulation », toutes les actions sont possibles. |
| expirée | |
| valide | Toutes les actions sont possibles. |

- Le statut du DMP du patient (EF_DMP12_01).

| Statut du DMP | Actions possibles |
|---|---|
| inexistant | Aucune action possible dans le cadre de la DMP compatibilité des LPS. La création et la réactivation des DMP sont prises en charge par « Mon espace santé ». |
| fermé | |
| actif | Toutes les actions sont possibles. |

- Des limitations sont également définies dans la matrice des droits fonctionnels [DMP-MDRF] implémentée dans le système DMP.

[5] L'acteur de santé ne peut plus à nouveau se déclarer « autorisé », ni accéder au DMP en mode « bris de glace » ou « centre de régulation ».
Pour information, un professionnel bloqué peut être retiré de la liste des professionnels bloqués par le patient ou le médecin traitant DMP (à la demande du patient) ce qui permettra ultérieurement à ce professionnel de se déclarer à nouveau « autorisé ».

| EX_3.3-1060 |
| --- |
| La suppression des documents dans le DMP d'un patient sans autorisation d'accès est réservée au profil Alimentation.<br>Précision : la suppression doit toujours pouvoir se faire sans autorisation. Cette exigence concerne tous les LPS implémentant le profil Alimentation. |

### 3.2.2.2 TD0.2 : test d'existence du DMP d'un patient et vérification de l'autorisation d'accès pour la consultation de ce DMP

La transaction est décrite dans le chapitre 3.3.2 du document [CI-GESTPAT] et utilise le message HL7 V3 Patient Registry Get Demographics Query (interaction PRPA_IN201307UV02) via un web-service.

Cf. § 4.2.2 pour une présentation de la structuration des messages HL7 V3.

L'élément `reasonCode/@code` doit être positionné à `TEST_EXST` (voir §5.6.2.5).

La transaction doit respecter les exigences concernant l'accès sécurisé au système DMP. Cf. TD0.1 au §5.3.

#### Données en entrée

La requête doit contenir l'INS du patient, dans le paramètre `Patient.id`, ainsi qu'un identifiant unique de requête généré par le LPS, dans l'élément `controlActProcess/queryByParameter/queryId`.

| Nom du champ | Card. | XPath HL7 | Alimentation données |
| --- | --- | --- | --- |
| Requête paramétrée | [1..1] | `queryByParameter` | |
| Identifiant unique de la requête | [1..1] | `queryId` | |
| Oid des requêtes dans le LPS | [1..1] | `@root` | Oid géré par le LPS |
| Identifiant de la requête dans le LPS | [1..1] | `@extension` | Id généré par le LPS |
| Statut de la requête | [1..1] | `statusCode/@code` | Fixé à « new » |
| Liste des paramètres | [1..1] | `parameterList` | |
| Paramètre de type Identifiant du patient | [1..1] | `patientIdentifier` | Le système DMP restreint la cardinalité [1..*] du CI-SIS à [1..1] |
| Valeur du paramètre (EF_DMP11_01) | [1..1] | `value` | |
| OID de l'identifiant | [1..1] | `@root` | Cf. [OID-INS]. |
| INS | [1..1] | `@extension` | Valeur de l'INS |
| Nom du paramètre, contraint par HL7 | [1..1] | `semanticsText` | Fixé à « Patient.id » |

**Tableau 8 : TD0.2 – données en entrée**

#### Données en sortie

En retour, le message HL7 V3 Patient Registry Get Demographics Query Response (PRPA_IN201308UV02) est renvoyé.

***En cas de succès de la transaction :***

Accusé de réception du traitement « ok » (valeur `AA` dans `acknowledgement/typeCode`).

***Si le DMP du patient existe :***

| Chemin XML | Alimentation données |
|---|---|
| `controlActProcess/queryAck/queryResponseCode/@code` | Valeur `OK` signifiant que le DMP du patient existe. |
| `controlActProcess/subject/registrationEvent/subject1/patient` | Bloc contenant les données du patient.<br>Cf. détail ci-dessous. |
| `…/patient/id` | Le ou les identifiant(s) du patient (EF_DMP11_01) :<br>• NIR utilisé comme INS, si connu ;<br>• INS-C si le DMP du patient existe (pendant la phase de transition entre les deux identifiants).<br>Peut contenir plusieurs valeurs qui se distinguent par l'attribut `root`. |
| `…/patient/patientPerson/name/family [@qualifier = 'SP']` | Nom d'usage (EF_DMP11_02)<br>NB : la valeur « NON RENSEIGNE » (13 caractères) indique que le nom d'usage n'est pas renseigné dans le DMP. |
| `…/patient/patientPerson/name/family [@qualifier = 'BR']` | Nom de naissance si renseigné (EF_DMP11_03) |
| `…/patient/patientPerson/name/given` | Prénom (EF_DMP11_04) |
| `…/patient/patientPerson/administrativeGenderCode/@code` | Sexe (EF_DMP11_05) |
| `…/patient/patientPerson/birthTime/@value` | Date de naissance (EF_DMP11_06) |
| `…/patient/patientPerson/name/prefix` | Civilité (EF_DMP11_07) |
| `…/patient/@statusCode` | Statut du DMP (EF_DMP12_01) |
| `…/patient/subjectOf/administrativeObservation [code/@code = 'COMPTE_INTERNET_OUVERT'] [code/@codeSystem = '1.2.250.1.213.4.1.2.9']` | Le statut du compte internet est contenu dans l'élément value/@value<br>• « true » : le compte internet existe,<br>• « false » : le compte internet n'existe pas. |
| `…/patient/subjectOf/administrativeObservation [code/@code = 'RATTACHEMENT_ENS'] [code/@codeSystem = '1.2.250.1.213.4.1.2.3']` | Le statut du rattachement est contenu dans l'élément value/@value<br>• « true » : le DMP est rattaché à un « Mon espace santé »,<br>• « false » : le DMP n'est pas rattaché à un « Mon espace santé ». |
| `controlActProcess/subject/registrationEvent/effectiveTime/@value` | Date de fermeture (EF_DMP12_02) |
| `controlActProcess/reasonOf/detectedIssueEvent/code` | Motif de fermeture (EF_DMP12_03) |
| `controlActProcess/reasonOf/detectedIssueEvent/text` | Raison de fermeture (EF_DMP12_04) |
| `attentionLine` (à la racine du message) | |

| | |
|---|---|
| avec un élément fils `keyWordText/@code="AUTORISATION"`<br>Exemple :<br>`<attentionLine>`<br>`<keyWordText code="AUTORISATION" codeSystem="1.2.250.1.213.4.1.2.6.1"/>`<br>`<value xsi:type="CV" code="VALIDE" codeSystem="1.2.250.1.213.4.1.2.6.2"/>`<br>`</attentionLine>` | Le statut de l'autorisation (EF_DMP04_01) est contenu dans l'élément `value/@code`. |
| `attentionLine` (second élément à la racine du message) | Cette information n'est pas retournée en authentification indirecte. |
| avec un élément fils `keyWordText/@code="STATUT_MT"`<br>Exemple :<br>`<attentionLine>`<br>`<keyWordText code="STATUT_MT" codeSystem="1.2.250.1.213.4.1.2.6.3"/>`<br>`<value xsi:type="BL" value="true"/>`<br>`</attentionLine>` | Le statut « médecin traitant DMP » (EF_DMP01_07) est contenu dans l'élément `value/@value`. |

**Tableau 9 : TD0.2 – données en sortie – le DMP existe**

***Si le DMP du patient n'existe pas :***

| Chemin XML | Alimentation données |
|---|---|
| `controlActProcess/queryAck/queryResponseCode/@code` | Valeur `NF` signifiant que le DMP du patient n'existe pas (EF_DMP12_01) |

**Tableau 10 : TD0.2 – données en sortie – le DMP n'existe pas**

Le message ne contient aucune occurrence de l'élément `controlActProcess/subject`.

***En cas d'erreur de la transaction :***

Un code et un message d'erreur sont renvoyés dans le message. Voir annexe 7.

### 3.2.3 DMP_0.3 : modifier l'autorisation d'accès (via TD0.3) pour la consultation du DMP

Le LPS permet à l'utilisateur les actions suivantes.

- Ajouter une autorisation d'accès pour la consultation du DMP du patient. Cf. DMP_0.3a.
- Supprimer une autorisation d'accès pour la consultation du DMP du patient. Cf. DMP_0.3b.

NB : ce découpage correspond aux fonctionnalités présentées dans les processus dans le chapitre 2.3.

Pour information : dans le LPS, les autorisations d'accès ne peuvent être donnés pour le compte d'une autre personne.

### 3.2.3.1 DMP_0.3a : ajouter une autorisation d'accès pour la consultation du DMP (via TD0.3)

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

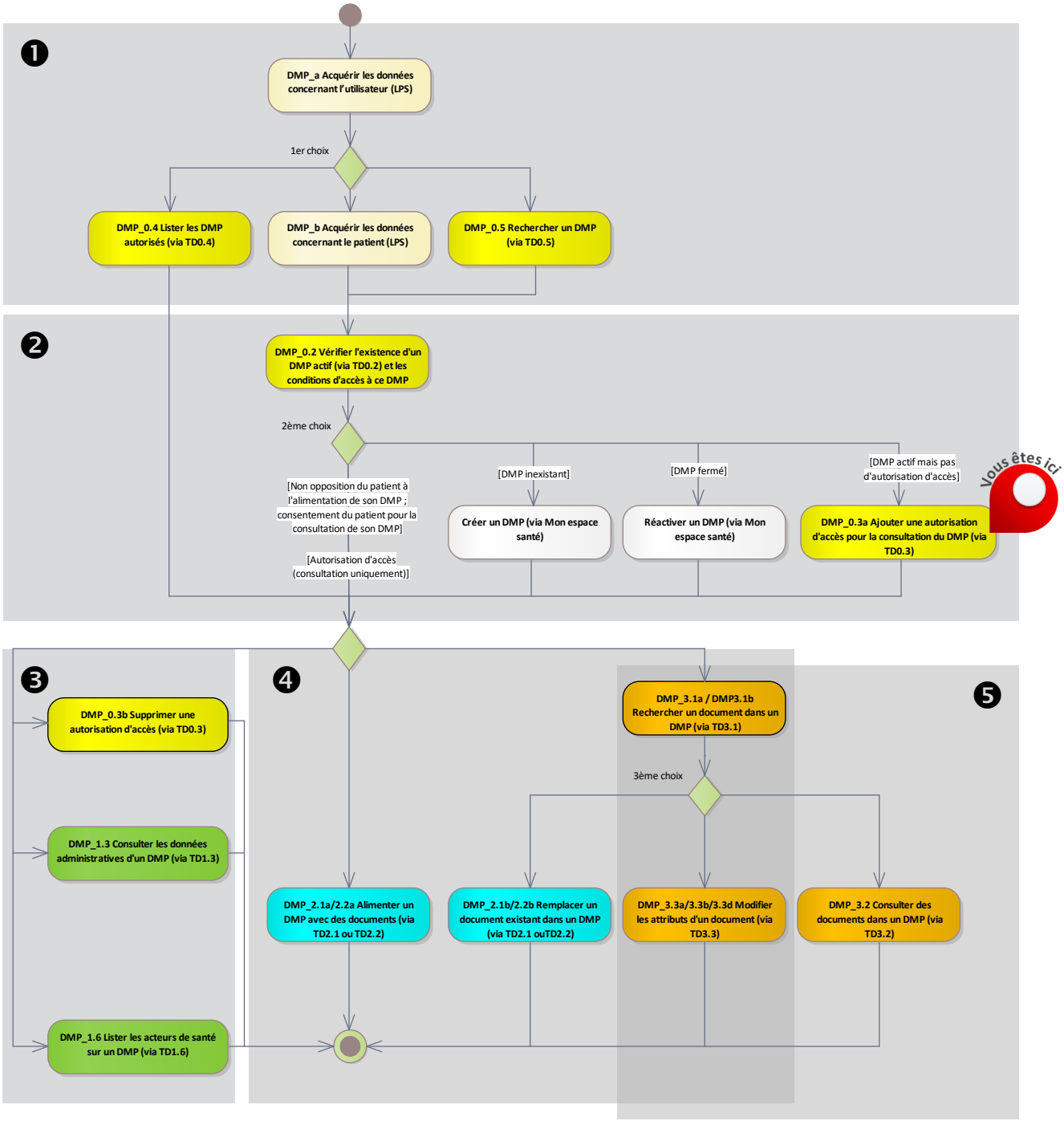



**Figure 14 : localisation de la fonctionnalité DMP_0.3a dans le processus regroupant les deux profils Alimentation et Consultation**

## Vue générale

***Description*** Cette fonctionnalité est réservée au profil Consultation. Elle est déclenchée suite

- à la détection d'une absence d'autorisation d'accès pour la consultation du DMP du patient ;
- et au recueil du consentement du patient concernant l'accès à son DMP par l'acteur de santé (cf. RG_0325 dans DMP_0.2).

Le LPS :

- acquiert la demande d'ajout d'une autorisation d'accès pour la consultation du DMP du patient (cf. RG_0410),
- appelle la transaction TD0.3 pour ajouter l'autorisation d'accès pour la consultation du DMP (cf. RG_0430).

***Entrées et prérequis*** L'INS du patient (EF_DMP11_01).

Statut de l'autorisation d'accès (EF_DMP04_01) inexistante ou expirée.

Consentement du patient pour la consultation de son DMP par l'acteur de santé (EF_DMP04_02).

***Sorties*** L'autorisation d'accès en consultation (EF_DMP04_01) valide.

## Règles de gestion

***[RG_0410] Acquérir la demande d'ajout d'une autorisation d'accès au DMP du patient***

**EX_0.3-1010**

Si l'autorisation d'accès en consultation du DMP d'un patient à un acteur de santé n'est pas définie ou si elle est expirée (EF_DMP04_01) et que le patient consent à la consultation de son DMP par l'acteur de santé (EF_DMP04_02), le LPS alimente automatiquement la donnée `action` avec la valeur `AJOUT`.

Cette exigence ne concerne que le profil Consultation.

L'ajout d'une autorisation d'accès en consultation n'est possible qu'après réception d'un statut retourné par le DMP indiquant qu'il n'y a pas ou plus d'autorisation d'accès au DMP du patient pour l'acteur de santé. Ce statut peut être récupéré :

- soit après la vérification de l'existence d'un DMP actif et des conditions d'accès à ce DMP (cf. DMP_0.2),
- soit après une utilisation d'une autre transaction.

**EX_0.3-1020**

En authentification directe, si le statut renvoyé par le DMP est « autorisation expirée », le LPS doit indiquer à l'utilisateur qu'il doit effectuer une nouvelle autorisation.

Cette exigence ne concerne que le profil Consultation.

***[RG_0430] Ajouter l'autorisation d'accès pour la consultation du DMP***

Conditions (EF_DMP04_02, cf. RG_0325 dans DMP_0.2) :

- le patient consent à la consultation à son DMP (RG_0410RG_0325).
- hors mode d'accès « bris de glace ».

Le LPS appelle la transaction TD0.3. Cf. chapitre 3.2.3.3 pour la description de la transaction.

### 3.2.3.2 DMP_0.3b : supprimer une autorisation d'accès (via TD0.3)

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

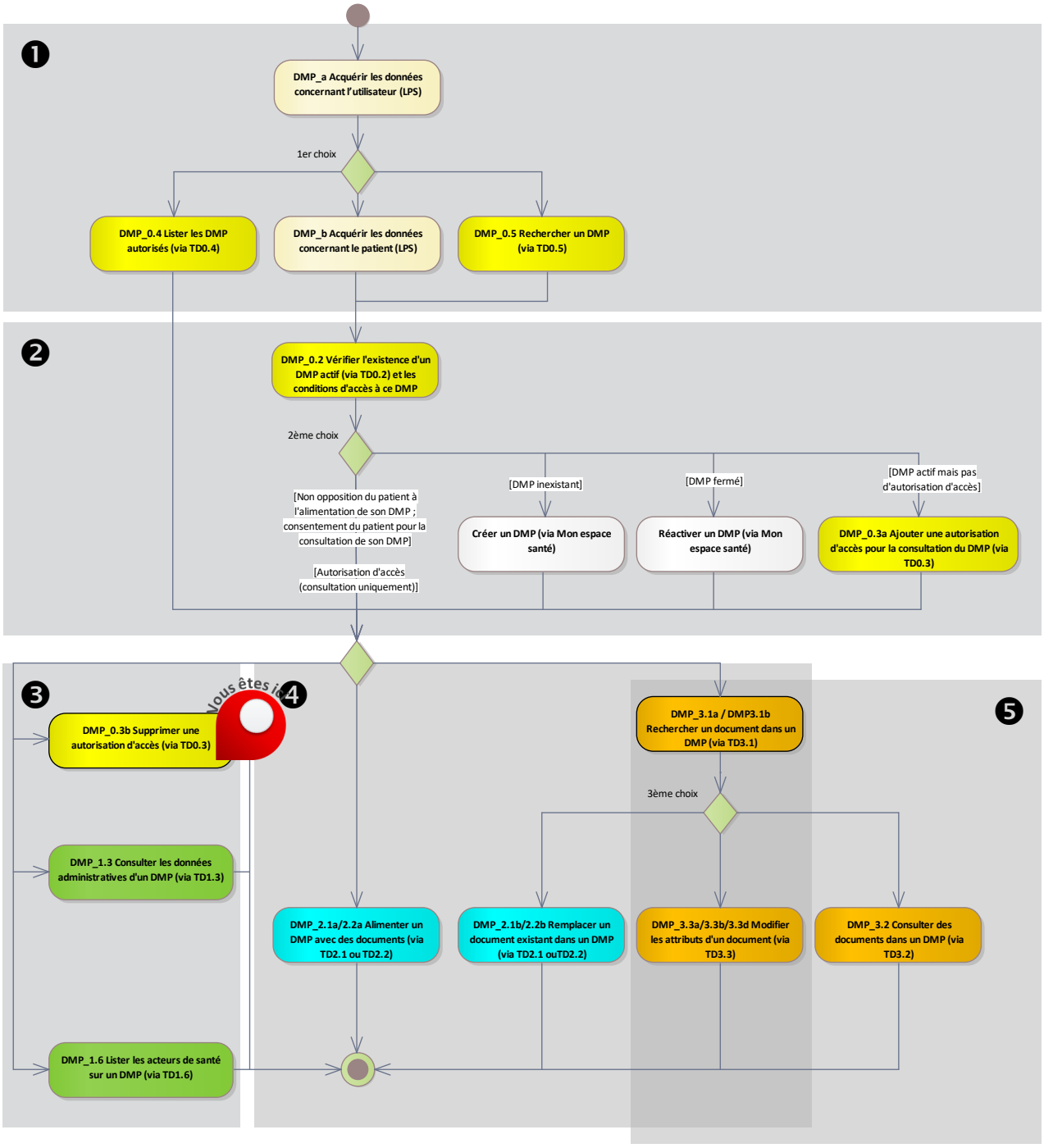



**Figure 15 : localisation de la fonctionnalité DMP_0.3b dans le processus regroupant les deux profils Alimentation et Consultation**

**Vue générale**

***Description*** Le LPS :

- acquiert la demande de suppression d'une autorisation d'accès au DMP du patient (cf. RG_0510),
- appelle la transaction TD0.3 pour supprimer l'autorisation d'accès (cf. RG_0520).

***Entrées et prérequis*** L'INS du patient (EF_DMP11_01).

Statut de l'autorisation d'accès (EF_DMP04_01) valide.

***Sorties*** Statut de l'autorisation d'accès (EF_DMP04_01) expirée.

**Règles de gestion**

***[RG_0510] Acquérir la demande de suppression d'une autorisation d'accès au DMP du patient***

A la demande de l'utilisateur, le LPS alimente la donnée `action` avec la valeur `SUPPRESSION`.

**REC_0.3-1031**

Les éléments de vocabulaire présentés dans les exemples d'IHM ci-dessous peuvent être intégrés au LPS.

Exemple d'IHM en authentification directe :

> Mettre fin à mon autorisation d'accès au DMP de M/Mme XXXX.

Exemple d'IHM en authentification indirecte :

> Mettre fin à l'autorisation d'accès de la structure de soins au DMP de M/Mme XXXX.

***[RG_0520] Supprimer l'autorisation d'accès***

Condition : le LPS a acquis la demande de suppression d'une autorisation d'accès au DMP du patient (RG_0510).

Le LPS appelle la transaction TD0.3. Cf. chapitre 3.2.3.3 pour la description de la transaction.

### 3.2.3.3 TD0.3 : mise à jour de l'autorisation d'accès

Cette transaction spécifique DMP permet de gérer l'autorisation d'accès :

- de l'acteur de santé identifié dans le VIHF,
- sur le DMP du patient identifié dans le VIHF par son INS.

Les actions possibles sont :

- mise à jour de l'autorisation d'accès (création ou recréation ou retrait),

La transaction doit respecter les exigences concernant l'accès sécurisé au système DMP. Cf. TD0.1 au §5.3.

**Données en entrée**

| Balises XML | Occur -rence | Format | Alimentation données |
|---|---|---|---|
| setAuthorization | 1 | - | |
| action | 1 | AN | Type d'action de mise à jour.<br>Valeurs possibles :<br>• AJOUT : ajout de l'autorisation,<br>• SUPPRESSION : suppression de l'autorisation. |

**Tableau 11 : TD0.3 – données en entrée**

**Données en sortie**

| Balises XML | Occur -rence | Format | Alimentation données |
|---|---|---|---|
| setAuthorizationResponse | 1 | - | |
| output | 1 | - | |
| status | 0..1 | 50AN | Code de retour : DMPOk (en cas de succès), ou code d'erreur (en cas d'erreur). |
| context | 0..1 | AN | Message d'erreur (en cas d'erreur). |

**Tableau 12 : TD0.3 – données en sortie**

***En cas d'erreur de la transaction :***

Un code et un message d'erreur sont renvoyés dans le message. Voir annexe 7.

### 3.2.4 DMP_0.4 : lister les DMP autorisés (via TD0.4)

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

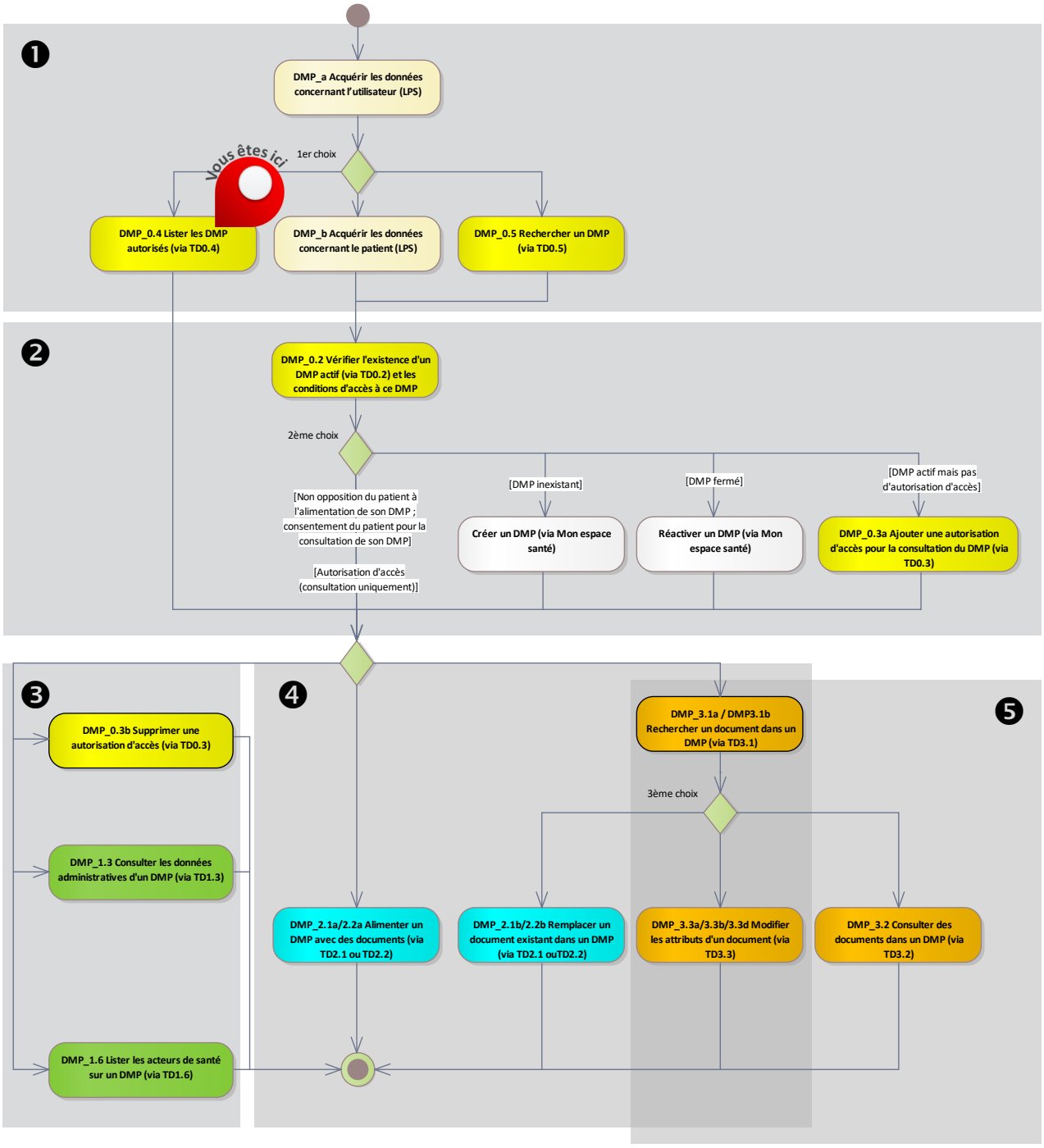



**Figure 16 : localisation de la fonctionnalité DMP_0.4 dans le processus regroupant les deux profils Alimentation et Consultation**

### 3.2.4.1 Description de la fonctionnalité

**Vue générale**

***Description***

Cette fonctionnalité utilise la transaction TD0.4 pour obtenir la liste des DMP autorisés.

Rappel : cette transaction ne doit être possible qu'en authentification directe.

Pour information, les usages sont les suivants :

1) Elle permet de récupérer la liste des nouveaux DMP autorisés pour l'acteur de santé (avec les INS de patient et les traits d'identités). Outre les habituelles informations d'authentification, il est possible de paramétrer en entrée une date à partir de laquelle la recherche est effectuée. Par exemple : (date du jour - 3 jours) ou (date du jour - 1 semaine). L'éditeur peut mettre en œuvre dans le LPS un appel planifié régulièrement à cette transaction (par exemple tous les 3 jours ou toutes les semaines).

2) Cette transaction permet de récupérer la liste des patients pour lesquels un nouveau document a été ajouté dans son DMP depuis une date donnée. Le retour est le même, seul le paramétrage en entrée est différent.

3) Elle peut être utilisée par un(e) non professionnel (par exemple, secrétaire médicale) pour rechercher la liste des patients d'un professionnel appartenant à la même structure.

Le LPS :

- acquiert les critères de recherche (cf. RG_0710),
- obtient la liste des DMP autorisés en appelant la transaction TD0.4 (cf. RG_0720),
- détermine, pour chaque DMP de la liste,
  - le statut du DMP (cf. RG_0730),
  - l'autorisation d'accès de l'acteur de santé (cf. RG_0740),
  - les actions possibles (cf. RG_0760),
- affiche la liste des DMP autorisés (cf. RG_0770),
- acquiert la sélection du DMP (cf. RG_0780).

***Entrées et prérequis***

Aucune.
(Les données nécessaires sont acquises pendant le déroulement de la fonctionnalité.)

***Sorties***

Une liste de DMP de patients (EF_DMP12).

**Règles de gestion**

***[RG_0710] Acquérir les critères de recherche***

Le LPS acquiert les données suivantes.

- La date de début de recherche (`startDate`)
- Le type de recherche (`dateType`) :
  - Recherche de la liste des nouveaux DMP autorisés depuis une date donnée (valeur LASTAUTORIZATION),
  - Recherche de la liste des DMP dans lesquels un nouveau document a été ajouté depuis une date donnée (valeur LASTDOC).

***Cas particulier***

***[CP1] Accès pour un non professionnel avec CPE (par exemple, une secrétaire médicale)***

Le LPS acquiert, en plus, l'identifiant du professionnel auquel un non professionnel avec CPE est rattaché (`psOwnerID`).

***[RG_0720] Obtenir la liste des DMP autorisés (EF_DMP12)***

Le LPS appelle la transaction TD0.4 en passant en entrée les critères de recherche acquis dans la règle de gestion RG_0710.

Cf. §3.2.4.2 pour la description de la transaction.

***Cas particulier***

***[CP1] Certains DMP dans la liste ne contiennent pas de NIR utilisable comme INS dans la donnée `patientIdentifier`***

Pour chaque DMP dans la liste ne contenant pas de NIR utilisable comme INS dans la donnée `patientIdentifier` :

- Obtenir l'INS du patient dans le respect du référentiel INS et des documents associés [REF-INS].
- S'il n'est pas possible d'obtenir cet INS, l'accès à ce DMP n'est pas possible via les interfaces LPS v2. Pour information, ce DMP reste accessible via le site Web-PS, avec l'INS-C. Cf. TD0.9 ou TD0.10.

***[RG_0730] Déterminer, pour chaque DMP de la liste, le statut du DMP (EF_DMP12_01)***

Le statut du DMP est actif.

NB : la transaction TD0.4 ne renvoie que des DMP actifs.

***[RG_0740] Déterminer, pour chaque DMP de la liste, l'autorisation d'accès en consulation de l'acteur de santé (EF_DMP04_01)***

L'autorisation d'accès de l'acteur de santé pour la consultation du DMP est valide.

**REC_0.4-1010**

Le LPS vérifie lors de la réception de la liste, pour chaque INS de patient retourné, si cet INS de patient existe dans l'annuaire local et « marque » l'INS de patient local pour noter l'information « DMP existe et acteur de santé autorisé pour la consultation de ce DMP ». Les traitements de ces DMP par la structure autorisée pourront alors se faire en tenant compte de l'accord (non opposition pour l'alimentation ; consentement pour la consultation) des patients.

***[RG_0760] Déterminer, pour chaque DMP de la liste, les actions possibles sur chaque DMP***

Toutes les actions sont *a priori* possibles.

Des limitations sont également définies dans la matrice des droits fonctionnels [DMP-MDRF] implémentée dans le système DMP.

***[RG_0770] Afficher la liste des DMP autorisés***

**EX_0.4-1020**

Lorsqu'elle est présentée à l'utilisateur, la liste des patients ayant autorisé l'accès à leur DMP comprend *a minima* les éléments de présentation suivants :

- Nom d'usage (EF_DMP11_02),
- Prénom (EF_DMP11_04),
- Nom de naissance (EF_DMP11_03).

| REC_0.4-1030 |
| --- |
| Si le nom d'usage (EF_DMP11_02) contient la valeur « NON RENSEIGNE » (13 caractères), il est recommandé de ne pas afficher cette valeur. |

*[RG_0780] Acquérir la sélection du DMP*

L'utilisateur sélectionne un DMP dans la liste des DMP.

La suite du processus se déroule pour le DMP sélectionné.

### 3.2.4.2 TD0.4 : liste des DMP autorisés

TD0.4 recherche les DMP de patients au statut « actif » pour lesquels l'acteur de santé a une autorisation d'accès au statut « valide ».

Il s'agit d'une transaction spécifique au DMP.

La transaction doit respecter les exigences concernant l'accès sécurisé au système DMP. Cf. TD0.1 au §5.3.

**Données en entrée**

| Balises XML | Occur-rence | Format | Alimentation données |
| --- | --- | --- | --- |
| `patientList` | 1 | - | |
| `startDate` | 1 | D | Date de filtrage à partir de laquelle la recherche est effectuée.<br>Format AAAAMMJJhhmmss. La date doit être passée en UTC. Le LPS doit traduire sa date locale en UTC. |
| `dateType` | 1 | AN | Type de recherche :<br>• `LASTAUTORIZATION` : recherche par rapport à la date d'autorisation de l'acteur de santé,<br>• `LASTDOC` : recherche par rapport à la date de dernier ajout d'un document. |
| `psOwnerID` | 0..1 | AN | Uniquement pour les non professionnels avec CPE. Cette donnée contient l'identifiant national de professionnel duquel retourner la liste des patients. |

**Tableau 13 : TD0.4 – données en entrée**

**Données en sortie**

| Balises XML | Occur-rence | Format | Alimentation données |
| --- | --- | --- | --- |
| `patientListResponse` | 1 | - | |
| `output` | 1 | - | |
| `patientlistData` | 0..n | - | En cas de succès, la réponse contient une occurrence de `patientlistData` par DMP trouvé. |

| | | | |
|---|---|---|---|
| patientIdentifier | 1..2 | - | Le ou les INS du patient pour chaque DMP trouvé :<br>• INS-C dans tous les cas (pendant la phase de transition entre les deux identifiants) ;<br>• NIR utilisable comme INS, si connu. |
| nationalId | 1 | 22AN | INS du patient (EF_DMP11_01). |
| nationalIdType | 1 | 20AN | OID des INS fournis afin de déterminer leur type (EF_DMP11_01) |
| lastName | 1 | 80AN | Nom d'usage (EF_DMP11_02)<br>NB : la valeur « NON RENSEIGNE » (13 caractères) indique que le nom d'usage n'est pas renseigné dans le DMP. |
| patronymicalName | 0..1 | 80AN | Nom de naissance (EF_DMP11_03) |
| firstName | 1 | 60AN | Prénom (EF_DMP11_04) |
| dateOfBirth | 1 | 8AN | Date de naissance (EF_DMP11_06) au format AAAAMMJJ. |
| MT | 1 | B | Statut médecin traitant DMP (EF_DMP01_07) |
| message | 1 | B | (Ce champ est obsolète et ne doit plus être utilisé par le LPS. Ignorer ce champ). |
| lastAccessDate | 1 | 14AN | Date de dernier accès sur le DMP du patient par l'utilisateur.<br>Format AAAAMMJJhhmmss. La date est retournée en UTC. Le LPS doit convertir dans sa date locale avant affichage à l'utilisateur. |
| lastUpdateDate | 1 | 14AN | Date de dernière modification des données administratives du DMP du patient.<br>Format AAAAMMJJhhmmss. La date est retournée en UTC. Le LPS doit convertir dans sa date locale avant affichage à l'utilisateur. |
| lastAddDate | 1 | 14AN | Date de dernier ajout d'un document dans le DMP du patient.<br>Format AAAAMMJJhhmmss. La date est retournée en UTC. Le LPS doit convertir dans sa date locale avant affichage à l'utilisateur. |
| status | 1 | 50AN | Code de retour : DMPOk (en cas de succès), ou code d'erreur (en cas d'erreur).<br>Voir annexe A7-1. |
| context | 0..1 | AN | Message d'erreur (en cas d'erreur).<br>Voir annexe A7-1. |

**Tableau 14 : TD0.4 – données en sortie**

Pour information : il y a une limitation du nombre de résultats retournés, issue d'un paramètre positionné sur le système DMP.

### 3.2.5 DMP_0.5 : rechercher un DMP (via TD0.5)

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

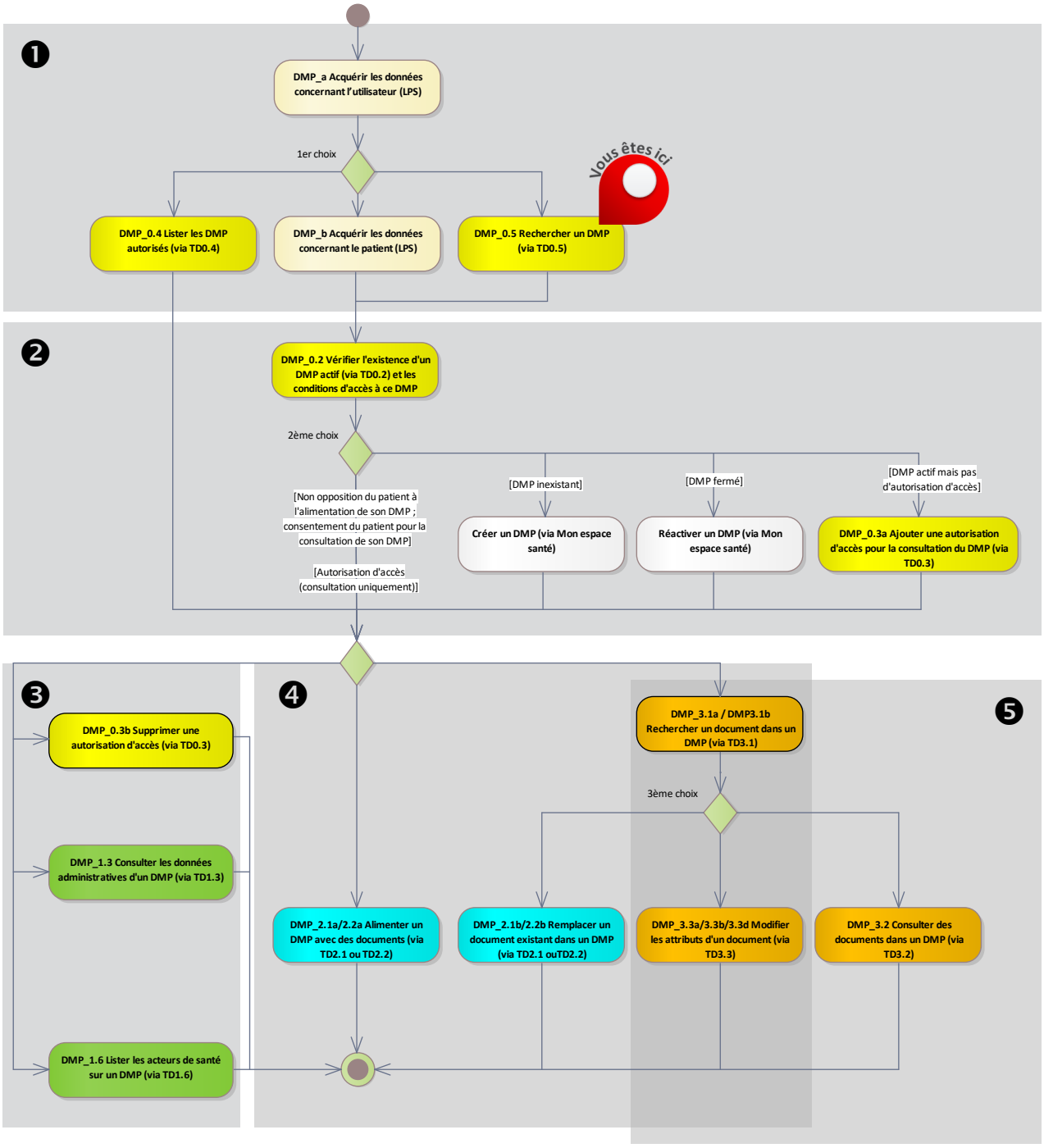



**Figure 17 : localisation de la fonctionnalité DMP_0.5 dans le processus regroupant les deux profils Alimentation et Consultation**

#### 3.2.5.1 Description de la fonctionnalité

**Vue générale**

***Description*** L'objectif de cette fonctionnalité est la recherche du DMP d'un patient lorsque l'utilisateur ne connaît pas l'INS du patient.

Cette fonctionnalité ne doit être utilisée qu'en cas d'impossibilité d'obtenir l'INS conformément au référentiel INS et des documents associés [REF-INS] (DMP_b). Dans tous les cas, les mesures à mettre en œuvre pour assurer la bonne identification du patient relèvent de la responsabilité de l'utilisateur. Elles sont décrites dans le Référentiel National d'IdentitoVigilance (RNIV) [REF-INS].

Cette fonctionnalité utilise la transaction TD0.5 pour faire une recherche à partir de traits d'identité et ainsi retrouver l'INS du ou des patients correspondant(s).

Le LPS :

- acquiert des critères de recherche (cf. RG_0810),
- obtient la liste des DMP correspondant aux traits d'identité du patient (RG_0820),
- affiche la liste des DMP trouvés (RG_0830),
- acquiert la sélection du DMP (RG_0840).

***Entrées et prérequis*** Aucune.
(Les données nécessaires sont acquises pendant le déroulement de la fonctionnalité.)

***Sorties*** Une liste de DMP de patients.

NB : uniquement les DMP actifs.

**Préambule**

NB : dans IHE PDQ, le séparateur utilisé dans les chemins identifiant les données est le point. Par exemple : `livingSubjectName.value.given.`

**Règles de gestion**

***[RG_0810] Acquérir des critères de recherche***

Le LPS acquiert au moins un critère de recherche parmi les données suivantes :

- Nom d'usage ou nom de naissance (`livingSubjectName.value.family`),
- Prénom (`livingSubjectName.value.given`),
- Sexe (`livingSubjectAdministrativeGender.value`),
- Date de naissance (`livingSubjectBirthTime.value`),

Le LPS peut acquérir également les données suivantes :

- Type de recherche sur les noms et le prénom (`value/@use` de `livingSubjectName`),
  - Recherche stricte si la donnée n'est pas fournie,
  - Recherche approchante si la donnée vaut `SRCH`,

Le fonctionnement des différents types de recherche est présenté dans le chapitre 3.2.5.2, page 70.

***[RG_0820] Obtenir la liste des DMP correspondant aux traits d'identité du patient***

Condition : le LPS a acquis un ou plusieurs traits d'identité du patient permettant de l'identifier.

Le LPS appelle la transaction TD0.5 en fournissant les données acquises précédemment. La transaction retourne les DMP correspondants.

Cf. §3.2.5.2 pour la description de la transaction.

**EX_0.5-1030**

Il est interdit de stocker les données des patients non concernés par la recherche de DMP et/ou de constituer une base de données avec celles-ci.

***Cas d'erreur***

***[CE1] Certains DMP dans la liste ne contiennent pas de NIR utilisable comme INS dans la donnée …/subject1/patient/id***

L'accès à ces DMP n'est pas possible via les interfaces LPS v2.

Pour information, ces DMP sont accessibles via le site Web-PS, avec l'INS-C. Cf. TD0.9 ou TD0.10.

***[RG_0830] Afficher la liste des DMP trouvés***

**EX_0.5-1010**

Le LPS doit afficher les deux noms retournés dans la réponse (nom d'usage (EF_DMP11_02) et nom de naissance (EF_DMP11_03)), si deux noms sont renseignés (cas d'une personne mariée par exemple).

**REC_0.5-1040**

Si le nom d'usage (EF_DMP11_02) contient la valeur « NON RENSEIGNE » (13 caractères), il est recommandé de ne pas afficher cette valeur.

**EX_0.5-1020**

L'usage des NIR fournis par la transaction TD0.5 doit être exclusivement réservé à l'accès au DMP d'un patient dans le cadre de sa prise en charge par un professionnel.

Le LPS ne doit pas afficher, ou rendre accessible aux utilisateurs, les NIR fournis par la transaction TD0.5, ni les exploiter en dehors de l'accès au DMP recherché par l'utilisateur via cette transaction.

***[RG_0840] Acquérir la sélection du DMP***

L'utilisateur sélectionne un DMP dans la liste des DMP.

La suite du processus se déroule pour le DMP sélectionné.

**Suite du processus**

Toutes les actions sont *a priori* possibles sur le DMP sélectionné si autorisation d'accès est au statut « valide » ou mode d'accès « centre de régulation ». Cf. fonctionnalité DMP_0.2 pour plus d'information.

### 3.2.5.2 TD0.5 : recherche sans INS de patient dans le système DMP

La transaction technique est définie dans [IHE-PDQV3] (ITI-47) au §3 et §3.47 Patient Demographics Query HL7 V3. La transaction utilise le message HL7 V3 « Patient Registry Find Candidates » (PRPA_IN201305UV02) pour la requête.

En retour, le message HL7 V3 « Patient Registry Find Candidates Query Response » (interaction PRPA_IN201306UV02) est renvoyé.

Note : La recherche ne supporte pas la réponse incrémentale (« continuation option » du profil PDQ V3, via le message « Query Control Act Request Continue/Cancel message (QUQI_MT000001UV01) »).

La transaction doit respecter les exigences concernant l'accès sécurisé au système DMP. Cf. TD0.1 au §5.3.

### Fonctionnement

Au moins 1 critère de recherche doit être passé en entrée (dans le cas contraire, un code erreur `DMPInvalidRequest` en renvoyé, accompagné d'un détail textuel indiquant la cause de l'erreur).

Recherche sur les noms

Un seul critère « nom » est à passer par le LPS. Le DMP recherche sur les deux noms : nom d'usage (ex. : marital) et nom de naissance.

La recherche sur les noms / prénom se fait de manière stricte si l'attribut `value/@use` de `livingSubjectName` n'est pas fourni. Dans ce cas, une recherche sur `given` = « Jean » et `family` « Dupond » ne retournera que les dossiers des « Jean Dupond ».

Si l'attribut `value/@use` de `livingSubjectName` est fixé à `SRCH`, alors une recherche sur `given` = « Jean » et `family`= « Du » retournera tous les dossiers dont le nom et le prénom commencent par « Jean » et « Du » (Jean Dupond, Jean Durand, Jean-Pierre Duval…).

Recherche sur le sexe

Une recherche sur le critère sexe avec la valeur `F` (Féminin) ou `M` (Masculin) est étendue automatiquement par le DMP à la valeur `U` (sexe indéterminé) (i.e. une recherche sur `F` ou `M` retournera également les DMP des patients dont le sexe est à `U`).

Résultat

La recherche est pour le moment restreinte à un maximum de 10 résultats : si le nombre de résultats à renvoyer dépasse le nombre maximum admissible par le DMP, la transaction renvoie une erreur `DMPTooManyResult`.

### Données en entrée

| XPath HL7 | Occur-rence | Description |
|---|---|---|
| `PRPA_IN201305UV02` | [1..1] | Racine du message HL7 |
| `@ITSVersion` | [1..1] | Fixé à `XML_1.0` |
| `Eléments « d'en-tête » du message […]` | [1..1] | Voir le chapitre 5.6.2.3. |
| `controlActProcess` | [1..1] | corps de la requête HL7 |
| `@classCode` | [1..1] | Valeur fixée à `CACT` |
| `@moodCode` | [1..1] | Valeur fixée à `EVN` |
| `Code` | [1..1] | |
| `@code` | [1..1] | Valeur fixée à `PRPA_TE201305UV02` |
| `@codeSystem` | [1..1] | Valeur fixée à `2.16.840.1.113883.1.6` |
| `queryByParameter` | [1..1] | |
| `queryId` | [1..1] | Identifiant unique de la requête, généré par le LPS |
| `@root` | [1..1] | Racine d'OID géré par le LPS |

| | | |
|---|---|---|
| @extension | [1..1] | Identifiant unique généré par le LPS |
| statusCode@ code | [1..1] | Valeur fixé à new |
| parameterList | [1..1] | Liste des paramètres de la requête |
| **livingSubjectAdministrativeGender** | [0..1] | Critère sexe |
| value/@code | [0..1] | Valeur du critère : M, F ou U |
| semanticsText | [0..1] | Fixé à LivingSubject.administrativeGender |
| **livingSubjectBirthTime** | [0..1] | Critère date de naissance |
| value/@value | [0..1] | Valeur du critère au format AAAAMMJJ |
| semanticsText | [0..1] | Fixé à LivingSubject.birthTime |
| **livingSubjectName** | [0..1] | Critères nom et/ou prénom |
| value/@use | [0..1] | Si présent : use = SRCH (permet une recherche approchante sur les nom/prénom)<br>Si non présent : recherche stricte sur les nom/prénom |
| value/family | [0..1] | Valeur du critère nom (au moins 2 caractères) |
| value/given | [0..1] | Valeur du critère prénom |
| semanticsText | [0..1] | Fixé à LivingSubject.name |

**Tableau 15 : TD0.5 – données en entrée**

**Données en sortie**

Note : Dans la version HL7 V3 2008 utilisée dans cette transaction, le code de retour est positionné dans l'élément : acknowledgement/typeCode/@code=AA (au lieu de acknowledgement/@typeCode=AA dans la version HL7 v3 2009).

| XPath HL7 | Occur-rence | Valeur / remarque |
|---|---|---|
| PRPA_IN201306UV02 | [1..1] | Racine du message HL7 |
| @ITSVersion | [1..1] | Fixé à XML_1.0 |
| Eléments « d'en-tête » du message […] | [1..1] | Voir le chapitre 5.6.2. |
| controlActProcess | [1..1] | corps de la requête HL7 |
| @classCode | [1..1] | Valeur fixée à CACT |
| @moodCode | [1..1] | Valeur fixée à EVN |
| code | [1..1] | |
| @code | [1..1] | Valeur fixée à PRPA_TE201306UV02 |
| @codeSystem | [1..1] | Valeur fixée à 2.16.840.1.113883.1.6 |
| subject | [0..N] | Occurrence d'un résultat de la réponse (un patient) |
| @typeCode | [1..1] | Valeur fixé à SUBJ |
| @contextConductionInd | [1..1] | Valeur fixé à false |
| registrationEvent | [1..1] | |

| | | |
|---|---|---|
| @classCode | [1..1] | Valeur fixée à REG |
| @moodCode | [1..1] | Valeur fixée à EVN |
| statusCode/@code | [1..1] | Valeur fixée à active |
| subject1 | [1..1] | |
| @typeCode | [1..1] | Valeur fixée à SBJ |
| patient | [1..1] | |
| @classCode | [1..1] | Valeur fixée à PAT |
| id | [1..2] | Le ou les INS du patient (EF_DMP11_01) pour chaque DMP trouvé.<br>• INS-C dans tous les cas (pendant la phase de transition entre les deux identifiants) ;<br>• NIR utilisable comme INS, si connu. |
| @root | [1..1] | Cf. [OID-INS]. |
| @extension | [1..1] | Valeur de l'INS du patient |
| statusCode/@code | [1..1] | Valeur fixée à active |
| patientPerson | [1..1] | |
| @classCode | [1..1] | Valeur fixée à PSN |
| @determinerCode | [1..1] | Valeur fixée à INSTANCE |
| name | [1..1] | |
| prefix | [0..1] | Civilité (EF_DMP11_07) |
| family[@qualifier="SP"] | [1..1] | Nom d'usage (EF_DMP11_02)<br>NB : la valeur « NON RENSEIGNE » (13 caractères) indique que le nom d'usage n'est pas renseigné dans le DMP. |
| family[@qualifier="BR"] | [0..1] | Nom de naissance (EF_DMP11_03) |
| given | [1..1] | Prénom (EF_DMP11_04) |
| administrativeGenderCode/@code | [1..1] | Sexe (EF_DMP11_05) |
| birthTime/@value | [1..1] | Date de naissance (EF_DMP11_06) au format AAAAMMJJ |
| addr | [0..1] | Adresse postale du patient (EF_DMP13) |
| postalCode | [0..1] | Valeur fixe « 00000 » (cinq zéros) |
| city | [0..1] | Valeur fixe « NON_RENSEIGNE »<br>NB : un caractère « _ » (underscore) est présent entre « NON » et « RENSEIGNE ». |
| subjectOf1 | [1..1] | |
| @typeCode | [1..1] | Valeur fixée à SBJ |
| queryMatchObservation | [1..1] | Indicateur de correspondance du résultat (pourcentage de correspondance par rapport aux critères passés) |
| @classCode | [1..1] | Valeur fixée à COND |
| @moodCode | [1..1] | Valeur fixée à EVN |
| code/@code | [1..1] | Pour le DMP : valeur fixée à POURCENTAGE |

| | | |
|---|---|---|
| value | [1..1] | |
| @xsi:type | [1..1] | Valeur fixée à INT |
| @value | [1..1] | Valeur de la correspondance en % |
| custodian | [1..1] | Organisation responsable de l'identité patient fournie (le DMP) |
| @typeCode | [1..1] | Valeur fixée à CST |
| assignedEntity | [1..1] | |
| @classCode | [1..1] | Valeur fixée à ASSIGNED |
| id/@root | [1..1] | OID du DMP : 1.2.250.1.213.4.1.1.1 |
| queryAck | [1..1] | Indicateur de retour de l'exécution de la requête |
| queryId | [1..1] | Identifiant de la requête envoyé par le LPS |
| @root | [1..1] | root de l'identifiant de la requête envoyé par le LPS |
| @extension | [1..1] | extension de l'identifiant de la requête envoyé par le LPS |
| queryResponseCode/@code | [1..1] | Voir [IHE-PDQV3] § 3.47.4.2.3 Expected Actions :<br>• OK si de la requête retourne au moins un résultat<br>• NF si de la requête ne retourne aucun résultat |
| resultTotalQuantity/@value | [1..1] | Nombre de résultats présents dans la réponse (*) |
| resultCurrentQuantity/@value | [1..1] | Nombre de résultats présents dans la réponse (*) |
| resultRemainingQuantity/@value | [1..1] | Nombre de résultats présents dans la réponse (*) |
| queryByParameter […] | [1..1] | Requête telle qu'elle est passée par le LPS en entrée |

**Tableau 16 : TD0.5 – données en sortie**

(*) ces champs servent habituellement à la recherche incrémentale ; ils sont toujours affectés avec la valeur du nombre de résultats de la réponse courante.

***En cas de succès de la transaction :***

- accusé de réception du traitement « ok » (acknowledgement/typeCode/@code=AA) ;
- indicateur de retour OK si un ou plusieurs résultats retournés ou NF si aucun résultat retourné pour les critères passés ;
- réponse au format HL7 V3 contenant la liste des patients retournés (une ou plusieurs occurrences de controlActProcess/subject).

***En cas d'erreur***

En cas d'erreur, la transaction retourne dans les éléments d'en-tête du message (voir chapitre 5.6.2.4 :

- l'accusé de réception du traitement en erreur (acknowledgement/typeCode/@code=AE),
- un code (acknowledgementDetail/@code),
- un message d'erreur (acknowledgementDetail/text).

Voir annexe A7-1.

### 3.2.6 DMP_0.9 : accès Web-PS Contextuel (TD0.9)

Cette fonctionnalité est décrite dans les éléments techniques. Cf. chapitre 5.4.

### 3.2.7 DMP_0.10 : accès Web-PS Contextuel en mode AIR (TD0.10)

Cette fonctionnalité est décrite dans les éléments techniques. Cf. chapitre 5.5.

## 3.3 DMP_1.x : données administratives du DMP d'un patient (profil Consultation seulement)

Ce chapitre décrit des fonctionnalités permettant de :

- Consulter les données administratives (DMP_1.3).
- Lister les acteurs de santé sur un DMP (DMP_1.6).

### 3.3.1 DMP_1.3 : consulter les données administratives d'un DMP (via TD1.3)

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

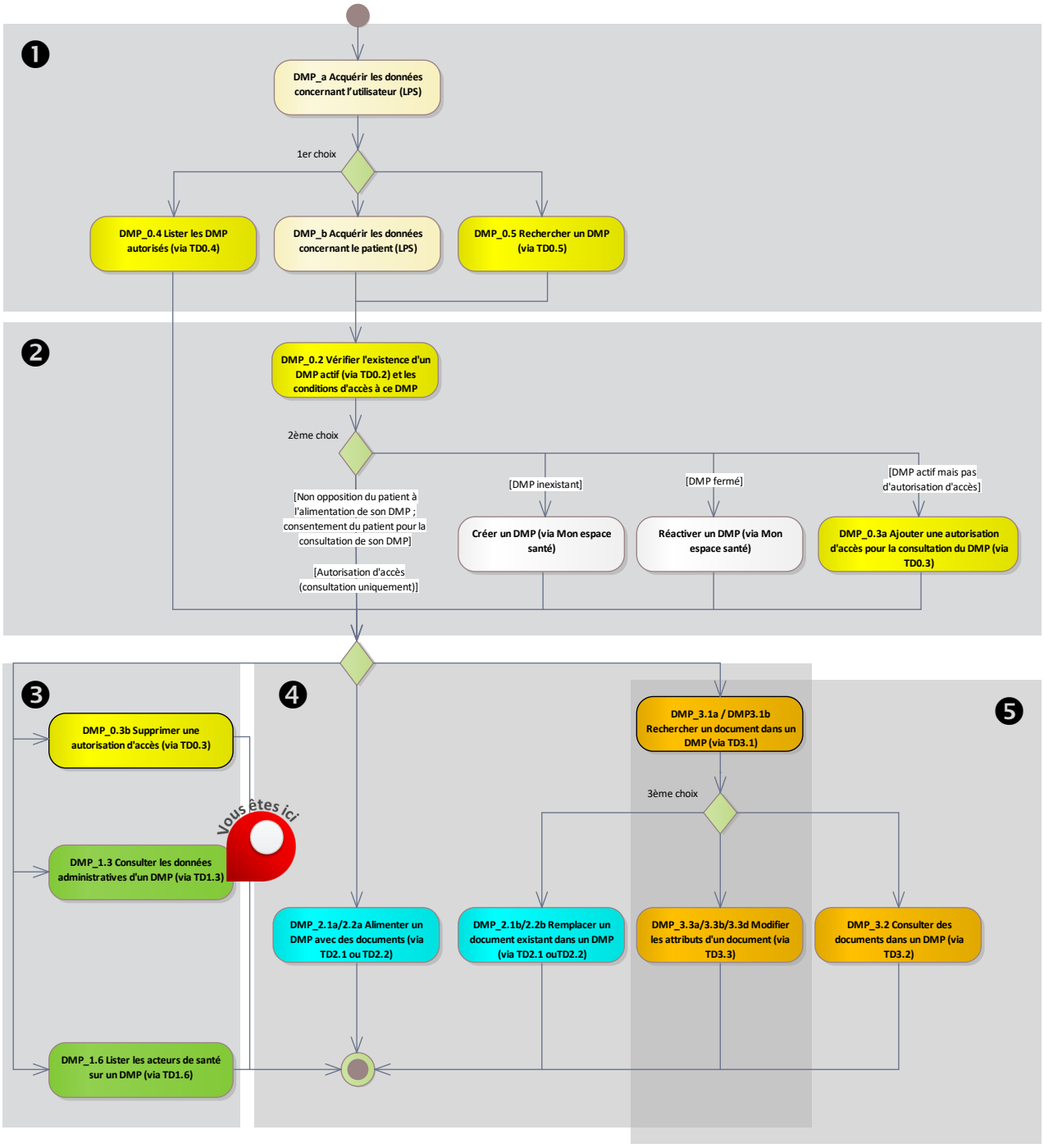



**Figure 18 : localisation de la fonctionnalité DMP_1.3 dans le processus regroupant les deux profils Alimentation et Consultation**

### 3.3.1.1 Description de la fonctionnalité

**Vue générale**

***Description*** Cette fonctionnalité permet de consulter les données administratives du DMP d'un patient. La mise à jour de ces données est prise en charge par « Mon espace santé ».

***Entrées et prérequis*** L'INS du patient (EF_DMP11_01).

Le statut « actif » du DMP du patient (EF_DMP12_01).

L'autorisation d'accès au DMP du patient (EF_DMP04_01) au statut « valide ».

***Sorties*** Les données administratives du DMP du patient.

**Règles de gestion**

***[RG_1320] Consulter les données administratives du DMP du patient***

Le LPS appelle la transaction TD1.3a.

Cf. §3.3.1.2 pour la description de la transaction.

***[RG_1330] Afficher les données administratives du DMP du patient***

Cf. les données décrites dans les chapitres 4.2.2 et 4.2.3.

**REC_1.3-1050**

Si le nom d'usage (EF_DMP11_02) contient la valeur « NON RENSEIGNE » (13 caractères) :

- il est recommandé de ne pas afficher cette valeur ;
- ne pas exécuter les règles de gestion suivantes de la fonctionnalité DMP_1.3.

### 3.3.1.2 TD1.3a : consultation des données administratives et de gestion d'un DMP

La transaction TD1.3a permet de récupérer la dernière version des données administratives et de gestion d'un DMP.

La transaction est décrite au §3.3.4 du [CI-GESTPAT] « Consultation de données de gestion de dossier ».

L'élément « reasonCode/@code » doit être positionné à « CNSLT_DATA » (voir §5.6.2.5).

La transaction doit respecter les exigences concernant l'accès sécurisé au système DMP. Cf. TD0.1 au §5.3.

**Données en entrée**

La transaction TD1.3a est quasiment identique à la transaction TD0.2 « Test d'existence et vérification de l'autorisation » décrite au §3.2.2.2.

Seules les données renvoyées par le DMP diffèrent.

**Données en sortie**

La transaction TD1.3a est quasiment identique à la transaction TD0.2 « Test d'existence et vérification de l'autorisation » décrite au §3.2.2.2.

Seules les données renvoyées par le système DMP diffèrent.

Contrairement au test d'existence, si le DMP du patient est fermé, aucune donnée concernant le patient n'est renvoyée (seul un code erreur est renvoyé).

***En cas de succès de la transaction :***

- accusé de réception du traitement « ok » (valeur `AA` dans `acknowledgement/typeCode`) ;
- les données administratives du patient sont renseignées dans l'élément pointé par le chemin XPath `controlActProcess/subject/registrationEvent/subject1/patient`, comme indiqué dans le §4.2.2 ; Les données suivantes (non modifiables) ne sont cependant pas renvoyées :
  - données du support Vitale ;
  - recueil du consentement patient à l'ouverture DMP ;
- s'il a été positionné dans le DMP du patient, les données du représentant légal sont renvoyées (dans : `controlActProcess/subject/registrationEvent/subject1/patient/patientPerson/personalRelationship`, puis détails dans le §4.2.3 « Représentant légal du patient »).

***En cas d'erreur***

En cas d'erreur de la transaction, un code et un message d'erreur sont renvoyés dans le message.

Voir annexe 7.

### 3.3.2 DMP_1.6 : lister les acteurs de santé sur un DMP (via TD1.6)

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

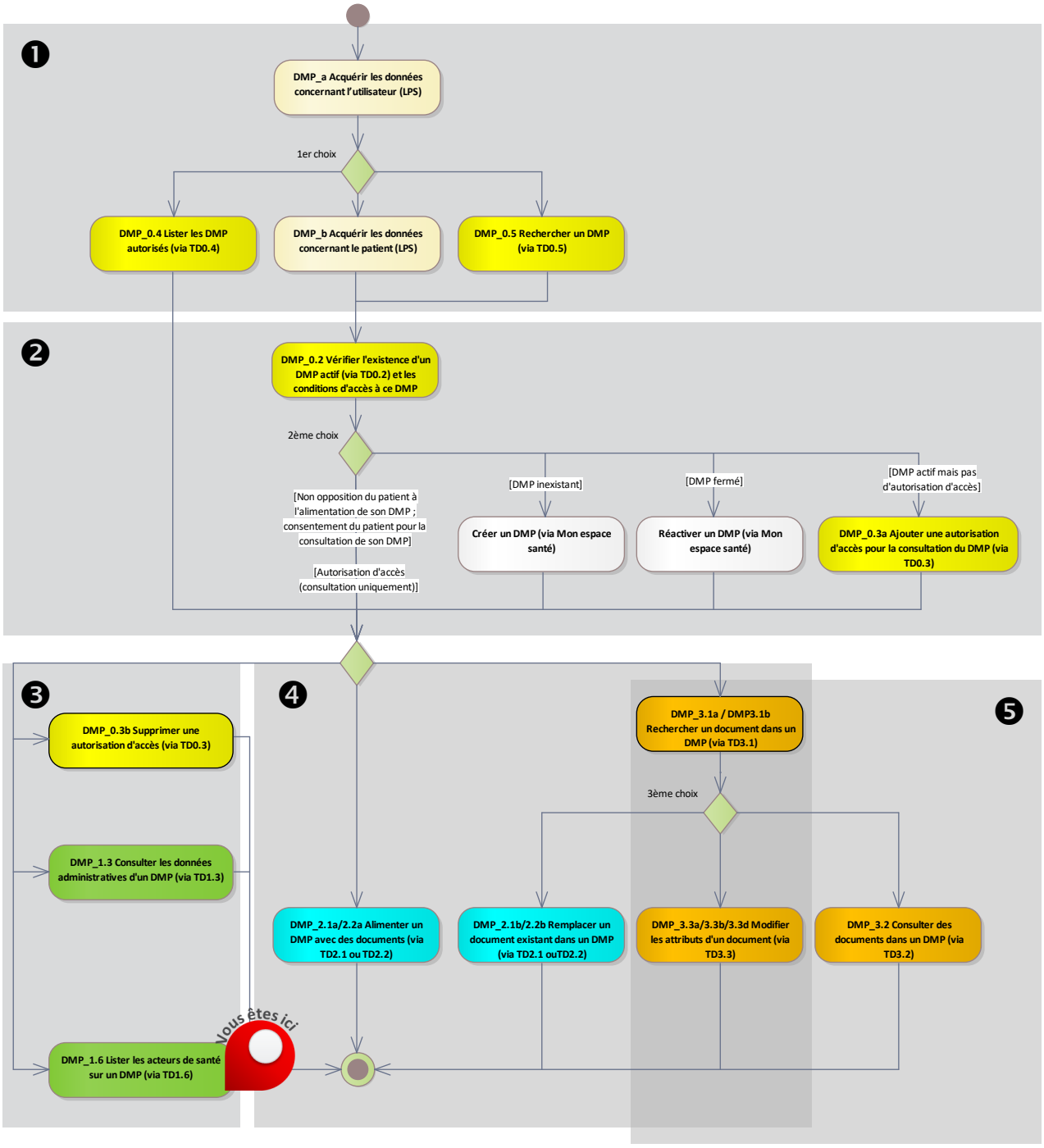



**Figure 19 : localisation de la fonctionnalité DMP_1.6 dans le processus regroupant les deux profils Alimentation et Consultation**

### 3.3.2.1 Description de la fonctionnalité

**Vue générale**

***Description***

Cette fonctionnalité permet d'appeler la transaction TD1.6 qui retourne, pour un DMP donné (à partir de l'INS du patient), la liste des acteurs de santé ayant ou ayant eu une autorisation sur ce DMP avec son statut (autorisé ou bloqué) et l'indication « médecin traitant DMP ».

L'utilisateur indique le type de recherche qu'il souhaite effectuer (cf. RG_1910) :

- acteurs autorisés,
- acteurs bloqués,
- ou les 2.

Le LPS :

- appelle la transaction TD1.6 et reçoit en retour le résultat de la recherche (cf. RG_1920),
- affiche la liste des acteurs de santé (cf. RG_1930).

***Entrées et prérequis***

L'INS du patient (EF_DMP11_01).

Le statut « actif » du DMP du patient (EF_DMP12_01).

L'autorisation d'accès au DMP du patient (EF_DMP04_01).au statut « valide ».

***Sorties***

Une liste d'acteurs de santé

**Règles de gestion**

***[RG_1910] Acquérir le mode demandé par l'utilisateur (`mode`)***

Le LPS peut ne demander :

- que la liste des acteurs de santé autorisés (`mode = ACTIVE`),
- que la liste des acteurs de santé bloqués (`mode = INTERDITE`),
- ou les 2 (`mode = TOUTE`).

***[RG_1920] Obtenir la liste des acteurs de santé***

Le LPS appelle la transaction TD1.6. Cf. description au chapitre 3.3.2.2.

***[RG_1930] Afficher la liste des acteurs de santé***

Le LPS doit convertir les dates/heures (`lastActionDate` et `startOfAuthorization`) en dates/heures locales pour l'affichage à l'utilisateur.

### 3.3.2.2 TD1.6 : liste des professionnels autorisés / bloqués sur le DMP d'un patient

Cette transaction retourne, pour un DMP donné (à partir de l'identifiant INS du patient), la liste des acteurs de santé ayant ou ayant eu une autorisation sur ce DMP.

La transaction doit respecter les exigences concernant l'accès sécurisé au système DMP. Cf. TD0.1 au §5.3.

**Données en entrée**

Note : L'INS du patient est passé dans le VIHF.

| Balises XML | Occur-rence | Format | Alimentation données |
|---|---|---|---|
| `listAuthorizationByPatient` | 1 | - | |
| `mode` | 1 | AN | Type de professionnels recherchés.<br>Valeurs possibles :<br>• `ACTIVE` : professionnels autorisés,<br>• `INTERDITE` : professionnels bloqués,<br>• `TOUTE` : professionnels autorisés et professionnels bloqués. |

**Tableau 17 : TD1.6 – données en entrée**

**Données en sortie**

***En cas de succès de la transaction :***

Le système DMP retourne les données décrites ci-dessous.

| Balises XML | Occur-rence | Format | Alimentation données |
|---|---|---|---|
| `listAuthorizationByPatientResponse` | 1 | - | |
| `output` | 1 | - | |
| `listOfAuthorizationByPatient` | 0..n(*) | - | Une occurrence pour chaque autorisation retournée (en cas de succès). |
| `nationalId` | 1 | 20AN | Identifiant national de l'acteur de santé :<br>• professionnel : ADELI, RPPS… (EF_DMP01_01)<br>• Structure : identifiant de la structure (EF_DMP02_01). |
| `nationalIdType` | 1 | 20AN | OID de l'identifiant fourni afin de déterminer son type :<br>• 1.2.250.1.71.4.2.1 pour les professionnels<br>• 1.2.250.1.71.4.2.2 pour les structures |
| `firstName` | 0..1 | 60AN | Prénom (de personne physique) (EF_DMP01_05).<br>Non renseigné pour une structure de soins. |
| `lastName` | 1 | 80AN | Nom de personne physique (EF_DMP01_04) ou morale (structure de soins) (EF_DMP02_02) |
| `lastActionDate` | 1 | 14AN | Date de la dernière action de l'acteur de santé sur le DMP du patient.<br>Format AAAAMMJJhhmmss. La date est retournée en UTC. |

| | | | |
|---|---|---|---|
| mode | 1 | AN | Valeurs :<br>• ACTIVE : professionnel autorisé,<br>• INTERDITE : professionnel bloqué. |
| startOfAuthorization | 1 | 14AN | Date de début d'autorisation.<br>Format AAAAMMJJhhmmss. La date est retournée en UTC. |
| codeSpeciality | (*) | | Code profession, et spécialité pour les médecins et pharmaciens (séparé par « / » dans ce cas).<br>Codé dans la nomenclature authorSpecialty de l'ANS.<br>Exemple pour médecin : G15_10/SM26.<br>Non renseigné pour une structure de soins. |
| libSpeciality | (*) | | Libellé associé à codeSpeciality : « profession / spécialité ».<br>Exemple pour un médecin : « Médecin - Qualifié en Médecine Générale (SM) ».<br>Non renseigné pour une structure de soins. |
| specificRight | | | Rôle spécifique de l'acteur de santé : valeur MEDECIN_TRAITANT si le professionnel est Médecin traitant DMP.<br>Non renseigné pour une structure de soins. |
| status | 1..1 | 50AN | Code de retour : DMPOk (en cas de succès), ou code d'erreur (en cas d'erreur).<br>Voir annexe A7-1. |
| context | 0..1 | AN | Message d'erreur (en cas d'erreur).<br>Voir annexe A7-1. |

**Tableau 18 : TD1.6 – données en sortie**

(*) Un professionnel ayant de multiples professions donnera lieu à plusieurs occurrences de listOfAuthorizationByPatient (le professionnel apparait N fois par profession), chacune avec une profession différente dans codeSpeciality et dans libSpeciality.

***En cas d'erreur de la transaction :***

Voir annexe 7.

## 3.4 DMP_2.x : alimentation du DMP d'un patient

Ce chapitre décrit deux fonctionnalités.

- La première permet d'ajouter de nouveaux documents dans le DMP d'un patient (DMP_2.1a/2.2a).
- La deuxième permet de remplacer un document dans le DMP d'un patient (DMP_2.1b/2.2b).

Ces fonctionnalités mettent en œuvre deux transactions :

- La transaction TD2.1 est utilisée pour les professionnels hors authentification par CPE.
- La transaction TD2.2 est utilisée pour les secrétaires médicaux du secteur libéral ou en EHPAD équipés d'une CPE (directement ou indirectement nominative), Le système DMP contrôle que le secteur d'activité de la structure à laquelle est rattachée la CPE est bien dans le « secteur libéral » ou le « secteur EHPAD ».

### *Organisation des métadonnées XDS et données CDA*

Les documents sont déposés dans le système DMP sous la forme de lots de soumission XDS organisés comme suit :

- Chaque lot de soumission XDS contient un ou plusieurs documents.
- Chaque document est décrit sous la forme suivante :
  - de métadonnées XDS,
  - de données d'en-tête CDA,
  - et d'un corps du document CDA.

Le corps du document CDA peut être :

- non structuré (PDF, texte ou image),
- ou structuré (XML).

Un document dont le corps est structuré (XML) peut être auto-présentable. Dans ce cas, le document intègre sa propre feuille de style.

Une illustration de l'organisation technique de ces données est disponible dans l'annexe A6-2.1.

## 3.4.1 DMP_2.1/2.2 : alimenter le DMP d'un patient avec des documents (via TD2.1 ou TD2.2)

### 3.4.1.1 DMP_2.1a/2.2a : alimenter le DMP d'un patient avec des *nouveaux* documents

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

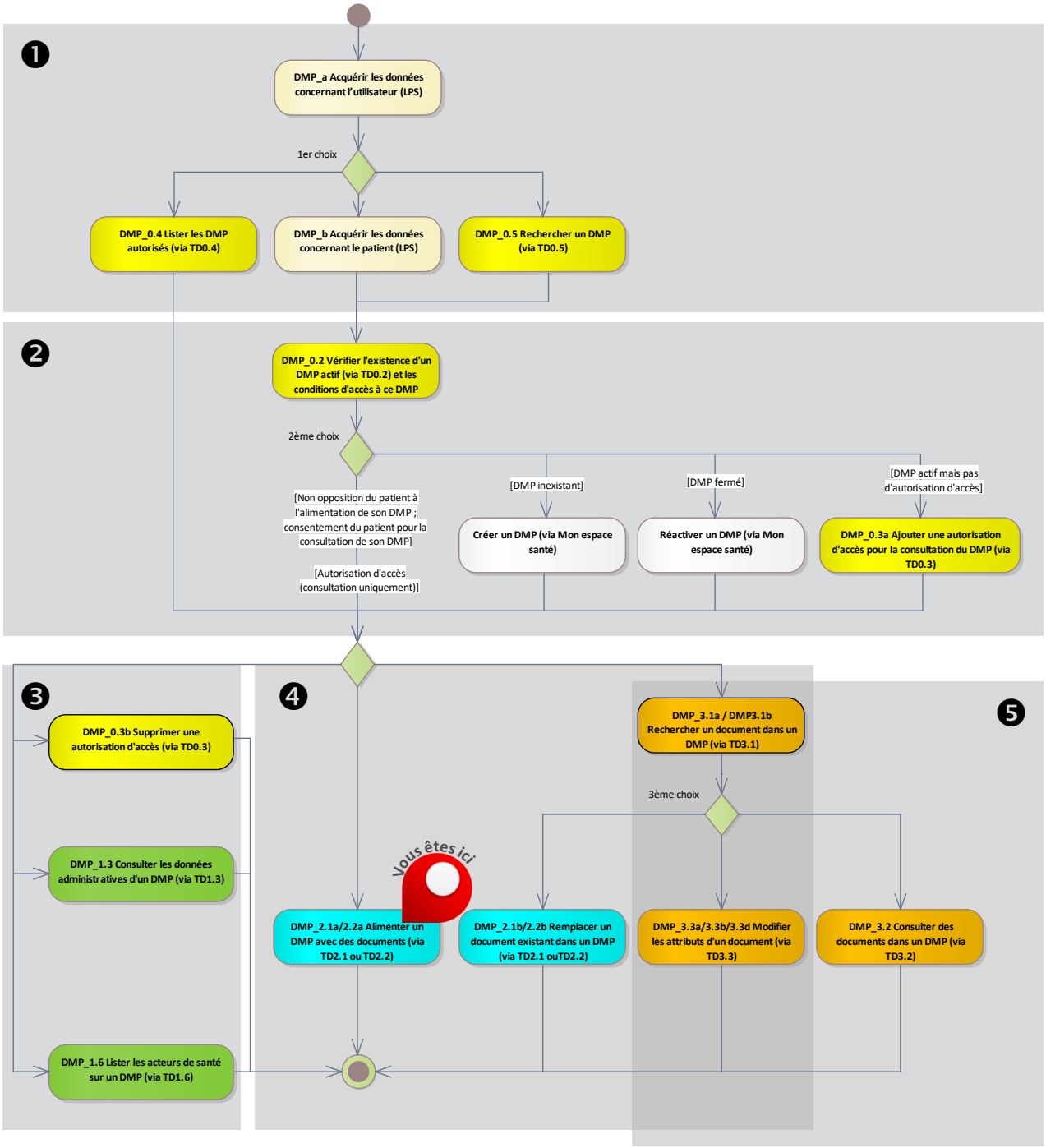



**Figure 20 : localisation de la fonctionnalité DMP_2.1a/2.2a dans le processus regroupant les deux profils Alimentation et Consultation**

**Vue générale**

***Description*** Cette fonctionnalité permet d'alimenter le DMP d'un patient avec un ou plusieurs nouveaux documents :

- décrits sous la forme de documents CDA et de métadonnées XDS,
- et transmis au système DMP sous la forme d'un lot de soumission XDS signé (XAdES).

La cinématique générale est la suivante.

Le professionnel constitue le ou les document(s) dans le LPS . Cf. §3.4.1.1.1

Le LPS :

- construit le ou les document(s)
  - construit le document au format CDA Cf. §3.4.1.1.2
  - alimente les métadonnées XDS Cf. §3.4.1.1.3
- réalise la signature du ou des document(s) (non obligatoire) Cf. §3.4.1.1.4
- constitue un lot de soumission XDS et signe ce lot (XAdES) Cf. §3.4.1.1.5
- soumet le lot de documents au système DMP Cf. §3.4.1.1.6

***Entrées et prérequis*** L'INS du patient (EF_DMP11_01).

Le statut « actif » du DMP du patient (EF_DMP12_01).

***Sorties*** Un DMP alimenté avec un ou plusieurs nouveaux documents.

## 3.4.1.1.1 Constituer le ou les document(s) dans le LPS

**Vue générale**

L'objectif de cette partie n'est pas de décrire la solution à mettre en œuvre dans le LPS pour récupérer les données ni d'édicter des règles ergonomiques qui sont laissées à l'appréciation de l'éditeur. Cette partie a par contre pour objectif de préciser certaines exigences ou recommandations portant sur des données particulières, ces exigences ou recommandations ayant ensuite un impact direct dans l'alimentation du DMP.

Le système DMP introduit des exigences supplémentaires par rapport aux normes XDS/CDA qui sont décrites dans les règles :

- acquérir le type du document (cf. RG_2010),
- acquérir le titre du document (cf. RG_2020),
- acquérir la visibilité du document (cf. RG_2030).

**Règles de gestion**

*[RG_2010] Acquérir le type du document (EF_DMP31_04)*

**EX_2.1-1010**

Les documents d'expression personnelle du patient ne peuvent pas être créés via l'interface LPS :

- classCode = 90, et les typeCode associés,
- et/ou les typeCode commençant par « DOCPAT ».

Le document "Données de remboursement" ne peut être alimenté que par l'assurance maladie. Il ne peut donc pas être créé via l'interface LPS (classCode = 60, et typeCode = REMB).

Le document « historique de vaccinations » est unique par DMP. Il est créé automatiquement par le SI DMP lors de l'ajout d'une première vaccination (soit via WebPS, soit lors de l'alimentation d'une première note de vaccination en LPS, soit par le patient lui-même via « Mon espace santé » ou Web Patient ou application mobile pour les DMP non associés à « Mon espace santé »). Il ne peut pas être créé via l'interface LPS (classCode = 52, et typeCode = 11369-6). Un fonctionnement spécifique est défini dans le chapitre 6.1.

*[RG_2020] Acquérir le titre du document*

Pour les documents, la taille maximale du champ "titre" est celle définie dans la norme XDS.b, à savoir 128 caractères : "Max length, 128 bytes, UTF-8".

**EX_2.1-1020**

Le titre du document doit être compréhensible et ne peut être arbitrairement tronqué à la limite de taille (128 caractères).

**EX_2.1-1030**

Le titre d'un document doit en refléter le contenu médical (le titre est saisissable par le professionnel).

**EX_2.1-1040**

Le titre d'un document doit être modifiable.

*[RG_2030] Acquérir la visibilité du document (EF_DMP31_03)*

**EX_2.1-1050**

A chaque alimentation du DMP à partir d'un LPS, l'acteur doit indiquer, pour chaque document :

- si le document doit être masqué aux professionnels ou pas ;
- si le document doit être visible au patient ou pas.

NB : un document ne peut pas être à la fois non visible au patient et masqué au professionnel tant que le paramètre `cumul-invisible_patient-masque_ps`[6] contient la valeur `false` (§ 3.1.1).

Si la gestion des mineurs est activée (cf. paramètre `fonctions-gestion-mineurs` au § 3.1.1) et que le patient est mineur :

- en cas de connexion secrète (cf. EX_0.1-1100 § 5.3.1.3), l'acteur ne peut déposer que des documents invisibles aux représentants légaux ;
- en cas de connexion non secrète, l'acteur doit indiquer si le document est visible ou invisible aux représentants légaux.

Pour l'alimentation automatique, le masquage aux professionnels et la visibilité au patient peuvent être déterminés à l'aide de règles spécifiques à chaque contexte (type de document, type d'établissement, …).

**REC_2.1-1060**

Exemple de mise en œuvre pour la confidentialité du document :

**Confidentialité du document**

**Pour le patient**

( ) Document non visible par le patient : vous souhaitez que ce document ne soit pas visible par le patient car il nécessite une information préalable par un professionnel.

**Pour les représentants légaux du patient**

( ) Document non visible par les représentants légaux.

**Pour les professionnels**

(x) Document visible par les professionnels autorisés à accéder aux documents du DMP du patient

( ) Document masqué aux professionnels : document visible uniquement par son auteur, les médecins traitants DMP et le patient.

Le professionnel peut rendre le document visible au patient (voir DMP_3.3), suite à la consultation d'annonce par exemple. Le professionnel peut aussi rendre le document visible aux représentants légaux du patient.

Cette caractéristique est portée par la métadonnée XDS `confidentialityCode` du document (cf. [CI-PARTAGE]).

[6] Le nom technique n'évolue pas. Il conserve le terme « PS ».

**REC_2.1-1065**

Les contraintes suivantes pourraient être levées dans le futur :

- « un document ne peut pas être à la fois non visible au patient et masqué au professionnel » (cf. paramètre `cumul-invisible_patient-masque_ps` § 3.1.1) ;
- « un document visible au patient ne peut pas être rendu invisible au patient » ;
- « un document visible aux représentant légaux ne peut pas être rendu invisible aux représentant légaux ».

Il est conseillé de pouvoir lever facilement les deux dernières contraintes, par exemple par paramétrage du logiciel.

#### 3.4.1.1.2 Construire le ou les document(s) de santé au format CDA R2 (et correspondance avec les métadonnées XDS)

**Vue générale**

Le système DMP introduit des exigences supplémentaires par rapport aux normes XDS/CDA. Ces exigences sont décrites dans les règles :

- acquérir les données CDA R2 (cf. RG_2110),
- acquérir le niveau de confidentialité du document (cf. RG_2120),
- acquérir les données CDA (et les métadonnées XDS) de type date/heure (cf. RG_2130).

Le LPS peut ensuite construire les documents de santé au format CDA R2 (cf. RG_2180).

**Règles de gestion**

*[RG_2110] Acquérir les données CDA R2*

Données obligatoires et facultatives

Les éditeurs doivent s'assurer que le logiciel gère l'ensemble des données obligatoires à fournir dans les transactions, les documents CDA et les métadonnées XDS.

Il faut dans un premier temps bien distinguer les données à fournir :

- dans un document CDA,
- dans les métadonnées XDS du document,
- dans les métadonnées XDS du lot de soumission.

Cardinalité des données CDA

Dans un document CDA, l'information est portée par la cardinalité indiquée pour chaque donnée dans les documents [CI-STRU-ENTETE] et les volets des documents structurés de la couche « contenu » publiés au CI-SIS.

- Lorsque la cardinalité est du type [0..*], la donnée n'est pas obligatoire et peut ne pas être fournie.
- Lorsque la cardinalité est du type [1..*], la donnée est obligatoire et doit être fournie.
- Lorsque la cardinalité est définie précisément comme dans [2..2], le nombre d'occurrences (ici 2) doit être respecté.

Dans certains cas, lorsque la donnée n'est pas connue, le LPS doit permettre d'indiquer, au moyen d'un attribut `nullFlavor`, la raison de l'absence de l'information.

Dans d'autres cas, l'utilisation de `nullFlavor` est interdite.

Cardinalité des métadonnées XDS

Pour les métadonnées XDS, il faut combiner cardinalités et code d'usage indiqués pour chaque donnée dans le document [CI-PARTAGE] (en particulier le récapitulatif « Code d'usage et Cardinalités »).

- Lorsque la cardinalité est du type [0..*] et le code d'usage = 'O' (Optionnel), la donnée n'est pas obligatoire.
- Lorsque la cardinalité est du type [0..*] et le code d'usage = 'R2' (Requis si connu), la donnée n'est pas obligatoire, mais lorsqu'elle est connue, elle doit être fournie.
- Lorsque la cardinalité est du type [1..*], le code d'usage sera forcément = 'R' (Requis). Dans ce cas, la donnée est obligatoire et doit être fournie.
- Lorsque la cardinalité est définie précisément comme dans [1..1], le nombre d'occurrences (ici 1) doit être respecté.

Quelle différence y a-t-il entre les données « requises » et « requises si connues » ?

Cette différence n'existe que pour les métadonnées XDS ; dans le cas des données d'un document CDA, cette subtilité n'existe pas et il faut se baser sur les cardinalités uniquement, avec la possibilité éventuelle d'utiliser un `nullFlavor`.

- Donnée requise (code d'usage R) : Le LPS doit obligatoirement gérer cette donnée et elle doit être obligatoirement renseignée et transmise dans les métadonnées XDS.
- Donnée requise si connue (code d'usage R2) : Le LPS doit aussi obligatoirement gérer cette donnée et permettre à l'utilisateur de la saisir (ou au système de la renseigner) dès lors qu'il la connaît afin qu'elle puisse être transmise dans les métadonnées XDS. L'utilisateur (ou le système) doit pouvoir déclarer qu'il ne connaît pas l'information via son interface de création du document (i.e. IHM pour un utilisateur). Le cas échéant, l'élément d'en-tête CDA correspondant n'est pas intégré dans le CDA et la métadonnée XDS correspondante n'est pas présente parmi les métadonnées XDS du document. »

En pratique, comment le LPS doit-il gérer les données R2 (du CI-SIS) ?

| Donnée | Donnée CDA [0..1] | Métadonnée XDS [R2] | Donnée du VIHF |
|---|---|---|---|
| Structure de soins (EF_DMP02_01)<br>Cette donnée étant obligatoirement renseignée dans le VIHF, il est fortement conseillé de la renseigner dans le document CDA et dans les métadonnées XDS. | `author/assignedAuthor/representedOrganization` | `authorInstitution`[7] | `Identifiant_Structure` [Obligatoire] |
| Rôle fonctionnel du professionnel<br>Cette donnée n'est pas dans le VIHF, optionnelle dans le document CDA et [R2] dans les métadonnées XDS.<br>L'éditeur est libre de gérer ou pas cette donnée mais lorsqu'elle est renseignée dans le CDA, alors il faut mettre la même valeur dans la métadonnée XDS. | `author/functionCode @displayName` | `authorRole` | [Cette donnée n'existe pas dans le jeton VIHF] |

[7] Exception : cette donnée est à renseigner obligatoirement dans le contexte du DMP. Cf. règle RG_2240.

| | | | |
|---|---|---|---|
| Profession et Spécialité du professionnel (EF_DMP01_03)<br>Dans le VIHF, la profession est obligatoire et la spécialité est conditionnelle (elle est obligatoire pour les médecins et pharmaciens). Il est fortement conseillé de les renseigner dans le document CDA et dans les métadonnées XDS. | `author/assignedAuthor/code@code`<br>`author/assignedAuthor/code@displayName`<br>`author/assignedAuthor/code@codeSystem` | `authorSpecialty` | `Urn :oasis :names :tc :xacml :2.0 :subject:role`<br>[Profession : Obligatoire]<br>[Spécialité : Conditionnelle] |
| Date de fin de l'acte<br>La date de fin de l'acte est généralement « considérée » comme obligatoire. Il est donc fortement conseillé de la renseigner. Dans certains cas, elle est égale à la date de début de l'acte. | `documentationOf/serviceEvent/effectiveTime/high@value` | `serviceStopTime` | [Cette donnée n'existe pas dans le jeton VIHF] |

***[RG_2120] Acquérir le niveau de confidentialité du document***

**REC_2.1-1100**

Ni le standard CDA ni le Cadre d'Interopérabilité des SIS ne précisent la manière dont chaque valeur possible du `confidentialityCode` (Normal, Restreint, Très Restreint) doit être interprétée. Un document ayant un niveau renforcé de confidentialité (restreint ou très restreint), devrait être remis en mains propres, ou envoyé sous pli scellé ou par message direct à son destinataire. Il ne devrait pas être mis en partage.

Si votre logiciel ne gère pas de niveau de confidentialité, il est recommandé de renseigner la donnée « confidentialityCode » avec la valeur N (Normal).

***[RG_2130] Acquérir les données CDA et les métadonnées XDS de type date/heure***

**EX_2.1-1110**

Les champs de type date/heure sont codés dans une zone de temps différente entre les métadonnées XDS et le CDA R2. Les champs date/heure XDS doivent être codés en UTC (Universal Time Coordinated) et ceux du CDA correspondant en date/heure locale du producteur du document incluant le décalage par rapport à UTC.

Le LPS devra donc transformer les dates/heure du CDA de la date/heure locale en date/heure UTC (ou inversement, de la date/heure UTC en date/heure locale dans le cas où les dates sont transformées des métadonnées XDS vers le CDA). Par exemple, l'heure locale en France métropolitaine est égale à UTC + 0100 (1 heure) en hiver et à UTC +0200 (2 heures) en été.

Illustration : 12h00 en heure locale en France métropolitaine correspond à :

- 11h00 en UTC en hiver,
- 10h00 en UTC en été.

*[RG_2180] Construire les documents de santé au format CDA R2*

**EX_2.1-1070**

Ces documents de santé doivent respecter les spécifications décrites dans les volets de la couche « contenu » du CI-SIS. Chaque volet de contenu est basé sur un socle commun se conformant au standard HL7 Clinical Document Architecture, Release 2.0 (CDA R2) publiés dans l'Edition Normative HL7 v3 de mai 2005.

Le document [CI-STRU-ENTETE] définit la structuration minimale des documents à respecter que ce soit pour les documents dits « non structurés » (document PDF, RTF…) ou pour les documents « structurés » (CDA R2 de niveau 3).

Enfin, un document de santé correspondant à un modèle structuré spécifié au CI-SIS doit être conforme au volet de ce document publié dans le CI-SIS.

Les jeux de valeurs embarqués dans le standard CDA, les jeux de valeurs définis par le volet « Structuration minimale des documents médicaux » et les jeux de valeurs définis par le volet spécifique au document structuré doivent être utilisés dans le document.

**EX_2.1-1071**

Tout document médical au format CDA R2 doit être conforme :

- au standard CDA R2 utilisé pour les documents médicaux (schéma xml CDA_extended.xsd). La conformité des documents CDA R2 peut se contrôler à partir :
  - du schéma XML « CDA_extended.xsd » pour la conformité au standard CDA. Tout écart détecté se traduit par la déclaration de non-validité du document.
  - du schématron correspondant au volet du document mis en œuvre pour les documents de santé structurés spécifiés au CI-SIS ou à défaut du schématron « CISIS_StructurationCommuneCDAr2 » pour les autres documents. Cette analyse produit un rapport listant les éventuelles non-conformités détectées ; la présence d'une seule non-conformité se traduit par la déclaration de non-conformité du document.
  - CDA_extended.xsd et le schématron « CISIS_StructurationCommuneCDAr2 » sont disponibles dans [TEST-CONTENU-CDA].
  - Les jeux de valeurs sont exploités par la vérification de conformité, toute valeur étrangère détectée se traduit par une non-conformité.
- aux spécifications internationales IHE de l'en-tête,
- aux spécifications françaises de l'en-tête (Volet Structuration minimale des documents de santé),
- aux spécifications internationales IHE du corps (sections, entrées et jeux de valeurs),
- aux spécifications françaises du corps (sections, entrées et jeux de valeurs) (Volet Modèles de contenus CDA),
- aux spécifications françaises du corps (sections et entrées créées par l'ANS pour les volets français) (Volet Modèles de contenus CDA),
- aux spécifications d'un document (en-tête et corps) (Volet du document).

**REC_2.1-1080**

Il est recommandé de prendre en compte dès la conception du LPS les tests à effectuer avec les schématrons. Les schématrons sont disponibles sur le site de l'ANS. Cf. [TEST-CONTENU-CDA].

**EX_2.1-1090**

Les familles de produits contenant des LPS de type EAI doivent nécessairement réaliser des contrôles de conformité de tous les documents CDA R2 (cf. exigence EX_2.1-1071) avant envoi au DMP.

Pour les documents « note de vaccination » (typeCode = 87273-9), le contrôle schématron ne suffit pas. Il faut également respecter les exigences décrites dans le chapitre 6.1.

***Cas particuliers de la règle de gestion RG_2180***

***[CP1] Construire les documents de santé au format CDA R2 auto-présentables***

Ce format est décrit dans [CI-STRU-ENTETE].

L'usage de CDA auto-présentables est optionnel mais est néanmoins soumis aux exigences décrites ci-après lorsqu'il est implémenté.

Impact sur les métadonnées XDS

L'usage de CDA auto-présentables en alimentation du DMP impose les spécificités suivantes dans les métadonnées XDS du document, décrites dans [CI-PARTAGE] :

- le champ `mimeType` doit prendre la valeur `application/xslt+xml`,
- s'il est signé électroniquement, le calcul des champs size et hash est spécifique et précisé dans [CI-PARTAGE].

**EX_2.1-1115**

Pour des raisons de sécurité, un LPS alimentant le DMP avec des CDA auto-présentables ne doit pas inclure de script (balise HTML <script>) ni de lien vers des ressources externes (styles CSS externes, import de scripts, iframes, fenêtres surgissantes, liens, images, vidéos, etc.) dans la feuille de style couplée au document. Seules sont autorisées des ressources encapsulées dans la feuille de style (liens internes, styles CSS inclus dans le document, images encapsulées…). La feuille de style couplée au document doit être autonome en termes de visualisation à l'utilisateur.

**EX_2.1-1116**

Pour des raisons de sécurité, un LPS alimentant le DMP avec des documents CDA auto-présentables ne doit pas permettre à tous ses utilisateurs de modifier la feuille de style XSL des documents qu'il produit. Si le LPS permet de modifier des feuilles de style « modèles » utilisées par le LPS pour constituer les CDA auto-présentables envoyés au DMP, seuls des acteurs autorisés (de type « administrateurs ») doivent pouvoir le faire. Le LPS doit mettre en œuvre des moyens pour protéger et confiner en son sein les feuilles de style des documents CDA auto-présentables qu'il produit.

**REC_2.1-1117**

Il est recommandé de respecter un format d'affichage A4 portrait pour les documents CDA auto-présentables.

#### 3.4.1.1.3 Acquérir les métadonnées XDS

**Vue générale**

Le système DMP introduit des exigences supplémentaires par rapport aux normes XDS/CDA qui sont décrites dans les règles suivantes :

- les règles concernant les métadonnées XDS des documents et du lot de soumission,
  - acquérir les métadonnées XDS (cf. RG_2210),
  - acquérir les identifiants uniques (cf. RG_2220),
  - acquérir les données concernant l'auteur (cf. RG_2230),
  - acquérir l'organisation (cf. RG_2240),
  - acquérir les commentaires (cf. RG_2250),
- les règles concernant les métadonnées XDS d'un document,
  - contrôler que l'ajout du document est effectué par l'auteur du document (cf. RG_2310),
  - déterminer le hachage du document (cf. RG_2320),
  - acquérir le cadre d'exercice de l'acte qui a engendré la création du document (cf. RG_2330),
  - acquérir l'identifiant principal du patient dans le système d'information du producteur du document (cf. RG_2340),
  - acquérir les traits d'identité du patient (cf. RG_2350),
- les règles concernant les métadonnées XDS d'un lot de soumission,
  - acquérir la date et heure d'envoi du lot de soumission (cf. RG_2410),
  - acquérir le titre du lot de soumission (cf. RG_2420),
  - acquérir le type d'activité de l'évènement clinique ayant abouti à l'envoi du/des document(s) du lot de soumission (cf. RG_2430).

**Préambule**

La mise en partage des documents nécessite la gestion de métadonnées (documents et lots de soumission) via le profil IHE XDS.b.

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 déjà stockées dans le LPS (titre du document, date de l'acte médical documenté, type du document…) ou
- du support d'authentification (carte CPx, certificat logiciel pour personne morale).

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

**EX_2.1-1125**

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

Taille maximum des champs ebXML

La longueur des champs est spécifiée dans IHE XDS.b ou à défaut dans ebXML mais dans certains cas, une longueur spécifique est précisée dans le présent document.

**Règles de gestion**

## Les métadonnées XDS des documents et du lot de soumission

*[RG_2210] Acquérir les métadonnées XDS des documents et du lot de soumission*

Les métadonnées XDS des documents à envoyer sont définies dans [CI-PARTAGE] « Métadonnées XDS d'une fiche ».

Les métadonnées du lot de soumission à envoyer sont définies dans [CI-PARTAGE] « Métadonnées XDS d'un lot de soumission ».

Les autres règles de gestion de ce chapitre indiquent les restrictions spécifiques au contexte DMP.

*[RG_2220] Acquérir les identifiants uniques des documents et des lots de soumission*

**EX_2.1-1130**

Chaque document et lot de document(s) produit par un LPS doit être identifié par un identifiant universel (champ XDS `uniqueId` au format OID) :

- soit le `uniqueId` est généré à partir d'un UUID (sous la branche OID 2.25), dans ce cas cet OID doit être stocké dans le LPS pour les recherches / remplacements futurs via ce même LPS ;
- soit le `uniqueId` est généré à partir d'une racine propre à l'installation du LPS et d'un élément « variable » mais unique vis-à-vis de la racine de l'instance du LPS installée (par exemple horodatage, ou identifiant interne du document dans le LPS) ; il incombe au LPS de pouvoir retrouver ce uniqueId pour les recherches / remplacements futurs via ce même LPS (par exemple en stockant le uniqueId ainsi généré, ou la partie variable uniquement à condition de savoir reconstruire le uniqueId complet).

*[RG_2230] Acquérir les données concernant l'auteur du document et du lot de soumission*

**[DEROGATION SPECIFIQUE DMP PAR RAPPORT AU CI-SIS]**

Le CI-SIS impose que les métadonnées `authorPerson` et `legalAuthenticator` correspondent à des personnes physiques (ou un dispositif médical pour `authorPerson`). `authorPerson` est aussi accompagné d'une métadonnée `authorInstitution` qui permet de connaître la structure de soins auquel appartient l'auteur (ce n'est pas le cas pour `legalAuthenticator`).

Si le responsable du document fourni par la structure de soins n'est pas significatif pour le lecteur, **il est accepté pour des problématiques d'affichage et de manière dérogatoire** que certaines données soient alimentées avec le nom d'une personne morale.

- Le LPS d'une structure de soins peut alimenter la métadonnée `authorPerson` du lot de soumission avec les informations d'une personne morale(*) (au lieu d'un nom de personne physique).
- Le LPS d'une structure de soins peut alimenter la métadonnée `authorPerson` du document avec les informations d'une personne morale(*) (au lieu d'un nom de personne physique).
- Le LPS d'une structure de soins peut alimenter la métadonnée `legalAuthenticator` du document avec les informations d'une personne morale(*) (au lieu d'un nom de personne physique).

(*) NB : les informations de la personne morale doivent être liées à la structure de soins.

La personne morale indiquée dans les métadonnées peut être la structure de soins elle-même ou un sous-ensemble plus « parlant » pour le lecteur du document (service, unité fonctionnelle).

Ces dérogations sont provisoires.

Tout document produit après la fin de la dérogation devra fournir l'information d'une personne physique dans les métadonnées. La dérogation continuera à s'appliquer pour les documents ayant alimenté le DMP avant la fin de la dérogation.

Dans ce cadre dérogatoire , les données `authorPerson` et `legalAuthenticator`, doivent être renseignées comme suit :

| Composant | Donnée | Valeur |
|---|---|---|
| Composant 1 | Identifiant | identifiant interne de la **personne physique** impliquée (ex : 3 + FINESS/id interne) |
| Composant 2 | Nom | libellé de la **personne morale** |
| Composant 3 | Prénom | type de **personne morale** entre parenthèses : par exemple, valeur `(structure de soins)`, `(service)` ou `(unité fonctionnelle)` |
| Composant 9 | Autorité d'affectation | **OID de l'organisation** (comme pour une personne physique |
| Composant 10 | Type de nom | Valeur **`U`** (Undefined) |
| Composant 13 | Type d'identifiant | Valeur **`EI`** (comme pour une personne physique) |

Le comportement nominal décrit dans le CI-SIS reste bien évidemment privilégié par le SI DMP.

***Cas particulier***

***[CP1] Alimentation du DMP par CPE (TD2.2)***

Dans le cas d'une alimentation via CPE, les métadonnées doivent être renseignées de la manière suivante :

- `authorPerson`
  - Composant 1 : Identifiant du porteur de CPE, lu en carte (i.e. identifiant de la structure + « / » + identifiant interne de l'employé dans la structure)
  - Composant 2 : Nom du porteur de CPE, lu en carte
  - Composant 3 : Prénom du porteur de CPE, lu en carte
  - Autres composants : identique à l'authentification directe
- `authorInstitution`
  - Composant 1 : Nom de la structure
  - Composant 10 : Identifiant de la structure
  - Autres composants : identique à l'authentification directe
- `legalAuthenticator`
  - Composant 1 : Identifiant du porteur de CPE, lu en carte (i.e. identifiant de la structure + « / » + identifiant interne de l'employé dans la structure)
  - Composant 2 : Libellé de la **personne morale**
  - Composant 3 : Type de **personne morale** entre parenthèses : valeur `(structure de soins)`, `(service)` ou `(unité fonctionnelle)`
  - Composant 9 : OID de l'organisation (comme pour une personne physique)
  - Composant 10 : Valeur **`U`** (Undefined)
  - Composant 13 : Valeur **`EI`** (comme pour une personne physique)

*[CP2] Alimentation du DMP en authentification indirecte avec identifiant FINESS*

Pour l'alimentation de la donnée structure auteur du document soumis `authorInstitution` (sous-champ identifiant) :

- en mode EJ : FINESS de l'entité juridique,
- en mode EJ/EG : FINESS de l'entité géographique,
- en mode EG : FINESS de l'entité géographique.

**[FIN DE DEROGATION SPECIFIQUE DMP PAR RAPPORT AU CI-SIS]**

*[RG_2240] Acquérir l'organisation à l'intérieur de laquelle les documents et les lots de soumission ont été produits (`authorInstitution`)*

Cette métadonnée est à renseigner obligatoirement avec l'identifiant de la structure de soins (EF_DMP02_01).

NB : cette métadonnée peut être alimentée différemment au niveau des documents et au niveau des lots.

*[RG_2250] Acquérir les commentaires (`comments`)*

Le DMP limite les champs `comments` des documents et des lots de soumission à 1000 caractères.

NB : les champs `comments` peuvent être alimentés différemment au niveau des documents et au niveau des lots.

**Règles de gestion**

**Les métadonnées XDS d'un des documents**

*[RG_2310] Contrôler que l'ajout du document est effectué par l'auteur du document*

**EX_2.1-1140**

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

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

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

*[RG_2320] Déterminer le hachage du document (`hash`)*

Le champ `hash` des métadonnées XDS est optionnel pour le producteur du document. Toutefois, s'il est fourni, le système DMP en vérifiera le calcul.

Il s'agit du hash XDS tel que défini dans les spécifications IHE XDS (voir IHE ITI TF Vol3 au § 4.1.7 : "SHA1 / Document hash calculated with SHA1 algorithm / See RFC 3174 US Secure Hash Algorithm 1 (SHA1), September 2001. The encoding is the Lexical Representation of hexBinary ([0-9a-fA-F])".

Si le document n'est pas signé, le hash doit être calculé sur le "binaire brut" de la pièce jointe au message SOAP (part MTOM, dans le cadre du DMP il s'agit d'un CDA R2) et non sur le XML CDA R2 canonisé.

Si le document est signé, se référer au document [CI-PARTAGE].

***[RG_2330] Acquérir le cadre d'exercice de l'acte qui a engendré la création du document (`practiceSettingCode`)***

Le cadre d'exercice décrit le contexte d'utilisation du LPS et peut être paramétré de manière fixe dans le LPS ou déduit du contexte d'usage du LPS.

Il ne peut pas être déduit de la carte CPx.

Les valeurs possibles du cadre d'exercice sont celles du jeu de valeurs « `practiceSettingCode` » (voir [CI-ANX-PS-STRU] et [FI-JEUX-VALEURS]).

Exemples : Ambulatoire, Dépistage, Maintien à domicile, Soins à domicile, Hospitalisation à domicile, Etablissement de santé, Soins palliatifs, SAMU/SMUR

Le cadre d'exercice est renseigné dans :

- la métadonnée XDS « PracticeSettingCode »
- la donnée de l'en-tête des documents CDA « documentationOf/serviceEvent/performer/assignedEntity/representedOrganization/standardIndustryClassCode »

***[RG_2340] Acquérir l'identifiant principal du patient dans le système d'information du producteur du document (`sourcePatientId`)***

Le champ `sourcePatientId` doit a minima contenir l'identifiant du patient dans le système émetteur du document (identifiant patient interne dans l'instance du LPS, IPP pour un CH par exemple). Il est inutile d'y mettre l'INS puisque celui-ci est transmis dans le champ `patientId` (EF_DMP11_01). En l'absence d'identifiant local, mettre l'INS.

Dans le cadre du DMP, la cardinalité de cette donnée est restreinte à [1..1].

***[RG_2350] Acquérir les traits d'identité du patient (`sourcePatientInfo`)***

Cette métadonnée contient plusieurs champs PID. Seul le champ PID-5 « Patient Name » est requis et il est lui-même composé de plusieurs composants dont :

- le composant 1 (requis) : Nom du patient,
  - le nom du patient doit être alimenté avec le nom de naissance si celui-ci est renseigné (EF_DMP11_03),
  - sinon le nom du patient doit être alimenté avec le nom d'usage (EF_DMP11_02).
- le composant 7 (requis) : type de nom (`L` pour Nom de naissance, `D` pour Nom d'usage, `S` pour Pseudonyme et `U` pour Inconnu).

**Règles de gestion**

### Les métadonnées XDS du lot de soumission

***[RG_2410] Acquérir la date et heure d'envoi du lot de soumission (`submissionTime`) (EF_DMP32_01)***

La date doit être égale à la date du jour de la soumission du lot vers le DMP (ceci permet d'effectuer des recherches par date de soumission dans le DMP). Si la date ne correspond pas à la date du jour, une erreur du type `XDSRegistryMetadataError` sera renvoyée par le Système DMP.

Le document est créé par le professionnel (lors de la rédaction d'un compte rendu par exemple) puis le LPS crée, puis signe le lot avant de l'envoyer.

La chronologie des dates "techniques" est donc la suivante :

1. date de création du document (cohérence à assurer entre XDS et CDA),
2. date de signature du lot (= date `creationTime` du document DSG de signature du lot, aussi égale à celle dans la pièce jointe XAdES sous `<SigningTime>`),
3. date de soumission du lot (`submissionTime`).

Si le lot est signé juste avant l'envoi (dans le même processus d'export), nous vous recommandons de faire en sorte que les dates 2) et 3) soient égales (en créant une référence en début de processus d'export par exemple, affectée à ces 2 dates).

***[RG_2420] Acquérir le titre du lot de soumission (`title`)***

La taille de cette donnée n'étant pas fixée dans XDS.b, c'est celle d'un type "Name/LocalizedString.value" de la norme ebXML sous-jacente qui s'applique, à savoir 256 caractères.

***[RG_2430] Acquérir le type d'activité de l'évènement clinique ayant abouti à l'envoi du/des document(s) du lot de soumission (`contentTypeCode`)***

Le jeu de valeurs associé est fourni dans [FI-JEUX-VALEURS] (voir le fichier JDV_J59-ContentTypeCode-DMP).

Il n'y a pas d'équivalent à ce champ dans le CDA.

Pour alimenter cette donnée, il faut prendre la valeur la plus appropriée dans la nomenclature par rapport au contexte métier du LPS.

Le document [CI-ANX-PS-STRU] indique au § 4.1 comment renseigner cette métadonnée. En établissement, un rapprochement avec le service à l'origine du document de santé peut être envisagé (paramétrage au niveau service / unité fonctionnelle).

#### 3.4.1.1.4 Signer le ou les document(s) (non obligatoire)

**Vue générale**

Le LPS peut signer chaque document (cf. RG_2510).

**Règles de gestion**

***[RG_2510] Signer le document***

La signature des documents n'est pas obligatoire.

Les documents peuvent cependant être signés conformément aux mécanismes spécifiés dans [CI-PARTAGE] « Imputabilité du contenu des documents » (signature XAdES).

L'annexe A6-1 décrit les contraintes de signature XAdES à mettre en œuvre pour le DMP.

En authentification directe

Si le document est signé, le certificat utilisé pour signer le document doit correspondre au responsable du document tel que présenté dans l'en-tête CDA et la métadonnée XDS `legalAuthenticator`.

| REC_2.1-1150 |
| --- |
| La signature par carte CPx entraînant un temps de traitement supplémentaire variable en fonction de la configuration matérielle (lecteur CPS), le LPS peut implémenter la possibilité de signer ou non les documents (en plus des lots de soumission) en fonction d'un paramètre au niveau du LPS, au niveau de l'utilisateur, ou encore laisser l'utilisateur décider au cas par cas s'il souhaite signer tel ou tel document. |

En authentification indirecte

Si le document est signé, il peut être signé avec le certificat de personne morale de la structure de soins. Dans ce mode d'authentification, il n'y a pas de correspondance entre la métadonnée XDS `legalAuthenticator` et le certificat.

### 3.4.1.1.5 Constituer et signer le lot de soumission

**Vue générale**

Le LPS :

- lie les documents dans un même lot de soumission (cf. RG_2610),
- signe le lot de soumission (cf. RG_2620),
- alimente les métadonnées du document portant la signature du lot de soumission (cf.RG_2630).

**Règles de gestion**

*[RG_2610] Lier les documents dans un même lot de soumission (EF_DMP32)*

Le LPS constitue un lot de soumission contenant un ou plusieurs documents.

**REC_2.1-1160**

Il est recommandé que le LPS permette au professionnel de sélectionner plusieurs documents à envoyer dans le DMP du patient, en indiquant pour chacun d'eux les paramètres de masquage aux professionnels et de visibilité au patient / représentants légaux (voir ci-dessous) et de constituer ainsi un lot de soumission avec plusieurs documents de santé d'un même patient en rapport avec un événement de soins.

Cela permettra notamment aux autres médecins de les identifier et d'y accéder beaucoup plus simplement. A titre d'exemple, lorsqu'une fiche RCP, un CR-Opératoire et un CR-ACP sont liés par le même lot de soumission, en accédant à la fiche RCP, le médecin peut voir qu'il existe 2 « documents liés ».

Un même document peut être référencé dans plusieurs lots de soumission.

Pour lier les documents entre eux dans un même lot de soumission, deux méthodes sont possibles :

- Les envoyer dans le DMP en même temps dans le même lot de soumission. Par exemple, il est recommandé d'envoyer dans le DMP du patient, dans le même lot de soumission, la fiche RCP, le CR-Opératoire, le CR-ACP et tout autre document que le médecin peut juger utile à la coordination des soins.
- Envoyer un nouveau document (par exemple la fiche RCP) et la référence des autres documents déjà déposés dans le DMP du patient dans le même lot de soumission. Cela implique que le LPS doit d'abord récupérer la référence des documents présents dans le DMP du patient à lier au nouveau document. Cf. DMP_3.1 au chapitre 3.5.1.

*Cas particuliers*

*[CP1] Envoyer des documents antérieurs à la date de création du DMP du patient*

Il est possible d'alimenter le DMP d'un patient avec des documents utiles à la coordination des soins et antérieurs à la date de création du DMP.

*[CP2] Premier envoi d'un document dans le DMP d'un patient*

**REC_2.1-1180**

Afin de favoriser le déploiement du DMP, à l'occasion du premier envoi d'un document vers le DMP pour un patient donné, il est recommandé que le LPS puisse sélectionner les documents du dossier patient non présents dans le DMP pour proposer au professionnel de les envoyer dans le DMP.

**EX_2.1-1190**

Le LPS doit implémenter une solution permettant à l'utilisateur d'identifier visuellement si des documents utiles à la coordination des soins peuvent être envoyés au DMP (message, icônes dans une liste de documents, etc.).

*[RG_2620] Signer le lot de soumission*

**EX_2.1-1170**

Afin de garantir l'imputabilité de la transmission des documents au sein du DMP, les lots de documents doivent être signés conformément aux mécanismes spécifiés dans [CI-PARTAGE] « Imputabilité du dépôt des documents » (signature XAdES).

*Cas particuliers*

*[CP1] Alimentation du DMP en authentification indirecte avec identifiant FINESS*

La signature utilise le certificat XaDES suivant :

- en mode EJ : certificat XaDES de l'entité juridique,
- en mode EJ/EG : certificat XaDES de l'entité juridique,
- en mode EG : certificat XaDES de l'entité géographique.

*[RG_2630] Alimenter les métadonnées du document portant la signature du lot de soumission*

Le document comportant la signature du lot de soumission est un document XML auquel sont associées des métadonnées permettant son indexation dans le système DMP.

Le document [CI-PARTAGE] « Imputabilité du dépôt des documents » précise comment renseigner ces métadonnées et en particulier la donnée `confidentialityCode` : 3 occurrences de la métadonnée `confidentialityCode` sont à alimenter respectivement avec les valeurs `N`, `MASQUE_PS`[8], `INVISIBLE_PATIENT`.

Note : la valeur `INVISIBLE_REPRESENTANTS_LEGAUX` n'est pas utilisée pour ce type de document.

*Cas particuliers*

*[CP1] Alimentation du DMP en authentification indirecte avec identifiant FINESS*

Pour l'alimentation de la donnée structure auteur du lot de soumission `authorInstitution` (sous-champ identifiant) :

- en mode EJ : FINESS de l'entité juridique,
- en mode EJ/EG : FINESS de l'entité géographique,
- en mode EG : FINESS de l'entité géographique.

Pour l'alimentation de la donnée structure auteur du document de signature du lot de soumission `authorInstitution` (sous-champ identifiant)

- en mode EJ : FINESS de l'entité juridique,
- en mode EJ/EG : FINESS de l'entité juridique,
- en mode EG : FINESS de l'entité géographique.

[8] Le nom technique n'évolue pas. Il conserve le terme « PS ».

#### 3.4.1.1.6 Soumettre le lot de documents au système DMP

**Vue générale**

Le LPS :

- détermine les identifiants des entités ebXML de la requête (cf. RG_2710),
- soumet le lot de documents au système DMP (cf. RG_2720).

**Règles de gestion**

*[RG_2710] Déterminer les identifiants des entités ebXML de la requête*

| EX_2.1-1200 |
| --- |
| Générer des identifiants internes à la requête dont le format n'est pas « uuid ». Par exemple, en utilisant des "compteurs" internes : document01, submissionSet01, cla1, cla2, assoc1 assoc2, etc. (exemples d'identifiants nommés avec un préfixe représentatif du type d'entité ebXML qu'ils identifient : permet de faciliter le débogage en phase de développement).<br>Ces identifiants internes seront régénérés en « uuid » par le système DMP lors du stockage de l'entité (lot ou document). |

Il est conseillé de ne pas stocker les identifiants internes au système DMP (entryUUID) dans le LPS. En cas de modification des métadonnées du document (via DMP_3.3), l'entryUUID stocké dans le système DMP change. Un entryUUID stocké auparavant comme référence au sein du LPS ne serait plus valable en cas de nouvelle modification des métadonnées du document (via DMP_3.3).

*[RG_2720] Soumettre le lot de documents au système DMP*

Le LPS appelle :

- la transaction TD2.1 pour les professionnels hors authentification par CPE,
- la transaction TD2.2 pour les professionnels en authentification par CPE.

Cf. §3.4.1.3 pour la description de ces transactions.

### 3.4.1.2 DMP_2.1b/2.2b : remplacer un document existant dans le DMP d'un patient

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

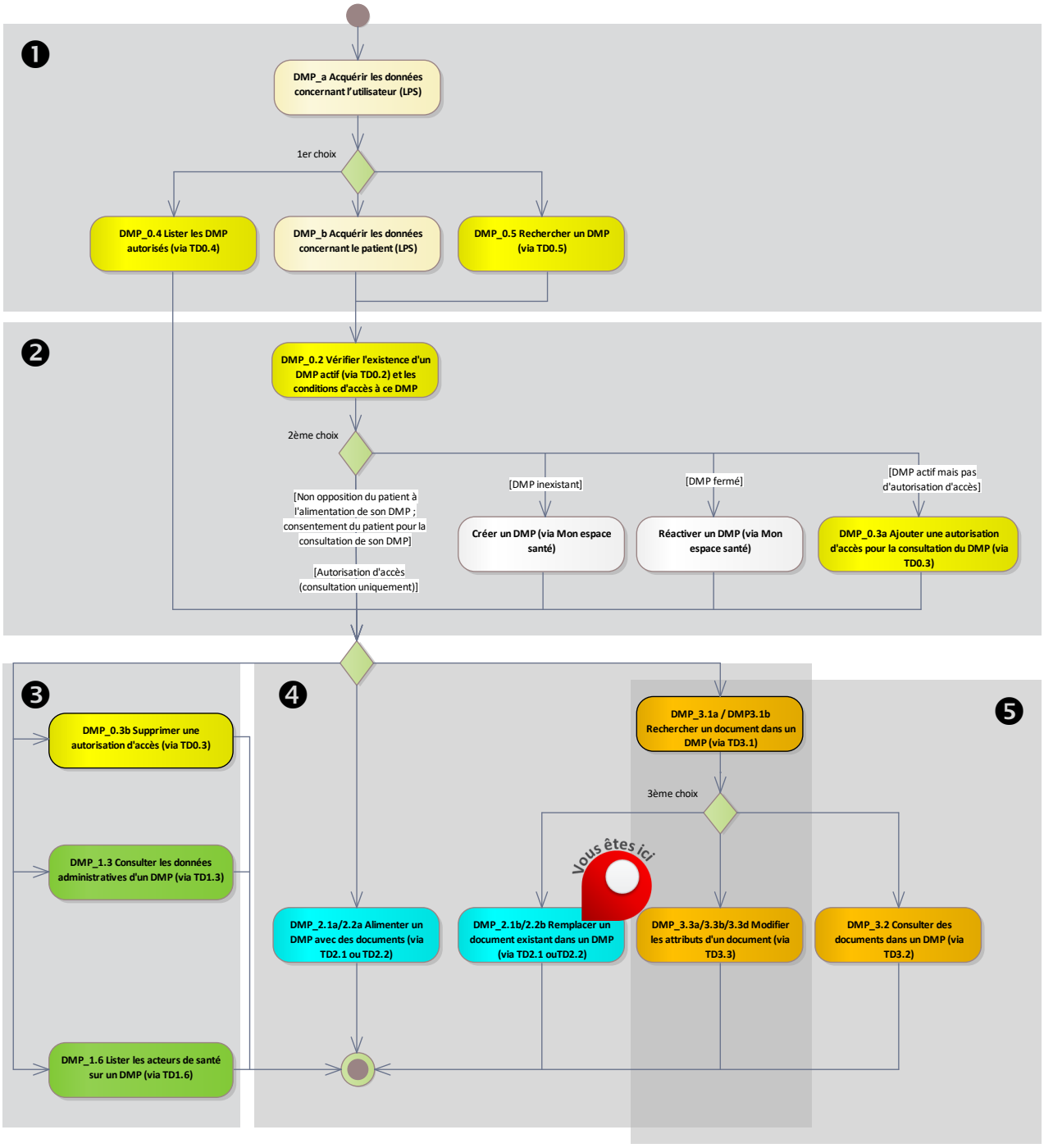



**Figure 21 : localisation de la fonctionnalité DMP_2.1b/2.2b dans le processus regroupant les deux profils Alimentation et Consultation**

NB : dans ce chapitre, les identifiants uniques des documents sont gérés à deux niveaux.

- Les identifiants uniques gérés par le LPS correspondent à la donnée CDA `uniqueId` et à la métadonnée XDS uniqueId (EF_DMP31_01).
- Les identifiants uniques gérés par le système DMP correspondent à la métadonnée XDS `entryUUID` (EF_DMP31_02).

## Vue générale

**EX_2.1-1210**

Le LPS doit proposer au professionnel la fonctionnalité de remplacement d'un document qui doit être conforme aux principes décrits ci-après.

***Description***

Cette fonctionnalité permet d'alimenter le DMP d'un patient avec une nouvelle version d'un document.

Soient X le document initial (`uniqueId` par exemple 1.2.3.X) et Y la nouvelle version du document (`uniqueId` par exemple 1.2.3.Y).

Pour remplacer un document initial X dans le DMP du patient par une nouvelle version Y, la cinématique est la suivante.

- L'utilisateur modifie le document X dans le LPS (corps et/ou métadonnées) pour créer le document Y.
- Le LPS a récupéré les identifiants du document X (`entryUUID` et `uniqueId`, cf. DMP_3.1).
- Le LPS construit le document Y au format CDA et alimente les métadonnées XDS.
  - CDA : `relatedDocument` = uniqueId du document X.
  - XDS : association `RPLC` sur l'`entryUUID` du document X.
- Le LPS constitue un lot de soumission XDS et réalise la signature XAdES du lot.
- Le LPS envoie la requête au système DMP.

***Entrées et prérequis***

L'INS du patient (EF_DMP11_01).

Le statut « actif » du DMP du patient (EF_DMP12_01).

Les identifiants entryUUID et uniqueId du document à remplacer obtenus par la fonctionnalité DMP_3.1 (EF_DMP31_01 et EF_DMP31_02).

L'identifiant de la nouvelle version du document (`uniqueId` par exemple 1.2.3.Y) (EF_DMP31_01).

***Sorties***

Le document X est remplacé par le document Y dans le DMP du patient.

## Préambule

D'un point de vue technique, le « remplacement de document » utilise la même transaction que pour une « 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 système DMP (repository XDS) pour remplacer dans le registre (registry XDS) l'ancienne fiche du document par la nouvelle.

Le système DMP gère le cycle de vie des documents comme suit.

- Le nouveau document est au statut « courant » (= dans la nouvelle fiche, la métadonnée `availabilityStatus` prend la valeur `Approved`).
- Le document remplacé passe au statut « obsolète » (= dans l'ancienne fiche, la métadonnée `availabilityStatus` prend la valeur `Deprecated`).
- Ces deux fiches sont liées par une association de type `RPLC` (replace).

**Règles de gestion**

***[RG_2910] Remplacer un document existant dans le DMP d'un patient***

Par rapport à une alimentation standard décrite dans le chapitre 3.4.1.1, un remplacement de document nécessite les éléments suivants.

- Dans les métadonnées XDS : une association de type `RPLC` entre le document remplaçant et le document remplacé (via le `entryUUID` du document remplacé). Les spécifications se trouvent dans [IHE-TF3] (chapitre Document Relationships).
- Dans les données CDA du document remplaçant un élément `relatedDocument/parentDocument/id` référençant le `uniqueId` du document remplacé. Voir [CI-STRU-ENTETE] relatedDocument.

### 3.4.1.3 TD2.1 et TD2.2 : alimentation en documents du DMP d'un patient

Les transactions TD2.1 et TD2.2 fonctionnent de la même manière mais avec des modes d'authentification différents :

- TD2.1 est utilisée en authentification par carte CPS/CPF ou en authentification indirecte.
- TD2.2 est utilisée en authentification par carte CPE.

Le profil IHE XDS.b utilisé pour la l'alimentation du DMP est présenté dans le chapitre 5.1.2.

La transaction est décrite dans [CI-PARTAGE] (IHE ITI-41 : Provide and Register Document Set-b).

**EX_2.1-1260**

L'alimentation d'un document vers le DMP exige l'usage du MTOM avec optimisation XOP dans la requête envoyée (voir profil IHE XDS (ITI volume 2 / ITI-41 ProvideAndRegisterDocumentSet-b au § 3.41.4.1.2 Message Semantics) et [CI-TR-CLI-LRD] § 3.2.5).

La transaction doit respecter les exigences concernant l'accès sécurisé au système DMP. Cf. TD0.1 au §5.3.

**Données en sortie**

***En cas de succès de la transaction :***

Le système DMP retourne un code `status` égal à `urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success`, conformément au profil XDS.b.

***En cas d'erreur de la transaction :***

Le système DMP retourne un code `status` égal à `urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure`, conformément au profil XDS.b, ainsi qu'un code d'erreur et éventuellement un message de détail. Le retour d'erreur est détaillé dans [IHE-TF3].

L'annexe A7-1 décrit les codes d'erreur utilisés dans le cadre du DMP.

***Détection de virus***

En cas de document contaminé par un virus, le service de gestion des documents retourne une erreur de type `DMPVirusFound`. Au sein de l'erreur, un message à caractère informatif indiquera quel est l'identifiant unique (uniqueId) du document infecté. Aucun document n'est alors enregistré dans le DMP.

***Vérification des signatures***

La signature du lot de soumission et/ou celle des documents sont vérifiées lors de la dépose. En cas d'erreur, une erreur `DMPInvalidSignature` est alors renvoyée. Dans ce cas, aucun document n'est alors enregistré dans le DMP.

## 3.5 DMP_3.x : consultation du DMP d'un patient

Ce chapitre décrit trois fonctionnalités.

- La première fonctionnalité (DMP_3.1) se décline en deux cas d'usage.
  - Pour les LPS donnant accès à la consultation des documents (DMP_3.2), cette première fonctionnalité permet de lister les documents contenus dans le DMP d'un patient (DMP_3.1a) afin de pouvoir ensuite consulter un document (DMP_3.2), modifier les attributs d'un document (DMP_3.3) ou remplacer un document (DMP_2.1b/2.2b). A ce jour, ce cas s'applique pour le profil « Consultation »
    - en authentification directe par CPS/CPF,
    - en mode AIR.
  - Pour les LPS ne donnant pas accès à la consultation des documents (DMP_3.2), le système DMP ne permet pas de récupérer les métadonnées des documents. Cette première fonctionnalité permet de rechercher l'identifiant technique d'un document (DMP_3.1b) afin de pouvoir ensuite supprimer (DMP_3.3c), archiver (DMP_3.3d) ou remplacer un document dans le DMP du patient (DMP_2.1b/2.2b). A ce jour, ce cas s'applique :
    - en authentification indirecte (hors mode AIR),
    - en authentification directe par CPE,
    - en authentification directe par CPS/CPF sans le profil « Consultation ».
- La deuxième permet de consulter un de ces documents (DMP_3.2).
- La troisième permet d'en modifier les attributs (DMP_3.3) :
  - masquer / démasquer un document aux professionnels,
  - rendre un document visible au patient,
  - rendre un document visible aux représentants légaux du patient,
  - archiver / désarchiver un document,
  - supprimer un document.

Pour consulter un document (DMP_3.2), il convient d'abord d'utiliser la fonctionnalité DMP_3.1a pour rechercher une liste de documents à partir de critères de recherche (seules les métadonnées de ces documents sont alors récupérées) puis d'utiliser ensuite la fonctionnalité DMP_3.2 pour récupérer les documents à consulter.

Pour modifier les attributs d'un document, il convient d'abord d'utiliser la fonctionnalité DMP_3.1 pour récupérer les métadonnées de ce document puis d'utiliser ensuite la fonctionnalité DMP_3.3 pour en modifier les attributs.

La fonctionnalité DMP_3.1 est également utilisée dans le profil « Alimentation » pour le remplacement d'un document par une nouvelle version de ce document. Cf. la fonctionnalité DMP_2.1b/2.2b dans le chapitre 3.4.1.2.

### 3.5.1 DMP_3.1 : Rechercher un document dans le DMP d'un patient (via TD3.1)

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

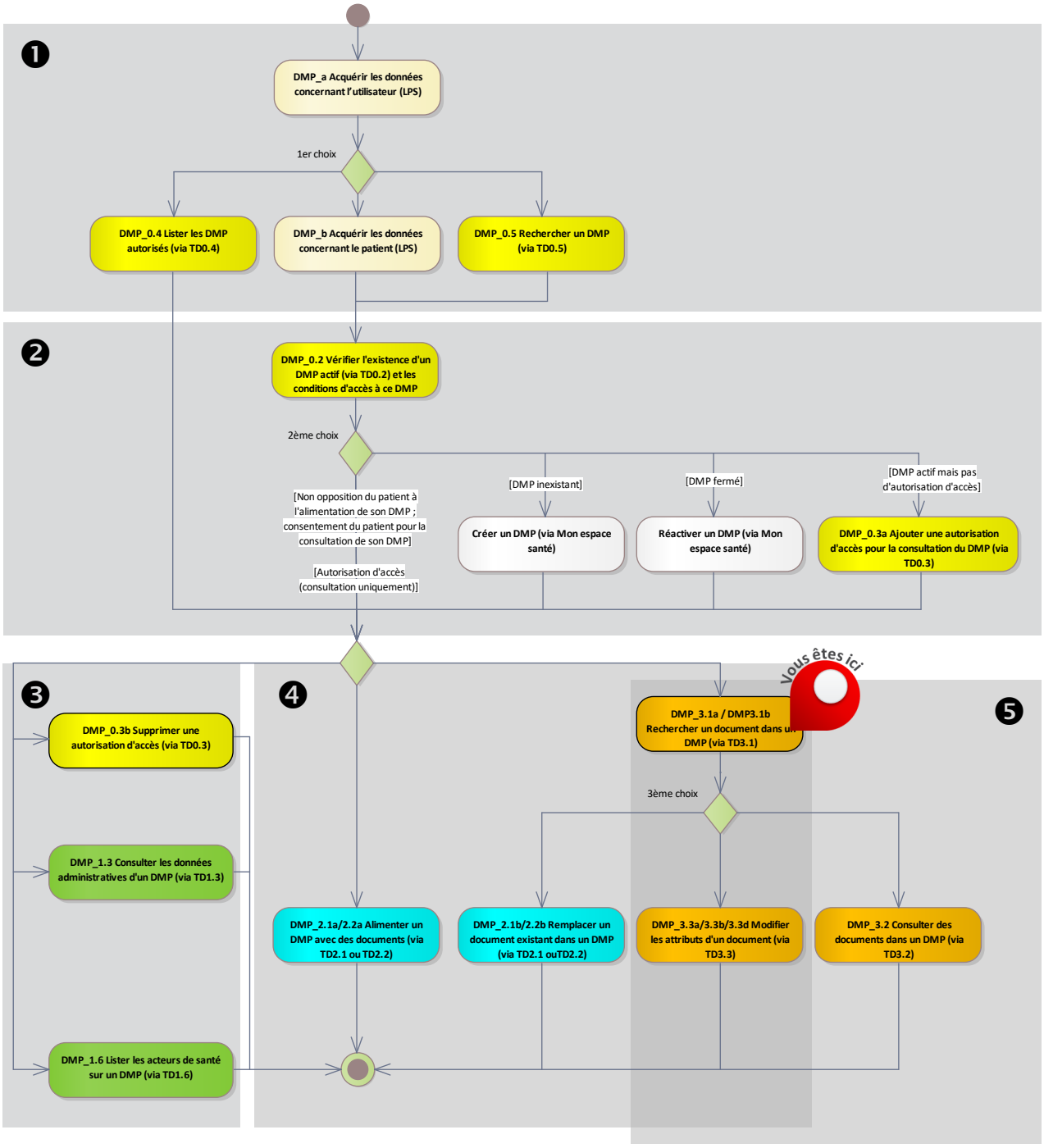



**Figure 22 : localisation de la fonctionnalité DMP_3.1 dans le processus regroupant les deux profils Alimentation et Consultation**

Les deux cas d'usage (DMP_3.1a et DMP_3.1b) sont présentés dans le chapitre 3.5.

#### 3.5.1.1 DMP_3.1a : sélectionner un document dans la liste des documents du DMP d'un patient (via TD3.1)

**Vue générale**

***Description***

Cette fonctionnalité permet de lister les documents du DMP d'un patient (cf. RG_3010) en indiquant des critères de recherche.

La cinématique générale est la suivante.

- L'utilisateur saisit un ou plusieurs critères de recherche dans le LPS. Cf. RG_3020.
- Le LPS appelle la transaction TD3.1. Cf. RG_3030.
- Le système DMP retourne les résultats au LPS.
- Le LPS affiche les résultats. Cf. RG_3040.
- L'utilisateur sélectionne un ou plusieurs document(s) et le LPS acquiert l'identifiant unique des document(s) sélectionnés. Cf. RG_3050.
- Le LPS détermine les actions possibles sur les documents sélectionnés. Cf. RG_3060.
  - consulter un document (DMP_3.2),
  - modifier les attributs d'un document (DMP_3.3),
  - ou remplacer un document (DMP_2.1b/2.2b).

***Entrées et prérequis***

L'INS du patient (EF_DMP11_01).

Le statut « actif » du DMP du patient (EF_DMP12_01).

L'autorisation d'accès au DMP du patient (EF_DMP04_01) au statut « valide ».

***Sorties***

La liste des documents consultables par l'utilisateur.

**Règles de gestion**

***[RG_3010] Indiquer l'INS du patient (EF_DMP11_01)***

Le LPS peut indiquer l'INS du patient dans le paramètre INS (`patientId`) de la requête. Sinon, l'INS du patient du VIHF sera utilisé.

***[RG_3020] Acquérir les critères de recherche***

**EX_3.1-1011**

Le LPS doit permettre à l'utilisateur de rechercher des documents sur le type du document (métadonnée `typeCode`).

**EX_3.1-1030**

La recherche de document doit proposer systématiquement à l'utilisateur la liste des documents actifs du DMP (champ XDS `availabilityStatus = « urn:oasis:names:tc:ebxml-regrep:StatusType:Approved »`).

Par ailleurs, la recherche de document doit proposer au professionnel de pouvoir choisir les critères suivants :

- avec ou sans les documents archivés (champ XDS `availabilityStatus = « urn:asip:ci-sis:2010:StatusType:Archived »`), l'activation pouvant se faire via une case à cocher « afficher les documents archivés » ;
- avec ou sans les documents masqués – fonctionnalité réservée au médecin traitant DMP – (champs XDS `confidentialityCode = « MASQUE_PS »`[9] de la nomenclature d'OID 1.2.250.1.213.1.1.4.13) ;
- avec ou sans les documents non visibles au patient (champs XDS `confidentialityCode = « INVISIBLE_PATIENT »` de la nomenclature d'OID 1.2.250.1.213.1.1.4.13) ;
- avec ou sans les documents non visibles aux représentants légaux (champs XDS `confidentialityCode = « INVISIBLE_REPRESENTANTS_LEGAUX »` de la nomenclature d'OID 1.2.250.1.213.1.1.4.13) ;
- avec ou sans les documents obsolètes (champ XDS `availabilityStatus = « urn:oasis:names:tc:ebxml-regrep:StatusType:Deprecated »`), l'activation pouvant se faire via une case à cocher « afficher les anciennes versions des documents (obsolètes / remplacés) ».

Le LPS est libre de mettre en œuvre d'autres critères de recherche.

***Cas particulier***

***[CP1] Recherche de document dans un intervalle temporel par rapport à une date de soumission***

**EX_3.1-1012**

Le LPS doit permettre à l'utilisateur de rechercher des documents sur la date de soumission du document dans le DMP. Cf. « Recherche de document soumis dans un intervalle temporel par rapport à une date de soumission » §3.5.1.3.

**EX_3.1-1020**

Le LPS doit permettre à l'utilisateur de rechercher des documents depuis la dernière connexion d'un professionnel au DMP du patient ou depuis la précédente recherche de documents de ce professionnel sur le DMP du patient. Il doit donc stocker en interne la date de dernière connexion du professionnel au DMP (ou date de dernière recherche des nouveaux documents), puis faire une requête sur les lots de soumission en passant cette date à la requête `FindSubmissionSets` dans le paramètre `$XDSSubmissionSetSubmissionTimeFrom` et combiner une ou d'autres fonctions pour récupérer les documents associés (voir « Recherche de document soumis dans un intervalle temporel par rapport à une date de soumission » au §3.5.1.3).

***[RG_3030] Rechercher les documents***

Le LPS appelle la transaction TD3.1.

Cf. §3.5.1.3 pour la description de cette transaction.

[9] Le nom technique n'évolue pas. Il conserve le terme « PS ».

*[RG_3040] Afficher la liste des documents*

**EX_3.1-1040**

Certains documents peuvent être produits par le patient, via son accès Web. Lors de la consultation du DMP, ces documents doivent être distingués des documents produits par des professionnels (code couleur différent, pictogramme…). Le LPS devra se baser sur le `classCode` XDS `90` (Expression du titulaire) et les `typeCode` commençant par « DOCPAT » pour distinguer les documents de « type patient ».

**EX_3.1-1050**

Le LPS ne doit pas refuser un type de document qu'il ne connaît pas :

- soit par un `typeCode / classCode` XDS non connu (type de document) ;
- soit par un `formatCode` XDS non connu (nouveau volet de contenu structuré par exemple).

Le LPS doit pouvoir afficher le document à l'utilisateur, par exemple à l'aide d'une feuille de style XSL standard - une feuille de style minimale, non normative, est fournie dans le CI-SIS (Outil de vérification des documents CDA, téléchargeable sur le site de l'ANS).

**EX_3.1-1055**

Du fait du caractère évolutif de l'identifiant du patient (métadonnée patientId dans les documents), le LPS ne doit pas filtrer les documents restitués par le système DMP sur ce critère.

Par exemple, le LPS doit afficher tous les documents restitués par le système DMP quelle que soit la valeur de métadonnée patientId (INS-C ou INS).

**EX_3.1-1080**

Lors de l'affichage des résultats à la suite de recherches de document, le LPS doit indiquer au professionnel l'état du document qui peut être :

- « **masqué aux professionnels** »,
- « **non visible par le patient** »,
- « **non visible par les représentants légaux** »,
- « **archivé** »,
- « **ancienne version obsolète** ».

Il n'y a pas de valeur spécifique pour un document « courant » (on ne précise pas d'état particulier).

**REC_3.1-1060**

Il est recommandé d'utiliser les termes indiqués ci-dessus en gras. L'éditeur peut aussi utiliser une icône représentant chacun de ces états.

Point d'attention sur les champs date/heure :

Les champs de type date/heure sont codés dans une zone de temps différente entre les métadonnées XDS et le CDA R2. Les champs date/heure XDS sont codés en UTC et ceux du CDA correspondant en heure locale incluant le décalage par rapport à UTC.

**EX_3.1-1070**

Il est demandé d'afficher la date du document en heure locale :

- dans le cas d'une recherche de documents (TD3.1 - IHE ITI-18 Registry Stored Query XDS) : en se basant sur la métadonnée XDS, avec conversion dans la date locale avant l'affichage à l'utilisateur.

***[RG_3050] Acquérir les métadonnées***

Condition : l'utilisateur veut consulter un ou plusieurs document(s) ou modifier les attributs d'un ou plusieurs document(s) ou remplacer un ou plusieurs document(s).

Le tableau ci-dessous indique les métadonnées à acquérir en fonction des actions à effectuer.

| | | UniqueId (EF_DMP31_01) | EntryUUID (EF_DMP31_02) | LogicalID (EF_DMP31_05) | Autres métadonnées |
|---|---|---|---|---|---|
| *DMP_3.2* | Consulter un document | X | - | - | - |
| *DMP_2.1b/2.2b* | Remplacer un document | X | X | - | (*) |
| *DMP_3.3a* | Masquer / démasquer un document aux professionnels | - | - | X | X |
| *DMP_3.3b* | Rendre un document visible au patient ou à ses représentants légaux | - | - | X | X |
| *DMP_3.3c* | Supprimer un document | - | X | - | - |
| *DMP_3.3d* | Archiver / désarchiver un document | - | X | - | - |

(*) en fonction du mode opératoire au niveau du LPS.

**Tableau 19 : métadonnées à acquérir en fonction des actions à effectuer**

***[RG_3060] Déterminer les actions possibles sur les documents sélectionnés par l'utilisateur***

Les actions possibles sur chaque document sont les suivantes :

- consulter ce document (DMP_3.2),
- modifier les attributs de ce document (DMP_3.3),
- remplacer ce document par une nouvelle version de ce document (DMP_2.1b/2.2b) (uniquement si le LPS intègre le profil Alimentation).

### 3.5.1.2 DMP_3.1b : rechercher l'identifiant technique d'un document (via TD3.1)

#### Vue générale

***Description***

Cette fonctionnalité permet, aux LPS qui n'implémentent pas DMP_3.1a, de rechercher l'identifiant technique d'un document (dans le système DMP) à partir de l'identifiant local au LPS de ce document.

Le LPS peut ensuite supprimer (DMP_3.3c), archiver (DMP_3.3d) ou remplacer un document dans le DMP du patient (DMP_2.1b/2.2b).

Cette fonctionnalité est mise en œuvre dans les LPS ne donnant pas accès à la consultation des documents (DMP_3.2). A ce jour, ce cas correspond aux situations suivantes :

- en authentification indirecte (hors mode AIR),
- en authentification directe par CPE,
- en authentification directe sans le profil « Consultation ».

La cinématique est décrite dans la règle RG_3110.

***Entrées et prérequis***

L'INS du patient (EF_DMP11_01).

Le DMP du patient est au statut actif (EF_DMP12_01).

L'autorisation d'accès au DMP du patient (EF_DMP04_01) au statut « valide » (sauf si le LPS implémente le profil Alimentation).

(Les données sont acquises pendant le déroulement de la fonctionnalité.)

***Sorties***

L'identifiant unique du document dans le système DMP (`entryUUID`) (EF_DMP31_02).

#### Règles de gestion

***[RG_3110] Déroulement du processus***

L'exigence ci-dessous illustre le cas de la suppression d'un document. D'autres actions sont décrites dans les cas particuliers.

**EX_3.1-1060**

**Recherche d'un document en authentification indirecte ou par CPE** (qui ne donne pas accès à la consultation) **ou en authentification directe sans l'accès à la consultation**.

Une disposition spécifique permet de rechercher l'`entryUUID` d'un document avec la TD3.1 pour pouvoir ensuite faire une action sur ce document.

1. L'utilisateur sélectionne en local dans le LPS le document (cf. RG_3120),
2. Le LPS récupère la référence `entryUUID` du document dans la Registry XDS du système DMP, à partir du `uniqueId` du document (cf. RG_3130),
3. Le LPS envoie une requête XDS de mise à jour de métadonnée TD3.3c (cf. RG_3140).

Limitation : un document qui aurait été remplacé ne peut pas être supprimé dans ce contexte. En effet, la fonction `GetDocuments` en `ObjectRef` ne retourne que les `entryUUID` de documents courants ou archivés (`availabilityStatus = Approved ou Archived`).

***Cas particulier***

***[CP1] Remplacement d'un document dans le DMP d'un patient***

Le même processus s'applique sauf la dernière étape qui est remplacée par la fonctionnalité DMP_2.1b/2.2b (cf. RG_3140).

***[CP2] Archiver un document dans le DMP d'un patient***

Le même processus s'applique sauf la dernière étape qui est remplacée par la fonctionnalité DMP_3.3d (cf. RG_3140).

***[RG_3120] Acquérir l'identifiant unique du document dans le LPS (`uniqueId`) (EF_DMP31_01)***

L'utilisateur sélectionne le document concerné dans le LPS.

Le LPS acquiert l'identifiant unique de ce document (`uniqueId`).

***[RG_3130] Acquérir l'identifiant unique du document dans le système DMP (`entryUUID`) (EF_DMP31_02)***

Le LPS appelle la transaction TD3.1, en utilisant la requête stockée `GetDocuments` en mode `ObjectRef` avec l'`uniqueId` en entrée.

Cf. §3.5.1.3 pour la description de la transaction TD3.1.

***[RG_3140] Déterminer les actions possibles sur le document***

Les actions possibles sont les suivantes :

- supprimer ce document (DMP_3.3c),
- archiver ce document (DMP_3.3d),
- remplacer ce document dans le DMP du patient par une nouvelle version de ce document (DMP_2.1b/2.2b).

### 3.5.1.3 TD3.1 : recherche de documents dans le DMP d'un patient

Le profil IHE XDS.b utilisé pour la consultation est présenté dans le chapitre 5.1.2.

La transaction est décrite dans [CI-PARTAGE] (IHE ITI-18 : Stored Query).

Les requêtes « Stored Query » disponibles via le web-service de la Registry du système DMP, ainsi que les critères de recherche de chaque requête, sont définis dans [IHE-TF2A] § 3.18.

La transaction doit respecter les exigences concernant l'accès sécurisé au système DMP. Cf. TD0.1 au §5.3.

Un fonctionnement spécifique concernant la recherche des données de remboursement est décrit dans le chapitre 6.2.

**Données en entrée**

Les données en entrée dépendent des critères de recherche disponibles pour la requête appelée (voir [IHE-TF2A] § 3.18).

A titre d'information, le tableau ci-après liste les Stored Query XDS mises en œuvre par le système DMP. NB : ce tableau de synthèse se focalise sur les paramètres d'entrée « requis » de type référence `uniqueId` (EF_DMP31_01) ou `entryUUID` (EF_DMP31_02), mais d'autres paramètres peuvent éventuellement être passés à chaque query (voir documentation IHE). Ces Stored Query XDS retournent les métadonnées d'un document (et non le document lui-même).

| Nom du query | Fonctionnalité |
|---|---|
| `FindDocuments` | Recherche multicritère de documents. |
| `FindSubmissionSets` | Recherche multicritère de lots de soumission. |

| | |
|---|---|
| `GetAll` | Récupération de tout le contenu XDS d'un DMP (documents, lots et associations).<br>Note : peu recommandé car peut être lent sur des DMP comportant beaucoup de documents. Peut servir pour la mise au point du LPS (développement). |
| `GetDocuments` | Récupération d'un ou plusieurs documents à partir de leurs `uniqueId` ou `entryUUID` en entrée (paramètres exclusifs). |
| `GetAssociations` | Récupération des associations liées à un ou plusieurs autres objets XDS (documents, lots) dont l'`entryUUID` est passé en entrée. |
| `GetDocumentsAndAssociations` | Récupération d'un ou plusieurs documents avec toutes leurs associations qui y sont liées, à partir de leurs `uniqueId` ou `entryUUID` en entrée (paramètres exclusifs) |
| `GetSubmissionSets` | Récupération d'un ou plusieurs lots de soumission à partir du `entryUUID` d'un ou plusieurs document(s) contenu(s) dans le lot.<br>En d'autre terme, récupération des lots dans lequel est référencé le document. |
| `GetSubmissionSetAndContents` | Récupération d'un lot de soumission avec tout son contenu (documents, associations), à partir de son `uniqueId` ou `entryUUID` en entrée (paramètres exclusifs) |
| `GetRelatedDocuments` | Retourne les documents qui sont liés par des associations à un document précis (seule l'association XDS de remplacement RPLC est autorisée dans le DMP), à partir du `uniqueId` ou `entryUUID` du document en entrée (paramètres exclusifs) |
| `FindDocumentByReferenceId` | Recherche multicritère de documents (idem FindDocuments), avec en plus un ou plusieurs « identifiants de référence » (`$XDSDocumentEntryReferenceIdList`) comme critère de recherche requis. |

**Tableau 20 : Stored Query XDS mises en œuvre par le système DMP**

***Recherche de document « basique »***

La requête adaptée à la recherche de document est `FindDocuments`.

***Recherche de document dans un intervalle temporel par rapport à une date d'acte***

La requête `FindDocuments` peut être utilisée avec les critères suivants (a minima) :

- date de début d'acte la plus ancienne (`$XDSDocumentEntryServiceStartTimeFrom`),
- date de fin d'acte la plus récente (`$XDSDocumentEntryServiceStopTimeTo`).

Deux critères supplémentaires sont possibles :

- date de début d'acte la plus récente (`$XDSDocumentEntryServiceStartTimeTo`),
- date de fin d'acte la plus ancienne (`$XDSDocumentEntryServiceStopTimeFrom`).

#### *Recherche de document soumis dans un intervalle temporel par rapport à une date de soumission*

Dans XDS, il n'existe pas de requête « Stored Query » pour rechercher les documents soumis au Repository du système DMP dans un intervalle temporel donné.

Plusieurs approches permettent néanmoins de le faire, en combinant plusieurs requêtes.

1. Combinaison de `FindSubmissionSet` et de `GetSubmissionSetAndContents` (soit N+1 appels de fonctions, en fonction du nombre N de lots retournés).
   a. Utilisation de la requête `FindSubmissionSets` pour rechercher les lots de soumission en spécifiant un intervalle temporel de soumission (date de soumission dans le DMP, critères `$XDSSubmissionSetSubmissionTimeFrom` et `$XDSSubmissionSetSubmissionTimeTo`) : retourne les lots de soumission.
   b. Pour chaque lot retourné, faire un GetSubmissionSetAndContents qui retourne le lot et ses documents.
2. Combinaison de `FindSubmissionSet`, de `GetAssociations` et de `GetDocuments` (soit 3 appels de fonctions).
   a. Utilisation de la requête `FindSubmissionSets` pour rechercher les lots de soumission en spécifiant un intervalle temporel de soumission (date de soumission dans le DMP, critère `$XDSSubmissionSetSubmissionTimeFrom` et `$XDSSubmissionSetSubmissionTimeTo`) : retourne les lots de soumission.
   b. Récupérer l'ensemble des `entryUUID` des lots retournés.
   c. Passer cette liste d'`entryUUID` à la fonction `GetAssociations`.
   d. Filtrer les retours sur les Associations de type `HasMember`, et récupérer la liste des `targetObject` (documents du lot).
   e. Appel de `GetDocuments` avec la liste des `entryUUID` des documents.

#### *Limitation de certains paramètres multivalués Et/Ou*

Le DMP restreint l'utilisation multivaluée Et/Ou des paramètres suivants :

- requête `FindDocuments` :
  - `$XDSDocumentEntryEventCodeList`;
  - `$XDSDocumentEntryConfidentialityCode`;
- requête `GetSubmissionSetAndContents` :
  - `$XDSDocumentEntryConfidentialityCode`.
- requête `FindDocumentByReferenceId` :
  - `$XDSDocumentEntryEventCodeList;`
  - `$XDSDocumentEntryConfidentialityCode;`
  - `$XDSDocumentEntryReferenceIdList`.

Pour ces requêtes et ces paramètres, le DMP supporte la sémantique « Et/Ou » mais pour un nombre fini de valeurs fixé à 5 pour les « Et ». En d'autres termes, un paramètre multivalué peut comporter un nombre infini de valeurs entre lesquelles un « Ou » doit être utilisé mais ne peut supporter que 5 valeurs pour lesquelles un « Et » doit être utilisé. En cas de dépassement du nombre de valeurs possible, un code d'erreur `XDSStoredQueryParamNumber` est retourné. La valeur `codeContext` contient alors, en plus du nom du paramètre et de la valeur associée, une entrée `maxAND=5`.

**[DEROGATION SPECIFIQUE DMP PAR RAPPORT AU CI-SIS]**

La réponse à une requête stockée (TD3.1) incluant les documents « obsolètes » (statut « Deprecated ») retourne toutes les versions de métadonnées du même document.

Dans les requêtes de type FindSubmissionSets ou GetAll, le système DMP retourne les lots de soumission liées à des opérations de mise à jour de la métadonnée « availabilityStatus » des métadonnées d'un document.

**[FIN DE DEROGATION SPECIFIQUE DMP PAR RAPPORT AU CI-SIS]**

***Recherche d'identifiant unique dans le système DMP***

Ce type de recherche est pris en charge par la requête stockée `GetDocuments` en indiquant `returnType="ObjectRef"`. Voir [IHE-TF2A] § 3.18.4.1.2.3.7.5 GetDocuments.

NB : ce type de recherche est à utiliser dans le cadre du profil Alimentation pour remplacer un document ou pour supprimer un document sans autorisation d'accès au DMP du patient.

**Données en sortie**

***En cas de succès de la transaction :***

Le système DMP retourne :

- un code `status` égal à `urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success`, conformément au profil XDS.b,
- les objets retournés par la requête (documents et/ou lots, et/ou association entre les documents et les lots).

La recherche de document est soumise à la restriction d'accès de la matrice d'habilitation du système DMP. Cf. [DMP-MHAB].

***En cas d'erreur de la transaction :***

Le système DMP retourne un code `status` égal à `urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure`, conformément au profil XDS.b. Le status `PartialSuccess` n'est pas géré par le DMP.

L'annexe A7-1 décrit les codes d'erreur utilisés dans le cadre du DMP.

## 3.5.2 DMP_3.2 : consulter des documents dans le DMP d'un patient (via TD3.2)

### 3.5.2.1 Description de la fonctionnalité

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

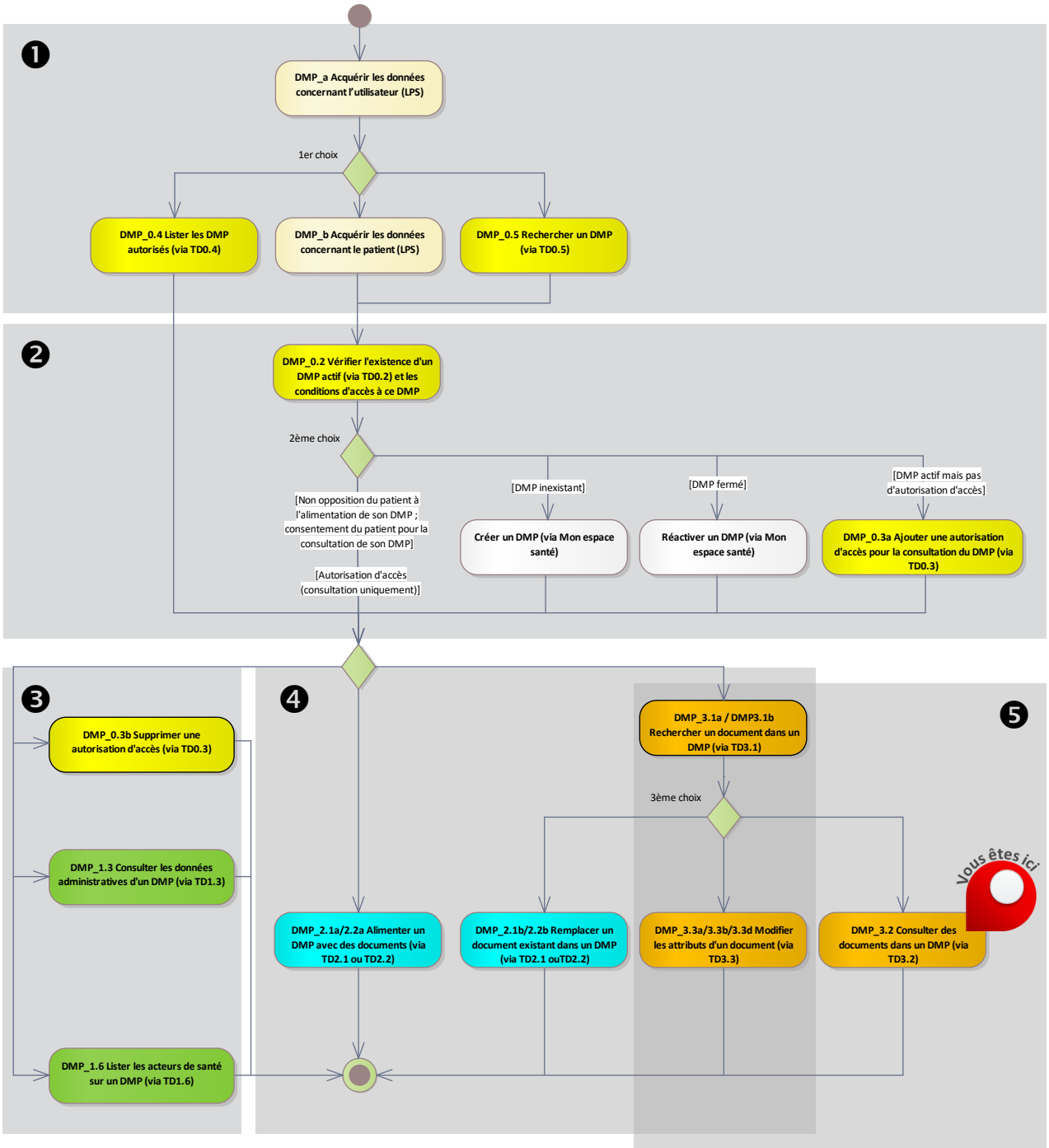



**Figure 23 : localisation de la fonctionnalité DMP_3.2 dans le processus regroupant les deux profils Alimentation et Consultation**

## Vue générale

***Description***

Cette fonctionnalité permet à l'utilisateur de télécharger et visualiser le contenu d'un document du DMP d'un patient.

Elle fait suite à la fonctionnalité « lister les documents d'un DMP » (DMP_3.1a) qui a permis à l'utilisateur de rechercher des documents dans le DMP d'un patient.

La cinématique générale est la suivante.

- L'utilisateur a sélectionné un ou plusieurs document(s) à consulter parmi les résultats retournés dans la fonctionnalité DMP_3.1a.
- Le LPS envoie une requête de demande de document au système DMP (TD3.2) à partir du ou des identifiants de document sélectionné(s). Cf. RG_3210.
- Le système DMP retourne le(s) document(s) au LPS.
- Le LPS affiche le(s) document(s). Cf. RG_3220.

***Entrées et prérequis***

L'INS du patient (EF_DMP11_01).

Le statut « actif » du DMP du patient (EF_DMP12_01).

L'autorisation d'accès au DMP du patient (EF_DMP04_01) au statut « valide ».

La liste des identifiants (uniqueId) des documents à consulter (issue de DMP_3.1a) (EF_DMP31_01).

***Sorties***

Les documents affichés par le LPS.

## Règles de gestion

### *[RG_3210] Télécharger les documents*

Le LPS appelle la transaction TD3.2 pour chaque document à consulter.

Cf. §3.5.2.2 pour la description de cette transaction.

**EX_3.2-1010**

Le LPS ne doit pas réaliser de téléchargement systématique du contenu des documents (i.e. ne pas réaliser de TD3.1 suivi d'une TD3.2 systématique pour chaque document retourné par la TD3.1).

Les documents DMP téléchargés à partir de la TD3.2 ne doivent, en aucun cas être conservés automatiquement en dehors du DMP.

Une action manuelle du professionnel est obligatoirement requise pour l'enregistrement dans le LPS de chaque document.

Sans action manelle du professionnel et après consultation, les documents DMP téléchargés à partir de la TD3.2 doivent être supprimés automatiquement.

Le LPS doit clairement afficher la provenance (DMP) du document enregistré dans le LPS, ainsi que la date de son enregistrement.

***[RG_3215] Afficher une alerte pour un document invisible au patient et/ou aux représentants légaux***

**EX_3.2-1025**

La consultation d'un document invisible au patient (`confidentialityCode = INVISIBLE_PATIENT`), doit donner lieu à une information du professionnel par l'affichage d'un message d'alerte de type :

"Attention, ce document n'est pas visible du patient"

La consultation d'un document invisible aux représentants légaux (`confidentialityCode = INVISIBLE_REPRESENTANTS_LEGAUX`), doit donner lieu à une information du professionnel par l'affichage d'un message d'alerte de type :

"Attention, ce document n'est pas visible des représentants légaux pour préserver le secret du mineur titulaire du DMP"

***[RG_3220] Afficher les documents téléchargés à partir du DMP***

**EX_3.2-1030**

Le LPS doit permettre l'affichage des données d'en-tête du document CDA R2.

**EX_3.2-1040 - Documents CDA R2 non structurés**

Le LPS doit prendre en charge et réaliser l'affichage des **documents CDA R2 dits « non structurés »**.

Un document non structuré peut être reconnu à l'aide du champ `formatCode` des métadonnées XDS associées au document **qui est égal à** l'une des valeurs suivantes :

- `urn:ihe:iti:xds-sd:pdf:2008`,
- `urn:ihe:iti:xds-sd:text:2008`,
- `urn:ihe:iti-fr:xds-sd:jpeg:2010`,
- `urn:ihe:iti-fr:xds-sd:rtf:2010`,
- `urn:ihe:iti-fr:xds-sd:tiff:2010`.

Le LPS doit extraire du champ `nonXmlBody/text` le corps du document qui est encodé en base 64, le décoder et en proposer l'affichage à l'utilisateur (les types mime autorisés sont pris en charge nativement par la plupart des OS).

Il se peut que la longueur de ce champ ne soit pas un multiple de 4. En effet, certaines librairies d'encodage base 64 ajoutent le padding de fin (le ou les caractère(s) « = » à la fin de la chaîne) et d'autres non. Il est donc important de savoir décoder des chaînes base 64 « sans padding », car les LPS pouvant envoyer des documents dans le DMP sont hétérogènes en terme de librairie d'encodage base 64. Il suffit de compléter avec la bonne valeur de padding de fin si la librairie utilisée ne le réalise pas déjà, et si la longueur n'est pas correcte.

**EX_3.2-1050 - Documents CDA R2 structurés**

Le LPS doit prendre en charge et réaliser l'affichage des **documents CDA R2 niveau 3 dits « structurés »**.

Un document structuré peut être reconnu à l'aide du champ `formatCode` des métadonnées XDS associées au document **qui est différent** des valeurs suivantes :

- `urn:ihe:iti:xds-sd:pdf:2008`,
- `urn:ihe:iti:xds-sd:text:2008`,
- `urn:ihe:iti-fr:xds-sd:jpeg:2010`,
- `urn:ihe:iti-fr:xds-sd:rtf:2010`,
- `urn:ihe:iti-fr:xds-sd:tiff:2010`.

La différence entre un document structuré CDA R2 « classique » et un document structuré CDA R2 « auto-présentable » est signalée par le champ `mimeType` des métadonnées XDS associées au document :

- `text/xml` pour les CDA R2 « classiques »,
- `application/xslt+xml` pour les CDA R2 « auto-présentables ».

**REC_3.2-1060**

Pour afficher le corps du document (organisé en structures XML), le LPS peut appliquer une feuille de style XSLT et afficher le résultat à l'utilisateur via un navigateur web, éventuellement encapsulé.

**REC_3.2-1065**

Il est recommandé d'afficher les documents CDA auto-présentables à l'aide de la feuille de style couplée au document. Pour visualiser un document CDA auto-présentable de manière simple et rapide (et sans développement spécifique), le LPS peut l'ouvrir directement dans un navigateur. Celui-ci réalise alors l'affichage automatiquement avec la feuille de style intégrée au CDA.

**REC_3.2-1070**

Le LPS peut « exploiter » les données structurées pour proposer des affichages à valeur ajoutée aux professionnels (par exemple, une courbe de résultat d'analyses biologiques).

**REC_3.2-1080**

Plusieurs documents peuvent être liés entre eux car ils constituent un ensemble cohérent pour un même épisode de soins. Lors de la consultation d'un document, il est conseillé d'afficher les documents qui lui sont liés. Cela permet notamment au médecin qui consulte un document d'identifier qu'il y a d'autres documents qui peuvent l'intéresser et d'y accéder beaucoup plus simplement.

Dans le système DMP,

- les documents soumis dans un même lot sont liés.
- Un même document peut être référencé dans plusieurs lots de soumission.
- Les documents peuvent être liés par `referenceIdList`.

Cf. REC_2.1-1160 dans RG_2610 au § 3.4.1.1.5.

Exemple de la fiche RCP :

Lors de la consultation de la fiche RCP, le médecin doit pouvoir facilement identifier qu'il existe un CR-Opératoire et un CR-ACP liés. Ce lien existe dès lors que ces 3 documents ont été groupés dans le même lot de soumission à l'alimentation du DMP.

**EX_3.2-1090**

Il est demandé d'afficher la date du document en heure locale :

- dans le cas d'une consultation de documents (TD3.2 - IHE ITI-43 RetrieveDocumentSet XDS) : en se basant sur les données d'en-tête CDA et en indiquant qu'il s'agit de l'heure locale du producteur du document.

### 3.5.2.2 TD3.2 : consultation d'un document dans le DMP d'un patient

Le profil IHE XDS.b utilisé pour la consultation est présenté dans le chapitre 5.1.2.

La transaction est décrite dans [CI-PARTAGE] (ITI-43 RetrieveDocumentSet).

La transaction doit respecter les exigences concernant l'accès sécurisé au système DMP. Cf. TD0.1 au §5.3.

**Données en entrée**

Identifiants des documents (XDSDocumentEntry.uniqueId) (EF_DMP 31_01) et les identifiants des repository où sont stockés les documents (XDSDocumentEntry.repositoryUniqueId). Ce dernier paramètre est toujours le même pour le DMP (il est récupéré dans la réponse fournie par la transaction TD3.1).

**Données en sortie**

***En cas de succès de la transaction :***

Le système DMP retourne un code `status` égal à `urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success`, conformément au profil XDS.b, ainsi que le ou les document(s) demandé(s).

***En cas d'erreur de la transaction :***

Le système DMP retourne un code `status` égal à `urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure`, conformément au profil XDS.b, ainsi qu'un code d'erreur et éventuellement un message de détail. Le retour d'erreur est détaillé dans [IHE-TF3].

La table 4.1-11 du doc [IHE-TF3] récapitule les codes d'erreur standards de XDS.

L'annexe A7-1 décrit les codes d'erreur utilisés dans le cadre du DMP.

### 3.5.3 DMP_3.3 : modifier les attributs d'un document (via TD3.3)

La figure ci-dessous vous permet de localiser la fonctionnalité dans le processus.

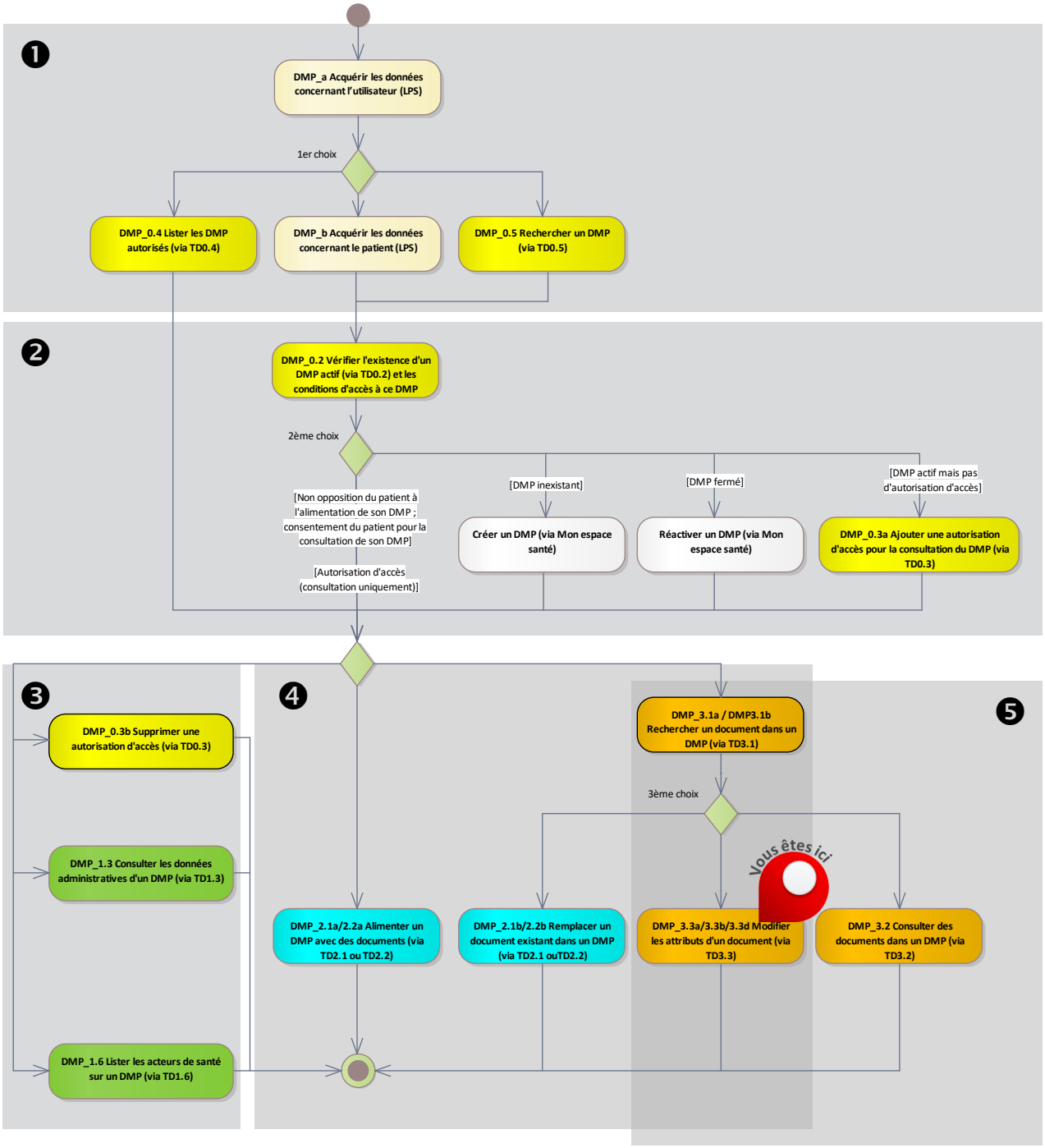



**Figure 24 : localisation de la fonctionnalité DMP_3.3 dans le processus regroupant les deux profils Alimentation et Consultation**

Cette fonctionnalité permet de mettre à jour les métadonnées suivantes d'un document, sans soumettre une nouvelle version du document :

- Masquage / démasquage d'un document aux professionnels,
- Visibilité d'un document au patient,
- Visibilité d'un document aux représentants légaux,
- Suppression d'un document,

- Archivage / désarchivage d'un document.

NB1 : la gestion de la visibilité et du masquage peut s'effectuer également lors de l'alimentation du DMP du patient (voir DMP_2.1/2.2).

NB2 : les possibilités de modification des attributs et de suppression d'un document sont limitées par la matrice d'habilitations du système DMP. Cf. [DMP-MHAB].

NB3 : si le LPS implémente le profil Alimentation, il n'est pas nécessaire d'avoir une autorisation d'accès pour supprimer des documents dans le DMP d'un patient.

NB4 : la gestion de la visibilité d'un document aux représentants légaux d'un mineur est conditionnée par l'activation de la gestion des mineurs. Cf. paramètre `fonctions-gestion-mineurs` § 3.1.1.

Deux fonctionnalités sont présentées dans les chapitres suivants :

- cf. DMP_3.3a/3.3b/3.3d pour la modification des métadonnées (hors suppression),
- cf. DMP_3.3c pour la suppression d'un document.

### 3.5.3.1 DMP_3.3a/3.3b/3.3d : modifier les attributs d'un document (via TD3.3a, TD3.3b et/ou TD3.3d)

#### Vue générale

***Description***

Cette fonctionnalité permet à l'utilisateur de modifier les attributs d'un document dans le DMP d'un patient.

- Masquage / démasquage d'un document aux professionnels,
- Visibilité d'un document au patient,
- Visibilité d'un document aux représentants légaux d'un mineur (si la gestion des mineurs est activée),
- Archivage / désarchivage d'un document.

Elle fait suite à la fonctionnalité DMP_3.1 qui a permis de rechercher l'identifiant technique d'un document.

La cinématique générale est la suivante.

- Le LPS affiche les attributs du document sélectionné. Cf. RG_3310.
- L'utilisateur indique l'action qu'il souhaite effectuer. Cf. RG_3320.
- L'utilisateur confirme l'action demandée. Cf. RG_3330.
- Le LPS envoie une requête de mise à jour des attributs d'un document au système DMP (TD3.3a ou TD3.3b ou TD3.3d). Cf. RG_3340.

***Entrées et prérequis***

L'INS du patient (EF_DMP11_01).

Le statut « actif » du DMP du patient (EF_DMP12_01).

L'autorisation d'accès au DMP du patient (EF_DMP04_01) au statut « valide » (sauf si le LPS implémente le profil Alimentation).

L'identifiant du document dans le système DMP issu de DMP_3.1 : entryUUID (EF_DMP31_02) ou LogicalID (EF_DMP31_05). Cf. RG_3050 §3.5.1.1.

***Sorties***

Les attributs du document sont modifiées dans le DMP du patient.

**Règles de gestion**

*[RG_3310] Afficher les attributs du document (EF_DMP31_03 et EF_DMP31_05)*

**REC_3.3-1010**

Pour « masquer/démasquer un document aux professionnels », « archiver/désarchiver un document », « rendre un document visible au patient » ou « rendre un document visible aux représentants légaux », le LPS peut présenter une IHM dédiée nommée « Modification des propriétés du document » à l'utilisateur.

Exemple possible de mise en œuvre :

Modification des propriétés du document

**Confidentialité du document**

**Pour le patient**

( ) Rendre le document visible par le patient : vous souhaitez que ce document soit désormais visible par le patient car il a bien reçu une information préalable par un professionnel.

**Pour les représentants légaux du patient**

( ) Rendre le document visible par les représentants légaux du patient.

**Pour les professionnels**

(x) Document visible par les professionnels autorisés à accéder aux documents du DMP du patient

( ) Document masqué aux professionnels : document visible uniquement par son auteur, les médecins traitants DMP et le patient.

**Archivage**

(x) Non archivé (toujours visible dans la liste des documents)

( ) Archivé (visible seulement si critère d'affichage des documents archivés sélectionné)

**EX_3.3-1020**

Lors de l'affichage des informations ci-dessus, le positionnement des boutons radios doit refléter l'état actuel du document en cours de modification.

*[RG_3320] Acquérir l'action demandée par l'utilisateur*

L'utilisateur modifie un ou plusieurs attribut(s) sur l'IHM proposée par le LPS.

Cf. exemple de mise en œuvre ci-dessus.

*[RG_3330] Acquérir la confirmation de l'action demandée par l'utilisateur*

**EX_3.3-1030**

Toute demande de masquage / démasquage doit donner lieu à une confirmation par l'utilisateur effectuant l'action : le LPS doit proposer un message de confirmation du masquage / démasquage.

**EX_3.3-1040**

La fonction « Rendre un document visible au patient » est irréversible et ne permet pas de rendre invisible à nouveau un document visible. Le LPS doit afficher un message demandant à l'utilisateur de confirmer l'action.

Il est conseillé de pouvoir facilement désactiver cet affichage, par exemple par paramétrage du logiciel. Cf. recommandation REC_2.1-1065.

**EX_3.3-1045**

La fonction « Rendre un document visible aux représentants légaux du patient » est irréversible et ne permet pas de rendre invisible à nouveau un document visible. Le LPS doit afficher un message demandant à l'utilisateur de confirmer l'action.

Il est conseillé de pouvoir facilement désactiver cet affichage, par exemple par paramétrage du logiciel. Cf. recommandation REC_2.1-1065.

La confirmation par l'utilisateur est facultative pour l'archivage et le désarchivage.

***[RG_3340] Effectuer l'action demandée par l'utilisateur***

Condition : l'utilisateur a confirmé l'action demandée (cf. RG_3320).

Le LPS appelle la transaction correspondant à l'action demandée par l'utilisateur.

- TD3.3a si l'utilisateur demande à masquer ou démasquer un document aux professionnels. Cf. § 3.5.3.3.1 pour la description de cette transaction.
- TD3.3b si l'utilisateur demande à rendre un document visible au patient ou à ses representants légaux.
  Cf. § 3.5.3.3.2 pour la description de cette transaction.
- TD3.3d si l'utilisateur demande à archiver ou désarchiver un document.
  Cf. § 3.5.3.3.4 pour la description de cette transaction.

### 3.5.3.2 DMP_3.3c : supprimer un document (via TD3.3c)

#### Vue générale

***Description***

Cette fonctionnalité permet à l'utilisateur de supprimer un document dans le DMP d'un patient.

La cinématique générale est la suivante :

- L'utilisateur indique qu'il souhaite supprimer le document sélectionné. Cf. RG_3410.
- L'utilisateur confirme l'action demandée. Cf. RG_3420.
- Le LPS envoie une requête de mise à jour des attributs d'un document au système DMP (TD3.3c). Cf. RG_3430.

NB1 : si le LPS implémente le profil Alimentation, il n'est pas nécessaire d'avoir une autorisation d'accès pour supprimer des documents dans le DMP d'un patient.

NB2 : pour information, seul l'auteur du document peut supprimer le document (contrôle effectué par le système DMP, cf. [DMP-MDRF]).

***Entrées et prérequis***

L'INS du patient (EF_DMP11_01).

Le statut « actif » du DMP du patient (EF_DMP12_01).

L'autorisation d'accès au DMP du patient (EF_DMP04_01) au statut « valide » (sauf si le LPS implémente le profil Alimentation).

L'identifiant du document dans le système DMP issu de DMP_3.1 (EF_DMP31_02).

***Sorties***

Le document est supprimé.

**Règles de gestion**

*[RG_3410] Acquérir la demande de suppression*

L'utilisateur indique qu'il souhaite supprimer le document sélectionné.

*[RG_3420] Acquérir la confirmation de la demande de suppression*

| EX_3.3-1050 |
| --- |
| La fonction de suppression d'un document est irréversible et un utilisateur ne peut pas annuler une suppression. Le LPS doit afficher un message demandant au professionnel de confirmer la suppression. L'utilisateur doit confirmer sa demande de suppression. |

*[RG_3430] Effectuer la suppression dans le DMP du patient*

Condition : l'utilisateur a confirmé l'action demandée (cf. RG_3420).

Le LPS appelle la transaction TD3.3c.

Cf. §3.5.3.3.3 pour la description de cette transaction.

### 3.5.3.3 TD3.3 : gestion des attributs d'un document

Le profil IHE XDS.b utilisé pour la consultation est présenté dans le chapitre 5.1.2.

La transaction utilisée est décrite dans [CI-PARTAGE] et les détails techniques d'implémentation de cette transaction sont décrits dans [IHE-MU] (IHE ITI-57 Update Document Set).

**[DEROGATION SPECIFIQUE DMP PAR RAPPORT AU CI-SIS]**

Le système DMP propage le changement de visibilité (`confidentialityCode`) aux anciennes versions des métadonnées.

**[FIN DE DEROGATION SPECIFIQUE DMP PAR RAPPORT AU CI-SIS]**

La transaction doit respecter les exigences concernant l'accès sécurisé au système DMP. Cf. TD0.1 au §5.3.

**Données en entrée**

Les données en entrée diffèrent en fonction de l'action à réaliser. Cf. les chapitres suivants.

- TD3.3a : masquer / démasquer un document aux professionnels ;
- TD3.3b : rendre un document visible au patient ou à ses representants légaux,
- TD3.3c : supprimer un document
- TD3.3d : archiver / désarchiver un document

**Données en sortie**

*En cas de succès de la transaction :*

Le système DMP retourne un code `status` égal à `urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success`.

*En cas d'erreur de la transaction :*

Le système DMP retourne un code `status` égal à `urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure`, ainsi qu'un code d'erreur et éventuellement un message de détail. Le retour d'erreur est détaillé dans [IHE-TF3].

La table 4.1-11 du doc [IHE-TF3] récapitule les codes d'erreur standards de XDS.

L'annexe A7-1 décrit les codes d'erreur utilisés dans le cadre du DMP.

#### 3.5.3.3.1 TD3.3a : masquer / démasquer un document aux professionnels

La transaction est décrite dans ITI-57 §3.57.4.1.3.3.1 Update DocumentEntry Metadata.

Toutes les métadonnées du document doivent être renvoyées au système DMP ;

Alimentation de la métadonnée `confidentialityCode`.

- Dans le cas du masquage aux professionnels, cette métadonnée doit contenir la valeur `MASQUE_PS`[10] dans la nomenclature d'OID 1.2.250.1.213.1.1.4.13.
- Dans le cas du démasquage, la valeur correspondant au masquage à un professionnel doit être retirée du champ.
- Les deux valeurs « masqué au professionnel » et « invisible au patient » ne sont pas possibles simultanément tant que le paramètre `cumul-invisible_patient-masque_ps`[10] contient `false`. Cf. § 2.4.4 et § 3.1.1.

D'autres données en entrée sont spécifiées au chapitre Update DocumentEntry Metadata.

Les données en sorties sont décrites dans TD3.3. Cf. chapitre 3.5.3.3.

#### 3.5.3.3.2 TD3.3b : rendre un document visible au patient ou à ses representants légaux

La transaction est décrite dans ITI-57 § 3.57.4.1.3.3.1 Update DocumentEntry Metadata.

Toutes les métadonnées du document doivent être renvoyées au système DMP.

Alimentation de la métadonnée `confidentialityCode`.

- Lorsque le document n'est pas visible au patient, cette métadonnée contient la valeur `INVISIBLE_PATIENT` dans la nomenclature d'OID 1.2.250.1.213.1.1.4.13.
- Pour rendre un document visible au patient, la valeur correspondant à l'invisibilité au patient doit être retirée des métadonnées XDS.
- Les deux valeurs « masqué au professionnel » et « invisible au patient » ne sont pas possibles simultanément tant que le paramètre `cumul-invisible_patient-masque_ps`[10] contient `false`. Cf. § 2.4.4 et § 3.1.1.
- Lorsque le document n'est pas visible aux représentants légaux du patient, cette métadonnée contient la valeur `INVISIBLE_REPRESENTANTS_LEGAUX` dans la nomenclature d'OID 1.2.250.1.213.1.1.4.13.
- Pour rendre un document visible aux représentants légaux du patient, la valeur correspondant à l'invisibilité aux représentants légaux doit être retirée des métadonnées XDS.

D'autres données en entrée sont spécifiées au chapitre Update DocumentEntry Metadata.

Les données en sorties sont décrites dans TD3.3. Cf. chapitre 3.5.3.3.

#### 3.5.3.3.3 TD3.3c : supprimer un document

Les données à envoyer sont décrites dans ITI-57 § 3.57.4.1.3.3.2 Update DocumentEntry AvailabilityStatus.

La transaction doit envoyer la valeur `urn:asip:ci-sis:2010:StatusType:Deleted` dans l'association « UpdateAvailabilityStatus » pour mettre à jour le champ `availabilityStatus` du document.

Les données en sorties sont décrites dans TD3.3. Cf. chapitre 3.5.3.3.

[10] Le nom technique n'évolue pas. Il conserve le terme « PS ».

#### 3.5.3.3.4 TD3.3d : archiver / désarchiver un document

Les données à envoyer sont décrites ITI-57 §3.57.4.1.3.3.2 Update DocumentEntry AvailabilityStatus.

Pour archiver un document, la transaction doit envoyer la valeur `urn:asip:ci-sis:2010:StatusType:Archived` dans l'association « UpdateAvailabilityStatus » pour mettre à jour le champ `availabilityStatus` du document.

Pour désarchiver un document, la transaction doit envoyer la valeur `urn:oasis:names:tc:ebxml-regrep:StatusType:Approved` dans l'association « UpdateAvailabilityStatus » pour mettre à jour le champ `availabilityStatus` du document.

La notion « d'archivage » d'un document est une notion d'archivage fonctionnelle pour l'utilisateur qui ne souhaite plus visualiser des documents qui ne sont plus utiles dans sa pratique médicale courante, et non d'un archivage "technique" au niveau du repository XDS : la métadonnée `documentAvailability` (décrite dans le supplément XDS MetadataUpdate) ne rentre pas en ligne de compte pour l'archivage de document dans le système DMP.

Si dans le système DMP, il existe un document avec une version en cours active (statut `urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`) et des versions antérieures au statut `Deprecated`, l'archivage de la version en cours du document n'est pas propagé aux versions antérieures du document. La version du document avec le statut `urn:oasis:names:tc:ebxml-regrep:StatusType:Approved` passe alors à l'état `urn:asip:ci-sis:2010:StatusType:Archived` mais les versions antérieures restent au statut `urn:oasis:names:tc:ebxml-regrep:StatusType:Deprecated`.

Les données en sorties sont décrites dans TD3.3. Cf. chapitre 3.5.3.3.

# 4 DESCRIPTION FONCTIONNELLE DES DONNEES

Ce chapitre récence les données utilisées dans plusieurs transactions.

Par exemple, le patient est représenté par l'entité qui porte la référence EF_DMP11. L'INS du patient est la donnée référencée 01 dans cette entité. La référence complète de cette donnée est EF_DMP11_01.

Les valeurs fixes et les précisions techniques sont indiquées dans la description des transactions.

**Description des données**

Les occurrences des données ne sont pas indiquées dans les tableaux ci-dessous car elles sont spécifiques à chaque message (requête ou réponse) de chaque transaction.

## 4.1 Données fonctionnelles

Le tableau ci-dessous est trié par ordre alphabétique des noms des entités fonctionnelles.

| Référence | Entité ou donnée | Description |
|---|---|---|
| **EF_DMP03** | **Acteur de santé** | Il s'agit soit de l'utilisateur, soit de la structure de soins. Cf. définition dans le chapitre 2.2.3. |
| | Cf. Utilisateur (EF_DMP01) ou Structure de soins (EF_DMP02). | |
| **EF_DMP13** | **Adresse postale du patient** | Cf. § 4.2.2. |
| EF_DMP13_01 | ligne d'adresse 1 | |
| EF_DMP13_02 | complément d'adresse | |
| EF_DMP13_03 | code postal | |
| EF_DMP13_04 | commune | |
| EF_DMP13_05 | pays | |
| **EF_DMP15** | **Adresse du représentant légal du patient** | Cf. § 4.2.3. |
| EF_DMP15_01 | ligne d'adresse 1 | |
| EF_DMP15_02 | complément d'adresse | |
| EF_DMP15_03 | code postal | |
| EF_DMP15_04 | commune | |
| **EF_DMP04** | **Autorisation d'accès au DMP d'un patient** | |
| EF_DMP04_01 | Statut de l'autorisation d'accès pour la consultation du DMP. | Cf. cycle de vie décrit dans le chapitre 2.4.2.<br>Liste des valeurs possibles pour l'attribut code :<br>• `NON_EXISTE` : autorisation inexistante,<br>• `INTERDIT` : blocage d'accès (professionnel uniquement),<br>• `EXPIRE` : autorisation ayant pris fin,<br>• `VALIDE` : autorisation valide.<br>Valeur pour l'attribut codeSystem : « 1.2.250.1.213.4.1.2.6.2 ». |

| | | |
|---|---|---|
| EF_DMP04_02 | Consentement du patient concernant l'accès pour la consultation de son DMP par l'acteur de santé. | Le patient peut consentir ou non à la consultation de son DMP par l'acteur de santé.<br>NB1 : cette donnée est gérée par le LPS en local (= hors SI DMP).<br>NB2 : lorsque le patient n'est pas en capacité de donner son accord, un accès en mode « bris de glace » est possible. |
| EF_DMP04_03 | Non opposition du patient concernant l'accès pour l'alimentation de son DMP par l'acteur de santé. | Le patient peut être opposé ou non à l'alimentation de son DMP par l'acteur de santé.<br>NB1 : cette donnée est gérée par le LPS en local (= hors SI DMP). |
| **EF_DMP16** | **Compte internet du patient** | |
| EF_DMP16_01 | Type de canal OTP | Valeurs : `SMS` ou `EMAIL`. |
| EF_DMP16_02 | Canal OTP | Représente soit une adresse mél, soit un numéro de téléphone.<br>Le format dépend du type de canal :<br>• uniquement des chiffres pour un numéro de téléphone,<br>• ou un format d'email standard. |
| EF_DMP16_03 | Identifiant de connexion pour l'accès au compte internet | Identifiant du compte internet patient attribué par le système DMP. |
| EF_DMP16_04 | Mot de passe pour l'accès au compte internet | Mot de passe du compte internet patient attribué par le système DMP (à usage unique lors de la création du compte ou lors de la regénération en cas d'oubli). |
| **EF_DMP12** | **DMP du patient** | |
| EF_DMP12_01 | Statut du DMP | Cf. présentation au §2.4.1. Valeurs possibles :<br>• `NF` : le DMP n'existe pas,<br>• `active` : le DMP est actif,<br>• `terminated` : le DMP est fermé. |
| EF_DMP12_02 | Date de fermeture | |
| EF_DMP12_03 | Motif de fermeture du DMP | Valeur `FERMETURE_DEMANDE_PATIENT` signifiant « Fermeture du DMP suite à la demande du patient ».<br>Valeur `FERMETURE_DECES_PATIENT` signifiant « Fermeture du DMP suite au décès du patient ».<br>Valeur pour l'attribut codeSystem : « 1.2.250.1.213.4.1.2.4 » |
| EF_DMP12_04 | Raison de fermeture du DMP | Texte libre. |

| | | |
|---|---|---|
| **EF_DMP31** | **Document** | |
| EF_DMP31_01 | Identifiant mondialement unique fourni par le LPS | Il s'agit de l'identifiant unique global du document affecté par le producteur du document, au format OID. Intervient dans CDA R2 et dans les transactions XDS Cette donnée est appelée uniqueId au niveau technique. |
| EF_DMP31_02 | Identifiant unique dans le système DMP | Il s'agit de l'identifiant unique du document affecté par le système DMP lors de l'indexation de celui-ci dans le DMP du patient, au format UUID.<br>Ce champ n'intervient que dans les transactions XDS et le nom de la variable est XDSDocumentEntry.entryUUID.<br>Si plusieurs versions du document sont manipulées, cet identifiant est différent pour chaque version du document. |
| EF_DMP31_03 | Visibilité | |
| EF_DMP31_04 | Type de document | |
| EF_DMP31_04 | Attribut d'archivage | |
| EF_DMP31_05 | Identifiant logique dans le système DMP | Il s'agit d'un identifiant, affecté par le système DMP, portant la même valeur pour toutes les versions d'un document. Cette donnée est appelée logicalId au niveau technique. |
| **EF_DMP32** | **Lot de soumission** | |
| EF_DMP32_01 | Date de soumission | |
| **EF_DMP11** | **Patient** | Cf. § 4.2.2. |
| EF_DMP11_01 | INS du patient | Identifiant National de Santé du patient (22 caractères alphanumériques).<br>Cf. [OID-INS] pour la liste des OID associés à cette donnée.<br>Dans HL7v3, l'OID est dans `@root` et la valeur de l'identifiant dans `@extension`.<br>Pour les transactions spécifiques DMP, cf. description de la transaction dans les chapitres correspondants.<br>Cette donnée peut aussi être véhiculée dans le jeton VIHF. Cf. § 5.3.2, § 5.3.3 et §5.3.4.5. |
| EF_DMP11_02 | Nom d'usage | |
| EF_DMP11_03 | Nom de naissance | |
| EF_DMP11_04 | Prénom | |
| EF_DMP11_05 | Sexe | Sexe administratif du patient.<br>• `M` : masculin,<br>• `F` : féminin,<br>• `U` : indéterminé. |
| EF_DMP11_06 | Date de naissance | Date de naissance du patient.<br>Certaines dates de naissance sont au format « lunaire » (mois > 12 et/ou jour > 31).<br>Cf. format dans la description des transactions. |

| | | |
|---|---|---|
| EF_DMP11_07 | Civilité | Valeurs :<br>• `M` : monsieur,<br>• `Mme` : madame,<br>• `Mlle` : mademoiselle.<br>NB : la valeur `Mlle` n'est plus autorisée en alimentation. Elle est conservée en consultation pour les anciens DMP. |
| EF_DMP11_08 | Pays de naissance | |
| EF_DMP11_09 | Téléphone portable | |
| EF_DMP11_10 | Téléphone fixe domicile | |
| EF_DMP11_11 | Email | |
| EF_DMP11_12 | consentement du patient à l'accès à son DMP en mode « bris de glace » | |
| EF_DMP11_13 | consentement du patient à l'accès à son DMP en mode « centre de régulation » | |
| **EF_DMP14** | **Représentant légal du patient** | Cf. § 4.2.3. |
| EF_DMP14_01 | Qualité | |
| EF_DMP14_02 | Civilité | |
| EF_DMP14_03 | Nom | |
| EF_DMP14_04 | Prénom | |
| EF_DMP14_05 | Téléphone portable | |
| EF_DMP14_06 | Téléphone fixe domicile | |
| EF_DMP14_07 | Email | |
| **EF_DMP02** | **Structure de soins** | |
| EF_DMP02_01 | Identifiant de la structure de soins | |
| EF_DMP02_02 | Nom | |
| **EF_DMP01** | **Utilisateur** | |
| EF_DMP01_01 | Identifiant | |
| EF_DMP01_02 | Mode d'accès | |
| EF_DMP01_03 | Profession et spécialité | |
| EF_DMP01_04 | Nom | |
| EF_DMP01_05 | Prénom | |
| EF_DMP01_06 | Secteur d'activité | |
| EF_DMP01_07 | Médecin traitant DMP | Liste des valeurs possibles :<br>• `false` : l'utilisateur n'est pas médecin traitant DMP,<br>• `true` : l'utilisateur est médecin traitant DMP. |

**Tableau 21 : données utilisées dans plusieurs transactions**

## 4.2 Données communes à plusieurs transactions HL7

### 4.2.1 Professionnel (ou personne exerçant sous la responsabilité d'un ou plusieurs professionnel(s)) auteur de l'action sur le dossier

L'auteur de l'action sur le dossier doit être fourni (lorsque demandé) dans l'élément `registrationRequest/author/assignedEntity`

| Nom du champ | Cardinalité | *Taille Max* | XPath HL7 | Remarques / contraintes |
|---|---|---|---|---|
| *Données d'identification du professionnel* | *[1..1]* | | *author/assignedEntity* | |
| *identifiant* | *[1..1]* | | *Id* | |
| OID de l'id | [1..1] | | @root | Valeur fixe : « 1.2.250.1.71.4.2.1 » |
| valeur de l'id | [1..1] | | @extension | Identifiant du professionnel; voir chapitre construction des identifiants des professionnels (**§ 3.1.1**) |
| rôle structurel (profession + spécialité) | [0..1] | | code | |
| OID de l'id | [1..1] | | @code | Valeur du code (« 1.2.250.1.213.1.1.4.5 » pour un professionnel ou « 1.2.250.1.213.1.1.4.6 » pour une personne exerçant sous la responsabilité d'un ou plusieurs professionnel(s)). D'autres valeurs sont disponibles dans le JDV_J56-AuthorSpecialty-DMP. |
| valeur de l'id | [1..1] | | @codeSystem | OID de la nomenclature authorSpecialty de l'ANS |
| nom | [1..1] | 80 | assignedPerson/name/family | Caractères accentués autorisés. Pas de caractères spéciaux excepté : [-' ] (tiret apostrophe espace) |
| prénom | [1..1] | 60 | assignedPerson/name/given | Caractères accentués autorisés. Pas de caractères spéciaux excepté : [-' ] (tiret apostrophe espace) |
| *Structure liée au professionnel* | *[1..1]* | | *representedOrganisation* | |
| *identifiant de la structure* | *[1..1]* | | *id* | |
| OID de l'id | [1..1] | | @root | Valeur fixe : « 1.2.250.1.71.4.2.2 » |
| valeur de l'id | [1..1] | | @extension | Identifiant de la structure ; voir chapitre sur la construction des identifiants des structures (**§ 3.1.1**) |
| nom de la structure | [1..1] | | name | Caractères accentués autorisés. Pas de caractères spéciaux excepté : [-' ] (tiret apostrophe espace) |

**Tableau 22 : données du professionnel**

### 4.2.2 Données du patient

Les données administratives et de gestion du patient sont fournies dans un élément « patient ».

| Nom du champ | Card. | *Taille max* | XPath HL7 | contrainte |
|---|---|---|---|---|
| *patient* | *[1..1]* | | *patient* | |
| *Identifiant patient : INS* | *[1..N]* | | *id* | ***(1)*** *en retour du test d'existence : 0 à N INS peuvent être retournés.*<br>***(2)*** *autres transactions : un INS* |
| OID d'affectation de l'INS | [1..1] | | @root | Cf. [OID-INS]. |
| *valeur de l'INS* | [1..1] | *22* | @extension | |
| statut du DMP | [1..1] | | statusCode/@code | Fixé à « `terminated` » pour la fermeture du DMP |
| *état civil du patient* | | | *patientPerson* | |
| Civilité | [0..1] | 5 | name/prefix | Valeur parmi : « `M` » « `Mme` » « `Mlle` »<br>NB : la valeur `Mlle` n'est plus autorisée en alimentation. Elle est conservée en consultation pour les anciens DMP. |
| Nom de naissance (légal) | [0..1] | 80 | name/family[@qualifier = 'BR'] | Nom de naissance (nom de famille)<br>Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-' ] (tiret apostrophe espace) |
| Nom d'usage | [1..1] | 80 | name/family[@qualifier = 'SP'] | Nom d'usage (ou « nom usuel »). Par exemple : nom marital<br>Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-' ] (tiret apostrophe espace)<br>NB : lors d'une consultation des données pour un DMP associé à un « Mon espace santé », la transaction retourne la valeur « NON RENSEIGNE » (13 caractères) si le nom d'usage n'est pas renseigné dans ce DMP. |

| | | | | |
|---|---|---|---|---|
| Prénom | [1..1] | 60 | name/given | Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-' ]<br>(tiret apostrophe espace) |
| Sexe (M,F,U) | *[0..1]* | 1 | administrativeGenderCode/@code | Valeur parmi « M » (Masculin), « F » (Féminin), « U » (Non connu) |
| Date de naissance | *[0..1]* | 8 | birthTime/@value | Format `AAAAMMJJ` |
| Pays de naissance | [0..1] | 38 | birthPlace/addr/country | |
| Téléphone portable | [0..1] | 4+10 | telecom[@use='MC']/@value | Valeur précédée de « `tel`: » |
| Téléphone fixe domicile | [0..1] | 4+10 | telecom[@use='HP']/@value | Valeur précédée de « `tel`: » |
| Email | [0..1] | 7+64 | telecom/@value | Valeur précédée de « `mailto`: » |
| *adresse du patient* | [0..1] | | *addr* | |
| **[DEROGATION SPECIFIQUE DMP PAR RAPPORT AU CI-SIS]** | | | | |
| ligne d'adresse 1 | [0..1] | 38 | streetAddressLine | Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-',/ ]<br>(tiret apostrophe virgule slash espace) |
| complément d'adresse | [0..1] | 38 | additionalLocator | Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-',/ ]<br>(tiret apostrophe virgule slash espace) |
| code postal | [0..1] | 10 | postalCode | |
| commune | [0..1] | 38 | city | Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-',/ ]<br>(tiret apostrophe virgule slash espace) |
| pays | [0..1] | 38 | country | Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-',/ ]<br>(tiret apostrophe virgule slash espace) |
| **[FIN DE DEROGATION SPECIFIQUE DMP PAR RAPPORT AU CI-SIS]** | | | | |
| *Représentant légal* | *[0..1] ** | | *personalRelationship […]*<br>*(détail du contenu dans le tableau du **§4.2.3**)* | |
| *opposition du patient à l'utilisation du DMP en mode « bris de glace »* | *[0..1] ** | | *subjectOf/administrativeObservation* | |

| | | | | |
|---|---|---|---|---|
| *code du concept "opposition au mode bris de glace"* | *[1..1]* | | *code* | |
| code du concept | [1..1] | | @code | « OPPOSITION_BRIS_DE_GLACE » |
| OID du système de codification du concept | [1..1] | | @codeSystem | « 1.2.250.1.213.4.1.2.3 » |
| *valeur* | *[1..1]* | | *value* | |
| type de la valeur (fixé à "BL") | [1..1] | | @xsi:type | Fixe : « BL » |
| valeur de l'opposition | [1..1] | | @value | « true » si opposition, « false » sinon |
| *opposition du patient à l'utilisation du DMP en mode « centre de régulation »* | *[0..1] ** | | *subjectOf/administrativeObservation* | |
| *code du concept "opposition du patient au mode centre de régulation"* | *[1..1]* | | *code* | |
| code du concept | [1..1] | | @code | « OPPOSITION_ACCES_URGENCE » |
| OID du système de codification du concept | [1..1] | | @codeSystem | « 1.2.250.1.213.4.1.2.3 » |
| *valeur* | *[1..1]* | | *value* | |
| type de la valeur (fixé à "BL") | [1..1] | | @xsi:type | Fixe : « BL » |
| valeur de l'opposition | [1..1] | | @value | « true » si opposition, « false » sinon |

**Tableau 23 : données administratives et de gestion du patient**

### 4.2.3 Représentant légal du patient

Le représentant légal du patient peut être fourni au LPS, par la fonction de récupération des données administratives.
S'il est fourni, le représentant légal est positionné dans l'élément « patient ».

| Nom du champ | Card. | *Taille Max* | XPath HL7 | Remarques / contraintes |
|---|---|---|---|---|
| *données du représentant légal* | *[1..1]* | | *personalRelationship* | |
| *qualité du représentant légal* | *[1..1]* | | *code* | *(père, mère, tuteur…)* |
| | [1..1] | | @code | Code à prendre dans le jeu de valeurs des qualités du représentant légal dans [FI-JEUX-VALEURS] |
| | [1..1] | | @codeSystem | OID de la nomenclature utilisée, associé au code |
| *adresse du représentant légal* | *[0..1]* | | *addr* | |
| ligne d'adresse 1 | [0..1] | 38 | streetAddressLine | Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-',/ ] (tiret apostrophe virgule slash espace) |
| complément d'adresse | [0..1] | 38 | additionalLocator | Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-',/ ] (tiret apostrophe virgule slash espace) |
| code postal | [0..1] | 10 | postalCode | |
| commune | [0..1] | 38 | city | Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-',/ ] (tiret apostrophe virgule slash espace) |
| téléphone portable | [0..1] | 4+10 | telecom[@use='MC']/@value | Valeur précédée de « `tel`: » |
| téléphone fixe | [0..1] | 4+10 | telecom[@use='HP']/@value | Valeur précédée de « `tel`: » |
| email | [0..1] | 7+64 | telecom/@value | Valeur précédée de « `mailto`: » |
| *conteneur HL7 pour l'identité* | *[1..1]* | | *relationshipHolder1* | |
| | *[1..1]* | | *name* | |
| civilité | [0..1] | | prefix | |
| nom | [1..1] | 80 | family | Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-' ] (tiret apostrophe espace) |
| prénom | [1..1] | 60 | given | Caractères accentués autorisés.<br>Pas de caractères spéciaux excepté : [-' ] (tiret apostrophe espace) |

**Tableau 24 : représentant légal du patient**

Le jeu de valeurs à utiliser pour coder la qualité du représentant légal est défini dans le fichier « ASIP-SANTE_QualiteRepresentantLegal_20180326_DMP.xml » publié dans l'espace Industriels. Cf. [FI-JEUX-VALEURS].
Cette liste de codes est susceptible d'évoluer (cf. REC_GEN-1370 § 5.2.4.8).

# 5 ÉLEMENTS TECHNIQUES

## 5.1 Présentation des standards, normes, référentiels

### 5.1.1 Le cadre d'interopérabilité des SIS

Les spécifications des interfaces avec le DMP s'appuient sur le cadre d'interopérabilité des systèmes d'information de santé de l'ANS définissant les standards (techniques, sémantiques et de sécurité) à utiliser dans les échanges de données de santé dans le contexte français.

La structuration standardisée des documents, spécifiée dans le CI-SIS contribue au développement de nouveaux usages et de nouvelles fonctionnalités par les éditeurs de LPS.

Par rapport au CI-SIS, le projet DMP s'inscrit dans le partage de contenus d'informations de santé (documents médicaux persistants) ; le LPS est le système source (parfois aussi appelé système initiateur) et le DMP est le système cible.

Cf. documents du CI-SIS dans l'annexe 4.

**Documents importants du CI-SIS**

Le CI-SIS fait en effet référence à des standards et recommandations internationaux (XDS, HL7…) que le lecteur devra maîtriser.

Pour le lecteur de profil développeur ou consultant, la lecture des documents listés ci-après permet également d'acquérir les connaissances techniques minimales pour être en mesure de rendre un LPS interopérable avec le DMP (cette lecture pourra se faire après la lecture de la présente spécification) :

- [CI-TR-CLI-LRD] Couche Transport Volet Synchrone Client Lourd ;
- [CI-GESTPAT] Couche Service Volet Gestion de Dossier Patient Partagé ;
- [CI-PARTAGE] Couche Service Volet Partage de Documents de Santé ;
- [CI-STRU-ENTETE] Couche Contenu Volet Structuration Minimale.

**Jeux de valeurs à utiliser**

Les jeux de valeurs sont décrits dans [FI-JEUX-VALEURS].

Ces jeux de valeurs sont :

- les classes de documents (classCode XDS), les types de documents (typeCode XDS) et le format de documents (formatCode XDS) ;
- la profession/spécialité (authorSpecialty XDS) qui peut être lue en carte CPx mais qui peut nécessiter un transcodage entre le code lu dans la CPx et le code décrit dans [CI-ANX-PS-STRU] ; dans le cas où la valeur est paramétrée dans le LPS (authentification indirecte par exemple), prendre la valeur la plus adaptée.
- le cadre d'exercice (practiceSettingCode XDS) qui peut être paramétré au niveau du LPS et le secteur d'activité (ou modalité d'exercice) (healthcareFacilityTypeCode XDS) qui peut être lu en carte CPx mais qui peut nécessiter un transcodage entre le code lu dans la CPx et le code décrit dans [CI-ANX-PS-STRU] ; dans le cas où la valeur est paramétrée dans le LPS (authentification indirecte par exemple), prendre la valeur la plus adaptée.
- type d'activité clinique (contentTypeCode XDS) ; dans le cas où la valeur est paramétrée dans le LPS (authentification indirecte par exemple), prendre la valeur la plus adaptée.

Les tables de transcodage des spécialités et des secteurs d'activité entre ADELI et RPPS sont dans [TRANS-ADELI-RPPS].

**Correspondances à respecter**

Le CI-SIS impose certaines règles de correspondances entre les valeurs des jeux de valeurs.

- Correspondance entre Classe et Type de document

La table de correspondance ASS_X16-CorrespondanceType-Classe-DMP du [FI-JEUX-VALEURS] contient la liste des correspondances possibles entre la classe de documents et le type du document. Par exemple :

| Classe | Type |
|---|---|
| 10 – Comptes rendus | 11488-4 CR ou fiche de consultation ou de visite |
| 10 – Comptes rendus | 11528-7 CR d'imagerie médicale |
| 11 - Synthèses | SYNTH Synthèse |

Par contre, il n'y a pas de table décrivant la correspondance précise entre le type de document et le format du document.

### 5.1.2 Le profil IHE XDS.b

La gestion des documents du DMP et 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 rentrant 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. Note : Par rapport à l'acteur IHE standard, les transactions registerDocumentSetb ainsi que les transactions ITI-44 ne sont pas accessibles à des systèmes externes au DMP sur la Registry 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 :

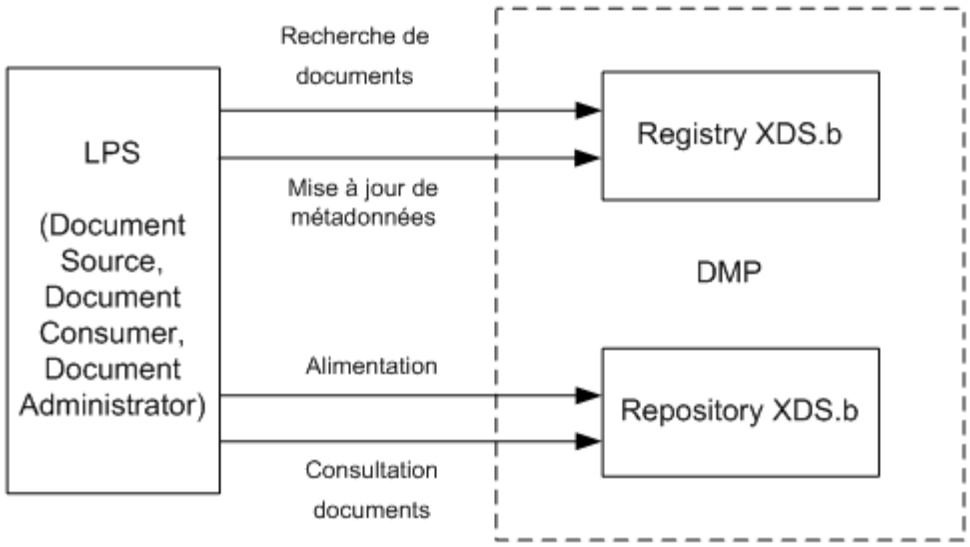



**Figure 25 : schéma de principe des acteurs XDS**

#### *Domaine d'affinité XDS (XDS Affinity Domain)*

Le domaine d'identification des patients au sein du DMP est l'INS : voir la métadonnée patientId dans [CI-PARTAGE].

Les jeux de valeurs associés au domaine d'affinité XDS sont définis dans [FI-JEUX-VALEURS].

Le DMP n'impose pas la mise en œuvre stricto sensu du profil IHE ATNA, groupé habituellement avec le profil XDS.b :

- les considérations d'authentification (« node authentication ») sont définies au §5.3.1,
- les considérations d'audit (« audit trail ») ne sont pas imposées au LPS ; l'audit est réalisé directement par le système DMP qui génère ses propres traces fonctionnelles et techniques (service d'audit du DMP) à la réception des flux. Le LPS peut néanmoins s'il le souhaite générer ses propres traces vers un « audit repository » de son choix (y compris lui-même).

#### *Les métadonnées XDS*

L'Alimentation qui met en œuvre le profil IHE XDS.b et la gestion des métadonnées des documents XDS est décrite au §3.4.1.1.3.

La Consultation utilisant également ce profil, les références décrites dans ce paragraphe s'appliquent également.

#### *Code exemple et aides*

Des exemples de messages XDS-b sont fournis en annexe A6-3.

Les documents [CI-PARTAGE] et [IHE-TF3] synthétisent les métadonnées des documents / lots XDS (nom, valeurs, types de données, entryUUID, statuts, codes erreurs XDS…).

***Gestion des erreurs***

La gestion des erreurs est conforme au profil IHE XDS.b, à la nuance suivante : le statut « urn:ihe:iti:2007:ResponseStatusType:PartialSuccess » n'est pas géré.

Le document de référence sur ce sujet est IHE TF3. Cf. chapitre 4.1.13.

Dans le cadre du DMP, le champ codeContext est structuré de la manière suivante : [;Info1[,Info2…]]

Les informations complémentaires (Info1, Info2, etc.) dépendent de la nature de l'erreur. Il peut s'agir par exemple d'un identifiant de document.

***Exemple : paramètre obligatoire manquant pour une recherche dans la registry.***

```
<RegistryResponse
xmlns="urn:oasis:names:tc:ebxml-regrep:registry:xsd:2.1"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure">
    <RegistryErrorList>
       <RegistryError errorCode="XDSStoredQueryMissingParam"
       codeContext="paramètre manquant : $XDSDocumentEntryPatientId"
       location="XDSRegistryAdaptor.registryStoredQuery"
       severity="Error" />
    </RegistryErrorList>
</RegistryResponse>
```

## 5.2 Architecture du système d'information

La mise en œuvre du service DMP dépend du métier géré par le LPS. Les besoins d'un Logiciel de cabinet (LGC) ne sont pas les mêmes que ceux d'un Système d'Information de Radiologie (SIR) ou de la Gestion Administrative des Malades (GAM) d'une structure de soins.

Dans ce chapitre, plusieurs types d'intégration du service DMP dans les systèmes d'information de l'utilisateur sont illustrés :

- Architecture LPS autonome ;
- Architecture dans une structure de soins ;
- Architecture des connecteurs EAI ;
- Architecture en mode Saas ;
- Architecture minimale.

Quelle que soit la solution d'architecture retenue, le LPS doit être conforme à la PGSSI-S de l'ANS (https://esante.gouv.fr/offres-services/pgssi-s).

Les architectures présentées dans ce chapitre ne représentent pas l'exhaustivité des solutions d'intégration possibles.

## 5.2.1 Architecture DMP-compatible

### 5.2.1.1 LPS autonome

Ce type d'architecture correspond, par exemple, au LGC.

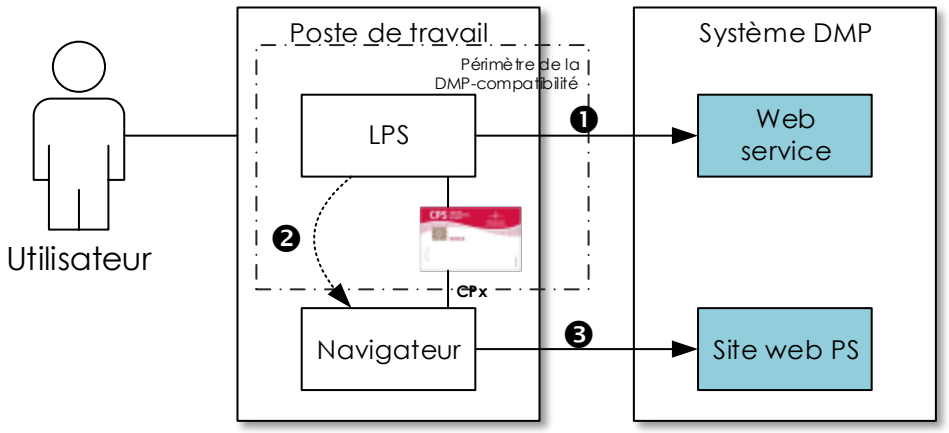



**Figure 26 : LPS autonome**

❶ L'utilisateur utilise sa carte CPx pour s'authentifier directement auprès du système DMP grâce à son LPS. Il soumet ensuite ses requêtes web-service au système DMP.

❷ S'il est nécessaire d'accéder au site web PS, le LPS forge une URL et la transmet à un navigateur web. Ce dernier peut être intégré au LPS, mais il peut être le navigateur par défaut de l'OS.

❸ Le navigateur soumet la requête HTTP au site web PS sur une liaison sécurisée TLS en authentification mutuelle sur la base du certificat de la carte CPx et de celui du site web PS. Le code porteur de la CPx est demandé à chaque ouverture du navigateur (la première fois ou les fois suivantes s'il a été fermé entre temps).

### 5.2.1.2 Structure de soins

Ce type d'architecture s'applique de façon générale aux structures utilisant des certificats logiciels de personne morale. Mais, comme dans le cas précédent, il est tout à fait possible pour une structure de soins de n'utiliser que des CPx pour ses transactions.

La structure de soins doit au préalable acquérir deux certificats logiciels de personne morale de l'IGC Santé de l'ANS :

- un certificat d'authentification pour réaliser les fonctions d'authentification ;
- un certificat de cachet pour réaliser les fonctions de signature électronique.

Le choix des certifcats est lié au mode d'authentification indirecte et au mode AIR (cf. chapitre 2.2.1).

- Mode EJ ou mode EJ/EG : certificats de l'entité juridique.
- Mode EG : certificats de l'entité géographique.

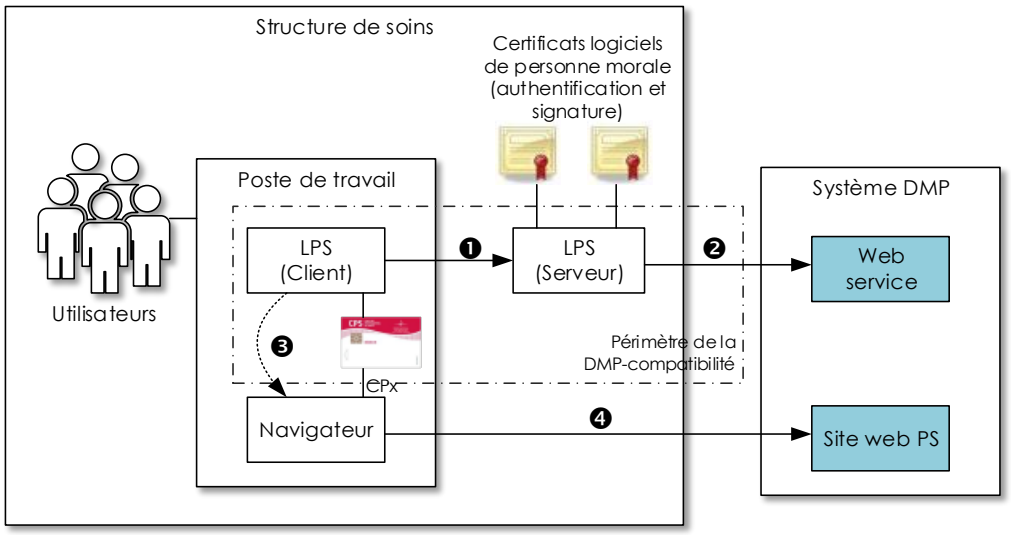



**Figure 27 : structure de soins (mode AIR non illustré pour l'accès au site web PS)**

❶ L'utilisateur s'authentifie sur un LPS hébergé au sein d'une structure de soins.

❷ La structure de soins s'authentifie auprès du système DMP avec son certificat logiciel d'authentification pour personne morale puis soumet ses requêtes web-service au système DMP. Ici, l'authentification de l'utilisateur est dite indirecte, car seule la structure de soins est capable de la réaliser.

❸ S'il est nécessaire d'accéder au site web PS, le LPS forge une URL et la transmet à un navigateur web. Ce dernier peut être intégré au LPS, mais il peut être le navigateur par défaut de l'OS.

❹ La liaison entre le site web PS et le navigateur est directe. Le poste de travail doit avoir accès à une connexion internet et à une carte CPx ou au mode AIR.

- Le navigateur soumet la requête HTTP au site web PS sur une liaison sécurisée TLS en authentification mutuelle sur la base du certificat de la carte CPx et de celui du site web PS. Le code porteur de la CPx est demandé à chaque ouverture du navigateur (la première fois ou les fois suivantes s'il a été fermé entre temps).
- Pour l'accès au site web PS en mode AIR, cf. TD0.10 au chapitre 5.5.

### 5.2.1.3 Cas des « Connecteurs / EAI »

Les LPS de type « Connecteur » (ou EAI, module ou solution « externe ») permettent à un ou plusieurs autres « LPS tiers » d'échanger, de collecter ou de concentrer des données, puis de s'interfacer avec le SI DMP afin d'alimenter, voire consulter le DMP. Ces composants logiciels interviennent le plus souvent dans les structures de soins pour pallier les problèmes d'interopérabilité liés à l'hétérogénéité des applications existantes.

Avertissement : du point de vue du GIE SESAM-Vitale, sont considérés comme « connecteurs / EAI » les solutions logicielles commercialisées en tant que telles, et non les modules techniques utilisés en interne par un éditeur pour ses propres solutions.

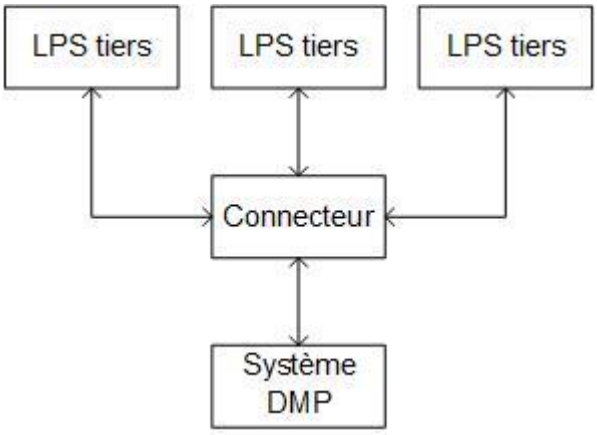



**Figure 28 : schéma fonctionnel du connecteur**

De par leur positionnement en termes de mise en œuvre, ces « connecteurs / EAI » sont admissibles à l'homologation à la DMP-compatibilité, moyennant certains aménagements en termes de prise en compte des exigences de DMP-compatibilité. En effet, ces logiciels n'étant pas directement en contact avec l'utilisateur final, certaines exigences peuvent (ou doivent) être déléguées contractuellement au « LPS tiers ».

La liste des exigences de DMP-compatibilité pouvant ou devant être déléguées est fournie dans l'annexe [PDV-HOMOLOGATION].

#### 5.2.1.4 Cas des logiciels en mode SaaS

L'utilisation d'un logiciel en mode SaaS suppose un accès distant de l'utilisateur final au logiciel et aux données de santé à caractère personnel gérées par ce logiciel.

Les données de santé à caractère personnel recueillies ou produites par l'utilisateur final du logiciel se retrouvent ainsi hébergées chez un tiers.

L'article L 1111-8 du code de la santé publique dispose que « les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet. Cet hébergement de données, quel qu'en soit le support, papier ou informatique, ne peut avoir lieu qu'avec le consentement exprès de la personne concernée ».

Les conditions d'hébergement de données de santé à caractère personnel sur support informatique ont été précisées par le décret 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel (codifié aux articles R 1111-9 à R 1111-15-1 du code de la santé publique). Ainsi, conformément à l'article L 1111-8 du code de la santé publique et au décret du 4 janvier 2006, toute personne physique ou morale hébergeant des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic ou de soins pour le compte d'un tiers, doit être agréée par décision du ministre en charge de la santé qui se prononce après avis de la CNIL et d'un comité d'agrément (organe consultatif créé par le décret 2006-6 sus-cité).

L'alternative suivante s'offre à l'éditeur de logiciels en mode SaaS pour l'hébergement des données de santé à caractère personnel :

- Être soi-même agréé pour l'hébergement de données de santé à caractère personnel ;
- Confier l'hébergement des données de santé à caractère personnel à un hébergeur agréé à cet effet.

Il convient de rappeler que des contrôles diligentés par la CNIL ou par l'IGAS peuvent être conduits pour s'assurer du respect des conditions de l'agrément et que le non-respect de l'obligation d'agrément est assorti de sanctions pénales.

L'ensemble des informations relatives à la procédure d'agrément ainsi que la liste des hébergeurs agréés sont disponibles sur le site de l'ANS : https://esante.gouv.fr/offres-services/hds/liste-des-herbergeurs-agrees

### 5.2.2 Architecture minimale hors DMP-compatibilité

Ce type d'architecture correspond à l'intégration de la seule transaction TD0.9 « Accès Web-PS Contextuel ». Ce type d'intégration minimale ne nécessite pas de passage en processus d'homologation de la DMP-compatibilité.

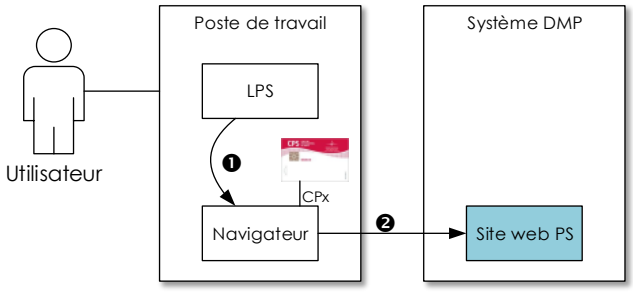



**Figure 29 : architecture minimale hors DMP-compatibilité**

❶ S'il est nécessaire d'accéder au site web PS, le LPS forge une URL et la transmet à un navigateur web. Ce dernier peut être intégré au LPS, mais il peut être le navigateur par défaut de l'OS.

❷ Le navigateur soumet la requête HTTP au site web PS sur une liaison sécurisée TLS en authentification mutuelle sur la base du certificat de la carte CPx et de celui du site web PS. Le code porteur de la CPx est demandé à chaque ouverture du navigateur (la première fois ou les fois suivantes s'il a été fermé entre temps).

### 5.2.3 Architecture minimale pour l'accès Web-PS Contextuel en mode AIR

Ce type d'architecture correspond à l'intégration de la seule transaction TD0.10 « Accès Web-PS Contextuel en mode AIR ». Ce type d'intégration minimale nécessite un passage en processus d'homologation de la DMP-compatibilité.

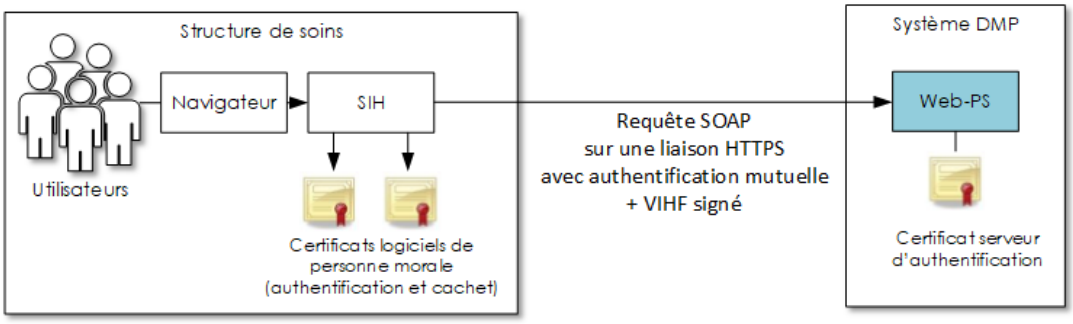



**Figure 30 : architecture minimale (mode AIR)**

NB : le schéma ci-dessus illustre le cas des SIH. Le mode AIR peut cependant s'appliquer au système d'information (SI) d'autres types de structure de soins.

Cf. TD0.10 au chapitre 5.5 pour plus d'informations sur l'accès Web-PS contextuel en mode AIR.

### 5.2.4 Configuration du système d'information de l'utilisateur

#### 5.2.4.1 Connexion internet

L'accès au système DMP nécessite une connexion à internet.

Cet accès ne s'effectue pas nécessairement entre le poste de travail de l'utilisateur et le système DMP. C'est le cas par exemple d'un LPS avec une architecture client/serveur en structure de soins.

Par contre, dès lors qu'un LPS ou un navigateur du poste de travail doit accéder au système DMP, ce poste de travail doit disposer d'une connexion internet.

Dans le cas où l'accès à internet est conditionné par la connexion préalable à un dispositif de restriction et/ou de sécurisation des accès internet (firewall, proxy), ce dispositif devra être en capacité de laisser passer les flux HTTP/TLS du DMP (ouverture éventuelle de l'accès aux URL du DMP, port TLS, etc.).

Pour une utilisation normale du système DMP, une ligne internet haut débit est nécessaire.

### 5.2.4.2 (sans objet)

### 5.2.4.3 Dispositifs matériels de lecture de cartes

Pour les LPS nécessitant un dispositif de lecture de cartes (CPx ou Vitale), le poste doit être équipé :

- d'un lecteur homologué SESAM-Vitale (Terminal Lecteur) ;
- ou d'un (ou deux) lecteur(s) PC/SC :
  - un lecteur si le LPS ne lit qu'une seule carte (carte Vitale seule ou carte CPx seule),
  - deux lecteurs en parallèle si le LPS lit la carte CPx et la carte Vitale.

### 5.2.4.4 Dispositifs logiciels de lecture des cartes

#### Cartes CPx

Le document de référence [CI-TR-CLI-LRD] spécifie les composants à utiliser pour la lecture des cartes CPx.

L'ANS fournit un middleware (librairies cryptographiques `CryptoLib`) permettant de lire les cartes CPx et d'établir des liaisons sécurisées TLS mutuelles.

Cette librairie cryptographique `CryptoLib` et son module `PKCS11` s'interfacent avec les composants standards de gestion de connexion TLS.

**EX_GEN-1480**

Le composant PKCS#11 de la Cryptolib CPS v4 ne doit plus être utilisé pour la signature des jetons VIHF et pour l'établissement de la connexion TLS sécurisée par CPx.

De même, si vous utilisez les API CPS dans ce cadre, celles-ci ne doivent plus être utilisées.

Il est nécessaire d'utiliser la version minimale de référence de la Cryptolib indiquée par le CNDA ou le GIE SESAM-Vitale et disponible sur le portail Espace Industriel du GIE SESAM-Vitale.

#### Carte Vitale et ApCV

**EX_GEN-1410**

Si le LPS intègre la lecture de la carte Vitale, il utilise :

- des API Lecture Vitale (pour un poste hors facturation S/V) (v.6.10 a minima),
- ou des API SSV (poste de facturation S/V) (CDC 1.40 a minima),

Si le LPS intègre la lecture de l'ApCV, il utilise le service de demande d'authentification et gestion du contexte ApCV [ApCV-SFG-004] [ApCV-MP-001].

Le LPS peut également implémenter le référentiel Lecture Vitale [RHCVIT] 5.02.01 et supérieur afin d'accéder aux cartes Vitale en alternative des API lecture Vitale et SSV ou bien si ces dernières ne sont pas disponibles sur l'environnement d'exécution du LPS.

**REC_GEN-1420**

Il est recommandé à l'éditeur qui souhaite intégrer la lecture d'une carte Vitale dans son LPS d'utiliser la dernière version des API de lecture Vitale. Les informations sur les API de lecture de carte Vitale sont disponibles sur le site du GIE SESAM-Vitale : `http://www.sesam-vitale.fr`

**EX_GEN-1430**

Les cartes Vitale de test (cartes de couleur blanche dédiées aux tests éditeurs) ou de démonstration (cartes de couleur verte avec "démonstration" indiqué en diagonale) ne doivent pas être utilisées sur l'environnement DMP de production. Les LPS doivent contrôler le type de carte Vitale remonté par l'API exploitation de la carte Vitale (EX_GEN-1410) et bloquer l'accès à l'environnement DMP de production pour ces types de cartes.

Cette exigence s'applique également aux ApCV de test et de démonstration.

#### 5.2.4.5 OID racine unique par instance du LPS

La production et la gestion de données dans le contexte DMP - comme tout échange de données de santé utilisant des standards internationaux tels que HL7 ou XDS - nécessitent la génération d'identifiants universels (mondialement uniques) pour certains concepts (identifiant de patient local, identifiant de personne, de structure, identifiant unique de document …).

Les standards utilisent pour cela des identifiants d'objets ISO (OID).

Selon HL7 France :

> « Dans l'arbre ISO (hiérarchie) des OID construits à partir d'une racine, chaque organisation/objet est identifiée par le nœud supérieur, et identifie à son tour les nœuds inférieurs.
>
> Un OID est une séquence de nombres entiers positifs séparés par des points (sans zéros non significatifs). Les OID sont alloués de manière hiérarchique de telle manière que seule l'autorité qui a délégation sur la hiérarchie "`1.2.3`" peut définir la signification de l'objet "`1.2.3.4`".
>
> Un OID est formé en concaténant à partir de la racine unique, les différents nœuds parcourus dans l'arbre pour atteindre l'objet identifié par cet OID. Chaque nœud possède un identifiant numérique. Le détenteur d'une racine d'OID (ex. : `1.2.3`) peut décliner autant de sous-branches qu'il le souhaite.
>
> L'AFNOR gère une branche d'OID identifiée « `1.2.250.1` ». Elle propose aux organisations françaises un service d'attribution d'OID sous cette branche. Des organisations autres que l'AFNOR proposent ce service, comme DICOM, HL7-US…»

La longueur d'un OID est limitée à 128 caractères.

Par exemple, une organisation ayant commandé à l'AFNOR un OID numérique (ex. : 999) aura un OID racine `1.2.250.1.999`.

**EX_GEN-1340**

L'éditeur doit disposer des racines d'OID nécessaires avant de commencer les démarches de DMP-compatibilité.

### 5.2.4.6 Unicité des identifiants d'objets générés par le LPS

**EX_GEN-1350**

Chaque identifiant généré doit être mondialement unique. À cette fin, l'instance du LPS installé chez l'utilisateur ou dans la structure doit posséder un OID racine qui lui est propre. La présente spécification n'impose aucune règle de génération de cet OID racine (ni de la déclinaison de celui-ci), si ce n'est qu'il doit être unique par instance du LPS. Il appartient à l'éditeur de s'assurer de la rigueur de sa méthode de génération d'identifiants uniques d'objets et du respect de l'exigence.

À titre d'exemple, un identifiant unique d'objet peut être obtenu :

- soit en utilisant une racine d'OID propre à l'éditeur du LPS, que celui-ci décline pour chaque LPS installé chez ses clients ;
- soit en utilisant l'OID propre à une structure, si celle-ci en possède une (ex. : un CHU peut déjà posséder un OID pour ses besoins internes) ;
- soit en générant une racine OID à partir d'un UUID 128 bits hexadécimal converti en décimal sous la branche `2.25` dédiée à cet usage par l'ITU (http://www.itu.int/ITU-T/asn1/uuid.html) ; exemple : `2.25.329800735698586629295641978511506172918`

Exemple possible d'implémentation avec un OID propre à l'éditeur :

- OID commandé par l'éditeur « Editeur-lambda » auprès de l'AFNOR : `1.2.250.1.999`
- OID du LPS « LPS-alpha » de l'éditeur « Editeur-lambda » : `1.2.250.1.999.1`
- OID de l'instance du « LPS-alpha » de l'« Editeur-lambda » installé dans le « Cabinet Dr Dupont » : `1.2.250.1.999.1.432`
- OID des identifiants uniques de documents gérés au sein du LPS « LPS-alpha » : `1.2.250.1.999.1.432.1`
- OID complet d'un identifiant de document : `1.2.250.1.999.1.432.1.98765`
- OID des identifiants de patients locaux gérés au sein du LPS « LPS-alpha » : `1.2.250.1.999.1.432.2`
- OID complet d'un identifiant patient local : `1.2.250.1.999.1.432.2.3456`

### 5.2.4.7 Encodage de caractères

**EX_GEN-1355**

Les messages doivent être encodés en UTF-8.

### 5.2.4.8 Gestion des jeux de valeurs et des référentiels

Le service de partage de documents médicaux du DMP utilise des jeux de valeurs qui doivent être facilement paramétrables et extensibles dans le LPS.

**EX_GEN-1360**

Compte tenu du caractère évolutif des jeux de valeurs, ceux-ci doivent être paramétrables dans le LPS par l'éditeur. La modification d'un jeu de valeurs ne doit pas perturber le fonctionnement du LPS.

**REC_GEN-1370**

Il est recommandé que le LPS soit en capacité d'intégrer une valeur en provenance du DMP qui n'est pas encore connue du LPS et de l'ajouter à son référentiel de valeurs.

#### 5.2.4.9 Synchronisation du temps

**EX_GEN-1460**

Quel que soit le profil de DMP-compatibilité choisi, le poste de travail (ou le « composant logiciel » communicant avec le système DMP s'il ne s'agit pas directement du poste de travail de l'utilisateur) doit être à l'heure, pour des problématiques d'horodatage des données médicales, de traçabilité et de pertinence de certains critères de recherche concernant la date.

Un délai trop long entre deux synchronisations (par exemple 1 fois par semaine) peut se révéler insuffisant dans la mesure où un décalage de plus de 3 secondes est rejeté par le système DMP (erreur `SOAP:Fault` contenant le message d'erreur du système DMP).

La synchronisation de temps doit se faire suivant la transaction IHE « Maintain Time » du profil IHE « Consistent Time » (CT : [IHE-TF1] § 2.2.7 et [IHE-TF2A] § 3.1). Ce profil utilise le protocole NTP. L'éditeur peut par exemple utiliser le pool de serveurs de temps français[11] « `fr.pool.ntp.org` ».

#### 5.2.4.10 Confidentialité du numéro d'homologation du LPS

Le LPS conforme à la DMP-compatibilité reçoit un numéro d'homologation qui est contrôlé lors de l'accès au DMP.

**EX_GEN-1490**

L'éditeur homologué à la DMP-compatibilité s'engage à garder secret le numéro d'homologation attribué par le CNDA et à se prémunir de la mise en œuvre de ce numéro dans d'autres logiciels que ceux référencés dans la famille de produit homologuée à laquelle est rattaché ce numéro.

## 5.3 TD0.1 Accès sécurisé au système DMP

L'accès aux interfaces SOAP des web-services du système DMP s'appuie sur le document [CI-TR-CLI-LRD] du CI-SIS

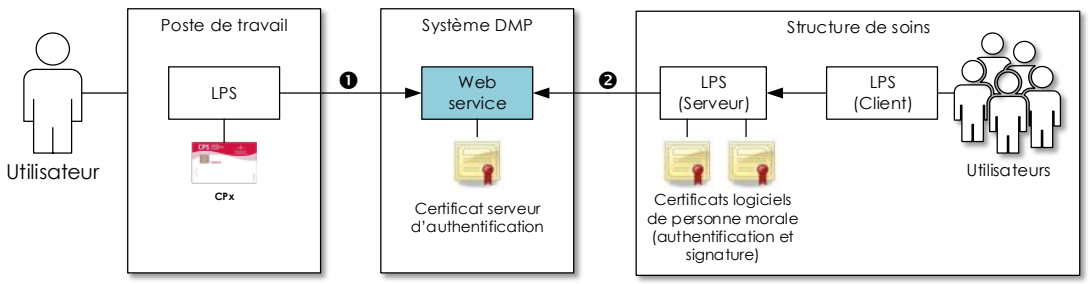



**Figure 31 : accès sécurisé (mode AIR non illustré)**

[11] L'éditeur qui souhaiterait utiliser ce pool de serveurs de temps est invité à se rapprocher du fournisseur du service pour en connaître les conditions d'utilisation et les engagements en termes de niveaux de services.

L'authentification de l'utilisateur sur le système DMP (authentification de l'utilisateur dans le cas d'une authentification directe ou de la structure de santé dans le cas d'une authentification indirecte) est un prérequis transversal à l'appel de toute fonction web-service DMP.

Il existe trois modes d'authentification au système DMP :

❶ *Authentification directe* : l'utilisateur utilise sa carte CPx pour s'authentifier directement auprès du système DMP. Cf. chapitre

❷ *Authentification indirecte* : l'utilisateur se connecte à un LPS hébergé au sein d'une structure de soins qui s'authentifie auprès du DMP au moyen d'un certificat logiciel d'authentification pour personne morale.

❸ *Authentification indirecte renforcée (AIR)* permet de mettre en œuvre des moyens d'authentification alternatifs à la CPS pour la consultation du DMP.

Le système DMP ne prend par en charge l'authentification par délégation définie dans le CI-SIS.

## 5.3.1 Exigences générales

### 5.3.1.1 Liaison sécurisée

Le LPS doit se conformer aux exigences de transport et de sécurisation des flux, visant à assurer l'intégrité, la confidentialité et l'imputabilité du contenu de chaque DMP, exprimées dans le document [CI-TR-CLI-LRD].

La mise en œuvre de la sécurité doit se conformer à l'ensemble des dispositions de sécurité des volets du CI-SIS implémentés par la présente spécification.

La connexion au système DMP depuis un LPS est assurée par l'établissement d'un canal TLS avec authentification mutuelle entre le LPS et le serveur DMP.

**EX_0.X-1030**

L'accès au système DMP exige l'établissement d'une liaison TLS sécurisé en version TLS 1.2.

Afin de conserver un niveau de sécurité suffisant (cf. Guide TLS du référentiel RGS de l'ANSSI), le LPS doit mettre en oeuvre une ou plusieurs des suites cryptographiques suivantes, qui sont les seules supportées par le serveur DMP (notation IANA) :

Les suites cryptographiques supportées sont listées dans la fiche d'information PDT-INF-579 - Référentiel des suites cryptographiques supportées par le système DMP.

**EX_0.X-1031**

Le LPS doit supporter l'extension TLS "SNI" (Server Name Indication). Le SNI est décrit par la section 3.1 de la RFC 4366 Transport Layer Security (TLS) Extensions (https://tools.ietf.org/html/rfc4366#section-3.1 ).

Pour information complémentaire voir https://fr.wikipedia.org/wiki/Server_Name_Indication

**Comptes à rebours – timer d'inactivité et timer de renégociation**

Le système DMP met en œuvre deux comptes à rebours (timer) sur le système de gestion des connexions sécurisées TLS. Ces deux timers démarrent lors de la connexion et sont remis à zéro selon des critères qui leur sont propres, définis ci-dessous :

- le premier, appelé « timer d'inactivité », provoque une coupure de la connexion TLS et du socket TCP/IP courant lorsqu'il arrive à son terme. Ce timer permet au système DMP de désallouer les ressources systèmes bloquées par une connexion inactive. Ce timer est remis à zéro à chaque fois que l'utilisateur connecté envoie une commande (via HTTP) au système DMP sur le socket courant ;

- le second, appelé « timer de renégociation », permet de contrôler régulièrement la présence de la modalité d'authentification cliente (carte CPx ou certificat de personne morale) et vient en complément du contrôle d'arrachage de la modalité qui doit être effectué coté client (opération décrite ci-après). Lorsqu'il arrive à son terme, il bloque l'exécution des commandes sur le système DMP et conditionne leur déblocage à l'exécution d'une opération de renégociation TLS.

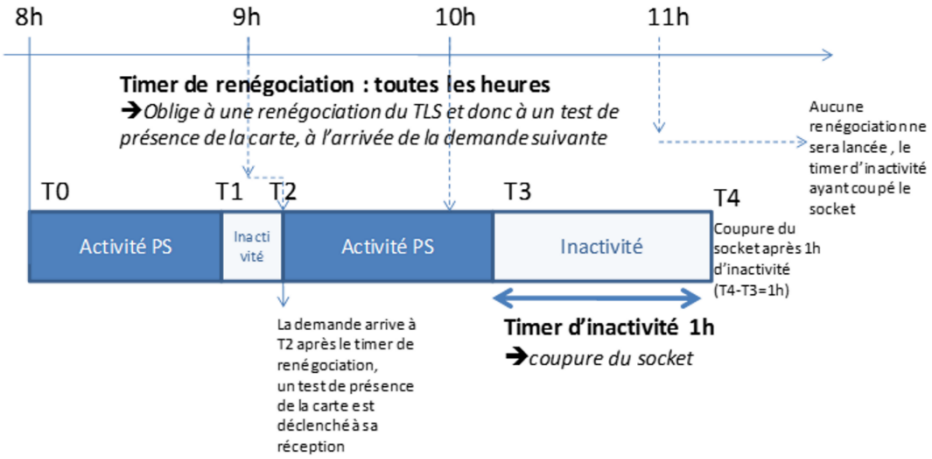



**Figure 32 : timer de renégociation et timer d'inactivité**

À ce stade, il est important de noter qu'il existe un timer d'inactivité par socket TCP/IP et un unique timer de renégociation pour tous les sockets TCP/IP ouverts par un même client (via la notion de session TLS).

Le système DMP met en œuvre ces deux timers sur un compte à rebours d'une heure : une heure depuis la dernière activité sur le socket courant pour le timer d'inactivité et une heure depuis la première connexion ou la dernière renégociation pour le timer de renégociation. Ces deux valeurs ont été choisies pour offrir le meilleur compromis performance/sécurité pour l'utilisateur.

En prenant par exemple pour hypothèse qu'une consultation dure en moyenne 20 minutes : pour le timer d'inactivité, cela permet de couper les connexions qui sont restées inutilisées alors que deux ou trois patients ont consulté le professionnel sans que celui-ci n'utilise le DMP.

**REC_0.X-1035**

Pour garantir la meilleure expérience utilisateur possible, le LPS doit gérer correctement la coupure du canal TLS par le système DMP (timer d'inactivité et timer de renégociation du canal TLS).

#### 5.3.1.2 Vérification du certificat serveur d'authentification du système DMP

Le certificat serveur des interfaces SOAP du système DMP est émis par l'IGC Santé de production. Une notice de présentation de l'IGC Santé est disponible sur https://industriels.esante.gouv.fr/.

**EX_0.X-1070**

Le LPS doit être en capacité de valider le certificat serveur du système selon la norme PKIX (voir RFC3280 sur http://tools.ietf.org/html/rfc3280 et RFC5280 surhttp://tools.ietf.org/html/rfc5280).

**REC_0.X-1090**

Il est recommandé de faire un contrôle de révocation des certificats serveur du système DMP.

**Certificat racine (AC) et listes de révocation des certificats (CRL)**

Le certificat utilisé par le système DMP est un certificat d'authentification serveur de la gamme élémentaire IGC Santé (SSL_SERV_SSL), fils de l'AC nommée "ACI-EL-ORG" elle-même fille de l'AC "ACR-EL". Les ressources liées à ces deux AC sont donc nécessaires pour valider le certificat du SI-DMP.

Les informations et ressources (fichiers) sur les Autorités de Certification (AC) sont disponibles sur le site http://igc-sante.esante.gouv.fr/PC/ dans la rubrique « Certificats d'autorités ».

Pour les LPS mettant un œuvre un contrôle de non-révocation des certificats basés sur les CRL, deux solutions sont possibles :

1. Utiliser le répondeur OCSP (Online Certificate Status Protocol) disponible pour l'IGC Santé
2. Télécharger régulièrement les CRL puis les utiliser de manière programmatique lors de la validation (en général en installant ou passant en paramètre les CRLs dans le composant technique de validation de certificat) ; les CRL du domaine Organisations de la gamme Elémentaire sont disponibles aux adresses suivantes :

- URL HTTP : http://igc-sante.esante.gouv.fr/CRL/ACI-EL-ORG.crl
- URL ldap : ldap://annuaire-igc.esante.gouv.fr/cn=AC IGC-SANTE ELEMENTAIRE ORGANISATIONS, ou=AC RACINE IGC-SANTE ELEMENTAIRE,ou=IGC-SANTE,ou=0002 187512751, o=ASIP-SANTE,c=FR?certificaterevocationlist;binary?base?objectClass=pkiCA
- URL ldap des delta CRL : ldap://annuaire-igc.esante.gouv.fr/cn=AC IGC-SANTE ELEMENTAIRE ORGANISATIONS, ou=AC RACINE IGC-SANTE ELEMENTAIRE,ou=IGC-SANTE,ou=0002 187512751, o=ASIP-SANTE,c=FR?deltarevocationlist;binary?base?objectClass=pkiCA

Les CRL IGC Santé sont publiées quotidiennement et sont valables 7 jours.

**REC_0.X-1100**

Pour assurer la sécurité des applications intégrant des certificats d'AC il est recommandé de comparer l'empreinte numérique des clés utilisées avec une source de confiance.

Les fichiers (clés) des AC et "`ACR-EL`" "`ACI-EL-ORG`" peuvent être récupérés à l'URL citée ci-dessus, et déployés avec le LPS.

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

- Automatiquement (dans la majorité des cas) par la librairie ou le composant logiciel de gestion des connexions TLS :
  - 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 certificat (autorités de confiance) propre au composant de connexion (cas de Java par exemple)
  - soit en intégrant ces fichiers dans le magasin des autorités de confiance de l'OS, utilisé par le composant (cas de Microsoft .Net par exemple).
- Manuellement, en comparant les empreintes ; pour les calculer :
  - cette information est calculée automatiquement par la visionneuse de certificat Windows (onglet "Détail", "<tout>", dernière ligne) ;

- vous pouvez utiliser la commande "`openssl X509 -fingerprint`" sur le fichier certificat ;
- vous pouvez utiliser les commandes "`sha1sum`" ou "`sha256sum`" sur le certificat dans sa forme DER.

Pour effectuer ce contrôle, le simple téléchargement du certificat du serveur DMP (par exemple depuis un environnement de test éditeur) constitue une mauvaise pratique. Il est demandé de bien valider le certificat à l'aide de sa racine ACI-EL-ORG. En effet, l'ajout du certificat du serveur DMP comme autorité de confiance dans le LPS (ou dans le système d'exploitation) n'est pas adaptée, car, à terme lors du renouvellement du certificat du serveur DMP (tous les 3 ans), cette mesure obligerait à mettre à jour tous les LPS déployés sur les postes de travail.

Pour l'accès au site web PS, le certificat serveur est émis par une IGC prise en charge automatiquement par les navigateurs récents lors de l'ouverture de l'accès Web PS (le LPS n'a pas besoin de valider cette IGC).

### 5.3.1.3 Gestion des redirections HTTPS 3xx

Le système DMP peut rediriger une requête HTTPS du LPS vers une autre URL.

**EX_0.X-1055**

Pour garantir le fonctionnement du système, le LPS doit savoir gérer les redirections HTTPS 3xx émises par le système DMP.

### 5.3.1.4 Le jeton VIHF

**EX_0.X-1060**

Un jeton SAML 2.0 (nommé VIHF, « Vecteur d'Identification et d'Habilitation Formelles ») doit transiter dans les messages.

Les données du VIHF (voir le § 4.3.1.5 « Contenu du jeton VIHF » de [CI-TR-CLI-LRD]) doivent être renseignées dans l'en-tête de chaque message SOAP transitant vers le système DMP.

La durée de vie du jeton VIHF est de 1 heure (voir champ `//Assertion/@IssueInstant`).

Le processus d'authentification peut renvoyer des codes d'erreur liés au traitement du VIHF sous forme de « `SOAP Fault` » (voir le § 4.3.1.7 « Codes d'erreurs liés au processus d'authentification et d'habilitation » de [CI-TR-CLI-LRD] et l'annexe A7-3 « Erreurs spécifiques du processus d'authentification »).

**Connexion secrète**

**EX_0.1-1100**

Le LPS doit permettre à l'utilisateur de mettre en œuvre une connexion secrète pour les mineurs, en concertation avec son patient. Cf. donnée `confidentiality-code` dans le VIHF.

Les modalités de mise en œuvre : détermination de l'âge (cf. exigence EX_GEN-1550 au § 3.1.3) et proposition systématique, choix utilisateur,… devront être précisées par l'éditeur lors de son passage en homologation.

NB : la formulation « connexion secrète » n'est pas imposée pour l'IHM du LPS. Il est nécessaire d'afficher un texte explicatif à l'utilisateur concernant cette fonctionnalité.

**EX_0.1-1115**

Afin d'éviter une sollicitation excessive du professionnel (par exemple : cas de prise en charge de très jeunes enfants), le LPS peut proposer un paramètre « âge minimum » en dessous duquel le LPS ne proposera pas systématiquement la connexion secrète pour un patient mineur.

Dans le cas où cette fonctionnalité est proposée :

- Le paramètre doit obligatoirement être défini à l'initiative du professionnel et sous sa responsabilité ;
- Le LPS doit obligatoirement solliciter régulièrement le professionnel pour repositionner ce paramètre ;
- Une information claire doit être délivrée au professionnel sur cette fonctionnalité ;
- Elle ne doit pas interdire une connexion secrète à l'initiative du professionnel malgré ce paramètre positionné.

Les modalités de mise en œuvre d'une telle fonctionnalité doivent être précisées par l'éditeur lors de l'homologation

### 5.3.2 Authentification directe

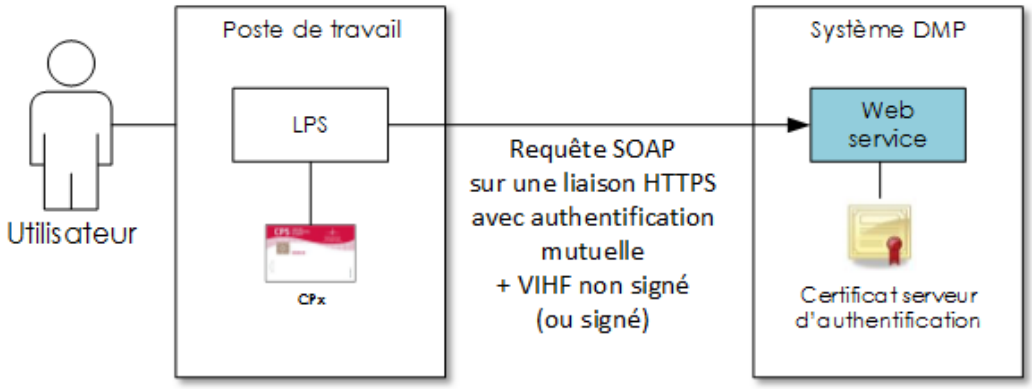



**Figure 33 : authentification directe**

Le LPS établit une liaison sécurisée TLS avec l'authentification mutuelle basée sur l'utilisation de la carte CPx. Un jeton VIHF accompagne toutes les requêtes SOAP. Le jeton VIHF peut être signé ou non. Dans le cas où il est signé, il convient de se reporter à l'exigence EX_0.1-1030 du chapitre suivant.

**EX_0.1-1010**

L'éditeur doit prendre les mesures techniques nécessaires pour éviter que l'accès aux fonctions cryptographiques de la CPx (sollicitations répétées du code PIN utilisateur, renégociation canal TLS,…) soit pénalisant pour l'expérience utilisateur.

**EX_0.X-1040**

Le LPS doit mettre en œuvre un protocole de détection de l'arrachage de la carte CPx.

Cette fonction, le cas échéant, déconnectera l'utilisateur du système DMP (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).

La fonction de détection de l'arrachage de carte s'assure que la carte CPx de l'utilisateur authentifié est toujours dans le lecteur de carte lors des demandes de transactions avec le système DMP.

Des préconisations techniques et des exemples d'implémentation sont disponibles dans le document [GUIDE-ARR-CPS] disponible dans l'espace Intégrateur CPS de l'ANS.

**REC_0.X-1050**

Il est recommandé de vérifier la date de fin de validité de la carte CPx lors du premier accès à la carte CPx pour la session courante de l'utilisateur.

En effet, le système DMP refuse la négociation TLS avec une carte CPx ayant expiré.

Le système DMP refuse également la négociation TLS avec une carte CPx révoquée (cas plus rare).

### Le VIHF en authentification directe

Les tableaux suivants décrivent le contenu du VIHF (en noir) et les contrôles réalisés par le système DMP (en bleu) selon le mode d'authentification.

| | **Champ du VIHF** | **CPS** (PS_TypeCarte = 0) ou **CPF** (PS_TypeCarte = 1) | **CPE** (PS_TypeCarte = 2) |
|---|---|---|---|
| **Emetteur** | //Assertion/ds:Signature<br>*Signature du VIHF* | Facultatif<br>Si une signature est fournie :<br>Contrôle de validité du certificat signataire.<br>Contrôle d'habilitation à signer du certificat signataire.<br>Contrôle de la signature du VIHF.<br>Contrôle de cohérence avec le DN de l'issuer. | Facultatif<br>Si une signature est fournie :<br>Contrôle de validité du certificat signataire.<br>Contrôle d'habilitation à signer du certificat signataire.<br>Contrôle de la signature du VIHF.<br>Contrôle de cohérence avec le DN de l'issuer. |
| | //Assertion/Issuer[12]<br>*Identité de l'émetteur contenue dans le certificat (DN).* | DN du certificat d'authentification de la CPS/CPF<br>Contrôle de cohérence avec le DN du certificat ayant initié la connexion TLS.<br>Si le jeton VIHF est signé : contrôle de cohérence avec le DN du certificat de signature | DN du certificat d'authentification de la CPE<br>Contrôle de cohérence avec le DN du certificat ayant initié la connexion TLS.<br>Si le jeton VIHF est signé : contrôle de cohérence avec le DN du certificat de signature |

[12] Selon la RFC 2253 (ex : CN=801234567890+SN=DUPONT+GN=JEAN,OU=Médecin,O=TEST,C=FR)

| | Champ du VIHF | **CPS** (PS_TypeCarte = 0) ou **CPF** (PS_TypeCarte = 1) | **CPE** (PS_TypeCarte = 2) |
|---|---|---|---|
| | //Assertion/Issuer/@Format<br>*Type de valeur utilisée pour renseigner le champ Issuer (X509)* | Constante :"urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"<br>Contrôle de la valeur | Constante :"urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"<br>Contrôle de la valeur |
| **Structure de soins** | Identifiant_Structure<br>*Identifiant de la structure de soins ou du cabinet.* | **Pour les CPS (hors remplaçant) :**<br>Struct_IdNat de la CPS[13]<br>Contrôle de présence dans l'annuaire<br>Contrôle de cohérence dans l'annuaire entre les structures de soins liées à l'identifiant du PS et la structure fournie.<br>**Pour les CPS de remplaçant :**<br>Struct_IdNat de la structure de rattachement<br>(à renseigner par le LPS)<br>Contrôle de présence dans l'annuaire<br>Pas de contrôle de cohérence dans l'annuaire entre les structures de soins liées à l'identifiant du PS et la structure fournie.<br>**Pour les CPF :**<br>à renseigner par le LPS<br>L'affectation d'un PS en formation à une structure, et sa mémorisation pour une durée limitée, est à la charge de l'éditeur.<br>Contrôle de présence dans l'annuaire<br>Pas de contrôle de cohérence dans l'annuaire entre les structures de soins liées à l'identifiant du PS et la structure fournie. | **Pour les CPE directement nominatives** :<br>Struct_IdNat de la CPE[13]<br>Contrôle de présence dans l'annuaire<br>Contrôle de cohérence dans l'annuaire entre les structures liées à l'identifiant du PE et la structure fournie.<br>**Pour les CPE non directement nominatives :**<br>Struct_IdNat de la CPE.<br>Contrôle de présence dans l'annuaire<br>**Pour les pharmaciens diplômés ou en formation et en remplacement exclusif, qui ont une CPE :**<br>à renseigner par le LPS |
| | Secteur_Activite<br>*Secteur d'activité dans lequel exerce l'utilisateur* | Struct_SectAct de la CPS/CPF<br>Contrôle que le secteur d'activité fait partie du jeu de valeurs HealthCareFacilityTypeCode<br>Contrôle que le secteur d'activité ne fait pas partie des secteurs d'activité interdits pour ce mode d'authentification | Struct_SectAct de la CPE<br>Contrôle que le secteur d'activité fait partie du jeu de valeurs HealthCareFacilityTypeCode<br>Contrôle que le secteur d'activité ne fait pas partie des secteurs d'activité interdits pour ce mode d'authentification |

[13] Pour pallier le problème de donnée dans la carte (FINESS juridique) différente des données de l'Annuaire Santé (FINESS géographique), il est possible d'utiliser la donnée de l'Annuaire Santé pour l'accès au DMP.

| | Champ du VIHF | **CPS** (PS_TypeCarte = 0)<br>ou **CPF** (PS_TypeCarte = 1) | **CPE** (PS_TypeCarte = 2) |
|---|---|---|---|
| **Utilisateur connecté** | //Assertion/Subject/NameID<br>*Identifiant de la personne connectée* | PS_IdNat de la CPS/CPF<br>Contrôle de cohérence avec le certificat d'authentification utilisé pour monter le canal TLS<br>Contrôle de présence dans l'annuaire PS | **Pour les CPE directement nominatives** :<br>PS_IdNat de la CPE<br>Contrôle de cohérence avec le certificat d'authentification utilisé pour monter le canal TLS<br>Contrôle de présence dans l'annuaire<br><br>**Pour les CPE non directement nominatives** :<br>PS_IdNat de la CPE<br>Contrôle de cohérence avec le certificat d'authentification utilisé pour monter le canal TLS<br>Contrôle que ce qui est avant le "/" est une structure présente dans l'annuaire et qu'elle est égale à Identifiant_Structure du VIHF<br><br>**Pour les pharmaciens diplômés ou en formation et en remplacement exclusif et qui ont une CPE :**<br>le PS_IdNat doit être transcodifié (avec xxxx = Identifiant national du pharmacien) :<br>si IdNat 3000000001/Axxxx ou 3000000018/A xxxx => remplacer 3000000001/A ou 3000000018/A par "0"<br>si IdNat 3000000001/Rxxxx ou 3000000018/R xxxx => remplacer 3000000001/R ou 3000000018/R par "8"<br>si IdNat 3000000001/Exxxx ou 3000000018/E xxxx => remplacer 3000000001/E ou 3000000018/E par "9" |

| | **Champ du VIHF** | **CPS** (PS_TypeCarte = 0)<br>ou **CPF** (PS_TypeCarte = 1) | **CPE** (PS_TypeCarte = 2) |
|---|---|---|---|
| | urn:oasis:names:tc:xspa:1.0:subject:subject-id<br>*Identité de l'utilisateur :*<br>*- Pour un utilisateur humain : nom, prénom, service au sein d'une structure.*<br>*- Pour une machine : nom du logiciel, nom du modèle, service au sein d'un établissement…* | Ne pas renseigner | **Pour les CPE directement nominatives :**<br>Ne pas renseigner<br>**Pour les CPE non directement nominatives :**<br>informations fournies par le LPS.<br>Pas de contrôle<br>**Pour les pharmaciens diplômés ou en formation et en remplacement exclusif et qui ont une CPE :**<br>Ne pas renseigner |
| | urn:oasis:names:tc:xacml:2.0:subject:role<br>*(1re occurrence obligatoire)*<br>*Profession de la personne connectée* | code contient<br>• la valeur de la donnée PS_Prof de la CPS codeSystem="1.2.250.1.71.1.2.7"<br>• ou la valeur de la donnée PS_FutureProf de la CPF codeSystem="1.2.250.1.71.1.2.8"<br>Contrôle de cohérence dans l'annuaire entre la profession liée à l'identifiant et le code de profession fourni | **Pour les CPE directement nominatives :**<br>code = "SECRETARIAT_MEDICAL"<br>codeSystem="1.2.250.1.213.1.1.4.6"<br>Contrôle du code et du codeSystem<br>**Pour les CPE non directement nominatives :**<br>code = "SECRETARIAT_MEDICAL"<br>codeSystem="1.2.250.1.213.1.1.4.6"<br>Contrôle du code et du codeSystem<br>**Pour les pharmaciens diplômés ou en formation et en remplacement exclusif et qui ont une CPE :**<br>code="21"<br>codeSystem="1.2.250.1.71.1.2.7"<br>Contrôle du code et du codeSystem |

| | Champ du VIHF | **CPS** (PS_TypeCarte = 0)<br>ou **CPF** (PS_TypeCarte = 1) | **CPE** (PS_TypeCarte = 2) |
|---|---|---|---|
| | urn:oasis:names:tc:xacml:2.0:subject:role<br>*(2e occurrence uniquement et obligatoirement pour les médecins et pharmaciens)*<br>*Spécialité de la personne connectée* | **Pour les médecins :**<br>code contient la valeur de la donnée PS_SpécRPPS de la CPS<br>codeSystem="1.2.250.1.71.4.2.5"<br>Contrôle de cohérence dans l'annuaire<br>Certaines spécialités n'ont pas accès au DMP en consultation.<br>*Exemple : les médecins du travail (SM25 et SCH35, ou activité FON 29 déclarée dans l'annuaire de santé)*<br>**Pour les pharmaciens :**<br>code contient la valeur de la donnée PS_TabPharm de la CPS<br>codeSystem="1.2.250.1.71.4.2.6"<br>Contrôle de cohérence dans l'annuaire<br>Certaines spécialités n'ont pas accès au DMP.<br>**Pour les CPF (médecins et pharmaciens)**<br>Valeurs paramétrables dans le LPS.<br>Exemple pour médecin :<br>code="SM26" codeSystem="1.2.250.1.71.4.2.5" displayName="Qualifié en médecine générale (SM)"<br>Exemple pour pharmacien :<br>code="DA" codeSystem="1.2.250.1.71.4.2.6" displayName="Pharmacien adjoint" | **Pour les CPE directement et non directement nominatives :**<br>non renseigné.<br>**Pour les pharmaciens diplômés et en remplacement exclusif et qui ont une CPE :**<br>code="A" ou "G"<br>codeSystem="1.2.250.1.71.4.2.6"<br>Contrôle de cohérence dans l'annuaire<br>**Pour les pharmaciens en formation et en remplacement exclusif et qui ont une CPE :**<br>non renseigné, car les pharmaciens en formation ne sont pas inscrits sur les tableaux. |
| | //Assertion/AuthnStatement/AuthnContext/AuthnContextClassRef<br>*Mode d'authentification en local* | Constante :"urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"<br>Contrôle de la valeur | Constante :"urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"<br>Contrôle de la valeur |
| **Assertion SAML** | //Assertion/@xmnls<br>*namespace xml SAML* | Constante :"urn:oasis:names:tc:SAML:2.0:assertion"<br>Contrôle de la valeur | Constante :"urn:oasis:names:tc:SAML:2.0:assertion"<br>Contrôle de la valeur |
| | //Assertion/@Version<br>*Version utilisée* | Constante : "2.0"<br>Contrôle de la valeur | Constante : "2.0"<br>Contrôle de la valeur |

| | Champ du VIHF | **CPS** (PS_TypeCarte = 0) ou **CPF** (PS_TypeCarte = 1) | **CPE** (PS_TypeCarte = 2) |
|---|---|---|---|
| | //Assertion/@ID<br>*Identifiant unique de l'assertion (uuid recommandé)* | identifiant unique de l'assertion | identifiant unique de l'assertion |
| | //Assertion/@IssueInstant<br>*Date et heure d'émission de l'assertion SAML* | Date et heure d'émission de l'assertion SAML<br>Contrôle que la date d'émission du VIHF :<br>- n'est pas dans le futur (date du système DMP + 3 secondes maximum)<br>- n'a pas plus d'une heure de moins que l'heure du système DMP. | Date et heure d'émission de l'assertion SAML<br>Contrôle que la date d'émission du VIHF :<br>- n'est pas dans le futur (date du système DMP + 3 secondes maximum)<br>- n'a pas plus d'une heure de moins que l'heure du système DMP. |
| | //Assertion/AuthnStatement/@AuthnInstant<br>*Date et heure d'authentification en local* | Date/Heure de connexion de l'utilisateur dans le système source | Date/Heure de connexion de l'utilisateur dans le système source |
| | //Assertion/Conditions/AudienceRestriction<br>*OID d'une PSSI (Politique de Sécurité des Systèmes d'Information) applicable* | Ne pas renseigner,<br>car aucune PSSI n'est définie à ce jour | Ne pas renseigner,<br>car aucune PSSI n'est définie à ce jour |
| | //Assertion/Conditions/@NotBefore<br>*Date et heure de début de validité de l'assertion* | Facultatif<br>Si présent, contrôle de la validité à l'instant I :<br>T < (NotBefore) < I < min(T+1h,NotOnOrAfter) | Facultatif<br>Si présent, contrôle de la validité à l'instant I :<br>T < (NotBefore) < I < min(T+1h,NotOnOrAfter) |
| | //Assertion/Conditions/@NotOnOrAfter<br>*Date et heure de fin de validité de l'assertion* | | |
| | VIHF_Version<br>*Version du VIHF utilisée* | Constante : "3.0"<br>Contrôle de la valeur | Constante : "3.0"<br>Contrôle de la valeur |
| | Authentification_Mode<br>*Mode d'authentification utilisé* | Constante : "DIRECTE"<br>Contrôle de la valeur | Constante : "DIRECTE"<br>Contrôle de la valeur |
| **Patient** | urn:oasis:names:tc:xacml:2.0:resource:resource-id<br>*Identifiant du patient concerné par la requête* | INS du patient<br>Contrôle si présent,<br>obligatoire dans les transactions qui concernent un DMP : TD0.2, TD0.3, TD1.x, TD2.x, TD3.x<br>(INS du patient pour lequel il y a un accès au DMP) | INS du patient<br>Contrôle si présent,<br>obligatoire dans les transactions qui concernent un DMP : TD0.2, TD0.3, TD1.x, TD2.x, TD3.x<br>(INS du patient pour lequel il y a un accès au DMP) |
| **Sys** | Ressource_URN | Constante : "urn:dmp" | Constante : "urn:dmp" |

| | Champ du VIHF | **CPS** (PS_TypeCarte = 0)<br>ou **CPF** (PS_TypeCarte = 1) | **CPE** (PS_TypeCarte = 2) |
|---|---|---|---|
| | *Ressource visée par l'utilisateur* | Contrôle de la valeur | Contrôle de la valeur |
| | urn:oasis:names:tc:xspa:1.0:subject:purposeofuse<br>*Mode d'accès demandé par l'utilisateur (normal, bris de glace ou centre de régulation).* | code=<br>- "**normal**" : pour un accès normal<br>- "**bris_de_glace**" : lorsque le PS a besoin de consulter le DMP d'un patient en cas d'urgence, sans avoir la possibilité de lui demander son autorisation<br>- "**centre_15**" : réservé aux LDR qui indiquent ainsi l'usage « centre de régulation » spécifique à leur rôle ;<br>Contrôle de valeur | code="**normal**"<br>Contrôle de valeur |
| | Mode_Acces_Raison<br>*Explication de la raison de l'usage du bris de glace.* | Obligatoire si mode bris de glace.<br>Contrôle de présence si mode bris de glace. | *Non applicable en CPE* |
| | urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code<br>*Restriction d'audience à appliquer aux traces générées par la transaction objet du flux* | Obligatoire si la fonctionnalité est activée[14] et si demande de connexion secrète au DMP.<br>`Valeur "INVISIBLE_REPRESENTANTS_LEGAUX^1.2.250.1.213.1.1.4.13"`<br>(traces d'accès au DMP non visibles aux représentants légaux du patient)<br>Ne pas fournir cette donnée dans les autres cas. | Obligatoire si la fonctionnalité est activée[14] et si demande de connexion secrète au DMP.<br>`Valeur "INVISIBLE_REPRESENTANTS_LEGAUX^1.2.250.1.213.1.1.4.13"`<br>(traces d'accès au DMP non visibles aux représentants légaux du patient)<br>Ne pas fournir cette donnée dans les autres cas. |
| **LPS** | LPS_ID<br>*Numéro de série ou identifiant de l'installation du logiciel* | Facultatif<br>(usage à des fins de suivi) | Facultatif<br>(usage à des fins de suivi) |
| | LPS_Nom<br>*Nom du logiciel utilisé* | Nom du LPS qui génère le jeton VIHF<br>Contrôle de cohérence avec le n° d'homologation (différencier les différents logiciels associés à un n° d'homologation). | Nom du LPS qui génère le jeton VIHF<br>Contrôle de cohérence avec le n° d'homologation (différencier les différents logiciels associés à un n° d'homologation). |
| | LPS_Version<br>*Version du logiciel utilisé* | N° de version du LPS qui génère le jeton VIHF<br>Contrôle de cohérence avec le n° d'homologation (différencier les différentes versions de logiciels associées à un n° d'homologation) | N° de version du LPS qui génère le jeton VIHF<br>Contrôle de cohérence avec le n° d'homologation (différencier les différentes versions de logiciels associées à un n° d'homologation) |

[14] Cf. paramètre `fonctions-gestion-mineurs` dans le chapitre 3.1.1.

| | Champ du VIHF | **CPS** (PS_TypeCarte = 0) ou **CPF** (PS_TypeCarte = 1) | **CPE** (PS_TypeCarte = 2) |
|---|---|---|---|
| | LPS_ID_HOMOLOGATION_DMP<br>*Numéro d'homologation du logiciel* | N° d'homologation du LPS.<br>Contrôle de l'homologation DMP-compatibilité validée pour la transaction appelée | N° d'homologation du LPS.<br>Contrôle de l'homologation DMP-compatibilité validée pour la transaction appelée |

**Tableau 25 : le jeton VIHF en authentification directe**

Les autres champs spécifiés dans le CI-SIS ne sont pas utilisés par le système DMP. Néanmoins, une requête avec un VIHF contenant ces champs ne sera pas rejetée par le système DMP.

### 5.3.3 Authentification indirecte

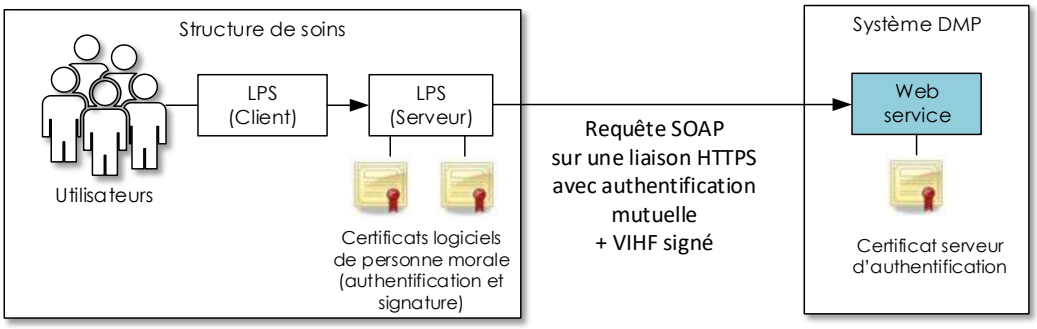



**Figure 34 : authentification indirecte**

Le LPS établit une liaison sécurisée TLS avec l'authentification mutuelle basée sur l'utilisation de certificat d'authentification de la structure de soins. Un jeton VIHF signé par le certificat de cachet de la structure de soins accompagne toutes les requêtes SOAP.

**EX_GEN-1450**

La structure de soins doit au préalable acquérir deux certificats logiciels de personne morale de l'IGC Santé de l'ANS :

- un certificat d'authentification pour personne morale (gamme élémentaire de type « `ORG_AUTH_CLI` ») pour établir la liaison TLS avec authentification mutuelle ;
- un certificat de cachet pour personne morale (gamme élémentaire de type « `ORG_SIGN` ») pour réaliser la signature électronique du jeton VIHF.

Pour l'alimentation du DMP avec identification FINESS de la structure de soins, deux modes sont ouverts à l'homologation DMP en fonction des FINESS et des certificats utilisés : mode EJ/EG, et mode EG. Un troisième mode EJ est fortement déconseillé. Cf. chapitre 2.2.1 pour plus d'information sur ce sujet.

**EX_0.1-1020**

L'utilisateur doit être authentifié localement (au sein de la structure d'exercice).

Le type d'authentification est déclaré dans le champ du jeton VIHF `/Assertion/AuthnStatement/AuthnContext/AuthnContextClassRef`.

**EX_0.1-1025**

L'identifiant interne de l'utilisateur doit :

- être unique au sein de la structure de soins, pérenne et non réutilisable ;
- être traité comme une chaîne de caractères indissociable et ne doit pas pouvoir être interprété par des applications ;
- pouvoir être utilisé pour retrouver la personne réelle (traçabilité).

### Le jeton VIHF en authentification indirecte

Pour apporter suffisamment de confiance dans l'authenticité et la validité du jeton VIHF transmis par la structure de soins, celui-ci doit être signé en XML-DSIG par le certificat de cachet de la structure de soins.

En effet le système DMP ne peut se baser sur d'autres informations fiables contrairement au mode d'authentification directe, notamment au niveau des informations d'identification de l'utilisateur connecté.

**EX_0.1-1030**

La signature XML-DSIG doit se situer dans un tag `<Signature>` entre l'élément `<Issuer>` et l'élément `<Subject>` de l'assertion (signature de type « `enveloped` »). Cette signature doit utiliser les algorithmes `SHA-1` pour les digests et « `SHA-1 with RSA` » pour la signature. Le certificat doit être présent dans l'élément : `//ds:Signature/KeyInfo/X509Data/X509Certificate`.

Les tableaux suivants décrivent le contenu du jeton VIHF (en noir) et les contrôles réalisés par le système DMP (en bleu) selon le mode d'authentification.

Il est conseillé d'utiliser les données de l'Annuaire Santé pour renseigner les champs du VIHF relatifs à l'utilisateur connecté.

| | Champ du VIHF | Alimentation et contrôle des données |
|---|---|---|
| Emetteur | //Assertion/ds:Signature<br>*Signature du VIHF* | Signature XML-DSIG avec le certificat de cachet de la structure de soins<br>Mode EJ : certificat de l'entité juridique<br>Mode EJ/EG : certificat de l'entité juridique<br>Mode EG : certificat de l'entité géographique<br>Contrôle de validité du certificat de cachet.<br>Contrôle d'habilitation à signer du certificat de cachet.<br>Contrôle de la signature du jeton VIHF.<br>Contrôle de cohérence avec le DN de l'issuer. |
| | //Assertion/Issuer[15]<br>*Identité de l'émetteur contenue dans le certificat (DN).* | DN du certificat de cachet utilisé pour signer l'assertion de la structure de soins<br>Mode EJ : DN du certificat de cachet de l'entité juridique<br>Mode EJ/EG : DN du certificat de cachet de l'entité juridique |

[15] Selon la RFC 2253 (ex : CN=testdmp.etablissement-de-test.fr, OU=10B0011797, L=Paris (75), O=TEST, C=FR)

| | Champ du VIHF | Alimentation et contrôle des données |
|---|---|---|
| | | Mode EG : DN du certificat de cachet de l'entité géographique<br>Contrôle de cohérence avec le DN du certificat ayant initié la connexion TLS.<br>Contrôle de cohérence avec le DN du certificat de cachet (le jeton VIHF est signé) |
| | //Assertion/Issuer/@Format<br>*Type de valeur utilisée pour renseigner le champ Issuer (X509)* | Constante :"urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"<br>Contrôle de la valeur |
| **Structure de soins** | Identifiant_Structure<br>*Identifiant de la structure de soins ou du cabinet.* | Struct_IdNat de la structure de soins<br>Mode EJ : FINESS de l'entité juridique<br>Mode EJ/EG : FINESS de l'entité géographique<br>Mode EG : FINESS de l'entité géographique<br>Contrôle de présence dans l'annuaire<br>Contrôle de cohérence entre le certificat et la structure fournie. |
| | Secteur_Activite<br>*Secteur d'activité dans lequel exerce l'utilisateur* | Fourni par le LPS<br>(le secteur d'activité n'est pas renseigné dans le certificat de personne morale)<br>Contrôle que le secteur d'activité fait partie du jeu de valeurs HealthCareFacilityTypeCode<br>Contrôle que le secteur d'activité ne fait pas partie des secteurs d'activité interdits pour ce mode d'authentification |
| **Utilisateur connecté** | //Assertion/Subject/NameID<br>*Identifiant de la personne connectée* | Fourni par le LPS<br>**Pour un utilisateur humain :** Identifiant du professionnel<br>**Pour les traitements automatisés :** Identifiant de la personne responsable du traitement<br>**Source de donnée :**<br>- soit identifiant national (commence par 0, 2, 8 ou 9)<br>Contrôle du 1er chiffre de l'identifiant et que sa longueur est conforme<br>- soit identifiant structure+ « / »+identifiant interne (commence par 1, 3, 4, 5, 6)<br>Contrôle de la cohérence avec le champ identifiant_structure<br>Mode EJ/EG : exemple si l'Id personne est un ID interne à l'ES<br>Id national de l'entité géographique = 10B0170262<br>➔ NameID = 30B0170262/XXX ;<br>Sinon on peut mettre un ID RPPS ou ADELI |

| | Champ du VIHF | Alimentation et contrôle des données |
|---|---|---|
| | urn:oasis:names:tc:xspa:1.0:subject:subject-id<br>*Identité de l'utilisateur :*<br>*- Pour un utilisateur humain : nom, prénom, service au sein d'une structure.*<br>*- Pour une machine : nom du logiciel, nom du modèle, service au sein d'un établissement…* | Fourni par le LPS<br>**Pour un utilisateur humain :**<br>Nom, Prénom et Service de l'utilisateur.<br>Contrôle de présence<br>**Pour les traitements automatisés :**<br>Nom du logiciel, Nom du modèle et Service.<br>Contrôle de présence |
| | urn:oasis:names:tc:xacml:2.0:subject:role<br>*(1re occurrence obligatoire)*<br>*Profession de la personne connectée* | **Pour les professionnels :**<br>Prendre la valeur de code la plus appropriée parmi les codes du jeu de valeurs CI-SIS "subjectRole" avec un codeSystem="1.2.250.1.71.1.2.7" (table G15)<br>ou une valeur du jeu de valeur TRE_G16-ProfessionFormation (Professions en formation (carte CPF)) avec un codeSystem="1.2.250.1.71.1.2.8"<br>Contrôle du codeSystem<br>**Pour les autres :**<br>Prendre la valeur de code la plus appropriée parmi les codes<br>• du jeu de valeurs CI-SIS "subjectRole" avec un codeSystem="1.2.250.1.213.1.1.4.6"<br>• ou une valeur du jeu de valeur TRE_R95-UsagerTitre (Usager de titre professionnel) codeSystem ="1.2.250.1.213.1.6.1.109"<br>• ou une valeur du jeu de valeur TRE_R94-ProfessionSocial (Profession du social) codeSystem ="1.2.250.1.213.1.6.1.4"<br>• ou une valeur du jeu de valeur TRE_R291-AutreProfession (Liste de professionnels non-membres d'une profession réglementée) codeSystem ="1.2.250.1.213.1.6.1.140"<br>Contrôle que code et codeSystem font partie du jeu de valeurs subjectRole |
| | urn:oasis:names:tc:xacml:2.0:subject:role<br>*(2e occurrence uniquement et obligatoirement pour les médecins et pharmaciens)*<br>*Savoir-faire de la personne connectée* | **Pour les médecins :**<br>Prendre la valeur de code la plus appropriée parmi les codes du jeu CI-SIS "subjectRole" de valeurs dont le codeSystem="1.2.250.1.71.4.2.5" (table R01)<br>Contrôle que code et codeSystem font partie du jeu de valeurs subjectRole<br>**Pour les pharmaciens :**<br>Prendre la valeur de code la plus appropriée parmi les codes du jeu de valeurs CI-SIS "subjectRole" avec un codeSystem="1.2.250.1.71.4.2.6" (table G05)<br>Contrôle que code et codeSystem font partie du jeu de valeurs subjectRole |
| | urn:oasis:names:tc:xacml:2.0:subject:role<br>*(3e occurrence obligatoire pour les professionnels caractérisés par leur rôle* | Prendre la valeur de code la plus appropriée parmi les codes<br>• du jeu de valeur TRE_R85-RolePriseCharge (Rôle dans la prise en charge des patients ou des usagers) codeSystem ="1.2.250.1.213.1.6.1.107" |

| | Champ du VIHF | Alimentation et contrôle des données |
|---|---|---|
| | *(ou fonction ou genre d'activité). Non requise pour les autres professionnels.)* | • ou du jeu de valeur TRE_R21-Fonction (Fonction) codeSystem ="1.2.250.1.213.1.6.1.17"<br>• ou du jeu de valeur valeur TRE_R22-GenreActivite (Genre d'activité) codeSystem ="1.2.250.1.213.1.6.1.19".<br>Cf. matrice d'habilitation pour les cas prévus par le SI DMP. |
| | //Assertion/AuthnStatement/AuthnContext/AuthnContextClassRef<br>*Mode d'authentification en local* | Prendre la valeur la plus appropriée parmi les valeurs possibles indiquées dans le document http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf<br>La valeur utilisée doit être cohérente avec le mode d'authentification locale de l'utilisateur dans le LPS<br>Contrôle de la valeur |
| **Assertion SAML** | //Assertion/@xmnls<br>*namespace xml SAML* | Constante :"urn:oasis:names:tc:SAML:2.0:assertion"<br>Contrôle de la valeur |
| | //Assertion/@Version<br>*Version utilisée* | Constante : "2.0"<br>Contrôle de la valeur |
| | //Assertion/@ID<br>*Identifiant unique de l'assertion (uuid recommandé)* | identifiant unique de l'assertion |
| | //Assertion/@IssueInstant<br>*Date et heure d'émission de l'assertion SAML* | Date et heure d'émission de l'assertion SAML<br>Contrôle que la date d'émission du jeton VIHF :<br>- n'est pas dans le futur (date du système DMP + 3 secondes maximum)<br>- n'a pas plus d'une heure de moins que l'heure du système DMP. |
| | //Assertion/AuthnStatement/@AuthnInstant<br>*Date et heure d'authentification en local* | Date/Heure de connexion de l'utilisateur dans le système source |
| | //Assertion/Conditions/AudienceRestriction<br>*OID d'une PSSI (Politique de Sécurité des Systèmes d'Information) applicable* | Ne pas renseigner,<br>car aucune PSSI n'est définie à ce jour |
| | //Assertion/Conditions/@NotBefore<br>*Date et heure de début de validité de l'assertion* | Facultatif<br>Si présent, contrôle de la validité à l'instant I :<br>T < (NotBefore) < I < min(T+1h,NotOnOrAfter) |
| | //Assertion/Conditions/@NotOnOrAfter<br>*Date et heure de fin de validité de l'assertion* | |
| | VIHF_Version<br>*Version du VIHF utilisée* | Constante : "4.0"<br>Contrôle de la valeur |

| | Champ du VIHF | Alimentation et contrôle des données |
|---|---|---|
| | | |
| | Authentification_Mode<br>*Mode d'authentification utilisé* | Constante : "INDIRECTE"<br>Contrôle de la valeur |
| **Patient** | urn:oasis:names:tc:xacml:2.0:resource:resource-id<br>*Identifiant du patient concerné par la requête* | INS du patient<br>Contrôle si présent,<br>obligatoire dans les transactions qui concernent un DMP : TD0.2, TD0.3, TD1.x, TD2.x, TD3.x<br>(INS du patient pour lequel il y a un accès au DMP) |
| **Système cible** | Ressource_URN<br>*Ressource visée par l'utilisateur* | Constante : "urn:dmp"<br>Contrôle de la valeur |
| | urn:oasis:names:tc:xspa:1.0:subject:purposeofuse<br>*Mode d'accès demandé par l'utilisateur.* | code=<br>- "**normal**" : pour un accès normal<br>- "**centre_15**" : réservé aux LDR qui indiquent ainsi l'usage « centre de régulation » spécifique à leur rôle<br>Contrôle de valeur |
| | Mode_Acces_Raison<br>*Explication de la raison de l'usage du bris de glace.* | *Non applicable en authentification indirecte*. |
| | urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code<br>*Restriction d'audience à appliquer aux traces générées par la transaction objet du flux* | Obligatoire si la fonctionnalité est activée[16] et si demande de connexion secrète au DMP.<br>Valeur "INVISIBLE_REPRESENTANTS_LEGAUX^1.2.250.1.213.1.1.4.13"<br>(traces d'accès au DMP non visibles aux représentants légaux du patient)<br>Ne pas fournir cette donnée dans les autres cas. |
| **LPS** | LPS_ID<br>*Numéro de série ou identifiant de l'installation du logiciel* | Facultatif<br>(usage à des fins de suivi) |
| | LPS_Nom<br>*Nom du logiciel utilisé* | Nom du LPS qui génère le jeton VIHF<br>Contrôle de cohérence avec le n° d'homologation (différencier les différents logiciels associés à un n° d'homologation). |
| | LPS_Version<br>*Version du logiciel utilisé* | N° de version du LPS qui génère le jeton VIHF<br>Contrôle de cohérence avec le n° d'homologation (différencier les différentes versions de logiciels associées à un n° d'homologation) |

[16] Cf. paramètre `fonctions-gestion-mineurs` dans le chapitre 3.1.1.

| | Champ du VIHF | Alimentation et contrôle des données |
|---|---|---|
| | LPS_ID_HOMOLOGATION_DMP<br>*Numéro d'homologation du logiciel* | N° d'homologation du LPS.<br>Contrôle de l'homologation DMP-compatibilité validée pour la transaction appelée |

**Tableau 26 : le jeton VIHF en authentification indirecte**

Les autres champs spécifiés dans le CI-SIS ne sont pas utilisés par le système DMP. Néanmoins, une requête avec un VIHF contenant ces champs ne sera pas rejetée par le système DMP.

### 5.3.4 Authentification indirecte renforcée (AIR)

Ce mode d'authentification vient en complément du mode d'authentification indirecte. Au niveau de la transaction vers le système DMP, l'impact majeur se situe sur le jeton VIHF décrit au chapitre 5.3.4.5.

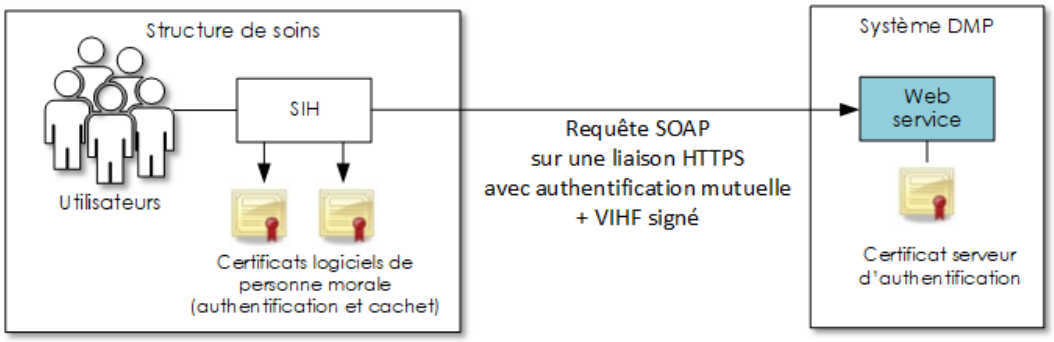



**Figure 35 – authentification indirecte renforcée**

NB : dans ce chapitre, les schémas illustrent le cas des SIH. Le mode AIR peut cependant s'appliquer au système d'information (SI) d'autres types de structure de soins.

L'établissement de la liaison sécurisée est conforme aux exigences du chapitre 5.3.1.

Les structures de soins peuvent s'inscrire dans un schéma d'authentification indirecte dite « renforcée ». Ce mode d'authentification permet de mettre en œuvre des moyens d'authentification alternatifs à la CPS pour la consultation du DMP.

L'authentification indirecte renforcée fait intervenir trois acteurs : le professionnel, utilisateur des outils mis à sa disposition par la structure qui l'accueille, la structure de soins qui habilite ses utilisateurs pour l'accès au DMP, et enfin, le DMP qui rend le service.

Les appels à la consultation en mode AIR sans que le PS dans la structure soit authentifié ou qu'il ait connaissance de l'utilisation de son identité sont strictement interdits en mode d'authentification AIR.

Seul l'utilisateur à l'origine de ces consultations en mode AIR doit pouvoir consulter les documents DMP des patients.

L'enjeu de l'authentification indirecte renforcée est de laisser une plus grande liberté à la structure de soins pour assurer l'authentification primaire des PS par les moyens adaptés à son environnement.

L'inscription dans ce mode est soumise à une auto-homologation de la part du directeur de l'établissement qui engage la responsabilité de sa structure sur le respect du référentiel d'exigences du DMP[17]. Celles-ci sont d'ordre organisationnel, technique et sécuritaire. Elles portent sur toute la chaîne d'authentification de l'utilisateur, depuis le processus d'enrôlement jusqu'au transport du jeton d'identification et d'habilitation (VIHF) pour l'accès au DMP. Cela passe par une authentification primaire forte de l'utilisateur.

#### 5.3.4.1 Exigences spécifiques au mode AIR

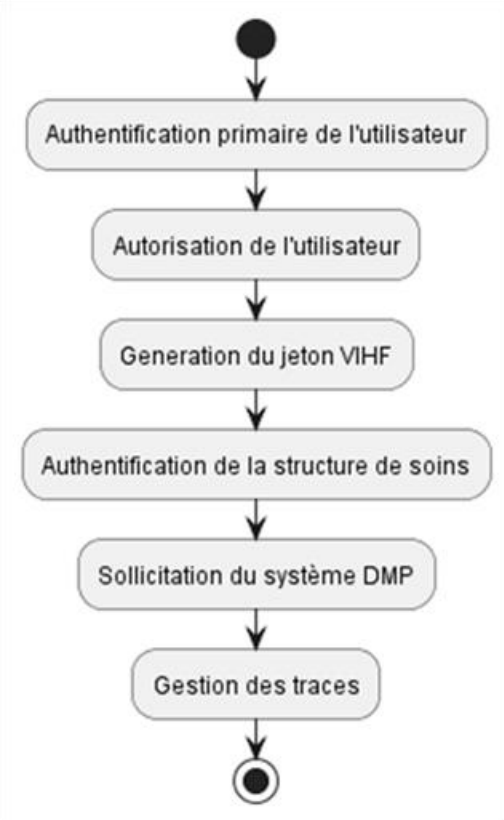



**Figure 36 – Processus général d'accès au système DMP**

[17] doc. [REF-DMP]

### Authentification primaire forte de l'utilisateur

Pour accéder au DMP, l'authentification des utilisateurs doit être forte, c'est-à-dire être réalisée à partir d'une combinaison de deux facteurs de natures différentes (par exemple « ce que je sais » : mot de passe, « ce que je possède » : une carte, un terminal mobile, ou encore un logiciel comme une application mobile, ou « ce que je suis » : une caractéristique biométrique du PS).

### Autorisation de l'utilisateur

L'autorisation de l'utilisateur à solliciter le système DMP doit être vérifiée par la structure de soins. Par exemple, l'appartenance à l'effectif, les plages de travail autorisées, la « qualité » des utilisateurs selon les exigences du DMP (profession, spécialité, secteur d'activité, etc.) doivent bien être contrôlées.

La sécurité d'un système d'information repose également sur le comportement et les pratiques des utilisateurs qui manipulent les applications et données de la structure. Les utilisateurs peuvent être le maillon faible de la chaîne de sécurité qu'un attaquant serait tenté d'exploiter pour pénétrer le réseau local. Un utilisateur sensibilisé aux menaces et risques pourra détecter et éviter une attaque.

**EX_AIR-010**

Le mode AIR est réservé au profil « Consultation » et au profil « Consultation Web-PS en mode AIR » décrit dans la matrice des droits fonctionnels. Les autres profils sont à mettre en œuvre avec les modes d'authentification classiques (directe et/ou indirecte).

**EX_AIR-020**

Le mode AIR est réservé aux professionnels (PS) référencés dans un répertoire national d'identité (SI RASS).

### Génération du jeton VIHF

La génération du jeton VIHF doit être sécurisée, pour se prémunir contre tout risque d'attaque et de vol de certificat ou encore d'attaque de type « man in the middle ».

Il appartient ainsi à la structure de soins de sécuriser l'espace des composants responsables de la génération du jeton VIHF. La structure de soins est responsable de l'intégrité des composants et des configurations mises en place et en assurera donc la sécurisation physique et logique. Il appartient également à la structure de soins d'assurer le maintien en conditions opérationnelles ainsi que le maintien du niveau de sécurité de la solution dans le temps.

**REC_AIR-010**

Il est recommandé de proposer un serveur de jeton VIHF centralisé afin d'en garantir la sécurité logique et physique (spécialement pour les certificats X509).

**EX_AIR-030**

Les applicatifs qui se connectent au serveur de jeton doivent s'authentifier. Seuls les applicatifs légitimes peuvent y accéder.

Un jeton VIHF possède une durée de vie limitée dans le temps et n'est pas réutilisable.

**EX_AIR-040**

Le jeton VIHF généré au sein de la structure de soins possède une durée de vie de 30 secondes. Ce jeton ne peut être utilisé que pour une seule sollicitation.

**EX_AIR-050**

Le jeton VIHF contient la méthode d'authentification primaire de l'utilisateur (cf. chapitre 5.3.4.5).
Pour le mode AIR, une seule valeur "`CONF_EXI_PGSSIS`" est permise. Celle-ci précise la conformité de la solution aux exigences du PGSSIS. Cette valeur est à positionner obligatoirement par les éditeurs.

**EX_AIR-070**

Le système d'information de la structure de soins doit être en mesure de tracer la génération d'un jeton VIHF et son utilisation. Ces traces doivent permettre d'identifier clairement l'utilisateur et la structure de soins (cf. l'annexe 9).

### Authentification de la structure de soins

L'authentification de la structure de soins auprès du système DMP est la seconde composante de l'authentification de l'utilisateur pour l'accès du DMP. Celle-ci s'effectue par le certificat de personne morale de la structure de soins, et en utilisant le protocole de sécurisation TLS en authentification mutuelle entre la structure de soins et le système DMP.

**EX_AIR-080**

La liaison avec le système DMP est établie en authentification mutuelle avec un certificat d'authentification pour personne morale de l'IGC Santé de l'ANS. Ce certificat doit être valide et ne doit pas être révoqué.

L'authentification de la structure de soins n'est possible qu'une fois que la procédure d'auto-homologation a été réalisée par son responsable.

Pour la consultation du DMP avec identification FINESS de la structure de soins, deux modes sont ouverts à l'homologation DMP en fonction des FINESS et des certificats utilisés : mode EJ/EG, et mode EG. Un troisième mode EJ est fortement déconseillé. Cf. chapitre 2.2.1 pour plus d'information sur ce sujet.

**Contrôle des Secteurs d'Activité**

Certains secteurs d'activité ne peuvent pas accéder au système DMP. Ceux-ci sont décrits dans la règle de gestion [RG_0060] du document [GI-DMPi] au chapitre 3.1.2.

### Sollicitation du système DMP

**EX_AIR-085**

Les appels à la consultation en mode AIR sans que le PS utilisateur dans la structure soit authentifié ou qu'il ait connaissance de l'utilisation de son identité sont strictement interdits en mode d'authentification AIR.

Seul le PS à l'origine de ces consultations en mode AIR doit pouvoir consulter les documents DMP des patients.

**EX_AIR-090**

Le système d'information de la structure de soins doit être en mesure de tracer les sollicitations du système DMP. Ces traces doivent permettre d'identifier clairement l'utilisateur et la structure de soins (cf. l'annexe 9).

### Gestion des traces

Les activités d'authentification primaire forte de l'utilisateur, de génération du jeton VIHF et de sollicitation du système DMP vont générer des traces. Ces traces sont conservées par la structure de soins et fournies sur demande à l'Assurance Maladie.

**EX_AIR-100**

Le système d'information de la structure de soins doit être en mesure de respecter la durée légale de conservation des traces. Celle-ci est alignée sur la durée de conservation du DMP. Aujourd'hui, les traces doivent être conservées 10 ans après la clôture du DMP puis détruites.

**EX_AIR-110**

Le système d'information de la structure de soins doit être en mesure de garantir la confidentialité, l'intégrité et la complétude des traces.

**EX_AIR-120**

Sur demande de l'assurance maladie, le système d'information doit permettre à une structure de soins d'extraire et de fournir toutes les traces dématérialisées d'un PS ou de plusieurs PS sur une période donnée dans un délai de 7 jours ouvrables. Les modalités d'échanges des traces avec l'assurance maladie seront définies lors de la demande.

### 5.3.4.2 Composants

Techniquement, le mode d'authentification indirecte renforcée repose sur les composants décrits ci-dessous. Ceux-ci peuvent être regroupés au sein d'un unique logiciel ou répartis dans plusieurs briques autonomes du système d'information.

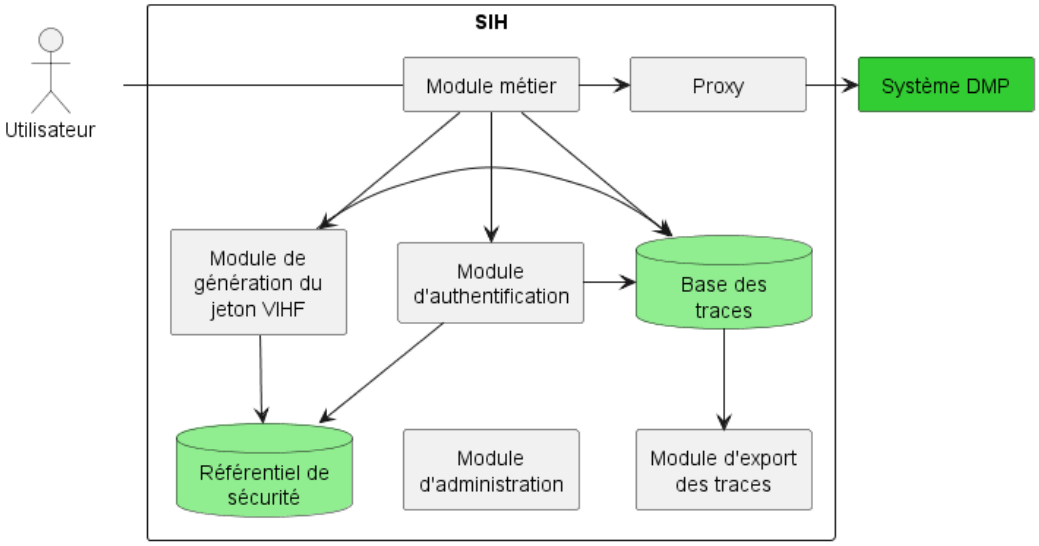



**Figure 37 – Composants minimaux pour l'accès TD0.1**

**Module Métier**

Le module métier est l'outil informatique de l'utilisateur. C'est à partir de ce dernier que l'utilisateur va s'authentifier sur le système d'information de la structure de soins et solliciter le système DMP.

**Module d'authentification**

Le module d'authentification s'appuie sur le référentiel de sécurité de la structure de soins pour authentifier les utilisateurs. Il transmet l'identité de l'utilisateur aux modules qui en dépendent.

**Module de génération du jeton VIHF**

Ce module a la responsabilité de générer le jeton VIHF signé. Cela peut nécessiter de contrôler les autorisations et de récupérer des attributs d'habilitation de l'utilisateur conservé dans le référentiel de sécurité. Chaque génération de jeton VIHF doit être tracée conformément à l'exigence.

Il est recommandé d'implémenter ce module sous forme de service centralisé pour en maîtriser la sécurité et le cloisonnement des certificats de la structure de soins. Dans le cas où le module est fourni sous forme de service centralisé, la liaison entre le module métier et le service doit être également sécurisée.

**Référentiel de sécurité**

Le référentiel de sécurité (annuaire, SSO, etc.) contient les utilisateurs de la structure de soins :

- Les authentifiants (certificat X509 par exemple) ;
- Les informations des utilisateurs (nom, prénom, spécialité, etc.) ;
- Les droits d'accès.

Il est utilisé par le module d'authentification pour authentifier les utilisateurs.

Il est utilisé par le module de génération du jeton VIHF pour déterminer les droits d'accès des utilisateurs.

**Proxy**

Le proxy permet aux modules métier de communiquer de manière sécurisée avec le système DMP sur Internet. Il se place ainsi en coupure de la communication entre le module métier et le système DMP et réalise une authentification mutuelle avec le système DMP de manière à certifier l'origine du flux HTTP.

Il est recommandé d'implémenter le proxy sous forme de proxy d'infrastructure pour en maîtriser la sécurité et le cloisonnement des certificats de la structure de soins et ainsi ne pas disperser les certifications d'authentification sur les postes de travail des utilisateurs.

**Base des traces**

Cette base contient les traces conformes aux spécifications (annexe 9). Elle est alimentée par les différents composants intervenant dans les échanges :

- Module métier ;
- Module de génération du jeton VIHF ;
- Module d'authentification.

Elle est accédée par les seuls administrateurs habilités via une fonction du module d'administration.

**Module d'administration**

L'administration doit permettre d'appliquer les exigences du système DMP :

- Configuration du certificat de cachet du jeton VIHF ;
- Configuration du certificat d'authentification ;
- Configuration des utilisateurs autorisés à accéder au système DMP ;
- Consultation des traces.

L'accès au module d'administration est restreint aux seuls administrateurs habilités.

**Module d'export des traces**

Sur demande, ce module permet d'extraire les traces de la base de traces.

### 5.3.4.3 Cinématique

L'utilisateur se connecte sur son LPS, il est authentifié au sein de l'annuaire de la structure de soins.

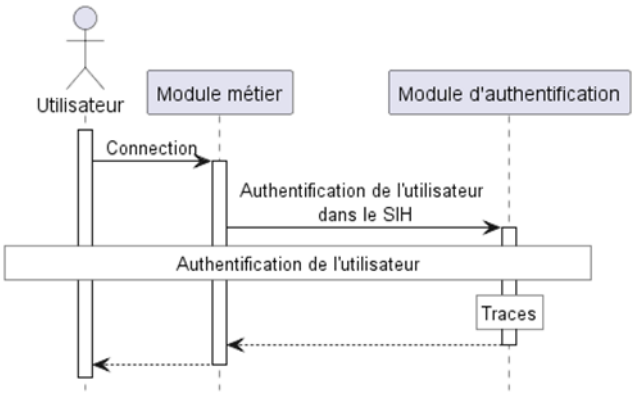



**Figure 38 – Authentification primaire de l'utilisateur**

L'utilisateur sollicite le système DMP.

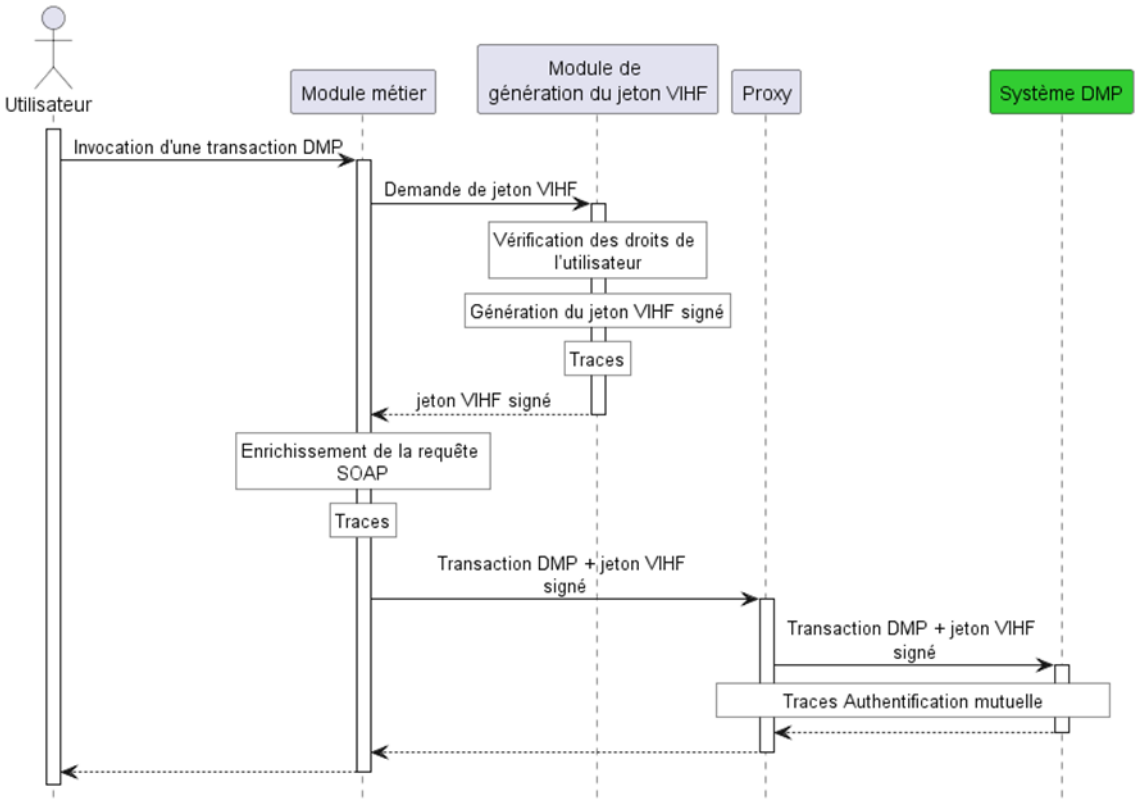



**Figure 39 – cinématique d'accès au système DMP**

- L'utilisateur invoque une transaction DMP sur son module métier.
- Le module métier sollicite le module de génération du jeton VIHF. Un nouveau jeton doit être demandé pour chaque transaction DMP.
- À partir des informations passées par le module métier et à partir des informations du référentiel de sécurité, le module de génération du jeton VIHF élabore le jeton VIHF signé conforme aux spécifications. Chaque génération de jeton VIHF doit être tracée. Le jeton VIHF est retourné au module métier.
- Le module métier insère le jeton VIHF dans les requêtes SOAP vers le système DMP. Un jeton VIHF est émis à chaque requête vers le système DMP, pour transmettre des informations nécessaires à la validation de l'authentification et à la détermination de ses droits d'accès. Le module métier doit tracer chaque sollicitation.
- La communication entre la structure de soins et le système DMP est sécurisée par le proxy de la structure de soins. Le proxy réalise une authentification mutuelle avec le système DMP et chiffre les données transmises via Internet.
- Le système DMP traite la requête et génère une réponse qui est transmise jusqu'au module métier en traversant le canal sécurisé formé entre le proxy de la structure de soins et le système DMP.

### 5.3.4.4 Transaction DMP

Les transactions DMP s'inscrivent dans le CI-SIS.

Toute requête sortante de la structure de soins possède un en-tête WS-Security incluant un jeton VIHF signé de la même manière qu'en authentification indirecte.

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" ... >
  <soap:Header>
    ...
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
    200401-wss-wssecurity-secext-1.0.xsd">

      <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ...>
      ...
      </saml2:Assertion>

    </wsse:Security>
  </soap:Header>
  <soap:Body>
  ...
  </soap:Body>
</soap:Envelope>
```

Si un des contrôles sur le VIHF n'est pas valide, alors une FAULT SOAP est renvoyée au client.

Les traces sont décrites dans l'annexe 9.

Les codes d'erreurs spécifiques sont décrits dans l'annexe A7-2.

### 5.3.4.5 Le jeton VIHF

Les champs SAML standards suivants doivent être renseignés dans l'élément XML `<saml2:Assertion>` par la structure de soins. Les champs sont tous requis à l'exception des attributs XML `<NotBefore>` et `<NotOnOrAfter>`. L'élément XML `<AudienceRestriction>` ne doit pas être présent.

Les tableaux suivants décrivent le contenu du jeton VIHF et les contrôles réalisés par le système DMP (en bleu).

Description de l'assertion `/soap:Envelope/soap:Header/wsse:Security/saml2:Assertion`

| | Champs du VIHF | Valeur |
|---|---|---|
| **Emetteur** | `./ds:Signature`<br>*Signature du VIHF* | Obligatoire<br>Signature XML-DSIG avec le certificat de cachet de la structure de soins<br>Mode EJ : certificat de l'entité juridique<br>Mode EJ/EG : certificat de l'entité juridique<br>Mode EG : certificat de l'entité géographique<br>Contrôle de validité du certificat de cachet.<br>Contrôle d'habilitation à signer du certificat de cachet.<br>Contrôle de la signature du jeton VIHF.<br>Contrôle de cohérence avec le DN de l'issuer. |

| | Champs du VIHF | Valeur |
|---|---|---|
| | ./Issuer<br>*Identité de l'émetteur contenue dans le certificat (DN).* | DN du certificat X509 de cachet utilisé pour signer l'assertion.<br>Mode EJ : DN du certificat de cachet de l'entité juridique<br>Mode EJ/EG : DN du certificat de cachet de l'entité juridique<br>Mode EG : DN du certificat de cachet de l'entité géographique<br>Contrôle de cohérence avec le DN du certificat ayant initié la connexion TLS.<br>Contrôle de cohérence avec le DN du certificat de cachet (le jeton VIHF est signé)<br>Pour le contrôle de cohérence, le système DMP vérifie que les champs suivants sont identiques : CN, OU, O, C |
| | ./Issuer/@Format<br>*Type de valeur utilisée pour renseigner le champ Issuer (X509)* | Constante : « urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName »<br>Contrôle de la valeur |
| **Structure de soins** | Identifiant_Structure<br>*Identifiant de la structure de soins depuis lequel la requête est émise* | Struct_IdNat de la structure de soins<br>Cet identifiant doit être celui inscrit dans la convention signée par la structure de soins (Spécifique au mode AIR).<br>Mode EJ : FINESS de l'entité juridique<br>Mode EJ/EG : FINESS de l'entité géographique<br>Mode EG : FINESS de l'entité géographique<br>Contrôle de présence dans l'annuaire<br>Contrôle de cohérence entre le certificat et la structure fournie. |
| | Secteur_Activite<br>*Secteur d'activité dans lequel exerce l'utilisateur* | Fourni par le système d'information de la structure de soins<br>Contrôle que le secteur d'activité fait partie du jeu de valeurs HealthCareFacilityTypeCode<br>Contrôle que le secteur d'activité ne fait pas partie des secteurs d'activité interdits pour ce mode d'authentification |
| **Utilisateur connecté** | ./Subject/NameID<br>*Identifiant de la personne connectée* | Fourni par le système d'information de la structure de soins<br>Pour les personnes physiques ayant un profil CPS :<br>Format : PS_IdNat<br>Contrôle du 1er chiffre de l'identifiant et que sa longueur est conforme |
| | urn:oasis:names:tc:xspa:1.0:subject:subject-id<br>*Identité de l'utilisateur (ex. nom, prénom et/ou service au sein de la structure de soins)* | Fourni par le système d'information de la structure de soins<br>**Pour les personnes physiques :**<br>Nom, Prénom et Service de l'utilisateur.<br>Contrôle de présence |

| | Champs du VIHF | Valeur |
|---|---|---|
| | `urn:oasis:names:tc:xacml:2.0:subject:role`<br>*(1re occurrence obligatoire)*<br>Prendre la valeur la plus appropriée parmi les codes des terminologies présentées et renseigner :<br>–"code"<br>–"codeSystem"<br>–"displayName" | La première occurrence de cet attribut du VIHF sera considérée comme le code profession de l'utilisateur.<br>**Synthèse :**<br>– Identifie la profession (code profession)<br>– Obligatoire (présent et non vide)<br>– Paramétrage possible dans le système d'information de la structure de soins<br>**Terminologie :**<br>– Pour les utilisateurs, utiliser le jeu de valeurs OID "1.2.250.1.71.1.2.7" (TRE_G15-ProfessionSante)<br>**Exemple :**<br>`<Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="10" codeSystem="1.2.250.1.71.1.2.7" displayName="Médecin"/>`<br>Contrôle que `code` et `codeSystem` font partie du jeu de valeurs autorisé. |
| | `urn:oasis:names:tc:xacml:2.0:subject:role`<br>*(2e occurrence)*<br>Prendre la valeur la plus appropriée parmi les codes des terminologies présentées et renseigner :<br>–"code"<br>–"codeSystem"<br>–"displayName" | **Pour les Médecins et pharmacien**<br>La seconde occurrence de cet attribut sera considérée comme le code de spécialité ordinale de l'utilisateur.<br>**Synthèse :**<br>– Identifie la spécialité<br>– Obligatoire (présent et non vide)<br>– Paramétrage possible dans le système d'information de la structure de soins.<br>**Terminologie :**<br>– Pour les médecins, utiliser le jeu de valeurs OID "1.2.250.1.71.4.2.5" (Ensemble des savoirs faire)<br>– Pour les pharmaciens, utiliser le jeu de valeurs OID "1.2.250.1.71.4.2.6" (Sous-section du tableau de l'Ordre des pharmaciens)<br>**Exemple :**<br><Role xmlns="urn:hl7-org:v3"<br>xsi:type="CE"<br>code="SM54"<br>codeSystem="1.2.250.1.71.4.2.5"<br>displayName="MédecineGénérale (SM)"/><br>Contrôle que code et `codeSystem` font partie du jeu de valeurs autorisé. |

| | Champs du VIHF | Valeur |
|---|---|---|
| | ./AuthnStatement<br>./AuthnContext<br>/AuthnContextClassRef<br>*Déclaration de la classe du contexte d'authentification* | ***Spécifique au mode AIR***<br>Prendre la valeur la plus appropriée parmi les valeurs possibles indiquées dans le document http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf<br>La valeur utilisée doit être cohérente avec le mode d'authentification locale de l'utilisateur dans le système d'information de la structure de soins<br>Contrôle de la valeur |
| | ./AuthnStatement<br>/AuthnContext<br>/AuthnContextDecl<br>*Mode d'authentification primaire du PS* | ***Spécifique au mode AIR***<br>Constante : « CONF_EXI_PGSSIS »<br>Contrôle de la valeur |
| **Assertion SAML** | ./@xmlns<br>*namespace xml SAML* | Constante : « urn:oasis:names:tc:SAML:2.0:assertion »<br>Contrôle de la valeur |
| | ./@Version<br>*Version SAML utilisée* | Constante : « 2.0 »<br>Contrôle de la valeur |
| | ./@ID<br>*Identifiant unique de l'assertion* | identifiant unique de l'assertion |
| | ./@IssueInstant<br>*Date et heure UTC d'émission de l'assertion SAML* | Date et heure d'émission de l'assertion SAML<br>Contrôle que la date d'émission du jeton VIHF :<br>- n'est pas dans le futur (date du système DMP + 3 secondes maximum)<br>- n'a pas plus de 30 secondes de moins que l'heure du système DMP. |
| | ./AuthnStatement/@AuthnInstant<br>*Date et heure locale d'authentification de l'utilisateur dans la structure de soins* | Date et Heure de connexion de l'utilisateur dans le système source |
| | ./Conditions<br>/AudienceRestriction<br>*PSSI (Politique de Sécurité des Systèmes d'Information) applicable* | Ne pas renseigner,<br>car aucune PSSI n'est définie à ce jour |

| | Champs du VIHF | Valeur |
|---|---|---|
| | ./Conditions/@NotBefore<br>*Date et heure UTC de début de validité de l'assertion* | Facultatif<br>Si présent, contrôle de la validité à l'instant i :<br>T < (NotBefore) < i < min(T+30s,NotOnOrAfter) |
| | ./Conditions/@NotOnOrAfter<br>*Date et heure UTC de fin de validité de l'assertion* | |
| | VIHF_Version<br>*Version du VIHF utilisée* | Constante : « 3.0 »<br>Contrôle de la valeur |
| | Authentification_Mode<br>*Mode d'authentification* | Constante : « INDIRECTE_RENFORCEE »<br>Contrôle de la valeur |
| **Patient** | urn:oasis:names:tc:xacml:2.0:resource:resource-id<br>*Identifiant du patient concerné par la requête* | INS du patient<br>Contrôle si présent<br>Obligatoire dans les transactions qui concernent un DMP : TD0.2, TD0.3, TD1.x, TD2.x, TD3.x<br>(INS du patient pour lequel il y a un accès au DMP)<br>***Spécifique au mode AIR***<br>Ce champ est obligatoire pour la TD0.1 et optionnel dans le cas d'un accès Web-PS AIR.<br>Dans le cas d'un accès Web-PS AIR TD0.10, ce champ doit être cohérent avec l'INS du patient présent dans l'URL. |
| **Système cible** | Ressource_URN<br>*Ressource visée par l'utilisateur* | Constante : « urn:dmp »<br>Contrôle de la valeur |
| | urn:oasis:names:tc:xspa:1.0:subject:purposeofuse<br>*Mode d'accès demandé par l'utilisateur.* | code=<br>- "**normal**" : pour un accès normal<br>"**bris_de_glace**" : lorsque le PS a besoin de consulter le DMP d'un patient en cas d'urgence, sans avoir la possibilité de lui demander son autorisation<br>- "**centre_15**" : réservé aux LDR qui indiquent ainsi l'usage « centre de régulation » spécifique à leur rôle<br>Contrôle de valeur |
| | Mode_Acces_Raison.<br>*Explication de la raison de l'usage du bris de glace* | Obligatoire si mode bris de glace.<br>Contrôle de présence si mode bris de glace. |

| | Champs du VIHF | Valeur |
|---|---|---|
| | urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code<br>*Restriction d'audience à appliquer aux traces générées par la transaction objet du flux* | Obligatoire si la fonctionnalité est activée et si demande de connexion secrète au DMP.<br>Valeur "INVISIBLE_REPRESENTANTS_LEGAUX^1.2.250.1.213.1.1.4.13"<br>(traces d'accès au DMP non visibles aux représentants légaux du patient)<br>Ne pas fournir cette donnée dans les autres cas. |
| LPS | LPS_ID<br>*Numéro de série ou identifiant de l'installation du logiciel* | Facultatif<br>(usage à des fins de suivi) |
| | LPS_Nom<br>*Nom du logiciel utilisé* | Nom du système d'information de la structure de soins qui génère le jeton VIHF<br>Contrôle de cohérence avec le n° d'homologation (différentier les différents logiciels associés à un n° d'homologation). |
| | LPS_Version<br>*Version du logiciel utilisé* | N° de version du système d'information de la structure de soins qui génère le jeton VIHF<br>Contrôle de cohérence avec le n° d'homologation (différentier les différentes versions de logiciels associés à un n° d'homologation) |
| | LPS_ID_HOMOLOGATION_DMP.<br>*Numéro d'homologation du logiciel* | N° d'homologation du système d'information de la structure de soins.<br>Contrôle de l'homologation DMP-compatibilité validée pour la transaction appelée |

Les autres champs spécifiés dans le CI-SIS ne sont pas utilisés par le système DMP. Néanmoins, une requête avec un VIHF contenant ces champs ne sera pas rejetée par le système DMP.

## 5.4 TD0.9 Accès Web-PS Contextuel

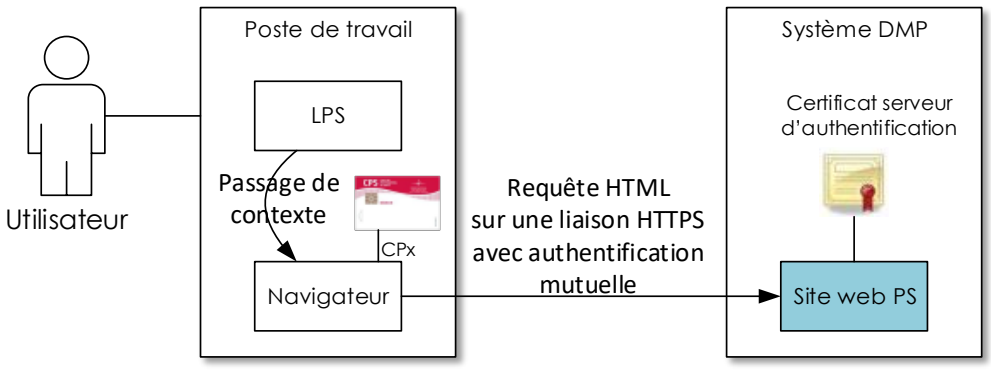



**Figure 40 : passage de contexte (TD0.9)**

Afin de simplifier l'accès du professionnel à certaines fonctionnalités du système DMP directement depuis le LPS, et en fonction du niveau d'intégration de ces fonctionnalités dans le LPS lui-même, le LPS doit être en capacité d'ouvrir une fenêtre navigateur internet sur une URL du système DMP, en passant des éléments de contexte d'utilisation (par exemple en passant le « contexte patient » au système DMP).

L'authentification du professionnel dans ce mode d'appel est assurée par une connexion TLS mutuelle entre le navigateur et le site web PS. La gestion du canal TLS par carte CPx est transparente pour le LPS et intégrée au navigateur dès lors que la librairie cryptographique « CryptoLib » de l'ANS est installée sur le poste du professionnel.

Le code porteur est demandé lors de la première authentification via le navigateur et, selon les navigateurs, lorsque le navigateur est rouvert après fermeture.

Note : Le fonctionnement du site web est hors périmètre de la DMP-compatibilité. Pour plus d'information sur ce sujet, cf. [DMP-ACCES-WEB].

Note 2 : un accès à la TD0.9 en mode Pro Santé Connect est possible. Cf. [FI-]

### 5.4.1 Exigences générales

**EX_GEN-1380**

Pour les LPS implémentant la transaction TD0.9 « Accès Web-PS contextuel», le poste de travail doit être équipé d'un des navigateurs compatibles avec les IHM Web-PS du DMP (voir annexe [DMP1-OS-NAVIGATEURS]).

**EX_GEN-1390**

La configuration du poste de travail pour l'accès web PS ne doit pas perturber le mode de fonctionnement du LPS et la configuration du poste de travail pour le LPS ne doit pas perturber le mode de fonctionnement de l'accès web PS.

**REC_0.9-1010**

La fenêtre de navigateur peut être encapsulée dans le LPS (recommandation forte), ou lancée en « fenêtre externe » (Client lourd) en respectant les contraintes décrites ci-dessous.

Dans le cas où une fenêtre externe est ouverte dans un navigateur, le LPS doit s'assurer qu'il n'existe pas, sur le poste de travail simultanément deux fenêtres DMP ouvertes de façon à éviter toute confusion entre « le patient local » au LPS et « le patient distant » sur le système DMP. Cela peut être réalisé par exemple en plaçant une constante dans le nom de fenêtre lors de sa création.

**EX_0.9-1020**

La mise en œuvre de la transaction TD0.9 passe a minima par l'implémentation de l'accès aux fonctionnalités « Accès au tableau de bord du professionnel » et « Page d'accueil du DMP d'un patient ». Les données en entrées des URL de passage de contexte doivent être respectées.

### 5.4.2 Spécification du passage de contexte

Un LPS peut appeler 9 URL distinctes pour permettre à l'utilisateur d'accéder au site web PS.

Le LPS peut transmettre l'INS du patient (sous la forme `<NIR>/<OID>`). Cet identifiant est représenté par [INS] dans la suite de ce chapitre.

Le LPS peut transmettre un ensemble de paramètres représenté par [paramètres] dans la suite de ce chapitre.

La valeur de l'URL de base (représentée par « URL_BASE » dans la liste suivante) dépend de l'environnement :

- Environnement de production : La valeur de l'URL de base est fournie dans le document [FI-URL].

- Environnement de mise au point : La valeur de l'URL de base est fournie par l'équipe DMP-compatibilité du CNDA.

Une URL de base se compose d'un *nom de domaine* et éventuellement d'une *URL racine*.

En phase de développement, de tests ou d'homologation du LPS, l'éditeur utilisera uniquement l'environnement de mise au point.

**EX_0.9-1030**

Compte tenu du caractère évolutif de l'URL de base, celle-ci doit être paramétrable dans le LPS par l'éditeur.

| # | Fonctionnalité | URL | Liste des paramètres obligatoires | Liste des paramètres optionnels |
|---|---|---|---|---|
| 1 | Accès au tableau de bord du professionnel | https://URL_BASE/AccesDirect/TableauDeBord ou https://URL_BASE/AccesDirect/TableauDeBord/[INS] | aucun | INS du patient |
| 2 | Page d'accueil du DMP d'un patient | https://URL_BASE/AccesDirect/DossierPatient/[INS] | INS du patient | aucun |
| 3 | Page d'information du patient (données administratives) | https://URL_BASE/AccesDirect/GestionDMPPatient/[INS] | INS du patient | aucun |
| 4 | Page de la liste des documents | https://URL_BASE/AccesDirect/Documents/[INS] | INS du patient | aucun |
| 5 | Page du parcours de soins | https://URL_BASE/AccesDirect/ParcoursDeSoins/[INS] | INS du patient | aucun |
| 6 | Page d'historique des accès d'un DMP | https://URL_BASE/AccesDirect/HistoriqueAcces/[INS] | INS du patient | aucun |
| 7 | Page de paramétrage du professionnel | https://URL_BASE/AccesDirect/Parametrages | aucun | aucun |
| 8 | Page du document volontés et souhaits du patient | https://URL_BASE/AccesDirect/VolontesEtDroits/[INS] | INS du patient | aucun |
| 9 | Carnet de vaccination (consultation ou création) | https://URL_BASE/AccesDirect/CarnetVaccination/[INS] | INS du patient | aucun |

**Tableau 27 : structure des URL d'accès direct**

Pour information, le tableau ci-dessous permet de mettre en rapport les transactions DMP des LPS et les URL disponibles pour le passage de contexte.

| | | TD0.9 Accès Web-PS Contextuel | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| AD = accès direct<br>AI = accès intermédiaire requis<br>(l'accès à la TD nécessite de passer par des pages intermédiaires dont le point d'entrée est l'URL indiquée) | | https://../TableauDeBord | https://../TableauDeBord/[INS] | https://../Parametrages | https://../DossierPatient/[INS] | https://../GestionDMPPatient/[INS] | https://../HistoriqueAcces/[INS] | https://../Documents/[INS] | https://../ParcoursDeSoins/[INS] | https://../VolontesEtDroits/[INS] | https://../CarnetVaccination/[INS] |
| TD0.2 | Test d'existence d'un DMP | | **AD** | | | | | | | | |
| TD0.3 | Mise à jour de l'autorisation | | | | **AD** | | | | | | |
| TD0.4 | Liste des dossiers autorisés | | **AD** | | | | | | | | |
| TD1.3 | Mise à jour des données administratives d'un DMP | | | | | **AD** | | | | | |
| TD1.6 | Liste des professionnels autorisés/bloqués sur un DMP | | | | | **AI** | | | | | |
| TD2.1 / TD2.2 | Alimentation en documents d'un DMP | | | | | **AI** | | | | | |
| TD3.1 | Recherche de documents sur un DMP | | | | | | | **AD** | | | **AD** |
| TD3.2 | Consultation d'un document sur un DMP | | | | | | | **AD** | | | |
| TD3.3 | Gestion des attributs d'un document | | | | | | | **AI** | | | |

**Tableau 28 : correspondance entre transactions et URL de passage de contexte**

| **SERVICES DU DMP DISPONIBLES EN ACCES WEB UNIQUEMENT** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Notifications : adresse de réception des alertes | | | **AI** | | | | | | | |
| | Notifications : paramétrage des alertes sur un DMP | | | | | **AI** | | | | | |
| | Traces d'un DMP | | | | | | **AD** | | | | |
| | Situation et cadre d'exercice | | | **AI** | | | | | | | |
| | Préférences Accès Web | | | **AI** | | | | | | | |
| | Demandes de copie partielle ou totale | | | | | **AI** | | | | | |
| | Affichage documents sur " parcours de soins" | | | | | | | | **AD** | | |
| | Page "volontés et droits" du patient | | | | | | | | | **AD** | |

**Tableau 29 : services du DMP disponibles en accès web uniquement**

## 5.5 TD0.10 Accès Web-PS Contextuel en mode AIR

Cette transaction est spécifique à l'authentification indirecte renforcée et offre un accès au DMP par le canal Web-PS sans nécessiter de carte CPx. Un accès Web-PS AIR ne permet pas la lecture de la carte Vitale.

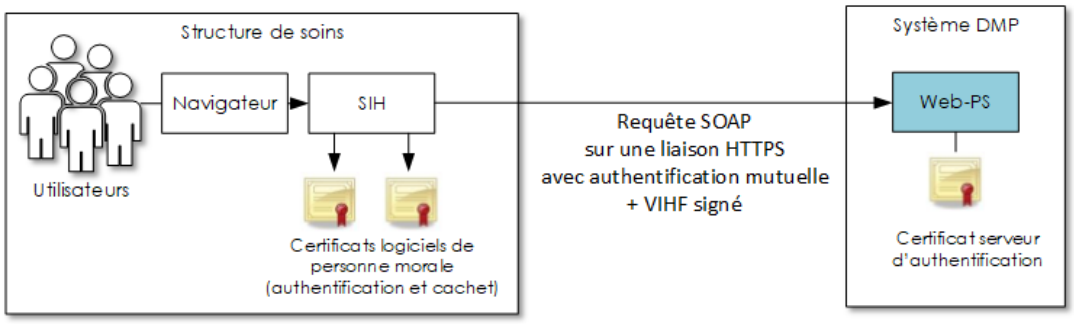



**Figure 41 – Accès Web-PS en mode AIR (TD0.10)**

NB : dans ce chapitre, les schémas illustrent le cas des SIH. Le mode AIR peut cependant s'appliquer au système d'information (SI) d'autres types de structure de soins.

Les exigences de mode AIR s'appliquent à la TD0.10. Cf. 5.3.4.

Le jeton VIHF du mode AIR est utilisé pour la TD0.10. Cf. 5.3.4.5.

Les traces sont décrites dans l'annexe 9.

### 5.5.1 Composants

Techniquement, le mode d'authentification indirecte renforcée vers le système DMP Web-PS repose sur les composants décrits ci-dessous. Ceux-ci peuvent être regroupés au sein d'un unique logiciel ou répartis dans plusieurs briques autonomes du système d'information.

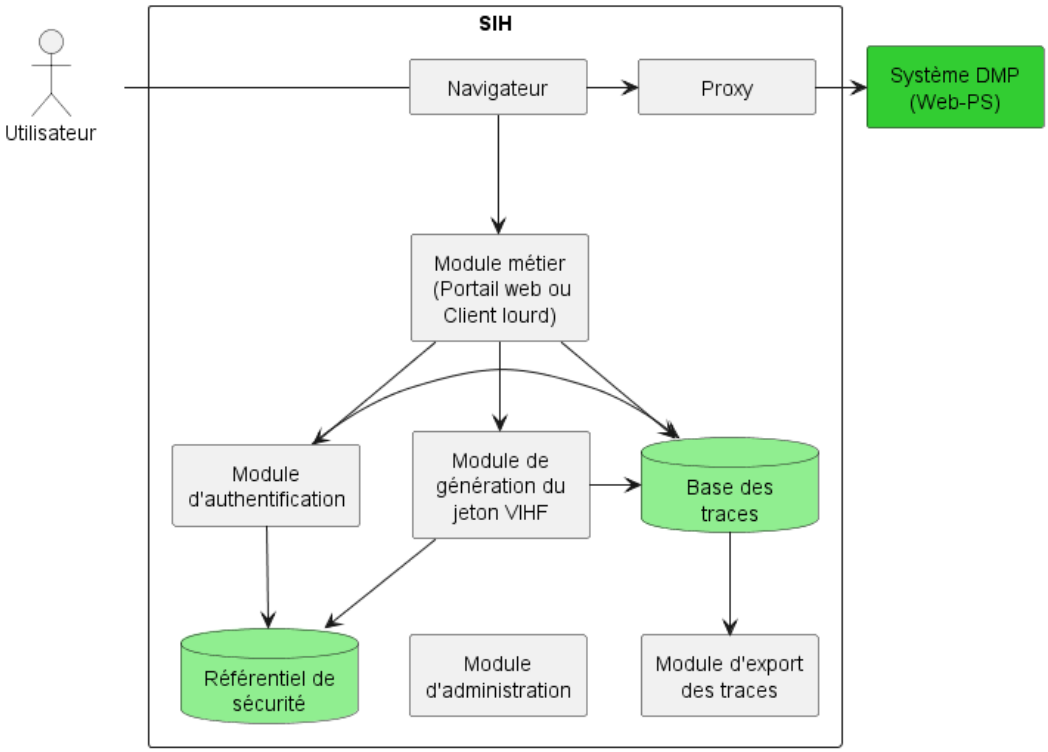



**Figure 42 – Composants minimaux pour l'accès navigateur**

**Le navigateur**

Le navigateur est le client du Système DMP Web-PS. Celui-ci doit se conformer à l'exigence [EX_GEN-1380] du chapitre 5.4.1.

**Le module métier**

Le module métier désigne l'outil utilisé par l'utilisateur pour se connecter au système DMP. Il peut être soit un **client lourd** sur le poste de travail, soit un **portail web interne** qui présenterait les services distants auxquels l'utilisateur a droit.

Le module métier permet aux utilisateurs de s'authentifier, de récupérer un jeton VIHF et d'être redirigés vers le système DMP. Il doit être capable à partir de l'identité de l'utilisateur, de fournir les informations nécessaires au module de génération du VIHF.

**Tous les autres composants peuvent être identiques à ceux mis en place pour l'accès web-service LPS pour le mode AIR (chapitre 5.3.4.2).**

L'établissement de la liaison sécurisée entre le proxy et le Système DMP Web-PS est conforme aux exigences du chapitre 5.3.1.

### 5.5.2 Cinématique

La cinématique d'accès au système DMP Web-PS repose sur les principes du profil SAML HTTP POST Binding[18]. Elle implique les étapes suivantes :

- Authentification de l'utilisateur par le module métier ;
- Ajout d'un jeton VIHF dans la première transaction DMP Web-PS pour transmettre l'identité de l'utilisateur ;
- Utilisation d'un navigateur pour transmettre les flux ;
- Mise en œuvre d'un proxy pour sécuriser les flux sur Internet ;
- Délégation des transactions DMP Web-PS suivantes au navigateur web.

Les échanges SAML sont donc uniquement utilisés à la première connexion de l'utilisateur sur le système DMP Web-PS. On distinguera alors — les échanges lors de la première connexion de l'utilisateur, — des échanges lors des transactions effectuées dans la même session.

Toute fermeture de navigateur ou perte de session utilisateur se traduit par une réauthentification complète avec échange SAML

Les chapitres suivants détaillent deux cinématiques liées au mode d'implémentation du logiciel utilisé par le professionnel.

- La première cinématique est mise en œuvre dans le cas de l'utilisation d'un **client lourd** sur le poste de travail de l'utilisateur.
- La seconde cinématique est mise en œuvre lors de l'utilisation d'un **portail web** dans la structure de soins.

[18] doc. [REF-DMP]

docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf" https://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

### 5.5.2.1 Client lourd, première connexion

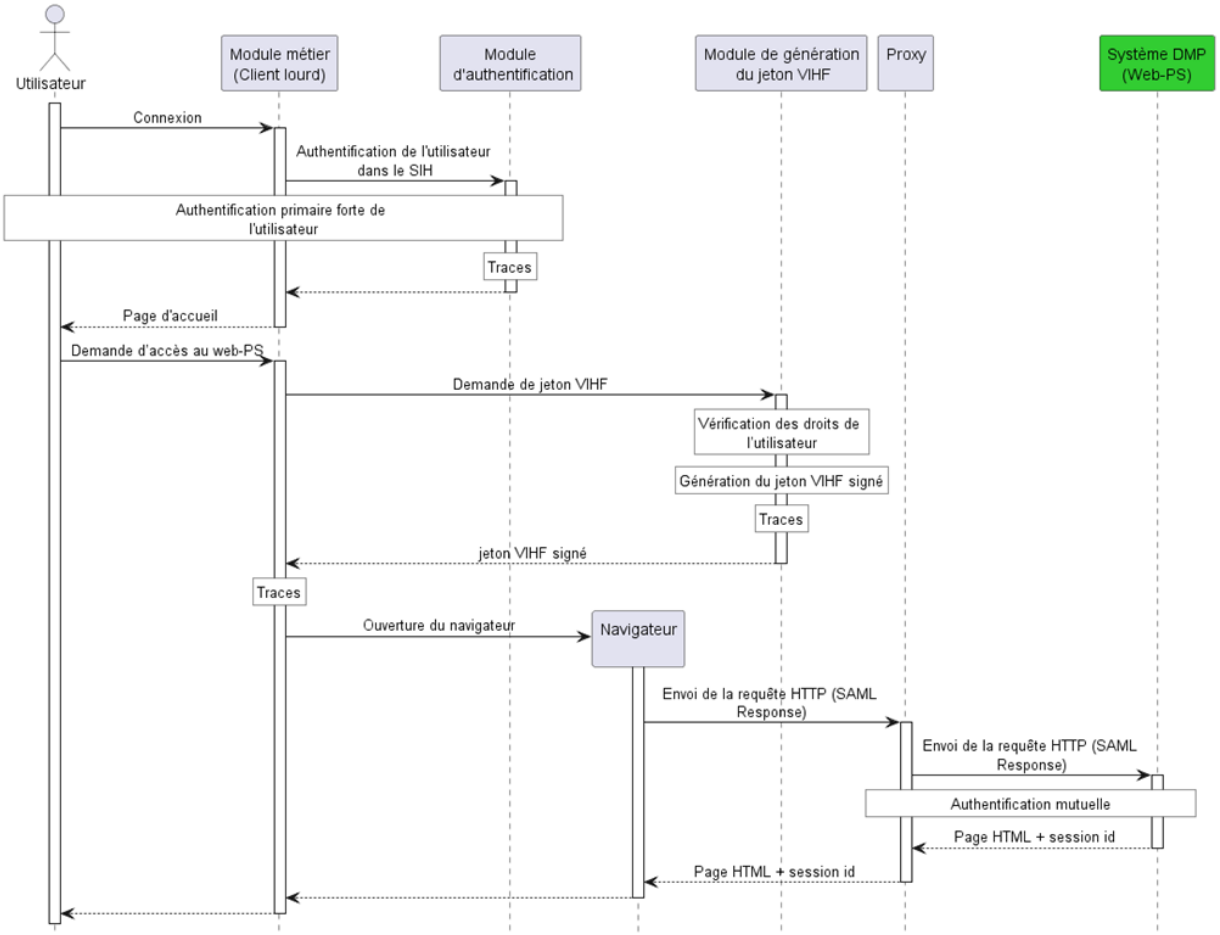



**Figure 43 – accès depuis un client lourd**

- L'utilisateur se connecte sur son module métier (client lourd) et s'authentifie.
- L'utilisateur décide d'accéder au système DMP. Il sélectionne un lien vers le DMP Web-PS que lui présente le module métier.
- Le module métier sollicite le module de génération du jeton VIHF.
- À partir des informations passées par le client lourd et à partir des informations du référentiel de sécurité, le module de génération du jeton VIHF élabore le jeton VIHF signé conforme aux spécifications. Chaque génération de jeton VIHF doit être tracée conformément aux exigences. Le jeton VIHF est retourné au module métier.
- Le module métier insère le jeton VIHF dans un document XML `<SAMLResponse>`. Cet élément est encodé en base 64 et inséré dans une requête POST. Le module métier doit tracer chaque sollicitation.
- Le module métier soumet la requête POST (décrite au chapitre 4.2.4) au système DMP en utilisant soit un navigateur intégré soit un navigateur externe.
- Le navigateur envoie la requête HTTP au système DMP Web-PS au travers du proxy de la structure de soins.
- La communication entre la structure de soins et le système DMP Web-PS est sécurisée par une authentification mutuelle et un chiffrement des données entre le proxy de la structure de soins et le système DMP.
- Le système DMP Web-PS extrait le jeton VIHF, le vérifie et génère une réponse HTML contenant un identifiant de session. L'ensemble est retourné au navigateur en traversant le canal sécurisé formé par le proxy de la structure de soins et le système DMP Web-PS.

### 5.5.2.2 Portail web, première connexion

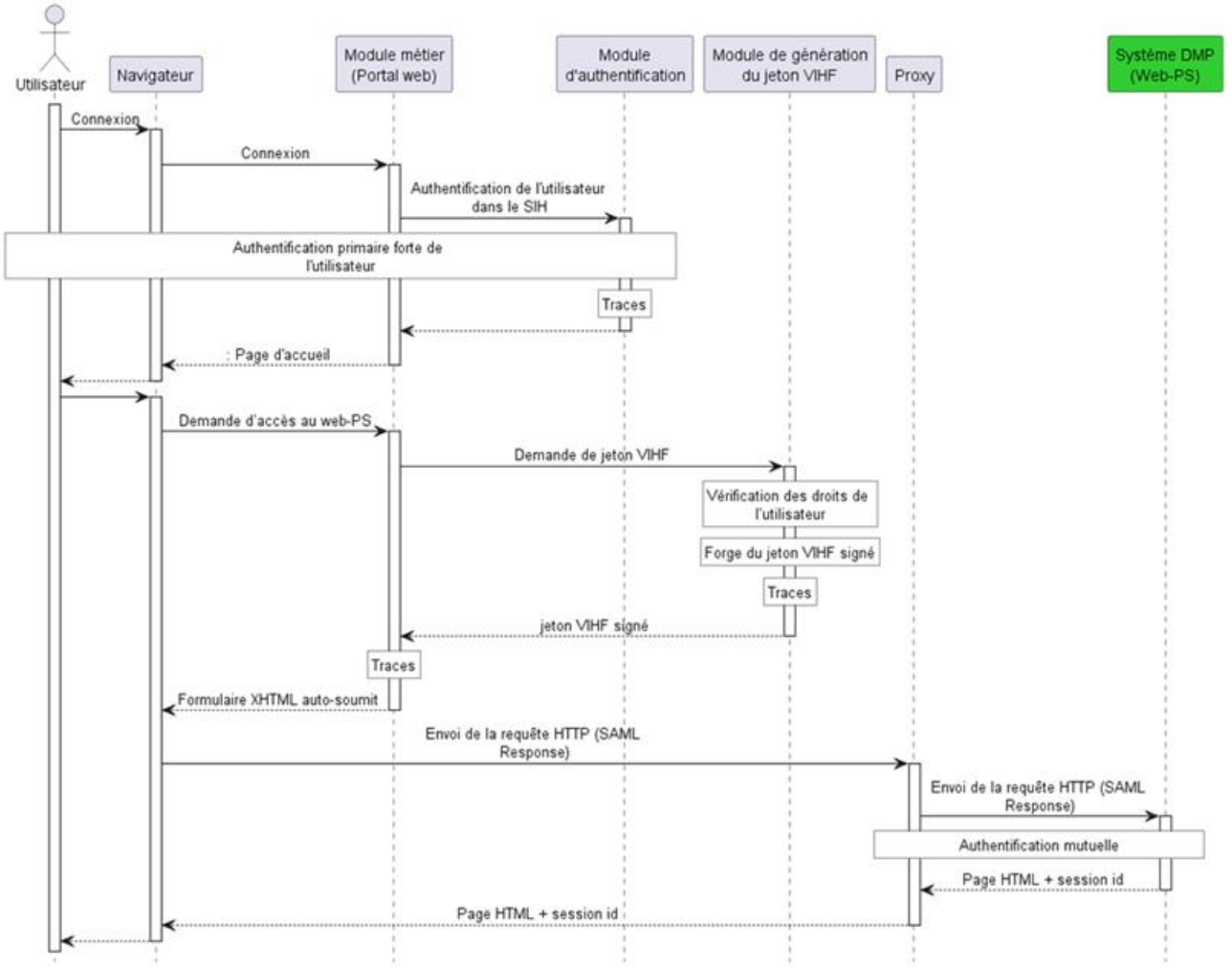



**Figure 44 – Connexion de l'utilisateur**

- L'utilisateur, à l'aide d'un navigateur classique, se connecte sur son module métier (Portail web interne) et s'y authentifie. L'utilisateur décide d'accéder au système DMP Web-PS. Il doit, pour ce faire, sélectionner un lien vers le DMP que lui présente son portail.
- Le portail web interne réceptionne la demande et sollicite le module de génération du jeton VIHF.
- À partir des informations du référentiel de sécurité, le module de génération du jeton VIHF élabore le jeton VIHF signé conforme aux spécifications. Chaque génération de jeton VIHF doit être tracée conformément aux exigences. Le jeton VIHF est retourné au portail web interne.
- Le portail web interne génère un document XML `<SAMLResponse>` contenant le jeton VIHF. Cet élément est encodé en base 64 puis inséré dans un formulaire XHTML auto-soumis qu'il retourne au navigateur web. Le portail web doit tracer chaque sollicitation.
- Le navigateur web soumet automatiquement ce formulaire XHTML dans une requête HTTP (décrite au chapitre 4.2.4) vers le système DMP Web-PS.
- La communication entre la structure de soins et le système DMP Web-PS est sécurisée par une authentification mutuelle et un chiffrement des données.
- Le système DMP extrait le jeton VIHF, le vérifie et génère une réponse HTML contenant un identifiant de session. L'ensemble est retourné au navigateur en traversant le canal sécurisé formé par le proxy de la structure de soins et le système DMP.

**Formulaire XHTML auto-soumis**

La réponse du portail web interne vers le navigateur est une page XHTML contenant un formulaire XHTML auto-soumis en JavaScript.

La page XHTML contient les éléments suivants :

```
<form method="post" action="<url du Web-PS>" ...>
    <input type="hidden" name="SAMLResponse" value="..." />
    ...
</form>
```

- L'action du formulaire (champ `action`)=`<URL du Web-PS>`
- La méthode du formulaire (champ `method`)=`POST`
- Un champ `input` de type « `hidden` » contient un `SAMLResponse` (identique au chapitre précédent) encodé en base 64

L'attribut `RelayState` du profil SAML HTTP POST Binding n'est pas utile pour le cas présent (à ne pas renseigner)

Pour que le navigateur du poste de l'utilisateur final puisse soumettre automatiquement le formulaire, la page XHTML contient l'élément suivant :

```
<body onload="document.forms[0].submit()">
```

### 5.5.2.3 Échanges suivants

Lorsque l'utilisateur est authentifié par le système DMP, tous les échanges suivants sont effectués avec l'identifiant de session fourni par le système DMP.

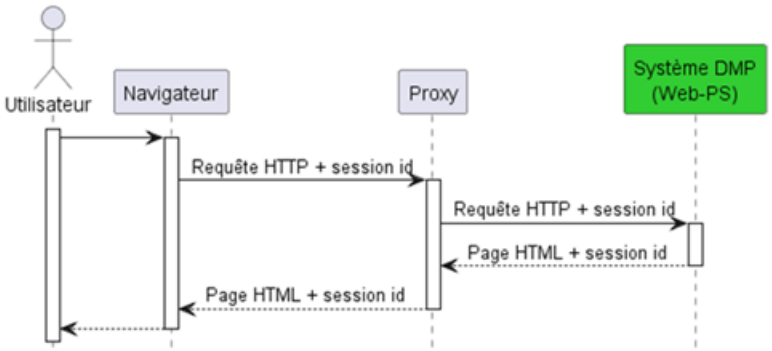



**Figure 45 – Échanges après authentification**

Après l'expiration du délai d'inactivité de la session applicative sur le système DMP Web-PS, l'utilisateur doit s'authentifier à nouveau en fournissant un jeton VIHF.

Les timers d'inactivité et timer de renégociation de la liaison sécurisée sont décrits dans la TD0.1. Cf. chapitre 5.3.1.1.

### 5.5.2.4 Requête HTTP (SAML Response)


**Figure 46 – Requête initiale**

Le corps de la requête POST doit contenir un jeton VIHF signé suivant le profil « SAML POST Binding ».

Spécifications du profil SAML Post Binding :

https://www.oasis-open.org/committees/download.php/56779/sstc-saml-bindings-errata-2.0-wd-06.pdf (Wiki : https://en.wikipedia.org/wiki/SAML_2.0#HTTP_POST_Binding)

### Requête HTTP

Le mode d'authentification renforcée nécessite l'utilisation de la méthode POST.

```
POST <URL du Web-PS> HTTP/1.1
Host : <nom de domaine>
Content-Type : application/x-www-form-urlencoded
Content-Length : nnn

SAMLResponse=<response>
```

`Le champ <response>` contient la `SAMLResponse` encodée en base 64.

L'attribut `RelayState` n'est pas utile pour le cas présent (à ne pas renseigner).

### SAMLResponse

```
<samlp:Response
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  ID=".."
  InResponseTo=""
  Version="2.0"
  IssueInstant="..."
  Destination="...">
  <saml2:Issuer>...</saml2:Issuer>
  <samlp:Status>
    <samlp:StatusCode
    Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml2:Assertion>
  ...
  </saml2:Assertion>
</samlp:Response>
```

| Élément XML | Valeur |
|---|---|
| ./@ID | *Identifiant unique de la SAMLResponse*<br>Format UUID |
| ./@Version | *Version SAML*<br>"2.0" |
| ./@InResponseTo | Vide pour le cas du DMP |
| ./@IssueInstant | *Date/Heure UTC de l'émission de la SAMLReponse*<br>Ce champ doit être identique au champ IssueInstant du jeton VIHF. |
| ./@Destination | *URL du Web-PS appelée en TD0.10*<br>Cet attribut doit être identique à l'URL appelée |
| ./Issuer | *Issuer de la SAMLReponse:*<br>Cet élément XML doit avoir la même valeur que l'élément XML <Issuer> du jeton VIHF |
| ./Status | *Statut de la demande de génération d'assertion.*<br>Le statut doit être en succès.<br><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/> |
| ./Assertion | *Jeton VIHF*<br>Copie de l'élément XML <saml2:Assertion> |

#### 5.5.2.5 Gestion des erreurs

En cas d'erreur, l'utilisateur est redirigé vers une page HTML d'erreur (code de statut HTTP 200). Le détail du message est visible dans le navigateur de l'utilisateur. Le module métier n'a pas la possibilité de récupérer l'erreur, car toutes les transactions sont déléguées au navigateur.

### 5.5.3 URL de la TD0.10

Dans le cadre d'une authentification indirecte renforcée une nouvelle URL s'ajoute :

`https://<nom de domaine>/AccesIndirectRenforce/…`

qui permet d'accéder au Web-PS sans nécessiter de la carte CPx, en transmettant optionnellement le INS-NIR (NIR + OID) en paramètre (ou optionnellement un INS-C).

Le mode d'authentification renforcée nécessite la présence de /AccesIndirectRenforce/ dans l'URL.

Les fonctionnalités sont les mêmes que pour la TD0.9.

Certaines URL ne sont pas accessibles en fonction du profil de l'utilisateur, conformément au tableau des droits fonctionnels (cf. matrice processus, acteurs, médias, onglet Matrice)

En authentification indirecte renforcée, toutes les requêtes initiales contiennent un jeton VIHF et exige l'utilisation de la méthode POST.

Le tableau suivant présente les URL des requêtes HTTP d'accès en authentification indirecte renforcée.

***Accès au tableau de bord du professionnel de santé***

`https://<nom de domaine>/AccesIndirectRenforce/TableauDeBord`

`https://<nom de domaine>/AccesIndirectRenforce/TableauDeBord/<NIR>/<OID>`

***Page récapitulatif du DMP d'un patient***

`https://<nom de domaine>/AccesIndirectRenforce/DossierPatient/<NIR>/<OID>`

***Page d'information du patient (données administratives)***

`https://<nom de domaine>/AccesIndirectRenforce/GestionDMPPatient/<NIR>/<OID>`

***Page de la liste des documents***

`https://<nom de domaine>/AccesIndirectRenforce/Documents/<NIR>/<OID>`

***Page du parcours de soins***

`https://<nom de domaine>/AccesIndirectRenforce/Parcoursdesoins/<NIR>/<OID>`

***Page d'historique des accès d'un DMP***

`https://<nom de domaine>/AccesIndirectRenforce/HistoriqueAcces/<NIR>/<OID>`

***Page de paramétrage du professionnel de santé***

`https://<nom de domaine>/AccesIndirectRenforce/Parametrages`

***Page du document volontés et souhaits du patient***

`https://<nom de domaine>/AccesIndirectRenforce/volontesetdroits/<NIR>/<OID>`

***Page du carnet de vaccination (consultation ou création)***

`https://URL_BASE/AccesIndirectRenforce/CarnetVaccination/<NIR>/<OID>`

## 5.6 Spécifications techniques communes

### 5.6.1 Documentation et références

#### 5.6.1.1 Documentation des web-services

La liste des URL de web-services par transaction et fonction, noms de méthodes, WSDL est fournie dans le tableau suivant

| | Transactions DMP | Standard | Opération | URL WebService (1) | WSDL |
|---|---|---|---|---|---|
| | **Accès sécurisé au DMP d'un patient** | | | | |
| *TD0.2* | Test d'existence et vérification autorisation | HL7 V3 | PatientGetDemographics_ PRPA_IN201307UV02 | /si-dmp-server/v2/services/patients | GestionDossierPatientPartage.wsdl |
| *TD0.3* | Mise à jour de l'autorisation d'accès | (ws) | setAuthorization | /si-dmp-server/v2/services/habilitations | habilitations.wsdl |
| *TD0.4* | Liste des dossiers autorisés | (ws) | patientList | /si-dmp-server/v2/services/patientsSpecific | patientSpecific.wsdl |
| *TD0.5* | Recherche sans INS de patient | IHE-PDQ | PDQSupplier_PRPA IN201305UV02 | /si-dmp-server/v2/services/patientsPDQ | PDQSupplier.wsdl |
| | **Données administrative du DMP d'un patient** | | | | |
| *TD1.3a* | Consultation des données administratives | HL7 V3 | PatientGetDemographics_ PRPA_IN201307UV02 | /si-dmp-server/v2/services/patients | GestionDossierPatientPartage.wsdl |
| *TD1.6* | Liste des professionnels autorisés / bloqués | (ws) | listAuthorizationByPatient | /si-dmp-server/v2/services/habilitations | habilitations.wsdl |
| | **Alimentation du DMP d'un patient** | | | | |
| *TD2.1* | Alimentation en documents | IHE XDS-b | DocumentRepository_ProvideAnd RegisterDocumentSet-b | /si-dmp-server/v2/services/repository | XDS.b_DocumentRepository.wsdl |
| *TD2.2* | Alimentation en documents, par CPE | | DocumentRepository_ProvideAnd RegisterDocumentSet-b | /si-dmp-server/v2/services/repositoryCPE | XDS.b_DocumentRepository.wsdl |
| | **Consultation du DMP d'un patient** | | | | |
| *TD3.1* | Recherche de documents | | DocumentRegistry_RegistryStoredQuery | /si-dmp-server/v2/services/registry | XDS.b_DocumentRegistry.wsdl |
| *TD3.2* | Consultation d'un document | | DocumentRepository_RetrieveDocument Set | /si-dmp-server/v2/services/repository | XDS.b_DocumentRepository.wsdl |
| *TD3.3a* | Masquer/démasquer un document aux professionnels | | DocumentRegistry_UpdateDocumentSet | /si-dmp-server/v2/services/registry | XDS.b_DocumentRegistry.wsdl |

| | Transactions DMP | Standard | Opération | URL WebService (1) | WSDL |
|---|---|---|---|---|---|
| ***TD3.3b*** | Rendre un document visible au patient ou à ses représentants légaux | | DocumentRegistry_UpdateDocumentSet | /si-dmp-server/v2/services/registry | XDS.b_DocumentRegistry.wsdl |
| ***TD3.3c*** | Supprimer un document | | DocumentRegistry_UpdateDocumentSet | /si-dmp-server/v2/services/registry | XDS.b_DocumentRegistry.wsdl |
| ***TD3.3d*** | Archiver/désarchiver un document | | DocumentRegistry_UpdateDocumentSet | /si-dmp-server/v2/services/registry | XDS.b_DocumentRegistry.wsdl |

(1) suffixe d'URL relative par rapport au nom de domaine du serveur

**Tableau 30 : WSDL des services**

**EX_GEN-1221**

Il est demandé à un LPS de prendre en compte rapidement le changement d'un nom de domaine (ou *hostname*) des URL Web Service.

Le délai de mise à jour à respecter sera communiqué par le GIE SESAM-Vitale.

#### 5.6.1.2 OID spécifiques aux messages de gestion du dossier patient

| OID | Utilisation |
|---|---|
| 1.2.250.1.213.4.1.2.2 | codeSystem des codes d'erreur retournés par les messages HL7 V3 |
| 1.2.250.1.213.4.1.2.3 | codeSystem de la nomenclature des politiques de consentements du DMP |
| 1.2.250.1.213.4.1.2.4 | codeSystem de la nomenclature des motifs de fermeture d'un DMP |
| 1.2.250.1.213.4.1.2.5 | nomenclatures d'institutions |
| 1.2.250.1.213.4.1.2.6.1 | codeSystem du concept d'autorisation d'un utilisateur sur un DMP |
| 1.2.250.1.213.4.1.2.6.2 | codeSystem de la nomenclature des valeurs d'autorisation d'un professionnel sur un DMP |
| 1.2.250.1.213.4.1.2.6.3 | codeSystem du concept de statut médecin traitant d'un utilisateur sur un DMP |

**Tableau 31 : OID spécifiques aux messages de gestion administrative du dossier**

### 5.6.2 Structure commune aux messages HL7

Ces fonctions de gestion administrative utilisent majoritairement des messages ***HL7 V3*** *du domaine « Patient Administration / Patient topic » de l'édition normative 2009 HL7 V3*, sur des web-services SOAP. Les messages HL7 sont décrits en détail dans le document [CI-GESTPAT].

Les transactions qui n'utilisent pas HL7 V3 utilisent des web-services propriétaires au système DMP.

#### 5.6.2.1 Encapsulation dans les trames SOAP

Les messages HL7 v3 sont encapsulés dans le corps de la requête SOAP du web-service appelé.

Exemple d'encapsulation :

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns="urn:hl7-org:v3" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
 <soap:Header>
    ...
 </soap:Header>
 <soap:Body>
 <PRPA_IN201311UV02 ITSVersion="XML_1.0">
    ...
 </PRPA_IN201311UV02>
 </soap:Body>
</soap:Envelope>
```

Cette trame est fournie à titre d'exemple, des WSDL fournis en annexe décrivant ces web-services.

#### 5.6.2.2 Notes de lecture

Dans les tableaux des chapitres suivants :

- les lignes en italique correspondent à des éléments parents ne contenant pas de valeur, mais des attributs et/ou des éléments fils ;
- l'indentation de la première colonne correspond à la hiérarchisation des éléments ;
- les éléments sont nommés en notation XPath par rapport à l'élément père ;
- la cardinalité (colonne Card.) intègre la notion de champ obligatoire (card. [1..x]) ou optionnel (card. [0..x]) ; un élément fils obligatoire ne doit être présent que si le père est obligatoire.

Les éléments suivants diffèrent d'un message à l'autre :

- l'élément racine, qui correspond au nom de l'interaction HL7 v3 utilisée ;
- les éléments fils de l'élément controlActProcess, qui correspond au corps de la requête ; ces éléments sont spécifiques à chaque requête et ne sont pas décrits ici (se reporter à la description de chaque message et aux exemples de messages fournis).

#### 5.6.2.3 Messages envoyés en entrée des web-services HL7 V3

**EX_1.X-1210**

Les messages HL7 v3 envoyés en entrée des web-services possèdent la structure commune minimale décrite dans le tableau ci-après

| XPath HL7 | Card. | Valeur / remarque |
|---|---|---|
| PRPA_XXXXXXXX | *[1..1]* | *Racine du message HL7* |
| @ITSVersion | [1..1] | Fixé à « XML_1.0 » |
| Id | *[1..1]* | *Identifiant unique du message HL7 (doit être mondialement unique)* |
| @root | [1..1] | OID racine des identifiants de messages HL7 produits par l'instance du LPS |
| @extension | [1..1] | Identifiant du message produit par le LPS |
| creationTime/@value | [1..1] | date et heure de la création du message au format YYYYMMDDHHMMSS - la date doit être passée en UTC– le LPS doit traduire sa date locale en UTC |
| interactionId | *[1..1]* | |
| @root | [1..1] | Valeur fixée à « 2.16.840.1.113883.1.6 » |
| @extension | [1..1] | Contient le nom de l'interaction HL7 V3 |
| processingCode | *[1..1]* | |
| @code | [1..1] | Les valeurs possibles pour cet élément sont : « P » (production – valeur utilisée en fonctionnement nominal) « D » (test/validation) « T » (formation) |
| processingModeCode | *[1..1]* | *Mode de traitement du message* |
| @code | [1..1] | Valeur fixée à « T » |
| acceptAckCode | *[1..1]* | |
| @code | [1..1] | Valeur fixe ; pour les messages en entrée : « AL » |

| | | |
|---|---|---|
| receiver | *[1..1]* | *Destinataire du message : serveur DMP* |
| @typeCode | [1..1] | Valeur fixée à « RCV » |
| device | *[1..1]* | |
| @classCode | [1..1] | Valeur fixée à « DEV » |
| @determinerCode | [1..1] | Valeur fixée à « INSTANCE » |
| id/@root | [1..1] | OID du serveur DMP : fixé à « 1.2.250.1.213.4.1.1.1 » |
| softwareName | [1..1] | Fixé à « DMP » |
| sender | *[1..1]* | *LPS émetteur du message* |
| @typeCode | [1..1] | Valeur fixée à « SND » |
| device | *[1..1]* | |
| @classCode | [1..1] | Valeur fixée à « DEV » |
| @determinerCode | [1..1] | Valeur fixée à « INSTANCE » |
| id/@root | [1..1] | OID de l'instance du LPS à renseigner par le LPS |
| softwareName | [1..1] | Nom du LPS (libre) |
| controlActProcess[…] | *[1..1]* | *corps de la requête HL7 (voir le détail dans chaque message)* |
| @classCode | [1..1] | Valeur fixée à « CACT » |
| @moodCode | [1..1] | Valeur fixée à « EVN » |

**Tableau 32 : structure commune des messages HL7 en entrée**

### 5.6.2.4 Messages retournés en sortie des web-services HL7 V3

Les messages HL7 v3 retournés par le système DMP en sortie des web-services possèdent la structure commune minimale décrite dans le tableau suivant :

| XPath HL7 | Card. | Valeur / remarque |
|---|---|---|
| PRPA_XXXXXXXX | *[1..1]* | *Racine du message HL7*<br>*Le nom de l'élément prend le nom de l'interaction* |
| @ITSVersion | [1..1] | Fixé à « XML_1.0 » |
| Id | *[1..1]* | *Identifiant unique du message HL7 (doit être mondialement unique)* |
| @root | [1..1] | OID racine des identifiants de messages HL7 produits le DMP<br>fixé à « 1.2.250.1.213.4.1.1.1.1 » |
| @extension | [1..1] | Identifiant du message produit par le système DMP |
| creationTime/@value | [1..1] | date et heure de la création du message au format YYYYMMDDHHMMSS (UTC) |
| interactionId | *[1..1]* | |
| @root | [1..1] | Valeur fixée à « 2.16.840.1.113883.1.6 » |
| @extension | [1..1] | Contient le nom de l'interaction HL7 V3 |
| processingCode | *[1..1]* | |
| @code | [1..1] | Les valeurs possibles pour cet élément sont : « P » (production – valeur utilisée en fonctionnement nominal) « D » (test/validation) « T » (formation) |

| | | |
|---|---|---|
| processingModeCode | *[1..1]* | *Mode de traitement du message* |
| @code | [1..1] | Valeur fixée à « T » |
| acceptAckCode | *[1..1]* | |
| @code | [1..1] | Valeur fixe ; pour les messages en sortie : « NE » |
| receiver | *[1..1]* | *Destinataire du message : LPS ayant fait la requête en entrée correspondante* |
| @typeCode | [1..1] | Valeur fixée à « RCV » |
| device | *[1..1]* | |
| @classCode | [1..1] | Valeur fixée à « DEV » |
| @determinerCode | [1..1] | Valeur fixée à « INSTANCE » |
| id/@root | [1..1] | OID de l'instance du LPS tel qu'il est présent dans le message en entrée correspondant |
| softwareName | [1..1] | Nom du LPS tel qu'il est présent dans le message en entrée correspondant |
| sender | *[1..1]* | *émetteur du message : « DMP »* |
| @typeCode | [1..1] | Valeur fixée à « SND » |
| device | *[1..1]* | |
| @classCode | [1..1] | Valeur fixée à « DEV » |
| @determinerCode | [1..1] | Valeur fixée à « INSTANCE » |
| id/@root | [1..1] | OID du serveur DMP : fixé à « 1.2.250.1.213.4.1.1.1 » |
| softwareName | [1..1] | Fixé à « DMP » |
| *acknowledgement* | *[1..1]* | *Accusé de réception du message de réponse* |
| @typeCode | [1..1] | Type d'accusé de réception :<br>▪ «AA» - « Acknowledgement Accept ». L'application destinatrice a traité correctement le message.<br>▪ «AE» - « Acknowledgement Error ». Une erreur s'est produite lors du traitement du message. |
| *targetMessage* | [1..1] | |
| *Id* | *[1..1]* | *Identifiant du message HL7 d'origine (message en entrée correspondant).*<br>*Dans le cas où une erreur s'est produite avant l'analyse de la requête empêchant ainsi de récupérer l'information id d'origine, le contenu de l'élément extension aura la valeur «* ID_MESSAGE_INCONNU *» (root sera vide)* |
| @root | [1..1] | OID fourni par le LPS dans le message d'origine |
| @extension | [1..1] | Identifiant fourni par le LPS dans le message d'origine |
| acknowledgementDetail | [0..1] | Détail de l'erreur<br>Cardinalité à [1..1] en cas d'erreur (si [acknowledgement/]@typeCode="AE") |
| *code* | *[0..1]* | Code de l'erreur renvoyé<br>Cardinalité à [1..1] en cas d'erreur |
| @code | [0..1] | La valeur du code d'erreur<br>Cardinalité à [1..1] en cas d'erreur |
| @codeSystem | [0..1] | Le système de codage ; pour le DMP : fixé à « 1.2.250.1.213.4.1.2.2 » |

| | | |
|---|---|---|
| | | Cardinalité à [1..1] en cas d'erreur |
| *text* | *[0..1]* | Message texte associé au code d'erreur<br>Cardinalité à [1..1] en cas d'erreur |
| *controlActProcess[…]* | *[1..1]* | *Corps de la requête HL7 de réponse (voir le détail dans chaque message)* |
| @classCode | [1..1] | Valeur fixée à « CACT » |
| @moodCode | [1..1] | Valeur fixée à « EVN » |

**Tableau 33 : structure commune des messages HL7 en sortie**

#### 5.6.2.5 Elément « reasonCode »

Certaines transactions utilisant le même point d'entrée SOAP et le même message, il est nécessaire de distinguer ces messages ; l'élément `controlActProcess/reasonCode` est donc obligatoire sur l'ensemble des messages HL7 V3 de gestion administrative du dossier.

Cet élément est constitué des attributs suivants :

- `reasonCode@code` : code spécifique à la transaction (les codes sont définis dans [CI-GESTPAT]) ;
- `reasonCode@codeSystem` : oid de la nomenclature ; valeur fixe = « 1.2.250.1.213.1.1.4.11 » ;
- `reasonCode@displayName` : libellé associé au code.

Exemple :

```
<PRPA_IN201307UV02 …>
<controlActProcess classCode="CACT" moodCode="EVN">
<reasonCode code="TEST_EXST" codeSystem="1.2.250.1.213.1.1.4.11"
displayName="Test d'existence de dossier"/>
…
</PRPA_IN201307UV02>
```

# 6 EXIGENCES ET RECOMMANDATIONS CONCERNANT LA GESTION DE CERTAINS DOCUMENTS

## 6.1 Note de vaccination et historique de vaccinations - évolution « carnet de vaccinations intégré aux LPS »

L'évolution « carnet de vaccinations intégré aux LPS » amène un nouveau fonctionnement mettant en œuvre des notes de vaccination permettant de manipuler chaque vaccination de manière individuelle. Le LPS peut ajouter, modifier et supprimer une vaccination sans avoir à manipuler l'historique de vaccinations. Pour chaque vaccination, il est possible de distinguer l'auteur de la vaccination, le vaccinateur et le(s) auteur(s) de la note de vaccination (cf. chapitre 6.1.2).

**EX_2.1-2000**

La prise en charge de cette évolution est obligatoire pour les LPS destinés aux médecins (médecine générale et pédiatrie), aux pharmaciens, aux sages-femmes, aux infirmiers ou aux infirmiers psychiatriques (code profession 10, 21, 50, 60 ou 69) en secteur libéral (y compris centres de santé) .

La prise en charge de cette évolution est facultative pour les LPS destinés aux autres codes profession.

### Mise en œuvre

Deux documents de santé sont mis en œuvre dans ce contexte [CI-VAC].

- La note de vaccination (typeCode = 87273-9) permet d'ajouter / modifier / supprimer / valider une vaccination dans l'historique de vaccinations (DMP_2.1a/2.2a, DMP_2.1b/2.2b, DMP_3.1b, DMP_3.3c).
- L'historique de vaccinations (typeCode = 11369-6) regroupe l'ensemble des vaccinations.
  - La création et la mise à jour de ce document à partir des notes de vaccination sont prises en charge par le SI DMP.
  - L'historique de vaccinations peut être recherché (DMP_3.1) et consulté (DMP_3.2). La version de la déclaration de conformité au modèle VAC du CI-SIS dans l'entête du CDA permet de distinguer les différentes versions :
    - Document CVA V1 du DMP : <templateId root="1.2.250.1.213.1.1.1.10"/>
    - Document CVA V2 (2020.01) du DMP (ou CVA V1 complété en V2) : <templateId root="1.2.250.1.213.1.1.1.37" extension="2021.01"/>[19]
    - Document CVA 2023.01 du DMP (mis en œuvre en 2023) : <templateId root="1.2.250.1.213.1.1.1.37" extension="2023.01"/>

**EX_2.1-2005**

Il est interdit d'envoyer une note de vaccination avec un « confidentialityCode » possédant une valeur autre que N (Normal).

NB : il n'est pas possible d'envoyer une note de vaccination en connexion secrète.

[19] Il est à noter qu'il y avait une erreur dans les exemples qui étaient fourni dans le volet VAC 3.1 du CI-SIS et que le templateId d'un CVA conforme au volet 3.1 devait être <templateId root="1.2.250.1.213.1.1.1.37"/> (sans l'extension). Ces exemples ne sont plus fournis par l'ANS.

### Illustration

La mise en œuvre de ces deux documents peut être résumée comme suit.

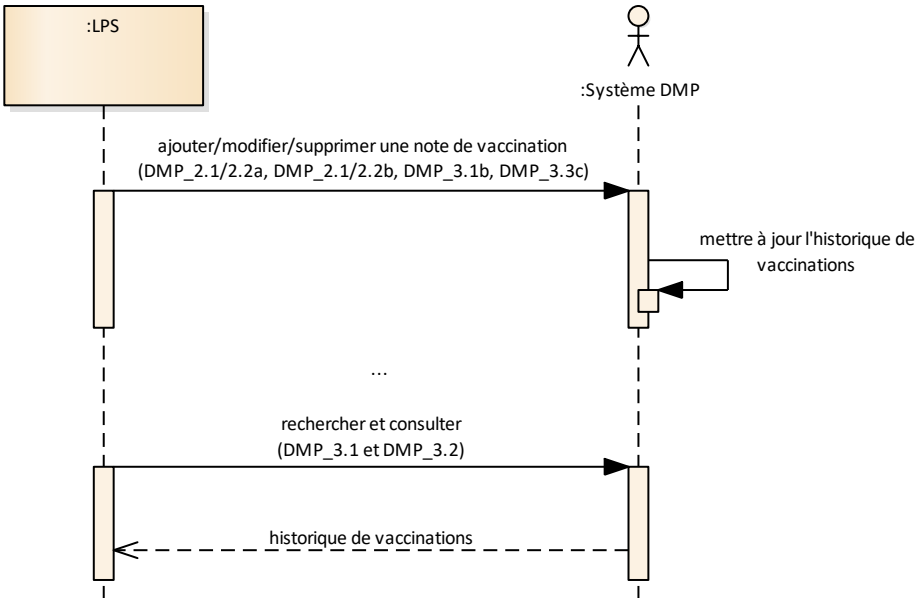



**Figure 47 : mise en œuvre de la note de vaccination et de l'historique de vaccination**

### Ajout d'une vaccination

L'ajout d'une vaccination s'effectue comme suit.

- Le LPS alimente le DMP avec une note de vaccination (DMP_2.1a/2.2a).
- Si l'historique de vaccinations n'existe pas, le SI DMP le crée et y ajoute la vaccination décrite dans la note de vaccination.
- Sinon, le SI DMP met à jour l'historique de vaccinations en y ajoutant la vaccination décrite dans la note de vaccination.

NB : il n'est pas nécessaire de consulter l'historique de vaccination avant d'alimenter le DMP avec une note de vaccination.

### Modification d'une vaccination

La modification d'une vaccination s'effectue via une modification de la note de vaccination concernée en deux étapes.

- Rechercher l'identifiant technique d'un document (DMP_3.1b)[20],
- Remplacer un document existant dans le DMP d'un patient (DMP_2.1b/2.2b).

### Suppression d'une vaccination

La suppression d'une vaccination s'effectue via une suppression de la note de vaccination concernée en deux étapes.

- Rechercher l'identifiant technique d'un document (DMP_3.1b)[20],
- Supprimer un document (DMP_3.3c).

[20] Les notes de vaccination sont enregistrés par le SI DMP au statut archivé (urn:asip:ci-sis:2010:StatusType:Archived). Il faut donc inclure les documents « Archived » aux recherches si on souhaite lister les notes de vaccination.

**Validation d'une vaccination**

Le fonctionnement suivant permet de valider une vaccination enregistrée par le patient.

- Le LPS alimente le DMP avec une nouvelle note de vaccination reprenant le même code CIS et la même date[21] que la vaccination à valider.
- Le SI DMP met à jour l'historique de vaccinations en supprimant la vaccination enregistrée par le patient et en ajoutant la vaccination enregistrée par le professionnel.

NB1 : il n'est pas nécessaire de consulter l'historique de vaccination avant de valider une vaccination enregistrée par le patient.

NB2 : les identifiants uniques des deux vaccinations sont différents.

NB3 : la validation s'effectue sous la responsabilité du professionnel, sur la base d'un document attestant l'identité du vaccinateur.

**Limitations**

Les limitations suivantes sont à noter concernant la note de vaccination.

- Dans un premier temps, seules les vaccinations effectuées sont prises en charge.
- Une note de vaccination peut être recherchée (DMP_3.1) mais ne peut pas être consultée (DMP_3.2).
- Une note de vaccination ne peut pas être masquée / démasquée aux professionnels (DMP_3.3a).
- Il est possible de rendre une vaccination visible au patient ou à ses représentants légaux (DMP_3.3b) mais cette action est sans effet sur l'historique de vaccinations dans le DMP.
- Une note de vaccination ne peut pas être archivée/désarchivée (DMP_3.3d).

Concernant l'historique de vaccinations, aucune action n'est réalisable sur ce document via l'interface LPS en dehors de la recherche (DMP_3.1) et de la consultation (DMP_3.2).

En cas d'alimentation d'une vaccination via le site web PS, aucune modification/suppression de cette vaccination n'est possible via l'interface LPS.

### 6.1.1 Nombre de vaccination par note de vaccination

**EX_2.1-2010**

Une note de vaccination ne peut contenir qu'une seule vaccination à des fins de granularité « unitaire » des actions de modification et de suppression de vaccination dans l'historique de vaccinations.

Un LPS peut néanmoins alimenter simultanément un DMP avec plusieurs notes de vaccination dans le même lot de soumission (1 seule requête vers le DMP contenant plusieurs notes de vaccination). Ceci doit être transparent pour l'utilisateur.

Il est exigé que ces notes soient toutes en version identique 2023.01.

[21] le code CIS est situé dans …/`manufacturedMaterial/code/@code`
(avec …/`manufacturedMaterial/code/@codeSystem="1.2.250.1.213.2.3.1"`)
et la date est située dans …/`effectiveTime/@value`

### 6.1.2 Auteur de la vaccination, vaccinateur et auteur(s) de la note de vaccination

**EX_2.1-2020**

Les acteurs « auteur de vaccination » et « vaccinateur » présents dans le contenu de la note de vaccination doivent (lorsque connus) également être ajoutés dans la liste des auteurs de la note de vaccination : cela permet à ces acteurs de pouvoir ensuite modifier ou supprimer la note de vaccination et donc les données de la vaccination dans l'historique de vaccinations.

L'acteur « vaccinateur » doit (lorsque connu) également être présent sous l'élément CDA `documentationOf/serviceEvent/performer` de l'acte principal documenté puisqu'il ne peut y avoir qu'une seule vaccination par note de vaccination.

Il est rappelé que les métadonnées présentes dans l'entête CDA doivent également être par cohérence présentes dans les métadonnées XDS (règle de DMP compatibilité), le nombre d'auteurs devra donc être identique entre la partie XDS et la partie entête CDA.

**Illustration**

Les cas présentés ci-dessous expliquent comment identifier l'auteur de la vaccination, le vaccinateur ainsi que l'auteur (ou les auteurs) de la note de vaccination.

- Cas simple : un médecin généraliste réalise une vaccination et enregistre cet acte dans le DMP.
  - L'auteur de la vaccination est le médecin généraliste.
  - Le vaccinateur est le médecin généraliste.
  - L'auteur de la note de vaccination est le médecin généraliste.
- Cas de reprise d'antériorité par un professionnel (appelé P1) d'une vaccination réalisée par un autre professionnel (appelé P2).
  - L'auteur de la vaccination est P1.
  - Le vaccinateur est P2.
  - Les auteurs de la note de vaccination sont P1 et P2.
- Cas de saisie par un médecin traitant DMP (appelé MT1) autre que l'auteur de la vaccination (appelé P2) ou le vaccinateur (appelé P3).
  - L'auteur de la vaccination est P2.
  - Le vaccinateur est P3.
  - Les auteurs de la note de vaccination sont MT1 et P2 (et P3 si différent de P2).
- Cas de saisie par une personne exerçant sous la responsabilité d'un ou plusieurs professionnel(s) (appelé A1) autre que l'auteur de la vaccination (appelé P2) ou le vaccinateur (appelé P3). Par exemple, la saisie peut être effectuée par une secrétaire médicale ou un préparateur en pharmacie équipé(e) d'une CPE.
  - L'auteur de la vaccination est P2.
  - Le vaccinateur est P3.
  - Les auteurs de la note de vaccination sont A1 et P2 (et P3 si différent de P2).
- Cas de saisie en authentification indirecte dans une structure de soins (appelée S1 en tant que « structure d'exercice de l'auteur ») par un professionnel (appelé P2) d'une vaccination réalisée par un professionnel (appelé P3).
  - L'auteur de la vaccination est P2.
  - Le vaccinateur est P3.

- Les auteurs de la note de vaccination sont S1 (authorInstitution) et P2 (authorPerson) (et P3 si différent de P2).

NB : l'auteur ne peut pas être un non PS ; la donnée profession/savoir-faire de l'auteur PS est obligatoire.

### 6.1.3 Identifiant des vaccinations

**EX_2.1-2030**

Les identifiants des vaccinations (i.e. identifiant des `entry/substanceAdministration`) dans les notes de vaccination doivent être générés de manière « mondialement unique », via un UUID (voir https://fr.wikipedia.org/wiki/Universally_unique_identifier) dans l'attribut `id/@root` seulement.

Cet identifiant sert ensuite à retrouver la vaccination dans l'historique de vaccinations lors de sa mise à jour par le SI DMP. Il ne doit donc jamais rentrer en conflit avec l'identifiant d'une autre vaccination.

Exemple :

```
<entry>
  <substanceAdministration classCode="SBADM" moodCode="EVN">
  [...]
    <id root="5ec4b84e-3082-4fea-9255-9b7fc7c3dfd0"/>
```

### 6.1.4 Données d'une note de vaccination

**EX_2.1-2035**

Seule la version 2023.01 du 08/03/2023 du volet VAC (CI-SIS) doit être utilisée pour l'alimentation du DMP.

**Illustrations**

***Données décrivant un vaccinateur connu et identifié avec un identifiant national de professionnel***

```
<performer typeCode="PRF">
    <assignedEntity>
        <id root="1.2.250.1.71.4.2.1" extension="899700195276" />
        <code    code="G15_10/SM41"    codeSystem="1.2.250.1.213.1.1.4.5"
displayName="Médecin - Pneumologie (SM)" />
        <addr nullFlavor="NASK"/>
        <telecom nullFlavor="NASK"/>
        <assignedPerson>
            <name>
                <given>ROBERT</given>
                <family>SPECIALISTE0019527</family>
            </name>
        </assignedPerson>
        <representedOrganization>
            <id root="1.2.250.1.71.4.2.2" extension="499700195276008"/>
            <name>CABINET M SPECIALISTE0019527</name>
        </representedOrganization>
    </assignedEntity>
</performer>
```

***Données décrivant un vaccinateur connu et non identifiable avec un identifiant national de professionnel***

```
<performer typeCode="PRF">
```

```
        <assignedEntity>
            <id nullFlavor="UNK" />
            <assignedPerson>
                <name>
                    <family>DURANT PAUL</family>
                </name>
            </assignedPerson>
        </assignedEntity>
    </performer>
```

## 6.2 Données de remboursement

Ce chapitre décrit les spécificités de l'interface LPS liées aux données de remboursement dans le DMP.

Ces données correspondent aux documents dont le `typeCode` est égal à « REMB ».

### Ajouter / modifier

Il n'est pas possible d'alimenter un DMP avec des données de remboursement.

Cf. exigence EX_2.1-1010 au chapitre 3.4.1.1.1.

### Modifier des attributs

Cette partie décrit les spécificités des modifications d'attributs en complément de la description de la fonctionnalité DMP_3.3 décrite au chapitre 3.5.3.

Il n'est pas possible de rendre des données de remboursement invisibles au patient et/ou aux représentants légaux.

Il n'est pas possible d'archiver ou de supprimer des données de remboursement.

### Rechercher

Cette partie décrit les spécificités des recherches de données de remboursement en complément de la description de la fonctionnalité DMP_3.1 décrite au chapitre 3.5.1.

#### *Préambule*

En production, les données de remboursements alimentées dans les DMP à partir de début 2022 (avec un historique potentiel de 12 mois) sont retournées aux LPS sous la forme d'un document CDA R2 **construit dynamiquement en fonction des critères de recherche fournis dans la TD3.1** (date de début et/ou date de fin). Les données du CDA R2 retournées sont uniquement celles incluses dans la période de recherche. Cf. les différents cas possibles dans les sections suivantes de ce chapitre. A partir de 2022, en cas de présence de données de remboursement, le document construit dynamiquement remplace le ou les éventuels documents précédents.

Par ailleurs les données « historique de remboursement » alimentées sous forme de document CDA « figé » par l'Assurance Maladie (non structuré en PDF ou en CDA structuré) perdurent également dans les DMP pour la période 2016 - 2021).

En fonction de la période de recherche, la requête de recherche des méta-données (TD3.1) peut retourner, si elle inclut les documents obsolètes :

- un document construit dynamiquement pour les remboursements à partir de 2022 (avec un historique potentiel de 12 mois),
- et/ou des documents « figés » concernant les remboursements entre 2016 et 2021 (au statut obsolète).

***Recherche de données de remboursement avec la requête `FindDocuments` avec les paramètres date de début et/ou date de fin d'acte (`$XDSDocumentEntryServiceStartTimeFrom` et/ou `$XDSDocumentEntryServiceStopTimeTo`)***

**EX_3.1-1015**

En cas de recherche de données de remboursement (typeCode REMB) avec la requête `FindDocuments` et les paramètres date de début (`$XDSDocumentEntryServiceStartTimeFrom`) et date de fin d'acte (`$XDSDocumentEntryServiceStopTimeTo`), la durée de la période de recherche entre ces deux dates doit être inférieure ou égale à la valeur du paramètre `hr-periode-max-mois` défini au chapitre 3.1.1.

Si seule la date de début (`$XDSDocumentEntryServiceStartTimeFrom`) est indiquée, la période de recherche considérée s'étend jusqu'à la date courante.

Pour information :

- si seule la date de début (`$XDSDocumentEntryServiceStartTimeFrom`) est indiquée et que la durée de la période entre cette date et la date courante est inférieure à la valeur du paramètre `hr-periode-max-mois`, la période de recherche correspond aux 12 mois suivant cette date de début ;
- si seule la date de fin (`$XDSDocumentEntryServiceStopTimeTo`) est indiquée, la période de recherche correspond aux 12 mois précédant cette date de fin.

NB : la durée de 12 mois est paramétrable dans le SI DMP et peut être amenée à évoluer.

***Recherche de tous les documents d'un DMP avec la requête `FindDocuments` avec les paramètres date de début et/ou date de fin d'acte (`$XDSDocumentEntryServiceStartTimeFrom` et `$XDSDocumentEntryServiceStopTimeTo`)***

La durée de la période de recherche des données de remboursement est limitée à la valeur du paramètre `hr-periode-max-mois` par le SI DMP. La période de recherche est déterminée par le SI DMP en fonction des dates passées en paramètre.

| Date(s) passée(s) en paramètre | | Période de recherche |
|---|---|---|
| date de début seule (`$XDSDocumentEntryServiceStartTimeFrom`) | | P mois suivant la date de début. |
| date de fin seule (`$XDSDocumentEntryServiceStopTimeTo`) | | P mois précédant la date de fin. |
| date de début (`$XDSDocumentEntryServiceStartTimeFrom`) et date de fin (`$XDSDocumentEntryServiceStopTimeTo`) | si période ≤ P mois | Période définie par la date de début et la date de fin. |
| | si période > P mois | P mois précédant la date courante. |

NB : P est la valeur du paramètre `hr-periode-max-mois`.

***Recherches sans paramètre date de début ni date de fin d'acte (`$XDSDocumentEntryServiceStartTimeFrom` / `$XDSDocumentEntryServiceStopTimeTo`)***

Pour toutes les requêtes de recherche de document (`FindDocuments` ou autres), si aucune date de début ni de fin n'est passée en paramètre, les données de remboursement correspondent aux 12 mois précédant la date du remboursement le plus récent dans le DMP du patient.

NB : la durée de 12 mois est paramétrable dans le SI DMP et peut être amenée à évoluer.

## 6.3 Imagerie

Le SI DMP met en œuvre trois nouveaux types de document :

- La demande d'acte d'imagerie (format CDA R2 Niveau 1) ;
- La référence aux objets d'un examen d'imagerie (format KOS DICOM ; formatCode : code=1.2.840.10008.5.1.4.1.1.88.59 / codingScheme = 1.2.840.10008.2.6.1, mimeType : « application/dicom ») ;
- Le compte-rendu d'imagerie (format CDA R2 Niveau 1).

Il est possible d'effectuer, sur ces documents, les mêmes actions que pour les autres documents du DMP (alimentation, recherche, consultation, masquage, archivage, suppression, remplacement, …).

Le SI DMP ne stocke pas les images/vidéos et ne gère pas l'accès aux images/vidéos ; Les documents référence aux objets d'un examen d'imagerie (format KOS DICOM) contiennent un lien permettant d'accéder aux images/vidéo ainsi que des métadonnées de l'examen d'imagerie référencé dans le KOS. Les modalités d'accès aux images/vidéos (ressources DICOMWeb) sont en dehors de la DMP-compatibilité des LPS. Cf. le volet Accès aux documents de santé en Imagerie du CI-SIS pour plus d'information.

Le SI DMP distingue deux types de LPS :

- Les LPS « compatibles partage d'imagerie » capables de lire un document au format « KOS DICOM » et d'accéder aux images/vidéos. Le LPS peut, s'il le désire, accéder aux images/vidéos, s'il dispose d'un Viewer DICOM.
- Les LPS « non compatibles partage d'imagerie » pour lesquels le SI DMP a un comportement spécifique. Cf. chapitre 6.3.3.

Chaque LPS doit être déclaré compatible (ou non compatible) avec le partage d'imagerie lors de son homologation DMP. En l'absence de déclaration, les LPS sont considérés par défaut comme non compatibles avec le partage d'imagerie.

### 6.3.1 Alimentation

Les LPS DMP-compatibles peuvent alimenter le SI DMP avec les documents d'imagerie suivants :

- KOS DICOM pour les LPS type PACS, DRIMbox ;
- « CR d'imagerie médicale » pour les LPS types RIS, DPI et autres ;
- Demande d'actes d'imagerie pour les LPS types LGC, DPI et autres.

Les LPS DMP-compatibles et sachant produire des documents « KOS DICOM », « CR d'imagerie » et/ou « demande d'acte d'imagerie » peuvent alimenter le SI DMP avec ces documents.

Contrainte : le SI DMP n'accepte pas les doublons de documents (binaire strictement identique). En cas de détection de doublon, le SI DMP retourne une erreur `XDSDuplicateUniqueIdInRegistry` au LPS.

Plusieurs documents d'imagerie peuvent être liés fonctionnellement en utilisant des « identifiants de référence » renseignés dans la métadonnée `referenceIdList` conformément aux volets ad-hoc du CI-SIS. NB : le SI DMP ne propage pas les actions effectuées sur un document aux documents qui lui sont liés, notamment en cas de suppression.

### 6.3.2 Recherche de documents d'imagerie

Le LPS peut utiliser tous les types de recherche de la transaction TD3.1, notamment :

- la recherche `FindDocuments` de base sans critère optionnel,

- et la recherche `FindDocumentByReferenceId` (identique au FindDocuments) en utilisant un « identifiant de référence » dans le critère `$XDSDocumentEntryReferenceIdList`.

Ces recherches sont possibles pour tous les LPS (compatibles avec le partage d'imagerie ou non).

**EX_3.1-2000**

L'implémentation de la recherche FindDocumentByReferenceId est obligatoire pour les LPS compatibles avec le partage d'imagerie.

Exemple : Récupération d'un KOS en passant en FindDocumentByReferenceId le StudyInstanceUID.

### 6.3.3 Consultation

Tous les LPS peuvent consulter les documents « CR d'imagerie » et « demande d'acte d'imagerie », qu'ils soient compatibles ou non avec le partage d'imagerie.

Pour les documents « KOS DICOM », le comportement du SI-DMP dépend de la compatibilité du LPS avec le partage d'imagerie.

- Si le LPS est déclaré compatible avec le partage d'imagerie, le SI DMP retourne les documents « KOS DICOM ».
- Sinon, le SI DMP retourne à la place de chacun des documents KOS DICOM un document générique (au format CDA R2 Niveau 1) avec un corps en texte brut indiquant des informations générales sur l'examen (Modalités, Régions Anatomiques …) et que le LPS ne permet pas de consulter les documents de références aux objets d'un examen d'imagerie.

# ANNEXES

## ANNEXE 1 GUIDE DE LECTURE

### Indications dans la marge

Les éléments importants et les remarques sont indiqués par une flèche dans la marge.

Les questions importantes sont indiquées par un point d'interrogation dans la marge.

Les alertes importantes sont indiquées par ce pictogramme dans la marge.

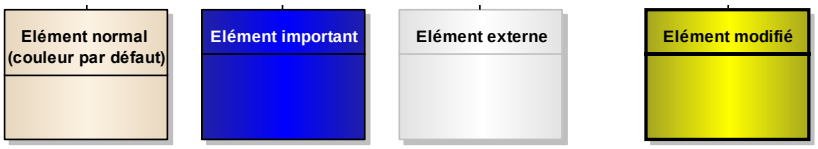
Les références documentaires sont indiquées par ce pictogramme dans la marge.

### Codes couleur

Les codes couleur suivants sont utilisés dans ce document :

- Texte surligné jaune = texte ajouté par rapport à la version précédente
- ~~Texte barré ou barré surligné jaune~~ = texte supprimé

Pour les diagrammes les codes couleur sont les suivants :




### Références

Certains éléments dans ce document sont référencés à l'aide d'un identifiant unique au sein de ce document. Les références suivantes sont utilisées :

- RG_... pour les règles de gestion ;
- EF_... pour les entités fonctionnelles ;
- CE_... pour les cas d'erreur (arrêt du fonctionnement du système) ;
- CP_… pour les cas particuliers (pas d'arrêt du fonctionnement du système) ;
- …

Ces références sont utilisées pour faire des renvois explicites vers les éléments concernés. NB : pour une donnée unitaire, on ajoute l'indice de cette donnée à la référence de l'entité fonctionnelle. Par exemple : EF_01_01 est un renvoi vers la première donnée unitaire de l'entité EF_01.

# ANNEXE 2 ABREVIATIONS

| Abréviations | |
|---|---|
| AC | Autorité de Certification |
| ADELI | Automatisation des Listes (répertoire de professionnels de santé en cours de remplacement par le RPPS) |
| AIR | Authentification indirecte renforcée |
| AFNOR | Agence Française de Normalisation |
| ANS | Agence du Numérique en Santé |
| ApCV | Application carte Vitale |
| CDA | Clinical Document Architecture |
| CI-SIS | Cadre d'interopérabilité des Systèmes d'Information de Santé de l'ANS |
| CNDA | Centre National de Dépôt et d'Agrément |
| CPE | Carte de Professionnel d'Etablissement |
| CPF | Carte de Professionnel de santé en Formation |
| CPS | Carte de Professionnel de Santé |
| CPx | CPS, CPF ou CPE |
| DMP | Dossier Médical Partagé |
| DN | Distinguished Name |
| EAI | Enterprise Application Integration |
| EG | Entité Géographique |
| EJ | Entité Juridique |
| FINESS | Fichier National des Etablissements Sanitaires et Sociaux |
| GAM | Gestion Administrative des Malades |
| HL7 | Health Level 7 |
| IHE | Integrating the Healthcare Enterprise |
| IGC | Infrastructure de Gestion de Clés |
| INS | Identifiant National de Santé |
| LDRM | Logiciel De Régulation Médicale |
| LPS | Logiciels de Professionnel de Santé |
| OID | Object Identifier (identifiant d'objets) |
| OTP | One Time Password (code d'accès à usage unique) |
| PDQ | Patient Demographic Query |
| PS | Professionnel de Santé |
| RASS | Référentiel des Acteurs Santé Social |
| RPPS | Répertoire Partagé des Professionnels de Santé |
| SAML | Security Assertion Markup Language |
| SAMU | Service d'Aide Médicale Urgente |

| | |
|---|---|
| SI DMP | Système Dossier Médical Partagé |
| SI | Système d'Information |
| SIH | Système d'Information Hospitalier |
| SIS | Système d'Information de Santé |
| SOAP | Simple Object Access Protocol |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| UTC | Universal Time Coordinated |
| VIHF | Vecteur d'Identification et d'Habilitation Formelles |
| XDS | Cross enterprise Document Sharing |

**Tableau 34 : abréviations**

# ANNEXE 3 (SANS OBJET)

# ANNEXE 4 DOCUMENTS DE REFERENCE

Le référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP) dans sa version de référence est disponible sur le site esante.gouv.fr.

| Appellation | Type et titre | Référence |
|---|---|---|
| REF-DMP | Référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP) | referentiel-de-securite-et-dinteroperabilite-relatif-a-lacces-des-professionnels-au-dossier-medical-partage-(dmp)… .pdf |

**Tableau 35 : référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP)**

Les documents du CI-SIS applicables sont présentés dans le tableau ci-dessous. Ils sont disponibles sur le site de l'ANS (https://esante.gouv.fr/offres-services/ci-sis/espace-publication).

| Appellation | Type et titre | Référence |
|---|---|---|
| CI-GESTPAT | Couche Service - Volet Gestion de dossiers patient partagés | Gestion de Dossiers Patient Partagés |
| CI-PARTAGE | Couche Service - Volet Partage de Documents de Santé | Partage de Documents de Santé |
| CI-TR-CLI-LRD | Couche Transport - Volet Transport Synchrone pour Client Lourd | Transport synchrone client lourd pour les services en santé |
| CI-STRU-ENTETE | Couche Contenu - Volet Structuration Minimale de Documents de santé | Structuration minimale de Documents de santé |
| CI-ANX-CDA | Annexe : Liens entre entête CDA et métadonnées | Lien entre l'en-tête CDA et les métadonnées XDS |
| CI-ANX-PS-STRU | Annexe Transverse : Sources des données métier pour les professionnels et les structures | Sources des données personnes et structures |

| | | |
|---|---|---|
| CI-VAC | Volet Vaccination (VAC_2023.01) | VAC - Vaccination |
| IMG-KOS | Volet Partage d'Examen d'Imagerie de santé | Références aux objets d'un examen d'imagerie |
| TEST-CONTENU-CDA | Outils de test (XSD, schématrons…) | Outil de vérification des documents CDA |

**Tableau 36 : documents de référence du CI-SIS**

Les documents de référence IHE/HL7 sont présentés dans le tableau ci-dessous.

| Appellation | Type et titre | Référence |
|---|---|---|
| IHE-TF1 | Profils d'intégration IHE<br>IHE IT Infrastructure Technical Framework, Volume 1 (ITI TF-1) | https://www.ihe.net/Technical_Frameworks<br>(section IT Infrastructure) |
| IHE-TF2A | Transactions – Partie I<br>IHE IT Infrastructure Technical Framework, Volume 2a (ITI TF-2a) | |
| IHE-TF2B | Transactions IHE – Partie II<br>IHE IT Infrastructure Technical Framework, Volume 2b (ITI TF-2b) | |
| IHE-PDQV3 | | |
| IHE-TF3 | Définition IHE des métadonnées XDS<br>IHE IT Infrastructure Technical Framework, Volume 3 (ITI TF-3) | |
| IHE-DSG | | |
| IHE-MU | Mise à jour de métadonnées XDS (XDS Metadata Update) | |

**Tableau 37 : documents de référence concernant IHE et HL7**

Autres documents de référence :

| Appellation | Type et titre | Référence |
|---|---|---|
| CHARTE-GRAPHIQUE_DMP-LPS | Charte graphique à destination des éditeurs de logiciels DMP-compatibles | Charte graphique à destination des éditeurs de logiciels DMP-Compatibles.zip disponible dans l'Espace Industriels |
| CHARTE-DOC-PATIENT | Principe d'élaboration du Document des secrets DMP | DMP_LPS_Principe_elaboration_du_document_des_secrets_DMP_v2.0.zip disponible dans l'Espace Industriels |
| FI-URL | Fiche d'information sur les URL paramètrables. | PDT-INF-547 disponible dans l'Espace Industriels |
| FI-JEUX-VALEURS | Fiche d'information sur les jeux de valeur | PDT-INF-554 disponible dans l'Espace Industriels |
| DMP1-OS-NAVIGATEURS | Liste des configurations compatibles avec le DMP | Cf. [FI-URL] |
| RHCVIT | Référentiel Lecture Vitale | Diffusion restreinte aux industriels ayant un contrat d'homologation avec le GIE SESAM-Vitale |

| | | |
|---|---|---|
| TRANS-ADELI-RPPS | Tables de transcodages des savoir-faire et secteurs d'activités ADELI vers RPPS | ASIP-SANTE_X01_<date>.tab : transcodages savoir-faire<br>ASIP-SANTE_X02_<date>.tab : transcodages secteur d'activité<br>(Fichiers inclus dans Transco_ADELI_RPPS_<date>.zip mis à disposition dans les annexes transaverses du CI-SIS) |
| [PDV-HOMOLOGATION] | Document fourni par le CNDA lors de la procédure d'homologation. | |
| PROCEDURE_CERTIF | Commande de certificats pour le DMP Procédure pour les structures non libérales (salariées) | https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS_Procedure_commande_CL_DMP_structures_non_lib%C3%A9rales_v30092021.pdf |

**Tableau 38 : autres documents de référence**

Les documents de référence suivants concernent la lecture des données accessibles à partir d'une application carte Vitale.

| Appellation | Type et titre | Référence |
|---|---|---|
| ApCV-SFG-004 | SFG - Appli carte Vitale - Authentifier et gérer le contexte ApCV | ApCV-SFG-004 |
| ApCV-MP-001 | GI - Authentifier et gérer le contexte ApCV | ApCV-MP-001 |

**Tableau 39 : documents de référence concernant la lecture des données accessibles à partir d'une application carte Vitale**

Les documents suivants illustrent le fonctionnement du système DMP et du site web PS. Ces documents sont fournis à titre indicatif en dehors du périmètre de la DMP-compatibilité.

| Appellation | Type et titre | Référence |
|---|---|---|
| DMP-MHAB | Matrice d'habilitations des professionnels | Cf. [FI-URL] |
| DMP-MDRF | Matrice des droits fonctionnels | PDT-INF-526 |
| | Matrice des droits fonctionnels mode AIR | PDT-INF-606 |
| DMP-ACCES-WEB | Accès au système DMP - Sites Web PS et Web Patient | PDT-INF-527 |

**Tableau 40 : documents illustrant le fonctionnement du système DMP et des sites web**

Les documents de référence suivants concernent l'identité INS des patients (matricule INS et les traits d'identité).

| Appellation | Type et titre | Référence |
|---|---|---|
| REF-INS | Référentiel INS et les documents associés : Guide d'implémentation de l'identité INS dans les logiciels, Référentiel National d'IdentitoVigilance, Foire aux questions, … | Cf. site de l'ANS |
| OID-INS | Liste des OID des autorités d'affectation des INS | INS: publication des OID des autorités d'affectation → Liste des OID des autorités d'affectation des INS |

**Tableau 41 : documents de référence concernant l'identification des patients et l'INS**

# ANNEXE 5 DECLINAISON DES PROCESSUS PAR PROFIL DE DMP-COMPATIBILITE

Le code couleur utilisé dans les schémas est rappelé dans le tableau ci-dessous.

| | Groupes de fonctionnalités | Description détaillée |
|---|---|---|
| *DMP_x* | **Fonctionnalités d'acquisition des données de contexte** | **3.1** |
| *DMP_0.x* | **Accès sécurisé au DMP d'un patient (via TD0.x)** | **3.2** |
| *DMP_1.x* | **Données administrative du DMP d'un patient (via TD1.x)** | **3.3** |
| *DMP_2.x* | **Alimentation du DMP d'un patient (via TD2.x)** | **3.4** |
| *DMP_3.x* | **Consultation du DMP d'un patient (via TD3.x)** | **3.5** |

**Tableau 42 : code couleur utilisé dans les schémas**

NB : la création et la réactivation d'un DMP sont prises en charge par « Mon espace santé ». Elles apparaissent sur fond blanc et ne sont plus référencées DMP_1.1 et DMP_1.2.

## A5-1 Processus « Alimenter le DMP d'un patient » (profil Alimentation)

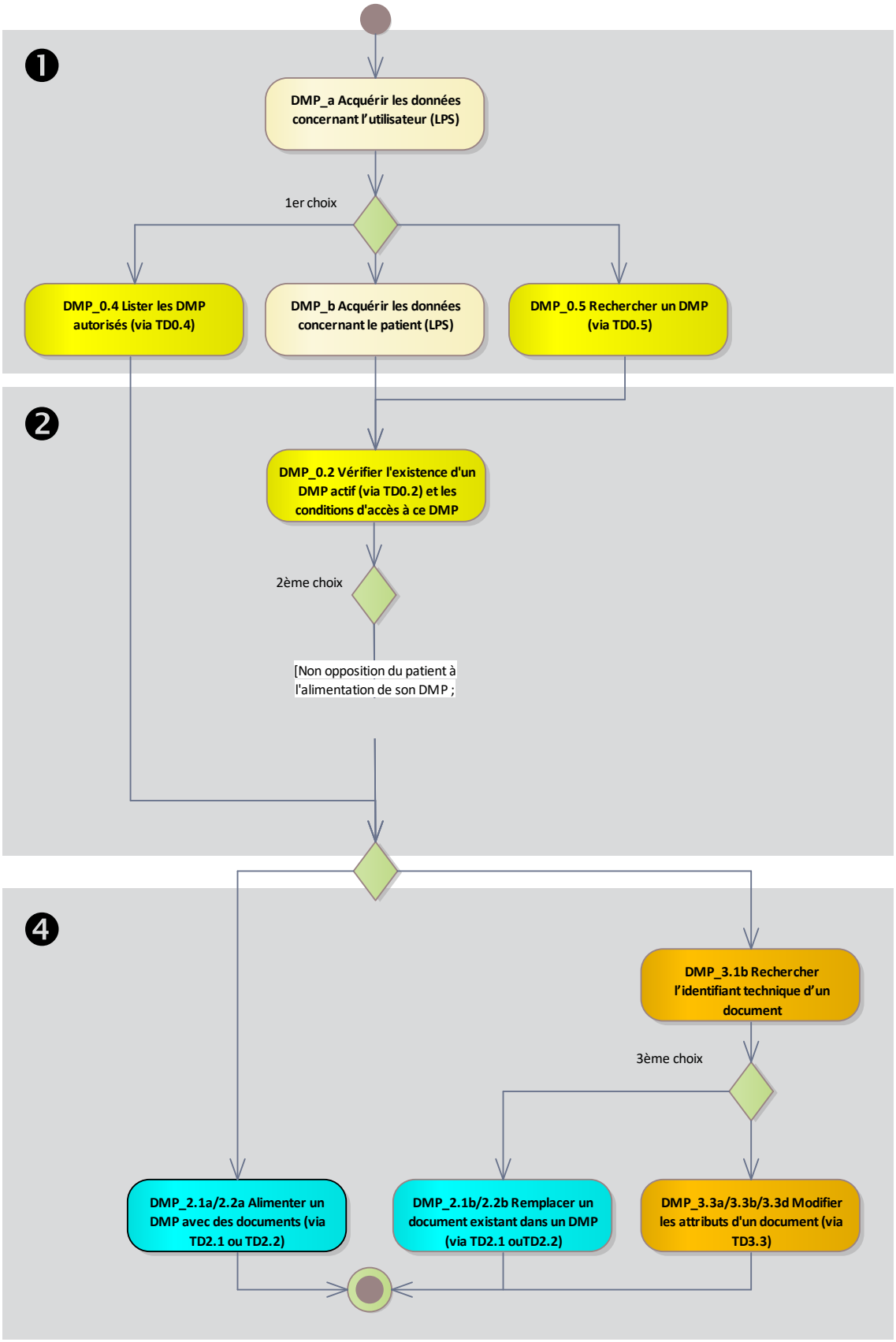



**Figure 48 : processus « Alimenter le DMP d'un patient »**

## A5-2 Processus « Consulter le DMP d'un patient » (profil Consultation)

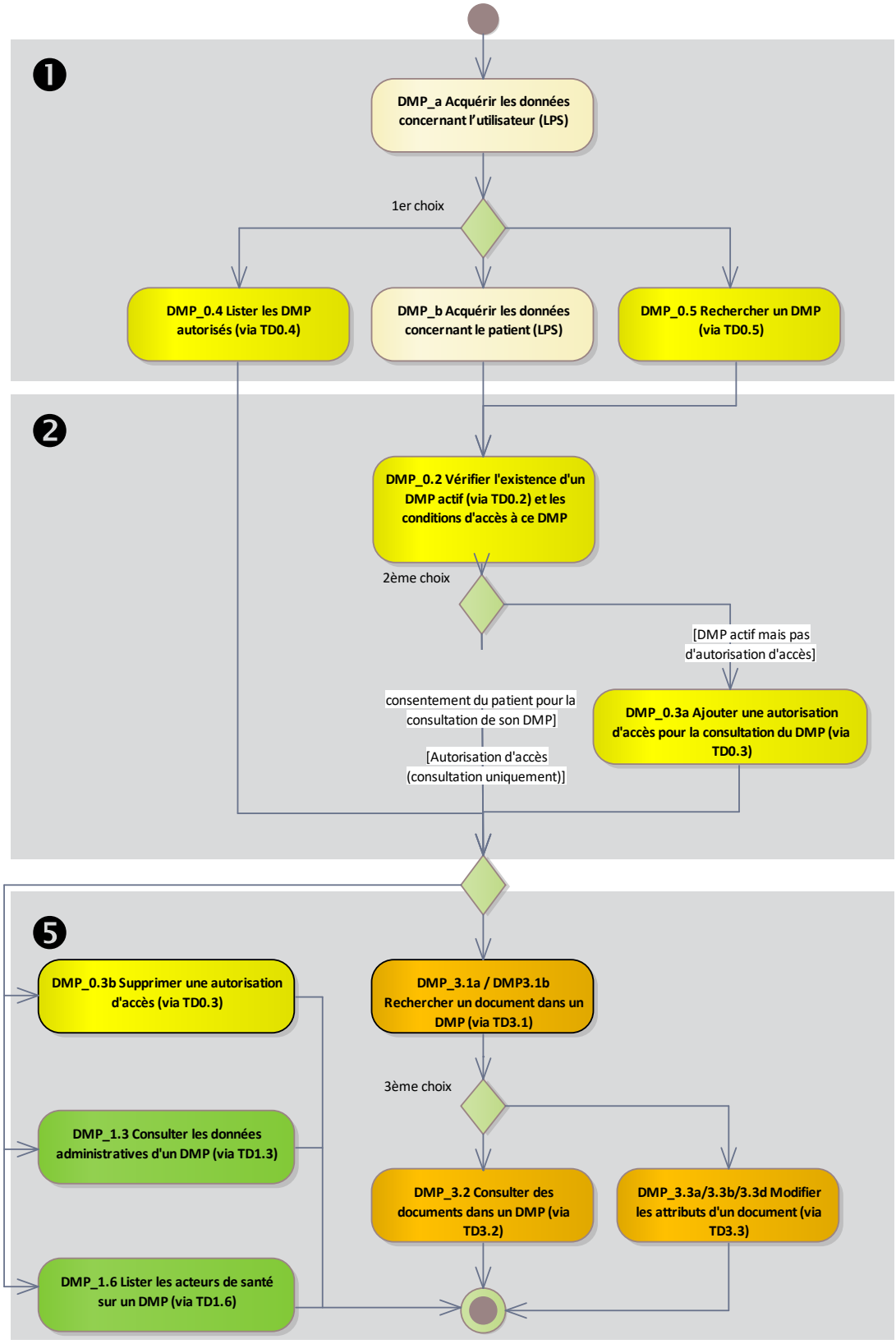



**Figure 49 : processus « Consulter le DMP d'un patient »**

# ANNEXE 6 AIDE A L'IMPLEMENTATION

## A6-1 Signature XAdES

Cette annexe définit les contraintes de signature XAdES à mettre en œuvre pour l'alimentation du DMP lors de la signature d'un lot de soumission (requise) et de la signature d'un document (optionnelle). La signature d'un lot de soumission utilise, en plus de ces contraintes, le profil IHE DSG, dont une aide à l'implémentation est fournie en annexe A6-2.

### A6-1.1 Principes généraux de XAdES

XML Advanced Electronic Signatures (XAdES) est une norme conçue par l'European Telecommunications Standards Institute (ETSI) pour permettre une mise en conformité des signatures électroniques avec la « Directive 1999/93/EC du Parlement Européen et du Conseil du 13 décembre 1999 sur le cadre communautaire des signatures électroniques ». Cette norme offre une boîte à outils permettant la mise en œuvre de signatures électroniques valables sur de longues durées.

XAdES est appliquée comme une surcouche à XML-DSIG.

La référence à utiliser dans le cadre du DMP est définie dans une note du W3C (voir [XADES-W3C]) expliquant les différents niveaux de signature XAdES (XAdES, XAdES-T, XAdES-C). Le premier niveau (XAdES) est requis, avec horodatage auto-généré de la signature (SigningTime). Les autres niveaux (XAdES-T, XAdES-C, etc.) ne sont pas supportés dans la version actuelle du SI DMP.

### A6-1.2 Rappel des principes de la signature électronique

Les principes de la signature électronique à maîtriser pour pouvoir s'engager dans la DMP-compatibilité sont :

- les grands concepts de cryptage et de condensat (fonction de hachage, http://fr.wikipedia.org/wiki/Fonction_de_hachage) et leur application dans le domaine des signatures électroniques,
- le concept d'indirection via condensat (voir la relation entre les balises `Reference` (http://www.w3.org/TR/xmldsig-core/#sec-Reference) et `SignatureValue` (http://www.w3.org/TR/xmldsig-core/#sec-SignatureValue)) et le concept de canonisation XML, qui sont des concepts fondamentaux de la norme XMLDSig (http://www.w3.org/TR/xmldsig-core/) utilisée pour le jeton VIHF et la signature des lots de soumission en alimentation de documents,
- la librairie métier utilisée pour la mise en œuvre du code DMP-compatible. L'éditeur doit pouvoir émettre des signatures électroniques, mais également les valider et effectuer une analyse initiale en cas d'anomalie de signature (généralement liée à un mésusage de la canonisation XML, des condensats ou de l'indirection via condensat). Il n'est pas forcément nécessaire d'utiliser la même librairie pour la génération et le contrôle (l'éditeur peut par exemple générer la signature en C et la contrôler en Java (http://java.sun.com/developer/technicalArticles/xml/dig_signatures/)).

## A6-1.3 Structure « XAdES W3C »

### A6-1.3.1 Structure XAdES de premier niveau applicable au DMP

Dans sa forme de premier niveau, XAdES ajoute à une signature XML-DSIG `<ds:Signature>`, l'ensemble des informations suivantes :

- un élément `//ds:Signature/ds:object/xades:QualifyingProperties` ;
  - (Voir annexe A6-1.3.2 ci-après)
- une référence `//ds:Signature/ds:SignedInfos/ds:Reference` portant sur le `<SignedProperties>` du `<xades:QualifyingProperties>` ci-dessus;
- une référence explicite et signée sur le certificat de signature (ou de cachet).
  Ceci peut être effectué de plusieurs façons parmi lesquelles :
  - ajout d'un nœud `<xades:SigningCertificate>` à l'ensemble de nœuds `//xades:SignedSignatureProperties` ;
  - ajout d'un nœud `//ds:Signature/ds:KeyInfo/ds:X509Data` portant le certificat utilisé pour la signature et ajout d'un nœud `//ds:Signature/ds:SignedInfos/ds:Reference` portant sur ce nœud `<ds:X509Data>`.

Note : le préfixe "`ds:`" indique que les éléments XML sont définis dans [XML-DSIG] et le préfixe "`xades:`" indique les éléments définis dans [XADES-W3C].

### A6-1.3.2 Description du <xades:QualifyingProperties>

```
<ds:Object>
      <xades:QualifyingProperties>

            <xades:SignedProperties>
                  <xades:SignedSignatureProperties>
                        <xades:SigningTime>
                              …
                        </xades:SigningTime>
                        <xades:SigningCertificate>
                              …
                        </xades:SigningCertificate>
                        <xades:SignaturePolicyIdentifier>
                        <xades:SignaturePolicyImplied/>
                        </xades:SignaturePolicyIdentifier>
                  </xades:SignedSignatureProperties>
                  <xades:SignedDataObjectProperties>
                  </xades:SignedDataObjectProperties>
            </xades:SignedProperties>

            <xades:UnsignedProperties>
                  <xades:UnsignedSignatureProperties>
                  </xades:UnsignedSignatureProperties>
            </xades:UnsignedProperties>

      </xades:QualifyingProperties>
</ds:Object>
```

- `SignedProperties` :
  - `SigningTime` (obligatoire) : date de signature (déclarative, renseignée par le LPS) prend pour valeur la date et l'heure à laquelle la signature XML-DSIG a été générée. Dans ce contexte, il est donc pertinent de prévoir une synchronisation NTP de l'horloge matérielle de la machine et / ou l'utilisation d'un serveur NTP par l'application gérant la signature. Au format `xsd:dateTime`, avec composant offset préconisé : soit en UTC (avec Z) ou en heure locale avec décalage horaire par rapport à GMT.
  - `SigningCertificate` (obligatoire) : référence des certificats
    Le noeud `<SigningCertificate>` contient une liste de plusieurs éléments `<Cert>` dont :
    - le premier `<Cert>` (requis) pointe obligatoirement le certificat utilisé pour la signature XML-DSIG ;
    - Les autres `<Cert>` pointent les certificats qui composent la chaîne de certification et ce jusqu'à la racine, mais ils sont facultatifs.
    - Le nœud `<Cert>` contient deux nœuds fils :
      - le premier, `<CertDigest>`, contient le condensat encodé au format base 64 du certificat dans sa forme binaire DER ainsi que la méthode utilisée pour générer ce condensat ;
      - le second nœud `<IssuerSerial>` est de type `ds:X509IssuerSerialType` et contient l'identifiant de l'émetteur du certificat et le numéro de série du certificat.

Les Autorités de Certification (AC) composant la chaîne de certification à intégrer peuvent être récupérées :

- Manuellement, pour l'IGC Santé, sur http://igc-sante.esante.gouv.fr/PC/
- Dynamiquement, à partir d'une version récente de la CryptoLib :
  - dans le dossier « coffre » de la CryptoLib[22] ;
  - dans le magasin de certificat de l'OS (après installation de la CryptoLib).

Pour le DMP, les AC utiles pour la signature XAdES sont :

1. pour l'authentification directe (carte CPx), pour l'IGC Santé
   - pour les CPS, CPF
     - **AC Racine** : gamme Fort (fichier ACR-FO.cer)
     - **AC Intermédiaire** : domaine Personnes Physiques (fichier ACI-PP-FO.cer)
   - pour les CDE, CPE
     - **AC Racine**: gamme Standard (fichier ACR-ST.cer)
     - **AC Intermédiaire** : domaine Personnes Physiques (fichier ACI-ST-PP.cer)
2. pour l'authentification indirecte, pour une structure utilisant des certificats **IGC Santé** (certificat d'organisation) :
   - **AC Racine** : gamme élémentaire (fichier ACR-EL.cer)
   - **AC Intermédiaire** : domaine organisation (fichier ACI-EL-ORG.cer)

[22] L'éditeur est invité à consulter les documentations d'installation de la CryptoLib disponibles sur https://industriels.esante.gouv.fr/ pour connaître l'emplacement du dossier « coffre », en fonction du ou des OS supporté(s).

Pour information, les autres fichiers installés dans le dossier "coffre" de la CryptoLib ne sont pas, pour le moment, utiles dans le processus d'alimentation du DMP.

- `SignaturePolicyIdentifier` (obligatoire) : référence à une politique de signature. Pour le DMP, ce champ sera laissé « implicite » avec l'ajout d'un élément fils `<SignaturePolicyImplied/>`.
- `SignedDataObjectProperties` (obligatoire) : nœud vide.

- `UnsignedProperties` :
  - `UnsignedSignatureProperties` (obligatoire) : nœud vide.

Exemple :

```
<QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.1.1#" Target="#OID_sign">

  <SignedProperties Id="S0-SignedProperties" xmlns="http://uri.etsi.org/01903/v1.1.1#">

    <SignedSignatureProperties>

      <SigningTime>2010-11-14T14:14:39.281+01:00</SigningTime> // date/heure de signature

      <SigningCertificate>
// Références et empreintes du certificat de signature et de ses certificats parents jusqu'à
la racine
        <Cert xmlns="http://uri.etsi.org/01903/v1.1.1#">
          <CertDigest>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>asifcL78Fhkv1TLUczwwxnTi6RY=</DigestValue>
          </CertDigest>
          <IssuerSerial>
            <X509IssuerName   xmlns="http://www.w3.org/2000/09/xmldsig#">CN=TEST   CLASSE-
1,OU=TEST PROFESSIONNEL,O=TEST,C=FR</X509IssuerName>
            <X509SerialNumber
xmlns="http://www.w3.org/2000/09/xmldsig#">1509588</X509SerialNumber>
          </IssuerSerial>
        </Cert>
        <Cert xmlns="http://uri.etsi.org/01903/v1.1.1#">
          <CertDigest>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue> JDjPyPJ1bLsmhQJz96DkfFeyIz4=</DigestValue>
          </CertDigest>
          <IssuerSerial>
            <X509IssuerName             xmlns="http://www.w3.org/2000/09/xmldsig#">OU=TEST
PROFESSIONNEL,O=TEST,C=FR</X509IssuerName>
            <X509SerialNumber                  xmlns="http://www.w3.org/2000/09/xmldsig#">
4370</X509SerialNumber>
          </IssuerSerial>
        </Cert>
        <Cert xmlns="http://uri.etsi.org/01903/v1.1.1#">
          <CertDigest>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue> cemsA/zjMXcHx/XV1CnqIJ7KIwU=</DigestValue>
          </CertDigest>
          <IssuerSerial>
            <X509IssuerName             xmlns="http://www.w3.org/2000/09/xmldsig#">OU=TEST
PROFESSIONNEL,O=TEST,C=FR</X509IssuerName>
            <X509SerialNumber                  xmlns="http://www.w3.org/2000/09/xmldsig#">
4353</X509SerialNumber>
          </IssuerSerial>
        </Cert>
      </SigningCertificate>

      <SignaturePolicyIdentifier>
        <SignaturePolicyImplied/>
// politique de signature positionnée à « implicite » en attente de la définition
d'une politique de signature
      </SignaturePolicyIdentifier>

    </SignedSignatureProperties>

    <SignedDataObjectProperties></SignedDataObjectProperties>

  </SignedProperties>

  <UnsignedProperties>
      <UnsignedSignatureProperties></UnsignedSignatureProperties>
  </UnsignedProperties>


</QualifyingProperties>
```

### A6-1.4 Erreurs fréquentes lors de la mise en œuvre

Une anomalie de signature peut être notamment due aux facteurs suivants :

- corruption des données référencées (balise `Reference`),
- mauvaise canonisation des données référencées dans une balise `Reference` le cas échéant,
- mauvais calcul du condensat sur une donnée référencée,
- mauvaise conversion du condensat binaire en base 64 dans une balise `Reference`,
- erreur dans la référence à une donnée « référencée » (la librairie effectue les calculs de la pièce jointe A mais les range sous l'intitulé B),
- mauvaise canonisation de la balise `Reference`,
- mauvais calcul du condensat sur la balise `Reference`,
- mauvaise signature RSA sur le condensat de la balise `Reference`,
- mauvaise conversion de la signature RSA binaire en base 64 dans la balise `SignatureValue`.

La liste ci-dessous recense les erreurs les plus fréquemment rencontrées lors de la mise en œuvre dans le LPS :

- En cas d'erreur **DMPInvalidSignature** il peut être utile de vérifier :
  - que la signature du lot de soumission n'est pas intervertie avec la pièce jointe CDA R2 dans le corps du message MTOM,
  - qu'il n'y a pas de problème de canonisation des éléments signés,
  - que les hash sont correctement calculés.
- Différentes erreurs **DMPInvalidSignature** sont possibles :
  - `DMPInvalidSignature : « Le controle de la signature du lot a échoué: Invalid signature : invalid reference hashes on : [#S0-SignedProperties] »` :
    - il peut s'agir d'un problème de canonisation sur certains sous-éléments de l'élément `SignedProperties` : les éléments `SignedProperties` et ses éléments fils (sauf `X509IssuerName` et `X509SerialNumber`) ne respectent pas les bons namespaces par rapport au schéma XAdES :
      - `SignedProperties` et ses éléments fils doivent être dans le namespace XAdES (http://uri.etsi.org/01903/v1.1.1#),
      - sauf `X509IssuerName` et `X509SerialNumber` qui sont des éléments standards XmlDSig, et qui par conséquent doivent être dans le namespace XmlDSig (http://www.w3.org/2000/09/xmldsig#),
    - la Signature XAdES présente dans les messages d'exemples TD2.1/TD2.2 reflète cela.
  - `DMPInvalidSignature : « Le controle de la signature du lot a échoué : Invalid signature : invalid SignedInfos »` :
    - en général, il faut débuguer le code : les hash des éléments `Reference` de `SignedInfo` sont faux (mal calculés), éventuellement suite à une mauvaise canonisation,

- DMPInvalidSignature : « Le contrôle de la signature du lot a échoué : Le contrôle de cohérence des condensats de la signature de la pièce jointe a échoué pour : urn:oid:1.2.250.1.59.905.20111001.1.2011101012.17090717^CR17090717 » :
  - le message renvoyé signifie que le condensat (hash) calculé pour le document de uniqueId = urn:oid:1.2.250.1.59.905.20111001.1.2011101012.17090717^CR17090717 n'est pas correct. Le DMP recalcule le condensat du fichier CDA et le compare avec la valeur fournie dans la signature XAdES (c'est ce condensat qui est ensuite signé par le certificat). Il est nécessaire de respecter le profil IHE DSG de signature de lot de soumission. Voir également la note en annexe A6-2.2.2 concernant la construction des OID et leur compatibilité avec IHE DSG.

## A6-2 Aide à l'implémentation du profil IHE DSG pour le DMP

Cette annexe constitue une aide à l'implémentation du profil IHE DSG (voir [IHE-DSG]) **pour la signature des lots de soumission envoyés au DMP via les transactions TD2.1/TD2.2** d'alimentation en documents.

Cette aide se veut didactique comme un tutoriel « pas à pas ». L'organisation de cette annexe (chronologie des paragraphes) suit la logique de construction d'une requête XDS.b et l'ordre de programmation des opérations à réaliser par l'éditeur pour la signature XAdES (voir [XADES-W3C]) du lot de soumission.

Cette annexe ne constitue pas une spécification et ne saurait remplacer la lecture du CI-SIS, des profils IHE XDS.b et DSG (pas de description des métadonnées XDS par exemple, ni d'un CDA) et s'attache à décrire les références entre les identifiants des parties de la requête XDS.b pour la construction d'une signature de lot de soumission.

Cette aide présente :

- des exemples commentés de XML de signature DSG de lot de soumission et de requête d'alimentation XDS.b (hors signature de document) au format MTOM ;
- une vulgarisation en français et résumée de la partie utile aux spécifications DMP du profil IHE DSG (voir [IHE-DSG]), pour sa partie signature d'un lot.

Cette aide ne traite pas de la signature des documents.

### A6-2.1 Structure d'une soumission XDS.b

La soumission de documents au DMP est effectuée par la transaction IHE ITI-41 ProvideAndRegisterDocumentSet-b (profil XDS.b) associée obligatoirement à la signature de lot de soumission IHE DSG (ref. [IHE-DSG]).

**Représentation schématique d'une soumission XDS.b**

La requête envoyée au serveur est constituée des éléments suivants, dans un paquet mime-multipart respectant MTOM/XOP :

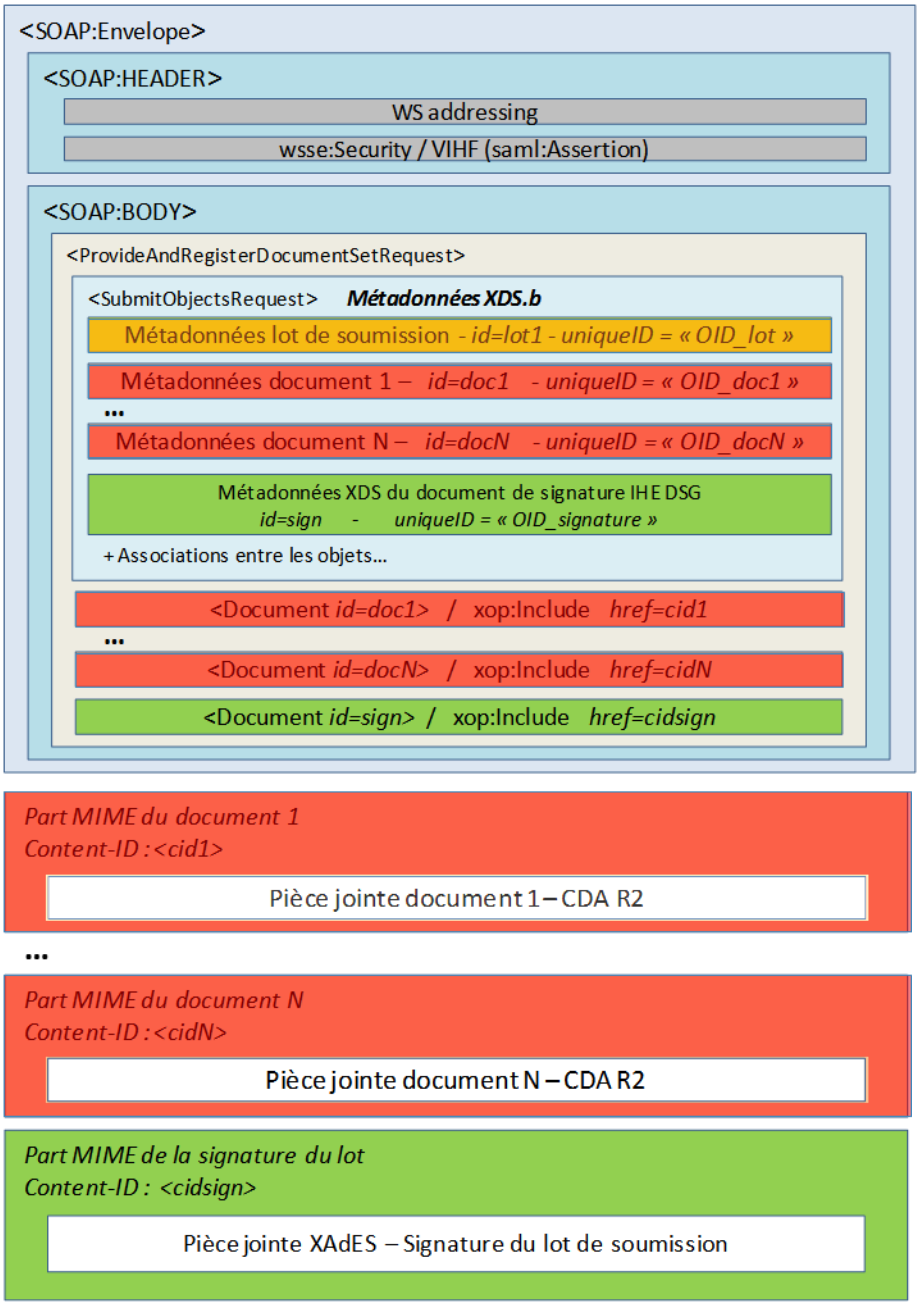



**Figure 50 : contenu d'une requête de soumission XDS.b**

Les codes couleur « orange », « rouge » et « vert » du schéma ci-dessous sont repris dans la suite du texte pour distinguer les trois de métadonnées comme indiqué ci-dessous.

**Relation entre les métadonnées XDS.b et le reste de la requête**

Les métadonnées XDS.b regroupent :

- Les métadonnées du lot de soumission (RegistryPackage ebXML)
  - Identifié au sein de la requête par un identifiant interne à la requête noté « lot1 » dans les exemples de ce document
  - Identifié par un uniqueId au format OID, noté « OID_lot » dans la suite du document
  - Cet OID_lot doit se retrouver en référence dans le Manifest IHE de la signature XAdES.

- Les métadonnées des documents du lot (1 à N) (ExtrincicObject ebXML)
  - Identifiés chacun au sein de la requête par un identifiant interne à la requête noté « doc1 » à « docN » dans les exemples de ce document
  - Identifiés chacun par un uniqueId au format OID noté « OID_doc1 » à « OID_docN » dans la suite du document
  - Ces OID_docN doivent se retrouver en référence dans le Manifest IHE de la signature XAdES.
- Les métadonnées d'un document de signature DSG (ExtrincicObject ebXML) ; le contenu de ces métadonnées est défini dans [CI-PARTAGE] « Imputabilité du dépôt des documents » :
  - Identifié par un uniqueId au format OID noté « OID_sign » dans la suite du document
  - Cet OID_sign doit se retrouver dans l'élément Signature/@Id de pièce jointe signature XAdES.

*Les codes couleurs utilisés ci-dessus pour représenter les divers identifiants sont repris dans les exemples dans la suite de cette aide.*

**Chronologie possible pour la construction de la requête XDS.b :**

1. Construire ou ajouter le(s) document(s) CDA (les documents CDA peuvent être préexistants) et calculer les hashs des documents.
2. Créer les métadonnées XDS du lot de soumission et son identifiant unique.
3. Créer les métadonnées XDS des documents et les identifiants uniques référençant les parties MTOM dans lesquelles sont écrits les CDA.
4. Créer les métadonnées XDS du document de signature et son identifiant unique.
5. Créer les associations entre le lot de soumission et les documents.
6. Créer la pièce jointe XAdES de signature du lot de soumission (voir détail au paragraphe suivant). Elle reprend dans son Manifest les différents identifiants uniques précédents (celui du lot de soumission et ceux des documents) et les hash de chaque document. La pièce jointe XAdES de signature du lot de soumission est donc nécessairement créée en dernier.

## A6-2.2 Construction de la pièce jointe XAdES de signature du lot de soumission

Une chronologie possible de construction de la pièce jointe XAdES de signature du lot de soumission est la suivante :

1) **Construction du `Manifest`** inclus dans `ds:Object` et qui sera signé.
2) **Construction du `QualifiyingProperties`** inclus dans `ds:Object`, dont l'élément `SignedProperties` sera signé.
3) **Construction du `SignedInfo`** à partir des `Références` et de leurs Hashs calculés suivant l'algorithme indiqué.
4) **Canonisation et signature du `SignedInfo`** (apposée dans `SignatureValue`)

*En pratique, il est recommandé de se baser sur une bibliothèque existante gérant a minima XML-DSIG pour effectuer la construction de la signature XAdES (ex. : API XMLSignature de Java), celle-ci gérant les problématiques de transformation, canonisation, calcul des digest et de la signature finale.*

### A6-2.2.1 Structure de base

La structure de base de la **pièce jointe XAdES d'un lot de soumission** est représentée ci-après :

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="OID_sign">

<SignedInfo>
[informations signées]
</SignedInfo>

<SignatureValue> [valeur de la signature] </SignatureValue>

<KeyInfo>
  <X509Data>
    <X509Certificate> [certificat X509 signataire] </X509Certificate>
  </X509Data>
</KeyInfo>

<Object>
  <SignatureProperties>
    // purposeOfSignature imposée par DSG ; le contenu dans SignatureProperty est
fixe
    <SignatureProperty Id="purposeOfSignature" Target="#OID_sign">
1.2.840.10065.1.12.1.14
    </SignatureProperty>
  </SignatureProperties>
</Object>

<Object>
  <Manifest Id="IHEManifest">
     [Manifest IHE DSG : références du lot à signer]
  </Manifest>
</Object>

<Object>
// propriété spécifiques XAdES
  <QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.1.1#"
Target="#OID_sign">
    <SignedProperties Id="S0-SignedProperties"
xmlns="http://uri.etsi.org/01903/v1.1.1#">
      [propriété XAdES à signer]
    </SignedProperties>
    <UnsignedProperties>
      <UnsignedSignatureProperties></UnsignedSignatureProperties>
    </UnsignedProperties>
  </QualifyingProperties>
</Object>

</Signature>
```

Il est possible de mettre `SignatureProperties`, `Manifest` et `QualifyingProperties` dans le même nœud `Object`, ou dans des nœuds `Object` différents (les deux constructions sont tolérées).
Un élément `SignatureProperties` est imposé par IHE DSG et doit faire référence à l'OID du document de signature. La valeur `1.2.840.10065.1.12.1.14` est positionnée par le CI-SIS (but de la signature : signature par la « Source » des données).

L'élément `KeyInfo/X509Data/X509Certificate` doit contenir le certificat X509 utilisé pour la signature.

*L'ordre des chapitres suivants suit l'ordre logique de programmation dans lequel les différents éléments doivent être construits.*

### A6-2.2.2 Construction du *Manifest*

Un Manifest XML doit être construit afin de référencer le lot de soumission et l'ensemble des documents le composant.

**Ajout de la référence au lot de soumission :**

Ajouter la référence au lot de soumission (son OID précédé de « urn:oid: ») dans un élément `Reference/@URI`, ainsi que son « hash null » (0 en base64).

```
<Manifest Id="IHEManifest">
      <Reference URI="urn:oid:OID_lot">
          <DigestMethod

   Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <DigestValue>AA==</DigestValue>
   </Reference>
</Manifest>
```

**Ajout de la référence à chaque document :**

Pour chaque document du lot[23] :

- Si le document est XML (CDA R2, en pratique toujours le cas dans le DMP), appliquer l'algorithme de transformation « `http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComment` » (canonisation) ;
- Calculer le hash sha1 de la pièce jointe ainsi transformée ;
- Insérer une référence dans le `Manifest`, avec le uniqueId du document (précédé de « `urn:oid:` ») dans un élément `Reference/@URI` et le hash dans `DigestValue`.

  **Note** : Le format d'un `uniqueId` de document peut être OID^Extension en XDS. Or, la version actuelle du DMP ne supporte pas le format OID^Extension pour cette référence dans le manifest. Il est donc demandé de n'utiliser pour les `uniqueId` de document que le format OID sans extension (ex. : «`urn:oid:1.2.850.2345.3245.13.58132`»).

```
<Manifest Id="IHEManifest">
    <Reference URI="urn:oid:OID_lot">
           <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
           <DigestValue>AA==</DigestValue>
    </Reference>
    <Reference URI="urn:oid:OID_docN">
           <Transforms>
                  <Transform   Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
                  // transformation à appliquer à la pièce jointe CDA R2 avant
hachage
           </Transforms>
           <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
           <DigestValue>  [digest  (hash)  de  la  pièce  jointe  du  document  N]
</DigestValue>
    </Reference>
</Manifest>
```

[23] Dans le cadre de la signature des lots un document est considéré comme faisant partie d'un lot s'il est lié à ce lot par une association de type « HasMember » dont la valeur de l'attribut « SubmissionSetStatus » est « Original » (les documents qui seraient soumis par référence (Association « HasMember » dont la valeur de l'attribut « SubmissionSetStatus » est « Reference ») ne font pas partie de la signature d'un lot).

### A6-2.2.3 Construction du *QualifiyingProperties*

Voir Annexe A6-1.3.2.

### A6-2.2.4 Construction du *SignedInfo*

L'élément `SignedInfos` doit contenir les éléments à faire signer par le certificat.

**Structure de base :**

```
<SignedInfo>
       <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
       <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
</SignedInfo>
```

**Ajouter les `Reference` :**

- au nœud `Manifest`, incluant le digest sha-1 de celui-ci
- au nœud `SignedProperties`, incluant le digest sha-1 de celui-ci

```
<SignedInfo>
       <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
       <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

    <Reference Type="http://www.w3.org/2000/09/xmldsig#Manifest"
URI="#IHEManifest">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue> [digest du manifest] </DigestValue>
    </Reference>

    <Reference Type="http://uri.etsi.org/01903/v1.1.1#SignedProperties" URI="#S0-
SignedProperties">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue> [digest des SignedProperties] </DigestValue>
    </Reference>


</SignedInfo>
```

### A6-2.2.5 Canonisation et signature du *SignedInfo*

La signature finale doit être apposée dans l'élément `<SignatureValue>`

- Canonization du SignedInfo suivant l'algorithme http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
- Signature rsa-sha1 du résultat de la canonization par le certificat de signature (ou de cachet)
- Injection du résultat dans `SignatureValue`.

## A6-2.3 Requête d'alimentation XDS.b commentée

Pour plus de lisibilité, les identifiants utilisés dans la requête commentée ci-après sont volontairement non signifiants. L'éditeur doit respecter le format approprié, OID ou identifiant interne à la requête.

```
------=_Part_0_18075465.1289232799781 // Part MIME du message SOAP
Content-Type:  application/xop+xml;  charset=UTF-8;  type="application/soap+xml";
action="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b";
Content-Transfer-Encoding: binary
Content-ID: <root.message@xyz>

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">

  <soap:Header>
    [WS-adressing]
    [wsse:Security / VIHF]
  </soap:Header>
  <soap:Body>
    <ProvideAndRegisterDocumentSetRequest...>

      <lcm:SubmitObjectsRequest>
        <rim:RegistryObjectList>
          <rim:RegistryPackage id="lot1">
            [métadonnées du lot de soumission]
            [uniqueId = OID_lot]
          </rim:RegistryPackage>
          <rim:ExtrinsicObject id="doc1" ...>
            [métadonnées du document 1]
            [uniqueId = OID_doc1]
          </rim:ExtrinsicObject>
          <rim:ExtrinsicObject id="docN" ...>
            [métadonnées du document N]
            [uniqueId = OID_docN]
          </rim:ExtrinsicObject>
          <rim:ExtrinsicObject id="sign1" ...>
            [métadonnées du document de signature]
            [uniqueId = OID_sign1]
          </rim:ExtrinsicObject>
          <rim:Association ... sourceObject="lot1" targetObject="doc1">
             [association (de type "HasMember") du doc1 dans le lot]
          </rim:Association>
          <rim:Association ... sourceObject="lot1" targetObject="docN">
             [association (de type "HasMember") du docN dans le lot]
          </rim:Association>
          <rim:Association ... sourceObject="lot1" targetObject="sign1">
             [association (de type "HasMember") du document de signature sign1 dans
le lot]
          </rim:Association>
          <rim:Association ... sourceObject="sign1" targetObject="lot1">
             [association (de type "signs") du document de signature sign1 dans le
lot]
          </rim:Association>
        </rim:RegistryObjectList>
      </lcm:SubmitObjectsRequest>

      <Document id="sign1">
        <xop:Include              xmlns:xop="http://www.w3.org/2004/08/xop/include"
href="cid:cidsign"/>
      </Document>
      <Document id="doc1">
        <xop:Include              xmlns:xop="http://www.w3.org/2004/08/xop/include"
href="cid:cid1"/>
      </Document>
      <Document id="docN">
        <xop:Include              xmlns:xop="http://www.w3.org/2004/08/xop/include"
href="cid:cidN"/>
      </Document>

    </ProvideAndRegisterDocumentSetRequest>
  </soap:Body>
</soap:Envelope>
```

```
------=_Part_0_18075465.1289232799781 // Part MIME de la pièce jointe XAdES de
signature du lot
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
Content-ID: <cidsign>
<?xml version="1.0" encoding="UTF-8"?>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="OID_sign">

  <SignedInfo>
    <CanonicalizationMethod
      Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference                    Type="http://www.w3.org/2000/09/xmldsig#Manifest"
URI="#IHEManifest">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue> [digest du manifest] </DigestValue>
    </Reference>
    <Reference  Type="http://uri.etsi.org/01903/v1.1.1#SignedProperties"  URI="#S0-
SignedProperties">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue> [digest des SignedProperties] </DigestValue>
    </Reference>
  </SignedInfo>

  <SignatureValue>NXejuzBMd1ZPm...</SignatureValue> // valeur de la signature

  <KeyInfo>
    <X509Data>
      <X509Certificate>MIIFVzCCBD+gAwIBA...</X509Certificate>  // certificat X509
signataire
    </X509Data>
  </KeyInfo>

  <Object>
    <SignatureProperties>
      // purposeOfSignature imposée par DSG ; le contenu dans SignatureProperty est
fixe
    <SignatureProperty Id="purposeOfSignature"
     Target="#OID_sign">1.2.840.10065.1.12.1.14</SignatureProperty>
    </SignatureProperties>
  </Object>

  <Object>
    <Manifest Id="IHEManifest"> // Manifest IHE DSG : références du lot à signer
      <Reference URI="urn:oid:OID_lot">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>AA==</DigestValue> //« Hash du lot », doit être égal à 0 en
base64
      </Reference>
      <Reference URI="urn:oid:OID_doc1">
        <Transforms>
          <Transform            Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/> // transformation à appliquer à la pièce jointe CDA R2
avant hachage
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue> [digest (hash) de la pièce jointe du document 1] </DigestValue>
      </Reference>
      [...]
      <Reference URI="urn:oid:OID_docN">
        <Transforms>
          <Transform            Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/> // transformation à appliquer à la pièce jointe CDA R2
avant hachage
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue> [digest (hash) de la pièce jointe du document N] </DigestValue>
      </Reference>
    </Manifest>
  </Object>
```

```
  <Object>
    <QualifyingProperties                xmlns="http://uri.etsi.org/01903/v1.1.1#"
Target="#OID_sign">

      <SignedProperties                                    Id="S0-SignedProperties"
xmlns="http://uri.etsi.org/01903/v1.1.1#">

        <SignedSignatureProperties>

          <SigningTime>2010-11-14T14:14:39.281+01:00</SigningTime> // date/heure de
signature

          <SigningCertificate>
          // Références et empreintes du certificat de signature et de ses
certificats parents
             jusqu'à la racine
            <Cert xmlns="http://uri.etsi.org/01903/v1.1.1#">
              <CertDigest>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                </DigestMethod>
                <DigestValue>asifcL78Fhkv1TLUczwwxnTi6RY=</DigestValue>
              </CertDigest>
              <IssuerSerial>
                <X509IssuerName xmlns="http://www.w3.org/2000/09/xmldsig#">
                  CN=TEST                                          CLASSE-1,OU=TEST
PROFESSIONNEL,O=TEST,C=FR</X509IssuerName>
                <X509SerialNumber xmlns="http://www.w3.org/2000/09/xmldsig#">
                  1509588</X509SerialNumber>
              </IssuerSerial>
            </Cert>
            <Cert xmlns="http://uri.etsi.org/01903/v1.1.1#">
              <CertDigest>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                </DigestMethod>
                <DigestValue> JDjPyPJ1bLsmhQJz96DkfFeyIz4=</DigestValue>
              </CertDigest>
              <IssuerSerial>
                <X509IssuerName xmlns="http://www.w3.org/2000/09/xmldsig#">
                    OU=TEST PROFESSIONNEL,O=TEST,C=FR</X509IssuerName>
                <X509SerialNumber xmlns="http://www.w3.org/2000/09/xmldsig#">
                    4370</X509SerialNumber>
              </IssuerSerial>
            </Cert>
            <Cert xmlns="http://uri.etsi.org/01903/v1.1.1#">
              <CertDigest>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
                </DigestMethod>
                <DigestValue> cemsA/zjMXcHx/XV1CnqIJ7KIwU=</DigestValue>
              </CertDigest>
              <IssuerSerial>
                <X509IssuerName xmlns="http://www.w3.org/2000/09/xmldsig#">
                  OU=TEST PROFESSIONNEL,O=TEST,C=FR</X509IssuerName>
                <X509SerialNumber xmlns="http://www.w3.org/2000/09/xmldsig#">
                  4353</X509SerialNumber>
              </IssuerSerial>
            </Cert>
          </SigningCertificate>

          <SignaturePolicyIdentifier>
            <SignaturePolicyImplied/>
             // politique de signature positionnée à « implicite » en attente de la
définition d'une politique de signature
          </SignaturePolicyIdentifier>

        </SignedSignatureProperties>

        <SignedDataObjectProperties></SignedDataObjectProperties>

      </SignedProperties>

      <UnsignedProperties>
        <UnsignedSignatureProperties></UnsignedSignatureProperties>
      </UnsignedProperties>

    </QualifyingProperties>
  </Object>
</Signature>
```

```
------=_Part_0_18075465.1289232799781 // Part MIME de la pièce jointe du doc 1
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
Content-ID: <cid1>
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<ClinicalDocument              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:hl7-org:v3">
  <realmCode code="FR"/>
  <typeId root="2.16.840.1.113883.1.3" extension="POCD_HD000040"/>
  <templateId      root="2.16.840.1.113883.2.8.2.1"      assigningAuthorityName="HL7
France"/>
  <templateId       root="1.2.250.1.213.1.1.1.1"       assigningAuthorityName="Cadre
InteropASIP"/>
  <templateId root="1.3.6.1.4.1.19376.1.2.20" assigningAuthorityName="IHE XDS-SD"/>
  <id root="OID_doc1"/>
...
</ClinicalDocument>

[...]

------=_Part_0_18075465.1289232799781 // Part MIME de la pièce jointe du doc N
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
Content-ID: <cidN>
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<ClinicalDocument              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:hl7-org:v3">
  <realmCode code="FR"/>
  <typeId root="2.16.840.1.113883.1.3" extension="POCD_HD000040"/>
  <templateId      root="2.16.840.1.113883.2.8.2.1"      assigningAuthorityName="HL7
France"/>
  <templateId       root="1.2.250.1.213.1.1.1.1"       assigningAuthorityName="Cadre
InteropASIP"/>
  <templateId root="1.3.6.1.4.1.19376.1.2.20" assigningAuthorityName="IHE XDS-SD"/>
  <id root="OID_docN"/>
...
</ClinicalDocument>
```

## A6-3 Code exemple

Des exemples de messages et trames SOAP d'échange avec le système DMP sont mis à disposition par le GIE SESAM-Vitale à titre indicatif.

Ils sont téléchargeables sur l'Espace industriels du GIE SESAM-Vitale.

Les exemples mis à disposition sont :

- **des messages HL7 V3** (gestion administrative du dossier)
  - sans_SOAP : messages HL7 V3 non encapsulés dans un message SOAP - complète la description de chaque message
  - avec_SOAP : messages HL7 V3 encapsulés dans un message SOAP
- **des trames SOAP de web-services spécifiques**
- **des trames SOAP XDS.b**

Attention :

- les exemples et les trames SOAP ne constituent ni une référence, ni une spécification.
- certaines trames ont été volontairement reformatées (XML indenté) pour plus de lisibilité.
- la cohérence fonctionnelle des valeurs d'exemples renseignées n'est pas garantie : l'éditeur devra s'assurer que les valeurs produites dans les champs des messages correspondent bien à un cas fonctionnel possible pour le DMP.
- les valeurs de signatures peuvent être non significatives (trames reformatées).

# ANNEXE 7 CODES D'ERREURS

## A7-1 Liste des codes d'erreurs

| Code erreur | Description de l'erreur |
|---|---|
| DMPSystemError | Erreur système |
| DMPFunctionDisabled | Les fonctions liées au secret des mineurs ne sont pas encore activées dans le système DMP. Veuillez contacter votre éditeur de logiciel. |
| DMPIdentityCertificationFailure | Les données permettant d'identifier le patient n'ont pas été trouvées (erreur %).<br>Note : le "%" est dynamique et remplacé par un code erreur du système.<br>Il est demandé d'afficher le message à l'utilisateur tel quel sans modification. |
| DMPIdentityCertificationBusy | Le service de fourniture des identités patients est provisoirement indisponible. Réessayer ultérieurement (erreur %).<br>Note : le "%" est dynamique et remplacé par un code erreur du système.<br>Il est demandé d'afficher le message à l'utilisateur tel quel sans modification. |
| DMPFound | Le DMP existe déjà |
| DMPPatientNotFound | Patient inconnu (DMP non trouvé) |
| DMPClosed | DMP fermé |
| DMPLPSNotValidated | LPS en cours de validation |
| DMPErrorLPS | Le LPS n'a pas accès à ce service |
| DMPAccessForbidden | Accès interdit (le professionnel a été interdit d'accès par le patient) |
| DMPAuthorizationNotFound | Le professionnel n'a pas l'autorisation d'accès à ce DMP |
| DMPAuthorizationExpired | Autorisation d'accès expirée |
| DMPAccessDeniedByRightsService | Accès refusé par la matrice de droits fonctionnels |
| DMPInvalidData | Données non conformes au regard des règles de gestion |
| DMPInvalidRequest | Requête invalide au regard de la norme spécifiée |
| DMPConcurrentAccess | Accès concurrent sur une métadonnée |
| DMPInvalidSignature | Signature non valide |
| DMPInvalidCertificate | Certificat non valide |
| DMPVirusFound | Virus détecté |
| DMPDataAlreadyUsed | Données déjà utilisées |
| DMPOutOfExperimentalArea | DMP hors région expérimentale |
| DMPFragmentCVAError | Une règle de gestion concernant l'ajout, ou la modification de vaccination via une note de vaccination n'est pas respectée et rejette le traitement. |

| | |
|---|---|
| DMPTooManyResult | Trop de résultats, l'utilisateur doit affiner sa recherche |
| DMPActorNotFound | Acteur non trouvé |
| DMPDocumentFormatError | Le document n'est pas au bon format (CDA R2) |
| DMPPatientAccessNotFound | Accès patient pour le DMP non trouvé |
| DMPPatientAccessAlreadyExists | Accès patient déjà existant pour le DMP |
| DMPPatientAccessOTPNotFound | Pas de canal OTP configuré pour le DMP |
| DMPPatientAccessOTPAlreadyExists | Canal OTP du même type déjà créé pour le DMP |
| DMPPatientAccessOTPDeleteForbidden | Interdiction de supprimer le dernier canal OTP présent dans le DMP du patient |
| XDSMissingDocument | Le document n'existe plus ou n'est plus disponible |
| XDSMissingDocumentMetadata | Métadonnées manquantes pour un document |
| XDSRegistryNotAvailable | Registry inaccessible |
| XDSRegistryError | Erreur interne au registre |
| XDSRepositoryError | Erreur interne au dépôt |
| XDSRegistryDuplicateUniqueIdInMessage | Un identifiant unique est utilisé plusieurs fois au sein de la requête |
| XDSRepositoryDuplicateUniqueIdInMessage | Un identifiant unique est utilisé plusieurs fois au sein de la requête |
| XDSDuplicateUniqueIdInRegistry | uniqueId=[valeur du uniqueId du doc soumis] ; Un document strictement identique existe déjà dans le DMP que vous tentez d'alimenter : même empreinte numérique détectée (hash) ; pour limiter les erreurs de doublons de document dans un même DMP, ceci n'est pas autorisé. |
| XDSNonIdenticalHash | Le hash d'un document envoyé ne correspond pas à celui reçu dans les métadonnées |
| XDSRegistryBusy | Registre occupé |
| XDSRepositoryBusy | Dépôt occupé |
| XDSRegistryOutOfResources | Le registre n'a plus assez de ressources |
| XDSRepositoryOutOfResources | Le dépôt n'a plus assez de ressources |
| XDSRegistryMetadataError | Erreur dans les métadonnées |
| XDSReplaceFailed | Remplacement de document impossible |
| XDSRepositoryMetadataError | Erreur dans les métadonnées |
| XDSTooManyResults | Trop de résultats |
| XDSExtraMetadataNotSaved | Métadonnées inconnues non sauvegardées |
| XDSUnknownPatientId | Patient inconnu |
| XDSPatientIdDoesNotMatch | Des identifiants patients différents au sein de la requête |
| XDSUnknownStoredQuery | Identifiant de requête inconnu |
| XDSStoredQueryMissingParam | Un paramètre obligatoire est manquant |
| XDSStoredQueryParamNumber | Plusieurs valeurs affectées à un paramètre mono valué |
| XDSRegistryDeprecatedDocumentError | Un document référencé est déprécié |
| XDSUnknownRepositoryId | Identifiant unique de l'entrepôt de documents du DMP (repository XDS) incorrect |

| | |
|---|---|
| XDSDocumentUniqueIdError | Document indisponible |
| XDSResultNotSinglePatient | (code XDS non utilisé) |
| PartialFolderContentNotProcessed | (code XDS non utilisé) |
| PartialReplaceContentNotProcessed | (code XDS non utilisé) |
| XDSMetadataUpdateError | Erreur lors de la mise à jour de métadonnées |
| XDSMetadataUpdateOperationError | Erreur de décodage de la requête |
| XDSMetadataVersionError | Erreur de version des métadonnées du document à mettre à jour lors d'une tentative de mise à jour des métadonnées (TD3.3) |
| UnresolvedReferenceException | Métadonnées de document inexistantes.<br>La référence des métadonnées du document (entryUUID ou logicalID) à remplacer ou pour lequel l'utilisateur veut modifier les métadonnées (masquage, archivage...) n'est pas trouvée |
| DMPAccessDeniedByExcededThreshold<br><br>*« Accès en consultation de DMP bloqué : dépassement du nombre de consultations de DMP autorisé sur une période de temps. »* | Le professionnel tente de consulter un DMP en LPS ou en Web-PS alors qu'il a dépassé un seuil de blocage |
| DMPAccessDeniedForStructure<br><br>*« Accès en consultation de DMP bloqué pour l'établissement. »* | Le professionnel tente de consulter un DMP en LPS ou en Web-PS alors que sa structure a été bloquée. |

**Tableau 43 : codes d'erreurs et signification**

Pour les transactions spécifiques DMP et en cas d'absence d'erreur, le système DMP retourne « DMPOk ».

L'éditeur doit prendre en compte les codes erreurs signalés par X dans le tableau ci-dessous.

| Codes erreur \ Transactions | Test d'existence d'un DMP d'un patient et vérification de l'autorisation d'accès (PatientGetDemographics_PRPA_IN201307UV02) | Mise à jour de l'autorisation d'accès (setAutorization) | Liste des DMP autorisés (PatientList) | Recherche sans INS de patients dans le système DMP (PDQSupplier_PRPA_IN201305UV02) | Consultation des données administratives et de gestion d'un DMP (PatientGetDemographics_PRPA_IN201307UV02) | Liste des PS autorisés / bloqués sur le DMP d'un patient (listAuthorizationByPatient) | Alimentation en documents du DMP d'un patient (DocumentRepository_ProvideAndRegisterDocumentSet-b) | Recherche de documents dans le DMP d'un patient (DocumentRegistry_RegistryStoredQuery) | Consultation d'un document dans le DMP d'un patient (DocumentRepository_RetrieveDocumentSet) | Gestion des attributs d'un document (DocumentRegistry_UpdateDocumentSet) |
|---|---|---|---|---|---|---|---|---|---|---|
| | TD0.2 | TD0.3 | TD0.4 | TD0.5 | TD1.3a | TD1.6 | TD2.1 TD2.2 | TD3.1 | TD3.2 | TD3.3 |
| DMPSystemError | X | X | X | X | X | X | X | X | X | X |
| DMPFunctionDisabled | X | X | X | X | X | X | X | X | X | X |
| DMPIdentityCertificationFailure | | | | | | | | | | |
| DMPIdentityCertificationBusy | | | | | | | | | | |
| DMPFound | | | | | | | | | | |
| DMPPatientNotFound | | X | | X | X | X | X | | X | X |
| DMPClosed | | X | | X | X | X | X | X | X | X |
| DMPLPSNotValidated | X | X | X | X | X | X | X | X | X | X |
| DMPErrorLPS | X | X | X | X | X | X | X | X | X | X |
| DMPAccessForbidden | | X | X | | X | X | X | X | X | X |
| DMPAuthorizationNotFound | | X | X | | X | X | X | X | X | X |
| DMPAuthorizationExpired | | X | X | | X | X | X | X | X | X |
| DMPAccessDeniedByRightsService | | X | X | X | X | X | X | | X | X |
| DMPInvalidData | X | X | X | X | X | X | X | | X | X |
| DMPInvalidRequest | X | | X | X | X | | X | | X | |
| DMPConcurrentAccess | | | | | | | X | | | X |
| DMPInvalidSignature | | | | | | | X | | | |
| DMPInvalidCertificate | X | X | X | X | X | X | X | X | X | X |
| DMPVirusFound | | | | | | | X | | X | |
| DMPDataAlreadyUsed | | | | | | | | | | |
| DMPOutOfExperimentalArea | | | | | | | | | | |
| DMPFragmentCVAError | | | | | | | X | | | |
| DMPTooManyResult | | | | X | | | | | | |
| DMPActorNotFound | X | X | X | X | X | X | X | | X | X |
| DMPDocumentFormatError | | | | | | | X | | | |
| DMPPatientAccessNotFound | | | | | | | | | | |
| DMPPatientAccessAlreadyExists | | | | | | | | | | |
| DMPPatientAccessOTPNotFound | | | | | | | | | | |
| DMPPatientAccessOTPAlreadyExists | | | | | | | | | | |
| DMPPatientAccessOTPDeleteForbidden | | | | | | | | | | |
| XDSMissingDocument | | | | | | | X | | | |
| XDSMissingDocumentMetadata | | | | | | | X | | | |
| XDSRegistryNotAvailable | | | | | | | X | | | |
| XDSRegistryError | | | | | | | X | X | X | X |
| XDSRepositoryError | | | | | | | X | | X | |
| XDSRegistryDuplicateUniqueIdInMessage | | | | | | | X | | | |
| XDSRepositoryDuplicateUniqueIdInMessage | | | | | | | X | | | |
| XDSDuplicateUniqueIdInRegistry | | | | | | | X | | | |
| XDSNonIdenticalHash | | | | | | | X | | | |
| XDSRegistryBusy | | | | | | | X | X | X | X |
| XDSRepositoryBusy | | | | | | | X | | X | |
| XDSRegistryOutOfResources | | | | | | | X | X | X | X |
| XDSRepositoryOutOfResources | | | | | | | X | | X | |
| XDSRegistryMetadataError | | | | | | | X | | | X |
| XDSReplaceFailed | | | | | | | X | | | |
| XDSRepositoryMetadataError | | | | | | | X | | | |
| XDSTooManyResults | | | | | | | | X | | |
| XDSExtraMetadataNotSaved | | | | | | | X | | | |
| XDSUnknownPatientId | | | | | | | X | X | X | X |
| XDSPatientIdDoesNotMatch | | | | | | | X | | | X |
| XDSUnknownStoredQuery | | | | | | | | X | | |
| XDSStoredQueryMissingParam | | | | | | | | X | | |
| XDSStoredQueryParamNumber | | | | | | | | X | | |
| XDSRegistryDeprecatedDocumentError | | | | | | | X | | | |
| XDSUnknownRepositoryId | | | | | | | | | X | |
| XDSDocumentUniqueIdError | | | | | | | | | X | |
| XDSMetadataUpdateError | | | | | | | | | | X |
| XDSMetadataUpdateOperationError | | | | | | | | | | X |
| XDSMetadataVersionError | | | | | | | | | | X |
| UnresolvedReferenceException | | | | | | | | | | X |
| DMPAccessDeniedByExcededThreshold | | | | | | | | X | X | |
| DMPAccessDeniedForStructure | | | | | | | | X | X | |

**Tableau 44 : codes erreur par transaction**

## A7-2 Liste des codes d'erreur spécifiques au mode AIR

| Code erreur et libellé associé | Description de l'erreur |
|---|---|
| `DMPAccessDeniedByRightsService`<br><br>*« Accès au DMP impossible : votre établissement n'est pas habilité à utiliser cette méthode d'authentification (indirecte renforcée) »* | La structure de soins ayant soumis la requête au SI DMP n'est pas habilitée à utiliser le mode d'authentification indirecte renforcée. |
| `DMPErrorLPS`<br><br>*« Accès au DMP impossible : votre logiciel n'est pas homologué pour réaliser cette action avec cette méthode d'authentification (indirecte renforcée). »* | Le logiciel de professionnel de soins (LPS) ayant soumis la requête n'est pas homologué pour utiliser le mode d'authentification indirecte renforcée, ou la transaction appelée n'est pas homologuée dans ce mode (ex : appel d'une TD2.1 alimentation DMP en authentification indirecte renforcée alors que le LPS n'est homologué pour cette transaction qu'en mode authentification indirecte). |
| `DMPActorNotFound`<br><br>*« Utilisateur non reconnu : le professionnel de santé n'est pas connu du référentiel DMP. »* | L'identifiant national du PS fourni dans le VIHF n'est pas présent dans l'annuaire interne des PS du SI DMP. |
| `DMPAccessDeniedByRightsService`<br><br>*« Accès au DMP impossible : votre profil utilisateur ne vous autorise pas à vous connecter avec cette méthode d'authentification (indirecte renforcée) »* | Le profil de l'utilisateur fourni dans le VIHF n'est pas autorisé à se connecter en mode d'authentification indirecte renforcée (profil différent de PS, MEDECIN ou MEDECIN_TRAITANT). |
| `DMPAccessDeniedByRightsService`<br><br>*« Accès au DMP impossible : le secteur d'activité auquel vous appartenez ne vous autorise pas à vous connecter avec cette méthode d'authentification (indirecte renforcée). »* | Le Web-PS reçoit une requête dont le secteur d'activité auquel le PS appartient n'est pas autorisé à se connecter en mode authentification indirecte renforcée. |
| `DMPInvalidRequest`<br><br>*« Accès au DMP impossible : erreur technique de votre logiciel, veuillez contacter votre responsable technique ou votre éditeur (cause : date de validité du jeton VIHF incorrecte). »* | La date de validité du jeton VIHF est incorrecte (trop vieux ou dans le futur) |
| `DMPInvalidRequest`<br><br>*« Accès au DMP impossible : erreur technique de votre logiciel, veuillez contacter votre responsable technique ou votre éditeur (cause : jeton VIHF déjà utilisé). »* | Le jeton VIHF a déjà été utilisé durant sa période de validité. |

| Code erreur et libellé associé | Description de l'erreur |
|---|---|
| `DMPInvalidRequest`<br><br>*« Accès au DMP impossible : erreur technique de votre logiciel, veuillez contacter votre responsable technique ou votre éditeur (cause : vérification du jeton VIHF en échec). »* | Le SI DMP ne peut pas vérifier la signature du jeton VIHF, car le jeton est mal signé. |
| `DMPInvalidRequest`<br><br>*« Accès au DMP impossible : erreur technique de votre logiciel, veuillez contacter votre responsable technique ou votre éditeur (cause : méthode d'authentification primaire de l'utilisateur non autorisée pour cet établissement). »* | La méthode de connexion primaire du PS déclarée dans le jeton VIHF n'est pas autorisée par la liste blanche paramétrée sur le SI DMP. |
| `DMPAccessDeniedByExcededThreshold`<br><br>*« Accès en consultation de DMP bloqué : dépassement du nombre de consultations de DMP autorisé sur une période de temps. »* | Le PS tente de consulter un DMP en LPS ou en Web-PS alors qu'il a dépassé un seuil de blocage |
| `DMPAccessDeniedForStructure`<br><br>*« Accès en consultation de DMP bloqué pour l'établissement. »* | Le PS tente de consulter un DMP en LPS ou en Web-PS alors que sa structure a été bloquée. |

## A7-3 Erreurs spécifiques du processus d'authentification (« SOAP Fault »)

Le processus d'authentification sur le SI DMP peut entraîner des retours d'erreur de « premier niveau » de type « SOAP Fault ».

Le tableau ci-dessous fournit les cas d'erreur fréquemment rencontrés lors de la mise au point du LPS (phase de développement) :

| Message d'erreur type retourné | Cause |
|---|---|
| DMPInvalidData;Le sujet de l'assertion (1234567890/013122) n'est pas un descendant de l'identifiant de structure du certificat : 1234567890 | Le format du champ NameID ne se conforme pas aux règles définies pour le jeton VIHF (voir §5.3.1.3).<br>Comme défini dans le CI-SIS, en authentification indirecte il y a une codification spécifique du premier chiffre de l'identifiant de la personne connectée (champ VIHF /Assertion/Subject/NameID) à effectuer en fonction du type d'identifiant de la structure (champ VIHF Identifiant_structure).<br>Voir le document ci-sis_anx_sources-donnees-professionnels-structures… .pdf qui donne les règles de codification du premier chiffre de chaque identifiant (§ 5.4 PS_IdNat pour NameID et § 5.5 Struct_IdNat pour Identifiant_structure).<br>Attention : si le candidat utilise un certificat de test contenant son identifiant SIRET pour ses développements, le certificat de production d'un établissement contient en général un FINESS (premier chiffre différent), et il faut donc prendre en compte ces règles correctement. |
| DMPInvalidData : xxxxxx : Structure introuvable | La structure liée au certificat n'est pas présente dans l'annuaire interne du SI DMP.<br>En phase de développement, il se peut que l'annuaire de l'environnement de développement du candidat ne soit pas à jour. |
| DMPInvalidData : xxxxxx : Profession non correspondante | En authentification directe, ce message d'erreur est remonté par le système DMP lorsque la profession fournie dans le jeton VIHF n'est pas renseignée correctement par rapport à la carte CPx utilisée (données de l'annuaire RASS).<br>Afin de renseigner correctement les différents champs du VIHF, l'éditeur doit consulter les documents suivants :<br>• Le présent document,<br>• [CI-TR-CLI-LRD],<br>• [CI-ANX-PS-STRU].<br>Certaines données doivent notamment être lues dans la carte CPx en authentification directe. Les données des cartes CPx sont vérifiées par le serveur DMP via l'annuaire RASS. |
| DMPInvalidData : xxxxxx : aucune spécialité pour médecin | Cette erreur est remontée lorsque le champ spécialité du médecin n'est pas fourni par le LPS. Pour les médecins et les pharmaciens, le LPS doit fournir un second champ "role" (attribut SAML de nom "urn:oasis:names:tc:xacml:2.0:subject:role") dans le jeton VIHF comportant la spécialité de l'utilisateur connecté, en respectant la nomenclature des "savoir faire RPPS". Il existe une particularité pour le transcodage du code « spécialité ADELI » (lu dans la carte) vers le code « savoir faire RPPS » (requis par le système DMP).<br>NB : une erreur équivalente peut se produire pour les autres occurrences de subject:role. |

| | |
|---|---|
| DMPInvalidData : Le PS n'a pas les droits d'accéder à ce dossier : PS et Structure non lies | En authentification directe, cette erreur est remontée lorsque le champ Identifiant_Structure du jeton VIHF n'est pas renseigné correctement par rapport à la carte CPS utilisée (cohérence entre les données de la carte et les données fournies dans le jeton VIHF).<br>Afin de renseigner correctement les différents champs du jeton VIHF, l'éditeur doit consulter les documents suivants :<br>• Le présent document,<br>• [CI-TR-CLI-LRD],<br>• [CI-ANX-PS-STRU].<br>Certaines données doivent notamment être lues dans la carte CPS en authentification directe.<br>Les données des cartes CPS sont vérifiées par le serveur DMP via l'annuaire RASS. |
| DMPInvalidCertificate;Le certificat ayant signé le jeton VIHF est invalide : Not a valid signature certificate | Il faut vérifier :<br>• que le certificat ayant signé le jeton VIHF est bien un certificat (réel pour la production ou de test pour les environnements de test) émis par l'IGC Santé (gamme élémentaire), non révoqué et valide (date de validité),<br>• que le certificat est bien un certificat de signature ou de cachet (la signature du jeton VIHF avec un certificat d'authentification n'est pas autorisée)<br>Pour le vérifier, on reconnait le type de certificat suivant sa capacité ("keyUsage"), pour les certificats IGC Santé<br>○ Pour les certificats d'Authentification : il faut avoir « keyUsage » à « digitalSignature »<br>○ Pour les certificats de cachet: il faut avoir « keyUsage » à « nonREpudiation » |
| Secteur d'activité non correspondant | Deux raisons possibles à cette erreur :<br>• soit le champ Secteur_Activite du jeton VIHF ne correspond pas à la carte ou au certificat utilisé pour l'authentification,<br>• soit le champ Identifiant_Structure du jeton VIHF ne correspond pas à la carte ou au certificat utilisé pour l'authentification (et par extension le secteur d'activité ne correspond pas à cette structure).<br>Dans le cas où le candidat utilise le code exemple, il doit l'adapter à son usage et plus particulièrement dynamiser les champs liés au contexte de ses utilisateurs (le secteur d'activité en est un) ; dans le code exemple en Java, le secteur d'activité est codé dans la classe com.dmp.security.vihf.handlers.VIHFClientHandler et dans les classes du package com.dmp.kit_editeur.vihf (selon que le jeton VIHF est signé ou non).<br>Le candidat doit envoyer dans le jeton VIHF les données associées à la structure représentée par le certificat présenté. |

**Tableau 45 : erreurs spécifiques du processus d'authentification (« SOAP Fault »)**

# ANNEXE 8 SYNTHESE DES ECARTS ENTRE LE SYSTEME DMP ET LE CI-SIS

Le tableau ci-dessous indique, pour chaque thème, la localisation de la description de l'écart.

| Thème | Description |
|---|---|
| Test d'existence DMP sur 1 ou plusieurs INS. | Restriction de cardinalité au niveau de `patientIdentifier` § 3.2.2.2, page 54. |
| Données concernant l'auteur du document et du lot de soumission. | Dérogation dans RG_2230 au § 3.4.1.1.3, page 93. |
| Gestion du masquage et de la visibilité d'un document. | Dérogation pour TD3.1 au § 3.5.1.3, page 113 et pour TD3.3 au § 3.5.3.3, page 124. |
| Sauvegarde des lots en cas de changement de `availabilityStatus` d'une fiche. | Dérogation pour TD3.1 au § 3.5.1.3 page 113. |
| Structure des éléments d'adresse dans le volet gestion de dossier partagé. | Dérogation au niveau de l'adresse du patient dans le § 4.2.2, page 133. |
| Champs du VIHF non utilisés par le système DMP | Précision § 5.3.2, page 160 et § 5.3.3, page 166 sous les tableaux décrivant les champs du VIHF. |

**Tableau 46 : Synthèse des écarts entre le système DMP et le CI-SIS**

# ANNEXE 9 SPECIFICATION DES TRACES AIR

La structure de soins doit tracer dans le cadre de l'accès au DMP :

- L'authentification de l'utilisateur ;
- La génération d'un jeton VIHF pour l'utilisateur ;
- La transaction DMP sollicitée (accès web-service TD0.1) ;
- La transaction DMP sollicitée (accès Web-PS TD0.10).

La trace d'une authentification de l'utilisateur doit comporter les éléments suivants :

- Date et heure (jusqu'à la seconde) de l'authentification (localisée) au format `xs:dateTime` ;
- Identifiant de la structure de soins tel qu'inscrit dans le VIHF (identique à l'élément `Identifiant_Structure` de l'assertion SAML) ;
- Identifiant national de l'utilisateur (identique à l'élément XML `<saml2:NameID>` de l'assertion SAML) ;
- Contexte d'authentification (identique à l'élément XML `<saml2:AuthnContextDecl>` de l'assertion SAML) ;
- Statut de l'authentification (succès ou échec).

La trace de génération du jeton VIHF doit comporter les éléments suivants :

- Date de génération (localisée) au format `xs:dateTime` ;
- Identifiant de la structure de soins tel qu'inscrit dans le VIHF (identique à l'élément `Identifiant_Structure` de l'assertion SAML) ;

- Identifiant national de l'utilisateur (identique à l'élément XML `<saml2:NameID>` de l'assertion SAML) ;
- L'identifiant unique du jeton VIHF, c'est-à-dire l'attribut `assertion/@ID` de l'assertion SAML ;
- Une copie du jeton VIHF transmis (base 64), contenant la signature.

Dans le cas des accès web-service, les traces de ces accès comportent les éléments suivants :

- Date et heure (jusqu'à la seconde) d'accès (localisée) au format `xs:dateTime` ;
- Identifiant de la structure de soins tel qu'inscrit dans le VIHF (identique à l'élément `Identifiant_Structure` de l'assertion SAML) ;
- Identifiant national de l'utilisateur (identique à l'élément XML `<saml2:NameID>` de l'assertion SAML) ;
- L'identifiant unique du jeton VIHF utilisé, c'est-à-dire l'attribut `assertion/@ID` de l'assertion SAML ;
- Identifiant de la transaction du DMP sollicitée ;

| Identifiant de la transaction DMP | Description |
|---|---|
| TD0.2 | Test d'existence |
| TD0.3 | Mise à jour de l'autorisation |
| TD0.4 | Liste des DMP autorisés |
| TD0.5 | Recherche d'un patient sans INS |
| TD3.1 | Recherche de document |
| TD3.2 | Consultation d'un document |
| TD3.3a | Masquer un document au PS |
| TD3.3b | Rendre un document visible au patient |
| TD3.3c | Supprimer un document |
| TD3.3d | Archiver un document |

Dans le cas des accès Web-PS, les traces de ces accès comportent les éléments suivants :

- Date d'accès (jusqu'à la seconde) d'accès (localisée) au format `xs:dateTime` ;
- Identifiant de la structure de soins tel qu'inscrit dans le VIHF (identique à l'élément `Identifiant_Structure` de l'assertion SAML) ;
- Identifiant national de l'utilisateur (identique à l'élément XML `<saml2:NameID>` de l'assertion SAML) ;
- L'identifiant du jeton VIHF utilisé, c'est-à-dire l'attribut `assertion/@ID` de l'assertion SAML ;
- URL du Web-PS appelée en TD0.10.

Sur demande, les traces doivent être fournies en CSV (séparateur « ; », encodé en UTF-8) avec en-tête. Un document de description du fichier de traces devra également être fourni.