

Cahier des Clauses Techniques Particulières

Accord-cadre n°AC.2023.1788

**MESDMP** (**M**on **E**space **S**anté – **D**ossier **M**édical **P**artagé)

Table des matières

[Préambule 7](#_Toc138774859)

[1 Glossaire 8](#_Toc138774860)

[2 Présentation de l’Assurance Maladie et du Numérique en Santé 12](#_Toc138774861)

[2.1 Présentation générale de l’Assurance Maladie 12](#_Toc138774862)

[2.1.1 Les missions de l’Assurance Maladie 12](#_Toc138774863)

[2.1.2 Le réseau de l’Assurance Maladie 12](#_Toc138774864)

[2.2 La Cnam 14](#_Toc138774865)

[2.2.1 Les missions de la Cnam 14](#_Toc138774866)

[2.2.2 L’organisation de la Cnam 15](#_Toc138774867)

[2.3 La Direction Déléguée des Systèmes d’Information (DDSI) 15](#_Toc138774868)

[2.3.1 Les Systèmes d’Information 15](#_Toc138774869)

[2.3.2 Les missions de la DDSI 16](#_Toc138774870)

[2.3.3 L’organisation de la DDSI 17](#_Toc138774871)

[2.3.4 Présentation géographique de l’organisation DDSI et des CTI-CEIR. 17](#_Toc138774872)

[2.4 La Direction déléguée à la gestion et à l’organisation des soins 19](#_Toc138774873)

[2.4.1 Direction opérationnelle du numérique et de l’innovation en santé (DIONIS) 20](#_Toc138774874)

[2.5 Présentation du contexte du Numérique en Santé 21](#_Toc138774875)

[3 Présentation de l’existant : MES et DMP 23](#_Toc138774876)

[3.1 Présentation du périmètre existant MES 23](#_Toc138774877)

[3.1.1 Présentation du périmètre fonctionnel MES 23](#_Toc138774878)

[3.1.2 Existant Mon Espace Santé et ses sous-produits 23](#_Toc138774879)

[3.1.3 Mon Espace Santé 24](#_Toc138774880)

[3.1.4 Sites et portails autour de Mon Espace Santé 48](#_Toc138774881)

[3.1.5 Indicateurs métier 52](#_Toc138774882)

[3.2 Présentation du périmètre technique MES 53](#_Toc138774883)

[3.2.1 Présentation générale de l’architecture de MES 53](#_Toc138774884)

[3.2.2 Présentation détaillée de l’architecture de MES 57](#_Toc138774885)

[3.2.3 Architecture Technique de MES 64](#_Toc138774886)

[3.3 Présentation du périmètre existant DMP 72](#_Toc138774887)

[3.3.1 Fonctionnalités du DMP 72](#_Toc138774888)

[3.3.2 Les documents du DMP 74](#_Toc138774889)

[3.3.3 Contexte d’accès au DMP par les PS 75](#_Toc138774890)

[3.3.4 WebDMP PS 76](#_Toc138774891)

[3.3.5 Interfaces DMP proposées aux LPS 76](#_Toc138774892)

[3.3.6 Interfaces DMP avec MES 79](#_Toc138774893)

[3.3.7 Site institutionnel DMP 80](#_Toc138774894)

[3.3.8 Support DMP 81](#_Toc138774895)

[3.3.9 Web MH 81](#_Toc138774896)

[3.3.10 SI Pilotage DMP 81](#_Toc138774897)

[3.4 Présentation du périmètre technique DMP 83](#_Toc138774898)

[3.4.1 Présentation générale de l’architecture du DMP 83](#_Toc138774899)

[3.4.2 Présentation détaillée de l’architecture du DMP 86](#_Toc138774900)

[3.4.3 Architecture Technique du DMP 98](#_Toc138774901)

[3.5 Besoins d’évolution et convergence MES DMP 100](#_Toc138774902)

[3.5.1 Convergence entre MES et le DMP 100](#_Toc138774903)

[3.5.2 Besoins d’évolution du système MES DMP 100](#_Toc138774904)

[3.5.3 Métriques de MESDMP 116](#_Toc138774905)

[3.6 Architecture envisagée à 3 ans (MES + DMP = MESDMP) 117](#_Toc138774906)

[4 Présentation générale de l’accord-cadre 123](#_Toc138774907)

[4.1 Objet et forme de l’accord-cadre 123](#_Toc138774908)

[4.2 Lieux d’exécution des prestations 124](#_Toc138774909)

[4.3 Livraison / Validation et réception des prestations 125](#_Toc138774910)

[4.3.1 Modalités de livraison 125](#_Toc138774911)

[4.3.2 Validation et admission des prestations 125](#_Toc138774912)

[5 Cadre organisationnel 126](#_Toc138774913)

[5.1 Principes et responsabilités respectives des acteurs 126](#_Toc138774914)

[5.2 Organisation des équipes 127](#_Toc138774915)

[5.3 Méthodologie de développement 129](#_Toc138774916)

[5.3.1 Méthodologie Agile 129](#_Toc138774917)

[5.3.2 Méthodologie de projet Cycle en V 135](#_Toc138774918)

[5.3.3 Exigences communes aux méthodes Agiles et cycle en V 137](#_Toc138774919)

[5.4 Rôles et activités clés 140](#_Toc138774920)

[5.4.1 Rôles Direction produit 141](#_Toc138774921)

[5.4.2 Rôles de niveau Delivery transverse 142](#_Toc138774922)

[5.4.3 Rôles au niveau Delivery des Features 143](#_Toc138774923)

[5.4.4 Rôles Direction services 144](#_Toc138774924)

[5.5 Comitologie 146](#_Toc138774925)

[5.5.1 Comitologie Pilotage 146](#_Toc138774926)

[5.5.2 Comitologie Produit 146](#_Toc138774927)

[5.5.3 Comitologie Feature Teams 146](#_Toc138774928)

[5.5.4 Comitologie Services 147](#_Toc138774929)

[5.6 Politique qualité 148](#_Toc138774930)

[6 Définition des besoins 152](#_Toc138774931)

[6.1 Exigences fonctionnelles 152](#_Toc138774932)

[6.1.1 Reprise de l’existant 152](#_Toc138774933)

[6.1.2 Identification/Enrôlement 152](#_Toc138774934)

[6.1.3 Gestion des comptes 152](#_Toc138774935)

[6.1.4 Gestion des notifications 152](#_Toc138774936)

[6.1.5 Consentement pour échanges de données avec MES 153](#_Toc138774937)

[6.1.6 Capacité d’interfaçage 153](#_Toc138774938)

[6.1.7 Expérience utilisateur, ergonomie et facilité d’utilisation de la solution 153](#_Toc138774939)

[6.1.8 Facilité d’intégration de briques supplémentaires 154](#_Toc138774940)

[6.1.9 SI PILotage 154](#_Toc138774941)

[6.1.10 Audit et statistiques 155](#_Toc138774942)

[6.2 Exigences d’Architecture et d’Exploitation 155](#_Toc138774943)

[6.2.1 Exigences d’Architecture Applicative 155](#_Toc138774944)

[6.2.2 Exigences d’Architecture Technique 159](#_Toc138774945)

[6.2.3 Exigences de Disponibilité 163](#_Toc138774946)

[6.2.4 Exigences de Volumétrie 167](#_Toc138774947)

[6.2.5 Exigences de Performance 167](#_Toc138774948)

[6.2.6 Exigences de Continuité 169](#_Toc138774949)

[6.2.7 Exigences de Supervision et métrologie 172](#_Toc138774950)

[6.2.8 Exigences Environnement logiciel 173](#_Toc138774951)

[6.2.9 Exigences spécifique liée au cluster de composants WAF 176](#_Toc138774952)

[6.3 Exigences générales 177](#_Toc138774953)

[6.3.1 Exigences de réversibilité 177](#_Toc138774954)

[6.3.2 Exigences de sécurité 179](#_Toc138774955)

[6.3.3 Exigences de Maintenabilité Opérationnelle 185](#_Toc138774956)

[6.3.4 Exigences de Recette 187](#_Toc138774957)

[6.3.5 Exigences de Support 187](#_Toc138774958)

[6.3.6 Exigences de Gestion des Risques 194](#_Toc138774959)

[7 Prestations adressées par l’accord-cadre 196](#_Toc138774960)

[7.1 Planning indicatif des prestations 196](#_Toc138774961)

[7.2 P1.1 - Pdc\_Init : Prise de connaissance et Initialisation 197](#_Toc138774962)

[7.2.1 Objet 197](#_Toc138774963)

[7.2.2 Exigences spécifiques 197](#_Toc138774964)

[7.2.3 Livrables 197](#_Toc138774965)

[7.2.4 Durée et point de départ des prestations 197](#_Toc138774966)

[7.3 P1.2 - Rep : Reprise de l’existant 197](#_Toc138774967)

[7.3.1 Objet 198](#_Toc138774968)

[7.3.2 Le cadre organisationnel 199](#_Toc138774969)

[7.3.3 Appropriation des connaissances 200](#_Toc138774970)

[7.3.4 Récupération des tickets d’incidents 200](#_Toc138774971)

[7.3.5 Récupération des tests automatisés 200](#_Toc138774972)

[7.3.6 Récupération des données 200](#_Toc138774973)

[7.3.7 Reprise des outils de monitoring des systèmes 201](#_Toc138774974)

[7.3.8 Mise en oeuvre d’une plateforme d’intégration continue et de déploiement continu afin de reprendre le patrimoine MES et DMP 201](#_Toc138774975)

[7.3.9 Livrables 204](#_Toc138774976)

[7.3.10 Exigences spécifiques 205](#_Toc138774977)

[7.3.11 Durée et point de départ des prestations 205](#_Toc138774978)

[7.4 P2 - PSE – Hébergement 206](#_Toc138774979)

[7.4.1 Objet 206](#_Toc138774980)

[7.4.2 Exigences spécifiques 206](#_Toc138774981)

[7.4.3 Livrables 208](#_Toc138774982)

[7.4.4 Durée et point de départ des prestations 208](#_Toc138774983)

[7.5 P3 - Conv : Convergence des systèmes MES et DMP 208](#_Toc138774984)

[7.5.1 Objet 208](#_Toc138774985)

[7.5.2 Exigences spécifiques 209](#_Toc138774986)

[7.5.3 Livrables 209](#_Toc138774987)

[7.5.4 Durée et point de départ des prestations 209](#_Toc138774988)

[7.6 P4 - Trans : Transverse 209](#_Toc138774989)

[7.6.1 Objet 209](#_Toc138774990)

[7.6.2 Exigences spécifiques 210](#_Toc138774991)

[7.6.3 Livrables 210](#_Toc138774992)

[7.6.4 Durée et point de départ des prestations 210](#_Toc138774993)

[7.7 P5 - Run\_MCO-S : Run, MCO et MCS 210](#_Toc138774994)

[7.7.1 Objet 210](#_Toc138774995)

[7.7.2 Exigences spécifiques 211](#_Toc138774996)

[7.7.3 Livrables 212](#_Toc138774997)

[7.7.4 Durée et point de départ des prestations 212](#_Toc138774998)

[7.8 P6 – Homologation NIS/NIS-2 212](#_Toc138774999)

[7.8.1 Objet 212](#_Toc138775000)

[7.8.2 Exigences spécifiques 212](#_Toc138775001)

[7.8.3 Livrables 212](#_Toc138775002)

[7.8.4 Durée et point de départ des prestations 212](#_Toc138775003)

[7.9 P7 - SMS\_Mail : Run SMS et Mail 213](#_Toc138775004)

[7.9.1 Objet 213](#_Toc138775005)

[7.9.2 Exigences spécifiques 213](#_Toc138775006)

[7.9.3 Livrables 213](#_Toc138775007)

[7.9.4 Durée et point de départ des prestations 213](#_Toc138775008)

[7.10 To1 – Réversibilité (tranche optionnelle) 214](#_Toc138775009)

[7.10.1 Objet 214](#_Toc138775010)

[7.10.2 Exigences spécifiques 214](#_Toc138775011)

[7.10.3 Livrables 214](#_Toc138775012)

[7.10.4 Durée et point de départ des prestations 214](#_Toc138775013)

[7.11 Prestations à bons de commandes 214](#_Toc138775014)

[7.11.1 Catalogue d’Unités d’œuvre (UO) 214](#_Toc138775015)

[7.11.2 Liste des unités d’œuvre (UO) 214](#_Toc138775016)

[7.11.3 Grille de lecture du catalogue d'unités d’œuvre 218](#_Toc138775017)

[7.11.4 Etat préparatoire à la Commande (EPC) 219](#_Toc138775018)

[7.11.5 Conditions particulières 220](#_Toc138775019)

[7.12 Liste des livrables principaux 220](#_Toc138775020)

[8 Liste des annexes 224](#_Toc138775021)

[1) MESDMP\_Annexe 01 – Personas 224](#_Toc138775022)

[2) MESDMP\_Annexe 02\_PAS 224](#_Toc138775023)

[3) MESDMP\_Annexe 03\_Catalogue Unités D’œuvre 224](#_Toc138775024)

[4) MESDMP\_Annexe\_04\_Documentation technique pour les Opérateurs MSSanté : 224](#_Toc138775025)

[5) MESDMP\_Annexe 05 – Manuel Utilisation Clear Quest – FS-FT 224](#_Toc138775026)

[6) MESDMP\_Annexe 06 – Workflow Clear Quest Fiche de Signalement 224](#_Toc138775027)

[7) MESDMP\_Annexe 07 – Workflow Clear Quest Fiche Tiers 224](#_Toc138775028)

[8) MESDMP\_Annexe 08 – Workflow Clear Quest Demande de service 224](#_Toc138775029)

[9) MESDMP\_Annexe 09\_Documents-Réversibilité sortante MES 224](#_Toc138775030)

[10) MESDMP\_Annexe 10\_Inventaire DMP 224](#_Toc138775031)

[11) MESDMP\_Annexe 11\_Description générale des mécanismes de chiffrement 224](#_Toc138775032)

[12) MESDMP\_Annexe 12\_Description détaillée de la protection des données 224](#_Toc138775033)

[13) MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique 224](#_Toc138775034)

[14) MESDMP\_Annexe 14\_DMP-Description Technique 224](#_Toc138775035)

[15) MESDMP\_Annexe 15\_MES-Outils Logiciels 224](#_Toc138775036)

[16) MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End 224](#_Toc138775037)

[17) MESDMP\_Annexe 17\_MES-Dossier Architecture Logicielle Front-End 224](#_Toc138775038)

[18) MESDMP\_Annexe 18\_MES-VMs Inventaire 224](#_Toc138775039)

[19) MESDMP\_Annexe 19\_MES-Référentiel des composants 225](#_Toc138775040)

[20) MESDMP\_Annexe 20\_MES\_FR-CNAM-ENS-HLD 225](#_Toc138775041)

[21) MESDMP\_Annexe 21\_DMP-AV-HSM 225](#_Toc138775042)

[22) MESDMP\_Annexe 22\_MES-Matrice des flux 225](#_Toc138775043)

[23) MESDMP\_Annexe 23\_PAQ\_Indicateurs\_Exemple de sommaire 225](#_Toc138775044)

[24) MESDMP\_Annexe 24\_Plan d’Assurance Qualité – Exemple de sommaire 225](#_Toc138775045)

[25) MESDMP\_Annexe 25\_Matrice de Gestion des risques 225](#_Toc138775046)

[26) MESDMP\_Annexe 26\_Scénario\_d’audit\_accessibilité 225](#_Toc138775047)

[27) MESDMP\_Annexe 27\_Scénario écoscore 225](#_Toc138775048)

[28) MESDMP\_Annexe 28\_Clients\_rapports\_SI\_PIL-DMP 225](#_Toc138775049)

[29) MESDMP\_Annexe 29\_Codes sources 225](#_Toc138775050)

Historique du CCTP MESDMP

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Statut | Rédacteur | Date |
|  |  |  |  |
|  |  |  |  |

# Préambule

Les phrases sur fond bleu correspondent à des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

# Glossaire

| Acronyme | Signification/Définition / Commentaire |
| --- | --- |
| AM | L’Assurance Maladie est une subdivision de la Sécurité sociale chargée de gérer les dépenses de santé. |
| Anomalie (ou Incident) | Voir « Incident » |
| Anonymisation | L’anonymisation est une technique irréversible qui consiste à supprimer tout caractère identifiant à un ensemble de données. Concrètement, cela signifie que toutes les informations directement ou indirectement identifiantes sont supprimées ou modifiées, rendant impossible toute ré-identification des personnes |
| ANS | Agence du Numérique en santé (ex ASIP Santé) |
| ARS | Agence Régionale de Santé |
| BO | Back-office |
| BSP | Bouquet de Services aux Professionnels (de soins) |
| BS | Bouquet de Services équivaut à BSP |
| CARSAT | Caisse d’Assurance Retraite et de la Santé au Travail |
| CCAP | Cahier des Clauses Administratives Particulières qui fixe les stipulations administratives du contrat. |
| CDR | Centre de recette |
| CGSS | Caisse Générale de Sécurité Sociale |
| CGU | Conditions Générales d’Utilisation |
| CI-SIS | Cadre d’Interopérabilité des Systèmes d’Informations de Santé |
| CMDB | « Configuration Management DataBase »  Base de données de gestion de configuration comportant tous les composants du système, permettant d’avoir une vue d’ensemble sur l’organisation de ces composants et d’en modifier leur configuration si nécessaire |
| CNIL | Commission nationale informatique et libertés |
| COG | Convention d’Objectifs et de Gestion qui régit les orientations de l’Assurance Maladie sous couvert de son autorité de tutelle, l’Etat. |
| CPAM | Caisse Primaire d’Assurance Maladie |
| CPS | Carte de professionnel de santé |
| CRAM | Caisse Régionale d’Assurance Maladie |
| Création ENS | Fait de créer les ressources techniques en back-office de l’ENS (création du compte, de la messagerie, de l’agenda, du DMP, etc.). En fonction des ressources la création peut être logique ou physique. |
| DevOps | Unification entre les équipes de développement et d’administration des infrastructures techniques, qui met l’accent sur la communication, la collaboration et l’intégration. |
| DevSecOps | Dans le processus DevOps, prise en compte des exigences sécurité dès la conception (approche security by design) et industrialisation des tâches sécurité dans la chaîne CI/CD, dans les infrastructures, le processus et les outils. |
| DIMA | Durée d'Indisponibilité Maximale Admissible |
| DMP | Dossier Médical Partagé |
| DPI | Dossier Patient Informatisé |
| DROM | Département et Région d'Outre-Mer : Territoire français qui constitue à la fois un département (DOM) et une région (ROM) d'outre-mer. |
| DTV | Dossier de Tests et de Validations.  Document décrivant la procédure pour tester le bon fonctionnement d’un service. Il doit être mis à jour à chaque changement. |
| ENS | Espace Numérique de Santé |
| EPC | Etat Préparatoire à la Commande |
| Enrôlement | Processus permettant à un usager d’accepter la création de son Espace Numérique de Santé |
| Feature teams | Ensemble des équipes qui travaillent sur un produit, disposant de l’ensemble des expertises leur permettant de réaliser les fonctionnalités complètes du produit sur leur périmètre. |
| FHIR | Fast Healthcare Interoperability Resource : norme d'interopérabilité conçue pour permettre l'échange de données de santé par voie électronique entre différents systèmes du secteur des soins de santé. |
| FI | Founisseur d’Identité |
| FO | Front-office |
| HAS | Haute Autorité de Santé |
| HDS | Hébergement des données de santé |
| Incident (ou Anomalie) | Il s’agit d’un incident ou anomalie de fonctionnement se présentant dans un contexte Hors Production (recette, …) ou en Production. |
| Initiative | Ensemble de tâches, axées sur un objectif commun, qui peuvent subdivisées en plusieurs brèves exigences ou requêtes, appelées user stories. |
| INS | Identifiant National de Santé.  La loi consacre le NIR – à défaut le NIA pour les personnes en cours d’immatriculation - comme identifiant national de santé (INS). |
| KPI | Indicateurs clés de performance |
| LPS | Logiciel des Professionnels de Santé |
| MCO | Maintien en Condition Opérationnelle |
| MCS | Maintien en Condition Sécurité |
| MES | Mon espace santé |
| MESDMP  (ou MESDMP) | Mon espace santé – Dossier Médical Partagé |
| MT | Médecin Traitant |
| NIA | Numéro identifiant d’attente, dans l’attente de l’inscription au répertoire national d’identification des personnes physiques. |
| NIR | Numéro d'inscription au répertoire national d'identification des personnes physiques. Il est délivré par l'INSEE et sert d'identifiant de la carte Vitale. (C'est le n° de Sécurité sociale). |
| Opt-out | « Option de retrait » (si l’utisateur n’a pas dit non, c’est oui). Pour MES : pas d’opposition d’un usager à la création de « Mon espace santé » implique la création. |
| Ordonnance numérique | Prescription électronique (médicaments et autres prescriptions à venir dans le cadre du plan Ma Santé 2022) |
| OTP | One-Time Password ou solution d'authentification utilisant des mots de passe à usage unique. |
| PAQ | Plan d’Assurance Qualité |
| PAS | Plan d’Assurance Sécurité |
| PDMA | Perte de Données Maximale Admissible |
| PGC | Plan de Gestion de Crise |
| PI | Product Increment |
| PMF | Poste Multi-Fonctions: Il constitue l'outil de travail sécurisé et standardisé qui autorise l'accès à l'ensemble des données et des ressources applicatives de l’Assurance Maladie. |
| PQGE | Plan Qualité de Gestion des Evolutions fait partie du PAQ et décrit le plan qualité autour des projets évolutifs |
| PQGS | Plan Qualité de Gestion des Services fait partie du PAQ et décrit le plan qualité autour des services assurant le maintien de la production |
| PQM | Plan Qualité Marché fait partie du PAQ et décrit le plan qualité applicable sur tout le périmètre de l’accord-cadre |
| PR | Plan de Réversibilité |
| Programme MESDMP | Organisation projet (Cnam avec le Titulaire) permettant de suivre et gérer l’ensemble du périmètre MESDMP |
| PS | Professionnel de Santé |
| PSE | Prestation Supplémentaire Eventuelle |
| Pseudonymisation | La pseudonymisation est une technique qui consiste à remplacer un identifiant (ou plus généralement des données à caractère personnel) par un pseudonyme. Cette technique permet la ré-identification ou l’étude de corrélations en cas de besoin particulier. |
| PV | Procès-Verbal |
| Régression | Une régression est une erreur introduite à la suite de la correction d'un Incident ou d’une Anomalie, d'une mise à jour logicielle ou technique, de l'ajout d'une nouvelle fonction ou de toute modification apportée. |
| RGAA | Référentiel général d'accessibilité pour les administrations |
| RGPD | Règlement général sur la protection des données |
| SNACS | Services Numériques d’Appui à la Coordination des Soins |
| SAML V2 | « Security assertion markup language » : Standard informatique définissant un protocole pour échanger des informations liées à la sécurité |
| SDM | Service Delivery Manager |
| SEO | « Search Engine Optimization » ou référencement naturel |
| SLA | Service Level Agreement |
| SSO | Single Sign On |
| Titulaire du compte MES | Personne « propriétaire » d’un compte Mon Espace Santé |
| TSM | Tower Service Manager |
| UGECAM | Union pour la gestion des établissements de caisses d'Assurance Maladie |
| UNOCAM | Union nationale des organismes d'Assurance Maladie complémentaire représente, à travers ses membres, tous les opérateurs en Assurance Maladie complémentaire : les mutuelles, les entreprises d'assurances, les institutions de prévoyance et le Régime local d'Alsace-Moselle. |
| US | User story |
| Usager | Personne « qui utilise » l’Espace Numérique de Santé d’un titulaire. L’usager peut être le titulaire de l’ENS, ou agir « pour compte » du titulaire. Un parent est usager de l’ENS dont son enfant (mineur) est titulaire. |

# Présentation de l’Assurance Maladie et du Numérique en Santé

## Présentation générale de l’Assurance Maladie

### Les missions de l’Assurance Maladie

L’Assurance Maladie protège durablement la santé de chacun – dans sa vie personnelle ou professionnelle – en agissant auprès de tous. C’est sa raison d’être. Concrètement, elle accompagne 60 millions d’assurés tout au long de leur vie, en prenant en charge leurs soins quels que soient leurs ressources, leur situation ou leur état de santé.

Elle garantit ainsi un accès universel aux droits et elle permet l’accès aux soins.

Elle fait également bien plus : elle agit en amont de la maladie et de ses complications, avec une offre de prévention sans cesse enrichie. Dans le milieu professionnel aussi, elle renforce ses dispositifs pour protéger les salariés les plus exposés ou les plus fragiles.

Elle joue par ailleurs un rôle de régulateur du système de santé, cherchant en permanence à concilier la meilleure qualité des soins et le meilleur coût, à travers ses analyses, ses propositions et son action sur le terrain. Pour améliorer l’efficacité du système, elle travaille main dans la main avec les professionnels et les établissements de santé, les entreprises et tous les acteurs concernés.

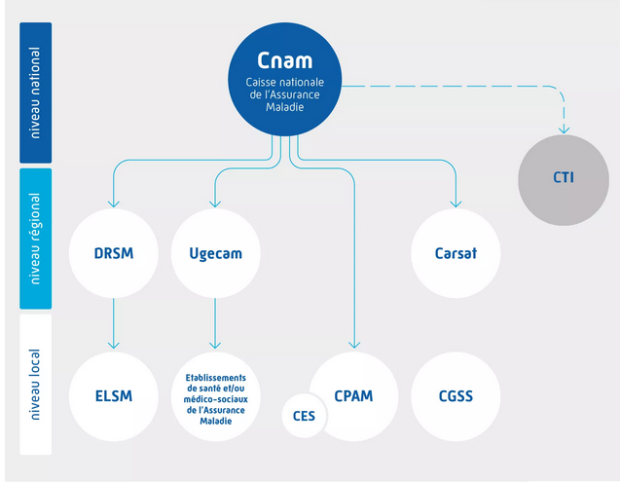
A travers sa branche Risques professionnels, l’Assurance Maladie a pour finalité de promouvoir un environnement de travail plus sûr et plus sain en réduisant les accidents et maladies professionnels. Elle s’appuie pour cela sur la complémentarité de ses 3 missions : indemniser et accompagner toutes les victimes de maladies et d’accidents ; fixer les taux des cotisations accidents du travail/maladies professionnelles des entreprises ; prévenir les accidents professionnels. Pour réaliser ces missions, la branche Risques professionnels s’appuie notamment sur l’expertise de 2 acteurs qu’elle finance, l’Institut national de recherche et de sécurité (INRS) et Eurogip.

Source : <https://assurance-maladie.ameli.fr/qui-sommes-nous/action/missions-generales>

### Le réseau de l’Assurance Maladie

Pour mener à bien ses missions liées à la maladie et aux risques professionnels, l’Assurance Maladie s’appuie sur un réseau étendu, composé de 152 organismes aux fonctions et domaines d’intervention complémentaires.

Le réseau se déploie au niveau national, régional et local, partout en France.



102 caisses primaires d’Assurance Maladie (Cpam) :

Les CPAM sont des organismes de droit privé exerçant une mission de service public. Elles jouent un rôle essentiel pour assurer les relations de proximité avec les publics de l’Assurance Maladie. Parmi leurs nombreuses missions, on trouve :

* + L’affiliation des assurés sociaux et la gestion de leurs droits à l’Assurance Maladie ;
  + Le traitement des feuilles de soins et des prestations d’Assurance Maladie ;
  + Le traitement des demandes de pensions d’invalidité et leur versement ;
  + L’instruction des déclarations d’accident du travail ou de maladies professionnelles - en lien avec le service médical de l’Assurance Maladie – et l’indemnisation des victimes ou de leur ayants-droits ;
  + L’application d’un plan d’action annuel sur la gestion du risque, en relation avec les professionnels de santé ;
  + Le développement d’une politique de prévention et de promotion de la santé. Pour cela, l’Assurance Maladie s’appuie sur un réseau de 89 centres d’examen de santé qui proposent aux assurés des actions de prévention individualisées selon l’âge et les facteurs de risque ;
  + La mise en œuvre d’une politique d'action sanitaire et sociale par des aides individuelles aux assurés - en collaboration avec le service social des caisses d'assurance retraite et de la santé au travail (Carsat) - et des aides collectives au profit d'associations ;
  + L’organisation des visites des délégués de l’Assurance Maladie chez les professionnels de santé ;
  + Le développement d’actions pour prévenir la désinsertion professionnelle à travers des cellules pluridisciplinaires regroupant les compétences des différents organismes (CPAM, Carsat, ELSM/DRSM) : service social, médical, prestations, etc.

16 caisses régionales (Carsat et Cramif) :

Les Carsat (caisses régionales d’assurance retraite et de la santé au travail), et la Cramif (caisse régionale d’Assurance Maladie d’Ile-de-France) sont en charge pour le compte des branches Assurance Maladie et Assurance Maladie – Risques professionnels de 3 missions pour lesquelles elles sont rattachées à la Cnam :

* + La prévention des risques professionnels ;
  + La tarification des risques professionnels ;
  + L’accompagnement des assurés en difficulté (service social)

16 directions régionales du service médical (DRSM) :

Le service du contrôle médical dispose d'un échelon local auprès de chaque caisse d'Assurance Maladie. Il est constitué de praticiens conseils (médecins, chirurgiens-dentistes, pharmaciens) et de personnel administratif. Acteur médical de la gestion du risque, le service du contrôle médical :

* + Conseille les assurés et les professionnels de santé sur la réglementation médico-sociale et sur le bon usage des soins ;
  + Accompagne les assurés et les professionnels de santé pour améliorer la prise en charge des affections de longue durée (ALD) ;
  + Analyse et contrôle les demandes de prestations des patients et les activités des professionnels et établissements de santé ;
  + Contrôle la bonne application de la réglementation et des pratiques médicales ;
  + Réalise des études ;
  + Participe à la reconnaissance du caractère professionnel de l’accident ou de la maladie ;
  + Evalue les séquelles suite à un accident ou à une maladie liés au travail à l’aide d’un barème spécifique et fixe le taux d’incapacité permanente qui donne droit à une indemnisation.

4 caisses générales de sécurité sociale (CGSS) et 1 caisse de sécurité sociale (CSS)

Dans les départements d’outre-mer - Martinique, Guadeloupe, Guyane, la Réunion et Mayotte - on ne trouve pas de CPAM mais des caisses générales de sécurité sociale (CGSS) ou caisse de sécurité sociale (CSS) dans le cas de Mayotte. Celles-ci regroupent tous les services de la Sécurité sociale : Assurance Maladie et risques professionnels, mais aussi assurance retraite, recouvrement des cotisations de sécurité sociale et allocations familiales.

13 unions de gestion des établissements de caisse d’Assurance Maladie (Ugecam)

Ces unions régionales gèrent les 225 établissements sanitaires et médico-sociaux de l’Assurance Maladie. Elles le font en conformité avec les dispositifs de planification sanitaire et médico-sociale et les priorités fixées par les Agences régionales de santé (ARS). Elles sont regroupées au sein du Groupe Ugecam, premier opérateur de santé privé à but non lucratif. Celui-ci est expert dans des domaines pointus : grands brûlés, obésité infantile, traumatismes crâniens et orthopédiques, pathologies médullaires, amputations.

9 centres de traitement informatique (CTI) dont 2 sont dédiés à l’hébergement des infrastructures du système d’information de l’Assurance Maladie et 3 centres d'éditique informatique régionale (CEIR)

Répartis sur l’ensemble du territoire, les centres de traitement informatique (CTI) sont chargés du traitement des données informatiques de l’Assurance Maladie. Ils ont été créés dans le but d’informatiser et de régionaliser la gestion des prestations versées aux assurés. Au fil du temps, les évolutions des besoins et de l’informatique les ont amenés à diversifier leurs activités.

## La Cnam

Avec plus de 2 500 salariés, la Caisse Nationale d'Assurance Maladie - Cnam - est la « tête de réseau » opérationnelle du régime d’Assurance Maladie obligatoire en France. Son rôle : impulser la stratégie au niveau national, puis coordonner et appuyer les organismes locaux qui composent son réseau.

La Cnam est un établissement public national à caractère administratif. Elle agit sous la double tutelle du ministère des Solidarités et de la santé et du ministère de l’Économie et des finances. La loi de réforme d'août 2004 a donné à l'Assurance Maladie de nouvelles responsabilités en matière de régulation du système de soins. La Cnam est donc organisée en conséquence avec, comme priorité, la gestion du risque.

### Les missions de la Cnam

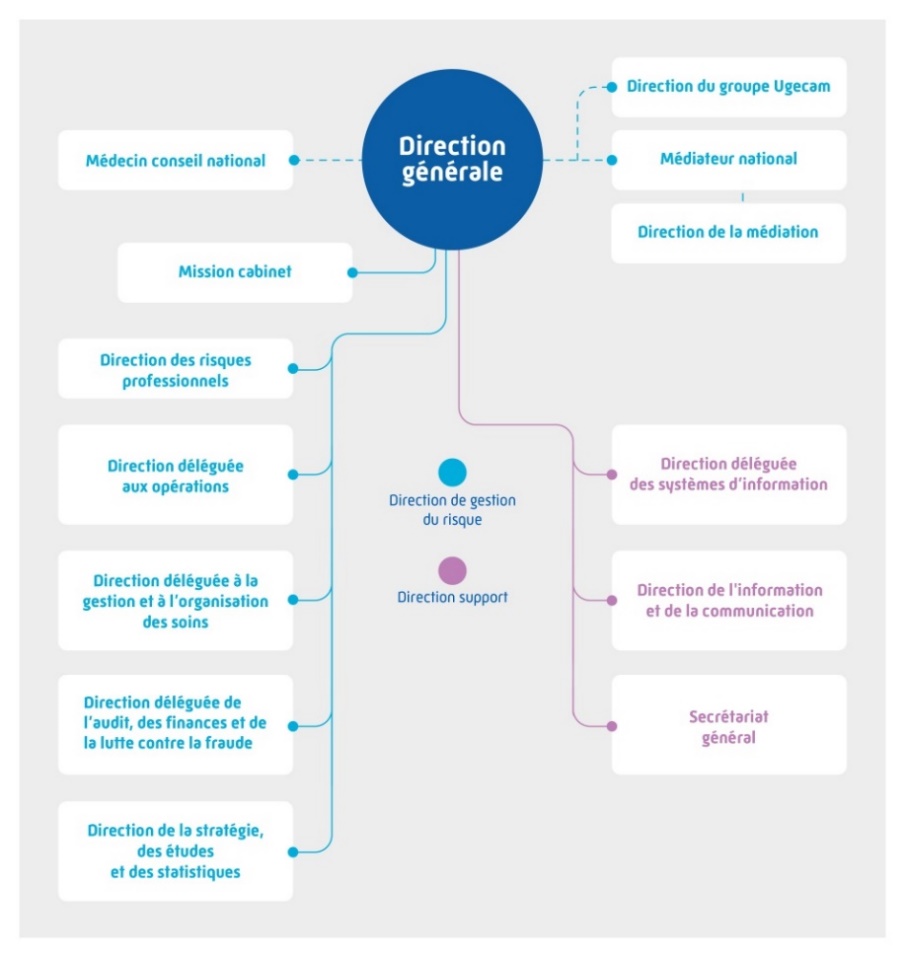
La Cnam :

* + Définit les orientations, les principes et les objectifs qui guident son action et elle en assure la mise en œuvre ;
  + Met en œuvre les accords « conventionnels » passés entre l’Union des caisses d’Assurance Maladie et les syndicats représentatifs des différentes professions de santé ;
  + Développe la maîtrise médicalisée des dépenses de santé et accompagne l’évolution des comportements de chacun ;
  + Définit et promeut la prévention de la maladie, des accidents du travail et des maladies professionnelles ;
  + Définit et pilote l’activité des organismes du réseau ;
  + Veille à ce que le service rendu aux publics soit homogène sur l’ensemble du territoire ;
  + Gère par ailleurs un des plus grands systèmes d’information en Europe…

Pour mener à bien ces missions, la direction générale de la Cnam s’appuie sur plusieurs directions dédiées à la gestion du risque et des directions supports.

Source : [https://assurance-maladie.ameli.fr/qui-sommes-nous/organisation/Cnam-tete-reseau](https://assurance-maladie.ameli.fr/qui-sommes-nous/organisation/cnam-tete-reseau)

### L’organisation de la Cnam



Source : https://assurance-maladie.ameli.fr

## La Direction Déléguée des Systèmes d’Information (DDSI)

La Direction Déléguée des Systèmes d’Information assure la qualité, l'évolutivité, la disponibilité et les performances des systèmes d’information de l’Assurance Maladie dans le respect des besoins de l'ensemble des organismes du réseau de l'Assurance Maladie.

### Les Systèmes d’Information

#### Le Système d’Information de l’Assurance Maladie

* + Plus de 1600 collaborateurs qui œuvrent pour maintenir, développer, assurer la qualité de service et exploiter l’ensemble du SI de l’AM ;
  + De nombreux contributeurs : les maîtrises d’ouvrage, les organismes du réseau et les partenaires ;
  + Une capacité à faire de plus de 274 000 jours / homme Fabrication et charges transverses ;
  + Plus de 500 projets gérés par an ;
  + Environ 480 applications référencées dans la cartographie des systèmes d’information ;
  + Plus de 1900 mises en production par an ;
  + Une capacité de stockage en mode Blocs de 10,8 Po d’utilisé sur 14,4 Po ;
  + Une capacité maximum d’impression de 1 milliard de pages et de 200 millions d’envois par an.

#### Le Système National de Données de Santé (SNDS)

Unique en Europe, voire au monde, le Système National des Données de Santé (SNDS) constitue une avancée considérable pour analyser et améliorer la santé de la population. Géré par la Caisse Nationale de l’Assurance Maladie (Cnam), le SNDS permet de chaîner :

* + Les données de l’Assurance Maladie (base SNIIRAM)
  + Les données des hôpitaux (base PMSI) ;
  + Les causes médicales de décès (base du CépiDC de l’Inserm) ;
  + Les données relatives au handicap (en provenance des MDPH - données de la CNSA) ;
  + Un échantillon de données en provenance des organismes d’Assurance Maladie complémentaire.

Le SNDS a pour finalité la mise disposition de ces données afin de favoriser les études, recherches ou évaluation présentant un caractère d’intérêt public et contribuant à l’une des finalités suivantes : l’information sur la santé, la mise en œuvre des politiques de santé, la connaissance des dépenses de santé, l’information des professionnels et des établissements sur leurs activités, l'innovation dans les domaines de la santé et de la prise en charge médico-sociale, la surveillance, la veille et la sécurité sanitaire.

Source : <https://www.snds.gouv.fr>

L’environnement dédié au SNDS est composé de :

* + 10 bases de données d’une volumétrie totale d’environ 650 Téraoctets (To), dont la base de production du SNDS (de capacité supérieure à 120 To) et 2 bases de restitution du SNDS (de capacité supérieure à 100 To chacune)
  + 230 applications informationnelles dont 60 Briques d’Intérêt Commun.
  + Une capacité de stockage de 2,7 Pétaoctets (Po) soit presque 2 milliards 900 millions de Mégaoctets (Mo)
  + 250 serveurs physiques et 750 serveurs virtuels.

### Les missions de la DDSI

La Direction Déléguée des Systèmes d'Information assure la qualité, l'évolutivité, la disponibilité et les performances de l’informatique de l’Assurance Maladie dans le respect des besoins de l'ensemble des organismes du réseau de l'Assurance Maladie.

A ce titre, elle a pour fonction :

* + D’anticiper l'évolution des besoins des utilisateurs et l'évolution des technologies pour en déduire les évolutions en termes de composants des systèmes, d'évaluation des budgets et de compétences nécessaires,
  + D’organiser les processus métiers de l'informatique dans un souci d'industrialisation et de qualité globale,
  + De mettre en œuvre les dispositifs qui optimisent les moyens dont elle dispose et contribuent au respect de ses engagements,
  + De promouvoir une culture de partage, de savoir-faire et de transparence,
  + De proposer à la direction générale les objectifs et les priorités concernant le système d’information, en accord avec les maîtrises d'ouvrage,
  + D’assurer l'ouverture du SI de l'Assurance Maladie vis-à-vis de l'extérieur en développant des partenariats avec les acteurs du monde de la santé et de la protection sociale, conformément aux objectifs fixés,
  + De s'assurer que l'activité informatique contribue totalement à l'atteinte des objectifs métiers,
  + D’organiser l'amélioration continue de son fonctionnement,
  + D’assurer le reporting de son activité par rapport aux instances de décision de la Cnam,
  + De veiller à la protection des données personnelles au sein de la DDSI.

### L’organisation de la DDSI

Le Directeur délégué est en charge de la DDSI, assisté d’une mission cabinet (CABDDSI).

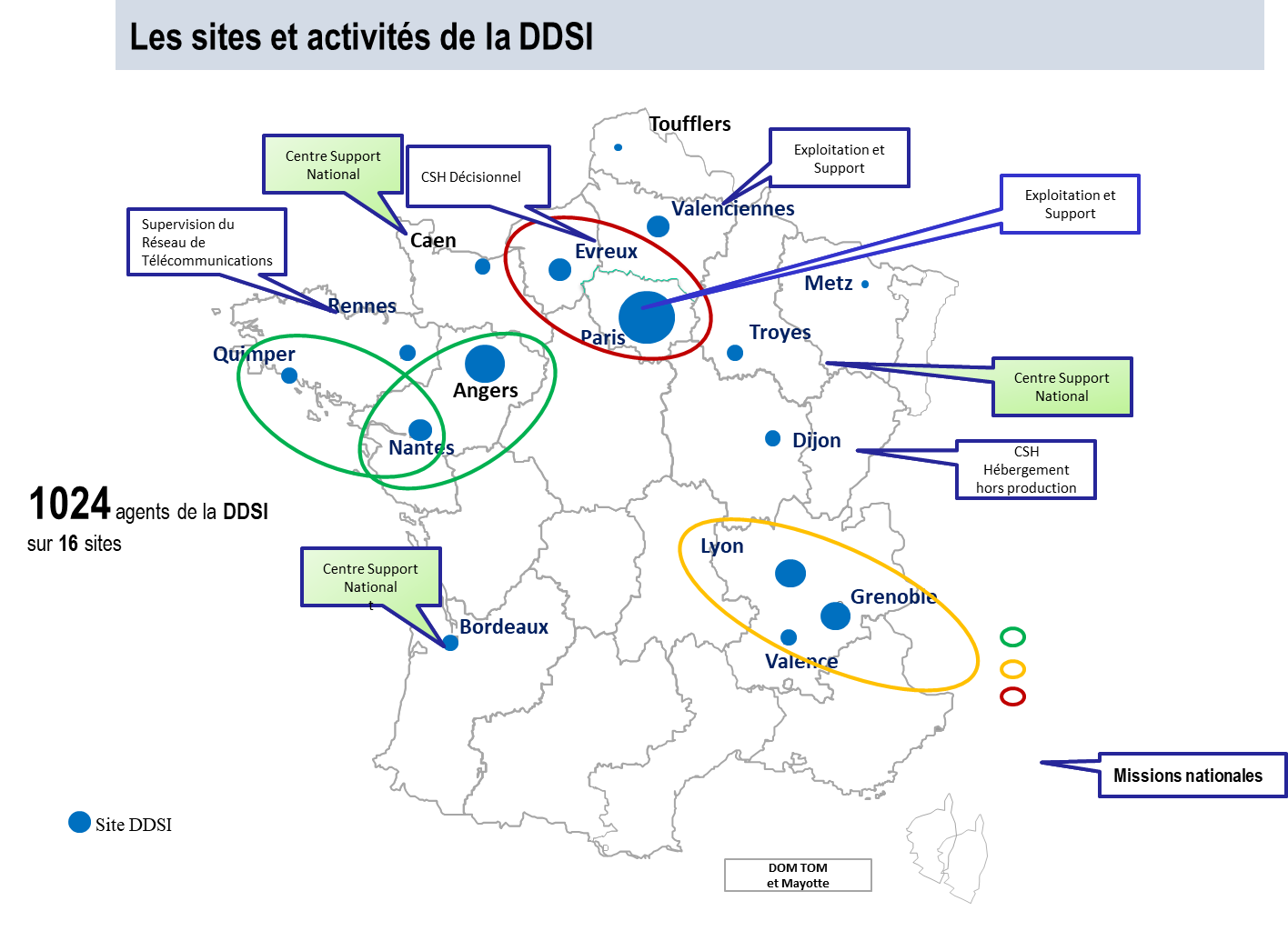
Sont placées sous sa responsabilité :

* + Pour la fabrication des projets et des produits, trois directions de pôle : Paris-Val-de-Seine (DPVS), Ouest (DPO), Rhône-Alpes (DPRA)
  + Pour la cohérence de la stratégie, la Direction du pilotage et des fonctions transverses (DPFT) et la Direction de la stratégie des ressources et des moyens (DSRM)
  + Pour les opérations du système d’information, la Direction des opérations et du service clients (DOSC) et la Direction technique et sécurité (DTS)

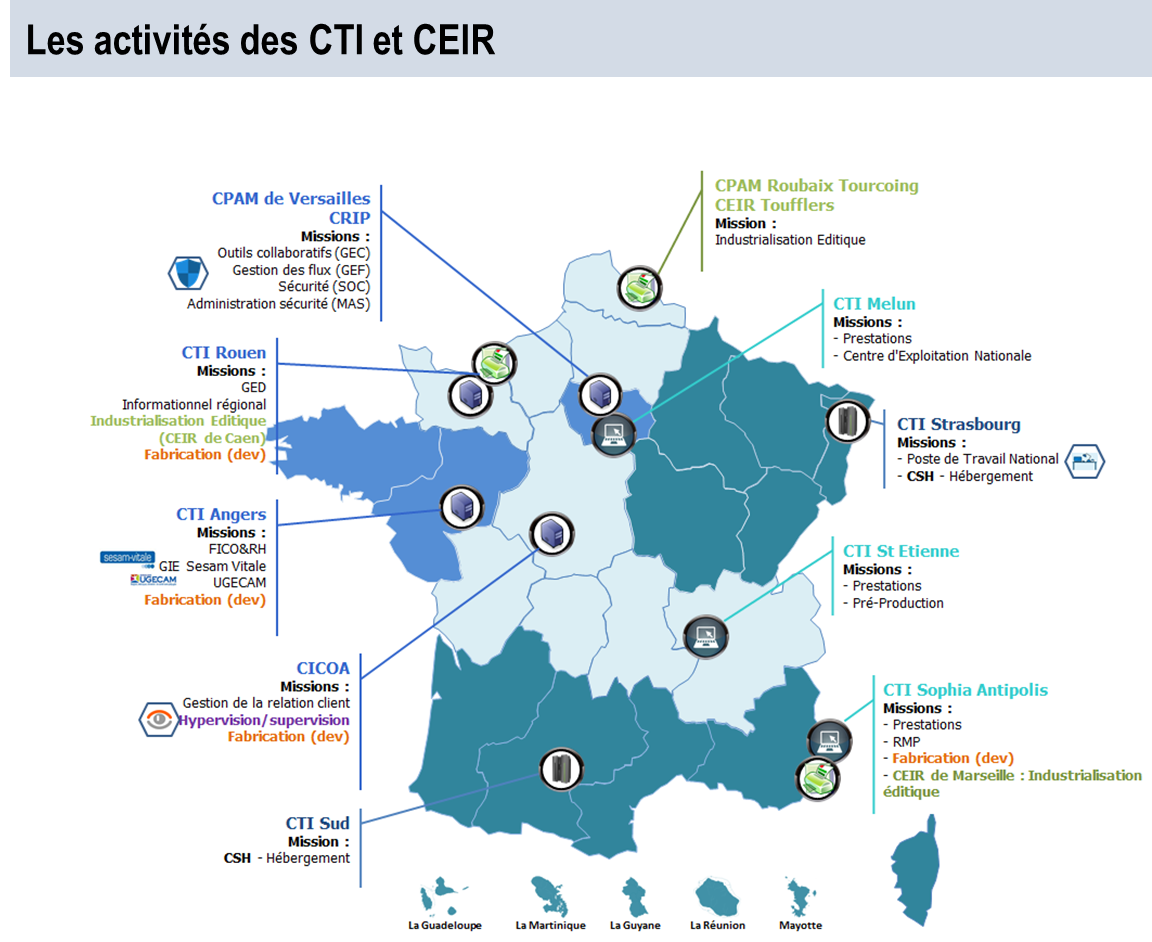
### Présentation géographique de l’organisation DDSI et des CTI-CEIR[[1]](#footnote-2).

La DDSI est implantée sur le siège à Paris et sur 16 sites dont le site de Quimper créé en 2020.

La carte ci-dessous présente les activités associées aux 16 sites.



Répartition géographique des Pôles de fabrication et des centres nationaux spécialisés associés à la DDSI.



## La Direction déléguée à la gestion et à l’organisation des soins

La Direction Déléguée à la Gestion et à l’Organisation des Soins (DDGOS) est responsable de la conception de la politique de gestion du risque de la Cnam tant au niveau des assurés que de l'offre de soins.

A ce titre elle :

* + Elabore les politiques et les plans d’actions liés aux orientations en matière de gestion du risque,
  + S’assure auprès de la direction déléguée aux opérations (DDO) de la déclinaison dans le réseau des plans d’actions ; conçoit les outils nécessaires au respect des objectifs de gestion du risque ;
  + Gère les relations avec les professions de santé libérales et les fédérations représentatives des établissements hospitaliers, assure la conduite des négociations conventionnelles avec ces professions de santé ainsi que la gestion et le suivi des accords conventionnels ;
  + Gère les relations entre l’UNCAM et l’UNOCAM en lien avec les autres directions de la Cnam ;
  + Coordonne au sein de la Cnam les relations avec les organismes complémentaires sur les questions réglementaires, en lien étroit avec la DDO qui gère l’opérationnalité ;
  + Veille à la protection des données personnelles au sein de la DDGOS.

Ses domaines d'actions principaux sont :

* + Développer la prévention et l’information de l’assuré,
  + Lutter contre les inégalités en matière de santé,
  + Favoriser la formation et l’information professionnelle et le développement de la qualité des soins,
  + Participer à la gestion du périmètre de la prise en charge collective,
  + Participer à la régulation de la constitution de l'offre de soins,
  + Utiliser la tarification pour favoriser les processus de soins les plus efficaces et la prévention.

La DDGOS a pour fonction de prendre les décisions, arbitrer ou préparer les arbitrages de la direction générale sur l’ensemble des projets sur la base des analyses et des évaluations des politiques et actions de gestion du risque mises en œuvre.

A ce titre elle :

* + Mesure et évalue les résultats de ses actions afin de les corriger si nécessaire,
  + Conseille la direction générale sur les politiques et plans de gestion du risque,
  + Propose des outils stratégiques sur l’organisation de l’offre de soins et fait évoluer le comportement des acteurs en lien avec la Direction de la stratégie, des études et des statistiques (DSES),
  + Joue un rôle d'expert pour la direction générale et les autres directions sur l'évolution de la réglementation dans le domaine du droit de la sécurité sociale et de la santé publique,
  + Assure la coordination sur les budgets et les plans d'actions de l'ensemble des directions, services, départements et missions rattachés et veille à la bonne intégration des activités des directions dans l’organisation générale des travaux de la Cnam,
  + Définit les besoins fonctionnels des SI de l’Assurance Maladie dans son champ d'activité et s'assure de leur mise en œuvre,
  + Assure le reporting à la direction générale sur les activités de l'ensemble de sa direction.

La DDGOS est composée d’une mission, quatre directions et deux départements :

* + La mission cabinet de la Direction déléguée à la gestion et à l’organisation des soins (CABDDGOS),
  + La Direction des assurés (DAS),
  + La Direction de l'offre de soins (DOS),
  + La Direction opérationnelle du numérique et de l’innovation en santé (DIONIS),
  + La Direction des services de la maîtrise d’ouvrage informatique (DSMOI),
  + Le Département de la réglementation (DREGL),
  + Le Département de l'évaluation et du marketing (DEM).

### Direction opérationnelle du numérique et de l’innovation en santé (DIONIS)

#### Missions de DIONIS

La Direction opérationnelle du numérique et de l’innovation santé est chargée de piloter la mise en œuvre opérationnelle de l’espace numérique de santé (ENS) et du bouquet de services aux professionnels de santé. À ce titre, elle a pour principales missions de :

* + Garantir la mise en œuvre de l’espace numérique en santé pour les usagers et du bouquet des services pour les professionnels de santé en mettant les utilisateurs au centre des travaux de conception ;
  + Déployer et enrichir :
* Le dossier médical partagé (DMP), l’INS et la messagerie sécurisée de santé (MSS),
* Les téléservices de l’Assurance Maladie destinés aux professionnels de santé dont la e-prescription,
* Garantir la cohérence et l’articulation des services existants avec l’espace numérique en santé et le bouquet de services,
  + Mettre en œuvre des actions d’accompagnement auprès des différents publics (patients, professionnels, organismes, éditeurs et industriels) afin d’accélérer le déploiement des différents produits proposés, d’en améliorer l’usage, en s’appuyant sur les organismes d’Assurance Maladie ;
  + Contribuer aux différents chantiers de la feuille de route numérique de Ma santé 2022 et à leur suivi ;
  + Suivre les activités du GIE-SIPS, notamment la base de médicaments Thesorimed en lien avec la e-prescription.

#### Composition de DIONIS

La DIONIS est composée de 4 départements :

* + Le département transverse d’animation et d’appui aux projets (DTAAP),
  + Le département de la maîtrise d’ouvrage de l’espace numérique de santé et du dossier médical partagé (DENSDMP),
  + Le département de la maîtrise d’ouvrage du bouquet de services aux professionnels de santé (DBSP),
  + Le département de la maîtrise d’œuvre d’appui aux projets (DMOE).

## Présentation du contexte du Numérique en Santé

La [feuille de route](https://esante.gouv.fr/actualites/lancement-de-la-feuille-de-route-du-numerique-en-sante-2023-2027) « Mettre le numérique au service de la santé », lancée le 17 mai 2023 par les ministres en charge de la santé et des solidarités, présente les priorités collectives pour les cinq prochaines années :

* **Axe 1 – Développer la prévention et rendre chacun acteur de sa santé.** Cet axe porte notamment des ambitions sur Mon espace santé (prévention personnalisée, carnet de santé de l’enfant, délégation à un aidant, meilleure définition par le patient de ses préférences sur ses données de santé, etc.).
* **Axe 2 – Redonner du temps aux professionnels de santé et améliorer la prise en charge des personnes grâce au numérique**. Cet qui porte notamment des engagements autour de l’accessibilité aux données de Mon espace santé pour les professionnels, et sur le bouquet de service aux professionnels (BSP) à la fois comme portail web et comme interfaces intégrées à leurs logiciels.
* Axe 3 – Améliorer l’accès à la santé pour les personnes et les professionnels qui les orientent ;
* **Axe 4 – Déployer un cadre propice pour le développement des usages et de l’innovation numérique en santé.** Cet axe inclut notamment des priorités sur la cybersécurité, la régulation des services numériques ainsi que l’attractivité de la santé pour les talents du numérique.

Son pilotage stratégique est assuré par la Délégation Ministérielle du numérique en santé « DNS », rattachée au ministres chargés de la santé, de l’action sociale et de la sécurité sociale.

La Cnam est partie prenante de la mise en œuvre de cette feuille de route et assure en particulier le pilotage opérationnel de Mon Espace Santé (MES). Elle est également en charge du DMP, de l’INS, de l’ordonnance numérique et du bouquet de services aux professionnels de santé (BSP).

**Mon espace santé** est fondé sur l’article 45 de la loi n°2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, dite loi OTSS, qui, en son sein le Dossier Médical (sur la base du Dossier Médical Partagé – DMP, la messagerie citoyenne pour échanger avec les professionnels de santé de manière sécurisée (sur la base de la MSSanté), l’agenda et le catalogue de services tiers référencés par la puissance publique.

Ce carnet de santé électronique des citoyens est une plateforme sécurisée, déployée à l'échelle nationale, centrée sur la gestion par les assurés de leur santé et de leurs données. Les services qui y sont proposés offrent notamment la possibilité d’accéder à une vision consolidée de toutes ses données de santé et d’interagir avec l’ensemble des acteurs de santé impliqués dans son parcours de soins (professionnels de santé et du médico-social, offreurs de solutions numériques de santé et de bien-être).

La conception de Mon espace santé a ainsi permis de porter une vision innovante du numérique en santé tout en capitalisant sur l'expérience DMP et en accélérant le déploiement des services numériques socles (Identité Nationale de Santé, Pro Santé Connect, DMP, messagerie sécurisée de santé) qui lui sont directement liés.

En miroir, sur des ressources techniques communes, le bouquet de services aux professionnels (BSP) permet aux professionnels d’alimenter et de consulter les données des patients qu’ils prennent en charge, par des interfaces depuis leurs logiciels, ainsi que par un portail web lorsque c’est nécessaire.

Le programme « Ségur Numérique », accompagne les professionnels et structures, ainsi que des entreprises du numérique en santé qui les équipent, dans cette démarche, avec des incitations financières. Les Agences Régionales de Santé (ARS), le réseau de l’Assurance Maladie et les Groupements Régionaux d’Appui au Développement de la e-Santé (GRADeS) concourent au déploiement sur le « dernier kilomètre ».



En particulier :

* + Les services socles d’identité permettent l’identification et l’authentification des usagers et des professionnels des secteurs sanitaire, médico-social et social.
  + Les règles sur l’interopérabilité, la sécurité et l’éthique sont respectivement regroupées dans trois cadres : CI-SIS, PGSSI-S, CENS ;
  + Les services socles d’échange (DMP, MSSanté, Ordonnance numérique, etc.) permettent des échanges standardisés et sécurisés, en toute confiance.

# Présentation de l’existant : MES et DMP

Le dispositif contractuel, dénommé MESDMP de manière simplifiée, recouvre :

* + L’ensemble des éléments constitutifs des produits DMP et Mon espace santé (Ressources, services, interfaces internes et externes, IHMs, sous-produits, etc.)
  + Les élements nécessaires à l’ouverture des ressources Mon espace santé pour les besoins du BSP.

## Présentation du périmètre existant MES

### Présentation du périmètre fonctionnel MES

Mon espace santé est un produit à part entière dont le maintien et l'évolution relève du présent accord-cadre.. A contrario, le bouquet de services aux professionnels de santé doit être vu comme un concept, et non pas un produit à part entière, constitué de services proposés aux professionnels de santé et du médico-social via différents moyens aux usagers concernés (IHM Web, API utilisées par des éditeurs tiers de services), cohabitant avec d’autres services conçus, développés, exploités par ailleurs, entre autre par la Cnam.

Ci-dessous une présentation macro des fonctionnalités existantes des produits et services constitutifs du périmètre de l’accord-cadre à la date de la rédaction du présent CCTP, puis une projection des évolutions fonctionnelles pressenties pour le système dans son ensemble.

### Existant Mon Espace Santé et ses sous-produits

Mon espace santé est un produit déployé sur le terrain depuis juillet 2021 (pilote sur 3 caisses), ayant fait l’objet d’un opt-out à hauteur de l’ensemble de la population (de janvier à août 2022).

Les quatre fonctionnalités principales de Mon espace santé prévues dans la loi OTSS, à savoir le Dossier médical, la messagerie sécurisée de santé et le catalogue de services, sont disponibles pour les usagers. L’agenda sera mis en place en 2023 et est intégré dans le marché. Elles ont été mise en œuvre en première intention sous forme de MVP (minimum viable product). Elles ont ensuite été améliorées au gré des versions successives de Mon Espace Santé. Ces fonctionnalités principales sont complétées par des fonctions transverses, comme l’activation du compte d’accès de l’usager, la connexion par divers moyens, la gestion des paramètres du compte, des traces, des consentements, des notifications associées aux évènements et un centre de notification, les mentions légales, la FAQ, un service de demande de support, le profil médical agrégat de divers ressources de données de santé, etc.

Les usagers de Mon espace santé relèvent de 2 catégories :

* + Les usagers ayant fait l’objet de l’opération d’opt-out, ne s’étant pas opposé à la création de leur Mon espace santé, mais n’ayant pas à date créé leur compte d’accès (également appelé profil d’accès). Ils sont, à la date de rédaction du présent CCTP, 66 millions. Cette part des usagers continue à croitre à hauteur des créations de Mon Espace Santé au fil de l’eau, soit 4.000 par jour, pour les nouveaux nés et les citoyens nouvellement arrivés sur le territoire et relavant d’un régime obligatoire de sécurité sociale. Les professionnels de santé peuvent interagir via leurs logiciels avec ces Mon espace santé, sur les composantes DMP (Documents) et Messagerie sécurisée de santé.
  + Les usagers ayant activé leur compte d’accès à Mon espace sante. Ils sont, à la date de rédaction du présent CCTP, 8,6 millions.

Une part de la population, faute d’avoir pu être contactée (sans coordonnées de contact, sans identifiant national de santé, pli ou mail d’information envoyé mais non distribué, autres situations particulières), et n’ayant pu de fait exprimer son opposition, ne dispose pas de Mon espace santé créé de manière automatique, mais peut néanmoins, sous réserve de remplir les prérequis, activer de manière autonome leur Mon espace santé via l’interface web du service.

A mai 2023, la répartition entre ces populations est la suivante :

|  |  |
| --- | --- |
| Part de MES/DMP accessibles par les professionnels de santé | 93% |
| Dont Part de comptes activés (sur 100%) | 12.4% |
| Part de comptes fermés ou opposés | 1.9% |
| Part de personnes non contactées | 5% |

Les versions Web et applications mobiles de Mon espace santé sont régulièrement mises à jour avec de nouvelles fonctionnalités répondant à des cas d’usages orchestrant les fonctionnalités de base. Ces cas d’usages font écho à l’objectif de proposer aux usagers des outils de prise en main de leur santé et de simplification de leurs échanges avec leurs professionnels de soins, dans un environnement sécurisé.

Dans la mesure du possible, les fonctionnalités de Mon espace santé sont proposées dans les 2 modalités (Web et Mobile), dans un temps proche, si ce n’est concomitant. Les fonctionnalités Mobile sont par ailleurs complétées pour répondre à des cas d’usages spécifiques aux contextes d’utilisation des smartphones, en mobilité.

Les usagers retrouvent Mon espace santé :

* + En version web (responsive) : [www.monespacesante.fr](http://www.monespacesante.fr)
  + En versions mobile :
* Sous Android :

<https://play.google.com/store/apps/details?id=fr.assurancemaladie.monespacesante&hl=fr_FR&showAllReviews=true&pli=1>

* Sous Apple :

<https://apps.apple.com/fr/app/mon-espace-sant%C3%A9/id1589255019>

### Mon Espace Santé

#### Principes généraux

##### Support utilisé (web ou mobile)

Quel que soit le support utilisé (web ou mobile), l’usager de Mon espace santé bénéficie d’un service public souverain, de qualité et de confiance, s’appuyant sur les grands principes suivants :

* + Une plateforme accessible à tous (site grand public) et hautement disponible.
* Un service rendu partout en France (Métropole et DROM) incluant les zones blanches ou à connexion limitée.
  + Des services conçus, hébergés et exploités dans un contexte souverain, dans le respect du RGPD (excluant notamment le transfert de données hors UE), en conformité avec la doctrine du numérique en santé, en particulier avec le Cadre d’interopérabilité des systèmes d’information de santé (CI SIS) et les directives de sécurisation des systèmes d’information de santé en vigueur (PGSSIS).
* <https://esante.gouv.fr/strategie-nationale/doctrine>
* <https://esante.gouv.fr/produits-services/ci-sis>
* <https://esante.gouv.fr/produits-services/pgssi-s>
  + Une navigation simple conçue dans les règles de l’art UX/UI (compréhensible, intuitive), rapide (performante, résiliente) et fluide. La conception de Mon espace assure une expérience utilisateur de qualité à toutes les étapes du parcours de l’usager.
* Mon espace santé propose une navigation similaire quel que soit le système d’exploitation utilisé. L’affichage est responsive et s’adapte aux différents écrans (smartphone, tablettes, desktop, etc.).
* Mon espace santé est conçu de manière itérative, sur la base d’observations des besoins, d’analyse des mesures d’usages et retours terrains : enquêtes et retours utilisateurs, tests de maquettes lors des cadrages de conception, mobilisation de la communauté pour projection sur de nouveaux cas d’usages, analyse de données analytics collectées, le tout contribuant à l’enrichissement de Persona utilisateurs de Mon espace santé permettant au fur et à mesure d’affiner la segmentation des usagers afin de répondre de manière de plus en plus précise à leurs besoins.
  + Des parcours utilisateurs répondant aux exigences du RGAA
* Le niveau minimum de conformité des IHM aux exigences du RGAA est fixé au niveau du meilleur coefficient d’accessibilité obtenu dans le cadre d’audit menés annuellement par un cabinet externe, mandaté par la Cnam. En mai 2023, le coefficient d’accessibilité de Mon espace santé est de 75% (RGAA 4.1).

<https://design.numerique.gouv.fr/accessibilite-numerique/rgaa/>

* + Une conception écoresponsable, répondant aux exigence de l’éco-score santé
* Le niveau minimum de l’écoscore de Mon espace santé est fixé au meilleur coefficient obtenu dans le cadre d’une évaluation annuelle. En mai 2023, le coefficient d’écoscore de Mon espace santé est de 75%.

<https://ecoscore-appli.esante.gouv.fr/>

* + Des services adaptés à la très large majorité du parc (desktop et mobile, OS et navigateurs) français, néanmoins dans le respect des niveaux de sécurité requis.
  + Le niveau de compatibilité est défini et revu régulièrement en fonction de l’évolution des recommandations constructeurs et éditeurs pour satisfaire aux exigences de sécurité de Mon espace santé et de compatibilité avec les outils de conception de Mon espace santé.
  + Des services s’appuyant sur les fonctionnalités natives du support sur lequel il est utilisé (ex. : géolocalisation, appareil photo, lecteurs biométriques d’identité, etc.) et sur les innovations technologiques venant régulièrement compléter l’état de l’art dans le domaine des services numériques (IoT via le catalogue des applications).
  + Des interfaces utilisateurs qui bénéficient du Design System « Mon Espace Santé » pour homogénéiser et accélérer le développement et la validation des pages :
* Un référentiel design, qui référence les composants utilisables et les règles applicables au design : règles d’usage, utilisation de la charte graphique (couleurs, illustrations, icônes, comportement, etc.)
* Un ensemble de composants « sur étagère » qui facilitent la mise en place de contrôles, d’auto complétion, de balises d’accessibilité, etc.
  + Des services garantissant la transparence sur les traitements opérés (traces des opérations, transparence sur les algorithmes de personnalisation, etc.)
  + Des services sécurisés à l’état de l’art.

##### Utilisation des personas

Afin de mieux identifier les besoins des Français, des personas ont été créés pour avoir une meilleure connaissance des critères de recrutement des utilisateurs.

Trois sources de données ont été identifiées pour segmenter les personas :

* + Apprentissages utilisateurs : des entretiens exploratoires et tests utilisateurs ont été effectués ;
  + Statistiques assurés : une segmentation des assurés de l'Assurance Maladie ;
  + Statistique population : des statistiques de la population française ont été effectuées.

Les données recueillies sont les suivantes :

* + Age
  + Sexe (sur l’Etat civil)
  + Fracture numérique
  + Revenu moyen
  + Facilité de faire des démarches administratives sur internet
  + Présence de maladies chroniques
  + Aidants
  + Parentalité

À la suite de l’étude de ces données, trois personas ont été créés [Voir Annexe « MESDMP\_Annexe 01 – Personas » :

* + Martine est une femme de 62 ans. Elle consomme beaucoup de soins (elle souffre d’une maladie chronique) et est proactive sur sa santé. Elle aide sa mère de 85 ans. Elle encourage ses Professionnels de Santé à mettre ses documents dans Mon Espace Santé (via le DMP) après une consultation, auto-alimente son compte MES et facilite une meilleure coordination des soins, entre autre pour une meilleure articulation ville-hôpital.
  + Inaya est une femme de 33 ans. Elle consomme des soins (mariée, elle a un enfant de 3 ans et est actuellement enceinte). Elle est experte concernant les démarches en ligne, elle anticipe ses RDV familiaux et retrouve facilement ses analyses (ce qui évite la prescription d’analyses et d’examens en double).
  + Amir est un homme de 45 ans. Il consomme peu de soins, est divorcé et a un enfant de 14 ans. Il rencontre des difficultés pour faire ses recherches administratives. Il a un compte MES ouvert mais ne l’utilise pas directement. En revanche, ses PS l’utilisent pour communiquer entre eux.

Ces personas sont essentiels à la conception des parcours utilisateurs de Mon espace santé. Ils permettent de conjuguer l’exigence de proposer des parcours répondant à des profils particuliers d’utilisateurs, mis en situation, tout en gardant pour cap l’universalité de Mon espace santé.

Les paragraphes ci-après ont pour objectif de décrire les caractéristiques majeures de ces services et des briques fonctionnelles qui les sous-tendent.

#### Pilotage par la donnée

Le Pilotage par la donnée de MES a pour objectif principal de suivre les usages des utilisateurs afin d’améliorer le produit pour qu’il réponde au mieux aux attentes de ces derniers. Pour répondre à ce besoin, deux outils de pilotage sont utilisés : Knowage et AT internet. Ce pilotage s’appuie principalement sur l’outil Knowage, logiciel d’analyse de données, qui nécessite de nombreuses actions manuelles pour obtenir les résultats escomptés et mener un pilotage fin.

En complément de ces outils de pilotage, une infographie hebdomadaire est produite pour suivre de près les indicateurs clés. Tous ces outils sont exploités par l’équipe Usages en lien avec les équipes de Mon Espace Santé.

##### Présentation de l’outil de Pilotage à froid Knowage

L’équipe « Usages » est en charge de développer les indicateurs sur l’outil Knowage. Cette équipe peut s’appuyer sur la Direction Produit et Design (DPD) et les *feature teams* pour recueillir les nouveaux besoins d’indicateurs. Une fois les demandes instruites, les modalités de récupération des données précisées, développées, le tout est exploité via dans une architecture BI en backoffice puis en front office sur l’outil Knowage.

Sur Knowage, sont déjà présents certains tableaux de bord de suivi des usages suivants sur différents pans fonctionnels :

* + Des tableaux de bord sur l’enrôlement où figurent des données sur les activations, les comptes d’accès mais aussi sur la répartition des usagers selon leur régime, caisse et centre de rattachement ;
  + Des tableaux de bord de suivi des usages des fonctionnalités « Documents », « Profil médical » (en particulier les mesures) et « Messagerie » ;
  + Un tableau de bord de suivi du nombre et du type de notifications envoyées aux usagers de Mon espace santé ;
  + D’autres tableaux de bord relatifs au catalogue de services, etc.

Ces tableaux de bord sont actualisés en fonction de la mise à disposition des données sources, en majorité à J+1.

##### Pilotage à froid de l'activité du Support de Mon espace santé

Le Pilotage à froid de l'activité du Support comprend les données des sollicitations téléphoniques ainsi que les données relatives aux formulaires de contact. La cellule statistique de DIONIS est en charge de récupérer les données provenant d’ODIGO, solution de centre de contact (GRC), pour les sollicitations téléphoniques et les données de l’outil de suivi des demandes de support de Mon Espace Santé (PSN1) pour les formulaires.

A partir de ces données, un tableau de bord de pilotage Excel est produit 2 fois par semaine par la Cnam. Ce tableau de bord permet de suivre l'évolution des appels au Support, des envois de formulaire, des motifs de sollicitation ou encore des taux de réponse.

Cette solution « manuelle » a vocation à évoluer vers un outil ad hoc. Il s’agit d’un des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

##### Présentation de l’outil de Webanalytics AT internet

AT internet est un outil de Webanalytics permettant de suivre les habitudes de navigation des utilisateurs sur le site web et l’application mobile. Il incombe aux équipes de Mon espace santé (équipes du Titulaire mais la possibilité reste ouverte que cette tâche soit transférée en cours d’exécution de l’accord-cadre aux équipes Cnam) de prendre en charge l’intégration des Tags au sein des pages web et mobile afin de traquer des actions précises. Un plan de taggage sur les différentes pages web MES permet de suivre les usages de façon continue sur AT internet.

AT internet propose deux manières d’exploiter les données de navigation, à savoir une utilisation des tableaux de bord préexistants et des tableaux de bord construits :

* + Nativement, il est possible d’obtenir des indicateurs sur l’audience du site et de l’application (géolocalisation, trafic général). L’outil permet aussi d’avoir des indicateurs sur les sources, les pages visitées, les appareils utilisés ou encore de réaliser des parcours de navigation.
  + En complément des rapports ont été construits pour suivre au mieux la navigation des utilisateurs sur certains groupes de pages clés : un rapport sur le catalogue de services, un rapport sur la messagerie ou encore sur le profil médical. Ces rapports sont générés par le Titulaire de façon mensuelle et permettent ainsi de suivre les tendances d’usage du site web et de l’application mobile de Mon espace santé.

AT internet est complété par Commanders Act, pour ses fonctionnalités de gestionnaire de Tag et pour ses fonctionnalités en matière de consentement à cookies.

##### Infographie de Mon Espace Santé

En complément des outils de pilotage présentés, une infographie hebdomadaire est produite par le Titulaire pour un suivi précis des indicateurs-clés. Cette infographie a plusieurs sources de données (outil de pilotage et sources manuelles). Elle est envoyée chaque semaine aux sponsors du programme.

L’infographie expose les Faits marquants de la semaine passée, le suivi de l’enrôlement, des téléchargements sur mobile, des données d’usages provenant de l’outil Knowage, des données de navigation provenant de AT internet et une partie relative au Support de Mon espace santé.

#### Tests utilisateurs et Data Desk

Dans le cadre de l’amélioration continue du produit Mon espace santé, des tests utilisateurs sont régulièrement conduits (dans le cadre de chaque incrément trimestriel) par le Titulaire et par la Cnam auprès d’une population d’utilisateurs selectionnée pour représenter au mieux les différents personas de Mon espace santé. Ces tests utilisateurs permettent d’enrichir la connaissance sur le produit et de centrer les développements sur les besoins et points de douleurs identifiés.

Des analyses plus poussées sur certains sujets sont conduites par un Data Desk. Il s’appuie notamment sur les tests utilisateurs ainsi que sur les outils de pilotage afin d’apporter des analyses précises sur certains points saillants, pour lesquels la direction Produit cherche des explications, des pistes d’amélioration. Ces rapports permettent d’orienter les enquêtes sur les besoins de la Direction Produit et Design et de maximiser la valeur ajoutée de chaque développement.

#### Mon Espace Santé WEB et Application Mobile

##### Web

La version Web de Mon espace santé évolue régulièrement à raison d’une version majeure environ tous les 3 mois, complétée par des versions intermédiaires ou correctives qui peuvent aller jusqu’à une fréquence hebdomadaire. Le périmètre fonctionnel du produit est de ce fait en évolution constante. A horizon juillet 2023, au-delà des fonctionnalités de base prévues par la loi OTSS (DMP, messagerie sécurisée, agenda et catalogue de services), le produit est étoffé de fonctionnalités supplémentaires.

Ces fonctionnalités correspondent à :

* + De l’amélioration des fonctionnalités de base, parmi lesquelles on peut citer :
* Connexion via France Connect niveau d’identité eiDAS 1.
* Gestion de la délégation d’accès des parents sur les Mon espace santé des enfants mineurs.
* Customisation de la home-page avec mise en place de Mon actu santé, module destiné à engager l’usager dans la gestion de sa santé grâce à la mise en avant d’informations et propositions d’actions personnalisées.
* Amélioration de l’expérience utilisateur afin qu’il soit, à la connexion, immédiatement guidé vers les évènements nouveaux dans son Mon espace santé grâce au centre de notification.
* Enrichissement de la fonctionnalité de gestion des documents grace à la mise en place de dossiers, gérés à la main du patient.
* Amélioration du carnet de vaccination pour aller vers du conseil et des rappels pour les usagers.
* Amélioration de la présentation de Mon histoire de santé.
* Enrichissement du profil médical avec de nouvelles rubriques comme celle de dépôt de pièces administratives ou une autre relative au handicap.
* Augmentation des rubriques mesures et habitudes de vie.
* Amélioration de la présentation des traces d’accès et des modalités de gestion des autorisations d’accès (blocage, masquage/démasquage de tous les documents en une fois).
* Fonctionnalités de rematérialisation, suppression des Mon espace santé sur demande de l’usager.
* Amélioration de la gestion de contenu proposée sur le service Mon espace santé par la mise en place d’un Content Management System (CMS) permettant de gérer les changements de contenus hors version applicative du produit.
* Optimisation de la présentation des applications référencées dans le catalogue de services.
  + Des parcours utilisateurs particuliers, articulant les fonctionnalités de base :
* Parcours de facilitation de préadmissions grâce à du partage de documents via la messagerie sécurisée.
* Mise en place de liens entre les documents et certaines rubriques du Profil médical.
* Parcours facilité d’envoi d’une ordonnance à une pharmacie disposant d’une boite aux lettres organisationnelle dans le cadre d’un primo échange à l’initiative de l’usager.
* Parcours spécifique pour gérer de manière optimisée le recours au support sur certains cas particuliers : signalement d’un document qui ne concernerait pas l’utilisateur via l’outil de support par mail de Mon espace santé.
* Incitation à l’alimentation du profil médical sur la base d’information remontées par le biais de Mon histoire de santé.
* Récupération de données structurées en CDA issues du DMP pour alimenter des ressources dans un but de présentation améliorée pour les besoins de usagers (courbes de croissances).
* Contribution à la chaîne d’édition de courrier postaux à partir de Mon espace santé.
* Gestion des mésusages potentiels.

Par ailleurs, des orientations transverses sont également développées, comme un parcours de santé de l’enfant sur la base des briques du Carnet de santé de l’enfant, au travers des mesures de santé, de conseils personnalisés aux parents, du carnet de vaccination et de l’alimentation des certificats des examens obligatoires de l’enfant, ou encore les premières briques de parcours de prévention, par le biais d’informations personnalisées, de rappels de vaccins, questionnaires de santé à réaliser par l’usager à l’atteinte de tranches d’âge spécifiques.

Il s’agit ici de partager quelques fonctionnalités proposées dans Mon espace santé, sans prétention de présenter l’exhaustivité ou la granularité la plus fine que recouvrent ces illustrations. A la notification du présent accord-cadre, l’existant fonctionnel de Mon espace santé, devra être repris, et le principe de versions itératives visant à apporter systématiquement une part de valeur supplémentaire au produit devra être reproduit dans un rythme au moins équivalent à celui pratiqué (versions majeurs trimestrielle, patch correction / micro évolutif à la semaine, versions intermédiaires en fonction de la nécessité métier).

Les IHM web sont développées dans le respect des exigences d’accessibilité. A mai 2023, Mon espace santé Web comptabilise un score de 75% (référentiel RGAA, cf. scénarios en annexe « MESDMP\_Annexe 26\_Scénario\_d’audit\_accessibilité »), score qui ne saurait être dégradé dans le cadre des évolutions fonctionnelles apportées au produit. E

Le produit Mon espace santé est développé dans le souci d’une implémentation écoresponsable au sens du référentiel écoscore. A mai 2023, Mon espace santé comptabilise un écoscore de 75 points (cf. scénario en annexe « MESDMP\_Annexe 27\_Scénario écoscore » ), score qui ne saurait être dégradé dans le cadre des évolutions fonctionnelles apportées au produit.

En cas de dégradation d’un des scores précités, le Titulaire met tous les moyens en œuvre, à ses frais, pour revenir, a minima, au score initial considéré, sans que cela n’impacte les chantiers en cours de réalisation, au plus tard le mois suivant la dégradation du score. A défaut, la Cnam peut appliquer les pénalités prévues au CCAP.

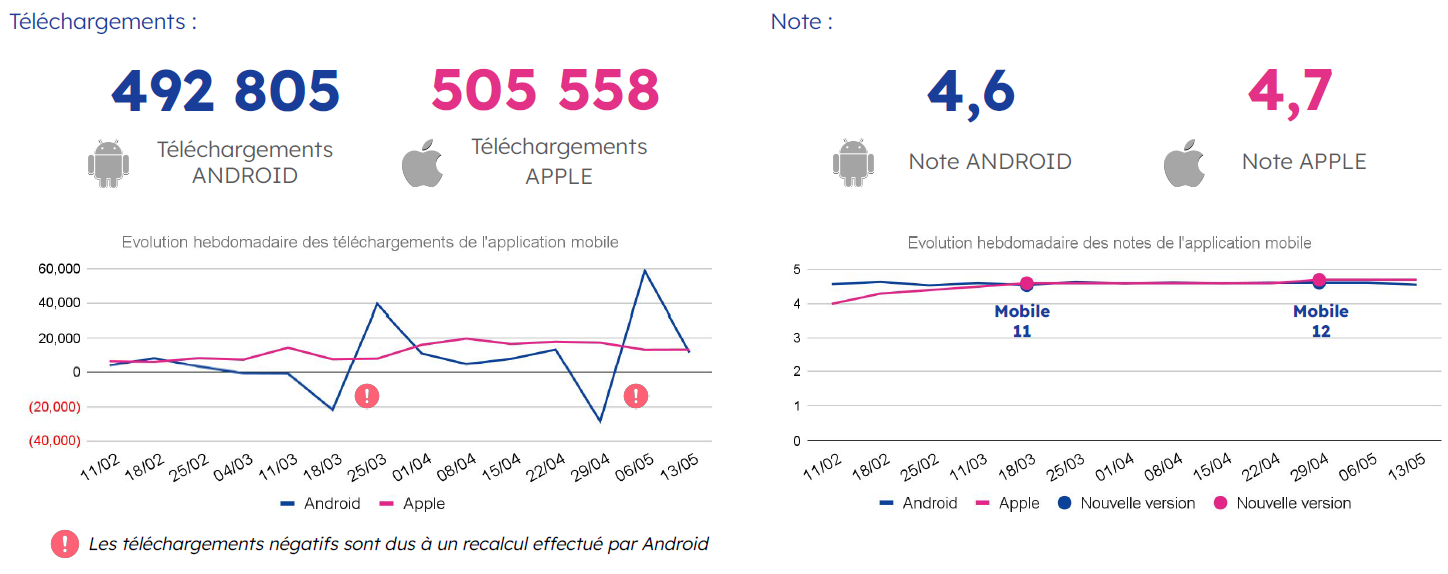
##### Application mobile

La version mobile reprend en très grande majorité les fonctionnalités proposées par la version web. L’objectif affiché d’un point de vue métier est d’offrir à l’usager une expérience utilisateur la plus universelle possible, qui garantisse qu’un utilisateur peut naviguer entre les différents types de device et retrouver néanmoins les mêmes fonctionnalités. Pour les quelques fonctionnalités qui seraient en écart, une incitation à retrouver la fonctionnalité sur le web est faite (malgré une potentielle dégradation de l’expérience utilisateur sur mobile lors du passage en web responsive). Dans la pratique, les ouvertures de services des versions application sont généralement opérées avec un décalage minime, lié d’une part à la nécessaire gestion de la compatibilité de la nouvelle version avec le back commun web et mobile, mais aussi au délai de déploiement sur les stores Apple et Android.

Pour profiter des capacités du mobile, certaines fonctionnalités ne sont disponibles qu’en mobile (ex. : scan de code barre pour faciliter l’obtention d’un vaccin par exemple). L’ergonomie de la version mobile est adaptée au média et peut différer de la version web.

Pour éviter la gestion de trop nombreuses lignes de produits Mon espace santé différentes, l’application mobile correspond à un unique produit (code unique), compilé ensuite pour être déployé sur les 2 plateformes Apple et Android.

L’évaluation des versions mobiles de Mon espace santé sont de 4,6 sur Android et 4,7 sur iOS en mai 2023.

Le niveau de confiance en ces solutions doit être maintenu, voire amélioré, tout au long de l’accord-cadre.

De par sa mise à disposition spécifique et le travail nécessaire pour répondre aux exigences de deux systèmes différents, des spécificités existent pour l’application mobile.

Afin de mener à bien les développements pour les applications mobiles de Mon Espace Santé, une forge spécifique pour mobile est employée (forge pour Android et forge pour Apple). L’application est packagée et déployée sur le store App Distribution afin de permettre de s’assurer de la bonne mise à disposition et suivre les versions des applications.

Le Titulaire garantit le maintien en conditions opérationnelles de l’application mobile sur les versions majeures des OS standard du marché et principaux terminaux (couverture cible de 85% par OS). Ce périmètre étant amené à évoluer (sortie de nouvelles versions d’OS ou de navigateur, obsolescence d’anciennes versions, sortie de nouveau mobile avec nouveau format), le Titulaire doit tenir compte des évolutions des parts de marché des versions des OS, des navigateurs et des mobiles. A mai 2023, les versions minimum pour lesquelles les applications sont disponibles sont Android 8.1 et iOS 13.

Le Titulaire doit donc prévoir que les versions développées et déployées soient compatibles avec ces versions et les versions ultérieures. En cours d’exécution de l’accord-cadre, la version minimale avec laquelle les applications mobiles sont compatibles peut être amenée à évoluer afin de respecter les contraintes de maintenabilité et de sécurité.

La Cnam se charge du déploiement des versions mobiles sur les stores Apple et Android. Cette partie est donc exclue du périmètre de l’accord-cadre.

##### SI Enrôlement et opposition ou activation ou création automatique de Mon Espace Santé

Au moment du déploiement initial de Mon espace santé, en janvier 2022, tous les bénéficiaires français de l’Assurance Maladie obligatoire ont été notifiés de la création à venir de leur espace santé et de leur droit d’opposition. A réception du courrier de notification (mail à 75% ou postal à 25% selon les coordonnées fiabilisées connues de l’Assurance Maladie), les usagers disposaient de 6 semaines pour réagir : procéder à une opposition, procéder à une activation ou ne pas se prononcer. Dans ce dernier cas, passé le délai de 6 semaines, le système composé des SI Enrôlement, SI Mon espace santé et SI DMP procédait à la création automatique des Mon espace santé.

Une création automatique ouvre un espace numérique de santé, contenant entre autres un DMP et une messagerie sécurisée de santé. Les usagers disposent également à l’activation ou à la création automatique de toutes les ressources nécessaires au bon fonctionnement de Mon espace santé à date. Les créations automatiques présentent l’avantage de rendre disponible, pour la grande majorité des patients, un DMP et une messagerie sécurisée, permettant aux professionnels de santé d’y déposer des documents ou envoyer des messages à l’usager, avec une probabilité importante de succès. Il s’agit là de l’initialisation d’un cercle vertueux souhaité, où l’implication des professionnels de santé dans la constitution du dossier de santé des patients engage les patients à activer leur Mon espace santé et à prendre en main leur santé. Pour cela, l’usager doit être amené à faire la démarche de créer son compte ou profil d’accès, entre autre par le biais de notifications d’évènements qu’il reçoit sur sa coordonnée connue de l’Assurance Maladie. Pour activer son espace santé, un assuré peut utiliser le code qui lui a été fourni dans sa notification initiale dans un délai de 6 semaines, ou bien en générer un nouveau si le précédent a expiré.

La création d’un Mon espace santé repose sur l’éligibilité d’un usager à en disposer. Les prérequis à cela sont d’une part d’être affilié à un régime d’Assurance Maladie obligatoire français (aujourd’hui, avec un numéro d’enregistrement au registre ou NIR certifié, à terme avec un numéro temporaire dit NIA également), d’autre part de disposer auprès de ce régime d’une carte Vitale et d’une coordonnée de contact fiabilisée. Ces pré-requis sont indispensables à l’authentification multi-facteurs d’un usager au moment où il procède au choix d’opposition ou d’activation de son Mon espace santé.

La Cnam est opérateur de l’enrôlement pour le compte de l’ensemble des régimes d’Assurance Maladie.

Ce n’est donc pas le SI Mon espace santé qui initie la création mais un SI de la Cnam dit SI Enrôlement.

Le SI Enrôlement a pour vocation de notifier les assurés de la possibilité pour eux d’ouvrir un espace santé, contrôler leur identité au moment d’activer MES et déclencher la création automatique de MES pour eux à échéance du délai d’opt-out (6 semaines après émission du courrier).

Pour ce faire, le SI Enrôlement s’appuie sur une base de données intégrant tous les assurés bénéficiaires d’un régime français d’Assurance Maladie, et sur des traitements automatisés (« *batchs* »). Si historiquement le SI Enrôlement a été fortement mobilisé dans le cadre de l’opération d’opt-out à l’échelle de l’ensemble de la population, son activité est aujourd’hui réduite au flux constitué du fil de l’eau des affiliations à un régime d’Assurance Maladie, soit les nouveaux nés, les passages à la majorité et les affiliés nouvellement bénéficiaires de l’Assurance Maladie. Soit un flux journalier d’environ 4000 nouveaux usagers éligibles à qui est soumis, par le SI enrôlement, leur droit d’opposition à Mon espace santé.

La base de données est alimentée par divers référentiels nationaux (SNGI, RNIAM, tous deux opérés par la Cnav, RFI, BDO opérés par la Cnam, ...). Les différents batchs constituant le traitement d’enrôlement permettent de faire évoluer les assurés au sein de la base au fil de différents contrôles, jusqu’à déclencher l’envoi d’une notification de droit d’opposition à Mon espace santé. Cette notification comporte un code temporaire et à usage unique, à utiliser pour compléter l’authentification d’un usager au moment de son utilisation. Une fois la notification parvenue à l’assuré destinataire, ou son représentant légal s’il est mineur, un batch particulier déclenche, dans le cas où un choix d’activation ou d’opposition n’a pas été fait par l’assuré dans les 6 semaines, une demande de création automatique auprès du SI de MES.

Par ailleurs, des webservices gérés par le SI Enrôlement sont mis en action à chaque tentative d’activation de MES par un usager. Des vérifications d’authentification auprès des référentiels d’identité et de la base Vitale (pour vérification du numéro de série de la carte) et du SI Enrôlement lui-même via le contrôle du code temporaire sont alors effectuées afin de valider l’action demandée (activation, opposition). En cas d’arrivée à échéance du code temporaire, l’usager peut, moyennant identification forte, récupérer en ligne un nouveau code temporaire fourni par le SI Enrôlement.

C’est le SI enrôlement qui pilote l’émission des courriers (mail et postaux) en interaction avec le système de communication sortante de la Cnam.

Le SI enrôlement génère les codes temporaires qui sont ensuite envoyés par le système mail/sms du SI Mon espace santé.

Le SI Enrôlement est régulièrement amélioré par une équipe Cnam dédiée à ce sujet, constituée d’une MOA, une MOE et un fabricant. L’exploitation du SI Enrôlement est assurée par le département d’intégration applicative (DIA) de la Cnam.

##### Identification électronique

Une fois l’enrôlement d’un usager fait, ce dernier dispose d’un profil ou compte d’accès à Mon espace santé et de moyens d’identification afférents qui lui permettent de se connecter, puis d’effectuer certaines opérations jugées sensibles, nécessitant une identification et authentification forte.

Pour assurer un accès sécurisé et fiabilisé à l’ensemble des données personnelles et de santé d’un usager, des dispositifs d’identification électronique proposant des niveaux de sécurité adaptés sont mis en place dans le cadre de Mon Espace Santé.

L’usager peut accéder à son compte Mon Espace Santé, via sa page de connexion, selon plusieurs modalités :

* + En utilisant un identifiant/mot de passe (créés au moment de l’enrôlement, seul le mot de passe est modifiable ensuite). Ce moyen d’identification électronique est couplé à une sur-sécurité du type code OTP. L’usager peut réceptionner ce code OTP selon différentes modalités (SMS, courriel).
  + En passant par la mire France Connect, ce qui lui donne la possibilité de choisir le fournisseur d’identité qu’il souhaite utiliser pour s’identifier à son Mon Espace Santé. La solution France Connect permet également de bénéficier d’une connexion SSO (Single Sign On), permettant à l’usager de passer d’un service « France Connecté » à un autre (exemple : service tiers référencé) sans besoin de réauthentification. En cas d’utilisation d’un service FranceConnect de niveau 1, un code OTP est également demandé.
  + Pour l’application mobile, à l’aide d’informations biométriques (exemple : empreinte digitale ou reconnaissance faciale) ou code de déblocage enregistrés dans son matériel (technologie WebAuthN/Fido2). Ce mode de connexion s’appuie sur les fonctionnalités natives du device pour authentifier l’utilisateur.

Au-delà de ces moyens d’identification pour la connexion à Mon espace santé, dans le système de santé (Mon espace santé, DMP, les logiciels des professionnels de santé), l’usager-patient doit être identifié par son Identité Nationale de Santé constitué de traits (marticule INS / NIR certifié, Nom de naissance, Prénom de naissance, Date de naissance, code insee de commune de naissance et sexe). C’est sur cette INS qu’est basé le principe d’identito-vigilance qui garantit que les données de santé d’un individu lui sont bien rattachées de manière univoque dans les différents systèmes d’information de santé.

<https://esante.gouv.fr/identite-nationale-de-sante/referentiel-national-d-identitovigilance>

##### Gestion des comptes

Après la création de son Mon espace santé, l’usager a la possibilité de gérer l’accès à ses données de santé.

Une fois connecté par le moyen de son choix, l’usager dispose de fonctionnalités lui permettant, entre autre, de gérer les paramètres associés à ses modalités de connexion : changement de mot de passe, révocation d’un device mobile apparié pour les besoins de l’authentification biométrique par exemple.

Un compte d’accès à un Mon espace santé est individuel. Seuls les majeurs disposent de compte d’accès. Le Mon espace santé d’un mineur est accédé par les majeurs disposant d’une délégation d’accès accordée sur justificatif (filiation connue de l’Assurance Maladie ou reconnaissance mutuelle entre parents de ce droit), en utilisant leur propre compte d’accès. Chaque action d’un usager est tracée dans le ou les Mon espace santé auxquels il accède. Concrètement, 2 parents ayant délégation d’accès sur le Mon espace santé de leur enfant mineur, sont identifiés chacun de manière individuelle et sont tracés tels quels dans le Mon espace santé de leur enfant. Au-delà de cette disposition destinée à sécuriser les accès à un Mon espace santé, cela présente l’avantage de faciliter la navigation d’un parent dans les Mon espace santé de ses enfants sans avoir besoin de se ré-identifier avec d’autres identifiants que les siens propres.

Pour chaque compte, au travers de la fonctionnalité Paramètres, l’usager est incité à renseigner les informations personnelles (adresse e-mail pour otp et notifications, numéro de téléphone portable pour otp) et a la possibilité de définir des préférences, ses paramétrages de notifications, de gestion de consentement et d’autorisation d’accès.

Parmi les éléments relatifs à la confidentialité :

* + L’usager peut décider de systématiquement masquer ou démasquer tous ses documents (anciens et à venir) aux professionnels de santé,
  + Décider des interdictions d’accès à son Mon espace santé / DMP par les professionnels de santé,
  + Décider des modalités d’accès en cas d’urgence (bris de glace, accès par un centre 15),
  + Enregistrer ses données de navigation relatives aux cookies de tracking webanalytics,
  + Voir son historique d’activité retraçant les traces d’accès à son Mon espace santé par lui-même, les personnes ayant eu délégation dans le temps, ou les professionnels de santé.

Concernant les accès aux documents du DMP, les autorisations ou interdictions d’accès sont appliqués dans le cadre du fonctionnement offert par le DMP. Ce cadre prévoit notamment que, par défaut, tous les professionnels de santé peuvent consulter les documents (non masqués) du DMP selon leur catégorie. Ces autorisations sont présentées dans la matrice d’habilitation du DMP, qui évolue régulièrement.

<https://www.dmp.fr/documents/d/dmp/matrice-habilitation>

Un usager peut néanmoins décider de bloquer, via ses paramètres, nominativement, l’accès d’un professionnel de santé à ses documents enregistrés dans son DMP.

L’usager peut également donner son consentement éclairé à échanges de données dans le cadre des applications référencées du catalogue de services. Il s’agit d’un consentement explicite, relatif au cadre exclusif des finalités de traitement proposées par le tiers, et révocable sur simple décision. A l’horizon juillet 2023, l’usager pourra donner son consentement à l’échange de données avec des applications proposant de lire ou écrire des mesures, des documents et des données d’évènements d’agenda.

D’autres fonctionnalités sont également proposées en mobile dans le menu Paramètres (signalement d’un problème sur l’application, avis et propositions d’amélioration).

Un Mon espace santé clôturé à la demande d’un usager ou suite à son décès est conservé 10 ans. Dans ce laps de temps, hors décès, l’usager peut réactiver son compte et disposer de tout son historique, néanmoins « gelé » à la date de clôture.

Un Mon espace santé supprimé (après droit de rétraction de 14 jours) est définitivement supprimé. Un usager peut toujours en recréer un, qui est cependant vierge de tout historique (hors données qui seraient alors reconstituées à partir des données de l’Assurance Maladie, comme l’historique de remboursement ou la connaissance du Médecin traitant déclaré qui seront réalimenté à la nouvelle création).

Un majeur peut être titulaire d’un compte d’accès sans avoir lui-même un Mon espace santé afin de disposer de moyens de connexion propres pour accéder à un Mon espace santé d’un mineur. La suppression d’un Mon espace santé n’entraîne la suppression du compte d’accès afférent que dans l’éventualité où ce dernier ne dispose d’aucune délégation active.

##### Gestion des traces et des notifications

###### Traces

Les traces d’activité sont systématiques dans Mon espace santé. Elles retracent l’activité de tous les acteurs intervenant sur les ressources de Mon espace santé, l’usager pour lui-même, l’usager dans le cadre d’une délégation d’accès au Mon espace santé d’un mineur, un professionnel de santé ou un service tiers. Toute action, création, modification, suppression, lecture est systématiquement tracée. Bien que l’exhaustivité des traces réside dans le système, la complexité des appels techniques réelle est masquée afin que les traces soient présentées de manière compréhensible à l’usager. Les traces sont normées afin de faciliter les instructions des différents niveaux de support habilités.

###### Notifications

Afin d’informer les usagers des évènements intervenant dans leur Mon espace santé (ou ceux sur lesquels ils ont une délégation d’accès), le système envoie des notifications.

En fonction des situations, l’usager reçoit des notifications déclenchées par des événements tels que l’accès à la liste des documents par un Professionnel de Santé, la consultation/visualisation du contenu d’un document par un Professionnel de santé, la mise à jour du service, l’ajout de données dans le DMP (hors Historique de remboursements), la réception d’un message, le rappel d’un rendez-vous médical, etc.

Certaines notifications sont réglementaires, et à ce titre non-optionnelles, telles que : Bienvenue dans Mon espace santé, notification vers l’ouvrant droit de la suppression de l’accès au MES d’un mineur en vue d’un passage à la majorité, accès d’un professionnel de santé en mode bris de glace, échéance annuelle de la saisie des directives anticipées, etc.

En règle générale, les services tiers référencés appariés à Mon espace santé gèrent leurs propres notifications. Toutefois, des notifications peuvent également être générées dans Mon espace santé suite à leurs actions : connexion avec un service tiers, déréférencement d’une application synchronisée, rappel du consentement pour une application synchronisée.

Les notifications transmises à l’usager par le système, quelle que soit leur forme (push, mail), sont soumises à des contraintes forte de confidentialité/sécurité. Elles ne peuvent mentionner aucune information médicale ou nominative. Leur rédaction est donc travaillée de manière à engager l’usager à se connecter à son Mon espace santé pour disposer de l’intégralité de l’information pertinente au sujet de l’évènement ayant conduit à l’émission de la notification.

Pour répondre à cette contrainte forte, Mon espace santé est doté d’un module Centre De Notification (CDN), dans lequel l’usager va pourvoir retrouver la notification reçue, le détail associé, et le cas échéant la possibilité d’atteindre directement l’objet de la notification (document, mail, évènement dans l’agenda, etc.). Certains évènements peuvent également être présentés dans le centre de notifications sans pour autant être associés à une notification mail ou push.

Pour procéder à certains paramétrages, à partir des paramètres de son profil administratif, l’usager a la possibilité de choisir le type de notifications qu’il souhaite recevoir pour certains évènements uniquement : notification push sur smartphone ou envoi par mail. A l’échelle du volume potentiel des notifications, des règles de gestion sont mises en place pour maîtriser les volumes de notifications émis au titre des évènements de Mon espace santé. La mise en place de la gestion des notifications s’inscrit dans la recherche d’un bon équilibre entre information suite à un événement et attente de l’usager. L’équilibre financier de l’ensemble (coût des envois courriel contre push, notification via le CDN ou par push sur smartphone) doit est considéré par les features teams concernées lors du déploiement de nouvelles notifications.

Par exemple, le choix push notifications n’est pas cumulable avec le choix notification par mail. De même, en cas de multiples notifications sur une période resserrée, par exemple dans le cas du dépôt de plusieurs documents par un établissement lors d’une sortie d’hospitalisation, les notifications sont cumulées en une seule et transmises en décalé. Il s’agit ici à la fois d’ancrer Mon espace santé dans une démarche écoresponsable et d’optimiser les coûts d’exploitation du système.

Le système de notifications est paramétrable de manière aisée, à chaud, pour permettre au métier de procéder à des adaptations rapides en cas de nécessité.

L’adressage de notifications est différencié selon que l’usager a créé ou pas son compte d’accès à son Mon espace santé.

* + Si l’usager a un compte d’accès : l’adresse utilisée en cas de notification mail est celle enregistrée dans le compte Mon espace santé de l’usager. Les push notifications sont quant à elle émises sur les devices sur lesquels l’application est installée, selon les paramètres retenus par l’usager y compris au niveau de son OS mobile.
  + Si l’usager n’a pas de compte d’accès : l’adresse mail utilisée est celle récupérée auprès de son régime d’Assurance Maladie (entrainant l’intervention de SI externes tels que celui de la MSA ou la MGEN par exemple).
  + Si l’usager n’a pas de compte d’accès et ne dispose pas d’une coordonnée mail fiabilisée connue par son régime d’Assurance Maladie (25% de la population) : les notifications doivent être transmises par courrier postal.

Pour des raisons économiques évidentes, ces notifications postales ne sont pas transmises unitairement.

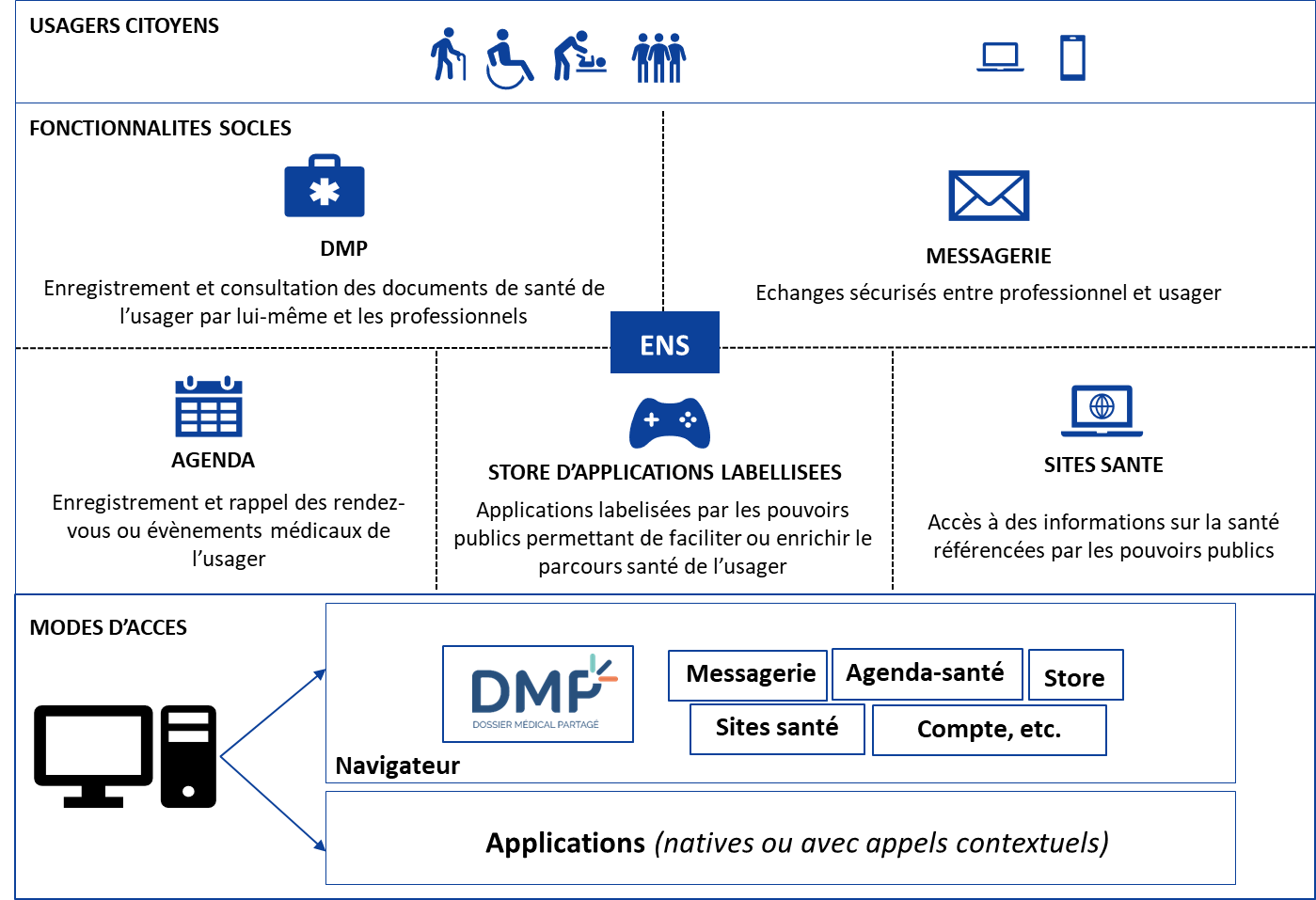
Pour répondre au besoin de pouvoir notifier cette part de la population a priori éloignée du numérique, un service de génération de courrier est proposé au sein du SI Mon espace santé. Ce service permet de générer des courriers, qui sont ensuite transmis à une chaîne éditique opérée par la Cnam (chaîne éditique CEREUS dont le format d’échange est AFP).

Il s’agit d’une chaîne de notification secondaire, qui doit néanmoins rester opérationnelle pour garantir la capacité du SI Mon espace santé à pouvoir générer dans des délais très courts, le temps de la constitution du modèle de courrier, des courriers, quelle que soit leur nature, si besoin.

A mai 2023, sont générés deux types de courriers :

* + Le courrier de synthèse des évènements survenus sur un Mon espace santé « sans adresse mail » : celui-ci vise à notifier tous les assurés ayant un Mon espace santé créé automatiquement mais ne l’ayant pas encore activé, afin de leur indiquer les éventuelles actions réalisées par un professionnel de santé sur leur espace ; entre autres, dépôt de document et envoi de message. Ce courrier ne devrait plus être émis à fin 2023 pour l’ensemble des usagers, mais pourrait néanmoins faire l’objet d’impression « unitaires » en fonction des demandes des usagers au support, au titre de leur droit RGPD.
  + Le courrier d’information aux usagers opposés à Mon espace santé mais toujours détenteurs d’un DMP de l’opération de régularisation de ces DMP/Mon espace santé afin qu’ils soient réintégrés au droit commun (pas d’existence de DMP non rattaché à un Mon espace santé).

##### Fonctionnalités Mon Espace Santé



Après s’être connecté à son compte, l’usager est redirigé vers la page d’accueil de Mon Espace Santé. Celle-ci lui permet un accès rapide à l’ensemble des fonctionnalités de Mon espace santé qu’il s’agisse des fonctionnalités socles ou de fonctionnalités transverses, articulant les fonctionnalités socles pour répondre aux enjeux d’un processus métier particulier.

Les fonctionnalités socles correspondent :

* + Au profil médical de l’usager ;
  + Aux Documents (basés sur le DMP), rubrique qui permet le stockage sécurisé et la consultation des documents et données de santé (brique documentaire et certaines données structurées) tant par l’usager que par les professionnels ;
  + A la messagerie sécurisée permettant des échanges entre l’usager et les professionnels assurant sa prise en charge ;
  + A l’agenda permettant de consolider les différents évènements de santé : rendez-vous médicaux, hospitalisations, tâches, etc. ;
  + Au catalogue de services de santé référencés par la puissance publique.

Les fonctionnalités transverses sont par exemple :

* + Page d’accueil support de la personnalisation des services ;
  + Centre de notification accompagnant l’usager vers les services ;
  + Transmission d’une ordonnance à une pharmacie ;
  + Auto-questionnaires de santé articulés avec le profil médical et amenant à des conseils personnalisés en prévention à l’attention des usagers ;
  + Processus de rematérialisation de l’ensemble des ressources de Mon Espace Santé à la demande de l’usager (DMP, messagerie, Agenda, profil médical, compte, données connues du support, etc.), prévoyant la constitution des archives et leur mise à disposition sécurisée à l’usager de son information ;
  + Processus de suppression de l’ensemble des ressources de Mon Espace Santé à la demande de l’usager (DMP, messagerie, Agenda, profil médical, compte, données connues du support, etc.) prévoyant un délai de rétractation, puis la coordination de la suppression des ressources et le cas échéant du compte d’accès et l’information à l’usager.

Les fonctionnalités de Mon espace santé évoluent de manière trimestrielle. Les fonctionnalités présentées ci-après le sont à titre indicatif et ne présument pas du périmètre fonctionnel de Mon espace santé à horizon de la notification du présent accord-cadre.

###### Profil médical

Dans Mon espace santé, l’usager est placé au centre de la prise en charge de sa santé au travers notamment de son profil médical.

Les données médicales contenues dans le profil médical permettent une meilleure prise en charge de la santé de l’usager, par la mise à disposition et le partage d’informations de santé pour le suivi de la personne.

Le profil médical comporte, à mai 2023, les rubriques suivantes :

* + Des rubriques que l’usager est libre de renseigner ou non :
* Suivi médical : Maladies et sujets de santé, Traitements, Hospitalisations, Handicaps
* Facteurs de risques : Allergies, Antécédents familiaux, Habitudes de vie (tabac et activité physique)
* Mesures de santé : Poids, Taille, Indice de Masse Corporelle, Tour de taille, Température, des mesures de glycémie, Tension artérielle, etc.
* Professionnels de santé : sélection de PS référencés dans l’annuaire santé, récupération du médecin traitant auprès des bases de l’Assurance Maladie
* Entourage et volontés : Entourage (personne de confiance, contact d’urgence, proche aidant, proche aidé, les directives anticipées, l’indication relative au don d’organes et de tissus
* Pièces administratives

Pour chaque mesure, l’usager peut ajouter, modifier ou supprimer une mesure et toutes ses mesures sont historisées. Les valeurs poids, taille, IMC, périmètre crânien ajoutées par l’usager sont présentées sous forme de courbes. Aux âges de l’enfant, des courbes de références (respectant les spécifications de l’INSERM et de fait correspondant aux courbes du carnet de santé des enfants) pour ces mesures sont également affichées. Un tableau de bord des mesures par défaut (concernant l’ensemble des usagers) est affiché. L’usager peut le personnaliser en choisissant d’afficher ou de masquer une ou plusieurs mesures parmi celles proposées. Tous les usagers ont sur ce tableau de bord les mesures de santé :

* + Pour les usagers âgés de moins de 5 ans, est affiché en plus le périmètre crânien ;
  + Pour les adultes, est affiché en plus le tour de taille.

Les mesures peuvent également être alimentées par des objets connectés référencés dans le cadre du catalogue de services Mon Espace Santé. Les règles s’appliquant sont alors celles définies par le fournisseur du service référencé dans le cadre de sa déclaration de finalité de traitement. L’usager ayant choisi d’apparier un service référencé a accepté ces finalités par son consentement éclairé à l’échange de données.

Pour répondre à l’ambition d’être interfacées à des services tiers, les mesures s’appuient sur les volets [du CI-SIS](https://esante.gouv.fr/volet-gestion-dagendas-partages) (cadre d’interopérabilité des SI en santé) et répondent aux exigences de la norme FHIR.

Les informations concernant la rubrique Entourage et volontés sont issues d’un seul document structuré du DMP. Ce document contenant les mentions précitées est dénommé Volonté et Droits du Patient (VDP).

Par le biais de ce document, l’usager peut gérer ses volontés et droits et ses directives anticipées au sein du profil médical :

* + Modifier les informations de son entourage (ajout/modification/suppression des contacts d’urgence, de la personne de confiance, des proches aidants et des proches aidés)
  + Modifier la mention relative au don d’organe, permettant à l’usager d’indiquer qu’il est au courant de la réglementation actuelle.
  + Saisir ses directives anticipées via un formulaire ou en téléchargeant un document préexistant.

Ces informations « Volonté et Droits du Patient » étant dans le DMP, elles sont donc accessibles aux Professionnels de Santé via leurs propres interfaces d’accès au DMP.

* + Une rubrique alimentée automatiquement :
* Mon Histoire de Santé est alimentée automatiquement par les historiques de remboursements de l’Assurance Maladie. Cette rubrique fait l’objet de traitements afin de proposer à l’usager une vue temporelle à différents niveaux de granularité (jour, mois, année). Par ailleurs des fonctionnalités d’incitation à récupérer de l’information à partir de cet historique sont mises en places. Elles servent à alimenter d’autres rubriques du profil médical de manière différenciée. L’usager peut ainsi récupérer un traitement à partir des informations de dispensation connues de l’Assurance Maladie, ou un professionnel de santé à ajouter à son cercle de professionnels traitants. Ces enrichissements ont vocation à être complétés pour tirer le meilleur parti de l’historique de remboursement au profit d’un meilleur accompagnement de l’usager pour mettre en visibilité les informations structurantes de son parcours de santé. Les données de Mon Histoire de Santé sont issues du DMP, qui les détient lui-même d’une chaine de liaison opérée par la Cnam. Du fait de cette construction, à mai 2023, l’historique de remboursement est alimenté dans un Mon Espace Santé / DMP sur déclenchement de l’usager à la création de son compte d’accès à son Mon Espace Santé. L’historique de remboursement est alors présenté dans Mon Espace Santé sous un délai de 48h au maximum. L’historique des remboursements évolue par ailleurs au gré des nouvelles cotations remboursées par l’Assurance Maladie et les règles de gestion de présentation de ces soins dans Mon Espace Santé doivent de ce fait être révisées et adaptées.
  + Une rubrique qui peut être alimentée à la fois par l’usager et par le Professionnel de santé :
* Le carnet de vaccination peut être conjointement renseigné par le Professionnel de santé depuis le DMP et par l’usager depuis Mon Espace Santé. Pour ajouter une vaccination, l’usager, comme le Professionnel de Santé, s’appuient sur un référentiel de vaccination mis à leur disposition. Ce référentiel est issu de la base Thésorimed et traité à la fois dans le DMP et dans Mon Espace Santé. Dans Mon Espace Santé, l’usager est également informé de toutes les vaccinations obligatoires ou recommandées à faire, suivant son âge. De la documentation générale relative à la vaccination lui est également proposée. Ces recommandations sont basées sur les celles du Ministère de la Santé et évoluent régulièrement. Le carnet de vaccination constitue un enjeu majeur du Mon Espace Santé des mineurs en tant que carnet de santé numérique des enfants.

Au-delà de la visualisation sur son interface Mon Espace Santé, l’usager a la possibilité, s’il le souhaite, de générer la synthèse de son profil médical (document au format PDF listant l’ensemble des données précitées hors Mon Espace Santé, et avec 10 valeurs maximum pour les mesures de santé) et l’enregistrer dans ses documents partageables avec les Professionnels de Santé. Il rend ainsi les données accessibles aux professionnels de santé autorisés à accéder à son DMP.

Ce document a pour but de faciliter le premier rendez-vous entre un patient et un professionnel de santé. Il combine en effet l’avantage de présenter des thématiques d’intérêt pour le professionnel et d’être un pense-bête pour le patient sur des sujets qu’il aurait potentiellement pu oublier au fil du temps. Du point de vue des professionnels de santé, ce profil médical est une vue de l’état de santé du patient par lui-même et vient en complément des informations contenues dans le volet de synthèse médicale éventuellement déposé dans le DMP du patient par un confrère. Le profil médical a également pour objectif de faciliter les processus de pré-admission dans les établissements de santé, généralement assurés par du personnel médico-administratif, en amont de l’intervention des professionnels de santé. Pour maximiser la réutilisation de ces données dans les logiciels des acteurs de santé destinataires, établissements comme professionnels libéraux, la structuration des données du profil médical sera petit à petit à renforcer.

Il est également possible pour l’usager de télécharger sa synthèse spécifique aux vaccinations ou aux allergies. Ces synthèses spécifiques sont uniquement téléchargeables et ne sont pas enregistrées dans les documents de l’usager sur son Mon Espace Santé. S’inscrivant dans les fonctionnalités proposées au titre du carnet de santé de l’enfant, elles sont destinées par exemple à une entrée en crèche ou à l’école pour les enfants.

Le profil médical est régulièrement enrichi de nouvelles fonctionnalités afin de permettre aux usagers un suivi rapproché, interactif de leur santé.

Tous les éléments contenus dans le profil médical d’un Mon Espace Santé peuvent faire l’objet d’une rematérialisation ou d’une suppression à la demande de l’usager dans le cadre global de la demande de rematérialisation ou de la suppression du Mon Espace Santé dans son intégralité.

###### Documents de santé

Les documents de santé sont un élément fondateur du dossier santé de chacun de nos concitoyens. Nous sommes néanmoins nombreux à connaitre des expériences complexes quand il s’agit de les récupérer auprès des professionnels de santé. Leur absence induit bien souvent des difficultés dans la coordination des soins. Le DMP historique avait pour but de palier à cette difficulté mais s’était heurté à la résistance à la fois des professionnels de santé que des usagers. Ces derniers expriment encore régulièrement leur attente, notamment à l’occasion des 2 premiers [comités citoyens](https://esante.gouv.fr/assises-citoyennes) qui ont été organisés sur ce sujet, à l’égard des professionnels de santé en matière de dépôt systématique des documents, mais les changements de pratique s’inscrivent dans un temps long. La mise en place de Mon espace santé, avec l’opt-out, et du Ségur de la santé, qui impose par voie règlementaire les dépôts et accompagne financièrement à grande échelle la mise à jour des logiciels métiers des professionnels de santé pour faciliter ces dépôts, devraient néanmoins ouvrir de nouvelles perspectives, avec une systématisation des dépôts de documents améliorant la visibilité à la fois des patients et des professionnels de santé. De fait, les enjeux de l’espace documentaire dans Mon espace santé sont cruciaux. A l’échelle d’une vie de soin, Mon espace santé doit permettre à un usager et à ses professionnels de trouver les documents qui feront gagner temps et efficacité dans la prise en charge au bénéfice de tous.

Afin de permettre aux usager la gestion et le partage de leurs documents de santé, la rubrique Document a été mise en place dans Mon Espace Santé. Cette rubrique s’appuie sur le fonctionnement du DMP. De ce fait, dans Mon espace santé sont gérés les différents types de documents et données gérés dans le DMP tels que prévus au CI-SIS : documents HL7 CDA R2 niveau 1 (semi-structurés, au niveau de l’en-tête), documents HL7 CDA R2 niveau 3 (structurés).

Les documents structurés de type CDA R2 niveau 3 ne sont pas systématiquement présentés dans la rubrique Documents, en particulier ceux relatifs aux volontés et droits du patients et carnet de vaccination qui sont présentés au niveau du profil médical de Mon espace santé.

Les documents structurés du type CDA R2 niveau 3 déposés par les professionnels de santé sont quant à eux présents. Des travaux restent cependant à mener pour améliorer leur présentation.

Depuis sa rubrique Documents l’usager peut :

* + Consulter les documents déposés par les Professionnels de Santé ou lui-même (au format pdf, txt, jpg et jpeg à date) ;
  + Ajouter des documents ;
  + Effectuer des actions sur ses documents ;
  + Supprimer les documents dont il est l’auteur ;
  + Modifier les documents dont il est l’auteur ;
  + Modifier la confidentialité de ses documents, et donc leur visibilité aux professionnels de santé ;
  + Créer et gérer des dossiers permettant le classement des documents ;
  + Effectuer des actions sur multiples documents à la fois, permettant :
* La suppression de multiples documents à la fois,
* Le déplacement de multiples documents à la fois dans un dossier.
  + Signaler un document pour remonter un problème aux agents du support Mon Espace Santé, en particulier quand un document a été déposé par un Professionnel de Santé par erreur ;
  + Envoyer un document via sa messagerie sécurisée de santé, en particulier une ordonnance à une pharmacie.

Tous les documents présentés dans la rubrique Document de Mon Espace Santé sont stockés dans le DMP. Cette présentation est réalisée par le biais d’API interfaçant les 2 systèmes DMP et Mon espace santé. Pour des questions de performances mais également à des fins d’applications de règles de gestion de présentation, un index des documents présents au DMP est maintenu côté Mon espace santé.

Les documents présents dans MES peuvent être déposés et consultés par l’usager lui-même, les professionnels ou établissement de santé, mais également par des services tiers référencés et pour lesquels l’usager a au préalable accepté un appariement.

Pour répondre à l’ambition d’être interfacés à des services tiers, les documents s’appuient sur les volets [du CI-SIS](https://esante.gouv.fr/volet-gestion-dagendas-partages) (cadre d’interopérabilité des SI en santé) et répondent aux exigences de la norme FHIR.

L’usager peut à tout moment modifier l’accès à ses documents par les Professionnels de Santé (personnes phyisques identifiées par leurs moyens d’identification personnels direct ou via un dispositif d’authentification indirect lorsqu’ils sont dans des structures de soins) ou par les services tiers via les divers outils de gestion de la confidentialité et des consentements présents au niveau de granularité du document lui-même (dans la rubrique Documents), ou au niveau de l’ensemble de son Mon espace santé (dans la rubrique Paramètres).

Les documents déposés par des professionnels de santé dans le DMP font l’objet d’une notification à l’usager, instantanée ou groupés et temporisée en fonction de la nature et du contexte de dépôt des documents.

Seul le professionnel de santé ayant déposé un document peut procéder à sa dépublication. Par contre, dans le cadre d’une demande de rematérialisation ou d’une suppression de l’intégralité d’un Mon espace santé, tous les éléments contenus dans le DMP d’un Mon espace santé peuvent être rematérialisés ou supprimés en masse à la demande de l’usager.

**Classement des documents et liens entre rubriques**

Un des enjeux majeurs de la présentation des documents dans les dossiers médicaux des patients est le classement des documents, pour lui-même mais également pour les Professionnels de Santé. Les fonctionnalités existantes, à date, en la matière sont issues pour une part importante de l’histoire du DMP. Et les fonctionnalités ajoutées présentent de premiers pas d’amélioration et simplification, du point de vue de l’usager. Les retours d’expériences terrain ne sont cependant pas encore assez conséquents pour considérer que la question de la présentation des documents est arrivée à maturité dans Mon Espace Santé pour les usagers, et dans le DMP du point de vue des professionnels de santé.

Les documents sont nativement classés dans le DMP selon une classification riche, à plusieurs niveaux, censée répondre historiquement aux besoins des professionnels de santé. Ces catégories font l'objet d'une normalisation dans le cadre CI-SIS par l'utilisation de référentiel de type de document (LOINC).

Chacune des grandes catégories existantes côté Professionnels de Santé (Synthèses, Traitements et Soins, Comptes rendus, Imagerie médicale, Biologie, Prévention, Certificats et Déclarations, Documents de l'usager) subdivisée en de nombreuses sous-catégories, comprend tout le détail des documents possibles, souvent compréhensibles par les seuls Professionnels de Santé.

Aussi, se trouve dans chacune de ces grandes catégories vues des Professionnels de Santé, une catégorie personnalisée correspondant aux documents déposés par l’usager (exemple « Mes synthèses » pour la catégorie « Synthèses »). L’usager peut ainsi déposer une synthèse qu'il a pu récupérer par d’autres voies, sans avoir à préciser s'il s'agit d'une « note de transfert » ou d'une « synthèse d'un épisode de soins ». Par construction, le Professionnel de Santé a accès à toutes les catégories y compris celles qui sont ajoutées pour l'usager.

La classification vue des Professionnels de Santé n’est pas adaptée au besoin des usagers patients. Pour la présentation des documents dans Mon Espace Santé, une classification « miroir » a été mise en place, elle simplifie la classification des documents du point de vue de l’usager en proposant un nombre de rubriques de 1er niveau plus explicite et sans 2nd niveau de détail. Les rubriques de classement des documents vues des professionnels de santé sont donc transcodées en rubriques simplifiées, en nombre et en vocabulaire utilisé, du point de vue du patient.

Depuis l’interface de Mon Espace Santé, l'usager peut donc consulter et alimenter son DMP selon la classification « usager ». Quel que soit son parcours utilisateur pour alimenter un document (depuis la rubrique documents, depuis le profil médical, depuis la messagerie sécurisée de santé, l'usager dispose d’un parcours unifié, lui permettant de qualifier le document qu'il dépose selon cette classification simplifiée. Le professionnel de santé voit quant à lui le document en question dans sa classification de premier niveau et bien identifié comme un document déposé par le patient (alors que les documents déposés par ses pairs sont a priori dans des répertoires apportant une meilleure qualification de la nature du document).

Ces dispositions, si elles simplifient les parcours utilisateurs des patients à court terme, ne répondent clairement pas à l’enjeu du volume de documents à l’aune du changement de pratique par les professionnels de santé et de l’empowerment des usagers. Ces changements de pratiques devraient amener à l’échelle d’une vie de parcours de santé un nombre conséquents de documents dans les Mon Espace Santé de chacun des citoyens et des besoins afférents de simplification du classement et de la recherche de documents pour les 2 parties, patients et Professionnel de Santé. Afin d’éviter l’engorgement dû à la conservation de documents plus pertinents, un marquage concernant l’historique des documents dans certaines catégories pourra compléter la fonctionnalité offerte.

En plus de cette classification par nature de documents dans le DMP, Mon Espace Santé propose à l'usager la possibilité de créer ses propres dossiers de classement. Par exemple, l’usager peut créer un dossier « Ma grossesse » ou « Opération du genou ». Il peut alors signifier via son interface Mon espace santé quels sont les documents qui relèvent de tel ou tel épisode de santé et du dossier lié. Il ne s’agit alors pas d’un classement physique d’un document dans le dossier mais d’un lien thématique. A un même document peuvent être associés plusieurs liens, le document en question peut donc être visible dans plusieurs dossiers et éventuellement liés à un item du profil médical.

Par exemple, un compte rendu de biologie traitant à la fois des marqueurs d’un cancer et d’une insuffisance cardiaque peut être lié dans le Mon Espace Santé d’un patient aux items suivants :

* + Compte-rendu déposé par le laboratoire, présent uniquement dans la catégorie Biologie du point de vue des professionnels de santé autorisés dans le DMP du patient
  + Visible « nativement » par le patient dans la rubrique « Résultats de biologie » dans son Mon Espace Santé
  + Rattaché par le patient à un dossier personnel « Cancer », visible par l’usager dans son dossier « Cancer » dans son Mon Espace Santé. Le dossier « Cancer » de l’usager n’est pas connu et pas visible du professionnel de santé.
  + Rattaché par le patient à un autre dossier personnel « Cœur », visible par l’usager dans son dossier « Cœur » dans son Mon Espace Santé. Le dossier « Cœur » de l’usager n’est pas connu et pas visible du Professionnel de Santé.
  + Ce compte-rendu de biologie peut également être lié à un item du profil médical, comme sur une saisie de la rubrique hospitalisation par le patient portant le motif « Remplacement pacemaker ».

Ces liens peuvent être mis à jour ou supprimés par le patient en fonction de ses besoins de classement ou de mise en avant d’un ou plusieurs documents nécessaires à un moment particulier de son parcours de soins.

Cette mécanique d’association de 2 objets de Mon Espace Santé ayant été conçue de manière universelle, d’autres liens peuvent être mis en place comme par exemple un lien d’un document avec un évènement de l’agenda.

###### Messagerie

L’usager dispose au sein de Mon espace santé d’une solution d’échanges de messages sécurisés avec les Professionnels de Santé enregistrés dans l’espace de confiance MSSanté. Cette solution d’échanges permet à l’usager de communiquer avec les Professionnels, équipés de boîtes aux lettres MSSanté, qui le prennent en charge.

Tous les échanges se font par utilisation d’un système de messagerie référencé dans l’Espace de Confiance « MSSanté » (<https://esante.gouv.fr/produits-services/mssante>).

Dans l’écosystème MSSanté, Mon espace santé est un opérateur de messagerie sécurisée de santé à part entière, ayant pour particularité d’être l’unique opérateur des messageries sécurisées de santé des citoyens.

Les boîtes de messagerie des Professionnels de Santé sont quant à elles gérées par de multiples opérateurs externes. Les interactions entre les messageries sécurisées de santé sont régies par le Référentiel Opérateurs de Messageries Sécurisées de Santé (ex-DSFT) ainsi que l’équivalent, pour les clients de messagerie, indépendants ou intégrés dans les logiciels métier des professionnels. Les logiciels de cabinet Ségur ont pour objectif de faciliter l’adressage de messages sécurisés entre Professionnel de Santé et patients, afin d’ancrer de nouvelles pratiques et de remplacer les échanges de messages concernant des sujets de santé par des boites aux lettres généralistes non sécurisées.

L’ensemble de la documentation technique (référentiel opérateur, référentiel client, etc.) est accessible sur <https://mailiz.mssante.fr/is/doc-technique>. La messagerie de Mon espace santé respecte les exigences applicables à « l’Opérateur usagers » du Référentiel (Versions actuelles et à venir) disponible sur le site de l’ANS.

Chaque usager, s’il ne s’est pas opposé à la création de Mon espace santé ou s’il n’a pas demandé la fermeture ou la suppression de son Mon Espace Santé, dispose d’une adresse de Messagerie, dont le nom de domaine, spécifique à Mon Espace Santé, appartient à la liste des domaines de l’Espace de Confiance MSSanté, le domaine réservé @patient.mssante.fr. Ainsi, plusieurs de 66 millions de boîtes aux lettres et d’adresses de messagerie ont été créées avec Mon Espace Santé. L’adresse d’une boite aux lettres MSSanté patient est construite sous la forme « matricule INS sur 15 caratères@patient.mssante.fr ».

La solution de messagerie sécurisée Mon Espace Santé dispose nativement de toutes les fonctionnalités « standard » d’un système de Messagerie, elle repose sur le serveur de messagerie Zimbra. Cependant, les échanges entre Professionnel de Santé et patient ne s’inscrivent pas dans des usages communs de messagerie. Les Professionnels de Santé sont notamment particulièrement attentifs à disposer des moyens de maîtriser ce canal de communication avec leurs patients. De ce fait, l’interface patient de la messagerie sécurisée de santé Mon espace santé a été adaptée pour proposer, dans un premier temps, uniquement les fonctionnalités de base nécessaires à un usage entre 2 interlocuteurs identifiés et ayant accepté ce canal d’échanges. Des règles particulières sont donc mises en place pour adapter la Messagerie aux spécificités des échanges entre un usager et des Professionnels.

Les principales fonctionnalités disponibles dans la Messagerie Mon espace santé sont :

* + Consulter les messages reçus et les pièces jointes associées, en mode « conversation »
  + Répondre/Répondre à tous à un message
  + Supprimer les messages d’une conversation
  + Enregistrer les pièces jointes dans la rubrique Documents, ou les télécharger sur son appareil
  + Ecrire un message à un Professionnel de Santé
  + Mode « brouillon » qui permet la sauvegarde automatique des messages en cours de rédaction
  + Rechercher une pharmacie parmi celles qui disposent d’une adresse MSSanté en boîte organisationnelle et la sélectionner en tant que destinataire d’un message pour partager une ordonnance de manière sécurisée avec un pharmacien
  + Accéder au détail d’un Professionnel expéditeur d’un message et ajouter le Professionnel dans sa liste de Professionnels de son Profil Médical

Toujours dans le souci d’équilibrer « effort à produire » et « valeur des fonctionnalités proposées par Mon Espace Santé », certaines fonctionnalités ne sont pas implémentées, dans l’attente de l’émergence de cas d’usage dont la valeur pourrait être objectivée comme par exemple : le transfert d’un message reçu.

Pour répondre aux particularités de cette messagerie entre patient et Professionnel de Santé, les spécificités suivantes ont été implémentées :

* + Restrictions quant à la sélection des destinataires : impossibilité de contacter n’importe quel professionnel qui dispose d’une adresse MSSanté, hormis avec les pharmaciens équipés d’une boite aux lettres organisationnelle, impossibilité de correspondre entre usagers ;
  + Mise en place d’un mécanisme pour permettre à tout Professionnel, à partir de sa Messagerie MSSanté, d’interdire à un usager d’échanger avec lui (hors pharmacies avec boîte aux lettres organisationelle) ;
  + Contrôle et restrictions sur les formats de pièces jointes, sur l’affichage de certains formats pour respecter les formats d’enregistrement dans le DMP et ne pas « polluer » l’usager avec des formats qu’il ne peut pas lire via son interface Mon Espace Santé ;
  + Personnalisation de messages renvoyés automatiquement : compte inexistant, compte fermé, INS invalide, etc.

Les messages reçus de la part de professionnels de santé font l’objet d’une notification instantanée à l’usager.

Tous les éléments contenus dans la messagerie sécurisée d’un Mon espace santé peuvent faire l’objet d’une rematérialisation ou d’une suppression à la demande de l’usager.

###### Agenda

L’objectif de l’agenda Mon Espace Santé est de proposer à l’usager une vue consolidée de tous ses événements (rendez-vous et tâches) de santé.

Dans la version de Juillet 2023 de MES, l’agenda permettra :

* + L’enregistrement d’évènements (rendez-vous et rappels) :
* En saisie manuelle par l’usager (rendez-vous et rappels),
* En récupérant des rendez-vous des services tiers référencés (par exemple : d’application de prise de rendez-vous, portail établissement, etc.) dès lors que l’usager a accepté de synchroniser ces services de prise de rendez-vous dans son catalogue de services Mon Espace Santé (cf §3.1.3.4.7.5 Catalogue de services Mon Espace Santé) ;
  + La modification et la suppression des rappels et rendez-vous enregistrés manuellement dans l’agenda Mon Espace Santé ;

Selon ses préférences de notifications enregistrées dans son profil administratif, l’usager pourra être notifié à l’échéance des rendez-vous et tâches.

Les fonctionnalités de l’agenda Mon Espace Santé sont amenées à être étendues progressivement :

* + Rappel d’actes de prévention ciblés selon le profil de l’usager (articulation avec la brique « Notifications »)
  + Alimentation de l’agenda par des événements provenant des parcours Assurance Maladie (ex. Parcours Programme d’Accompagnement du Retour à Domicile – PRADO)

L’agenda Mon Espace Santé s’appuie sur le volet [du CI-SIS](https://esante.gouv.fr/volet-gestion-dagendas-partages) (cadre d’interopérabilité des SI en santé) et répond aux exigences de la norme FHIR.

###### Catalogue de services Mon Espace Santé

L’objectif du catalogue de services référencés de Mon Espace Santé est de proposer à l’usager un ensemble de services référencés, proposant ou non des échanges de données avec Mon Espace Santé. Ces services référencés répondent à des exigences fortes en matière de sécurité, respect du RGPD, technique et interopérabilité et enfin éthique. Le catalogue de services, aussi appelé Store, incarne un des principes de l’Etat plateforme.

Le catalogue de services est une fonctionnalité sur laquelle nous disposons d’un recul limité au catalogue des applications référencées sans échanges de données depuis fin 2021. Sa proposition de valeur est à date assez frugale et se construira au fil de temps, en fonction des cas d’usage qui seront proposés par les patients et les éditeurs de services en santé. Le potentiel de référencement, avec ou sans échanges de données, est important. Au 15 mai 2023, 267 éditeurs ont mentionné être intéressés par l’offre de services. Parmi eux, 117 éditeurs ont réalisé des échanges avec la Cnam et 26 services sont en cours d’instruction. 23 services sont d’ores et déjà référencés au catalogue et consulté par 15% des utilisateurs connectés à Mon espace santé.

Les services référencés (applications mobiles, sites web, objets connectés, etc.) sont proposés par des éditeurs de solutions publics et privés, nationaux ou locaux, en marque propre ou marque blanche. Ces services des domaines de la santé et du bien-être sont référencés par les pouvoirs publics dont l’ambition est d’apporter un gage de confiance à l’usager. Le catalogue de services Mon espace santé éclaire les usagers dans le choix de ces services en santé. Dans sa version la plus élaborée, le service tiers peut être appariés au Mon espace santé d’un usager (après consentement éclairé sur la base des finalités de traitement présentées par l’éditeur) pour permettre l’échange de données entre Mon espace santé et le service tiers concerné. Ces échanges de données nécessitent de fait un appariement emportant une identification précise de l’usager concerné par les échanges à venir. Dans sa version de Juillet 2023, l’échange de données ne sera possible que pour les Mon espace santé des patients majeurs (et pour eux-mêmes).

Dans Mon espace santé, le catalogue de services affiche à l’usager l’ensemble des services référencés. L’usager peut trouver un service via une fonction de recherche ou en parcourant l’ensemble du catalogue (classement par ordre alphabétique). Il lui appartient s’il le souhaite de télécharger une application en question à partir des stores officiels.

L’usager peut choisir de synchroniser un service tiers à son Mon espace santé. Des retours d’expérience captés dans le cadre de l’appel à candidature mené en 2020 et 2021, le processus d’appariement est plus naturel à partir du service tiers. Néanmoins, il est également possible à partir de Mon espace santé. A partir de la fiche de présentation du service tiers présentée dans Mon espace santé, l’usager est invité à donner son consentement pour accepter l’échange de données entre ce service et les fonctionnalités socles de son Mon espace santé (agenda, DMP, Profil Médical, Messagerie etc.).

Ce consentement devra se faire de manière éclairée (nature de la donnée échangée, fréquence de l’échange, finalités à l’échange de données, moyens de recours, textes applicables, etc.).

A partir de son compte Mon espace santé au niveau des paramètres, l’usager peut à tout moment gérer ses consentements relatifs à de l’échange de données avec des services tiers référencés : autoriser, retirer ses consentements, désynchroniser un service numérique référencé et consulter les traces des flux échangés. Il reçoit également des notifications dans le contexte d’une synchronisation avec un service numérique référencé, selon les choix qui ont été faits au moment de l’implémentation des échanges. En règle générale, Mon espace santé ne se substituera pas à l’application tierce en matière de notifications à l’usager. Cependant, Mon espace santé notifiera parfois l’usager, comme par exemple pour lui rappeler les consentements en cours et l’inviter à les revoir, ou dans des contextes particuliers comme lorsque l’administrateur Mon espace santé procédant au déréférencement d’un service en informerait les usagers concernés.

Une fois le consentement enregistré, l’échange de données (de back-office à back-office) peut avoir lieu selon les conditions retenues par l’usager, pour alimenter ou consulter :

* + Des documents médicaux ciblés du DMP
  + Des mesures de santé du profil médical
  + Des événements de santé du type rendez-vous médicaux et tâches de l’Agenda

L’accès des services numériques référencés du catalogue de services aux ressources de Mon espace santé se fait par des interfaces de programmation (API) sécurisées et répondant aux standards en vigueur décrits dans le cadre d’interopérabilité des systèmes de santé édité par l’Agence du Numérique en Santé.

Fonctionnement de l’API Appariement

L’API Appariement (respectant le standard OAuth2.0) permet d’assurer la connexion entre un profil Mon Espace Santé et un profil d’un service numérique référencé. L’intérêt de cette API Appariement est de faire l’interface entre un service numérique référencé et les API dites « métiers » qui correspondent aux API Document, Mesures, Agenda et par la suite Messagerie. Cette API Appariement permet également de protéger l’échange de données entre un profil Mon espace santé et le service numérique référencé.

###### Les parcours transverses

Accompagnement contextualisé de l’usager et prévention

Les tests utilisateurs sont unanimes sur les attentes des usagers en matière de personnalisation de leur espace. Cette attente est à conjuguer avec le cadre juridique complexe encadrant à la fois Mon espace santé et le DMP. Toute personnalisation doit être proposée en permettant aux usagers, pour eux-mêmes ou dans le cadre d’une délégation d’accès, de faire valoir leurs droits, afférents aux finalités d’utilisation de leurs données personnelles.

En 2023, Mon espace santé propose déjà des contenus et parcours personnalisés en fonction des critères âge et sexe, ou des parcours contextualisés.

A titre d’exemple, les blocs Mon actu santé proposent des contenus différenciés :

* + Pour les femmes de 25 à 26 ans, incitation au dépistage en lien avec le cancer du col de l’utérus : « Le test HPV-HR cherche la présence de papillomavirus à haut risque sur le col de l'utérus. (Valable également sur d’autres tranches d’âge) »
  + Pour les femmes de 50 ans, incitation au dépistage du cancer du sein : « Tous les 2 ans, participez au dépistage gratuit du cancer du sein grâce à une mammographie »
  + En période de forte chaleur, conseil pour tous

Ces contenus font l’objet d’une programmation dynamique, via CMS, pour que l’usager puisse disposer de contenus variés et nouveaux à chacune de ses visites.

La prévention s’appuie sur des informations propres de l’usager (début 2023 sexe et âge, dès parution d’un nouveau décret Mon espace santé prévu à l’automne 2023, sur d’autres critères) à partir desquelles des messages de prévention peuvent être portés auprès de l’usager.

A partir de l’automne 2023, dans le cadre du plan gouvernemental de prévention, des auto-questionnaires seront proposés aux usagers de Mon espace santé. Quatre tranches d’âges se verront proposé un auto-questionnaire spécifique à leur tranche d’âge. Cet auto-questionnaire comporte des questions sur l’état de santé et sur les habitudes de vie de l’usager. Cet auto-questionnaire une fois saisi par le patient fait l’objet d’une synthèse sous forme de pdf mis à disposition des professionnels de santé via le DMP. Certaines questions sont liées à des rubriques du profil médical et font l’objet d’une circularisassion : l’auto-questionnaire alimente le profil médical, le cas échéant le profil médical peut alimenter une prochaine version du questionnaire ou le questionnaire de la tranche d’âge suivante.

Il s’agit de d’accompagner l’usager dans la collecte des données pertinentes qui permettront un échange facilité avec les professionnels de santé mais également de proposer, s’il y consent à disposer de contenus / conseils santé et bien-être plus adaptés via son Mon espace santé, lesquels pourront engager l’usager dans d’autres actions : prendre un rendez-vous, entamer le suivi d’une mesure, l’appariement d’une application tierce etc.

Carnet de santé de l’enfant

Dès 2023, Mon espace santé évolue pour devenir le carnet de santé numérique des enfants. L’IHM des Mon espace santé des mineurs sont travaillées pour proposer des parcours spécifiques aux parents. Le grand public étant attaché au carnet de santé papier, cette transformation des usages s’inscrit dans le temps long. Les carnets papier et numérique cohabitent. Le carnet de santé numérique est doté de propositions de valeur similaires au carnet papier : contenus adapté en fonction de l’age de l’enfant, présentations des contenus qui répondent aux questions des parents, bibliothèque de conseils, etc, à l’instar de tout ce qui est proposé dans le carnet de santé papier. Le carnet de santé numérique apporte en plus les fonctionnalités augmentées par le potentiel du numérique : rappels, incitations dynamiques, conseils personnalisés et adaptés, etc.

### Sites et portails autour de Mon Espace Santé

#### Site institutionnel Mon Espace Santé

Un portail web est mis à disposition du grand public. Ce site affiche d’une part un contenu informationnel commun à tous, des informations relatives à Mon Espace Santé, la liste de l’ensemble des services tiers référencés, etc. Il s’agit également de mettre à disposition des informations ciblées aux usagers.

#### Portail de support Mon Espace Santé

##### Niveaux de support

Afin d’assurer le support de Mon espace santé, un workflow précis est défini pour préciser les modalités de la coordination entre les différents acteurs du processus de support.

Les grands principes de l’organisation du support sont les suivants :

Au niveau 0, les assurés peuvent résoudre leurs problématiques via les notifications reçues par email/courrier ou le site monespacesante.fr notamment par le biais de la rubrique Aide.

S’ils ne trouvent pas de réponse à leurs questions via ces médias, les usagers peuvent contacter le support de niveau 1 Mon espace santé via 2 canaux : le canal téléphonique ou le formulaire de contact :

* + Le support téléphonique (34 22) :
  + Les téléconseillers du 34 22 interviennent sur les motifs de contact suivants : des informations générales sur le service, l’enrôlement, des demandes d’opposition ou de clôture, des renseignements sur le dossier / dépannage, l’aide à l’usage.
  + La Cnam gère ces questions de niveau 1 via un prestataire externe –géré hors de cet accord cadre- et ses CPAM de manière ponctuelle. Les questions de niveau 1+ sont traitées par des CPAM spécifiquement mobilisées dans ce cadre, pour les assurés du Régime Général, ou par la MSA pour les usagers MSA, Assemblée Nationale & Sénat, RATP et SNCF.
  + Le formulaire de contact, accessible sur le site monespacesante.fr après connexion de l’usager : Les formulaires de contact sont reçus et traités par la CPAM du Puy-de-Dôme. Ceux-ci portent sur des demandes d’informations générales sur le service, d’aide à l’usage ou d’intervention sur le dossier / dépannage.
  + Le niveau 2 de support est assuré selon la partie du système d’information concerné, par la Cnam elle-même, le titulaire en charge de Mon espace santé ou le titulaire du DMP. Il permet l’analyse technique des tickets escaladés depuis le niveau 1 et le cas échéant l’adressage vers le niveau 3.
  + Le niveau 3 concerne quant à lui d’autres acteurs et des systèmes d’information intervenant indirectement dans les processus Mon espace santé, comme par exemple des tickets concernant des acteurs de la gestion des bénéficiaires Cnam ou autre régime utilisés pour les services d’Enrôlement, ou d’identification (service de n° de série carte Vitale, service de coordonnées, etc.)
  + Pour les incidents techniques et sécurité de la plateforme de Mon espace santé, le titulaire responsable du périmètre Mon espace santé assure l’ensemble des niveaux de support.

##### Moyens d’authentification et de connexion

Les agents du support externes se connectent au portail de support via ID / mot de passe + un otp mail en tant que second facteur d’authentification (impliquant l’enrôlement de leur adresse mail).

Les agents du support interne Cnam ou MSA se connectent au portail de support via SSO à partir de leur identification interne professionnelles, cette connexion s’appuie sur le protocole interops.

##### Informations manipulées

Le support répond aux interrogations de l’usager concernant le statut de son comptes profil Mon Espace Santé et DMP, la liste des délégataires, le statut « demande de rematérialisation » et l’historique des tickets.

Il dispose aussi d’informations sur le demandeur, dans l’éventualité où celui-ci n’est pas titulaire de l’Espace Santé concerné par la demande sur lequel il doit quand même impérativement disposer d’une délégation d’accès, telles que les coordonnées personnelles et les informations listées précédemment.

##### Actions du support

* + Les actions du support de niveau 1 sont les suivantes : Opposition, Clôture, Désappariement d’une application référencée appariée précédemment à un Mon espace santé (catalogue de services), Dissociation des appareils enrôlés (connexion à Mon espace santé par biométrie ou autre facteur d’authentification géré par le device mobile lui-même), Annulation demande de suppression de données Mon espace santé , Création d’un ticket d’escalade.
  + Ceux des niveaux supérieurs peuvent être : Suppression données Mon espace santé , Rematérialisation données Mon espace santé.

Lors de la création des tickets, il est possible de les caractériser en indiquant : une application et une offre de service, la gravité, une information sur l’accord donné ou non par l’usager sur la consultation de ses traces. Ces informations permettent de flécher le traitement des tickets en fonction de leur nature au bon niveau et au bon interlocuteur dans le cadre du workflow de traitement de la demande de l’usager.

##### Cycle de vie d’une demande

Un agent peut réaliser plusieurs actions : abandonner un ticket, l’escalader, le transférer, le dupliquer, le clôturer, l’annoter, visualiser le contexte du bénéficiaire, contacter l’usager, effectuer différentes recherches sur les tickets.

Lorsqu’une demande est escaladée, elle peut être clôturée, à nouveau escaladée, abandonnée, retournée ou un ticket peut être créé.

##### Pilotage du support et traces

Le pilotage est réalisé à plusieurs niveaux :

* + Pilotage à chaud : Volumétrie en temps réel, par statut des tickets ou des demandes, par plateau d’affectation des agents ou par régime d’appartenance des usagers sur l’ensemble tickets et des demandes de la base ;
  + Pilotage à froid (demande) : Un seul fichier quotidien est généré, contenant des informations telles que le motif de contact de la demande, le régime de l’usager, Volume d’entrée à J-1, etc. ;
  + Pilotage à froid (ticket) : Un seul fichier quotidien est généré avec les informations telles que les applications, les offres de service, les tickets crées à J-1, escaladés ou retournés, etc.

Toutes les actions du support doivent être tracées et consultables par l’usager.

##### Outillage du support

Pour l’ensemble des niveaux de support, un outil est nécessaire pour assurer le support aux services proposés dans le cadre de Mon Espace Santé. Un outil a été développé spécifiquement pour cet usage : PSN1.

Ainsi, le Titulaire reprend l’outil PSN1 (actuellement utilisé) ou propose un outillage comprenant, a minima, les mêmes fonctionnalités. Il s’agit d’un des sujets sur lesquels la Cnam attend des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

Cet outil doit permettre aux plateformes support de :

* + Consulter les données relatives au compte-profil Mon espace santé du demandeur après sécurisation de son identité et d’apporter des réponses ;
  + Effectuer les actions de niveau 1 ;
  + Escalader et tracer les dossiers nécessitant une analyse et une expertise plus importante vers le Niveau 2-3, via une fonctionnalité de ticketing ;
  + Recevoir et traiter les formulaires de contact envoyés par les usagers depuis leur profil Mon espace santé ;
  + Piloter l’activité.

L’outil doit par ailleurs s’interconnecter avec les outils de ticketing de niveau 3.

L’outillage de support de niveau 1 sert d’appui à l’ensemble des services proposés aux utilisateurs.

Cet outillage doit proposer les fonctionnalités suivantes :

* + Un accès sécurisé avec un niveau d’authentification fort ;
  + Une capacité de traçage de toutes les actions entreprises dans le cadre du support (pour tous les niveaux) ;
  + Une base documentaire sur laquelle les opérateurs peuvent s’appuyer pour optimiser leur prise en charge des tickets, et à laquelle ils p également contribuer ;
  + Un module de pilotage / reporting de gestion des demandes, incidents et problèmes ;
  + L’interfaçage avec les outils de gestion des tickets-demandes / incidents de la Cnam est demandé, et est précisé dans le cadre de la définition du workflow complet de support ;
  + Toute évolution technologique permettant d’améliorer le service rendu à l’usager et l’efficacité des équipes en charge du support peut venir compléter ces modalités.

La valorisation des développements utiles à l’outillage du support (N1,N1+, N2 et N3) (y compris avec les outils Cnam) est comprise dans la prestation P5 - Run\_MCO-S : Run, MCO et MCS ». Les développements concernant les connecteurs avec l’ecosystème hors SI-Cnam font l’objet de commandes sur la base d’UO.

##### Outillage du Support aux éditeurs

Dans le courant de 2023, avec l’ouverture du catalogue de services avec échanges de données, le support aux éditeurs est inclus dans le workflow de traitement des demandes (tickets d’incidents en provenance des éditeurs à la fois dans le cadre de leur processus de référencement et dans le cadre de l’exploitation en production. Les fonctions administration de cette nouvelle branche de support seront affinées lors de l’ouverture du catalogue de services, à partir de juillet 2023.

#### Portail d’Administration du Catalogue de Services (PACS) Mon Espace Santé

Le Portail d’Administration du Catalogue de Services (PACS) a pour objectif de gérer le contenu et les informations affichées dans le Catalogue de Services pour des services numériques référencés, qu’ils soient avec ou sans échange de données. Il permet de créer et paramétrer les différentes finalités avec l’éventuel échange de données réalisé par le service numérique référencé. Cet outil est, à date, à destination du GIE SESAM-Vitale, qui est le pilote du processus du référencement avec l’Agence du Numérique en Santé, ainsi qu’à destination du Titulaire de l’accord-cadre.

La finalité de ce PACS est de mettre en ligne les fiches des services numériques référencés sur le catalogue de services Mon espace santé avec l’ensemble des informations et paramétrages nécessaires à leur bon fonctionnement.

Ce PACS est installé à la fois en production et sur un environnement spécifique dit Editeur afin de gérer les tests d’homologation technique d’un service candidat au référencement sur Mon espace santé.

Il permet également de suivre le workflow des états d’une fiche solution jusqu’à son potentiel déréférencement (création de la fiche du service numérique, début des tests sur l’environnement Editeur, homologation du service numérique, mise en ligne de la fiche en production, suspension d’une fiche, déréférencement d’une fiche).

#### Site d’information pour le référencement éditeurs Mon Espace Santé

Ce site permet d’initialiser le parcours des éditeurs dans les différentes étapes du processus de référencement de leurs services. Il vise à leur offrir l’accès à l’ensemble des informations leur permettant d’intégrer le parcours de référencement (critères de sélection, étapes, etc.), la documentation nécessaire à leur référencement (guide du référencement, formulaires de référencement, exigences techniques pour l’échange de données, les spécifications techniques des API, la charte d’intégration graphique et une FAQ). Enfin, ce site de demande de référencement vise à orienter les éditeurs dans le parcours de référencement. Une fois référencés, les services sont publiés et accessibles via ce site.

Il permet également d’afficher l’ensemble des services numériques référencés ainsi que les documents liés à leur référencement (PV de commission de référencement, les délibérations, certaines pièces justificatives des dossiers…).

La documentation publique des API liées à l’échange de données ainsi que le guide d’implémentation associé sont également publiés sur cette page.

A partir du second semestre 2023, des travaux sont engagés entre les acteurs institutionnels du processus de référencement pour dessiner plus précisément le rôle et les services associés à ce site, en articulation avec les services proposés par l’ANS dans le cadre de la plateforme Convergence notamment.

#### Content management system (CMS)

Certaines pages de Mon espace santé sont adossées au CMS Drupal (content management system).

A date, les pages concernées sur MES sont :

* + Site institutionnel et les pages qui y sont rattachées (CGU, accessibilité, aide en ligne, etc.)
  + Page d’accueil connectée (message de prévention)
  + Bandeau d’alerte sur la page d’accueil et site institutionnel
  + Carte vaccination du profil médical
  + Matrice d’habilitation du DMP
  + Gestion des services référencés dans le menu catalogue de service
  + Site institutionnel du catalogue de services (editeurs.monespacesante.fr)
  + Contenu du support (gestion des motifs et des réponses types).

Ce CMS permet de gérer différents types de contenus, du texte dont des liens internes à Mon Espace Santé ou externes, des illustrations notamment.

### Indicateurs métier

Au niveau de la supervision métier, la solution fournit un ensemble d’indicateurs clé permettant de mesurer la performance et de s’assurer que MES et le DMP répondent aux exigences des services proposés par la puissance publique (disponibilité, temps de réponse, etc.). Cette solution doit pouvoir s’interfacer avec les outils de gestion de support de la Cnam :

* + Suivi des usages : ces indicateurs visent à évaluer de manière générale l’efficacité du service proposé aux usagers. Il s’agit de mesurer d’une part l’audience et l’engagement des usagers dans MES (exemple : nombre de connexions, nombres d’actions liées aux fonctionnalités, etc.) et d’autre part, la facilité d’usage et la performance des contenus (exemple : durée moyenne par visite, les pages suscitant le plus d’intérêt, etc.). Pour assurer la pertinence de ce suivi et offrir une vision plus complète, ces données doivent être couplées à d’autres informations provenant de sources externes comme les appels au support, les retours des professionnels utilisant les fonctionnalités miroir du BSP, etc. L’objectif final est de définir les points de frictions et les difficultés rencontrés par l’usager et de proposer des solutions adaptées permettant d’optimiser son parcours au sein de MES.
  + Un outillage performant, ergonomique, esthétique, riche en composants (permettant a minima la génération des principaux types de graphiques et tableaux avec tri et filtres dynamiques), sécurisé, flexible, personnalisable, interopérable (export csv), doit être mis à disposition pour restitution des données d’usage et pour les mesures d’audience. (Plusieurs solutions peuvent cohabiter, par exemple : une solution de Business Intelligence (BI) pour les usages et une solution pour les mesures d’audience)
  + Suivi de l’efficience du produit du point de vue des utilisateurs : en complément du suivi des usages, il permet d’améliorer l’expérience utilisateur en définissant des indicateurs de suivi de l’accessibilité et de la disponibilité du service (supports les plus utilisés, temps de chargement des pages, durée d’indisponibilité, etc.). Il s’agit également d’évaluer le référencement de MES à travers des indicateurs SEO. L’outil permet de monitorer la performance globale du produit MES, incluant le respect des SLA et le suivi des anomalies rencontrées en production sur l’ensemble de la chaîne applicative.
  + Un outillage performant, ergonomique, esthétique, riche en composants (permettant a minima la génération des principaux types de graphiques et tableaux avec tri et filtres dynamiques), sécurisé, flexible, personnalisable, interopérable (export csv), devra être mis à disposition pour restitution des données d’usage et pour les mesures d’audience. (Plusieurs solutions peuvent cohabiter : par exemple : une solution pour BI pour les usages et une solution pour les mesures d’audience)

Pour les besoins du métier, en particulier dans le cadre de sa relation avec le client, le métier souhaite disposer d’une visibilité sur la supervision du service : des outils affichant des informations en temps réel de disponibilité des services et de suivi des erreurs sont mis en place. Les temps de réponses des services doivent pouvoir être mesurés de manière automatique.

Pour MES, actuellement le SI PILotage s’appuie sur l’outil Knowage mais nécessite beaucoup d’actions manuelles pour permettre d’obtenir les résultats attendus pour mener un pilotage fin comme attendu.

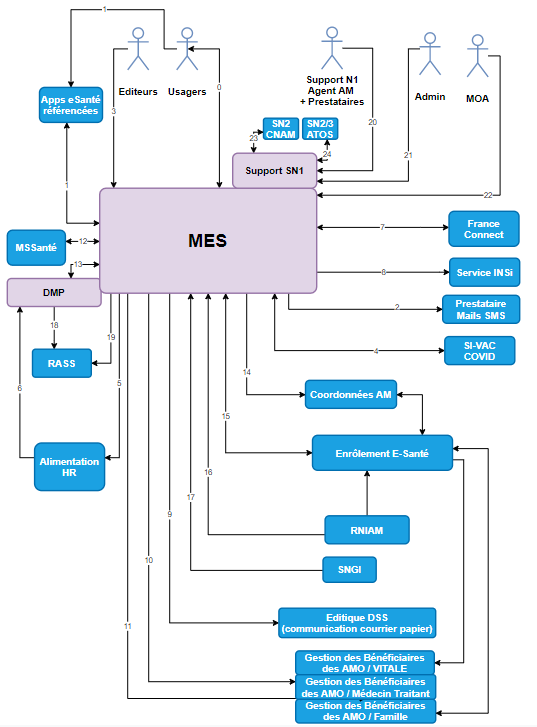
Le Titulaire de l’accord-cadre doit proposer et mettre en place un outil de suivi et de pilotage de l’activité sur MES (cf. EXG\_FON\_19).

## Présentation du périmètre technique MES

### Présentation générale de l’architecture de MES

Ce chapitre permet d’avoir une vision globale de MES et de ses interractions avec les différents systèmes d’informations partenaires.

#### Interfaces externes



Source : Annexe « MESDMP\_Annexe 22\_MES-Matrice des flux » Fig. Archi-01

Mon Espace Santé est un système possédant des interactions avec d’autres systèmes d’information.

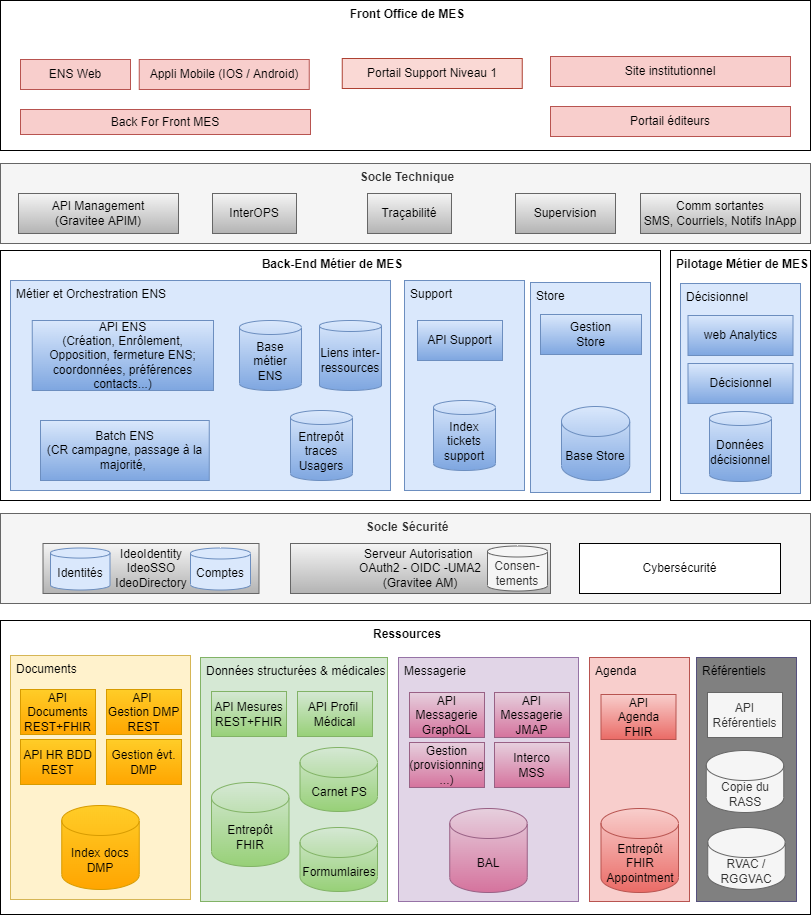
Ci-dessous se trouvent une brève description des flux tels que décrits sur la figure Archi-01 :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Composant | Commentaire | Déclenchement du flux vu de MES | Type déclenchement | Origine du déclenchement |
| 0 | Usagers | Appels des frontaux vers MES  - Accès à toutes les APIs d'usage publiques exposées par la couche métier de MES  - Probablement accès à certaines APIs non ouvertes aux apps eSanté | entrant | unitaire | utilisateur |
| 1 | Apps eSanté référencées | En fonction des cas, accès aux API Suivantes :  - Authentification (Cas d'usage de sso sur la base de l'authentification MES) et Appariement des comptes  - Consentement (Pour la gestion des accès aux ressources)  - Les Ressources MES (documents, données structurées, messagerie, agenda) | entrant | unitaire | utilisateur |
| 2 | Prestataire Mail SMS | Communications sortantes Mails et SMS  - Authentification (via OTP)  - Notifications eSanté (dépôt de document, message…) | sortant | en masse | Par MES sur événements |
| 3 | Editeurs | Industriels :  - Fournisseurs de Dispositifs médicaux  - Quantify Yourself  - Fournisseurs de services eSanté  Cas d'usage :  - Enrolement des services / apps eSanté au sein de l'écosystème de MES  - Spécification des flux possibles pour la demande de consentement aux titulaires  - Validation des services / apps eSanté et des flux possibles pour la demande de consentement aux titulaires | entrant | unitaire | Editeurs |
| 4 | SI-VAC COVID | Récupération des attestations de vaccination à l'activation | entrant | unitaire | SI-VAC |
| 5 | Alimentation HR | Pilotage de l'alimentation HR | sortant | unitaire | par MES suite à une activation |
| 6 | DMP | Dépôt du HR vers le DMP | entrant | unitaire | Middle Office HR DMP |
| 7 | FC | Vérification du jeton d'identité FC | sortant | unitaire | utilisateur |
| 8 | INSi | Téléservice pour effectuer la réconciliation d'identité sur la base des traits d'identité lors de la première authentification FC uniquement | sortant | unitaire | par MES à la suite d'une authent de l'utilisateur |
| 9 | Editique DSS | Courriers postaux liés à des campagnes E-Santé (prévention,…), au respect des obligations d’information RGPD, … | sortant | en masse | batch de MES |
| 10 | Benef AMO/MT | Changement liés aux droits à l'Assurance Maladie (choix du médecin traitant,…) | entrant | unitaire | SI Interrégime (CNAM) |
| 11 | Benef AMO/Famille | Récupération de la famille de droit (lien Ouvrant Droit / Ayant droit) pour initier le représentant légal présumé | entrant | unitaire | SI Interrégime (CNAM) |
| 12 | MSSanté | Pour s'interfacer avec les BAL des PS sur l'ecosystème MSSanté, il est nécessaire que la ressource Messagerie / Espace d'échange de MES implémente une façade d'accès à l'écosystème MSSanté de la même manière que les opérateurs MSSanté doivent le faire actuellement. Cela ne présage pas de la manière dont la messagerie est implémentée dans MES. C'est néanmoins obligatoire pour se connecter à MSSanté. | entrant | unitaire | Utilisateur  PS |
| 13 | SI DMP | Notifications pour utilisation de la comm sortante  Traces  Evenements issus du DMP | entrant | unitaire | suite à changement d'état sur le DMP (par exemple) |
| Les accès depuis le SI DMP couvrent les cas suivants :  - Notifications réglementaires  - Evenements  - Validation authentification  - Validation habilitations  - Récupération des traits d'identité | entrant | unitaire | utilisateur |
| Les accès au SI DMP couvrent les cas suivants :  - Gestion du DMP d'un titulaire  - Consultation et versement de documents  - Consultation et alimentation des données structurées  - Accès aux traces du DMP  - Vérification des accès au niveau du socle de sécurité  - Accès à la copie du RASS dans le SI DMP | sortant | en masse | MES |
| Création initiale  - Gestion des DMP | sortant | en masse | MES |
| 14 | Coordonnées AM | Récupération des coordonnées fiabilisées des AMO en cas d'absence ou d'obsolescence des coordonnées e-santé dans MES | sortant | unitaire | utilisateur |
| 15 | Enrôlement eSanté | Authentification de l'usager lors de la phase d'enrôlement. | sortant | unitaire | utilisateur |
| Déclenchement des créations auto d'MES | entrant | en masse | batch CR notif à la CNAM |
| 16 | RNIAM | Changement d'affiliations aux régimes d'Assurance Maladie (naissances, autres entrées/sorties) | entrant | Unitaire | batch à la CNAV |
| 17 | SNGI | Changement liés aux données de l'état civil (décès...) | entrant | en masse | batch à la CNAV |
| 18 | RASS | Récupération des informations PS | entrant | unitaire | DMP |
| 19 | RASS | Récupération des informations PS | entrant | unitaire | MES |
| 20 | PSN1 Support | Accès par les agents des plateforme support niveau 1 à l'outillage de GRC MES | entrant | unitaire | Agent |
| 21 | PSN1 Admin | Accès par les agents administrateurs à l'outillage de GRC MES | entrant | unitaire | Agent |
| 22 | Usages MES | Accès par les agents MOA à l'outillage de BI MES | entrant | unitaire | Agent |
| 23 | ITSM N2 CNAM | Escalade support N1 MES vers support N2 Cnam | sortant | unitaire | PSN1 |
| 24 | ITSM N2/N3 ATOS | Escalade support N1 MES vers support N2 ATOS (le cédant = titulaire de l’accord-cadre n°AC.2020.1324) | sortant | unitaire | PSN1 |

#### Composants Internes

Mon Espace Santé se compose de différents sous-systèmes permettant d’en assurer l’intégralité des fonctionalités.

Le schéma ci-après regroupe ces sous-sytèmes par grandes zones applicatives.



Source : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End » Fig Archi-02

Zone « Front Office de MES » :

Cette zone contient les différentes interfaces utilisateurs permettant les accès à MES pour les différentes populations (Grand Public, Usagers, Agents du support, Editeurs de services tiers, etc.).

Le Back For Front (BFF) est également inclus dans cette zone.

Zone « Back-End Métier de MES » :

Cette zone contient l’ensemble des logiques métier nécessaires à MES pour rendre les services attendus et accessible via la zone Front Office.

Les traitements de masse nécessaires au maintien opérationnel de MES, à la qualité/fraicheur des données et à la gestion du cycle de vie des Espaces de Santé individuels font également partie de cette zone.

Zone « Pilotage Métier de MES » :

Cette zone contient les dispositifs de Business Intelligence permettant de produire les indicateurs clés de pilotage des usages de MES.

Zone « Ressources » :

Cette zone contient les ressources utilisées par MES et accessibles à un usager de MES.

Elle contient également des gisements de données de référence.

Zone « Socle Technique » :

Cette zone regroupe l’ensemble des dispositifs techniques permettant à MES d’interagir avec d’autres systèmes d’informations, de maîtriser et superviser l’opérationnalité de MES et d’offrir les moyens nécessaires au respect des exigences de traçabilité du système MES.

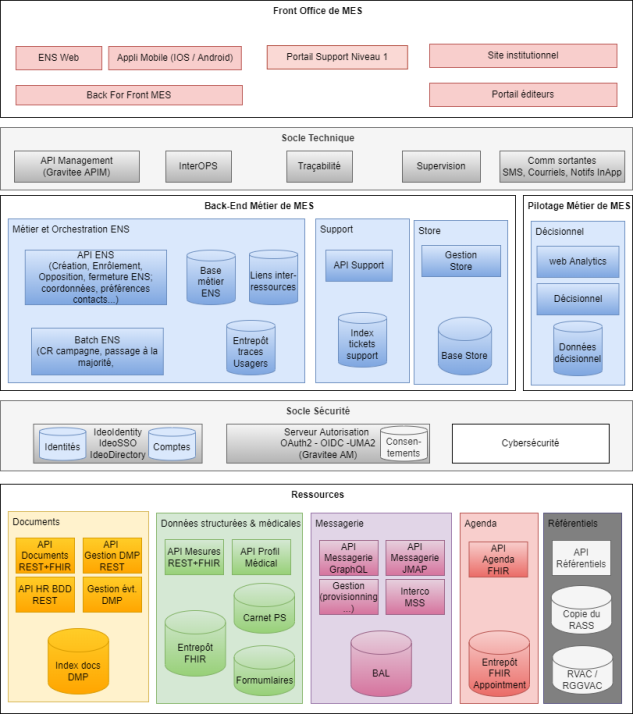
Zone « Socle Sécurité » :

Cette zone regroupe l’ensemble des dispositifs, API et gisements nécessaires à la mise en œuvre de la sécurité au sein de MES.

### Présentation détaillée de l’architecture de MES

NB : Pour une meilleure compréhension et exhaustivité de l’existant, le schéma de présentation générale des composants internes de MES (Fig. Archi-02) du chapitre précédent a été légèrement modifié et restructuré par rapport aux schémas existants dans la documentation architecturale opérationnelle de MES qui est référencée en annexe : les renvois vers les chapitres des annexes peuvent donc ne pas suivre une logique totalement « linéaire ».

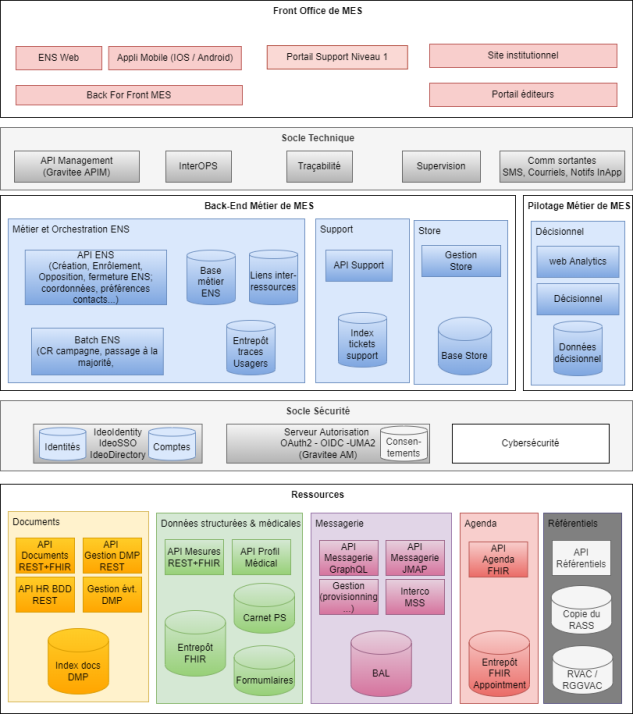
#### Front Office de MES



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + ENS Web : Annexe « MESDMP\_Annexe 17\_MES-Dossier Architecture Logicielle Front-End »: §5.2
  + Appli Mobile : Annexe « MESDMP\_Annexe 17\_MES-Dossier Architecture Logicielle Front-End »: §5.4
  + Back For Front MES : Annexe « MESDMP\_Annexe 17\_MES-Dossier Architecture Logicielle Front-End »: §5.3
  + Site Institutionnel : Annexe « MESDMP\_Annexe 17\_MES-Dossier Architecture Logicielle Front-End »: §5.5
  + Portail éditeurs : Annexe « MESDMP\_Annexe 17\_MES-Dossier Architecture Logicielle Front-End »: §5.6
  + Portail Support Métier N1 : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: § 6.8.2

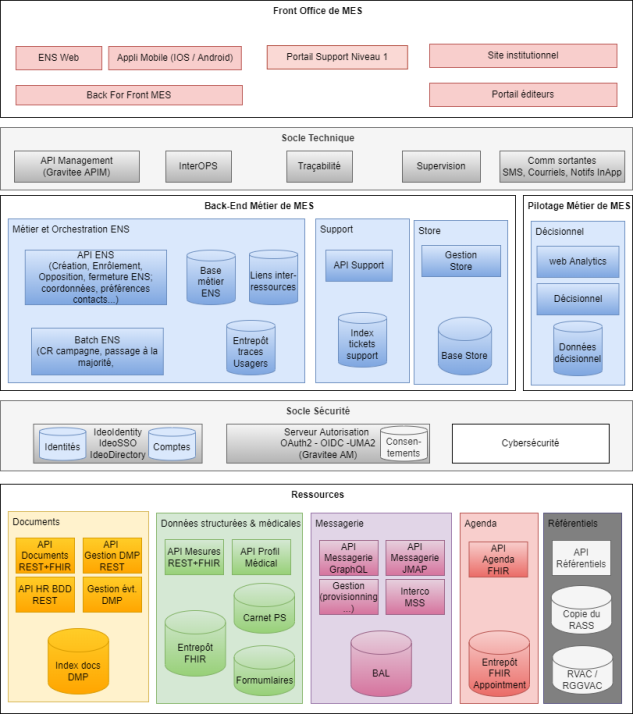
#### Back-End Métier de MES



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + Métier et Orchestration ENS : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End » : §6.2.2.2, 6.4.1, 6.4.2, 6.4.5, 6.4.6, 6.7.6
  + Support : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End » : §6.8
  + Store : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End » : §6.10

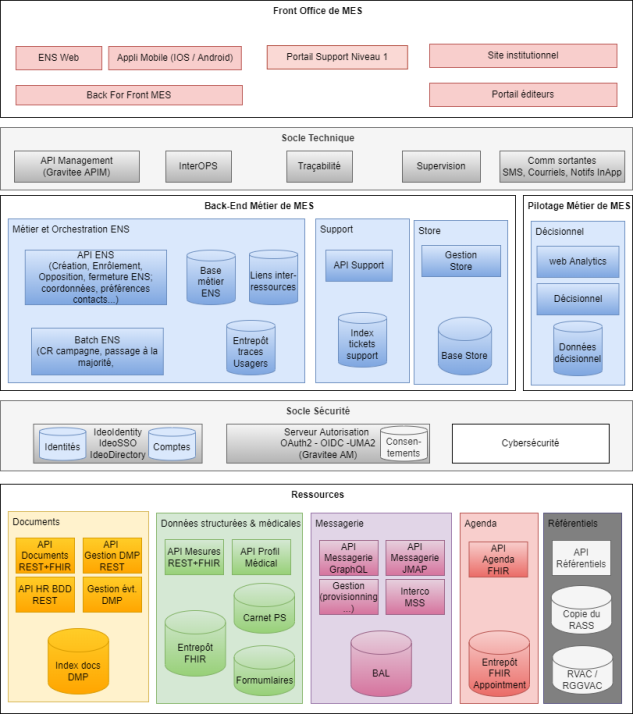
#### Pilotage Métier de MES



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + Web Analytics : Annexe « MESDMP\_Annexe 17\_MES-Dossier Architecture Logicielle Front-End »: §6.4.4
  + Décisionnel : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.4.3

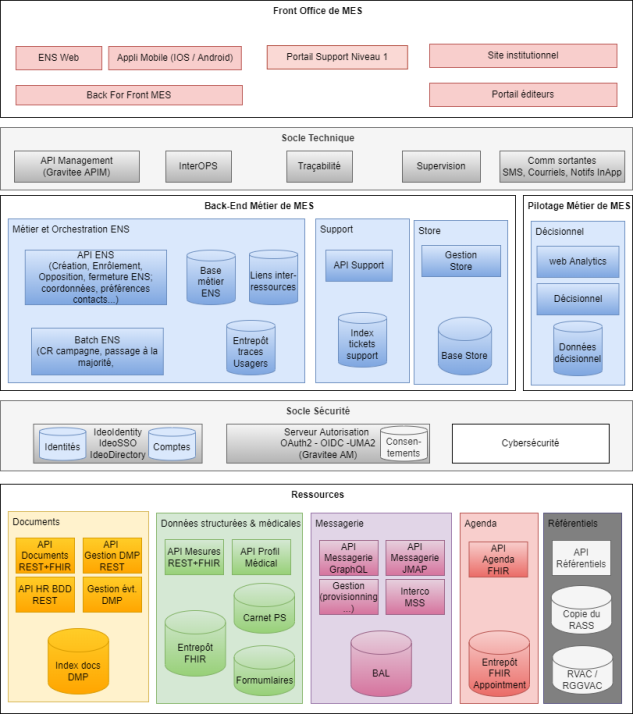
#### Ressources



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + Documents : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.5
  + Données Structurées & Médicales : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.7
  + Messagerie : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.6
  + Agenda : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.9
  + Référentiels : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.12

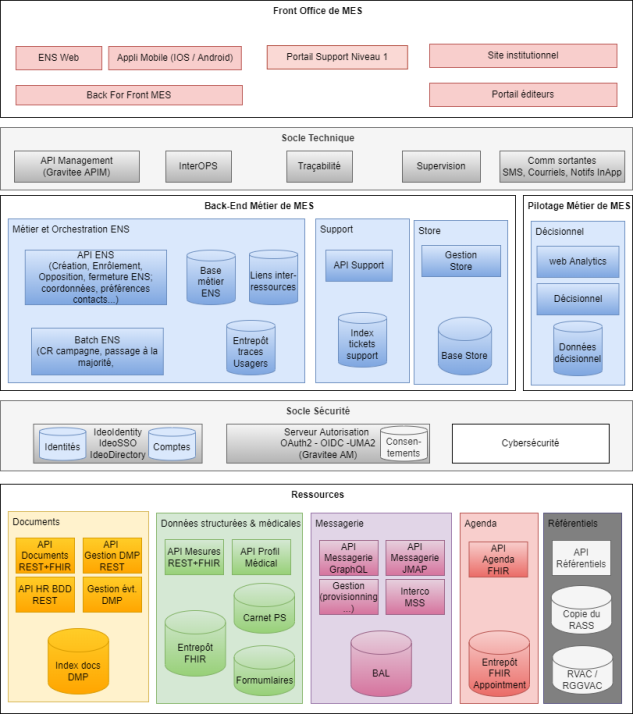
#### Socle technique



L’ensemble du détail des éléments d’architecture relatifs à cette zone se trouve dans les documents suivants :

* + API Management : Annexe MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.2.1
  + InterOPS : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.2.5
  + Traçabilité : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.2.2
  + Supervision : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.2.3
  + Communication Sortante : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.2.4

#### Socle sécurité



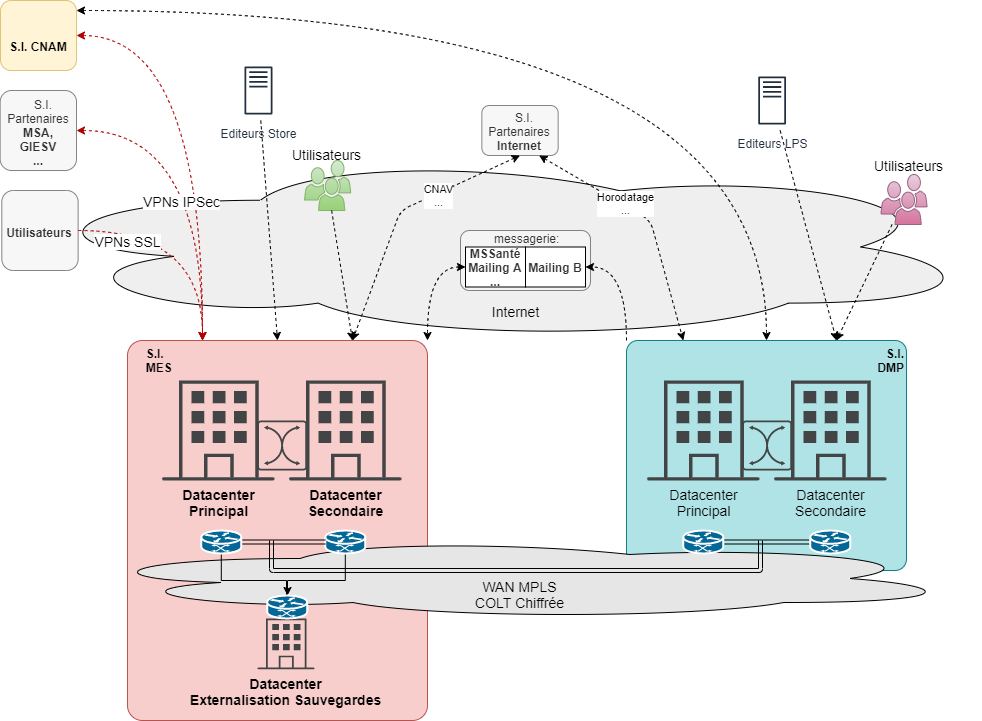
L’ensemble du détail des éléments d’architecture relatifs à cette zone se trouve dans les documents suivants :

* + Identités et Compte : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End » : §6.3.1, §6.3.3
  + Authentification et Access Management  : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.3.1
  + Consentements : Annexe « MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End »: §6.3.2

### Architecture Technique de MES

#### Aperçu MES+DMP

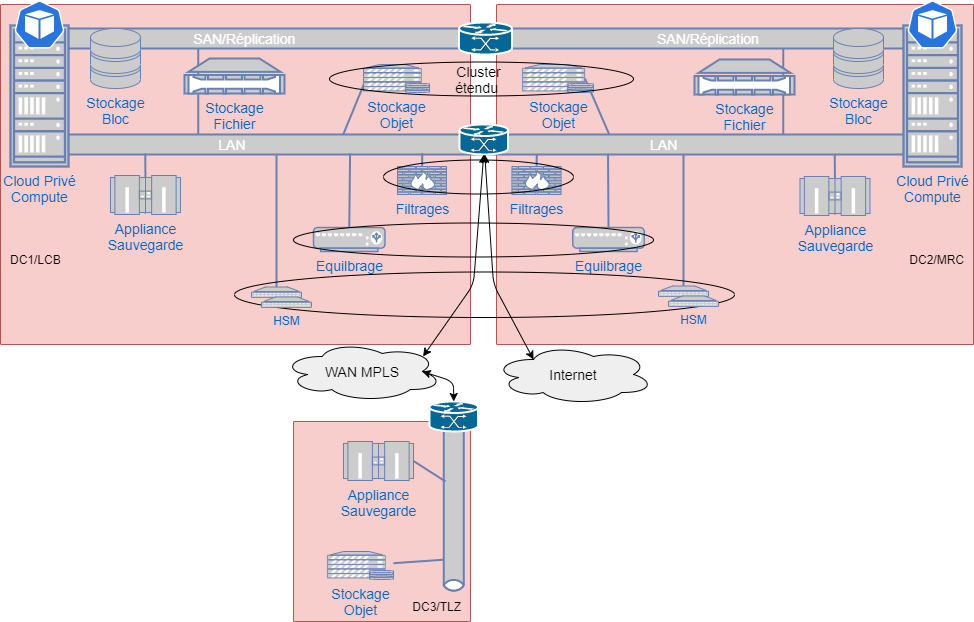
Actuellement les hébergements de MES et du DMP sont confiés à deux Titulaires différents.



Le MES et le DMP sont l’un et l’autre déployés sur deux datacenters propres à chacun des deux hébergeurs auxquels ils ont été confiés. Au sein d’une paire, les datacenters sont interconnectés. Les deux paires de datacenters sont raccordées par le biais d’un WAN MPLS COLT.

Chaque hébergeur s’appuie sur sa propre infrastructure redondante, sécurisée, pilotée, pour son raccordement à Internet.

#### Présentation générale de MES



Principaux composants de l’infrastructure MES :

* + Deux datacenters principaux situés en région parisienne.
  + Un troisième datacenter destiné aux sauvegardes, à 250 km des précédents.
  + Des équipements de réseaux, de filtrage (Firewall, WAF), d’équilibrage, en cluster étendus sur les deux datacenters.
  + Une infrastructure Cloud privé (VMWare) de serveurs, répartie sur 2 zones de disponibilité en actif/actif.
  + Plusieurs instances d’une plateforme d’orchestration de conteneurs installées chacune sur un cluster de VMs.
  + Un stockage bloc et fichier (NAS) répliqué entre les 2 datacenters.
  + Une plateforme de stockage objet, basée sur le logiciel Open Source Ceph, étendue sur les deux datacenters. Elle est dédiée au contenu des boites aux lettres de la messagerie proposée par MES.
  + Une sauvegarde croisée des stockages bloc et fichier entre les datacenters principaux, sauvegarde externalisée sur le 3ème datacenter.
  + Une externalisation du stockage objet sur le 3ème datacenter.

#### Description détaillée de MES

##### Les datacenters

Ils sont au nombre de trois :

* + Les deux datacenters principaux, situés en région parisienne sont montés en « dual-site ».
  + Le troisième, destiné principalement à l’externalisation des sauvegardes, est situé à plus de 250 kms des précédents.

Le dimensionnement et les équipements de chacun des deux datacenters principaux leur permettent de rendre seul le service ainsi que de supporter la totalité de la charge de MES en cas d’indisponibilité du second datacenter.

Ils fournissent des services mutualisés et sécurisés :

* + Accès à Internet : plage d’adresses publiques, multiples FAI, disponibilité via BGP, anti-DDOS, garantie de bande passante minimale (1Gbps pour MES).
  + Dual-site : interconnexion point à point de niveau 2, via boucles optiques redondées.
  + Infrastructure d’accès destinée aux exploitants et administrateurs de l’hébergeur. Une solution non mutualisée à destination d’une sous-population d’administrateurs est en cours d’étude.
  + Zone d’interconnexion entre les environnements mutualisés de l’hébergeur et les infrastructures dédiées à MES.
  + Monitoring centralisé.
  + Hébergement des infrastructures et services spécifiques à MES (HDS).

##### Les environnements

Il y a 2 types d’environnements :

* + L’environnement de production.
  + Les environnements hors-production.

Les ressources physiques et logiques situées sur l’infrastructure dédiée par l’hébergeur à MES sont dans leur grande majorité affectées uniquement à l’un des deux types d’environnements précédents :

|  |  |
| --- | --- |
| Partage/Dédié | Ressources |
| Présents sur l’environnement de production uniquement. | Certains éléments de sécurité spécifiques (sondes et matériels SIA, etc.). |
| Ressources matérielles partagées par les 2 types d’environnements. | Les équipements éthernets.  Les clusters de filtrage (Firewalls Zone Front/Zone Back, WAF).  Le cluster de répartition de charge.  La Baie de stockage.  Le Système de sauvegarde. |
| Ressources matérielles dédiées à un 1 seul type d’environnement. | Châssis.  Eléments de calcul (lames, etc.).  Cluster HSM avec KMS embarqué.  Cluster Ceph. |
| Ressources logiques partagées par les 2 types d’environnements. | Les 2 Clusters VMWARE par datacenter d’administration et outillage.  La « Route Domain » Zone Front du répartiteur de charge. |
| Ressources logiques dédiées à un 1 seul type d’environnement. | La « Route Domain » Zone Back du répartiteur de charge.  Les LUNs et datastores , etc.  Les 4 cluster VMWARE par datacenter, « applicatifs ».  Les 2 cluster d’orchestration de containers (OpenShift) par datacenter.  Les bastions WALLIX.  Les VLAN. |

##### Les éléments réseau et sécurité

De façon générale, sauf cas d’exception précisés ci-dessous, il s’agit de deux boitiers physiques (1+1), un par datacenter, fonctionnant en haute disponibilité, en mode actif/passif (A/P). Celui qui est actif peut l’être au sein d’un datacenter alors que les autres ressources (réseau, compute, etc.) sont opérationnelles au sein du second datacenter. La bascule est automatique, sans perte de session.

|  |  |
| --- | --- |
| Catégorie | Référence |
| Filtrage réseau Zone Front (1+1 - A/P) | Firewall Juniper intégrant une fonction IPS |
| Filtrage réseau Zone Back (1+1 - A/P) | Firewall Fortinet |
| Filtrage applicatif (2+2 - A/A) | WAF Rohde&Schwarz |
| Répartiteur de charge (1+1 - A/P) | Big IP F5 |
| Passerelle VPN (1+1 - A/P) | Stormshield |
| Appliance SFTP d’admin (standalone) | Bertin |
| TAP et sondes IDS | Jizo |
| Conformité postes | Forescout |
| Boitiers HSM  (2+2 - A/A) Prod /  (1+1 - A/A) Hors-Prod1 / (1+1 - A/A) Hors-Prod2 | Utilisé pour le chiffrement et la pseudonymisation, le socle cryptographique est constitué par des boitiers HSM physiques redondés et d’un serveur de clé (KMS)  Boitiers HSM Trustway Proteccio |

A ceci s’ajoutent les équipements Ethernet, switchs cœur de réseau, les switch d’accès, etc.

Les éléments logiques du réseau :

* + 1 LAN étendu à travers les 2 datacenters principaux, il supporte les zones Front/Back/Sauvegarde.
  + 1 LAN sur le 3ème datacenter, il supporte les zones Back/Sauvegarde.

Ces LANs sont segmentés via des VLANs qui sont spécifiques à une zone.

La plage d’adressage IP utilisée sur l’infrastructure de MES est 10.38/16.

Il existe 3 types de flux, administration (PMAD et bastions), sauvegarde, applicatifs (tous les autres). Ils transitent par des VLANs distincts.

Les flux sont systématiquement filtrés au niveau inter-VLAN (Firewalls L3 Statefull, routeurs filtrants pour la sauvegarde).

Le nombre de VLAN, toutes zones confondues, est de l’ordre de 300.

La zone Front agglomère :

* + Les interfaces de MES : les DMZ accueillant les composants frontaux de MES (SFTP, SMTP, Proxy…).
  + Avec l’extérieur : Internet, VPN site-à-site avec les partenaires de MES, VPN SSL et IPSec Client, WAN MPLS avec l’hébergeur du DMP,

La zone Back accueille, dans différents VLANs, tous les composants internes de la solution ENS :

* + L’environnement de production et ceux de hors-productions.
  + Les serveurs applicatifs.
  + Les équipements d’infrastructure : management réseau, vCenter VMware, ESXi, etc.
  + Les machines de rebond et bastions internes.
  + Les servitudes (DNS, LDAP, etc.).

Le cluster de Firewall Front porte :

* + L’ensemble du routage/filtrage de tous les VLANs de la zone Front.
  + Les fonctions de passerelle VPN IPsec.
  + Les fonctions IDS/IPS.
  + Le nattage des adresse IP de MES vis-à-vis de l’extérieur (Internet, partenaires, DMP).

Le cluster de Firewall Back porte :

* + L’ensemble du routage/filtrage de tous les VLANs de la zone back et interzone.
  + L’accès au 3ème datacenter d’externalisation.

Le répartiteur de charge porte :

* + Une segmentation logique par 3 « Route Domain » (1 en zone front, 2 en zone back).
  + Une topologie « one arm » nécessitant l’usage du NAT source.

Le WAN MPLS Colt :

* + Interconnecte la zone Front avec le DMP (Datacenter Nominal + Datacenter PRA).
  + Interconnecte la zone Back avec le 3ème datacenter.
  + Chiffre les flux empruntant les interconnexions précédentes.

##### Les éléments de calcul

Dans chaque datacenter principal les éléments de calcul sont agglomérés en 3 groupes (châssis) disjoints, 2 sont dédiés à l’environnement de production, le 3ème aux environnements hors-production.

Ces éléments de calcul sont au nombre de 23 par datacenter. Selon le cluster de virtualisation VMWare auxquels ils sont associés (ESX), leurs configurations matérielles peuvent différer. Par élément de calcul :

* + Format lame
  + 2 processeurs
  + 20 à 40 cores par processeur
  + 768 à 1536 Go par lame.

L’ensemble des éléments de calcul présenté précédemment est intégré à une infrastructure vSphere sous licences vCloud Suite Enterprise et vCenter Server standard, version 7.x.

Dans un datacenter principal, les éléments de calcul sont répartis entre 6 cluster VMWARE monodatacenter :

* + Administration VMWARE : 2 ESX.
  + Outillages et services d’infrastructure : 2 ESX.
  + Environnements hors-production - système d’orchestration de containers : 4 ESX.
  + Environnements production - système d’orchestration de containers : 4 ESX.
  + Environnements hors-production – VM hors container : 6 ESX.
  + Environnements production - VM hors container : 5 ESX.

Les différents clusters sont dimensionnés de façon à ce que la perte d’un nœud ESX soit compensée par les nœuds restant.

Les éléments de calcul du second datacenter principal sont organisés de manière similaire.

Les 2 datacenters sont reliés par un domaine SSO unique, dans un « vCenter Enhanced Linked Mode ».

###### Les systèmes d’orchestration de containers

Les différentes instances du système d’orchestration sont construites sur une plateforme de container basée sur Kubernetes, celle supportée par Red Hat OpenShift Container Platform (OCP) V4.x.

Elles sont destinées à héberger les applications métiers MES conteneurisées ainsi que les outils de développement « forge ».

|  |  |
| --- | --- |
| Chaque cluster OCP est mono datacenter (non étendu).  Chaque cluster OCP de hors-production supporte plusieurs environnements.  Chaque clusters OCP est associé à un cluster VMware et utilise le cloud provider VMware pour déployer via VCenter les VM OpenShift Masters, Infrastructures et Workers.  L’accès aux applications métiers MES conteneurisées a lieu via les Global Load Balancer F5 qui répartissent la charge sur les Ingress Router localisés sur les nœuds d’infrastructure des 2 clusters OpenShift d’un même environnement . | C:\Users\FRANGIAMONE-30746\Documents\FFR\DOC\Projets\ENS\PAN\PAN2023\PAN-2023-FFR-OpenShift.png  + 3 VM master par cluster OPC |

|  |  |  |
| --- | --- | --- |
| Containers en environnement de production | Nombre de containers  Ordre de grandeur | Types, exemples |
| Logiciels (middleware…) | 30 | Ideo, Elastic, Drupal, Gravitee, varnish… |
| Applicatifs | 120 |  |

###### Les VMs hors container

Le fonctionnement de l’application ENS est centrée sur des PODS s’appuyant sur des composants middleware en VM avec des flux passant au travers de différents composants réseau dont des VIP assurant l’équilibrage et la haute disponibilité.

Les composants middleware sont :

* + Les bases métier PostgreSQL. Chaque domaine métier (Agenda, Store, Enrôlement, etc.) dispose d’un serveur qui lui est propre. Un serveur peut contenir plusieurs bases PostgreSQL différentes, elles même comportant plusieurs schémas différents en fonction des choix de conception applicative. L’architecture mise en œuvre utilise un serveur (VM) principal et un serveur secondaire en actif / passif avec transfert asynchrone des journaux transactionnels.
  + Le bus de données KAFKA. Il assure la fonction de messagerie applicative. Il est constitué de 3 serveurs sur le 1er datacenter (DC1), ce qui lui assure une haute disponibilité limitée à DC1. Protection par SRM/VMWARE pour reprise sur DC2, etc.
  + La Bases de données MongoDB. L’API manager Gravitee s’appuie sur une base MongoDB pour sa configuration. Il est constitué d’un cluster, étendu sur DC1&DC2, de 5 VMs réparties en 4 nœuds Data et 1 nœud témoin (protégé par SRM/VMWARE).
  + Les annuaires LDAP et SGBDR MySQL utilisés par Idéo (Authentification et SSO). MySQL est déployé sur un serveur primaire en DC1 et secondaire en DC2. OpenLDAP est déployé avec 2 instances, une dans chaque datacenter, en mode multi-master.
  + Les relais de messagerie en DMZ pour communication sortante. Destinés à un usage lors de la phase d’authentification, selon le choix de l’utilisateur un courriel ou un SMS avec un code OTP est émis. A l’heure actuelle, MES s’appuie pour ces émissions sur un service externe de l’opérateur SFR. L’envoi de courriel est réalisé par des relais SMTP « RET » en DMZ. La communication des PODS vers les serveurs SMTP s’effectue au travers d’un VIP en DMZ assurant à la fois équilibrage et haute disponibilité.
  + Les proxy Interops. Ils s’appuient sur la suite jeton (GIP-MDS) qui implémente le standard Interops. Ils sont utilisés pour les échanges, avec la Cnam principalement, sous les formes Interops-A et Interops-P. Ils portent les fonctions proxy/reverse-proxy et serveur de jeton V3. Une instance par datacenter derrière une VIP.
  + La messagerie Zimbra. Les VM sont déployées en une soixantaine d’instances composées chacune de : Jetty, Mariadb, openldap. Chaque VM prend en charge les boites aux lettres (jusqu’à 1 milion) d’une partie des assurés. Le « Message Store » s’appuie sur CEPH en mode objet. Chaque datacenter héberge 50% des serveurs. Ils sont protégés par SRM/VMWARE en cas de nécessité de reprise de la totalité des serveurs sur un seul datacenter par exemple.
  + Les relais de messagerie MSSanté. La communication avec la messagerie MSSanté est assurée par deux groupes de relais SMTP :
* Des serveurs MTA (Mail Transfer Agent, un par datacenter) simples relais en zone interne
* Des relais SMTP MSSAnté en DMZ. Des enregistrement MX publics (flux entrants depuis internet) et internes permettent une haute disponibilité.
  + Les relais SFTP. Les échanges fichiers sont assurés par plusieurs (groupes de) serveurs SFTP. Leur architecture s’appuie sur une paire (DC1&DC2) de serveurs SFTP par groupe ci-dessous, une VIP par paire, un NAS en réplication sur les 2 datacenter :
* En zone interne, 1 groupe : pour « Usage ».
* En DMZ, 3 groupes : pour « ENR/Cnam », « DMP/WorldLine », « Editique/Cnav ».
  + Les clusters ELASTIC. Ils sont au nombre de 3, l’un est mis en œuvre en association avec le logiciel Zammad, chacun des deux autres clusters étant « étendu » sur les 2 datacenters. Ils sont instanciés sous OpenShift.

|  |  |  |
| --- | --- | --- |
| Cluster VMWARE | Nombre de VM / datacenter  Ordre de grandeur | Types, exemples |
| Admistration | 5 | PMAD, gestion stockage, sauvegarde Networker… |
| Outillage | 15 | Proche ci-dessus + SIA et sécurité, CEPH de supervision et VM de validation techniques… |
| PROD - Application | 100 | * Serveurs « techniques » : openshift/install/DHCP/etc., PMAD, SIA(WALLIX, etc.), SIEM, sauvegarde Networker, AD, GIT, etc. * Serveurs « progiciels » : Maincare/Ideo/MySQL/OpenLdap, Zimbra (33/datacenter), etc. * Serveurs « applicatifs » : Kafka, MongoDB, PostgreSQL, SFTP, SMTP MSS, SMTP autres, suite Jeton, etc. |
| Hors-PROD - Application | 300 | Idem ci-dessus + Elastic, Ceph, etc. en environnements techniques. Plusieurs environnements. |

En PROD, 85% des VM utilisent RedHat Enterprise Linux 8, 10% Windows 2019 ou 2016, le reste se répartit entre Suse Linux Enterprise Server, Centos 7, Debian, etc.

##### Les éléments de stockage

Concernant les stockages en mode bloc et fichier, se trouvent dans chacun des 2 datacenters :

* + Une baie de stockage de type DELL/EMC Unity XT 680F.
  + Une capacité utile de 134To, compression incluse.
  + Un emplacement prévu dans le rack pour l’éventuel ajout d’un tiroir de disques (25 max) supplémentaire.
  + Une fabrique SAN redondante (avec 2 switchs Brocade).
  + Les switchs SAN peuvent, si nécessaire, être étendus par ajout de port (24 max) et licences SFP.
  + Une interconnexion entre les 2 datacenters principaux, des fabriques précédentes ainsi que des baies pour leur réplication, au travers de liens spécialisés dédiés.

Concernant le stockage en mode objet :

* + Ce service de stockage est construit en juxtaposant un certain nombre de serveurs sur lesquels est déployée la solution de stockage distribué CEPH.
  + Nativement distribué et hautement disponible il assure une réplication des données sur les 2 datacenter. La configuration protège de la perte aussi bien d’un serveur que d’un datacenter entier.
  + C’est la solution « Red Hat Ceph Storage » qui est mise en œuvre.

|  |  |  |  |
| --- | --- | --- | --- |
| Environnement | Type de serveurs | Caractéristiques | Précisions |
| Production | Physique (3+3)  Physique (1) | 1 CPU/24C  RAM 64Gb  SSD 2To / HDD 32To  NIC 2x10Gbps  10C, 16Gb, 500Go | Ceph étendu sur les 2 datacenters principaux.  Accès à travers de VIP F5. 15 To occupés à mi-2023  Témoin protégeant du « split brain » sur le 3ème datacenter |
| Externalisation | Physique (3) | 1 CPU/24C  RAM 64Gb  SSD 2To / HDD 32To  NIC 2x10Gbps | Cluster d’externalisation des données sur le 3ème datacenter  Cette externalisation s’appuie sur une configuration multi-site des Rados Gateway. |
| Hors-Production | Physique (2+2) | 1 CPU/24C  RAM 64Gb  SSD 2To / HDD 32To  NIC 2x10Gbps | Ceph étendu sur les 2 datacenters principaux.  Accès à travers de VIP F5. |
| Techniques | Virtuels |  |  |

Les usages du :

* + Stockage bloc : porté par la baie DELL/EMC Unity XT 680F. 25 To compressés dédupliqués occupés à mi-2023.
* L’espace de stockage des datastores VMware (volume des VMs gérées par VMware)
* L’espace de stockage des volumes Openshift via un driver CSI.
  + Stockage objet : porté par le cluster de serveurs étendu entre les 2 datacenters principaux. Les usages sont :
* A travers son connecteur compatible Ceph, Zimbra y place les mails/PJ…
* Le groupe SFTP Editique.
  + Stockage fichier : porté par la baie DELL/EMC Unity XT 680F. 4 To compressés dédupliqués occupés à mi-2023. Plusieurs serveurs NAS fournissent des exports NFS aux serveurs qui en ont l’usage. Ils sont typés PROD ou Hors-PROD et sont positionnés dans des VLAN distincts (1VLAN PROD, 1 VLAN Hors PROD). Ils sont spécifiques à un usage : SFTP Usage, SFTP ENR, SFTP DMP, SFTP Editique, PODS Openshift Elastisearch, Zone d’échange exploitants... En Hors-PROD les environnements sont isolés par utilisation de volumes propres à l’environnement.

Certains POD Openshift, à travers un driver CSI, en sont aussi utilisateurs.

##### Les éléments de sauvegarde

L’architecture de sauvegarde est basée sur les technologies EMC Datadomain et Networker.

Les composants de la solution se déclinent comme suit :

* + Composants logiciels, VM, i.e. Data Protection Suite Networker :
* 1 Serveur Networker Serveur Recovery (NSR) dans le premier datacenter.
* 1 Serveur Networker Management Console (NMC) dans le premier datacenter.
* 2 Serveurs Global Storage Node (GSN), 1 par datacenter principal.
  + Composants matériels i.e. DELL-EMC² PowerProtect (ou DataDomain) :
* 2 PowerProtect DD6900 de 94 TB Utile, un au sein de chacun des 2 datacenters principaux pour stocker les sauvegardes croisées.
* 1 PowerProtect DD6900 de 94 TB Utile, au sein du 3ème datacenter pour l’externalisation des sauvegardes des serveurs de production.

Selon le cas de figure, la sauvegarde d’une machine virtuelle est réalisée :

* + Majoritairement par backup des snapshot en utilisant NVP (Networker Vmware Protection) qui est connecté au vcenter. Les sauvegardes passent par le réseau de sauvegarde dédié.
  + A la demande des agents networker peuvent être installés sur certaines machines de base de données si un dump de la base n’est pas suffisant. Dans ce cas la sauvegarde passe directement par le réseau de sauvegarde dédié.

## Présentation du périmètre existant DMP

### Fonctionnalités du DMP

Le DMP est un service de santé pré-existant à Mon espace santé. Il permet à l’usager de conserver de manière sécurisée et permanente ses données et documents de santé.

En accédant à son DMP via Mon espace santé, l’usager bénéficie d’un espace de stockage sécurisé de ses données et documents de santé hébergés dans le système d’information DMP. Il peut :

* + Ajouter et classer lui-même des documents ;
  + Consulter les données (hébergées par le DI DMP) classées dans des rubriques distinctes et présentées sous un format document (exemple : compte-rendu de biologie, synthèse médicale, etc.) ou sous un format structuré (exemple : données de remboursement dites « Historique de remboursement base de données ») ;
  + Disposer des documents et données alimentés par des professionnels de santé ou des services tiers référencés sous réserve du recueil de son consentement ;
  + Modifier la visibilité aux Professionnels des documents stockés.

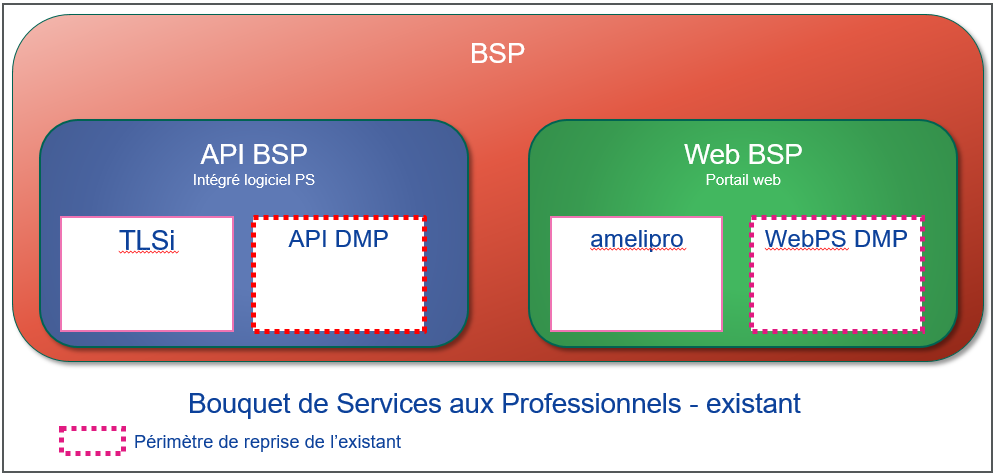
Nativement (hors Mon espace santé), le DMP communique avec les logiciels des professionnels de santé via des API nommées TD X.X. Ces transactions permettent aux professionnels de santé, de même, de déposer, consulter, dépublier, et globalement gérer des documents de santé via leurs interfaces (webDMP et logiciels métiers).

Dans le cadre de son adossement à Mon espace santé et au Bouquet de services aux professionnels de santé, d’autres API sont mises en place au sein du système d’information DMP. Elles permettent d’assurer les fonctionnalités d’échanges d’informations entre le système d’information DMP et le système d’information Mon espace santé d’une part et le système WebBSP / amelipro d’autre part. Pour ce qui est de Mon espace santé, ces fonctionnalités recouvrent tous les échanges relatifs au compte Mon espace santé (création, mise à jour, fermeture, suppression), ainsi que toutes les informations relatives à la gestion de part et d’autres des documents (quelle que soit leur niveau de structuration) : information de DMP vers Mon espace santé des actions entreprises par des professionnels de santé (dépôt, modification, dépublication, traces, etc.) et informations de Mon espace santé vers le DMP des actions entreprises par le titulaire du Mon espace santé ou son représentant légal (ajout de document, modification, suppression, changement de confidentialité unitaire ou sur l’ensemble des documents, etc.). Ces échanges recouvrent également des interactions automatisées, comme le déclenchement du traitement des historiques de remboursement (à l’activation par l’usager), ou les mises à jour des traits d’identité de l’Identifiant National de Santé issues du référentiel SNGI (sur changement), ou encore les actions entreprises par des services tiers référencés et appariés par l’usager à son Mon espace santé, sous couvert de l’autorisation données par l’usager lors de l’appariement. Pour ce qui concerne les services aux professionnels de santé, des services sont également disponibles au niveau du DMP pour permettre la gestion de documents issus d’amelipro (Dépôt, consultation).

Accessibles aux usagers via leur MES, le DMP l’est également par les Professionnels de santé, via des services offerts dans le Bouquet de Services aux Professionnels (BSP). Le BSP regroupe par ailleurs un certain nombre d’autres services en ligne que ceux du DMP, proposés via un portail « amelipro » ou en accès depuis leur Logiciels des Professionnels de Santé (LPS) interfacé aux services du SI Cnam (Téléservices intégrés – TLSi).

Deux modes d’accès au DMP sont proposés aux Professionnels : par l’intermédiaire d’un portail dédié, le « web DMP PS » (<https://www.dmp.fr/web/dmp/ps>) – voir son [tutoriel](https://www.dmp.fr/documents/d/dmp/tutoriel-webps-dmp) – , ou par l’intermédiaire de leur Logiciel Métier (LPS) interfacé avec le service DMP (interfaces SOAP, de nature très différentes aux interfaces REST/FHIR proposées sur la partie “documents” aux applications pour le citoyen référencées à Mon espace santé avec échange de donnés).

La figure suivante présente de façon sommaire le périmètre du BSP existant et le sous-ensemble qui doit être repris dans le cadre du présent accord-cadre.



En complément des cas d’usage d’alimentation des documents médicaux par le patient depuis Mon espace santé et par le PS, la Cnam est autorisée à alimenter les DMP en données (de remboursement) ou documents (notes de vaccination, attestation de vaccination Covid par exemple).

La création des DMP en masse via l’opération d’opt-out de Mon espace santé permet de mettre à disposition des professionnels de santé les documents et données contenus dans les dossiers du plus grand nombre des patients, qui restent néanmoins maitres des autorisations données aux professionnels. Les usagers peuvent ainsi explicitement s’opposer au dépôt de documents dans leur DMP, mais également activer le principe de masquage de documents, ou aller même jusqu’au blocage nominatif d’un professionnel de santé s’ils ne souhaitent. Dans tous les cas, l’usager est informé des dépôts de documents et accès par un professionnel de santé.

### Les documents du DMP

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

<https://industriels.esante.gouv.fr/produits-et-services/ci-sis-cadre-d-interoperabilite-des-systemes-d-information-de-sante>

Les documents contenus dans le DMP sont organisés selon plusieurs catégories détaillées ci-dessous.

En complément des cas d’usage d’alimentation des documents médicaux par le patient dans MES et par le PS comme décrit aux chapitres suivants, la Cnam est autorisée à alimenter les DMP en données de remboursement, et ne nécessite pas de déclaration d’autorisation explicite à accéder au DMP (sauf opposition explicite du titulaire du DMP, après activation de l’option sur MES par la Cnam permettant aux titulaires d’exprimer ce refus).

Le document Historique des remboursements (CNAM-HR) comprend des données administratives (patient, auteur du document, etc.) et des données médicales ayant fait l’objet d’un remboursement.

Le processus d’alimentation des HR consiste à réceptionner les flux de données de remboursement en provenance du Middle Office et à les intégrer dans une base de données.

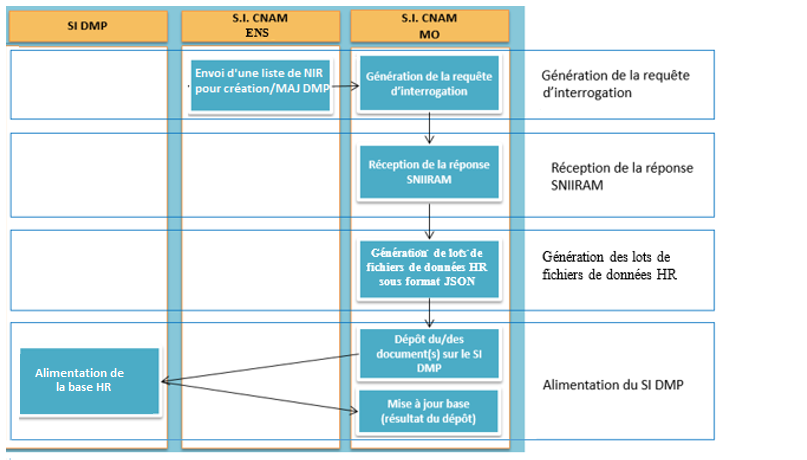


Figure : Processus d’alimentation d’un DMP en données de remboursements

Le service consultation est destiné à être appelé par d’autres composants SI DMP : le socle (requête Logiciel PS), le WebPS, le WebMH, le service de rematérialisation et l’API ENS.

Le processus de restitution des HR consiste à récupérer les données HR stockées dans la base de données pour un DMP.

Enfin, dans le cadre de la vaccination COVID, la Cnam a mis en place un service SI Vacci-COVID, système d’information qui répertorie les données de vaccinations COVID des individus vaccinés en France (ayant ou non un DMP) permettant l’intégration des vaccinations COVID dans le carnet de vaccination de chaque DMP.

Un traitement d’intégration de ces vaccinations est mis en œuvre au sein du SIDMP.

### Contexte d’accès au DMP par les PS

L’accès aux DMP est réservé aux professionnels de santé de l’équipe de soins et/ou bénéficiant d’une autorisation par le titulaire du DMP. Les droits d’accès desdits professionnels répondent en sus à une matrice des habilitations fixées préalablement par l’ANS et le Code de la santé publique. Cette matrice permet de différencier les professionnels du fait de leur profession ou de droit particulier affectés par le patient ou par la nature de la prise en charge.

De surcroît, le « médecin traitant DMP » dispose d’un accès spécifique au DMP. En effet, ce dernier accède à l’ensemble des informations contenues dans le DMP y compris celles rendues inaccessibles par le titulaire. Le titulaire du DMP peut décider d’attribuer ce droit à tout professionnel de santé de son choix. A contrario, le titulaire peut à tout moment décider de masquer des informations aux professionnels de santé de son choix ; ces informations restent cependant accessibles au professionnel de santé qui les déposées.

Le titulaire peut également refuser expressément l’accès à son DMP à tout professionnel de santé de son choix (liste d’exclusion).

Les professionnels de santé disposent également d’un accès spécifique en cas de situation d’urgence (articles L. 1111-17 et R. 1111-39 du code de la santé publique).

Les personnes exerçant sous la responsabilité d’un professionnel de santé peuvent alimenter un DMP au nom et pour le compte d’un professionnel de santé. Cette faculté d’alimentation ne donne aucun droit de consultation des données.

Ainsi, le système informationnel du DMP doit être en capacité de reconnaitre un professionnel de santé et de lui affecter les droits en fonction de la matrice des habilitations tout en prenant compte de l’ensemble des droits particuliers.

### WebDMP PS

Une IHM Web est mise à disposition des utilisateurs qui n’auraient pas de LPS compatibles.

Le professionnel peut se connecter au Web DMP soit à partir de sa carte de professionnel physique (carte de type CPS) ou en utilisant l’application mobile E-CPS et le téléservice Pro Santé Connect mis en œuvre par l’Agence du Numérique en Santé.

La couverture fonctionnelle de cette interface Web est identique à celle proposée aux éditeurs de logiciels LPS, décrite dans le paragraphe suivant.

### Interfaces DMP proposées aux LPS

Les professionnels intervenant en santé peuvent se connecter au système d’hébergement DMP :

* + Soit via un LPS ou un via l’accès web en utilisant leur carte CPS ;
  + Soit via un LPS en utilisant le certificat serveur de l’établissement où ils travaillent.

| Fonctionnalité | Action | Ressource - URI |
| --- | --- | --- |
| Accès au DMP | Accès au DMP du patient (INS, traits d’identité) | Permet la recherche d’un patient par son INS ou ses traits d’identité pour accéder à son DMP. |
| Accès au DMP du patient via lecture carte vitale | Permet l’accès au DMP d’un patient via la lecture de sa carte vitale. |
| Accès à la liste des patients rattachés au PS | Permet l’accès à la liste des patients rattachés au PS. |
| Accès à la liste patient d’un PS par une Carte de Personnel d’Etablissement (CPE) secrétaire médicale | Permet l’accès via une CPE secrétaire médicale à la liste des patients enregistrés pour un PS. |
| Autorisation d’accès à un DMP | Permet de recueillir l’autorisation d’accès au DMP via l’accord patient.  Permet de recueillir l’autorisation d’accès au DMP via l’accord du représentant légal.  Permet de recueillir l’autorisation d’accès au DMP via l’accès en urgence. |
| Données issues de MES | Données administratives non modifiables reçues de MES | Rend non modifiables les données administratives du patient et du représentant légal reçues de MES. |
| Donnée Volontés et droits non modifiable, issues de MES | Rend non modifiables les données Volontés et droits du patient issues de MES :   * Personne à prévenir en cas d’urgence ; * Personne de confiance ; * Proche(s) aidé(s) ; * Proche(s) aidant(s) ; * Directives anticipées : Consulter les directives anticipées ou déposer les directives anticipées ; * Don d’organes et de tissus : Permet d’indiquer si le patient est averti ou non de la loi sur le don d’organes. |
| Documents d’un DMP | Types de documents acceptés dans le DMP | Les types de documents acceptés dans le DMP sont des documents de types : TXT, JPEG, TIFF, PDF, RTF. |
| Catégorisation des documents dans le DMP | Les catégories de documents disponibles dans le DMP sont :   * Synthèses ; * Traitements et soins ; * Comptes rendus ; * Imagerie médicale ; * Biologie ; * Prévention ; * Certificats/déclarations ; * Données de remboursement ; * Autres documents déposés par le patient. |
| Liste des documents d’un DMP | La liste des documents d’un DMP peut être présentée, triée et filtrée selon différents critères définis. |
| Recherche de document | La recherche d’un document présent dans le DMP peut être effectuée selon différents critères définis. |
| Gestion des actions possibles sur les documents d’un DMP | Les actions possibles sur les documents d’un DMP sont :   * L’ajout d’un document ; * La consultation d’un document ; * La modification d’un document ; * La suppression d’un document ; * L’archivage d’un document ; * Le désarchivage d’un document. |
| Parcours de soins : vue des documents du DMP | Permet la vue chronologique des documents du DMP d’un patient. |
| Téléchargement d’un document du DMP | Permet le téléchargement d’un document du DMP aux formats : PDF, TXT, RTF, JPG, TIFF, CDA ou XDM. |
| Gestion des versions du document | Permet la gestion et visualisation des versions d’un document du DMP. |
| Gestion de la confidentialité du document (masquage) | Permet la gestion de la confidentialité des documents en permettant le masquage d’un document par le patient aux PS. |
| Gestion de la visibilité / invisibilité d’un document | Permet de rendre visible ou invisible un document pour le patient en attendant la consultation d’annonce. |
| Autres dossiers médicaux | Consultation du dossier pharmaceutique | Permet la consultation du dossier pharmaceutique. |
| Consultation du dossier médicale santé au travail | Permet la consultation du dossier médical santé au travail. |
| Carnet de vaccination (CVA) | Gestion des vaccinations | Permet l’ajout, la modification et la suppression d’une vaccination dans le CVA. |
| Historique des vaccinations | Permet d’accéder à l’historique des vaccinations reçues par le patient avec une fonction de tri selon la date ou la pathologie. |
| Version du CVA | Permet la gestion de la version du document CVA. |
| Gestion des autorisations | Liste des professionnels et établissements autorisés à accéder à un DMP | Permet d’afficher la liste des professionnels et établissements pour lesquels le PS a demandé un accès au DMP accepté par le patient. |
| Droits d’accès en contexte d’urgence | Permet de consulter les droits d’accès au DMP dans un contexte d’urgence. |
| PS non autorisés à accéder au DMP | Permet de consulter la liste des PS non autorisés à accéder à un DMP. |
| Autres fonctionnalités du DMP | Gestion de l’historique de remboursement | Permet la gestion de l’historique de remboursement. |
| Suivi des demandes patients | Permet le suivi des demandes de copie intégrale ou partielle du DMP par le patient. |
| Gestion du médecin traitant DMP | Permet la gestion du médecin traitant DMP. |
| Gestion des notifications | Permet la gestion des adresses de réception des alertes. Les Professionnels qui accèdent au dossier d’un patient peuvent demander à être notifiés par mail ou SMS sur certains évènements : ajout d’un document, accès en mode urgence par un autre Professionnel par exemple. Le SI DMP actuel gère, indépendamment du système de notification usagers de MES, l’envoi de ces notifications sur les coordonnées mail/téléphoniques renseignées par les Professionnels. |
| Gestion de l’Historique des accès | Permet la consultation de l’historique des accès selon le statut du PS. |
| Gestion de la connexion secrète | Permet l’accès au DMP d’un mineur pour permettre de bloquer l’envoi d’une notification au(x) représentant(s) légal(aux) lors de l’accès et empêcher la consultation des traces de l’accès, afin de préserver le secret du mineur titulaire du DMP. |
| Information sur l’état du DMP | Permet de donner l’information sur l’état du DMP (ouvert ou fermé), sans information sur MES. |
| Message d’alerte | Permet d’envoyer des messages d’alerte au PS sur son DMP (information au PS qu’il va quitter le DMP d’un patient pour ouvrir celui d’un autre patient) |
| Information du PS connecté | Permet d’informer de la connexion d’un PS au DMP. |
| Gestion de la situation et du cadre d’exercice | Permet de gérer la situation et le cadre d’exercice d’un PS. |
| Gestion des adresses de réception des notifications | Permet des gérer la liste des adresses de réception des notifications DMP. |
| FAQ | Permet d’accéder à la FAQ DMP. |
| Tutoriel du web PS | Permet d’accéder au tutoriel du WebPS. |
| Bandeau d’alerte | Permet de visualiser le bandeau d’alerte DMP. |
| Gestion des symboles | Permet la gestion des symboles. |

Selon le niveau d’implémentation des fonctions DMP dans son LPS, le Professionnel peut accéder au DMP de son patient :

* + Par les fonctions spécifiques DMP du tableau ci-dessus, 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 direct à certaines URL du site webDMP PS appelées depuis son LPS en passant des éléments de contexte d’utilisation (par exemple en passant le « contexte patient » au système DMP). Cela permet d’accéder à des fonctions non encore implémentées dans son LPS par exemple.

### Interfaces DMP avec MES

L’interfaçage avec MES est géré par l’API DMP. Cette API DMP (interface avec MES) regroupe deux applications distinctes :

1. Une Authorization Management et une API Management (qui s’appuient sur la brique open-source Gravitee), se chargeant pour la première de la gestion de l'autorisation (jeton) et pour la seconde de la redirection vers les différentes API fonctionnelles (Service Annuaire des PS et des Structures (SAPS), service DMP) ;
2. Une API fonctionnelle qui permet d’accéder aux fonctions du DMP (gestion et fonction d’usage).

Les fonctions mises en œuvre dans le cadre de l’API DMP sont réparties en différentes familles de fonctions correspondant à des fonctionnalités distinctes au sein du DMP :

* + **L’autorisation :** cette fonction est transverse à l’ensemble de l’API DMP, elle constitue un prérequis afin d’accéder aux autres fonctions de l’API DMP sauf pour les fonctions techniques qui ne nécessitent pas d’autorisation ;
  + **La gestion du DMP :** cette famille de fonctions correspond à la création ou modification d’un DMP, à la consultation d’un DMP, à la fermeture d’un DMP, à la réactivation d’un DMP, à la récupération du statut du DMP et de son compte d’accès DMP et au rattachement d’un DMP à un compte MES via MES (service DMP) ;
  + **Les fonctions d’usage du DMP :** cette famille de fonctions regroupe toutes les fonctions d’usage d’un DMP (gestion des documents, des autorisations d’accès (consentement au mode bris de glace/urgence, habilitations), des abonnements aux notifications, gestion des médecins traitants DMP, des représentants légaux, accès aux traces, demande de rematérialisation) (service DMP) ;
  + **Les fonctions techniques :** cette famille de fonctions regroupe les recherches sur l’annuaire des professionnels de santé et établissement de santé, elle peut être réalisée sans autorisation sur un dossier DMP donné (service SAPS).

| **Famille de fonctions** | **Action** |
| --- | --- |
| **Autorisation** | Fonctions transverses à toutes les fonctions de l’API DMP |
| **Gestion du DMP** | Création d’un DMP |
| Modification d’un DMP |
| Consultation d’un DMP |
| Réactivation d’un DMP |
| Fermeture d’un DMP |
| Récupération de l’existence d’un DMP (+ informations) |
| Rattachement d’un DMP à MES |
| Demande de destruction d’un DMP |
| **Usage du DMP** | Liste des consentements sur un DMP |
| Mise à jour d’un consentement |
| Ajout d’un consentement |
| Suppression d’un consentement (déblocage d’un professionnel ou retrait du statut médecin traitant DMP) |
| Consultation de l’abonnement aux notifications |
| Consultation du représentant légal dans le DMP |
| Ajout du représentant légal dans le DMP |
| Modification du représentant légal dans le DMP |
| Suppression du représentant légal dans le DMP |
| Recherche multicritères de document |
| Recherche multicritères de lot de soumission |
| Consultation du contenu d’un document |
| Accès rapide à la dernière version d’un document |
| Ajout (alimentation) d’un document |
| Suppression logique (dé-publication) d’un document |
| Archivage d’un document |
| Désarchivage d'un document |
| Masquage d’un document |
| Démasquage d'un document |
| Consultation des données HR Bdd |
| Accès à l’historique des traces |
| Commande d’une rematérialisation |
| Lister les commandes de rematérialisation |
| Téléchargement d’une commande |
| **Technique** | Recherche multicritères de professionnels |
| Récupération des informations détaillées sur un professionnel |
| Récupération des informations d’une liste de professionnels |
| Récupération des informations détaillées sur une structure |
| Récupération du référentiel vaccinal |

Des travaux ont lieu en 2023 pour permettre un interfaçage avec AmeliPro (BSP), cet interfaçage doit être repris dans l’accord-cadre objet du présent CCTP. Un état des lieux est fait en début de phase P1.1 - Pdc\_Init : Prise de connaissance et Initialisation.

### Site institutionnel DMP

Un portail web est mis a disposition des professionnels intervenant en santé. Ce site affiche d’une part un contenu informationnel sur le service DMP et permet aux professionnels intervenant en santé d’accèder aux services DMP.

Un portail web est mis à disposition du grand public. Ce site affiche d’une part un contenu informationnel commun à tous, des informations relatives à MES, la liste de l’ensemble des services tiers référencés, etc. Il s’agit également de mettre à disposition des informations ciblées aux professionnels : il s’agit de présenter l’articulation des fonctionnalités de MES avec les services qui leur sont proposés à travers le BSP (fonctionnalités en miroir) et en particulier avec le DMP et la MSS (Messagerie Sécurisée de Santé).

D’autres pages du DMP utilisent le CMS Lifefray.

### Support DMP

Concernant le support du DMP, quand la demande concerne un patient, les différents niveaux de support sont les suivants :

* + Niveau 1 : PSN1 ;
  + Niveau 2 : PSN Cnam ;
  + Niveau 3 : Titulaire de l’accord-cadre.

Les outils employés sont les suivants : PSN1, Clearquest, FSP et courriels.

Quand la demande concerne des professionnels de santé, les différents niveaux de support sont les suivants :

* + Niveau 1 : Editeur ou CIS DNS ou PF de Service de Moulin ;
  + Niveau 2 : GIE SESAM VITALE ;
  + Niveau 3 : Titulaire de l’accord-cadre.

Les outils employés sont les suivants : Clearquest et courriels.

### Web MH

Dans le cadre de la gestion des données de santé, nous définissons le rôle du « médecin de l’hebergeur (Web-MH) » comme gestionnaire des données de santé au sein de l’exploitation applicative.

Le médecin de l’hébergeur participe aux processus de gestion des incidents, dès lors que l’incident a un impact sur les données de santé à caractère personnel ou sur le respect des droits des personnes concernées par les données de santé.

Le médecin de l’hébergeur s’engage à assister l’hébergeur dans toute démarche ayant un lien direct ou indirect avec l’exercice de ses missions.

Pour exercer ses missions le médecin hébergeur utilise un outil spécifique, le Web MH, aux fonctionnalités similaires à celles du web DMP PS.

Les fonctionnalités propres du Web MH sont les suivantes :

* Lister des demandes de copie de DMP prêtes pour l’ensemble des utilisateurs,
* Lister les demandes de copie expédiées pour l’ensemble des patients,
* Lors de la demande de suppression d’un document pour un patient, un service permet de déterminer s'il existe déjà un ticket de demande de suppression définitive pour ce document,
* Gérer et effectuer des demandes de copie de DMP des patients,
* Verifier si une demande de destruction de DMP existe déjà.

A partir de cet outil, le médecin traite toute demande émanant d’une personne dont les données de santé sont hébergées, qui vise à obtenir la communication de tout ou partie de ses données hébergées, ainsi que l’historique des accès à ses données et des consultations, le contenu des informations consultées et des traitements éventuellement opérés.

### SI Pilotage DMP

#### Introduction

Le système d’information de pilotage du DMP (SI Pilotage DMP) est un portail dédié au suivi des statistiques d’usages du DMP et de son déploiement. Les données sont issues de traces fonctionnelles générées par le SI-DMP, ces traces sont écrites par le SI-DMP et liées aux usages des titulaires des DMP et des acteurs de santé qui les prennent en charge. Avant d’être envoyées au SI PILOTAGE les traces sont anonymisées et vidées de toutes données directement ou indirectement identifiantes. L’implémentation des rapports et indicateurs est faite au fil de l’eau jusqu’à j-1 ; l’accès aux indicateurs est en libre-service pour les utilisateurs disposant d’un identifiant et d’un mot de passe délivrés par la Cnam. Les clients des rapports et les rapports consultables sont précisés en Annexe « MESDMP\_Annexe 28\_Clients\_rapports\_SI\_PIL-DMP ».

#### Principales caractéristiques

Les principales caractéristiques du Pilotage DMP sont les suivantes :

* + D’être fondé principalement sur les traces anonymisées « élémentaires » émises par le SI-DMP, sans reconstitution d’objets Dossier et Document en analysant celles-ci chronologiquement comme précédemment, donc intégrées « au fil de l’eau » ;
  + D’être recentré sur l’activité du SI-DMP en ne prenant en compte que les traces les plus récentes (36 mois glissants d’historique) ;
  + D’exploiter en conséquence certains cumuls généraux directement issus du SI-DMP ;
  + D’enrichir les traces anonymisées lors de leur intégration au SI PILOTAGE afin qu’elles deviennent autoporteuses et qu’aucune jointure ne soit nécessaire (que ce soit avec un référentiel ou entre-elles) lors de leur exploitation.

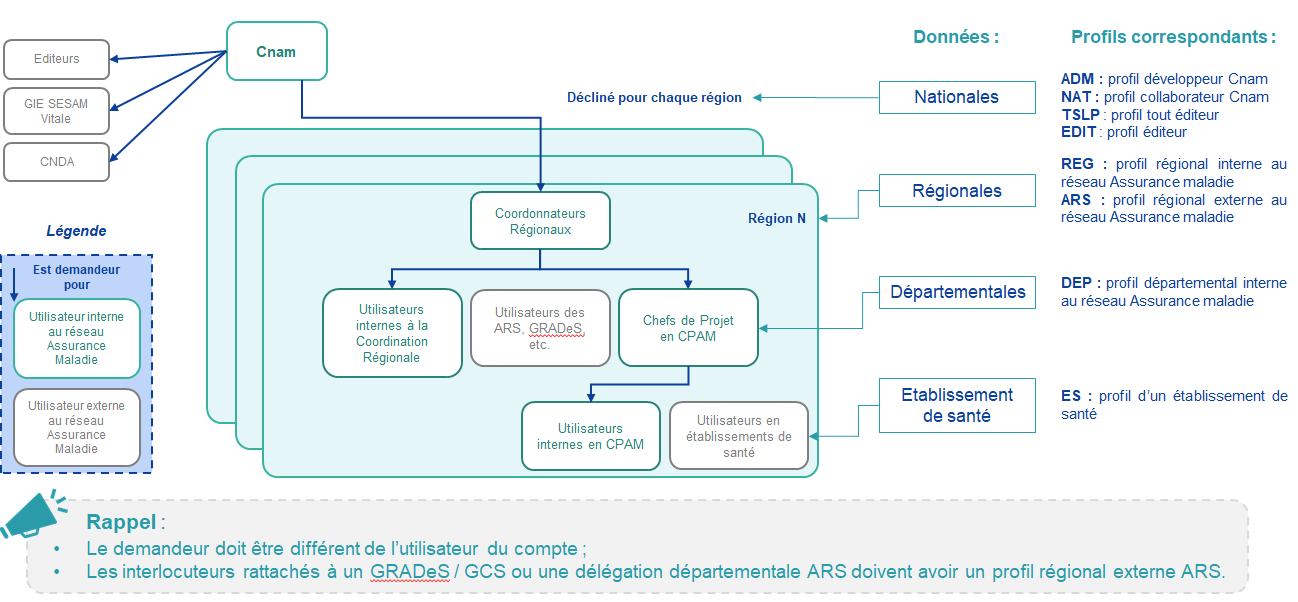
#### Composition du SI Pilotage

Le front office comporte au total 8 types de profils utilisateurs, donnant des accès différenciés et un profil d’habilitation différent selon l’utilisateur : utilisateurs administrateurs ayant des droits étendus (utilisateurs Cnam habilités en écriture), profil national interne Cnam (utilisateurs Cnam habilités en lecture seulement), utilisateurs régionaux, départementaux, etc. les différents profils sont imbriqués les uns aux autres afin de permettre à l’utilisateur ayant le plus de droits d’accéder à l’ensemble des données des autres profils. Les différents profils sont composés de tableaux de bords de suivi des usages (autour de 80 tableaux de bords), chacun de ces tableaux de bord est composé de tables élémentaires sous forme de tableaux graphiques (autour de 350 tables élémentaires). Les tables élémentaires sont, elles, composées d’un ensemble d’indicateurs issus des champs des traces fonctionnelles issues du SI-DMP (autour de 200 champs de données).

Le back office comprend 70 types de traces fonctionnelles issues des différentes connexions et actions sur le système DMP (cela représentait en 2022, 820 millions de traces générées), autour de 40 règles de gestion, et référentiels partagés avec le SI-DMP.

Enfin, un service d’export permet de gérer et de mettre à disposition des équipes Cnam des données à plat qui servent à des besoins non couverts par la solution technique (suivi Ségur, rémunérations conventionnelles, extraction mensuelle à destination de l’Observatoire National des Flux, etc.).

#### Accès au SI Pilotage du DMP



Le SI pilotage DMP dispose de 8 types de profils utilisateurs, comme illustré sur le schéma, 3 au niveau national, 2 régionaux, 1 départemental et deux dédiés aux établissements de santé et éditeurs. Chaque utilisateur est associé à un profil d’habilitation dédié, la création de ces comptes d’accès associés à chacun de ses profils est régie par des règles strictes dictées par des exigences sécurité. Une procédure précise existe et est communiquée au Titulaire après notification de l’accord-cadre.

#### Principe de fonctionnement des données calculées

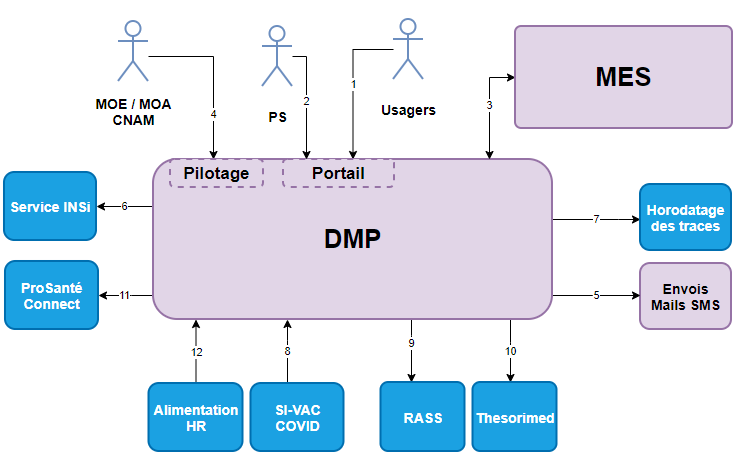
Le SI Pilotage se base principalement sur les traces d’activité « élémentaires ». Du fait de la durée limitée de conservation des traces 36 mois glissants et du principe directeur d’interdire toute jointure, y compris entre les traces elles-mêmes, les comptages ne doivent se décliner que suivant des données contenues initialement dans la trace ou enrichies auprès de référentiels, le SI PILOTAGE utilise le référentiel du SI-DMP, enrichi si nécessaire.

## Présentation du périmètre technique DMP

### Présentation générale de l’architecture du DMP

Ce chapitre permet d’avoir une vision globale du DMP et de ses interactions avec les différents systèmes d’informations partenaires.

#### Interfaces externes

Fig. Archi-03

Le DMP est un système possédant des interactions avec d’autres systèmes d’information.

Les flux décrits sur la figure Archi-03 sont précisés ci-après :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Composant | Commentaire | Déclenchement du flux vu du DMP | Type déclenchement | Origine du déclenchement |
| 1 | Usagers | Accès à l'ancien portail d'information patients du DMP (à décommissionner) | entrant | unitaire | utilisateur |
| 2 | PS | Accès au portail d'information PS du DMP et point d'entrée vers le WebPS DMP | entrant | unitaire | utilisateur |
| 3 | MES | Pilotage des créations, Appel API documents | entrant | unitaire | MES |
| Appel API Coordonnées, et API événement dépôt de document | sortant | unitaire | DMP |
| 4 | MOE/MOA CNAM | Accès aux statistiques anonymisées | entrant | unitaire | utilisateur |
| 5 | Envoi Mails SMS | Communications sortantes Mails et SMS aux PS | sortant | unitaire | DMP |
| 6 | Service INSi | Vérification ou recheche de l'identifiant national de santé auprès du téléservice | sortant | unitaire | DMP |
| 7 | Horodatage des traces | Système permettant d'assurer le caractère probant des traces du DMP | sortant | unitaire | DMP |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 8 | SI-VAC COVID | Dépôt par lots des données de vaccination | entrant | unitaire | SI-VAC |
| 9 | RASS | Référentiel des acteurs de santé | sortant | unitaire | DMP |
| 10 | Thesorimed | Nomenclatures médicaments | sortant | unitaire | DMP |
| 11 | ProSanté Connect | Authentification OIDC PS | sortant | unitaire | DMP |
| 12 | Alimentation HR | Dépôt par lots des données de remboursements pour constituer l'historique de soins | entrant | masse | SI CNAM |

#### Composants Internes

Le DMP se compose de différents sous-systèmes applicatifs (SSA) permettant d’en assurer l’intégralité des fonctionalités.

Le schéma ci-après positionne ces SSA et le patrimoine applicatif qu’ils regroupent :

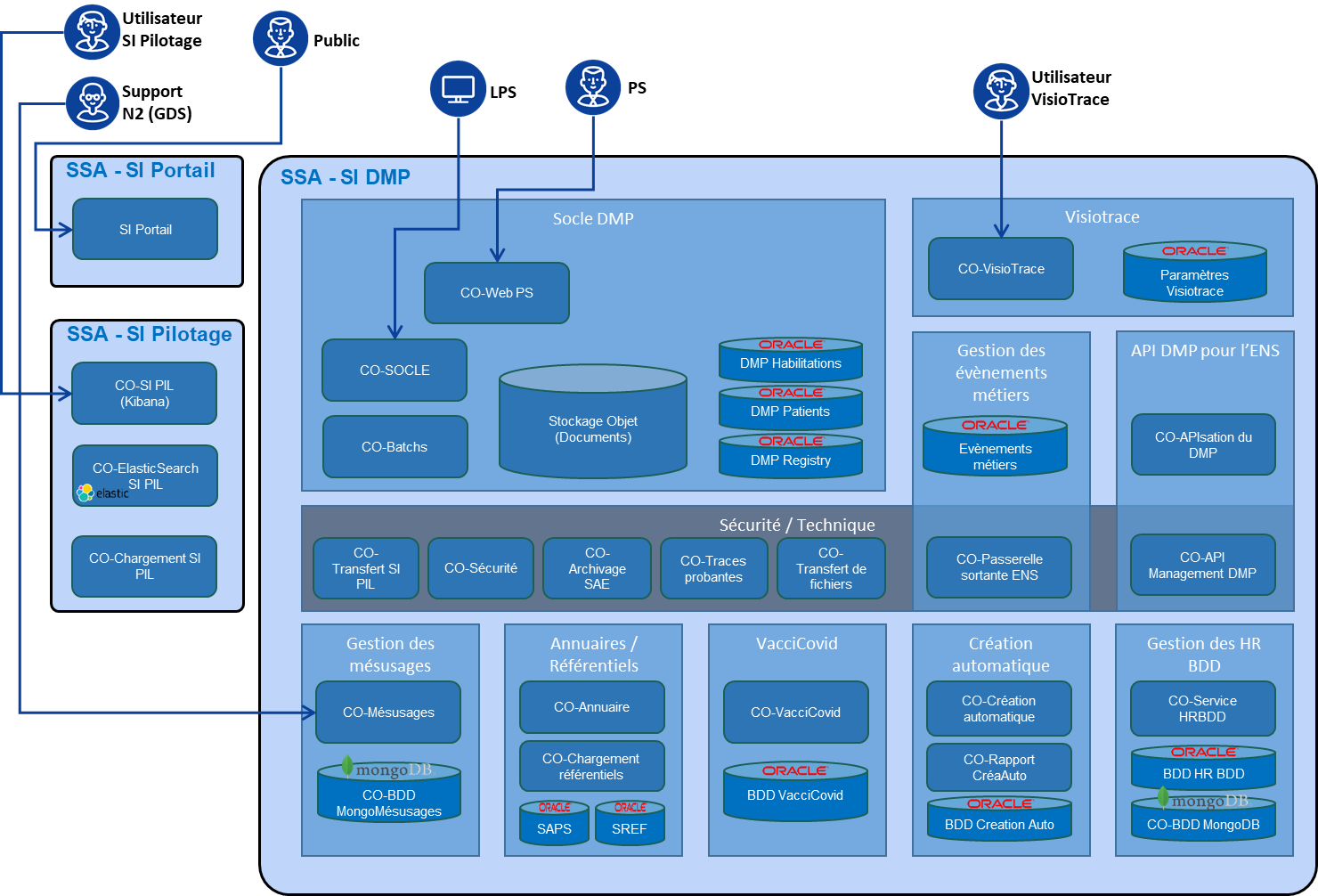


Fig Archi-04

SSA « SI Portail» :

Ce sous-système contient les composants permettant de publier le contenu éditorial et documentaire sur le Portail DMP (https://www.dmp.fr/).

SSA « SI DMP » :

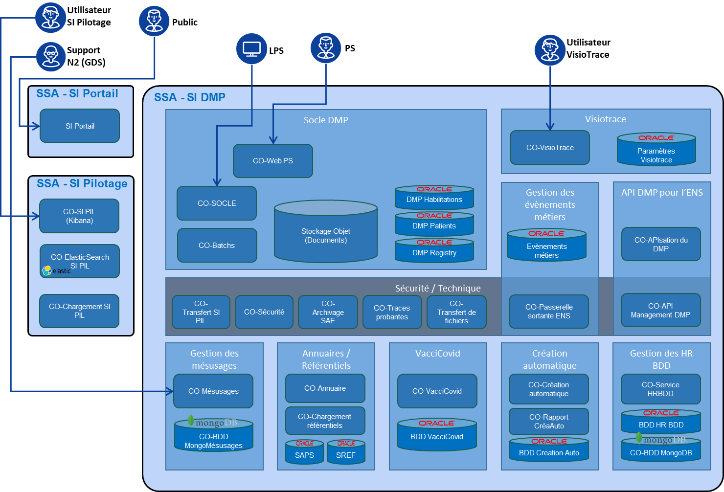
Ce sous-système contient l’ensemble des composants assurant la gestion de tous les documents pris en charge par le DMP, la publication des API permettant aux Logiciels des Professionnels de Santé (LPS) de l’utiliser, ainsi qu’une IHM à destination des PS permettant d’alimenter et de consulter les DMP de leurs Patients.

SSA « SI Pilotage » :

Cette zone contient les dispositifs de Business Intelligence permettant de produire les indicateurs-clé de pilotage des usages du DMP à des fins statistiques et Métier.

### Présentation détaillée de l’architecture du DMP

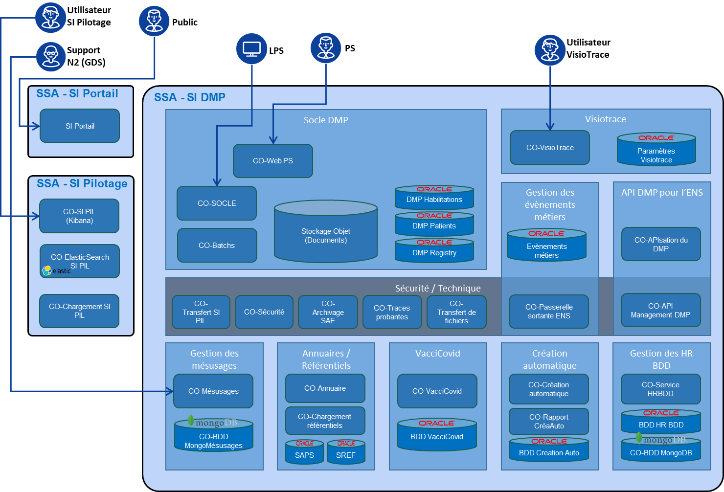
#### SI Portail



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + SI Portail : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.11

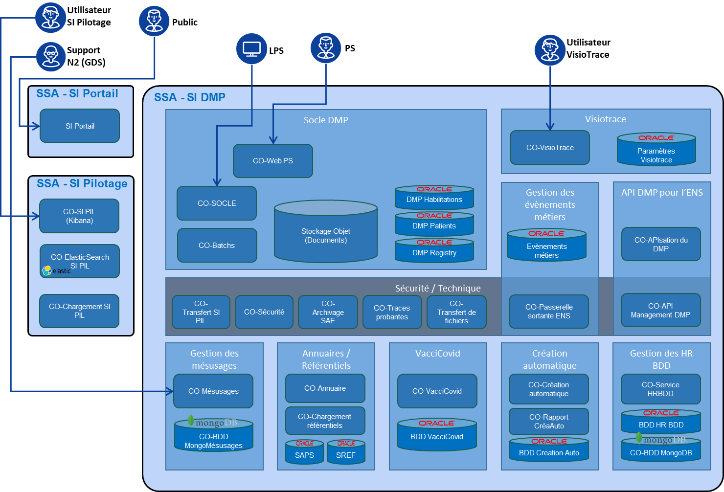
#### SI Pilotage



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-SI PIL : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.5
  + CO-ElasticSearch SI PIL : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.5
  + CO-Chargement SI PIL : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique » : §4.5

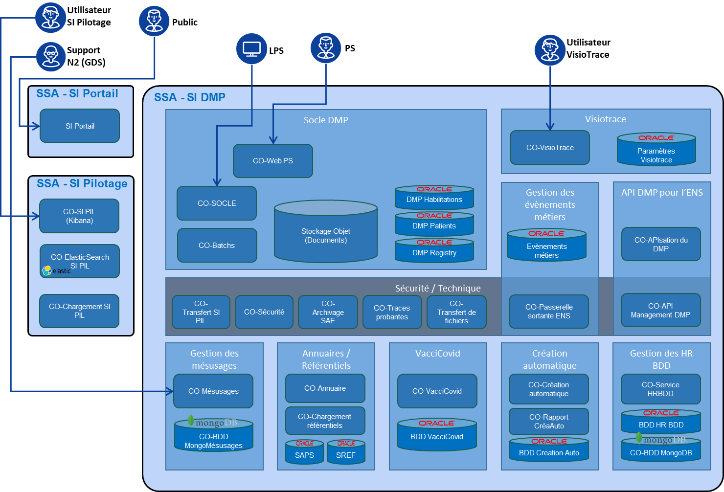
#### Socle DMP



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-WebPS : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.10
  + CO-SOCLE : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.10
  + CO-Batchs : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.10
  + Stockage Objet : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique » : §6.5

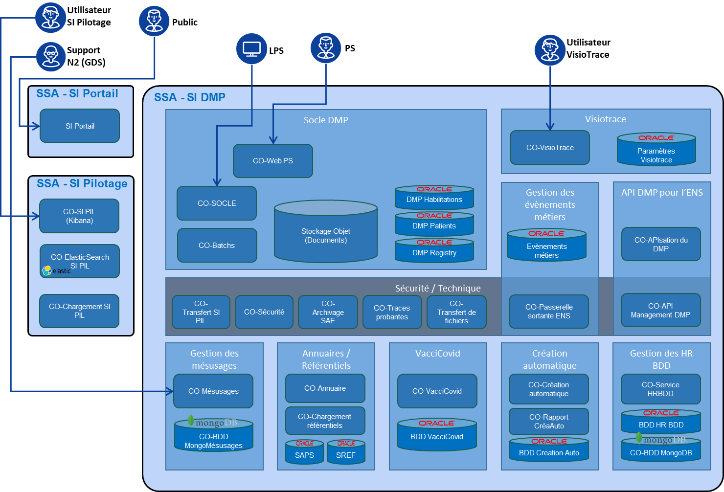
#### Visiotrace



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-VisioTrace : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.12

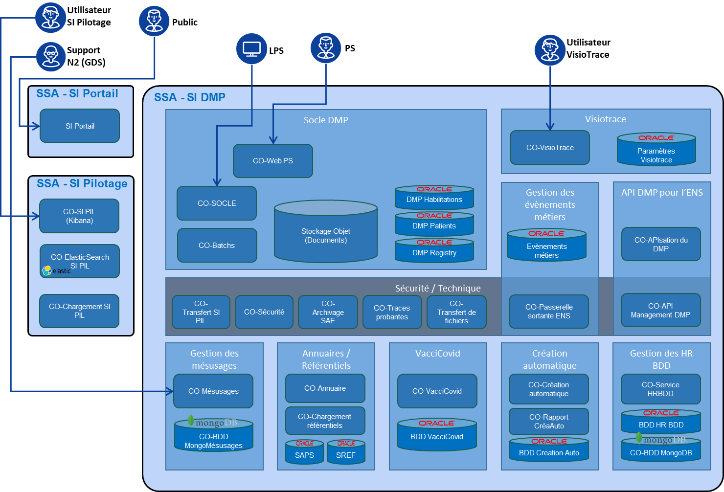
#### Gestion des évènements métiers



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-Passerelle ortante ENS 23: §4.2 et 3.2.5

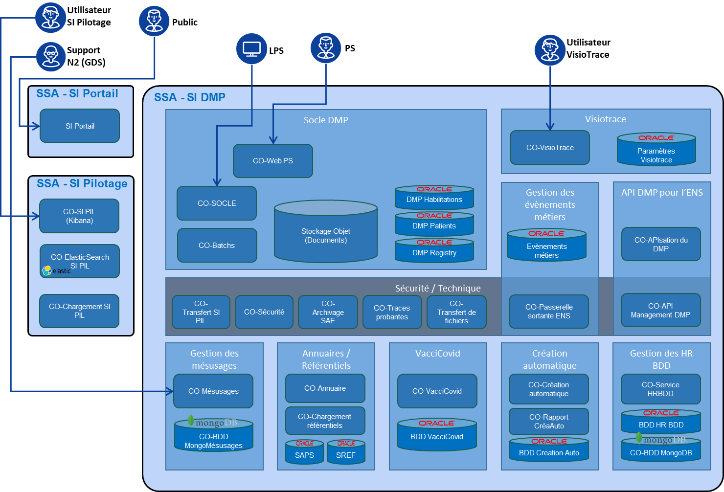
#### API DMP pour l’ENS



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-APIsation du DMP : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.6
  + CO-API Management DMP : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.6 et §3.2.3

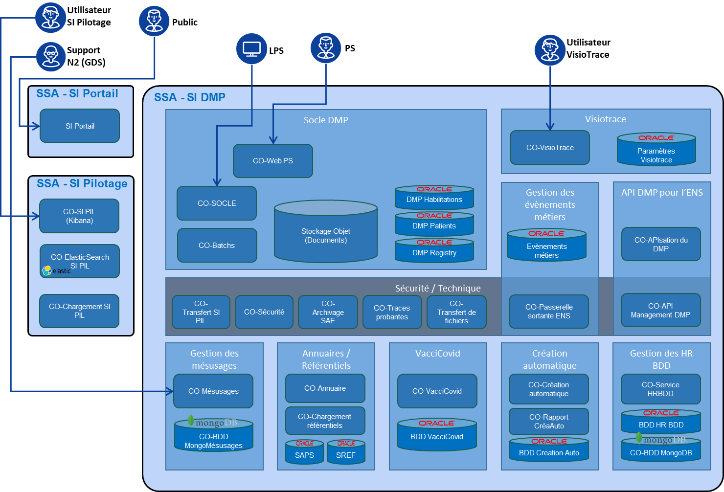
#### Gestion des mésusages



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-Mésusages : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.4
  + CO-BDD MongoMésusages : Annexe MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.4

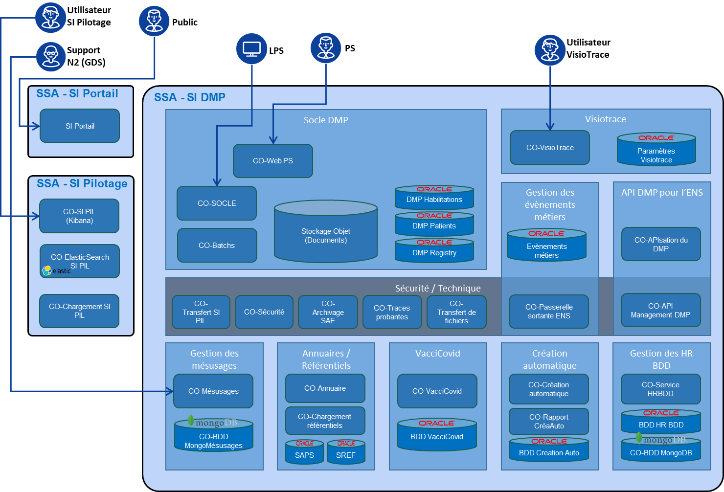
#### Annuaires / Référentiels



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-Annuaire : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.3
  + CO-Chargement référentiels : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.9

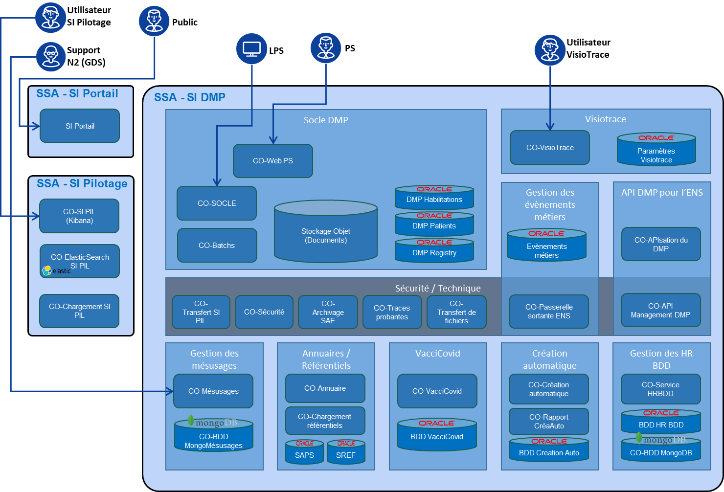
#### VacciCovid



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-VacciCovid : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique » : §4.8

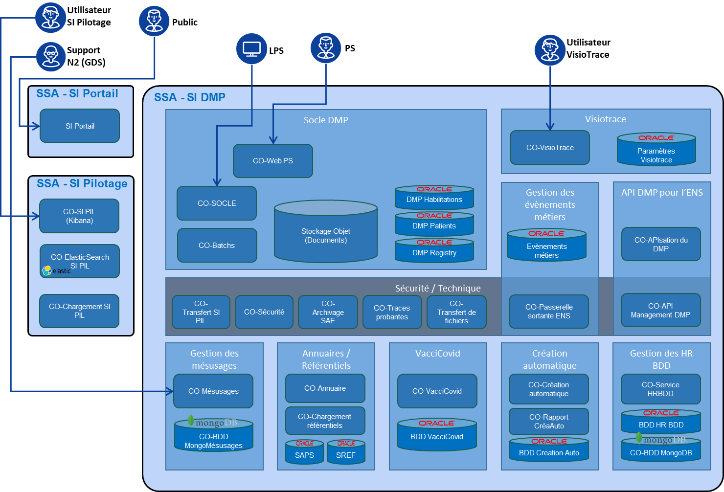
#### Création automatique



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-Création automatique : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.7
  + CO-Rapport CréaAuto « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.7

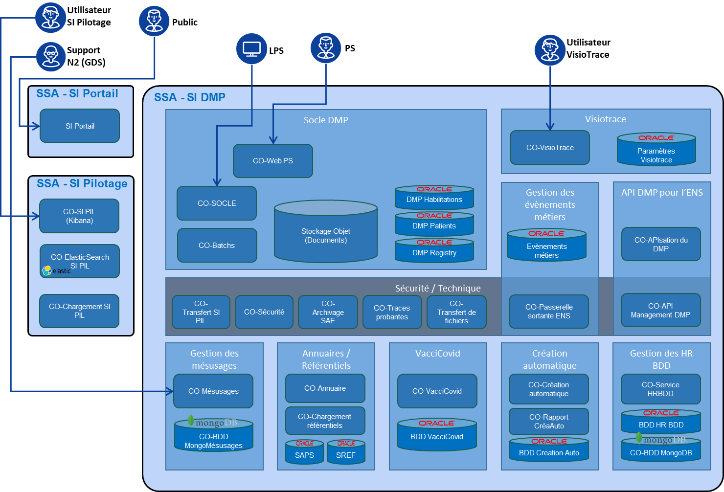
#### Gestion des HR BDD



L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-Service HRBDD : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.3
  + CO-BDD MongoDB : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.3

#### Sécurité / Technique

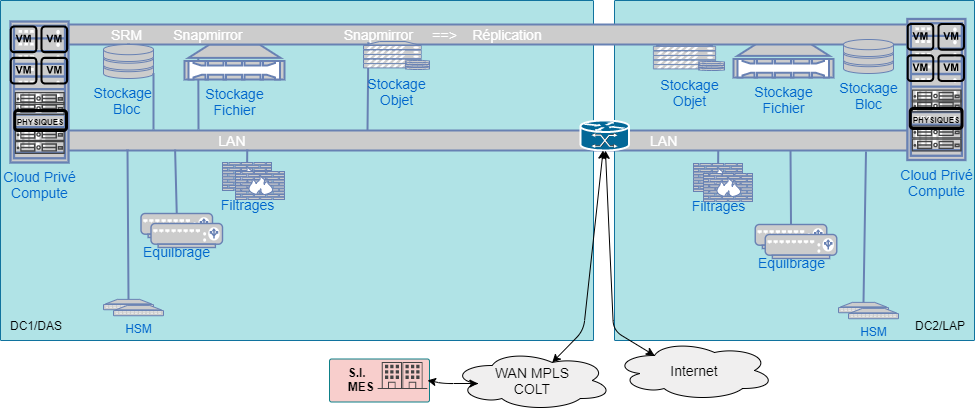


L’ensemble du détail de l’architecture de cette zone et du patrimoine applicatif qui la constitue se trouve dans les documents suivants :

* + CO-Transfert SI PIL : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.5
  + CO-Sécurité : Annexe « MESDMP\_Annexe 21\_DMP-AV-HSM »
  + CO-Archivage SAE : Annexe MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.12
  + CO-Traces probantes : Annexe MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.12
  + CO-Transfert de fichiers : Annexe MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.3, §4.7, §4.8, §6.6
  + CO-Passerelle sortante ENS « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.2 et 3.2.5
  + CO-API Management DMP : Annexe « MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique »: §4.6 et §3.2.3

### Architecture Technique du DMP

#### Présentation générale de DMP



Principaux composants de l’infrastructure DMP :

* + Deux datacenters situés en région lilloise :
* Le datacenter primaire, actif et supportant la totalité de l’activité ;
* Le datacenter secondaire, passif et destiné au secours (PRA).
  + Des équipements de l’hébergeur mutualisés vis-à-vis de ses différents clients : de bascule Internet, de sécurité mutualisés.
  + Des équipements dédiés au DMP : réseaux, de filtrage (firewalls et WAF), d’équilibrage, en clusters locaux au primaire, dupliqués dans le secondaire.
  + Une infrastructure Cloud privé proposant des serveurs virtualisés (VMWare) et physiques.
  + Trois systèmes de stockage : bloc, fichier (NAS) et objet (S3) répliqués vers le secondaire au rythme de leur mise à jour dans le primaire.
  + Quelques puits d’informations SGBD répliqués vers le secondaire au niveau middleware.
  + Sauvegarde.
  + Hébergement des infrastructures et services spécifiques au DMP (HDS).

#### Présentation détaillée de DMP

##### Les environnements

Il y a 2 types d’environnements :

* + L’environnement de production ;
  + Les environnements hors-production.

Les environnements hors-production sont présents sur le datacenter primaire uniquement, non intégrés dans le PRA. Les serveurs virtualisés de ces environnements sont gérés au sein d’un cluster VMWARE distinct.

L’environnement de production bénéficie de ses propres éléments d’infrastructure (serveurs, stockage, filtrage au moins).

##### Les éléments réseau et sécurité

|  |  |  |
| --- | --- | --- |
| Catégorie | Référence | Précision |
| Routage/Equilibrage | Big IP F5 DNS GSLB | Mutualisé pour l’ensemble des clients |
| Filtrage réseau DMZs ou front | Firewall Cisco ASA | Dédié DMP. (HA – DC1) (DC2 idem en PRA) |
| Filtrage réseau Zone Middle/Back | Firewall Checkpoint | Dédié DMP. (HA – DC1) (DC2 idem en PRA) |
| Filtrage applicatif (WAF, etc.) | Big IP F5 ASM | Dédié DMP. (HA – DC1) (DC2 idem en PRA) |
| Equilibrage | LVS, HaProxy | Dédiés DMP. (HA – DC1) (DC2 idem en PRA) |
| Boitiers HSM | Boitiers HSM Trustway Proteccio | Dédiés DMP. (HA – DC1) (DC2 50% en PRA) |

A ceci s’ajoutent les équipements Ethernet, routeurs filtrants, etc.

Une segmentation fine des VLAN est en place, permettant de différentier et isoler :

* + Les environnements ;
  + Les zones de l’application (serveurs frontaux, d’application, de données, de stockage, de clé, etc.) ;
  + Les zones d’administration.

Les éléments logiques du réseau :

* + La plage d’adressage IP utilisée sur l’infrastructure de DMP est 10.42. et 10.35.
  + Les flux sont systématiquement filtrés au niveau inter-VLAN (Firewalls L3 Statefull).
  + Le nombre de VLAN applicatifs de production du datacenter principal est de l’ordre de 15. les VLANs ne sont pas étendus entre les 2 datacenters.

##### Les éléments de calcul

Le datacenter secondaire est équipé de façon quasi identique au primaire. On trouve donc dans chacun des datacenter pour l’environnement de production :

* + Une dizaine de serveurs équipés d’ESXi intégrés en un cluster VMWARE ;
  + Une dizaine de serveurs « autonomes » ou intégrés dans des clusters de logiciels. Ne sont pas comptabilisés les serveurs sur lesquels s’appuient certaines des solutions de stockage.

Pour l’environnement de production, au sein du datacenter principal, une centaine de VM sont installées.

Parmi les serveurs physiques, se trouve un cluster Oracle RAC, avec 2 nœuds (16 cores/224Go RAM par nœud) en datacenter primaire et stockage (40To) en baie SAN. Une réplication Dataguard en mode passif sur le second cluster RAC en datacenter secondaire est activée.

##### Les éléments de stockage

Le datacenter secondaire est équipé de façon identique au primaire. On trouve donc dans chacun des datacenter :

* + Stockage mode bloc (Oracle/Mongo/ELK/Datastore des VM…) :
* Une baie de stockage de type HPE Primera A650,
* Une capacité utile de 130 To. Projection consommation à fin 2023, environ 50To. Croissance constatée 15To/an.
  + Stockage mode fichier (SAE, etc.) :
* Une baie de stockage à base de nœuds de type NetApp FAS2xxx,
* Une capacité utile de 140 To. Projection consommation à fin 2023, environ 40To. Croissance constatée 10To/an.
  + Stockage mode objet (Documents, etc.) :
* Un cluster S3 StorageGrid/Webscale, NetApp,
* Une capacité utile de 470 To. Projection consommation à fin 2023, environ 250To. Croissance constatée 50To/an.

Les outils de réplication NetApp et StorageGrid sont chargés de la duplication des données vers le datacenter secondaire.

##### Les éléments de sauvegarde

Le datacenter primaire dispose d’un système de sauvegarde s’appuyant sur un infrastructure mutualisée.

En outre :

* + La sauvegarde des données S3 (oobjet) s’appuie sur une infrastructure dédiée associée à la solution Point.
  + Le cluster Oracle-RAC : RMAN + Backup&Recovery de CommVault.
  + Les cluster MongoDB : Backup&Recovery de CommVault.
  + Le SAE : SnapVault de NetApp.

## Besoins d’évolution et convergence MES DMP

### Convergence entre MES et le DMP

Les besoins désignés infra sont inclus dans les prestations définies au §7.5 « P3 - Conv : Convergence des systèmes MES et DMP ».

| Besoins | Description générale |
| --- | --- |
| Mise en place d’une convergence | Mettre en place une convergence entre MES et DMP qui soit progressive, en tirant parti des ressources. |
| Enrichissement pendant la convergence | Pendant la convergence entre MES et DMP, conserver la capacité d’enrichir les produits (pas de période sans évolution visible par les usagers). |
| Convergence et continuité de service | Conserver une continuité de service lors de la mise en œuvre des opérations de convergence entre MES et DMP. |
| Décommissionnement du Web DMP | Décommissionnement progressif du Web DMP en fonction de la stratégie retenue par la Cnam quand la solution devant le remplacer sera opérationnelle, déployée et utilisée par les Professionnels de Santé. |

### Besoins d’évolution du système MES DMP

#### Feuille de route du numérique en santé 2023-2027

La première ambition affichée par la feuille de route 2023-2027 (cf <https://esante.gouv.fr/strategie-nationale>) consiste à faire entrer Mon espace santé dans la vie quotidienne des citoyens. Adossées à cette nouvelle version, plusieurs enjeux seront au cœur des développements du nouveau dispositif Mon espace santé - Bouquet de services aux professionnels, au premier rang desquels la généralisation des usages dans le quotidien des patients et des professionnels.

L’objectif affiché affiché dans la feuille de route 2023-2027 consiste à faire entrer Mon espace santé dans nos vies quotidiennes. Après la généralisation de Mon espace santé au S1 2022, l'objectif principal des développements du dispositif MES-BSP sera dorénavant de créer suffisamment de valeur pour rencontrer un usage massif et changer les habitudes de tous, patients comme professionnels de santé (pour les citoyens, il s’agit de récupérer systèmatiquement ses documents de santé à la sortie de chaque épisode de soin, partager son ordonnance avec son pharmacien, suivre le parcours de santé de ses enfants…). À date, plus de 93% des citoyens disposent d’un profil MES, et 13% d’entre eux s’y sont déjà connectés une fois. L’enjeu est de largement développer l’activation pour l’ensemble de la population et de construire des parcours adaptés, favorisant la retention et la régularité des usages pour les personnes qui en ont le plus besoin (parcours maladies chroniques et familles).

Une ambition forte est de poursuivre le développement Mon espace santé en miroir d’un nouveau projet associé, le Bouquet de services aux professionnels. Cela permettra de faciliter les accès de tous professionnels de santé (libéraux, en établissement sanitaire, en établissement médico-social, etc.) aux données des profils Mon espace santé des patients qu’ils prennent en charge, via des API intégrées à leurs logiciels métiers – qui évoluent en ce sens dans les vagues du programme Ségur Numérique – et via un portail Web BSP (pour les professionnels, il s’agit notamment de fluidifier l’accès aux informations médicales et administratives nécessaires à la prise en charge et de classer cette information da façon pertinente pour en simplifier l’usage).

Les fonctionnalités de MES/BSP ont vocation à s'étendre en fonction des besoins professionnels et ainsi que des usages citoyens identifiés.  La feuille de route du Numérique en santé prévoit notamment des évolutions sur Mon espace santé sur le carnet de santé de l’enfant, la prévention personnalisée, la consultation des images en radiologie (projet DRIM-M, basé sur un index / lien dans les compte-rendus d’imagerie alimentés à Mon espace santé, permettant d’accéder aux PACS distants), la déléguation d’accès à un aidant (au delà de délégation automatique mineurs vers parents), l’amélioration significative des possibilités d’expression de ses préférences d’accès (autorisation manuelle d’un professionnel, organisation de la délégation inter-professionnelle, expression des préférences sur la réutilisation secondaire, etc.), la meilleure exploitation des données des historiques de remboursements et autres documents structurés (biologie pour le groupe sanguin, ...), etc.

En particulier, dans le cadre du projet de développement d’un prévention personnalisée dans Mon espace santé, soutenue par les [recommandations citoyennes](https://esante.gouv.fr/sites/default/files/media_entity/documents/221204_avis-comite-citoyen_vdef.pdf) dans ce domaine, les données alimentées par les professionnels et les usagers (et leurs services référencés) ont vocation à être exploitées au sein de Mon espace santé dans le but d’apporter plus de valeur à l’usager (recommandations, contenus personnalisés, etc.). Les éléments et fonctionnalités relatifs à la prévention pourront ainsi être développés afin de personnaliser le contenu proposé aux usagers, en fonction de leur profil et sur la base du consentement de ces derniers. En permettant des rappels personnalisés selon les pathologies ou selon des profils identifiés, l’usager pourra ainsi être engagé dans un parcours de santé dynamique. Par exemple, des recommandations de visite à un dentiste pourraient être poussées par rapport à la date des dernières consultations. Par extension, un volet d’informations relatives à la situation socio-économique de l'usager pourra par exemple être intégré à MES afin de relayer plus largement les politiques de santé publique.

Pour piloter finement de le déploiement de ces usages, une attention toute particulière sera porté à l’évolution des outils de suivi et de pilotage (knowage, SI pilotage DMP…) afin de disposer d’éléments d’analyse fine des parcours utilisateurs, des comportements des professionnels et des enjeux prioritaires liés à l’activation par les citoyens, l’alimentation et la consultation par les professionnels ainsi que la fréquence des usages et la rétention du côté des utilisateurs « patients ».

Par ailleurs, l'exploitation des données de santé des usagers à des fins secondaires (recherche, innovation, pilotage des politiques publiques, etc.) constitue une opportunité de développement, qu’il conviendra de travailler avec les citoyens, dans le cadre juridique en vigueur.

Enfin, de par son ouverture aux services proposés par des tiers, Mon espace santé a vocation à s’enrichir en proposant au fil du temps de plus en plus de services du marché à l’usager. L’ouverture des échanges de données avec les services référencés de son choix au sein du catalogue de services ira dans le sens d’une augmentation les usages en rassemblant les données de santé des usagers dans le carnet de santé électronique des citoyens Mon espace santé, tout en ouvrant ces données aux professionnels et aux services tiers auxquels le patient consent. Cette démarche d'ouverture et d’échange avec des tiers impliquera de s'assurer que les éditeurs référencés se conforment aux critères retenus et à l’état de l'art en matière d'interopérabilité, d'éthique, de conformité juridique et d'exigences de sécurité.

De manière générale, dans la continuité de ce qui a déjà été entrepris, la prise en compte d’une démarche RSE intégrée constituera une priorité clé, notamment à travers des thématiques d’'éco-responsabilité, éco-conception et d'accessibilité dont les exigences continueront à être pleinement intégrées au le développement du site et de l'application Mon espace santé, au regard notamment des critères mesurés par l'Eco-score ainsi que le RGAA.

De façon coextensive, l'exploitation des données de santé des usagers selon les règles juridiques et RGPD en vigueur constituent une opportunité de développer leur utilisation secondaire dans le cadre de la recherche en santé numérique. Ces projections d’usage sont un enjeu majeur de l’architecture du système Mon espace santé DMP. Ce point sera détaillé dans les prochaines versions du CCTP.

#### Les besoins du métier au-delà des fonctionnalités

Au-delà des attendus relatifs à des fonctionnalités ou parcours amenés à servir l’ambition de faire croitre les usages de Mon espace santé et du DMP, et construits sur la base de la construction de cas qui émergent au fur et à mesure, le Titulaire complète le dispositif organisationnel existant pour contribuer efficacement au cycle d’évolution du système Mon espace santé DMP. Ses axes d’intervention doivent répondre aux attentes exposées dans les chapitres ci-dessous.

##### Continuité de service et disponibilité

Le système Mon espace santé DMP est un système adressant à la fois le grand public à l’échelle de l’ensemble de la population (BtoC), et les professionnels de santé (BtoB), en direct ou via les logiciels métier développés par des éditeurs. Mon espace santé DMP est le fer de lance, la partie visible de l’iceberg du numérique en santé. De ce fait, pour les 2 publics, la qualité de service doit être de haut niveau : peu de bug ou d’incidents, des délais de recouvrance en cas de bugs ou d’incident courts, et une haute disponibilité, incluant le principe de minimisation des indisponibilités, y compris programmées. Quand elles sont impératives, les indisponibilités doivent être programmées sur des plages horaires impactant le moins possible les utilisateurs. Le Titulaire doit éclairer les conditions et mettre en place l’organisation et les outils permettant de répondre à cet attendu, y compris pour la pahse d’initialisation du présent accord-cadre et pour la phase de convergence des 2 systèmes. Les indicateurs relatifs à la disponibilité du système sont précisés au §6.2.3.

##### Supervision et communication sur incidents

La supervision des 2 systèmes Mon espace santé et DMP, puis du système convergé est indissociable de la qualité de service attendue. Le Titulaire doit mettre en œuvre l’organisation et les outils nécessaires à une supervision métier, appuyée sur la supervision technique et applicative, mais toujours vue du point de vue de l’utilisateur final, qu’il soit usager ou professionnel de santé. Cette exigence emporte également la nécessité d’application de processus de communications permettant aux autres acteurs impliqués d’avoir le bon niveau de visibilité pour mener à bien leurs propres actions. Au titre de ces acteurs, on compte les acteurs en charge du support (support téléphonique et mail de niveau 1, externalisé et ou en caisse, à l’attention des usagers ou des professionnels de santé, GIE Sesam Vitale pour le support aux éditeurs, etc.), de la communication (en lien avec toute opération de communication ou évènement pouvant être impacté par un dysfonctionnement, et impliquant un risque d’image pour l’institution), de l’accompagnement auprès des publics (en CPAM et en ARS-Grades). A l’échelle du produit Mon espace santé DMP, ces acteurs se comptent par centaines.

##### Gestion de l’innovation et de l’écoute client

Pour répondre à l’enjeu d’adoption des prochaines années pour les deux publics concernés par Mon espace santé à savoir les usagers et les professionnels de santé, il est nécessaire :

* + De connaître nos utilisateurs de manière concrète et opérationnelle : avoir un dispositif continu de remontée de leurs propositions d’amélioration et de détection des anomalies ; avoir la capacité de tester auprès d’eux des améliorations ou de nouveaux services avant de lancer leur développement ; avoir la capacité de suivre et d’évaluer après l’ouverture la qualité des nouveautés et leur adoption sur le terrain ;
  + D’être en capacité de détecter les services innovants qui permettent de privilégier à la fois les activations et les usages de Mon espace santé avec un regard sur les usagers mais également les professionnels en articulation avec la mise en œuvre du Bouquet de services aux professionnels.

Sur le volet écoute client, le Titulaire doit proposer des méthodes éprouvées et/ou novatrices ainsi que des outils permettant de parfaire la connaissance client. Il s’agit, par exemple, d’accompagner les acteurs de la Cnam avec ces propositions afin de mieux connaître leurs usagers, leurs comportements sur le produit, potentiellement l’impact du comportement des professionnels sur l’utilisation de Mon espace santé par les usagers. Ces propositions peuvent prendre différentes formes selon l’expérience du Titulaire : formation / accompagnement dans la mise en place d’un panel utilisateurs et dans l’organisation de son fonctionnement et les outils pour l’animer, mise en place de métriques et d’outils pour suivre le comportement avec les modalités organisationnelles associées à ce recueil d’informations et à leur suivi. Le Titulaire propose des profils adaptés pour accompagner cette écoute client et précise l’articulation des ces travaux avec le fonctionnement général des évolutions de Mon Espace Santé dans la feuille de route du produit.

Sur le volet innovation, le Titulaire doit proposer une méthode de travail, une organisation et des outils permettant d’identifier des services innovants susceptibles de susciter fortement l’adoption. Pour ce faire, il propose :

* + Une organisation pour réaliser une veille fonctionnelle et technique au niveau de l’accord-cadre et permettant d’identifier des services à valeur ajoutée susceptibles de créer l’adhésion du plus grand nombre ;
  + Les modalités d’analyse des services identifiés afin de confirmer l’opportunité de la mise en œuvre : tests auprès des publics (usagers / PS / établissements) ; modalités d’intégration dans MES et de mise à disposition des professionnels le cas échéant ; analyse de faisabilité et de coût ; estimation des usages, etc.
  + Les modalités (fonctionnelles, organisationnelles, juridiques et financières) de mise en œuvre de ces fonctionnalités au sein de MES y compris lorsque ces services existent et sont offerts par des acteurs tiers hors Cnam et Titulaire ;
  + L’articulation de ces travaux avec le fonctionnement général des évolutions de MES dans la feuille de route du produit ;
  + L’évaluation de l’adoption de ces services par les usagers.

La Cnam attend des propositions sur l’évaluation des métriques valeur métier de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

##### Pilotage / statistiques

Comme le décrit le §3.5.4.2.3 sur l’écoute client, le suivi des usages et des parcours utilisateurs revêt un enjeu majeur. Cet enjeu concerne tant la vision des usages par les usagers que par les professionnels pour être en mesure d’identifier des comportements des uns impactant le comportement des autres. Ceci implique la capacité à construire des indicateurs transverses, à être en capacité de les faire évoluer à chaque fois que les usages à mesurer vont évoluer, et enfin de restituer ces mesures aux différents acteurs afin qu’elles soient utiles dans la construction du produit mais surtout de l’accompagnement qui est fait sur le terrain auprès de ces publics.

Aujourd’hui, deux systèmes de pilotage différents existent, l’un dédié à MES et l’autre au DMP. Ces outils sont indispensables actuellement afin de garantir un suivi des usages et notamment, pour ce qui concerne le DMP, dans l’usage professionnel, le suivi du déploiement Ségur, des indicateurs conventionnels, et l’outillage des équipes terrain qui accompagnent le déploiement.

Le Titulaire doit maintenir ces deux solutions le temps de la mise en œuvre effective de la convergence entre les deux systèmes.

Pendant la période nécessaire de continuité de services des deux systèmes de suivi des usages de Mon espace santé et du DMP, pour répondre à l’enjeu des usages le Titulaire propose :

* + Les modalités de production d’indicateurs consolidés entre les deux systèmes afin de répondre au plus vite au besoin d’une vue globale ;
  + Les outils et systèmes nécessaires à cette production.

En parallèle, le Titulaire propose une cible pour la gestion des données d’usage et de la production d’indicateurs. Cette cible doit impérativement intégrer plusieurs dimensions :

* + La capacité d’enrichir très rapidement des indicateurs d’usage dès que le suivi d’une fonctionnalité, d’une version d’un parcours utilisateur le nécessite y compris en ayant la vue des professionnels avec l’usage DMP ;
  + La capacité de produire des indicateurs et tableaux de bord de manière automatisée ;
  + La capacité de décliner la restitution des informations d’usage en fonction des besoins : suivi macro pour une vision politique, suivi en profondeur et individualisé pour des acteurs terrain, suivi des parcours en fonction de profils pour les évolutions et évaluations du produit, etc. ;
  + Un système avec des outils permettant à des utilisateurs non statisticiens ou datascientist de l’utiliser ;
  + Une dimension technologique éprouvée. Le Titulaire peut utilement présenter des expériences sur des produits similaires.

Les ou les systèmes de pilotage doivent être adaptables dans le même rythme que Mon espace santé/DMP. Les développements afférents doivent être réalisés sur le modèle d’une organisation agile et répondre aux exigences exprimées par ailleurs dans ce CCTP.

Le pilotage des évolutions du système fera l’objet d’une comitologie spécifique permettant de s’assurer régulièrement de l’adéquation des données produites aux besoins de pilotage de l’ensemble des produits.

Il est attendu que la continuité des fonctionnalités de webanalytics assurées par AT internet et Commanders act soit assurée selon le même modalités : licences fournies par la Cnam, reprise du plan de taggage et des tableaux de bord, et exploitation par le titulaire.

La continuité de production des livrables (en particulier infographies et analyses des données) doit être assurée, et complétée au fur et à mesure par de nouveaux livrables récurrents ou adhoc en réponses aux besoins exprimés.

##### Adaptation du marché

Afin de s’assurer une adaptabilité par rapport aux évolutions qui pourront être matérialisées dans le cadre de la prestation couverte par le marché, une clause de revoyure doit permettre d’ajuster les attendus à la vue de l’évolution du contexte du projet. Il s’agit d’un des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

##### Conception basée sur la donnée et l’observation des usages

###### Evolution des Personas et études utilisateurs

Les personas de Mon Espace Santé ont vocation à vivre, être complétés, pour affiner au fur et à mesure des apprentissages la connaissance du niveau d’interaction et d’attente des segments d’utilisateurs de Mon Espace Santé en fonction de leur profil.

Les caractéristiques des 3 persona pré-cités sont complétés au fur et à mesure de l’évolution de Mon Espace Santé (couverture fonctionnelle, nouveaux cas d’usages, niveau de déploiement, situation conjoncturelle, etc.). D’autres personas sont également crées au fur et à mesure de l’affinage des parcours utilisateurs visés. De nouveaux personas sont déjà envisagés sur de nouvelles tranches d’âge, notamment en lien avec l’orientation stratégique de faire de la prévention personnalisée.

###### Expérience utilisateurs / tests utilisateurs

En vue d’enrichir les personas, afin de bénéficier de retours utilisateurs qualifiés et ciblés, une communauté d’usagers Mon espace santé a été recrutée depuis Mon espace santé. Cette communauté peut être sollicitée par e-mail pour répondre à des questionnaires ou être invitée à des focus group par exemple.

En complément de cette communauté, le Titulaire doit activer des dispositifs de sélections d’usagers pour constituer des panels permettant de tester des maquettes, des idées ou concepts qui servent de base à l’établissement de la feuille de route opérationnelle ou guident le choix d’implémentation de certains parcours utilisateurs. Ce dispositif doit être activable de manière récurrente dans le cadre de la préparation en incrément n de l’incrément n+1.

Ces démarches s’appuient sur des outils à fournir par le Titulaire, tels que :

* + Outil de recherche utilisateur, tests d’utilisabilité, interview type lookback
  + Interface de design collaboratif type Figma et Figjam
  + Outil en appui à la recherche utilisateur, allant de la description des protocoles d’expérience à des recommandations UX, type glean.ly
  + Outil de gestion de questionnaires, QCM, enquête de satisfaction personnalisés en ligne, type Eval&Go

Le Titulaire peut proposer des outils similaires, mais doit dans ce cas, s’attacher à récupérer toute la connaissance déjà acquise précédemment.

##### Conception agile

###### Conception incrémentale

Le Titulaire doit apporter sur l’ensemble des chantiers, quelle qu’en soit la nature, une approche fondée sur les principes de l’agilité, selon une approche pragmatique, itérative, concentrée sur la maximisation de l’apport de la valeur aux usagers tout en minimisant les coûts et délais de mise en œuvre. Toute nouvelle fonctionnalité, tout nouveau parcours, conçu sur le fondement de la recherche utilisateurs, doit être vue par un prisme « Minimum Viable Product », tout en gardant le recul nécessaire pour qu’il ou elle puisse s’intégrer de manière cohérente dans le produit pré-existant, afin d’éviter notamment l’effet « mille-feuilles » de fonctionnalités non coordonnées qui ne seraient pas comprises de nos usagers. Cette approche vaut pour l’ensemble des produits et chantiers engagés au titre de Mon espace santé et du DMP (et leurs produits associés). Toute évolution de Mon espace santé et du DMP doit systématiquement s’accompagner d’une analyse d’impact sur le système de pilotage des données, le portail de support, etc.

Du point de vue des usagers finaux (citoyens et professionnels de santé), les versions des produits Mon espace santé et DMP (API exposées à tiers comprises) doivent avoir des rythmes d’évolution courts, tels que présentés pour Mon espace santé, pour contribuer de manière efficace, pertinente à la croissance des usages du numérique en santé.

Les observations et la recherche utilisateurs faites sur les premières versions des fonctionnalités ou parcours guident les évolutions suivantes, selon le cycle classique d’amélioration continue de la valeur apportée. Cette dernière peut être une valeur directe ou indirecte en cas d’amélioration moins visible du point de vue de l’usager mais allant vers plus d’industrialisation des processus. Au titre de l’industrialisation de la conception, le Titulaire doit reprendre l’ensemble du patrimoine y concourant : maquettes dynamiques, Design system notamment pour gagner du temps en conception, sécuriser les implémentations, faciliter les tests et le support.

###### Delivery agile à l’échelle

Le périmètre adressé par le présent accord-cadre est un périmètre large et hétérogène :

* + Clients : usagers à hauteur de la population, professionnels de santé
  + Expositions web, mobile, API pour tiers
  + Produits externes et produits « internes », s’adressant néanmoins à des publics également très variés (Cnam, MSA,prestataires de support, éditeurs, institutionnels, etc.) : portail de support, Systèmes de pilotage, CMS, outils d’administration

L’organisation des chantiers, et leur extrème coordination, est un facteur essentiel à la réussite des itérations des différents produits.

Si l’organisation actuelle sur Mon espace santé peut être qualifiée de « safe-like » (équipes organisées autour de features, rituels assimilables à la gestion d’un release-train) et constitue un modèle intéressant duquel il convient de s’inspirer, il importe que le Titulaire fasse par ailleurs des propositions concrètes pour mener à bien la convergence organisationnelle de travail souhaitée : aller vers une organisation agile de l’ensemble de l’activité (i.e tous les produits du périmètre), tout en gérant l’hétérogénéité des chantiers sur l’ensemble des produits, en fonction des différentes phases de l’accord-cadre (initialisation, convergence technique / fonctionnelle, rythme de croisière sur le système cible). Pour cela, le Titulaire doit conjuguer une forte stabilité des équipes staffées sur les chantiers, afin de bénéficier sur du temps long de l’apprentissage individuel de chacun et de la dynamique de groupe, et une capacité d’adaptation systémique à appliquer à chaque changement de contexte du portefeuille des chantiers à mener.

###### Validation / recette

La qualité des logiciels livrés et mis à disposition de nos usagers est fondamentale à plusieurs titres :

* + Les services proposés portent intrinsèquement l’exigence de la qualité nécessaire au maintien de la confiance accordée par les usagers à ces services, synonyme de la poursuite du développement des usages en masse.
  + La maîtrise par la Cnam du dimensionnement de son support de niveau 1 (usagers et professionnels de santé) doit être assurée, et ne pas subir d’effet volume lié au fait que le niveau de recours au support de niveau 1 est directement proportionnel au niveau de bugs rencontrés par les usagers.

Au vu du volume d’utilisateurs de Mon espace santé et du DMP, et au rythme des versions de produits attendus, le Titulaire doit mettre en place une organisation adaptée à l’enjeu de la validation des produits délivrés. Les principes classiques de la recette agile doivent être appliqués : implication au plus près des équipes de développement, automatisation des tests au maximum. La forte intégration de multiples systèmes d’information dans l’éco-système Mon espace santé DMP demande également une attention particulière, à couvrir par des tests à réaliser de bout en bout de l’ensemble des systèmes impliqués. Le Titulaire propose, quand la nature des chantiers le permet, des modes d’organisation alternatifs permettant de réduire au maximum les délais et les risques entre l’expression d’un besoin et sa mise en service pour les usagers.

###### Déploiement continu

D’un point de vue organisationnel, en lien avec la complexité de l’éco-système Mon espace santé DMP, en particulier le nombre d’environnements nécessaires à l’offre de service (environnements de développements, de tests, d’intégration, de tests de bout en bout, à destination des éditeurs du catalogues de service, de la DMP compatibilité, pour les tests des opérateurs de MSS professionnels de santé, et autres usages tels qu’environnement de démonstration), le Titulaire doit outiller ses déploiements de manière automatisée sur tous les environnements, assurer la maîtrise des déploiements (en limitant les opérations manuelles) et sécuriser ainsi les délais de mise à disposition des versions sur l’ensemble des environnements.

D’un point de vue métier, le Titulaire doit mettre en place, dès la prise de connaissance et l’initialisation, les moyens techniques et organisationnels pour rendre possible des déploiements sous forme de canari tests, consistant à déployer une fonctionnalité ou un parcours sur un sous ensemble de la population cible. Ce déploiement ayant pour but de maîtriser la mise en ligne d’une nouvelle fonctionnalité, d’être en mesure de canaliser les retours terrains afférents et de pouvoir gérer des ajustements, correctifs et évolutifs avant de lancer la fonctionnalité ou le parcours considéré à l’échelle de l’ensemble de la population. Les critères de sélection de la sous-population concernée peuvent être divers : géographique, âge, canal web ou mobile, usagers ayant déjà engagé un parcours lié au parcours à tester, sur la base du volontariat d’utilisateurs, au hasard dans la limite d’un quota, etc.

##### Administration

Mon espace santé DMP est un système complexe, sur lequel porte un véritable enjeu de dynamisme et de réactivité. Malgré le périmètre croissant de fonctionnalités, parcours et services proposés aux différents types d’utilisteurs des produits, le Titulaire doit proposer des outils et des organisations permettant au maximum une administration décorellée des process de delivery et des versions d’applicatifs. Les principaux champs sur lesquels il est attendu des solutions d’administration, éventuellement à la main d’autres acteurs que le Titulaire (comme la Cnam ou un de ses sous-traitants) en charge de l’exploitation du système sont présentés ci-après. Le principe de prévoir des moyens d’administration hors exploitant prévaut à chaque fois que cela paraît pertinent.

###### Content Management System (CMS)

Les outils de CMS permettent d’ajouter supprimer, modifier le contenu des pages des sites, indépendamment des mises en production.

L’objectif est de rendre l’intégralité des contenus de Mon espace santé / DMP gérable via CMS afin de donner à la Cnam la latitude pour pouvoir adapter à chaud ces contenus.

Au vu de l’importance croissante des besoins éditoriaux des sites, l’outil CMS doit :

* + Pouvoir répondre à des enjeux de planification et automatisation de la diffusion des contenus éditoriaux selon un calendrier défini
  + Permettre de prévisualiser le rendu des contenus avant la mise en ligne
  + Pouvoir cibler l’affichage des messages en fonction de critères de segmentation (âge, sexe, activité dans Mon Espace Santé, données personnelles connues de Mon Espace Santé ou de l’Assurance Maladie, etc.)
  + Permettre une utilisation facilitée via une interface *user friendly* (pas de connaissance HTML ou informatique spécifique pour ajouter des contenus)
  + Permettre la gestion d’images et illustrations
  + Permettre la gestion de plus en plus de pages de Mon espace santé
  + Permettre que de multiples acteurs puissent gérer des contenus (prévoir une hiérarchie des droits : validateur, éditeur, modérateur, etc.)

Au-delà des besoins éditoriaux exprimés ci-dessus, le principe d’un CMS « augmenté » de type Plateforme d’expérience Digitale permettrait de répondre au besoin de plus en plus prégnant de personnalisation des contenus en fonction de critères caractérisant tel ou tel segment d’usagers.

###### Autres besoins d’administration

L’environnement dit Editeur, initialement dédié au référencement des services tiers candidats au référencement Mon espace santé évolue pour répondre à d’autres besoins, notamment pour permettre le processus de DMP-compatibilité pour les éditeurs de logiciels métiers à destination des professionnels de santé, pour permettre aux opérateurs de Messagerie sécurisée de santé aux professionnels de santé de faire des tests d’interfaçage de leurs services avec la messagerie sécurisée citoyenne.

Du fait de cette évolution projetée des usages de l’environnement Editeur, le périmètre fonctionnel du Portail d’administration peut, le cas échéant, évoluer et aller vers des fonctionnalités d’administration plus larges, couvrant les usages pré-cités, ou permettant de disposer de Mon espace santé dit de démonstration ou test. Les modalités d’administration de ces nouveaux contextes restent à construire à la date de rédaction du présent CCTP, en particulier pour construire l’offre de services destinée à la gestion des comptes fictifs et à mettre à disposition des usagers (création, suppression, remise à 0, etc.), les jeux d’essais et bouchons techniques associés (limitant l’adhérence avec les systèmes d’information hors du périmètre de l’exploitant), la gestion des comptes d’accès aux outils type CMS ou SI Pilotage, etc.

##### Accompagnement technico organisationnel

###### Accompagnement RGPD

Au vu du périmètre large adressé sur l’ensemble Mon espace santé et DMP, de la sensibilité des données gérées, de la complexité d’exercice des droits des utilisateurs usagers et professionnels de santé, et du rythme attendu sur les évolutions visées, le Titulaire doit proposer un accompagnement spécifique de la prestation en matière d’application du RGPD. Cette prestation consiste au suivi des travaux, conseil aux équipe en matière de RGPD pouvant influer sur les modalités d’implémentation, mise à jour de l’ensemble de la documentation RGPD, en particulier EIVP/AIPD. Ces prestations s’exécutent au fil des versions évolutives des systèmes puis ensuite sur le système convergé. Elles se font sous le pilotage des services juridiques de la Cnam.

###### Accompagnement au référencement et événements

Le Titulaire doit prévoir une organisation permettant d’accompagner la gestion du catalogue de services référencés Mon espace santé. En marge du delivery des API et interfaces nécessaires pour le catalogue de services, cette prestation inclut le support aux éditeurs dans leurs accrochages au SI Mon espace santé et son industrialisation. Le Titulaire travaille, sur ce point, en coordination avec le GIE Sesam Vitale. Cette prestation inclut également la participation, voire l’organisation d’évènements type conférences, hackathon / projectathon pour permettre l’émergence de nouveaux besoins (fonctionnels, organisationnels, etc.).

#### Prévision des futurs besoins fonctionnels

Les besoins décrits ci-après sont fournis à titre informatif et ne sont pas exhaustifs.

Ils ont pour but de présenter des évolutions de Mon Espace Santé et du DMP pouvant être réalisées pendant le durée d’exécution de l’accord-cadre, dans le cadre de bons de commande. Dans le cas ou une évolution aurait été mise en œuvre avant la notification de l’accord-cadre, elle constitue du patrimoine à faire évoluer dans le cadre d’une démarche d’amélioration continue.

##### Identification/Enrôlement/cohérence avec les identités du point de vue des PS

| Fonctionnalités | Description générale |
| --- | --- |
| Enrôlement mineurs | Offrir la possibilité à un jeune mineur de se connecter à son Mon espace santé avant ses 18 ans. Définir de manière collatérale quels sont ses droits et ceux de ses responsables légaux sur ses données et documents de santé. |
| Nouveaux nés | Récupérer les données de santé des nouveaux nés au plus près de la naissance, en tenant compte du principe d’opt-out qui sera soumis à ses représentants légaux selon les principes déjà en place (mécanisme basé sur l’ouvrant-droit principal connu de l’Assurance Maladie) |
| Nouvelle campagne d’enrôlement | Mener de nouvelles campagnes d’enrôlement pour parvenir à proposer Mon espace santé à des populations qui n’ont pas pu être enrôlées dans la campagne de masse pour des raisons techniques notamment |
| Gestion des NIA | Gérer des Espaces Santé pour les personnes immatriculées au SNGI avec un numéro d’identification provisoire (NIA, en particulier les populations bénéficiaires de l’aide médicale d’Etat – AME) |
| Enrôlement population particulière | Permettre l’enrôlement des populations particulières à travers la définition des aidants / aidés et des tutelles |
| Enrôlement via FC | Réaliser un enrôlement pour des usagers via France Connect (niveaux eiDas à préciser en fonction des exigences sécurité) |
| Opt-in via appli carte vitale | Déployer l’activiation en opt-in par authentification appli carte Vitale |
| Capacité de relance des activations | Réaliser un suivi des activations, en ciblant et en incitant les usagers qui n’auraient pas activé leur Mon espace santé à le faire. |
| Obtention de l’INS | Permettre au système Mon espace santé DMP d’interroger le service INSi afin de procéder à de la réconciliation d’identité en cas de doute (raisonnable / maîtrisé) sur une identification DMP / Mon espace santé |

##### Authentification

| Fonctionnalités | Description générale |
| --- | --- |
| FranceConnect + | Prévoir de mettre en place une authentification via France Connect+ (fournisseurs d’identité eIDAS 2 ou 3), sans facteur complémentaire envoyé par Mon espace santé, en complément de la fonctionnalité actuelle d’authentification par France Connect (fournisseurs d’identité eIDAS 1 ou 2 ou 3) avec facteur complémentaire envoyé par Mon espace santé. |
| TOTP | Mettre en œuvre un Timebased One Time Password comme solution d’authentification forte à MES (via l’application MES elle-même ou via une application spécialisée souveraine). |
| Amélioration biométrie | Améliorer le parcours biométrique pour la connexion à l’application mobile, voir pour l’implémenter sur d’autres OS (Mac / PC). |

##### Gestion des comptes

| Fonctionnalités | Description générale |
| --- | --- |
| Evolution id administratives | Permettre au système d’accepter les appels pour transmission des évolutions de données d’identité administratives (y compris la date de décès) – abonnement – mode évènementiel si l’implémentation n’a pas été finalisée au lancement du marché. |
| Evolution gestion IR | Permettre au système d’accepter les appels pour transmission des évolutions de données liées à la gestion par le régime d’Assurance Maladie du titulaire (y compris les coordonnées) – abonnement – mode évènementiel |

##### Consentements

| Fonctionnalités | Description générale |
| --- | --- |
| Consentement ouverture des données non anonymisées | Gérer le consentement pour le partage des données non anonymisées (mais pouvant être pseudonymisées) avec des tiers (ex : HDH, Open AI, Santé Publique France, INSERM, etc.) |
| Partage de données anonymisées | Partager des données anonymisées de masse n’ouvrant pas à l’obtention d’un consentement. |
| Choix concernant la réutilisation secondaire | Le titulaire peut renseigner ses choix vis à vis de la réutilisation secondaire de ses données pour certaines finalités (recherche, etc.). |
| Rendre consommable par d’autres services les préférences des citoyens vis à vis de leurs données | Les préférences d’accès fixées par le citoyen dans Mon espace santé peuvent être consommables par API (MES ou BSP) par d’autres services (Dossier patient informatisé local, Plateforme des données de santé, etc.), afin d’éviter que le patient ne doive ré-exprimer ses choix à chaque fois auprès de chaque interlocuteur du système de santé. |

##### Délégation d’accès à un tiers professionnel

| Fonctionnalités | Description générale |
| --- | --- |
| Permettre à un professionnel de déléguer un accès à d’autres professionnel | Prévoir que via le dispositif MES BSP le professionnel – éventuellement uniquement le médecin traitant pour commencer - puisse déléguer des accès à un autre professionnel, en transparence et contrôle du titulaire |

##### Expérience utilisateur, ergonomie et facilité d’utilisation de la solution

| Fonctionnalités | Description générale |
| --- | --- |
| Accessibilité pour non francophone | Disposer d’un site fonctionnel avec une langue autre que le français |
| Accès BSP | Permettre dans le BSP un accès via le portail Sesali à des PS européens aux documents de santé d’un usager, sans contrôle d’identité vis-à-vis d’un référentiel de Professionnels. |
| Fournir proactivement un accès à un professionnel ou répondre à sa demande d’accès | Pour certains cas d’usages (professionnels hors matrice d’habilitation, médecine du travail, professionnels européens via le réseau MaSanté@UE, etc.) le patient doit pouvoir proactivement exprimer dans Mon espace santé son accord pour l’accès d’un professionnel, ainsi que répondre à une demande d’un professionnel qui lui serait notifiée. |

##### Services tiers en santé et bien-être

| Fonctionnalités | Description générale |
| --- | --- |
| Version des API | Gérer le versioning des API à destination des éditeurs de solutions référencées au catalogue de services. |
| API client de messagerie citoyenne pour les applications du catalogue MES | Création d’une API du catalogue de services Mon espace santé permettant de relever les messages de la boite de messagerie citoyenne Mon espace santé |
| API pour le catalogue BSP | Créer des API BSP équivalentes à celles du catalogue MES, en complément de ce qui existe déjà (TLSi, DMP intégré), pour les solutions aux professionnels |

##### Gestion du site MES et des sites institutionnels

| Fonctionnalités | Description générale |
| --- | --- |
| Changements ergonomiques | Réaliser des changements ergonomiques sur le site pour permettre de répondre aux usages qui peuvent évoluer durant l’accord-cadre. |
| Planification et automatisation | Permettre à l’outil CMS de répondre à des enjeux de planification et d’automatisation de la diffusion des contenus éditoriaux selon un calendrier défini |
| Prévisualiation du rendu | Permettre à l’outil CMS de prévisualiser le rendu des contenus avant la mise en ligne |
| Affichage selon segmentation | Permettre à l’outil CMS de cibler l’affichage des messages en fonction de critères de segmentation (âge, sexe, activité dans Mon espace santé, données personnelles connues de Mon espace santé ou de l’Assurance Maladie, etc.) |
| Interface user friendly | Permettre à l’outil CMS une utilisation facilitée via une interface userfriendly (pas de connaissance HTML ou informatique spécifique pour ajouter des contenus) |
| Gestion d’images et illustrations | Permettre à l’outil CMS la gestion d’images et illustrations |
| Multi-acteurs | Permettre dans l’outil CMS que de multiples acteurs puissent gérer des contenus (prévoir une hiérarchie des droits : validateur, éditeur, modérateur, etc.) |
| Adaptation au service web destinataire | Permettre à l’outil CMS de différencier les contenus en fonction du device (web, mobile) |

##### Gestion des documents

| **Fonctionnalités** | **Description générale** |
| --- | --- |
| Alimentation MES enfant | Alimenter automatiquement le MES de l’enfant par les professionnels de santé. |
| Récupération données au plus tôt | Récupérer les données au plus près de la naissance de l’enfant (récupération des informations depuis le DPI de la mère). |
| Formats structurés | Exploiter les documents en format structuré (CDAR2 N3) pour alimenter les catégories de MES (dont profil médical, habitudes de vie, etc.) |
| Passage de données en bases | Conserver les données sous le format document mais d’en charger d’autres dans des bases de données pour alimentation de MES |
| Recherche dans les documents | Utiliser un moteur de recherches par le biais duquel des documents sont retrouvables (via mot clé ou par saisie dans le moteur) avec des résultats pertinents.  La fonctionnalité peut être limitée aux documents dans un premier mais doit aussi pouvoir être généralisée à l’ensemble des services usages et professionnels de santé. |
| Suppression de documents | Permettre aux usagers de supprimer des documents déposés par des PS ou des tiers dans leur MES. |
| Modification de documents | Permettre à un usager ou un PS de modifier le titre d’un document déposé par un PS dans le MES du titulaire. |
| Actions unitaires sur les documents par l’opérateur Cnam | Permettre, selon un cadre juridique qui reste à définir, à l’opérateur Cnam de disposer de rôles spécifiques lui permettant d’agir sur des documents unitaires, sous réserve de l’autorisation de l’usager ou d’un professionnel de santé. Ces rôles peuvent différencier des profils administratifs de profils médicaux, et sont destinés à remplacer le rôle du Médecin Hébergeur, tout en supportant l’échelle du déploiement de Mon espace santé DMP. |
| Actions de masse sur les documents par l’opérateur Cnam | Permettre, selon un cadre juridique qui reste à définir, à l’opérateur Cnam, éventuellement après consultation de sociétés savantes, de procéder à des actions d’administration de documents ou données afin de gérer leur profondeur à l’échelle d’une vie. Par exemple : supprimer ou archiver en stockage froid les CR de tests Covid négatifs. |
| Gestion de la fraîcheur des données | Optimiser la gestion du volume de données contenu dans les MES et la fraîcheur de ces données [purge, archivage de données froides, etc.]. |
| Délai affichage HR | Permettre un affichage plus rapide lors de l’enrôlement de l’usager. Le délai pour obtenir les HR est actuellement de 48 heures |
| Profondeur historique HR | Augmenter l’affichage de la profondeur d’historique des remboursements (au-delà des 12 mois glissants actuellement) sur les interfaces Mon espace santé comme DMP. |

##### Profil médical et habitudes de vie

| Fonctionnalités | Description générale |
| --- | --- |
| Collecte de données | Mettre en oeuivre un service de génération de collecte de données (via questionnaires) avec intégration dans les bases MES pour renseignement profil médical, habitudes de vie ou vivier. |
| Signature du patient | Gérer la signature du patient (avec base légale ou non) pour s’assurer que son souhait est bien respecté. (exemples non exhaustifs : pour la gestion du don d’organe, de la fin de vie, à l’occasion d’un parcours de pré-admission dans un établissement de soins). |
| Evolution des catégories | Ajouter / faire évoluer / masquer des catégories existantes |
| Mise à disposition de données anonymisées | Prévoir, si la loi l’autorise, la possibilité de mettre à disposition des données **anonymisées** ou **pseudonimisées** pour un usage secondaire des données (épidémiologiques, veille sanitaire, recherche…). |

##### Parcours de prévention

| Fonctionnalités | Description générale |
| --- | --- |
| Parcours de prévention personnalisé | Si la loi l’autorise, mettre en œuvre des parcours de prévention personnalisés en tenant compte, par exemple, des antécédents familliaux, vaccins ou autres informations jugées utiles comme des moments de vie. |
| Prévention selon activité professionnelle | Mettre en place des campagnes de prévention en s’appuyant sur le type d’activités professionnnelles. |
| Prévention selon parcours sociaux | Mettre en œuvre des campagnes de prévention en s’appuyant sur les parcours sociaux des usagers. |
| Prévention selon données environnementales | Prévoir de mettre en œuvre des campagnes de prévention en s’appuyant sur les données environnementales (situations géographiques…) |

##### Agenda

| Fonctionnalités | Description générale |
| --- | --- |
| Intégration à des programmes | Prévoir de lier les agendas à des programmes et études menées (ex : Cohorte Constances, etc.). |
| Articulation avec les parcours de prévention | Intégrer l’agenda dans les parcours de prévention quels qu’ils soient |
| Représentation « ligne de vie » | Prévoir des parcours UX permettant à l’usager de parcourir la « chronologie » de tous ses évènements de santé dans une forme type « ligne de vie » |
| Accès des professionnels aux données d’agenda | Donner accès aux données d’agenda aux professionnels de santé via l’API agenda (notamment pour les professionnels de la coordination, DAC, CPTS…) |

##### Messagerie

| Fonctionnalités | Description générale |
| --- | --- |
| Messagerie instantanée | Mettre en œuvre une solution de messagerie instantanée entre usager et autres acteurs (PS, support, etc.) et gérer les conditions d’acceptation de mise en œuvre de cette messagerie par les acteurs. |
| Périmètre destinataires | Prévoir le périmètre de Professionnels avec qui un usager peut échanger peut-être alimenté par des sources externes comme par exemple : cercle de soins de l’usager, médecin traitant, liste noire, professionnels récemment identifiés dans l’historique de remboursement, etc... |
| Extension d’accès | Prévoir l’API Messagerie : des applications du Store MES pourront proposer relever la boite d’un titulaire MES avec son consentement (diversification des clients de messagerie citoyenne). |

##### Bibliothèque de contenus personnalisés

| Fonctionnalités | Description générale |
| --- | --- |
| Bibliothèque de contenus | Mettre à disposition des usagers un espace d’informations sous forme d’une bibliothèque de contenus répondant à des critères de personnalisation (par exemple sous forme d’articles, éventuellement de vidéos sous réserve de compatibilité avec la démarche éco-responsable, de quizz, etc.) à destination des usagers. |

##### Accompagnement de la communauté

Pour assurer les interactions avec la communauté, à la date de récation du présent CCTP, la solution Eval&Go est utilisée pour créer, suivre le remplissage et analyser les réponses des questionnaires. L’outil permet également d’envoyer des e-mails pour inviter et relancer les usagers à répondre aux questionnaires.

Nous souhaitons développer la taille et les modalités de sollicitations de cette communauté, c’est pourquoi nous souhaitons pouvoir :

| Fonctionnalités | Description générale |
| --- | --- |
| Gestion questionnaires | Concevoir des questionnaires du plus simple (questions ouvertes, fermées, échelles, etc.) au plus complexes (intégration de vidéo, tests de maquettes, etc.) |
| Segmentation participants | Réaliser une segmentation des participants en fonction des réponses apportées. |
| Réalisation de tests utilisateurs | Réaliser des tests utilisateurs (tests de maquettes, focus groups en distanciel, etc.) |
| Première analyse | Permettre à la solution de fournir nativement une première analyse des résultats de l’enquête. |
| Croisement entre questionnaires | Croiser les réponses d’un participant à différents questionnaires. |
| Invitation par courriel | Inviter les usagers à répondre aux questionnaires par courrier mis en page aux couleurs de Mon Espace Santé. |

##### Communication sortante aux détenteurs de Mon Espace Santé

A ce jour les bénéficiaires d’un profil Mon espace santé (activé ou non) sont informés des actions réalisées par des tiers dans leur espace par e-mails (réception d’un nouveau document, d’un nouveau message, …). Les canaux e-mail et SMS sont également utilisés pour les notification de type « gestion du compte » (réception de code provisoires, d’accès, de connexion, partage du profil d’un enfant avec un second responsable légal, interactions avec le support, etc.).

Ces communications sont déclenchées / envoyées de manière automatique. L’ajout et la modification du contenu de ces notifications sont réalisés à l’occasion de MEP de nouvelles versions de Mon espace santé.

Au-delà des notifications envoyées dans le cadre de l’utilisation du service Mon espace santé, des messages ad hoc pourraient être envoyés aux usagers sur la base des coordonnées connues dans Mon espace santé. Un outil de conception de campagnes e-mailing est alors nécessaire afin de pouvoir envoyer une nouvelle typologie de communication promotionnelle/informationnelle visant à la promotion du service Mon espace santé, la promotion des thématiques de l’Assurance Maladie, l’envoi d’une newsletter, la diffusion de messages des pouvoirs publics, etc.

| **Fonctionnalités** | **Description générale** |
| --- | --- |
| Campagnes ciblées | Permettre l’envoi de campagnes ciblées en fonction de critères issus des bases de MES |
| Suivi des campagnes | Disposer du suivi statistique de chaque campagne (ouverture, clic, hard bounce, soft bounce, etc.) |

##### Support

|  |  |
| --- | --- |
| **Fonctionnalités** | **Description générale** |
| Alimentation GRC Cnam | Prévoir d’offir la possibilité d’alimenter la GRC Cnam (usager disposant ou non d’un MESDMP actif) pour faciliter la réponse aux sollicitations de support. |

##### SI Pilotage

| **Fonctionnalités** | **Description générale** |
| --- | --- |
| Pilotage transverse Mon espace santé et DMP | Disposer d’une vue consolidée de flux et items des systèmes Mon espace santé et DMP pour en assurer un meilleur pilotage. |
| Renforcement sécurité | Mettre en œuvre une solution de traçabilité des connexions utilisateurs et renforcement sécurité, ainsi que mise en place d’un suivi statistique des usages du SI Pilotage. |
| Indicateurs Usage RNIAM | Mettre en œuvre les indicateurs d’Usage RNIAM :   * + Régime   + Caisse   + Centre   + Statut   + Nb ENS   Exemple :   * + Tableau de répartition des ENS par Régime / Caisse / Centre / Statut avec filtrage dynamique pour chaque donnée   Ces listes ne sont pas exhaustives |
| Indicateurs Usage Notifications | Mettre en œuvre les indicateurs Usage Notifications :   * + Template Notification   + Type de notif (règlementaire, Document, ENS, Store, etc.)   + Date   + Canal (Courrier, Mail, sans)   Exemple :   * + Tableau de répartition des notifications par type/date + filtre période   + Nombre d’Usagers ayant reçus X notifications par mail   Ces listes ne sont pas exhaustives |
| Indépendance de la Cnam sur SI PIL DMP | Les utilisateurs accèdent en toute autonomie aux données et au suivi des usages des DMP, afin de répondre au mieux aux besoins de chacun. |
| Indicateurs Pilotage support à froid | Mettre en œuvre les indicateurs Pilotage support à froid :   * + Date du jour   + Motif de contact   + Régime de l’usager   + Niveau Support (1,2, etc.)   + Canal (téléphone, formulaire)   + Volume d’entrée   + Statut : traité, dissuadé, etc.   + Volume de sorties   + Solde   Exemple :   * + Appels * Soldes : nombre d’appels par niveau, Taux de décroché * Répartition des appels par Régime % * Répartition des appels par motif % * Courbe Evolution des sollicitations (Appels, Traités) * Tableau détaillé des répartitions par groupes de trafic * Tableau détaillé des appels par motif   + Formulaires * Soldes : Nb de formulaires, Nb Traité, Nb En cour, Taux de formulaire traités * Courbe Evolution des sollicitations (Reçus, Traités, Restants) * Tableau cumulé détaillé des formulaires * Tableau détaillé des formulaires par motif * Répartition des formulaires par motifs et par groupes de trafic   + Formulaires + Appels * Sollicitations par Niveau du Support * Sollicitations par Groupe de Traffic (Régime)   Ces listes ne sont pas exhaustives |

### Métriques de MESDMP

Concernant les indicateurs d’usages actuels :

* + 66M de comptes créés
  + 8,7M de comtes activés
  + 200 000 nouvelles activations par mois
  + Plus de 400 000 visiteurs hebdo

Dans le cadre de la montée en puissance de MESDMP, la montée en puissance des usages est ambitieuse. Il convient donc de prévoir un dimensionnement qui permette de répondre *a minima* aux objectifs suivants :

* + Atteindre un rythme de 250 millions de documents de santé par an alimentés dans Mon espace santé par les professionnels fin 2023 et 400 millions fin 2026.
  + Permettre à 1 million de patients de préparer un bilan de prévention dans Mon espace santé d’ici 2027
  + Référencer plus de 100 applications proposant des échanges avec Mon espace santé d’ici fin 2026

Un élément déterminant de la qualité de la prise en charge est l’accès effectif des professionnels au dossier et à l’historique médical de leurs patients. C'est tout l'enjeu de la vague 2 du Ségur numérique : les actions d’amélioration continue des fonctionnalités de Mon espace santé doivent se poursuivre pour permettre cet accès fluide et ergonomique aux professionnels et aux établissements en « vie réelle », quel que soit leur contexte d'exercice. En complément de l’accès via le portail web du DMP, les professionnels pourront accéder simplement de manière synthétique et ergonomique aux données structurées, issues de Mon espace santé (synthèses, prescriptions, lettres de liaison, biologie, profil médical, etc.) intégrées directement dans leur logiciel métier, en ville et en établissement. Cet accès est essentiel, notamment en cas d’urgence.

Il est ainsi prévu que plus de 50% des médecins en activité consultent au moins une fois le contenu du profil Mon espace santé de leurs patients dans l'année d’ici fin 2026.

Dans le cadre de la Convention d’Objectifs et de Gestion (COG), les objectifs suivants sont visés par la Cnam :

* + Nombre d’activations (part des MES activés) :
* 2023 : 20%
* 2024 : 30%
* 2025 : 40%
* 2026 : 50%
* 2027 : 60%
* Totalité sur 7 ans.
  + Nombre de DMP alimentés par au moins un document :
* 2023 : 35%
* 2024 : 45%
* 2025 : 55%
* 2026 : 65%
* 2027 : 75%

Les éléments de volumétrie du système d’information sont décrits en §7.4 « P2 - PSE – Hébergement ».

## Architecture envisagée à 3 ans (MES + DMP = MESDMP)

Afin d’illustrer les transformations architecturales couvertes par l’accord-cadre, une vision de l’architecture d’une cible à 3 ans présentée ci-après. Le candidat propose une trajectoire architecturale. Il s’agit d’un des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

Ces transformations doivent permettre, d’une part, de faire converger les 2 systèmes actuels (DMP et MES) pour former le nouveau SI MESDMP et, d’autre part, de mettre en œuvre les mécanismes et dispositifs nécessaires à l’atteinte des objectifs de facilitation de circulation de l’information entre les Professionnels et les Usagers, notamment au travers du concept de *Ressources Partagées*.

Une Ressource Partagée est systématiquement envisagée dès lors qu’une donnée doit être partagée entre un Professionnel et un Usager. Elle prend naturellement la forme d’une « Ressource » au sens ROA du terme et des propriétés associées (autonomie, agnostique du contexte métier, RESTful, etc.).

L’un des critères principaux définissant une Ressource Partagée est son obligation de mettre en œuvre un Contrôle d’Accès tenant compte des tous les éléments de sécurité propres aux 2 populations qui la consomment (Professionnels et Usagers) et non pas uniquement conditionné par des contraintes liées au Systèmes d’Informations qui l’héberge (SI CNAM, SI MESDMP ou autres).

Le dispositif de Contrôle d’Accès aux Ressources Partagées doit donc tenir compte aussi bien des Consentements et Délégations accordées par les usagers que des Habilitations et Délégations (ex. : PS remplaçant) des Professionnels pour régir les demandes d’accès aux Ressources Partagées.

La convergence doit s’opérer sur de nombreux axes et plus particulièrement, du point de vue architectural adressé par ce paragraphe, des axes suivants :

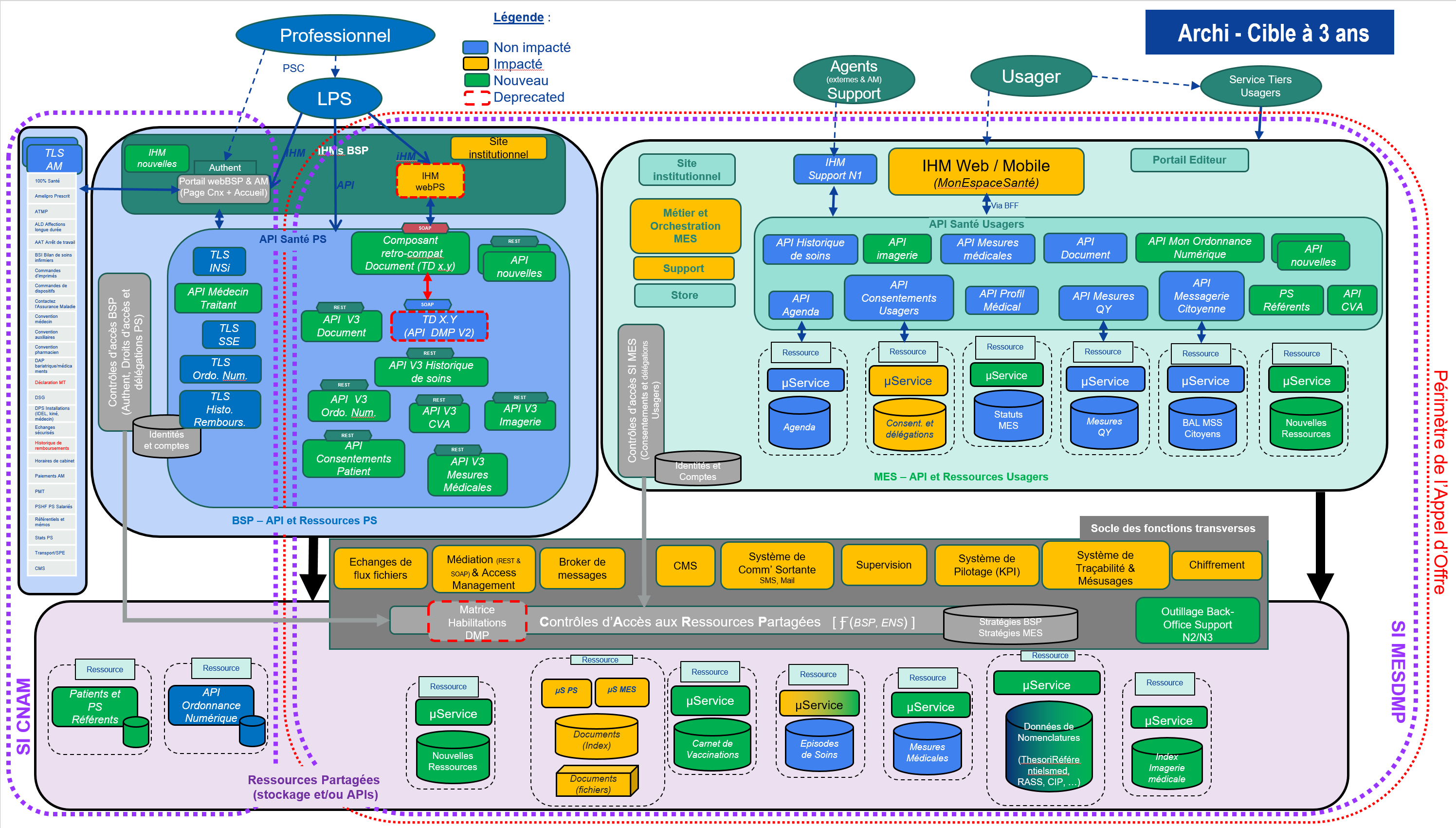
* + Axe fonctionnel : en favorisant, dès que cela est possible, la mutualisation des fonctions communes aux 2 systèmes.

L’essentiel des actions en lien avec cet axe se retrouvent dans le Paragraphe *E. Socle des fonctionsTransverses* : ci-après.

* + Axe applicatif :
* Conséquence directe de la convergence des fonctions communes, il s’ensuit une rationalisation des applicatifs portant ces fonctions, et donc une diminution du patrimoine applicatif permettant la simplification du dispositif global.
* Convergence des styles d’architecture, avec en première intention, une rénovation du style majoritairement « Monolithique » du SI DMP vers un le style de MES, orienté « ressources & µservices ».
* Mise en œuvre opérationnelle des Ressources Partagées
  + Axe technologique : favorisée par la convergence applicative, la rationalisation / homogénéisation de la stack technique de développement est également un des objectifs poursuivis.

Cette convergence inclut également la convergence d'hébergement/d'infrastructures pour laquelle le candidat doit proposer une stratégie de mise en place. Il s’agit d’un des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

**Proposition d’architecture à 3 ans pour le système MESDMP :**

**NB** : Pour des questions de clarté, le SI CNAM est fortement simplifié et ne comporte que les éléments pertinents pour ce CCTP fig. Archi-05

**Description des évolutions à opérer à 3 ans :**

1. IHMs BSP :
   1. Reprise/adaptation du site dmp.fr
   2. IHM WebDMP PS : reprise partielle de la partie non intégrée par la CNAM au démarrage du marché
   3. Contrôles d’accès BSP :
      1. Authentification déléguée à Pro Santé Connect (ANS) et/ou AmeliPRO/WebBSP (OpenID Connect)
      2. Mode dégradé de l'authentification en cartes CPS (mTLS X.509)
      3. Annuaire PS régalien copie du RASS/RPPS+ (Annuaire Santé) => voir Ressources Partagées
      4. Contrôles d'accès aux services : matrice d'habilitations « statique » + délégation inter PS « dynamique ».
2. API Santé PS :
   1. Toutes les API doivent être exposées vie des dispositifs de médiation ( voir Socle des fonctions transverses : API Management/REST et médiation SOAP)
   2. Les API REST, dès que cela est possible, doivent respecter le standard FHIR et le CI-SIS (lorsqu’il y a lieu)
   3. Les API peuvent proposer des ressources de type aggrégé, c’est-à-dire qu’elles modélise une aggrégation de différentes ressources partagées (ex. : SSE)
   4. Mise en place de la façade SOAP de rétro-compatibilité API V2 permettant de décommisionner les API V2 *(soap)* du DMP (TD x.y) historiques
   5. Création des API V3 *(rest)* pour les ressources suivantes :
      1. Document
      2. Carnet de Vaccination
      3. Histoire de Soins
      4. Ordonnance Numérique
      5. Consentement Patient
      6. Mesures médicales
      7. … et pour toute nouvelle ressource jugée nécessaire
3. Ressources Partagées :

*NB : implique la mise en œuvre du Contrôle d’Accès aux Ressources Partagées (CARP) pour chacune d’entre elles*

* 1. Création de la ressource partagée Documents :
  2. Consolidation des API PS et MES exisantes du DMP pour les adapter au CARP
  3. Création de la ressource partagée Carnet de Vaccination :
  4. Transformation de la solution actuelle du DMP qui considère le Carnet de Vaccination comme un « document » pour en faire une ressource « structurée » comportant une liste de lignes de vaccination.
  5. Création de la ressource partagée Episodes de Soins :
  6. Création du µS sur le gisement NoSQL existant actuellement dans le DMP (et « déplacement » de ce gisement dans la zones des Ressources Partagées = cf. NB ci-dessus)
  7. Création de la ressource partagée Mesure Médicales :
  8. Adaptation / Reprise partielle du gisement actuel des Mesures de MES pour en faire une ressource partagées
  9. Création de la ressources partagée Index Images Médicales
  10. Reprise dans le SI MESPBS & passage en ressource partagée de la ressources Ordonnance Numérique de la CNAM.
  11. Création de la ressource partagée Données Référentielles :
  12. Adaptation/Enrichissement du gisement actuellement opéré par MES (contenant au 05/2023 des copies de l’Annuaire Santé de l’ANS et d’une partie du ThesoriMed concernant les vaccins. Potentiellement à venir : codes CIP pour les boites de vaccins, etc.)
  13. Passage en SGBD Open source sur index Documents
  14. … et toute nouvelle ressource jugée nécessaire

1. MES – API et Ressources Usagers :
   1. Mise en place de l’accueil du push des stratégies d’accès en provenance de MES
   2. Création API Santé Usagers pour les ressources suivantes :
      1. Carnet de Vaccination
      2. Ordonnance Numérique
      3. Index d’Imagerie Médicale
      4. … et pour toute nouvelle ressource jugée nécessire
   3. Passage en ressources partagée des Mesures Médicales : dissociation des Mesures « Quantify Yourself »
   4. Exposition du statut d’existence de MES
   5. Adaptation et Exposition de la ressource « consentement » pour le BSP afin de prendre en compte les nouveaux usages (ex : cas du Médecin du travail, Aidant/Aidé, etc.)
   6. Evolution du Métier et Orchestration MES : autonomie de MES pour le processus d’enrôlement
      1. Ajout de la fonction d’éligibilité d’un usager à ouvrir un MES
      2. Ajout de la fonction de génération et de contrôle de validité du code unique d’enrôlement
      3. Ajout de la fonction de notification d’information initiale
   7. Evolution Support :
      1. Adaptation du dispositif actuel de MES au système mis en place pour le support N2 et N3 apporté par le titulaire du Marché.
      2. Extension du domaine de support au périmètre des utilisateurs (PS) ( ex-DMP + nouvelles API Santé PS)
   8. IHM Web et Mobile : prise en compte des évolutions pour les nouveaux usages
2. Socle des fonctionsTransverses :

*NB : Cette zone de MESDMP découle de la convergence entre le SI DMP et le SI MES et de la rationalisation des dispositifs permettant l’implémentation des fonctionnalités qu’elle contient : la « nature » de l’impact est donc systématiquement à traduire comme une fusion ou un remplacement.*

* 1. Création du dispositif de Contrôle d’Accès aux Ressources Partagées (CARP) :
     1. Mise en place de l’accueil du push des stratégies d’accès en provenance de MES
     2. Intégration de la Matrice d’Habilitation du DMP dans le CARP
     3. Mise en place de l’accueil du push des stratégies d’accès en provenance du BSP

*NB : ce dispositif permet d’avoir un contrôle d’accès aux ressources partagées consolidant les stratégies issues de MES (délégation entre usagers et consentements) et du BSP (délégation entre Professionnels et Habilitations)*

* 1. Echanges de flux fichiers  
     MESDMP nécessite de pouvoir échanger des fichiers en mode –a minima- SFTP ou CFT
  2. Médiation (REST & SOAP) & Access Management

MESDMP nécessite toutes les fonctions de médiation que requiert sa nature de plateforme d’exposition de services (SOAP ou REST) ou son style d’architecture principalement à base de µServices.

Il va également de soi que ces médiations contribuent fortement à la complétude du socle de Sécurité (via l’access management nativement inclus) ou à celle de la Traçabilité et de la Supervision.

* 1. Broker de messages

MESDMP, avec son architecture orientée µServices, nécessite un broker de message fiable, performant et pérenne.

* 1. CMS

Une partie de MESDMP requiert de gérer et de publier du contenu rédactionnel. La centralisation de ce contenu dans un CMS est est un facteur clé de qualité, de réactivité et de cohérence du système.

* 1. Système de Comm’ Sortante (SMS et mails)

MESDMP doit pouvoir communiquer avec les usagers et les PS selon différentes modalités : principalement via SMS et mails.  
*NB* : pour les communication via courriers papier, c’est la solution Editique DSS actuelle qui sera pérennisée *(*cf *§3.2.1.1 Interfaces externes*, flux 9)

* 1. Supervision

MESDMP nécessite les dispositifs permettant la supervision (et l’alerting) de l’ensemble du Système.

* 1. Système de pilotage (KPI)

MESDMP doit pouvoir produire les indicateurs clé nécessaire à son pilotage métier. Ce dispositif est de type « BI ».

* 1. Système de Traçabilité & Mésusages

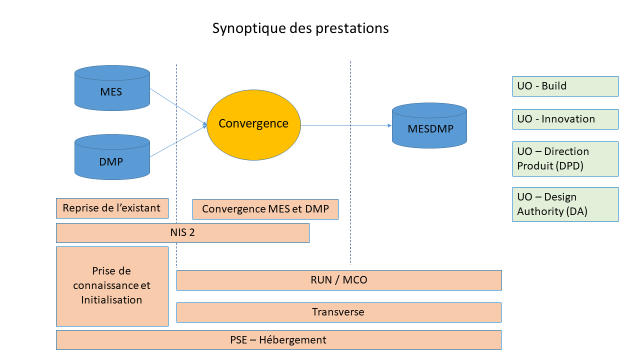
L’ensemble de l’activité dans MESDMP doit produire les différents niveaux des différents types de traces exigibles pour l’ensemble des finalités imposées par les besoins métier, le RGPD, les exigences de sécurité, les réquisitions judiciaires, de détection des mésusages...

* 1. Chiffrement

MESDMP manipulant des données personnelles et médicales pour l’ensemble de la population, la fonctionalité de chiffrement est particulière critique et « centrale ».

* 1. Outillage Back-Office Support Niveau 2 et 3

# Présentation générale de l’accord-cadre



*Remarque : le synoptique est présent à titre illustratif, la convergence peut démarrer en même temps que la reprise de l’existant par exemple. La Cnam laisse latitude aux candidats de faire d’autres propositions.*

## Objet et forme de l’accord-cadre

Le présent accord-cadre adresse les prestations suivantes, définies au §7.

* + P1.1 - Pdc\_Init : Prise de connaissance et Initialisation (§7.2),
  + P1.2 - Rep : Reprise de l’existant (§7.3),
  + P3 - Conv : Convergence des systèmes MES et DMP (§7.4.3),
  + P4 - Trans : Transverse (§7.6),
  + P5 - Run\_MCO-S : Run, MCO et MCS (§7.7),
  + P6 – Homologation NIS/NIS2 (§7.8),
  + P7 - SMS\_Mail : Run SMS et Mail (§7.9)
  + To1 – Réversibilité (tranche optionnelle) (§7.10), en cas d’affermissement de la tranche.

En outre, dans l’hypothèse où la Cnam décide de retenir la PSE, définie au §7.4, l’accord-cadre adresse également l’hébergement de la solution du dispositif MESDMP chez le Titulaire.

L’accord-cadre est composé d’une tranche ferme de d’une tranche optionnelle telles que :

* + La tranche ferme adresse :
* Les prestations forfaitaires suivantes :
* P1.1 - Pdc\_Init : Prise de connaissance et Initialisation (§7.2),
* P1.2 - Rep : Reprise de l’existant (§7.3),
* P3 - Conv : Convergence des systèmes MES et DMP (§7.4.3),
* P4 - Trans : Transverse (§7.6),
* P5 - Run\_MCO-S : Run, MCO et MCS (§7.7),
* P6 – Homologation NIS/NIS2 (§7.8),
* P7 - SMS\_Mail : Run SMS et Mail (§7.9)
* Les prestations à bons de commande définies au §7.11.
* Dans l’hypothèse où la Cnam décide de retenir la PSE, l’accord-cadre adresse également les prestations forfaitaires d’hébergement de la solution du dispositif MESDMP, chez le Titulaire, §7.4.
  + Les tranches optionnelles adressent :
* To1 : Les prestations forfaitaires définies au §7.10 « To1 – Réversibilité (tranche optionnelle) »
* To2 : Les prestations forfaitaires en cas d’hébergement en interne définies au §7.3 « P1.2 - Rep : Reprise de l’existant ».

Les prestations doivent être réalisées conformément aux modalités d’organisation et aux exigences définies dans le présent CCTP.

## Lieux d’exécution des prestations

Le Titulaire assure sa propre logistique. Il réalise les prestations dans ses locaux sur les environnements techniques mis en place par ses équipes. Les ressources nécessaires à la réalisation des prestations hébergées par la Cnam sont accessibles via une connexion sécurisée à la charge du Titulaire.

Certaines prestations peuvent nécessiter une intervention avec une présence sur un des sites.

D’une manière générale, les prestations peuvent se dérouler :

* + Dans les locaux du Titulaire,
  + Dans les locaux de la Cnam (Siège à Paris et site provinciaux).

Il est précisé que :

* + Les réunions, ateliers, prestations d'accompagnement s'effectuent à partir de plateaux communs (physique et virtuel), à la Cnam ou dans les locaux du Titulaire, permettant aux équipes mixtes (Cnam et Titulaire) une meilleure intégration et une collaboration plus fluide au quotidien. Dans le cadre du projet, ces plateaux permettent d’accueillir l’ensemble des équipes mixtes à l’occasion des rituels.
  + Des déplacements occasionnels sont à prévoir sur tout le territoire national.
  + Les équipes sont principalement situées à :
* Paris
* Lyon / Grenoble / Valence
* Angers/Nantes
* Valenciennes
* Clermont-Ferrand, Evreux, Lons le Saunier, Quimper,etc.

De manière générale, le modèle de delivery des prestations mis en place par le Titulaire doit répondre aux objectifs de réactivité et d’échange, d’efficacité et de sécurité.

Les personnels Cnam doivent pouvoir avoir accès aux environnements de travail ad hoc chez le Titulaire en étant à distance : environnements de développement web et mobile notamment. De même pour les éventuels prestataires de la Cnam pouvant être amenés à travailler dans le cadre des prestations objet du présent accord-cadre (accès via VPN Cnam ou via leur propre VPN).

## Livraison / Validation et admission des prestations

### Modalités de livraison

Toute livraison doit être accompagnée d’un Bordereau récapitulatif de Livraison (BRL) qui indique, a minima, la liste des livrables et la date de livraison effective. Le BRL est émis et signé par le Titulaire et contresigné par la Cnam.

### Validation et admission des prestations

La Cnam est seule habilitée à se prononcer sur la vérification et l’admission des prestations.

Les modalités de vérification et d’admission des prestations sont définies dans le présent CCTP et, le cas échéant, précisées dans le PAQ.

Les vérifications comprennent :

* + Des vérifications quantitatives, qui ont pour pour objet de contrôler la conformité entre la quantité livrée ou le travail fait et la quantité ou le travail défini dans les prestations forfaitaires ou prévu dans les unités d’œuvre commandées par la Cnam ;
  + Des vérifications qualitatives, qui ont pour objet de permettre à la Cnam de contrôler notamment que le Titulaire :
* A mis en oeuvre les moyens définis dans l’accord-cadre, conformément aux prescriptions qui y sont fixées ;
* A réalisé les prestations définies dans l’accord-cadre comme étant à sa charge, conformément aux dispositions contractuelles.

Les opérations de vérifications qualitatives ont également pour objet de contrôler les conformités à la politique de sécurité. Elles comprennent, le cas échéant, deux étapes : la vérification d’aptitude (VA) et la vérification de service régulier (VSR).

Pour toute livraison, la Cnam dispose du délai, propre à chaque type de livrable (logiciel, documentaire, etc.), défini dans le PAQ propre à chaque type de livraison, à compter de la date de réception du BLR, pour vérifier la recevabilité de la livraison. Si une relivraison imputable au Titulaire est nécessaire, le délai précité est reconduit à compter de la date de relivraison. En cas de retard, le retard imputable au Titulaire est égal au nombre de jours calendaires cumulés pour chaque relivraison.

À l’issue des opérations de vérification des prestations, la Cnam prend une décision d’admission des prestations, d’admission avec réfaction, d’ajournement, ou de rejet conformément aux stipulations du CCAP. La Cnam communique se décision au Titulaire pour information.

La décision d’admission est matérialisée par la production d’un PV par la Cnam. Ce PV est signé par la Cnam et communiqué pour information au Titulaire.

# Cadre organisationnel

## Principes et responsabilités respectives des acteurs

*Remarque : Outre les principes contractuellement définis qui régissent la relation entre la Cnam et le Titulaire, et la répartition détaillée des rôles et responsabilités des parties précisée dans le Plan d'Assurance Qualité proposé par le Titulaire et validé par la Cnam, la Cnam attire plus particulièrement l'attention des candidats sur les points importants décrits ci-dessous.*

La Cnam entend participer activement à la réalisation, au maintien et au pilotage du dispositif MESDMP, dans une logique d’organisation unique et intégrée, sous forme d’équipes mixtes intégrant à la fois les ressources du Titulaire et des ressources Cnam, quel que soit le champ d’activité concerné.

En ce sens, la Cnam dispose d’une réelle maitrise de l’ensemble du périmètre technique, applicatif, fonctionnel, exploitation et support relatif à l’architecture et à la sécurité et pénétre l’ensemble de ces chantiers au sein de l’organisation définie.

La Cnam fournit les informations nécessaires en matière d'exigences liées à la sécurité, la confidentialité et l'accès aux données objet de référencement, d'enregistrement, de traitements et de sauvegarde au sein de Mon espace santé et du Dossier Médical Partagé.

En terme de confidentialité, le Titulaire s’engage à mettre en œuvre des engagements de confidentialité pour tous les acteurs qui sont amenés à travailler sur des données de production, dans le cadre de leur fonction précisément déterminée dans le processus. Le Titulaire doit expliquer les modalités de traçabilité et de contrôle des actions de ces acteurs afin de s’assurer que les engagements sont respectés.

La Cnam entend disposer de la meilleure information possible tout au long de l'exécution de l’accord-cadre afin d'être en mesure d'exercer au mieux son rôle parmi lequel le droit de diligenter, autant que de besoin, les audits nécessaires pour vérifier la mise en application effective par le Titulaire des règles et des obligations en conformité avec les réglementations françaises.

Pour ce faire, parmi les rôles que le Titulaire doit développer dans son PAQ, il apporte une attention particulière sur les aspects suivants :

* + Le Titulaire a pour responsabilités principales de réaliser, héberger le cas échéant, exploiter et maintenir le dispositif Mon espace santé / DMP interfacé, entre autre, avec le système d'information de la Cnam, dans des conditions de sécurité et de performance définies. Par ailleurs, le Titulaire a une obligation de conseil qui l'engage à fournir à la Cnam un ensemble de services d'accompagnement permettant de réussir la mise en œuvre des choix techniques et organisationnels dans un contexte de volumétries importantes, de gestion de données sécurisées, le tout à un haut niveau de qualité de service.
  + Le Titulaire s'engage à fournir une solution opérationnelle assortie d'engagements sur les performances et les services conformes au CCTP.
  + Le Titulaire assure la qualification technique, fonctionnelle et benchs du dispositif MESDMP, y compris pour les besoins du BSP, dans l’interconnexion avec les services du SI de la Cnam et des SI des autres organismes/fournisseurs. La coordination de ces activités est assurée par le Titulaire, accompagnée, le cas échéant, par les équipes de la Cnam.
  + Le Titulaire assure la coordination des travaux d'intégration de bout-en-bout de la solution et la recette globale permettant de prononcer la réception et la mise en service du dispositif MESDMP exploité par le Titulaire. Dans ce cadre, le Titulaire donne entière visibilité à la Cnam sur la réalisation des tests : stratégie, couverture, couverture de tests automatisées, limites, campagnes, preuves et compte-rendus d’exécution, etc.
  + Le Titulaire assure la production et le maintien en condition opérationnelle et de sécurité du dispositif MESDMP conformément aux exigences de qualité, de sécurité et de performances contractuellement définies. Il donne visibilité entière sur l’ensemble des outils et processus mis en œuvre dans le cadre de la production et le maintien en condition opérationnelle et de sécurité. Dans le cadre des workflows de traitement des anomalies, les équipes Cnam doivent être prévues en tant qu’acteur du workflow.
  + Le Titulaire s'engage à maintenir à jour un dictionnaire exhaustif des données et à fournir à la Cnam les moyens et outils lui permettant de répondre à tout moment à toutes sollicitations des organes de l'Etat quant au respect des réglementations en vigueur matière de protection des données santé. A ce titre, le Titulaire est en charge de la mise à jour des AIPD relatifs aux traitements couverts par l’accord-cadre, dont la première version lui est remise lors de l’initialisation de l’accord-cadre.
  + Le Titulaire a l'obligation de maintenir à jour toutes les documentations des solutions mises en œuvre dans le cadre de l’accord-cadre ainsi que le plan de réversibilité permettant à la Cnam d'exercer la réversibilité dans les termes définis dans le présent CCTP.
  + Le Titulaire a l'obligation d’assurer le support nécessaire aux acteurs externes utilisateurs des environnements hors production, pour les besoins des processus de DMP compatibilité, de référencement des services tiers au catalogue de services Mon espace santé et dans le cadre de tests avec d’autres opérateurs de Messagerie Sécurisée de santé. Ce support inclut les processus d’ouverture des flux, d’habilitation d’accès aux éditeurs concernés, de fourniture des moyens nécessaires aux opérations (en particulier des comptes fictifs), de remise à niveau régulier des environnements, de support opérationnel en cas de difficulté rencontrée par un des éditeurs concernés, etc. Le Titulaire a également en charge la communication des indisponibilités de l’environnement considéré auprès des acteurs adhoc. Cette activité peut être étendue à des évènements spécifiques type projectathon.

## Organisation des équipes

Le Titulaire met en œuvre une organisation cohérente et collaborative.

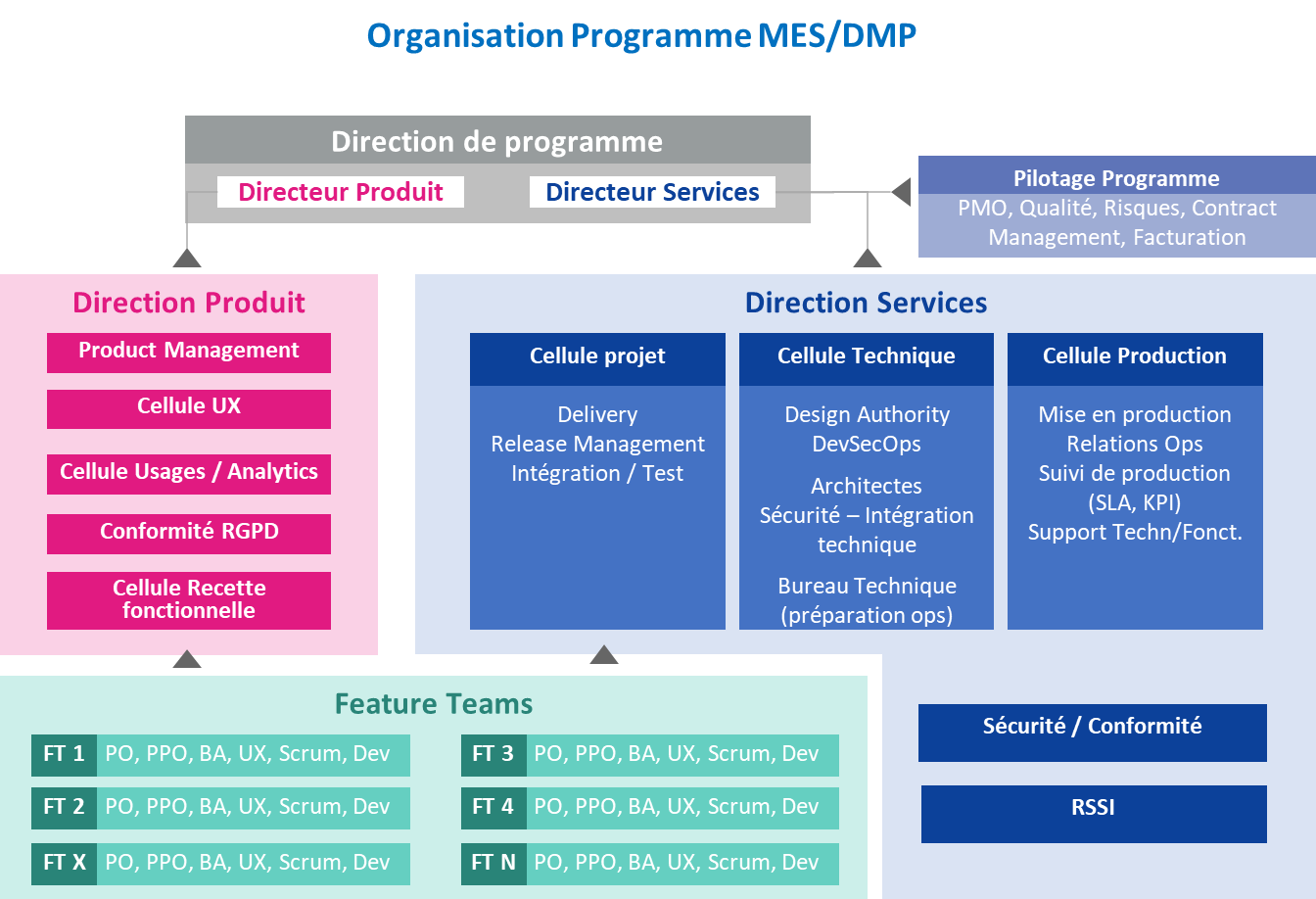
L’organisation cible à mettre en place doit couvrir les fonctions nécessaires à la conception, à la réalisation, au maintien et à l’exploitation du dispositif MESDMP : les dimensions « Métier » et « Services ».

Les entités formées pour répondre aux différentes dimensions du programme sont composées de membres de la Cnam et du Titulaire qui travaillent en équipes mixtes pour concevoir, réaliser, maintenir et exploiter le dispositif MESDMP.

L’organisation s’articule autour :

* + D’une Direction Programme co-animée par le Titulaire et la Cnam ;
  + D’une Direction Produit mixte Titulaire et Cnam ;
  + D’une Direction Services mixte Titulaire et Cnam :
* Une cellule technique en appui de la conception solution, applicative, technique et d’exploitation ;
* Une cellule projet en appui du delivery ;
* Une cellule de suivi de production et du support
  + De feature teams mixtes Titulaire et Cnam.

L’organisation intégrée du dispositif cible Cnam / Titulaire est détaillée dans le schéma ci-après (cette organisation peut évoluer en fonction des besoins du projet) :



Dans le cadre de la participation au programme, la Cnam assure la responsabilité de la maîtrise d’ouvrage et de la maîtrise d’œuvre dudit programme.

Dans le cas des équipes mixtes, le Titulaire conserve la responsabilité pleine et entière du service et du delivery.

Dans le cadre de ces équipes mixtes et du travail collaboratif en découlant, la Cnam met à disposition une force de réalisation (ressources Cnam opérationnelles) intégrant différents types de profils :

* + Product Manager, en appui à la Cnam sur le champ de la responsabilité des produits (Mon Espace Santé / DMP et sous-produits)
  + Product Owners pour la réalisation de features s’inscrivant dans la réalisation des produits (Mon espace santé / DMP et sous-produits)
  + Développeurs agile web formés à la méthode agile
  + Profils d’architecture, sécurité, opérations, suivi projet / release / delivery (type proxy-PO de profil maîtrise d’œuvre), PMO, Qualité, Contract manager et PMO projet.

Ces ressources opérationnelles Cnam collaborent au dispositif mis en place par le Titulaire avec lequel elles travaillent en parfaite coordination. Le Titulaire doit néanmoins toujours prévoir d’assurer seul ce type de rôle sur l’ensemble des sujets le cas échéant. La Cnam et le Titulaire s’attachent néanmoins à préserver tant que faire se peut, en fonction des contraintes de services, le maximum de continuité dans la constitution des équipes.

Au sein de la Direction Services, une cellule Technique mixte comprend une entité responsable de la cohérence technique, sécurité et applicative du dispositif MESDMP. Cette cellule embarque également une Design Authority, responsable de la cohérence entre les dimensions Produit, Delivery et Architecture.

## Méthodologie de développement

Le produit MESDMP doit être développé selon la méthodologie agile. Toutefois, par exception, elle se réserve la possibilité de mettre en œuvre un mode projet en cycle en V.

### Méthodologie Agile

#### Grands principes agiles

Conformément aux principes de la méthode, la Cnam met en oeuvre une approche basée sur une gestion des priorités en fonction de l’estimation de la valeur et des coûts. L’objectif recherché est de garantir la mise en place d’un service doté d’une forte valeur ajoutée dans les meilleurs délais et au meilleur coût.

Le Titulaire doit rechercher l’efficacité pour maximiser la valeur avec des livraisons fréquentes.

Conformément aux principes de la méthode, la Cnam s’appuie sur la notion de timebox (bloc de temps limité). Si une ou plusieurs fonctionnalités prévues ne sont pas terminées, elles sont reportées dans le sprint suivant, sans surcoût, afin de ne pas retarder la livraison. L’objectif est d’avoir un avancement avec une régularité rassurante et d’éviter le syndrome du « fini à 90% ».

La date est immuable avec l’objectif d’apporter un maximum de valeur pour cette date. Les fonctionnalités « must have » sont positionnées en début de sprint et les fonctionnalités mineures, « should have » sont positionnées en fin de sprint.

Les réalisations ne se font pas domaine par domaine sur toute la profondeur, mais selon la valeur et la séquence d’usage. La priorité est donnée à la plus forte valeur pour un faible coût avec la possibilité de s’arrêter à un niveau de valeur jugé satisfaisant afin de dégager des marges de manœuvre pour intégrer des besoins non prévus initialement, s’avérant nécessaires ou avec une plus grande valeur ajoutée.

L’acceptation au changement est donc souhaitée par la Cnam. Les coûts et les délais étant fixes le périmètre et la manière de l’adresser sont les variables d’ajustement. Dans ce cadre le Titulaire doit mettre en place un dispositif permettant de sécuriser les engagements opérationnels et la flexibilité avec l’application du mécanisme de «trade-in/trade-out ».

Si la méthode Agile doit privilégier la collaboration et la discussion, la conservation des traces des échanges et des décisions via des comptes rendus réguliers reste indispensable et impérative.

L’enjeu de MESDMP est de répondre efficacement aux attentes et aux besoins des usagers. Les fonctionnalités proposées au sein de MESDMP doivent être conçues, développées et mises à disposition des utilisateurs dans des délais courts et avec une logique d’amélioration continue. Pour répondre à ces exigences de time-to-market, MESDMP doit être réalisé et piloté en respectant les principes de la méthode agile. L’équipe MESDMP s’appuie sur des outils assurant la maîtrise et la réactivité des livraisons. La plateforme DevSecOps permet de mettre en production quotidiennement, et cela, de manière transparente et sécurisée pour les usagers de MESDMP. Actuellement le rythme des mises en production est le suivant : une release trimestrielle correspondant à un PI, une version majeure mensuelle, une version mineure hebdomadaire.

Pour ce faire, la Cnam se positionne en tant que Product Owner (PO) des produits constituant le MESDMP. Elle peut déléguer au Titulaire certains sujets, avec des Product Owners (PO) dédiés issus des équipes du Titulaire. La Cnam doit bénéficier des principes de l’agilité de la conception jusqu’à l’exploitation idéalement sur la totalité des chantiers de MESDMP.

Dans le cadre de la mise en application de la méthodologie Agile, le Titulaire s’engage à respecter les principes de l’agilité à l’échelle (atuellement la Cnam est organisée en SAFe like) et faire preuve de transparence et de franchise dans ses relations avec la Cnam. Le Titulaire agit en bonne intelligence et de bonne foi et s’inscrit dans une logique collaborative, consensuelle, itérative et incrémentale. Il doit construire son organisation à partir de l’organisation définie avec la Cnam dans la prestation P1.1 - Pdc\_Init : Prise de connaissance et Initialisation.

Le Titulaire s’engage à analyser au cours d’un point mensuel *a minima* l’utilisation de la démarche Agile au sein de ses équipes pour mettre en oeuvre des axes d’amélioration (approche Lean) et rendre cette démarche plus efficiente encore en cours d’exécution de l’accord-cadre. Il produit des indicateurs à définir dans le PAQ démontrant cette efficience.

L’organisation des travaux s’appuie sur des séquences (Product Increment) de 2 à 3 mois découpés en sprint de 2 à 4 semaines. Les features développées sont livrées et revues à chaque sprint et mises en production en suivant le principe de *continuous delivery*.

Le cadrage des EPIC, des features et des users story est réalisé par la Cnam avec l’appui du Titulaire via des UO de cadrage.

La priorisation des users story (US), leur intégration dans le backlog et leur inscription dans les sprints du PI sont réalisées par chaque feature team sur la base d’échanges sincères entre les membres de la feature team et notamment entre le product owner (PO) et les développeurs. La direction du produit coordonne la cohérence des releases.

Le cadrage et la revue portent aussi bien sur les fonctionnalités que sur les exigences techniques et la qualité, le respect des contraintes réglementaires (dont RGPD), l’exploitabilité et la sécurité du code.

Ces séquences de priorisation doivent être réalisées en amont des sprints et de son engagement et doivent être confirmées au lancement du sprint.

L’engagement d’une feature team à réaliser les user story inscrites au PI doit porter sur au moins 80 % de sa capacité.

Chaque Feature Team ne doit pas consacrer plus de 20 % de sa capacité aux correctifs, rework, MCO, qui restent cependant dûs par le Titulaire sans surcoût pour la Cnam.

Les US d’un sprint engagé, non finalisées, sont reportées au sprint suivant sans surcoût.

Par ailleurs, par Feature Team, si les users story qui ont fait l’objet d’un engagement ne sont pas réalisées à au moins 80%, la partie non réalisée doit être réalisée sur le PI suivant en sus de l’engagement nominal. Le Titulaire prend les mesures nécessaires pour renforcer l’équipe à ses frais pour prendre en charge ces US non réalisées.

L’évaluation de l’atteinte des objectifs définis sur chaque itération se concrétise par l’atteinte de valeur pour l’usager, le respect des *features* décrites et le maintien du service.

Les travaux agiles (x sprints constituant un PI avec une release) font l’objet de bon de commande des UO de cadrage agile et développement agile.

Si les résultats de l’audit de code n’atteignent pas les niveaux minimum exigés, le Titulaire s’engage à produire, à ses frais, un nouveau code respectant les niveaux de qualité exigés. Un outil d’audit de code automatisé doit être fourni et mis en œuvre par le titulaire et doit être un livrable avant Mise en production.

Le Titulaire de l’accord-cadre a un devoir de conseil et d’accompagnement des équipes de la Cnam quant à l’organisation agile DevSecOps demandée par la Cnam ainsi qu’aux technologies répondant au mieux aux critères énoncés supra.

#### Constitution des équipes et collaboration

La méthode s’appuie sur des cycles courts qui nécessitent, de la part de tous, un traitement des demandes à court terme dans un délai serré.

Les parties s’engagent à avoir, au sein de l’équipe projet, des représentants dotés d’un pouvoir de décision engageant leur entité respective pour permettre des arbitrages effectifs dans l’intérêt du projet. De même, les parties s’engagent à adapter l’organisation projet et ses méthodes de travail aux principes et processus des méthodes Agile.

Le Titulaire s’engage à mettre en place les moyens nécessaires pour fluidifier cette collaboration en termes opérationnels, notamment en assurant une exploitabilité continue de ses livraisons : à chaque fin du sprint, les fonctionnalités livrées doivent être opérationnelles et doivent pouvoir être mises en production.

Le Titulaire met en place les moyens nécessaires afin d’assurer les principes suivants :

* + Dans le cas d’un changement d’équipier en cours de mission à l’initiative du Titulaire, un recouvrement est à la charge du Titulaire pour assurer le maintien de la compétence et du niveau de service attendu. A l’issue d’un délai convenu mutuellement (minimum de 5 jours ouvrés) avant le début du recouvrement, une mesure est effectuée avec la matrice de compétences concernée. Si l’évaluation est insuffisante (en deçà des seuils), la Cnam peut demander une extension de la période de recouvrement pour 5 jours ouvrés supplémentaires. Si au terme de cette période, l’évaluation est toujours insuffisante, la Cnam peut récuser l’intervenant proposé.
  + Au-delà des compétences de l’équipe, le Titulaire s’engage sur la pérennité et la flexibilité de son équipe (diminution de personnel ou montée en charge) afin de s’adapter aux besoins du projet. Le Titulaire s’engage à adresser cette flexibilité d’équipe en respectant les délais suivants d’ajustement :
* Diminution avec préavis de la Cnam de 5 jours.
* Augmentation sous un délai de 10 jours ouvrés maximum.

#### Cadrage Agile

Au sens large, on entend par « cadrage » l’ensemble des activités visant à déterminer le contexte, les enjeux et les objectifs du projet.

La phase de cadrage est décidée à la seule initiative de la Cnam et s’applique en amont de toute commande visant à engager la fabrication d’un incrément de produit livré en production.

L’approche orienté « Produit » s’attache, durant cette phase, à faire émerger « la vision » d’une version du produit. Elle est construite en équipe au travers d’ateliers, puis consolidée durant la vie du projet. La vision donne naissance à des macro-fonctionnalités qui s’affinent ensuite sous la forme d’histoires utilisateur (ou US pour User Story) constituant ainsi un premier portefeuille de fonctionnalités (backlog produit).

#### Estimation du calcul des stories points

Pour faciliter l’organisation du sprint backlog et l’estimation des stories points, la Cnam privilégie une méthode de type planning poker qui offre les avantages suivants :

* + La combinaison des estimations individuelles de l’équipe de la réalisation mène à de meilleures évaluations. Les informations incomplètes sont détectées plus rapidement (selon les expériences et les sensibilités, l’explication rapide des estimations met en évidence des taches potentiellement surestimées, oubliées, ou sous-estimées).
  + L’estimation étant directement validée par l’équipe de réalisation, l’engagement de l’équipe est plus fort, ce qui sécurise la date de livraison.
  + Elle permet à la Cnam de mieux comprendre les évaluations.

La Cnam considère qu’au plus tard à partir du quatrième sprint cette pratique permet d’arriver à des estimations fiables pour les sprints et d’ajuster la pertinence des poids du backlog produit.

Pour faciliter la compréhension, mieux aborder le niveau de complexité et éviter les litiges sur cette phase, un catalogue de référence est établi sur la base des premières stories représentatives.

#### Spécificité de la phase préparatoire des sprints

L’objectif ciblé est d’avancer selon un rythme très dynamique avec des gains rapides et réguliers, de véhiculer chez toutes les parties prenantes une forte image d’évolutions continues apportant à chaque fois une forte valeur ajoutée. Cette stratégie n’est possible qu’avec une bonne préparation initiale avant d’entrer dans le cycle itératif.

La phase préparatoire doit permettre de :

* + Créer les équipes impliquées dans la réalisation du projet.
  + Mettre en place la méthode proposée, présenter/initialiser les outils collaboratifs nécessaires, valider les modalités de fonctionnement et les processus communs.
  + Mettre en place les conditions organisationnelles, humaines, et procédures projets nécessaires à la réalisation dans de bonnes conditions des sprints suivants.
  + Valider l’organisation et les instances de validation / décision.
  + Valider l’application du plan assurance qualité.
  + Valider l’application du plan assurance sécurité.
  + Valider les hypothèses techniques.
  + Partager les exigences du dossier d’architecture, du plan de reprise d’activité et de la convention de service.
  + Mettre en place l’environnement technique nécessaire au projet, conformément au dossier d’architecture validé (Environnement de développement, d’intégration continue, de recette interne, de validation client, etc.).
  + Mettre en place l’usine de production logicielle validée par la Cnam permettant d’assurer l’intégration continue du code, l’automatisation de l’exécution des tests, la livraison automatique et le contrôle automatique de code.
  + Réaliser l’intégration aux différents systèmes d’information utiles au projet.
  + Valider la procédure de déploiement continue.
  + Affiner le backlog.
  + Confirmer un macro-planning global de référence avec le nombre de sprints envisagés.
  + Établir le contenu du sprint suivant.

#### Livrable des stories et des conditions du fini associées

Chaque story définie par la Cnam, pour être traitée en sprint par le Titulaire, doit contenir ses conditions du fini (acceptations). Les conditions du fini décrivent le comportement attendu de la story et formalise les tests avant l’écriture du code (Test Driven Development).

Cette méthode permet de décrire le besoin et le test associé en une seule étape avec les avantages suivants :

* + Limite l’effort de rédaction d’un cahier de recette en permettant d’organiser le plan de tests fonctionnel à destination des acteurs de recette de la Cnam.
  + Simplifie l’automatisation des tests, ce qui permet de livrer en continue sereinement grâce à un nombre suffisamment conséquent de tests automatisés de non-régression.

#### Gestion de la documentation produit

Le Titulaire maintient, à partir des spécifications de la story validée, une documentation produit suffisante de l’ensemble des composants du produit. La documentation produit est un livrable de spécification qui respecte les mêmes règles de description que les livrables de spécification du cycle en V.

La documentation doit recouvrir les spécifications, le dossier d’architecture fonctionnel et technique, les dossiers d’interfaces, les cahiers de tests, rapport de performances, rapport de qualité de code, le dossier de sécurité, les notes de sécurité et le dossier d’exploitation, dossier CNIL et RGPD.

La mise à jour documentaire d’une release précédente e doit être réalisée au plus tard lors du premier sprint de la release suivante pour validation par le PO de la feature team.

Le Titulaire maintient une documentation produit suffisante, permettant une réversibilité / transmission efficace au fil de l’eau de l’ensemble des composants du produit.

#### Mise en place d’un outil de suivi visuel

La transparence nécessaire doit se traduire par un accès permanent aux indicateurs et informations du projet : sprint, release, backlog produit, stories, indicateurs de vélocité et de qualité.

Afin de collaborer au mieux, l’outil de suivi visuel et collaboratif permet de :

* + Se rendre compte de difficultés (éléments bloqués),
  + De partager la vision de ce qui est fait, en cours et reste à faire à un instant T, à la fois au niveau détaillé (story tâches) et au niveau tableau de bord global (périmètre, coût, délai)

Chaque story est gérée individuellement et suit un workflow précis modélisé dans l’outil JIRA de la Cnam. Le Titulaire initie l’accord-cadre sur la base des workflow et tableaux de bord existants et les fait par la suite évoluer en fonction des besoins et de l’organisation.

La Cnam met à disposition les tableaux Kanbans et les outils Jira et Confluence de la Cnam pour la documentation. Le titulaire doit s’intégrer dans l’utilisation de ces outils.

#### Agilité à l’échelle

La taille du projet rend nécessaire la constitution de plusieurs équipes Agile en parallèle. Le suivi et la coordination de ces équipes doivent être assurés par le Titulaire.

Pour mettre en oeuvre cette mise à l’échelle, le Titulaire organise ses équipes de 3 à 6 personnes pour respecter les bonnes pratiques reconnues de l’Agilité.

La méthode retenue par la Cnam est SAFe like.

#### Recette Front Office/Back Office

Dans le cadre de la recette, la mise en place de la stratégie de recette dépend à la fois des exigences à remplir afin de prononcer un PV de recette validé par l’Agent Comptable.

L’exécution des recettes peut être réalisée par les équipes projet PO, par des experts Cnam et/ou par délégation au Titulaire (sous responsabilité Cnam) selon le besoin et le chantier concerné.

Pour ce faire, le titulaire doit prévoir une organisation en miroir entre ses équipes et les équipes Cnam pour assurer :

* + La définition d’une stratégie de recette adaptée à chaque livraison et des moyens à mettre en œuvre en fonction de l’enjeu du chantier correspondant pour pouvoir prononcer la validité de la recette tout en s’inscrivant dans la démarche agile.
  + La mobilisation des experts Cnam nécessaires, le cas échéant, à une recette sur un chantier relatif ou en adhérence avec le SI Cnam.
  + L’organisation et la coordination des différentes recettes ainsi que du suivi des plannings et de la contribution à l’amélioration des processus si nécessaire.

Le Titulaire est responsable de la fourniture des données de tests, de leur pseudonymisation, des éventuels bouchons et injecteurs nécessaires.

Mise en place de l’automatisation des tests :

La Cnam est attentive à la mise en place de tests automatisés pour fiabiliser la qualité des réalisations et permettre un déploiement continue du projet. Le rapport positif des tests automatisés est une condition nécessaire à toutes mises en production.

Au sein des projets itératifs, les tests du titulaire s’articulent autour de deux pratiques essentielles :

* + La production d’un référentiel de tests automatisés couvrant de façon systématique les fonctionnalités définies et assurant en permanence la vérification de conformité aux besoins métier,
  + La mise en oeuvre de tests exploratoires manuels couvrant les nouvelles fonctionnalités produites lors du sprint.

Mise en place d’une plateforme d’intégration continue :

Afin d’éviter l’effet tunnel lié à la phase de développement, d’optimiser le lissage des activités pour l’ensemble des ressources sur toute la durée du projet, la livraison des développements validés doit être faite en flux continu.

L’objectif est d’avoir l’intégralité des développements « done » continuellement accessible par la Cnam.

Les tests sur *devices* sont réalisés sur un environnement non ouvert sur Internet, via DNS privée. Le Titulaire doit donc prévoir la possibilité de modifier le root de son matériel.

Les tests unitaires doivent être automatisés.

#### Exigences

Outre les exigences définies dans les unités d’œuvre, le Titulaire respecte les exigences spécifiques suivantes :

| Exigences | Description générale |
| --- | --- |
|  | La transparence nécessaire doit se traduire par un accès permanent aux indicateurs et informations du projet, aux activités en cours et à leurs avancements : sprint, release, backlog produit, stories, indicateurs de vélocité et de qualité. |

### Méthodologie de projet Cycle en V

Par exception, la Cnam se réserve la possibilité de mettre en œuvre un mode projet en cycle en V. Les exigences de chaque activité sont décrites dans les paragraphes suivants.

Dans le cadre d’une demande de développement cycle en V  :

En réponse à une demande Cnam de développement cycle en V, le Titulaire communique à la Cnam un état préparatoire à la commande (EPC), sur le fondement des unités d’œuvre prévues à l’accord-cadre, couvrant l’ensemble des travaux nécessaires à la mise en œuvre de la nouvelle version. Ceci couvre le cycle complet de conception, développement, validation, intégration, VA, mise en production et VSR. Les évolutions sont réalisées par le Titulaire dans le cadre de ses engagements en termes de disponibilité, intégrité, confidentialité, auditabilité, exploitabilité et performances.

#### Conception et spécifications

Le Titulaire organise et anime le recueil des besoins permettant de préciser les exigences fixées par la Cnam. Le Titulaire est responsable de la conduite de cette phase, celle-ci devant se conclure par la production de la documentation nécessaire et suffisante au lancement des activités de réalisation de la version.

Cette activité permet également de préparer la recette de la solution et prend en compte les exigences de réversibilité en fin d’accord-cadre.

#### Recette des prestations par la Cnam

Le Titulaire :

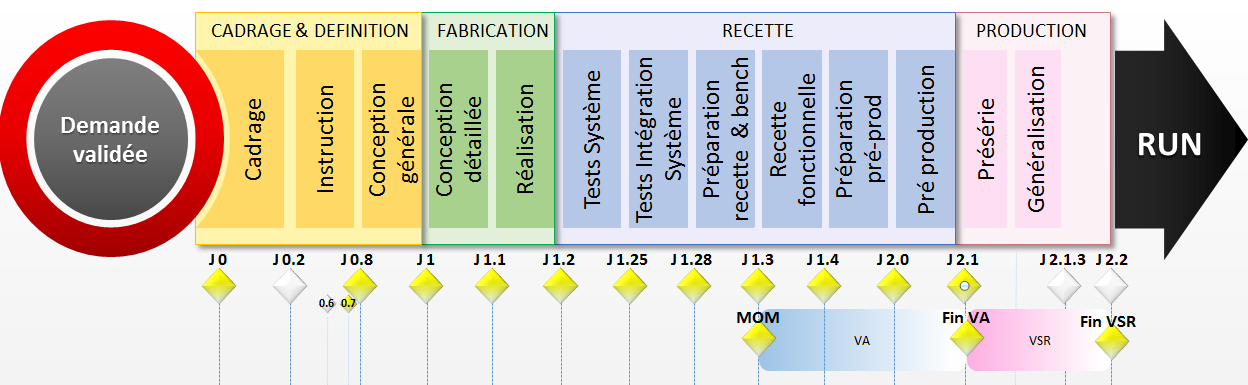
* + Met à disposition de la Cnam plusieurs environnements de test opérationnels (fonctionnels, sécurité),
  + Participe aux comités de pilotage de la recette,
  + Assure le maintien en conditions opérationnelles des environnements utilisés,
  + Intervient sur les environnements pour effectuer les actions nécessaires au bon déroulement de la recette fonctionnelle (lancement de traitement, réinitiaisation d’environnement),
  + Prend en compte et corrige les anomalies remontées par la Cnam.

#### Synchronisation des versions du Titulaire avec les versions de la Cnam

Lors de la réalisation d’une nouvelle version applicative par le Titulaire, une nouvelle version des applicatifs Cnam en lien avec le parc applicatif du Titulaire peut également être réalisée.

Lors de la phase d’étude et du chiffrage d’une version par le Titulaire, le planning précis des deux versions est défini pour coordonner les travaux entre la Cnam et le Titulaire.

Le cycle de vie d’une version au sein de la Cnam est le suivant :



| Exigences | Description générale |
| --- | --- |
|  | Lors de la réalisation d’une version, le Titulaire s’engage à mettre des environnements applicatifs opérationnels interconnectés avec les environnements applicatifs de la Cnam à partir de la phase de réalisation J1.1 jusqu’à la phase de pré-production J2.1 comme décrit en 6.2.8 Exigences Environnement logiciel  Lors de la phase d’initialisation de l’accord-cadre, le PAQ et le processus de gestion des changements définissent les modalités de mise à disposition d’environnements applicatifs lors d’évolution du parc Applicatif Cnam en lien avec le parc Applicatif du Titulaire. |
|  | Lors des phases de Bench et de pré-production de la Cnam, les environnements applicatifs interconnectés avec les environnements applicatifs de la Cnam mis à disposition doivent être respectivement de type Bench et pré-production. |

Les travaux réalisés durant les différentes phases sont les suivantes (liste non exhaustive) :

* + Réalisation : Cette phase correspond aux développements des demandes d’évolution ou de correction ainsi qu’aux tests unitaires. Le besoin est d’avoir un environnent applicatif permettant de dérouler les cas techniques et fonctionnels en développement
  + Test Système : Cette phase correspond à la vérification du package d’installation par le Titulaire en amont de la livraison à la Cnam. Cette phase se déroule sur un environnement Cnam confié au fabricant. Le besoin est d’avoir un environnent applicatif permettant de dérouler les cas techniques et fonctionnels pour s’assurer de la bonne communication entre les modules applicatifs et la bonne exécution de quelques cas passant fonctionnels.
  + Test d’intégration Système : Cette phase correspond à la vérification du package d’installation par la Cnam en déroulant la procédure d’installation sur un environnement Cnam spécifique d’intégration. Le besoin est d’avoir un environnent applicatif permettant de dérouler les cas techniques et fonctionnels pour s’assurer de la bonne communication entre les modules applicatifs et la bonne exécution de quelques cas passant fonctionnels.
  + Bench : Cette phase correspond au déroulement de test de Bench sur un environnement dédié pour s’assurer de la tenue de la charge de scénario prédéfini et pour identifier le point de rupture du service. Le besoin est d’avoir un environnement de Bench permettant de remplir les objectifs du tir de bench.
  + Préparation Recette et Recette fonctionnelle : Cette phase correspond à la vérification d’aptitude de l’application et permet de confirmer les résultats de l’intégration vis-à-vis de l’installation. Le besoin est d’avoir un environnent applicatif permettant de dérouler les cas fonctionnels permettant de valider les attendus fonctionnels.
  + Préparation Pré-production et Pré-production : Cette phase correspond à la vérification du package d’installation en condition de production : c'est-à-dire sur un environnement iso-production. Cet environnement Cnam de pré-production aux mêmes spécificités en terme technique mais aussi sécurité. Le besoin est d’avoir un environnent applicatif permettant de dérouler les cas fonctionnels permettant de valider la bonne communication entre les modules applicatifs et la bonne exécution de quelques cas passant fonctionnels.

#### Exigences

Outre les exigences définies dans les unités d’œuvre, le Titulaire respecte les exigences spécifiques suivantes :

| Exigences | Description générale |
| --- | --- |
|  | Le Titulaire intègre le raffinement des exigences issu de la phase de conception au sein de son outil de suivi des exigences. |
|  | La totalité de la solution doit faire l’objet d’une documentation complète qui doit être livrée à la Cnam avant toute mise en production.  Un soin particulier doit être apporté au document décrivant l’architecture Fonctionnelle, Applicative et Technique (« Dossier d’Architecture ») qui doit être contrôlé par la Cnam.  Pendant la phase d’étude, la mise à jour du dossier d’architecture constitue un entrant obligatoire au lancement des développements.  A ce titre, ce dossier d’architecture doit décrire des éléments compatibles avec le méta-modèle d’architecture de la Cnam permettant son intégration au référentiel d’architecture d’entreprise et à sa cartographie. |

### Exigences communes aux méthodes Agiles et cycle en V

Outre les exigences définies dans les unités d’œuvre, le Titulaire respecte les exigences spécifiques suivantes :

| Exigences | Description générale | |
| --- | --- | --- |
|  | Le Titulaire développe et paramètre l’ensemble du périmètre applicatif ou, selon la nature de la prestation attendue, met en place l’ensemble des moyens humains et techniques nécessaire. Cette activité intègre aussi notamment :   * + La préparation, la réalisation et la documentation des tests unitaires, sur l’environnement de développement fournit par le Titulaire.   + La réalisation de l’intégration sur un environnement dédié incluant la préparation, la réalisation de la documentation de la version permettant l’installation et l’exploitation de la solution.   + La préparation, la réalisation et la documentation des tests de recette du Titulaire comprenant :   La recette fonctionnelle de chacune de ces prestations multi-devices ;  Des tests de bout-en-bout en cas de réalisation entre un système réalisé par le Titulaire et un système tiers ;  Des tests de charge permettant notamment d’attester de la capacité du système à satisfaire les exigences de niveau de service définies pour les prestations de maintien en conditions opérationnelles ;  Des tests de non régression. | |
|  | Le Titulaire met en place et maintient l’environnement de développement nécessaire à la réalisation de la prestation | |
|  | Le Titulaire organise les ateliers nécessaires à la conception du produit : planning, ordre du jour, support de présentation, animation, comptes rendus. | |
|  | Le Titulaire réalise les fonctionnalités demandées, conformément aux spécifications validées. | |
|  | Le Titulaire apporte son expertise à la Cnam pour la constitution du dossier CNIL en lien avec le périmètre du Titulaire. | |
|  | Le Titulaire anime la composante SSI, organise les ateliers et comités nécessaires et rédige les livrables liés tel que le dossier de sécurité des systèmes d’informations : analyse des risques, choix de solutions, risques non couverts. | |
|  | Documentation produit : le Titulaire maintient une documentation produit suffisante, permettant une transmission efficace au fil de l’eau de l’ensemble des composants du produit. | |
|  | Architecture technique adoptée par le Titulaire : Le Titulaire doit exposer l’architecture technique (matérielle, middleware, etc.) mise en œuvre dans sa solution. | |
|  | Le Titulaire rédige et tient à jour le plan de gestion des configurations. | |
|  | Le Titulaire rédige et exécute les tests unitaires et documente l’exécution de ces tests : plans de tests, tests passés, résultats d’exécution des tests. | |
|  | Le Titulaire s’engage sur la qualité du code des logiciels développés et sur le respect des normes fixées pour la réversibilité de fin d’accord-cadre, ainsi que sur les exigences fonctionnelles de sécurité. | |
|  | Le Titulaire doit mettre en place une gestion des codes sources et du versionning des versions décrites dans le plan de gestion des configurations. Il est responsable du bon versionning des versions et des modifications. Sur demande de la Cnam et à tout moment de l’accord-cadre, le Titulaire doit être capable de fournir les sources de l’applicatif | |
|  | Le Titulaire met à jour le Plan d’assurance et Plan d’Assurance Qualité en fonction des précisions apportées durant la phase de réalisation. | |
|  | Le Titulaire est responsable de la recette (technique, fonctionnelle (y compris bout en bout et non régression), d’intégration, performance et sécurité) concernant son périmètre. Il fournit sa stratégie de recette concernant l’ensemble des devices. Après validation de la Cnam, il exécute et restitue les résultats de sa recette, ainsi que le plan d’actions de résolution des anomalies détectées quel que soit leur niveau. | |
|  | Suite aux opérations de recette du Titulaire, ce dernier livre les prestations recettées sur un environnement de recette fonctionnelle à destination de la Cnam, afin que la Cnam puisse procéder à la recette fonctionnelle et des tests de sécurité permettant de réaliser la vérification d’aptitude. | |
|  | Le Titulaire intègre l’ensemble de ces plans de tests au sein d’un référentiel de tests pour chaque prestation d’évolution réalisée | |
|  | Le Titulaire développe et maintient les outils et moyens de tests :  bouchons, émulateurs, autres dispositifs permettant de procéder aux tests des différents systèmes indépendamment les uns des autres ;  outils de gestion de contextualisation des données et leur remise en état | |
|  | Le titulaire met en place et partage le cahier de test des phases d’automatisation des tests. | |
|  | | Le Titulaire s’engage à répondre aux exigences de la Cnam pour assurer son déroulement et permettre à la Vérification d'Aptitude d'être prononcée.  Préalablement au prononcé d’une validation d’aptitude, la Cnam se réserve cependant le droit de procéder par elle-même à des tests de sécurité et d’intrusion ainsi que des opérations de vérification à partir de l’environnement de recette qui lui est dédié. |
|  | | Le Titulaire livre les prestations sur un ou des environnements de recette fonctionnelle afin que la Cnam puisse procéder à des tests de recette fonctionnelle et de sécurité |
|  | | Le Titulaire doit participer à la recette intégrée du produit de bout-en-bout avec les autres acteurs impliqués : implication dans l’intégration, passage des tests, prise en compte des résultats de tests, etc. |
|  | | Le Titulaire s’engage à coordonner les tests de bench dans le cas où la Cnam souhaite intégrer des modules applicatifs interfacé avec le SI-ENS (SI-enrolement), SI-Cnam hébergés par la Cnam ou un tiers, et donc mesurer la performance globale du système. |
|  | | Le Titulaire traite les anomalies remontées par la Cnam suivant la procédure de gestion des anomalies définie en annexes « MESDMP\_Annexe 06 – Workflow Clear Quest Fiche de Signalement » et « MESDMP\_Annexe 07 – Workflow Clear Quest Fiche Tiers ». |
|  | | La Cnam qualifie chaque anomalie selon les niveaux définis dans le Plan Qualité Gestion des Evolution. A titre d’exemple, les considérations suivantes peuvent être envisagées :  Anomalie bloquante :   * Il s’agit de tout incident ou anomalie de fonctionnement rendant impossible l’utilisation en production d’un logiciel ou d’une de ses fonctionnalités critiques. * Il peut également s’agir de la détection d’une vulnérabilité jugée critique par la Cnam.   Anomalie grave :   * Il s’agit de tout incident ou anomalie de fonctionnement restreignant l’utilisation en production d’un logiciel pour une partie seulement de ses fonctionnalités ; les fonctionnalités critiques restant toutes opérationnelles. * Il peut également s’agir de la détection d’une vulnérabilité jugée élevée par la Cnam.   Anomalie gênante :   * Il s’agit de tout incident mineur ou anomalie mineure de fonctionnement permettant toutefois l’utilisation complète en production du logiciel dans l’ensemble de ses fonctionnalités, même si celle-ci se fait au moyen d’une procédure de contournement.   Un ensemble d’anomalies graves ou gênantes, empêchant dans leur ensemble une utilisation ergonomique du service, ou nuisant à l’image de l’application, peut donner lieu à la création d’une anomalie bloquante pour la mise en production, sur décision de la Cnam. Ces éléments sont précisés dans le PQGE. |
|  | | Le Titulaire peut demander une requalification de la sévérité des anomalies en apportant des éléments concrets. La Cnam décide en dernier ressort de la criticité et de la priorisation des anomalies en fonction notamment de l’impact pour les utilisateurs et l’image du service |
|  | | Le Titulaire procède au traitement des anomalies détectées. |
|  | | Les anomalies en recette doivent être prises en compte et corrigées par le Titulaire selon les délais suivants :   |  |  | | --- | --- | | Gravité | Résolution (en heure ouvrable) | | Bloquante | 48h | | Grave | 5j | | Gênante | 10j |   Pour un bon de commande, le taux d’anomalie, calculé suivant la formule ci-dessous, doit être strictement inférieur à 0.1.  (Nb anomalie bloquante + Nb anomalie grave + Nb Anomalie Gênante) / (Prix du bon de commande en € HT / 500)  Si ces niveaux d’exigence ne sont pas atteints, la Cnam peut appliquer les pénalités définies au CCAP. |
|  | | L’absence d’anomalie bloquante pour la mise en production à l’issue de la période de recette est un prérequis au prononcé par la Cnam de la validation d’aptitude d’une prestation livrée par le Titulaire. |
|  | | Le Titulaire se met en capacité de répondre aux demandes d’intervention sur les environnements de recette fonctionnelle de la Cnam. Ces interventions sont inscrites dans le cadre de l’avancée des tests de recette fonctionnelle ou de sécurité. Le catalogue de demandes d’intervention en recette fonctionnelle comprend a minima :  Lancement de traitement  Mise à jour des environnements afin de réinitialiser les jeux de données de recette de manière régulière et automatique  Réalisation de copies de BDD de référence  Réinitialisation de la BDD à partir d’une copie de référence  Une demande de changement en recette fonctionnelle doit être réalisée en 48 heures ouvrées à compter de la date de déclaration. |
|  | | Le Titulaire décrit et tient à jour, au sein du PQGS, met en place et maintient les moyens, les processus de gestion des services en production notamment sur les services :  de gestion du catalogue de services ;  de gestion des changements ;  de gestion de configurations ;  de gestion de la disponibilité ;  de gestion des incidents ;  de gestion des problèmes ;  de gestion de la supervision ;  de gestion des déploiements et des mises en production ;  de gestion du niveau de service.  de gestion du plan de continuité des activités. |
|  | | Le Titulaire décrit et tient à jour sa procédure d’installation et décrit notamment le minutage de cette installation. |
|  | | Le Titulaire installe en environnement de pré-production l’ensemble des éléments réalisés, recettés et dont le bilan a été validé par la Cnam, et teste ainsi sa procédure d’installation en pré- production.  Suite au test d’installation, le Titulaire fournit un bilan de la mise en pré-production et affine, si nécessaire, sa procédure d’installation. |
|  | | Le Titulaire met en production l’ensemble des éléments réalisés, recettés puis validés par la Cnam conformément à la procédure de mise en production testée puis validée par la Cnam et uniquement sur décision formelle de la Cnam.  Suite à la mise en production, le Titulaire fournit un bilan de cette mise en production. |

## Rôles et activités clés

Dans le cadre de la mise en œuvre de l’organisation schématisée ci-dessus, un certain nombre de rôles clés et activités associées sont attendus et précisés ci-dessous. Ces profils peuvent être assurés selon le contexte, par des personnels Cnam, par des personnels du Titulaire, ou encore en binôme.

Il est précisé que l’organisation doit, par essence, être adaptée au besoin en fonction des périodes de l’accord-cadre. Le présent accord-cadre comporte différentes phases et des activités très différentes les unes des autres : initialisation, convergence Mon espace santé /DMP, offre de service pour les besoins du BSP, etc.

De périmètre très large, l’accord-cadre engage un nombre conséquent de collaborateurs Cnam et du Titulaire. Le Titulaire veille à proposer à chaque fois que nécessaire des adaptations de l’organisation, en concertation avec la Cnam, destinées à améliorer le fonctionnement de l’ensemble du dispositif. Ces améliorations doivent être objectivées sur la base de 4 indicateurs clés :

* + Indicateurs de vitesse :
* Fréquence de déploiement : mesure l’optimisation du flux de production de valeur
* Délais de livraison en production du code produit : mesure la rapidité de mise à disposition en production du code finalisé
  + Indicateurs de stabilité :
* Temps de remise en condition opérationnelle et de sécurité : mesure la performance de correction d’un défaut
* Taux d’erreur : mesure la qualité du code livré

L’ensemble de l’organisation doit être au service du maintien du niveau de ces indicateurs, dont certains doivent encore être étalonnés. A titre indicatif, à mai 2023, les valeurs partiellement objectivées sur le seul périmètre Mon Espace Santé pour les indicateurs de vitesse sont, à l’exception de chantiers de grande ampleur, approximativement les suivantes :

* + Fréquence de déploiement :
* 1 fois par semaine pour du patch
* 1 fois par mois pour une version majeure
  + Délais de livraison en production du code produit :
* 1 semaine sur une branche TMA / MCO
* 2 versions majeures par trimestre

### **Rôles Direction produit**

|  |  |
| --- | --- |
| Rôles | Activités |
| Product Manager (de différents niveaux :   * multi-produit (ex : Mon espace santé et DMP) * monoproduit (ex : Mon espace santé ou Mon espace santé mobile) * parcours multifeatures au sein d’un produit | * Met en œuvre les moyens pour identifier les opportunités Produits * Qualifie le potentiel d’usage des opportunités Produit au regard de tests utilisateurs et de données quantitatives * Construit sur la base de tous les entrants la proposition de feuille de route produits * Formalise auprès des sponsors les ambitions et impacts Produits pour validation * Porte les attentes produits dans le cadre des instances du type PI Planning, Release Management * Pilote les cadrages Produit exploratoires * Pilote les cadrages opérationnels des Features Teams sur les activités de cadrage * Assure les rituels de niveau produit, en particulier dans sa composante offre de services * Suit la réalisation du delivery pour apporter les priorités du Product Management * Suit la production, les usages des produits, les différents niveaux de support, les niveaux de services et en fait un reporting à ses commanditaires * Assure la production des supports nécessaires aux différentes instances de partage autour du produit (intra et extra projet) |
| Lead Design | * Organise, structure et homogénéise les livrables designer en cadrage et delivery * Compose et pilote les équipes design (sourcing, staffing, rotation) * Collabore : outillage design, animation des rituels et meetings * Accompagne la montée en compétences des équipes * Standardise et harmonise les processus de conception * Mesure : Suivi des travaux « User research » quantitatifs (Indicateurs d’usage) et qualitatifs (Retour terrains et tests utilisateurs), en particulier en appui aux communautés d’utilisateurs * Contribue à la priorisation des roadmaps des Feature Teams et sujets transverses pour passage à l'échelle * Est garant du Design system MESDMP * Apporte aux équipes l’expertise nécessaire pour assurer la conception de composants et de parcours conformes aux exigences d’accessibilité |
| Lead Data Desk | * Accompagne les Features Teams dans la construction des indicateurs métiers pertinents pour le suivi des usages * Compile les données des différentes sources disponibles, indicateurs métiers MESDMP dont ceux du catalogue de services, données de webanalytics, indicateurs métiers DMP, et toutes autres sources pertinentes, pour en dégager des tendances et des informations qui servent les propositions d’orientation stratégique du Product management * Suit des données de production pour construction et maintenance d’abaques standard d’usages, partage avec les acteurs du suivi de production pour acculturation et accompagnement pour assurer une réactivité ad hoc à des comportement atypiques (hors abaque) * Identifie les variations et les investigue, pose les hypothèses en conséquence * Fait corréler avec les hypothèses d’usage * Oriente les parties prenantes et la Direction produit * Veille au suivi des mésusages des systèmes * Construit et actualise les tableaux de bord de suivi des usages à des fins de communication |

### **Rôles de niveau Delivery transverse**

|  |  |
| --- | --- |
| Rôles | Activités |
| Responsable Delivery transverse (type release train manager) | * Prend la responsabilité du périmètre visé dans le cadre d’un incrément (ou train) * Suit l’exécution du delivery en regard des objectifs sur la période concernée * Met en place les mécanismes de reporting et alerte si nécessaire * Construit avec les équipes concernées les plans de remédiation aux difficultés rencontrées pour maintenir les objectifs visés. * Est responsable des indicateurs de vitesse mentionnés en début du présent paragraphe. * Suit l’avancement des instructions nécessaires à la construction du ou des trains suivants en fonction de la feuille de route proposée par le Product Management et la Direction Services * Travaille avec les coordonnateurs ci dessous (cellule technique, cellule production avec FT et Direction produit) * Assure la restitution de la livraison faite dans le cadre d’un train |
| Coordonnateur Cellule technique / Features teams (FT) et Direction produit | * Facilite la compréhension entre les attentes métiers et les exigences de conception * Aide à l’identification des points durs et remonte à l’arbitrage les cas le nécessitant le plus en amont possible |
| Coordonnateur cellule production / Features teams et Direction Produit | * Suit la production d’un point de vue métier, en coordination avec le SDM * Se coordonne avec le responsable du delivery transverse pour la prise en compte des anomalies en fonction du contexte (SLA) et du niveau d’exécution du train par ailleurs * Remonte des arbitrages si nécessaires à la Direction de programme * Coordonne les features teams dans la prise en charge des anomalies, priorise les sujets pour mise en production en fonction de leur impact après concertation avec le responsable du delivery transverse * Coordonne le suivi opérationnel de la production avec le Data desk * Contribue avec le SDM au suivi des indicateurs de suivi des délais de résolutions des incidents. |
| Responsable recette | * Responsable de l’ensemble des activités de recette des systèmes intégrés (non bouchonnés), y compris techniques et sécurité * S’assure que les recettes puissent être réalisées dans les conditions attendues * Réalise le suivi de la recette d’une version dans sa globalité * Veille à la maintenance, la complétude et l’amélioration du patrimoine de tests, y compris les tests automatisés * Reporte et partage régulièrement avec l’ensemble des équipes sur ce patrimoine de tests automatisés de manière à optimiser les recettes à tous le niveaux (y compris au niveau des features teams) |
| Responsable recette fonctionnelle | * Est responsable de la recette fonctionnelle des releases majeures et mineures * S’assure que les prérequis et les entrants sont fournis aux équipes de recette * Réalise le suivi des recettes fonctionnelles en articulation avec les centres de recette de la Cnam |
| DPO Data Protection Officer / Expert RGPD | * Instruit les exigences RGPD relatives aux fonctionnalités des produits * Accompagne les équipes dans la démarche « privacy by design » * Assure la conformité au RGPD du Titulaire * Met à jour les AIPD |

### **Rôles au niveau Delivery des Features**

|  |  |
| --- | --- |
| Rôles | Activités |
| Product Owner | * Priorise le backlog de fonctionnalités à développer au cours des sprints à venir sur la base des orientations définies par le Product Management et la Direction services * Est responsable du périmètre en delivery au cours du sprint en cours * Anime la revue avec la Direction Produit et le responsable du delivery transverse * Est responsable du traitement des anomalies de production relevant de son périmètre, en articulation avec le responsable du delivery transverses et des équipes en charge du suivi du MCO. |
| Proxy PO | * Appui le Product owner (de compétences nativement orientées plus sur du fonctionnel et du métier) dans sa compréhension et dans sa prise en charge des sujets techniques * Décline les exigences techniques et sécurité au sein de la feature teams pour assurer leur bon niveau de prise en charge par tous les profils |
| Scrum Master | * Est responsable de l’application de la méthodologie Agile au sein de la FT * Est responsable de l’amélioration continue de la FT * Facilite les échanges et participe à la recherche de solutions au quotidien * Anime les rituels agiles de type Sprint Demo à l’issue des sprints, Daily Meeting, Sprint Retrospective, etc |
| Business Analyst | * Est responsable de la déclinaison des fonctionnalités en US * Est responsable du suivi opérationnel du delivery et de la capacité de la FT * Est garant de la cohérence technique et du back-office du périmètre de la Feature team * Anime les instances : Affinage, Sprint Planning |
| UX Designer | * Est responsable de l’expérience utilisateur et de l’aspect visuel des fonctionnalités à développer, dans le respect du cadre défini par le Lead Design * Contribue à la conception et à la déclinaison du Design System dans la conception de chaque fonctionnalité * Réalise des tests d’usage auprès des utilisateurs pour garantir l’adaptation des fonctionnalités aux besoins des usagers * Travaille en articulation avec le Lead Data desk pour se nourrir et alimenter en retour la boucle de collecte de la donnée destinée à éclairer les orientations de la feuille de route. |
| Développeur | * Développe (code) des US à développer au sein de chaque FT * Participe à l’affinage et à la planification des US à développer au sein des sprints * Les développeurs peuvent en fonction des cas présenter des compétences, voir des expertises sur différents type d’activités ou technologies : Front, Back, full-stack, Mobile, etc. |
| Testeur | * Teste les fonctionnalités développées au cours du sprint sur les différents environnements d’intégration, de recette et de préprod |

### **Rôles Direction services**

#### *Cellule technique*

|  |  |
| --- | --- |
| Rôles | Activités |
| Technical Lead | * Est responsable de la cohérence de l’architecture de la plateforme MES/DMP en termes de choix techniques, logiciels, sécurité et performance |
| Architecte Lead | * Est responsable de la cohérence de l’architecture Applicative de la plateforme MES/DMP en termes de choix techniques et sécurité |
| Architectes | * Architectes Infrastructure si le Titulaire a la responsabilité de l’hébergement * Architectes Technique et Logiciel * Architectes Applicatifs * Architectes Fonctionnels * Architectes Transverses * Architectes Sécurité |
| Responsable DevSecOps | * Coordonne les équipes de développement, de sécurité et ops afin de garantir la prise en compte de la sécurité dans l’intégration des composants * Garantit la mise en œuvre des bonnes pratiques DevSecOps * S’assure que les process et outils de CI/CD répondent aux exigences du DevSecOps et réalise le suivi de l’amélioration continue du process DevSecOps |
| Responsable intégration technique | * Est en charge du suivi de tous les chantiers intégration technique et de la mise en œuvre des chaînes d’accrochage techniques et sécurité |
| Bureau Technique | * Réalise les déploiements et opérations techniques sur l’ensemble des environnements * Pilote et réalise le support N3 * Réalise les tests de performance |

#### Cellule projet

|  |  |
| --- | --- |
| Rôles | Activités |
| Release Manager | * Pilote l’ensemble des phases d’une version depuis sa définition jusqu'à sa mise en production * S’assure de la cohérence d’ensemble du contenu des releases et du respect de livraison dans le calendrier défini. |
| Delivery leader | * S’assure de la mise à disposition des moyens et ressources pour que les FT puissent réaliser les travaux * Réalise le suivi d’avancement des FT * Agit et alerte si nécessaire quand les FT font face à des difficultés ou des blocages |
| Intégration recette | * S’assure de l’intégration et des recettes des versions sur les différents environnements * S’assure de l’évolution et de l’automatisation des scenarios de tests techniques/fonctionnels/performances/sécurité |

#### Cellule Production

|  |  |
| --- | --- |
| Rôles | Activités |
| SDM | * Assure le respect des engagements de services * Manage et coordonne les équipes opérationnelles pour assurer un service de qualité et atteindre les engagements liés au contrat de service * Identifie, partage et met en œuvre les axes d’amélioration pour garantir la qualité de service * Assure la présentation des KPI auprès de la Cnam |
| TSM Infrastructure / Applicatif | * S'assure que les services sont fournis conformément à la description du service et que tous les SLAs sont atteints * Veille au maintien de la qualité des services et identifie les axes d'amélioration continue. * Assure la gestion des incidents |
| TSM Réseau | * Pilote les sujets et l’équipe d’ingénieur réseau |
| TSM Support N2 | * Pilote le support N2 |
| Equipe OPS | * S’assure que la chaîne d’intégration continue est fonctionnelle et veille à l’amélioration continue de cette chaîne CI/CD * Réalise l’intégration et les déploiements des versions applicatives sur les différents environnements d’intégration et de recette |

#### *Cellules Sécurité / RSSI*

|  |  |
| --- | --- |
| Rôles | Activités |
| Directeur de projets Cyber | * Reporte, organise/prépare et assure les instances de gouvernance Sécurité, suit l’avancement des PKI Sécurité * Pilote les projets sécurité |
| RSSI  Responsable de la Sécurité des Systèmes d’Information | * Veille au respect de la confidentialité, l’intégrité, la disponibilité et la traçabilité des données ou informations, vision transverse du Build au RUN * Est « porteur de secrets » dans les cérémonies de clés, garantit le respect des indicateurs * Est en charge d’expliciter les risques à la demande de la Cnam et ou de faire intervenir des experts du domaine * Assiste la DPO/RGPD, valide et réalise les demandes d’ouverture de cellule de crise, et participe à l’astreinte managériale |
| Ingénieur DevSecops | * Contrôle la bonne application opérationnelle du processus DevSecOps * Est en charge d'intégrer la dimension sécurité à toutes les étapes du projet et à l'automatiser * Garantit la mise à jour des contacts Sécurité dans le processus |
| SOC : Client Security Manager  Incident handler  Analyste SOC | * Est le point d’entrée contractuel (Soc Manager) * Garantit la mise à jour des contacts Sécurité dans le processus * Assure l’encadrement technique des analystes SOC * Participe à l’amélioration des règles de corrélation et des processus * Est en charge de la gestion des incidents de sécurité majeurs * Exploitation : identifie et qualifie les incidents de sécurité, effectue le triage, crée les notifications, traite les incidentes, lance les escalades Gestion de règles de détection |
| Consultant Cartographie des données | * Garantit la mise à jour et le suivi de la cartographie (protection des données) en collaboration avec la DPO GRP |
| Consultant Analyse des risques | * Réalise les analyses de risque sous la direction de l’Adjoint RSSI, du suivi avec la Cnam (à la demande du client) |

## Comitologie

NB : La comitologie présentée ci-après peut être reproduite à l’identique par le candidat ou ou faire l’objet de propositions d’amélioration/adaptation. Cela constitue des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

Les exigences associées à la comitologie sont notamment mentionnées dans le §6 « 6Définition des besoins » et sont détaillées, le cas échéant, dans le PAQ.

### **Comitologie Pilotage**

|  |  |  |  |
| --- | --- | --- | --- |
| INSTANCE | | FREQUENCE | OBJECTIFS |
| COMOP | | Hebdomadaire | Consolidation des suivis opérationnels (DPD, delivery, infra, sécurité, production) |
| COMOP Restreint | | Hebdomadaire | Pilotage stratégique du programme |
| COMAFI | | Trimestriel | Suivi contractuel et financier |
| Gestion Qualité | Mensuel | | Suivi de la Qualité/PAQ et des indicateurs (y compris PAS) |
| Gestion des Risques | Mensuel | | Revue des risques projets |

### **Comitologie Produit**

|  |  |  |
| --- | --- | --- |
| INSTANCE | FREQUENCE | OBJECTIFS |
| PI Planning | Trimestriel | Instance majeure de priorisation et planification du contenu à développer par chaque FT au cours de l’incrément à venir |
| Daily Meeting Direction Produit | Quotidien | Suivi des tâches prioritaires, travaux communs, adhérences de l’incrément N |
| Weekly Meeting Direction Produit | Hebdomadaire | Suivi et gestion de la préparation de l’incrément N+1 |
| Sprint Demo | Bimensuel | Session de revue au format Démonstration des éléments conçus par chaque FT à l’issue de chaque Sprint |

### **Comitologie Feature Teams**

Chaque Feature Team met en œuvre la comitologie Agile Scrum nécessaire à son fonctionnement en vue de la conception des fonctionnalités propres à son périmètre

|  |  |  |
| --- | --- | --- |
| INSTANCE | FREQUENCE | OBJECTIFS |
| Daily Meeting Feature Team | Quotidien | Suivi des actions quotidiennes sur le sprint en cours |
| Sprint Planning | Bimensuel | Planification des fonctionnalités à développer au cours du sprint à venir |
| Discovery / Expérience utilisateur | Hebdomadaire | Instance d’échange sur les parcours et l’expérience utilisateur des fonctionnalités à développer au cours des prochains sprints |
| Affinage | Hebdo | Cadrage et estimation de complexité des fonctionnalités à concevoir au cours des sprints suivants |
| Review | Hebdomadaire | Echange hebdomadaire avec la Direction Produit pour suivi de l’avancement, des adhérences et arbitrages le cas échéant |
| Sprint Rétrospective | Bimensuel | Instance d’amélioration continue du fonctionnement de l’équipe |

### **Comitologie Services**

#### *Cellule technique*

|  |  |  |
| --- | --- | --- |
| INSTANCE | FREQUENCE | OBJECTIFS |
| Comité DA/DT | Hebdomadaire | * Partage et suivi des instructions en cours * Présentation des principaux chantiers Techniques/Sécurité * Revue du backlog de la Design Authority |
| Gestion des points de douleurs | Hebdomadaire | Traitement des difficultés opérationnelles rencontrées par les FT en cours de delivery de l’incrément en cours |

#### *Cellule Projet*

|  |  |  |
| --- | --- | --- |
| INSTANCE | FREQUENCE | OBJECTIFS |
| Daily Bug | En fonction de la phase du projet | Instance de suivi de la prise en compte des correctifs au titre du MCO |
| CODEL | Bimensuel | * Partage de l’avancement du delivery * Remontée des risques et alertes du delivery |
| Comité release management | Hebdomadaire | Partage des plannings des releases futures, en particulier pour le suivi des dépendances avec les SI externes. |

#### *Cellule Production*

|  |  |  |
| --- | --- | --- |
| INSTANCE | FREQUENCE | OBJECTIFS |
| Daily Prod | En fonction de la phase du projet | Suivi de la production |
| CORUN | Trimestriel | * Suivi de la Production et du MCO * Suivi des SLA / KPI Production et Support * Suivi des processus GDI/GDD/GDC * Roadmap des MEP |
| COPROD | Hebdomadaire | Suivi du Run |

#### *Cellules Sécurité / RSSI*

|  |  |  |
| --- | --- | --- |
| INSTANCE | FREQUENCE | OBJECTIFS |
| COSEC | Bimensuel | Revue des sujets Sécurité pour arbitrages (chantiers sécurité en cours, la définition de la trajectoire sécurité du projet et de l’ensemble des points nécessitant une décision structurante pour le projet et également la MCS) |
| ComopSec | (\*) | Suivi des sujets sécurité opérationnels, des activités de MCS et des décisions afférentes. Des sachants opérationnels et experts techniques sont invités régulièrement à participer à ce comité pour les points spécifiques le nécessitant, afin de pouvoir alimenter le comité avec les informations précises permettant d’éclaircir des points en suspens : par ex. pour apporter des précisions techniques sur un correctif suite à une vulnérabilité, pour apporter des précisions techniques ayant permis de conclure du niveau de vraisemblance et de gravité d’une vulnérabilité, etc |
| ComOpSOC | (\*) | Suivi des activités du SOC |
| Comité DevSecop | (\*) | Security by design, suivi des indicateurs sécu du DevSecOps |

(\*) : Les comités opérationnels ont initialement lieu avec une fréquence hebdomadaire. La Cnam peut réduire cette fréquence selon le contexte du projet

## Politique qualité

La politique qualité consiste à décliner de façon pragmatique, dans un cadre adapté au présent accord-cadre, l'ensemble des normes en vigueur et spécificités de la Cnam, pour obtenir la qualité des services et des produits.

S’agissant des prestations, l'approche qualité retenue doit respecter les aspects essentiels suivants : organisation, communication, documentation, contrôle, tableaux de bord, plan d’amélioration agrégé, respect des normes et développements à l’état de l’art pour les aspects techniques, delivery et sécurité, respect des moyens et processus pour le MCO, le MCS et le PAQ.

La politique qualité doit être structurée et documentée notamment au travers d'un Plan d'Assurance Qualité (PAQ) constitué :

* + D’un Plan Qualité du Marché (PQM) : modalités relatives à la Planification et à l’Organisation de l’accord-cadre, à la gestion de la Qualité et à l’amélioration continue.
  + D’une Convention de Services (CS) : précise le contenu de l’engagement de service du Titulaire, avec les indicateurs associés, a minima pour l’ensemble des exigences décrites dans le CCTP et le CCAP.
  + D’un Plan Qualité Gestion des Evolutions (PQGE) : modalités relatives à l’acquisition et à l’implémentation des Produits et Services.
  + D’un Plan Qualité Gestion des Services (PQGS) : modalités relatives à la délivrance et au support des Produits et Services (a minima : anomalies, incidents, vulnérabilités, problèmes, supervision, changements, réclamations, configurations, disponiibilités, déploiements et mises en production, etc.).
  + D’un Plan de Gestion de Crise (PGC).
  + D’un Plan de Réversibilité (PR) : modalités relatives à la réversibilité de la solution en fin d’accord-cadre.

Le PQM, le PQGE, le PQGS et le PR deviennent applicables dès la première version validée par la Cnam.

Il est rappeleré que le PAQ ne peut avoir pour objet ni pour effet de modifier les engagements et obligations souscrits au titre de l’accord-cadre.

Un sommaire du PAQ est fourni en annexe : MESDMP\_Annexe 23\_PAQ\_Indicateurs\_Exemple de sommaire.

Les éléments du PAQ comprennent l’ensemble des exigences liées aux prestations et que le Titulaire s’engage à respecter.

Le Titulaire respecte les exigences spécifiques suivantes :

| Exigences | Description générale |
| --- | --- |
|  | Le Titulaire s’engage à fournir une première version du PAQ au plus tard à trois (3) mois après la réunion de lancement de l’accord-cadre.  Et à livrer l’ensemble des éléments du PAQ avant la fin de la phase d’initialisation de l’accord-cadre. |
|  | Le Titulaire s’engage à appliquer et à faire évoluer le PAQ dès le début de la prise de responsabilité (fin de la phase d’initialisation)  Et à fournir une nouvelle version de PAQ a minima à la fin de la 3ème Phase de la reprise : Prise de responsabilité par le Titulaire |
|  | Les éléments du PAQ et ses annexes font l'objet d'évolutions régulières a minima tous les deux mois, pendant toute la durée de l’accord-cadre, suite à des changements ou à la demande de l’une des Parties (Cnam ou Titulaire). Ces évolutions font l’objet d’une validation par la Cnam. |
|  | La qualité fait l’objet d’une instance de suivi (Comité Qualité) dont la fréquence est à définir avec le Titulaire (a priori mensuelle) |
|  | Le Titulaire pilote ses prestations de façon pro active et est force de proposition.  Le Titulaire garantit une cohérence entre les différents chantiers et prestations réalisées. |
|  | le Titulaire se conforme au PAQ validé par la Cnam et assiste celle-ci dans l’atteinte des objectifs liés à la politique qualité définie. |
|  | La politique qualité de la Cnam est définie par la Direction de la Cnam. Dans le cadre de la démarche Qualité ISO 9001, les principaux axes retenus sont les suivants :   * la satisfaction des interlocuteurs de la Cnam (« clients externes » au sens de la norme ISO 9001) ; * la sécurité financière et juridique des activités menées par la Cnam ; * l'amélioration des compétences des collaborateurs de la Cnam (« clients internes » au sens de la norme ISO 9001) |
|  | Le Titulaire s’engage :   * à appliquer a minima les Normes, Agréments et Réglementations en vigueur ou leur équivalent : ISO 9001, ISO 10005, ISO 10006, ISO 14001, ISO 19011, ISO 27001, ISO 22301, HDS, ISAE 3402 et IEEE 829-2008 * à respecter les autres normes décrites dans chaque chapitre du CCTP le cas échéant * à en fournir les preuves factuelles (certifications, justifications, etc.), avant le démarrage de la prestation et durant l’éxécution de l’accord-cadre |
|  | Le Titulaire doit réaliser l’auto-évaluation de conformité aux exigences de qualité et suivre les indicateurs définis dans la Convention de Service (dont indicateurs de qualité). Il s’engage à informer la Cnam des risques, des écarts et à faire des propositions de mise en conformité ayant trait à la qualité. |
|  | Le Titulaire doit informer l'ensemble des intervenants des dispositions retenues au titre de la qualité. Chaque intervenant doit avoir une parfaite connaissance des éléments applicables à son domaine d'intervention figurant dans le PAQ.  La Cnam se réserve la possibilité de déclencher les opérations de contrôle lui permettant de s'assurer que les intervenants maîtrisent et appliquent les dispositions figurant dans le Plan Qualité Projet. A l’issue, le Titulaire, sur demande de la CNAM, doit assurer la mise en oeuvre des plans et recommandations associés qui en découlent. |
|  | Le Titulaire remet toute documentation produite au cours de l’accord-cadre sous un format compatible avec les outils bureautiques utilisés par la Cnam (suite Office) conformément aux exigences de sécurité.  Par défaut, les documents doivent être conformes à la charte graphique de la Cnam, le formalisme et toutes contraintes de la Cnam (taille des documents, nommage, etc.) |
|  | Le Titulaire s’engage à :   * adresser toute demande de modification du PAQ ou de dérogation temporaire au PAQ au comité Qualité (lequel traite la demande et/ou la remonte à une instance supérieure). * diffuser, dès lors qu'une modification est apportée au PAQ, validé par la Cnam, la nouvelle version à tous les intervenants du projet. Chaque partie se charge de faire connaître les changements au sein de son organisation. * décrire au sein du PAQ l’organisation mise en place pour répondre aux objectifs liés à la gestion des ressources humaines, en particulier les règles de gestion des ressources mutualisées (priorisations, urgences, etc.). * documenter au sein du PAQ sa participation à des comités non explicitement prévus par l’accord-cadre. * documenter au sein du PAQ le contenu et les modalités de suivi et de reporting, ajustés en fonction des besoins. * informer l'ensemble des intervenants des dispositions retenues au titre de la qualité. Chaque intervenant doit avoir une parfaite connaissance des éléments applicables à son domaine d'intervention. |
|  | Le Titulaire nomme un correspondant qualité.  Ce correspondant qualité du Titulaire garantit la mise en application des dispositions prévues dans le PAQ, sensibilise les équipes du Titulaire au respect des dispositions qualité décrites au PAQ, veille à proposer des actions d’améliorations, participe activement aux audits qualité planifiés par la Cnam, ainsi qu’au traitement des écarts constatés et assure en permanence l’interface qualité entre le Titulaire et le responsable Qualité de la Cnam.  Il prépare également les indicateurs qualité attendus pour les comités de pilotage et de suivi. Dans le cadre du suivi, ces indicateurs sont fournis ponctuellement selon les demandes de la Cnam et a minima mensuellement. |
|  | Sur demande de la Cnam, le Titulaire s’engage à délivrer, le cas échéant, les accès nécessaires à tout document permettant la préparation, la réalisation et le suivi d’un audit mené par la Cnam ou par un tiers désigné par la Cnam. Ces audits peuvent porter sur les thèmes suivants (liste non exhaustive) :   * pilotage et gestion de projet * qualité (respect de la bonne application du PAQ, contrôle qualité d’un livrable, etc.) * organisation * développement, intégration, exploitation, etc. * fonctionnel * technique (Architecture, Revue de code applicatif, etc.) * performance * patch correctif * CMDB * gestion des changements d’environnement * test d’intégration et validation (fonctionnelle et technique) * test d’intrusion, de vulnérabilité ou de robustesse * gestion de la réversibilité.   La Cnam se réserve le droit de faire accompagner l’auditeur par un ou plusieurs de ses experts techniques.  Si l’audit prend la forme de tests d’intrusion, de vulnérabilité, de robustesse ou de performance, le Titulaire mobilise son chef de projet gestion des risques SSI en tant qu’interlocuteur privilégié de l’auditeur, du directeur de projet et du RSSI de la Cnam, tant pour l’organisation, la mise en œuvre que le suivi des audits.  Pour tous les autres audits, le correspondant qualité du Titulaire est l’interlocuteur privilégié de l’auditeur, du directeur de projet et du responsable Qualité de la Cnam (organisation, mise en œuvre et suivi des audits).  A l’issue d’un audit mené par la Cnam ou un tiers désigné par la Cnam, un rapport d’audit est établi et la Cnam communique au Titulaire les points d’amélioration identifiés pour action. |
|  | Suite au constat d’écarts lors d’un audit, le Titulaire :   * présente un plan d’actions pour la correction de ces écarts à la Cnam et le met en œuvre. * met en place les mesures correctives prévues par le plan d’actions validé par la Cnam.   Le Titulaire prend à sa charge le temps passé pour la participation aux audits, à l’analyse et aux traitements des écarts constatés.  Suite à la mise en œuvre d’un plan d’actions par le Titulaire, la Cnam constate la correction des écarts et lève les écarts s’il y a lieu. |
|  | Dans le cadre du plan qualité du MESDMP, la Cnam peut réaliser ou faire réaliser, par un tiers, des audits du code (type CAST) de l’ensemble des développements spécifiques réalisés dans le cadre de la mise en œuvre de la solution SI MESDMP. Pour ce faire, le code est mis à disposition de la Cnam de manière spécifique. De plus, la conformité du processus de développement et de la mise en œuvre peut être audité. |
|  | Dans le cadre de la fourniture des indicateurs mentionnés dans le PAQ (CS), le Titulaire communique à la Cnam les preuves de ses calculs et donne accès à la Cnam à l’ensemble des outils et aux données ayant contribué au calcul des indicateurs (outils de gestion des anomalies/incidents, outils de gestion de sécurité, etc.). |
|  | Le Titulaire propose les 10 indicateurs les plus structurants permettant d’évaluer la qualité des prestations. La Cnam décide au final des indicateurs à retenir (parmi ceux proposés par le Titulaire et/ou d’autres) ? |

# Définition des besoins

## Exigences fonctionnelles

### Reprise de l’existant

| Fonctionnalités | Description générale |
| --- | --- |
| Reprise et maintien de l’existant | Reprise de tous les éléments et fonctionnalités de MES et du DMP |
| Continuité de service | S’assurer de la continuité de service durant toute la durée de l’accord-cadre (y compris phase d’initialisation/réversibilité). |

### Identification/Enrôlement

| Fonctionnalités | Description générale |
| --- | --- |
| Identité de l’usager | Pour l’enrôlement, le service doit s’interfacer avec les services de la sécurité sociale afin de valider l’identité de l’usager ou de l’ouvrant droit avant l’activation de MES. |

### Gestion des comptes

| Fonctionnalités | Description générale |
| --- | --- |
| Gestion du cycle de vie | Le système de Métier doit gérer le cycle de vie de MES, ressources et compte MES en faisant évoluer les changements d’états des éléments constituant son MES (décisions du titulaire de MES ou changements induits par d’autres acteurs autorisés). |

### Gestion des notifications

| Fonctionnalités | Description générale |
| --- | --- |
| Notifications par SMS | Le système de gestion des notifications pour le titulaire du compte MES doit acheminer les SMS auprès de tous les opérateurs téléphoniques (physiques ou virtuels) exerçant en France (Métropole et DROM). |
| Changement d’opérateur SMS | Le système de gestion des notifications pour le titulaire du compte MES doit pouvoir s’adapter au changement d’opérateur en charge d’expédier les SMS vers les usagers ou les PS. |
| Gestion des préférences de notification | Le système doit enregistrer les choix de configuration du profil par le titulaire du compte MES.  Il doit gérer les préférences de communication (choix du canal de notification /OTP) en fonction des services et des usages et potentiellement interrogeable par les services transverses du socle technique |
| Pilotage du débit | Le système doit disposer des moyens de piloter le « débit » des notifications vers les usagers (pour des questions de coût ou pour éviter de surcharger l’usager en notifications). |
| Etat de l’art | Respecter l’état de l’art sur les notifications (SMS, push mobile, courriel, courrier, voire autre dispositif). |

### Consentement pour échanges de données avec MES

| Fonctionnalités | Description générale |
| --- | --- |
| Gestion du consentement | Le consentement pour l’accès à ses données et leurs utilisations est géré au niveau de MES. |

### Capacité d’interfaçage

| Fonctionnalités | Description générale |
| --- | --- |
| Capacité d’interfaçage | La solution doit être en capacité de s’interfacer avec les services de la sphère sociale avec comme objectif d’assurer une intégration transparente pour les utilisateurs. Il peut être envisagé, en fonction des besoins, différents degrés d’interfaçages :   * Intégration par un appel contextuel * Intégration par abonnement à des évènements émis par la sphère sociale * Intégration par échange en masse |

### Expérience utilisateur, ergonomie et facilité d’utilisation de la solution

La construction de l’expérience utilisateur et l’ergonomie de MES s’appuie sur l’ensemble des principes suivants :

* + Comprendre les attentes et besoins des usagers de MES à travers la mise en place d’enquêtes et d’ateliers citoyens sur le terrain ;
  + Identifier les dernières tendances et usages les plus marquants de la transformation numérique, de manière générale, et du secteur de la e-santé plus particulièrement, à travers la réalisation de benchmarks et de veille des tendances ;
  + Prendre en compte les besoins et usages des acteurs tiers pouvant accéder ou proposer des services au sein de MES (ex. : professionnels, éditeurs/offreurs de services) en interrogeant les parties prenantes.

La construction de l’univers graphique du produit MES s’appuie sur l’univers de marque défini par la Direction de Communication de la Cnam (DICOM).

Le front office de MES doit pouvoir s’adapter et évoluer au rythme des besoins utilisateurs et aux interactions avec son écosystème. Ces principes s’inscrivent dans une démarche centrée sur l’utilisateur et ont pour objectif d’offrir à l’usager un parcours utilisateur optimal à travers une plateforme adaptée et facile d’utilisation.

Les fonctionnalités du SI MES et leurs mises en œuvre doivent pouvoir s’adapter continuellement aux besoins des usagers de manière à maximiser l’apport de valeur et in fine l’usage de MES. Pour ce faire, le Titulaire met en place des boucles de rétroaction les plus dynamiques et complètes possibles. Ces boucles s’appuient sur des retours d’usages, des analyses d’usages, des enquêtes et des focus groupes.

La conception du Front Office MES doit respecter les exigences suivantes.

| Fonctionnalités | Description générale |
| --- | --- |
| Ergonomie et utilisabilité des interfaces | Assurer une cohérence de la navigation quelles que soient les conditions d’utilisation de MES. L’usager doit profiter d’une expérience utilisateur simple et pertinente au sein de MES. Les transitions d’un support à un autre doivent être logiques, faciles et garantissant l’aboutissement du parcours utilisateur engagé. |
| Fiabilité et performance | En plus de la facilité d’accès et de disponibilité, MES doit être un service performant s’appuyant sur des exigences techniques permettant d’assurer des temps de réponse et de chargement optimaux dans toutes les conditions d’usage. |
| Mise à jour du produit MES (FO et BO) | Les opérations de mise à jour (mise en production applicative) ainsi que les maintenances techniques (mise à jour des socles techniques de la plateforme) doivent être transparentes pour l’usager. |
| Responsivité des interfaces | Ce critère est indispensable car il permet à l’ensemble des usagers adressés par MES de profiter d’une expérience utilisateur de qualité quel que soit le support utilisé (desktop, smartphone, tablette, etc.) |
| Universalité du service | L’expérience utilisateur s’appuie sur les principes dictés dans le RGAA 4 afin de faciliter la lisibilité à l’ensemble des usagers et ainsi de permettre l’accessibilité au grand public.  L’audit du 31 janvier 2023 indique que MES respecte à 75% les critères du RGAA 4.1. Il est nécessaire de s’assure que le respect de ces critères ne soit pas réduit. |
| Eco-responsabilité | MES s’inscrit dans une démarche d’éco-responsabilité. Son Eco-Score est de 74. Le projet doit s’inscrire dans cette démarche et faire en sorte de maintenir ou d’améliorer ce score en réutilisant les parcours utilisés. |

### Facilité d’intégration de briques supplémentaires

| Fonctionnalités | Description générale |
| --- | --- |
| Modularité | Le Titulaire s’engage à mettre en place une architecture et une organisation des développements logiciels permettant :   * Une facilité d’intégration de briques supplémentaires * Une facilité de modification et déploiement en production d’évolution ciblée sur un délai cours en parallèle des versions évolutives structurantes en cours.   Le dispositif de prise en compte de cette exigence par le Titulaire est décrit dans son offre et reprise dans le PAQ. |

### SI PILotage

| Fonctionnalités | Description générale |
| --- | --- |
| Outil de pilotage | Disposer d’un outil de pilotage (pour MES ou suite à la convergence MESDMP) qui permette de disposer d’indicateurs de pilotage avec un nombre d’actions manuelles limité nécessaires pour les obtenir.  Pouvoir interfacer cet outil avec des sources de données externes (ex. : ATInternet) en limitant là encore les actions manuelles nécessaires. |
| Automatisation de la gestion des comptes | Mettre en oeuvre l’automatisation de la gestion des comptes utilisateurs au moins pour les demandes de modifications de mot de passe et des demandes de créations et de suppressions de comptes utilisateurs. |

### Audit et statistiques

| Fonctionnalités | Description générale |
| --- | --- |
| Mesure des audiences | Les mesures d’audiences doivent couvrir l’application Web et l’application Mobile.  L’ensemble des pages du site Web et de l’application Mobile doivent faire l’objet de mesures d’audience.  Les indicateurs classiques de mesures d’audience sont attendus:   * + - Audience : Visiteurs, Nb de visite, Temps moyen passé sur le site, pic d’activité, etc.     - Pages : Nombre de pages vues, Nombre de visiteurs par page (top 5), temps moyen par page, pages d’entrées, pages de sortie, etc.     - Suivi des Clics : boutons, liens, etc.     - Navigation : l’outil doit permettre le suivi de parcours utilisateur prédéfini. Ex : connexion, ajout d’un document, etc.     - Cette liste n’est pas exhaustive et sera complétée lors de la parution du CCTP définitif. |
| Evolutivité des Indicateurs des d’usages | Le système de remontée d’indicateurs d’usage doit pouvoir s’adapter au moment du déploiement de nouvelles fonctionnalités.  Cela implique la création de nouveaux indicateurs ainsi que l’évolution des anciens indicateurs (création de croisement, recoupement) |

## Exigences d’Architecture et d’Exploitation

### Exigences d’Architecture Applicative

Les exigences générales d’architecture qui s’appliquent à l’existant et doivent être respectées tout au long de l’accord-cadre sont définies ci-après.

NB : Dans la description des exigences, le terme « Système » représente l’ensemble du patrimoine applicatif concerné par le présent CCTP (Mon Espace Santé + le SI DMP + les évolutions à venir), également appelé MESDMP (Mon Espace Santé – Dossier Médical Partagé)

| Exigences | Description générale |
| --- | --- |
| Patterns d’Architecture | La conception et l'architecture applicative du Système doit être modulaire et faciliter l'évolutivité de la solution. Les principes de séparation des responsabilités, d'architecture résiliente aux défauts, d'encapsulation, d'interopérabilité, et de testabilité doivent être appliqués pour les différents éléments constituant la solution.  Parmi les mises en œuvre, on retrouve notamment :   * Découplage Front / Back (usage d’un BFF) * Usage d’une médiation systématique (API Management, etc.) * µS dès que cela est possible (modularité, autonomie, etc.) * Utilisation préférentielle de l’évènementiel / fil de l’eau (Broker de messages, etc.) dès que ce pattern est adapté au besoin * Possibilité d’orchestration du parcours d’un usager « de bout en bout » * Les Traitements de masse périodiques, à l’échelle de l’intégralité du système et de ses 70 milions d’ENS, doivent être possibles dans des délais raisonnables (< 1 mois). |
| Continuité de service | Assurer la continuité de service vis-à-vis des clients actuels (LPS et Usagers) du Système et sa rétrocompatibilité (= sans impact sur ses clients) durant tout le temps de sa convergence vers la cible à 3 ans |
| SLA | Le Système doit veiller à apporter :   * Scalabilité : le Système doit être conçu de manière à ce que l’augmentation des moyens de traitement (préférentiellement la capacité « horizontale » par multiplication des instances, couplée si nécessaire à une augmentation « verticale » des caractéristiques des instances) permette de répondre aux sollicitations actuelles et futures. * Elasticité : le Système doit être conçu de manière à ce que, sans intervention manuelle ou quelconque modification d’architecture, il soit en capacité de traiter une augmentation d’usage de 5 à 10 fois la moyenne prévue. * Résilience : Le Système doit être implémenté de manière à ce que les conséquences des erreurs d’exécution soient circonscrites au strict périmètre de la fonctionnalité concernée, sans autre impact sur le service rendu par le reste du Système. * Performance : <voir Exigences du § 6.2.5> * Disponibilité : <voir Exigences du §6.2.3> * Robustesse : <voir Exigences du §6.2.6> |
| Traçabilité / Auditabilité | Le Système doit offrir un ou des dispositifs garantissant la consignation et la rétention -sur la durée ad hoc- des éléments de trace permettant de mener des investigations a postériori à des fins de diagnostics fonctionnels, techniques ou sécuritaires.  NB : cette exigence, comme toutes les autres, s’applique dans le respect strict des exigences de Sécurité et de respect du RGPD |
| Open Source / Standards | Dès que cela est possible, et en accord avec la Cnam, le Système doit mettre en œuvre des solutions à base de logiciels et de technologies OpenSource et respectant des standards publics établis.  De manière générale, il est également demandé de minimiser le nombre de technologies utilisées pour les développements (en gardant leur utilisation légitime, sans détournement). |
| Chiffrement/  Confidentialité des données | Le Système doit garantir la confidentatialité des données sensibles qu’il manipule et mettre en oeuvre toute mesure nécessaire pour en rendre l’accès non autorisé impossible.  Parmi ces mesures exigibles, on trouve celle du chiffrement de toutes les données sensibles par nature ou dont l’usage combiné avec d’autres données peut mettre la confidentialité d’informations personnelles en péril.  NB : cette exigence est une reformulation d’une partie du corpus d’exigences concernant la Sécurité. Voir le § 6.3.2pour plus de détails. |
| Authentification | Le Système doit permettre l’authentification renforcée (au moins 2FA) de ses usagers (Grand public ou Professionnels utilisateurs du Système).  NB : cette exigence est une reformulation d’une partie du corpus d’exigences concernant la Sécurité. Voir le § 6.3.2 pour plus de détails. |
| Conformité RGPD | Le Système doit garantir le respect du RGPD pour l’ensemble de ses usagers |
| Accessibilité | Le Système doit être conçu de manière à ce que l’accessibilité soit garantie avec le maintien d’un RGAA  >75% |
| Accès Multicanaux | Le Système doit être conçu de manière à ce qu’il soit utilisable via différents dispositifs.  Pour les usagers (selon les exigences de la Cnam) :   * Version Web (responsive) * Version mobile (IOS / Androïd, etc.)   Pour les écosystèmes tiers :   * Expositions d’API |
| Pilotage métier | Le Système doit disposer d’une solution autonome et configurable permettant la production d’indicateurs statistiques clés pour effectuer le pilotage par le Métier (Système Décisionnel / BI). |
| Archivage | Le Système doit disposer d’une solution de conservation des données sur la période légale dans les conditions de preuves exigibles. |
| Gestion de l’obsolescence | Le Système doit toujours être maintenu « à jour » sur l’ensemble de ses technologies et produits utilisés.  De façon similaire, les éventuelles dettes architecturales consignées (induites, ponctuellement et transitoirement par des exigences opérationnelles) doivent être résorbées dans un délai inférieur à 3 versions majeures. |
| Interopérabilité avec Sphère Sociale | Le Système doit être capable d’interagir avec la Sphère Sociale (partenaires parmi ceux référencés dans les § Interfaces externes de MES et Interfaces externes du DMP), notamment en mettant en œuvre le protocole InterOPS, aussi bien pour les appels de services que pour les accès par des agents de la Sphère sociale aux IHM les concernant (Assurance Maladie requise, autres à étudier selon besoins). |
| Sécurité | Cf. section dédiée 6.3.2 Exigences de sécurité |
| Documentation d’Architecture applicative | L’ensemble des documents d’architecture doit être maintenu à jour et publié régulièrement (a minima pour chaque release).  Parmi les documents (liste non exhaustive) exigés :   * Dossier d’architecture Applicative et logicielle (comportant, pour chaque composants applicatifs mentionné, ces fonctionalités principales) * Dossier d’architecture Technique (environnements de Run + Infrastructure + Topologie réseau…)   Il est impératif qu’un dispositif permette une navigation simple entre ces 2 documents afin de répondre rapidement à des questions du type :   * Sur quel environnement d’exécution tourne un composant donné * Quels sont les composants qui partagent un environnement de run (middleware, ressources mémoire ou matérielles) donné.   NB : Idéalement, ces documentations doivent pouvoir être générées à partir d’un outil de gestion de Référentiel d’Architecture |
| Frugalité et éco-responsabilité | Le critères de frugalité énergétique et de l’éco-responsabilité doit être pris en compte dans le design de l’architecture du Système en accord avec les enventuels arbitrages métier que cela nécessite. |
| Supervision et métrologie | L’observabilité du Système doit être garantie afin de pouvoir accomplir les activités de Supervision/alerting et de métrologie (compléments : voir le 6.2.7 Exigences de Supervision et métrologie) |
| API d’Accès ressources partagées | Les ressources sont partagées entre les écosystèmes Mon *Espace Santé (MES)* et *Bouquet de Service aux Professionnels (BSP)*. Aucune de ces ressources n’est accessible directement par les applications clientes. MES (comme le BSP) doit donc exposer une couche d’interface rendant l’accès à ces ressources possible. | |
| Prise en compte du CI-SIS | Le Cadre d’Interopérabilité des Systèmes d’Informations de Santé (CI-SIS) doit être appliqué aux composants du Système implémentant l’intéropérabilité à chaque fois qu’un des volets du CI-SIS est légitimement applicable au contexte d’usage de la fonctionalité considérée. | |
| Usage de la Médiation | Pour chaque communication entre composants applicatifs du Système, l’usage d’un dispositif de médiation doit être privilégié.  Parmi les finalités recherchées (*NB : applicables selon les types de communication et la nature des composants communicants)*:   * Facilite le 1er niveau de découplage entre producteur et consommateur. * Facilite l’interopérabilité protocolaire entre producteur et consommateur (« middleware ») * Autorise des adaptations applicatives pour minimiser les impacts de montée de version des fournisseurs de données (ceux qui exposent les APIs) * Autorise des paramétrages de SLA externalisés des implémentations des producteurs et/ou consommateurs (Régulation de la qualité de service) * Garantit un 1er niveau de sécurité et le rejet des appels issus des composants applicatifs non autorisés en liaison avec le socle technique de sécurité. * Facilite les opérations de maintenance en gérant l’indisponibilité potentielle des fournisseurs de service (donne l’information aux clients « consommateurs » de MES) * Garantit que l’intégralité des sollicitations qu’il reçoit (Evènement des ressources, Appels) fait l’objet d’un traitement (nominal, exception, erreur, etc.) * Assure le 1er niveau de traçabilité (niveau technique a minima) et d’alimentation des indicateurs de fréquentation | |
| Cohérence fonctionnelle des API | La dénomination des objets et champ en entrée / sortie de l’API doit être cohérente et homogène d’une API à l’autre | |
| Gestion des erreurs | Le retour de l’API doit permettre de faire la différence entre une réelle erreur technique du serveur d’API, une donnée manquante en entrée de l’appel (requête non conforme) ou encore une erreur levée par un service de plus bas niveau | |
| Traçabilité des appels | Pour chaque appel aux API les traces qui doivent être générées doivent permettre a minima d’établir un diagnostic | |
| Traçabilité des appels | Pour chaque appel aux API, une trace doit être générée comprenant a minima les informations suivantes :   * + Client appelant   + Opération appelée (path / verbe HTTP)   + Date / heure d’appel   + Temps de réponse   + Code retour http et éventuel code retour métier   + Nombre d’éléments retournés   NB : les exigences de sécurité/chiffrement, confidentialité, conformité RGPD, etc. s’appliquent à cette exigence comme à toutes les autres. | |
| Documentation des API | La publication des API du BO doit être outillée, documentée et organisée via des revues régulières. Ceci concerne aussi bien les demandes de création de nouvelles API que les évolutions d’API existantes.  Le BO doit proposer un dispositif et une documentation d’accompagnement à 2 niveaux :   1. Fonctionnel, à destination du représentant fonctionnel du service FO (PO, MOA) ou de manière plus générale, des équipes de réalisation du client pour :    * Introduire l’API et ses capacités    * Expliciter les liens entre le besoin fonctionnel du client et les fonctionnalités exposées par l’API   Ce premier niveau doit permettre une compréhension mutuelle maximale entre le client FO et le fournisseur BO   1. Technique, à destination des équipes de réalisation du service FO, pour :    * S’approprier techniquement le service    * Amorcer les séquences d’appels REST à effectuer pour couvrir les principaux cas d’utilisation client    * Faciliter les tests, du développement à la recette fonctionnelle   Ce second niveau permet de simplifier la mise en œuvre et d’éviter les confusions et usages non pertinents / inefficaces de l’API. | |
| Rétrocompatibilité et version d’API | Dans le cas d’une évolution d’API existante, la rétrocompatibilité doit être garantie pour tous les clients consommateurs de l’API.   * Une rupture de compatibilité est une décision exclusivement à la main de la Cnam. * Le Système doit permettre d’avoir plusieurs versions d’une même API en production en même temps et doit fournir les moyens de gérer le taux de bascule progressif des clients d’une version vers une autre dans le cas de versions d’API retro-compatibles. | |
| Données froides | Le Système doit disposer d’une solution de stockage de « données froides » permettant la rétention sur une longue période d’une grande quantité de données à moindre coût (au prix d’un accès non immédiat pour l’utilisateur final). | |

### Exigences d’Architecture Technique

Les exigences générales d’architecture technique qui s’appliquent à l’existant et doivent être respectées tout au long de l’accord-cadre sont définies ci-après.

#### ART1 – Interconnexion avec la Cnam et les autres partenaires

L’Assurance Maladie dispose de 2 datacenters de production informatique : le CSH SUD à Toulouse et le CSH GE à Strasbourg. Ces 2 centres sont chacun équipés d’accès redondants et sécurisés à Internet.

L’interconnexion, entre les différents partenaires, dont la Cnam et le Titulaire, dont il est question dans ce paragraphe sert essentiellement :

* + A fournir les services applicatifs via l’interconnexion avec les SI des partenaires (échanges de fichiers, de messages Transactionnels et au fil de l’eau en mode synchrones et asynchrones, accès à des IHM hébergées par le Titulaire (Support, etc.) et proposées aux agents des partenaires) tant pour les environnements Production que Hors Production.
  + A l’accès aux environnements hors production dès que nécessaire (représentativité nécessaire pour les tests de bout en bout).
  + Au partage des outils nécessaires à la gestion des incidents, des problèmes, des anomalies et au partage des états des services de MESDMP.
  + A l’accès aux environnements collaboratifs pour partage des documents contractuels.

| Exigences | Description générale |
| --- | --- |
|  | La solution réseau est à la charge du Titulaire. Sont notamment inclus dans sa prestation pendant la durée de l’accord-cadre, sans faire l’objet d’une facturation particulière :   * La mise en place des interconnexions réseaux. * Leur gestion technique conjointe avec les experts de la Cnam et des autres partenaires. * Leurs évolutions. * La résolution des dysfonctionnements éventuels. |
|  | Le Titulaire établit puis maintient, en la mettant à jour lors de toute évolution des services, une matrice exhaustive des flux pendant toute la durée de la prestation.  Afin que la Cnam puisse construire sa politique de filtrage et de NAT au niveau de ses équipements périmétriques, le Titulaire fournit de manière exhaustive l’ensemble des informations (adresses IP, protocoles et ports). Cette matrice est transmise à la Cnam, a minima, lors des Comités de Pilotage. |
|  | Quelle que soit l’organisation du Titulaire concernant sa gestion de la solution réseau d’interconnexion (sous-traitance partielle, totale, aucune, etc.), il met à disposition :   * L’expertise nécessaire au dialogue avec les experts réseau de la Cnam (évolutions, troubleshooting). * Les moyens (techniques, contractuels, etc.) d’intervention rapide en cas de dysfonctionnement ou d’évolution urgente. * Un suivi des interconnexions réseau publiant des indicateurs de reporting opérationnels (sur la nature des flux, la volumétrie des échanges, le nombre d’incidents, etc.). * Un moyen pour partager en temps réel les indicateurs précédents avec les équipes de la Cnam. |
|  | Le Titulaire désigne un contact technique en charge de la réalisation des interconnexions réseaux et du maintien en conditions opérationnelles du service. Les informations permettant l’ouverture et le suivi des incidents et des demandes relatives aux interconnexions réseaux, notamment, sont précisées dans son offre :   * La description du processus de traitement des incidents et des demandes, * La procédure d’ouverture d’un ticket d’incident ou d’une demande et les informations à fournir par la Cnam (n° d’appel, n° client, etc.), * La procédure d’escalade.   Ces informations sont géalement consignées dans le Plan d’Assurance Qualité (PAQ) établi entre la Cnam et le Titulaire. |
|  | Toute intervention sur les équipements se trouvant sous la responsabilité du Titulaire et impactant le service de MESDMP doit faire l’objet de l’envoi d’un avis d’intervention à la Cnam au minimum 15 jours calendaires avant la date de cette intervention. Le Titulaire doit obligatoirement préciser a minima :   * La référence client du ou des sites impactés. * Les dates et horaires de l’intervention. * La raison de l’intervention.   Dans la mesure du possible, la Cnam demande que ces interventions soient effectuées entre 22h et 6h.  Cette règle s’applique pour toute intervention, qu’elle soit à l’initiative du Titulaire ou qu’elle fasse suite à une demande d’évolution ou de modification de la Cnam. Dans ce dernier cas, les opérations programmées en Heure Non Ouvrée (HNO) ne fent pas l’objet d’une facturation supplémentaire. |
|  | Le Titulaire est en capacité de reproduire et faire évoluer en respectant l’état de l’art les dispositifs d’interconnexion mis en place (liaison point-à-point, VPN IPSec, VPN SSL, MPLS, etc.) avec la Cnam et les différents partenaires existants.  Ceci en adéquation avec les engagements de services requis dans le cadre du présent CCTP, notamment concernant :   * Les taux de disponibilité mensuel et annuel des services. * Le nombre maximum d’indisponibilités quotidien, hebdomadaire, mensuel et annuel. * La garantie de temps de rétablissement. * Les temps de réponse. |
|  | Le Titulaire doit mettre en place un processus de translation d’adresses NAT pour toutes les applications proposées par le Titulaire accessibles depuis la Cnam ou les autres partenaires. |
|  | Le Titulaire démontre dans son offre sa capacité à interagir avec :   * Un nombre de partenaires important. * Des solutions adaptées aux besoins. * Des délais de mise en service maitrisés. |
|  | Le Titulaire précise dans son offre s’il s’appuie sur ses services propres ou sur ceux d’un fournisseur tiers. |

#### ART2 – Interfaçage avec la Cnam et les autres partenaires

|  |  |
| --- | --- |
| Exigences | Description générale |
| Echanges de fichiers | Les échanges de ce type du Titulaire doivent s’inscrire dans le cadre de la solution prévue à la Cnam, basée sur le principe d’un SAS de dépôt et de réception :   * Mode Asynchrone. * Protocoles : Pesit SSL ou SFTP en mode certificat (pas de user/password). * Les tailles limites standard des fichiers sont de PESIT/500Mo, SFTP/200Mo ; la volumétrie quotidienne est limitée à 2Go/24h. * Le système du Titulaire vient déposer ou récupérer les flux fichiers auprès du système de la Cnam. |
| Services Web SOAP | Le Titulaire étant client ou fournisseur selon le cas d’usage doit être en conformité avec InterOps-A. |
| Services Web REST | Le Titulaire étant client ou fournisseur selon le cas d’usage doit être en conformité avec InterOps-R. |
| Web SSO inter-portails | Le Titulaire étant client ou fournisseur selon le cas d’usage doit être en conformité avec InterOps-P. |
| Services d’éditique de la Cnam | Les échanges avec le système d’éditique de la Cnam doivent s’inscrire dans le cadre de la solution prévue à la Cnam:   * Dépôt de fichiers dans le SAS Cnav destiné à cet usage. * Dans un format AFP à destination des systèmes d’impression industriels. |

#### ART3 – Documentation de Conception d’Architecture Technique

|  |  |
| --- | --- |
| Exigences | Description générale |
|  | HLD de l’infrastructure et de ses services transverses : donne une description macroscopique de l’architecture du système (zones, stockage, compute, sauvegarde, éléments de sécurité, réplications, services transverses, etc.).  LLD des composants et des services de l’infrastructure ainsi que des middleware : détaille les choix d’architecture et fonctionnement retenus notamment pour en assurer les disponibilité, duplication, sauvegarde, etc.  Ces documents sont fournis par le Titulaire et maintenus à jour par le Titulaire. |

#### ART4 – Description de la solution du Titulaire

|  |  |
| --- | --- |
| Exigences | Description générale |
|  | Architecture technique adoptée par le Titulaire :  Le Titulaire expose l’architecture technique (matérielle, virtualisation, conteneurisation, middleware, etc.) mise en œuvre dans sa solution.  Il précise en quoi les choix faits sont compatibles avec un transfert de l’infrastructure et de ses services lors d’une réversibilité chez un autre hébergeur, SecNumCloud notamment. |
|  | Architecture technique adoptée par le Titulaire pour garantir la haute disponibilité nécessaire aux SLA exprimés (jusqu’à 99,9% 24/7) :  Le Titulaire expose l’ensemble des solutions qu’il met en œuvre (multi-salles, dual-sites, continuité réseau, multi-opérateurs réseau, peering, débits, virtualisation, cluster étendus, réplication, etc.) pour atteindre le niveau de continuité de service nécessaire à l’hébergement du SI de l’ENS. |
|  | Architecture technique adoptée par le Titulaire pour le PRA :  Le Titulaire expose l’ensemble des solutions qu’il met en œuvre (site, réseau, réplication, sauvegarde, externalisation, etc.) pour se préparer à un éventuel Plan de Reprise d’Activité du SI de l’ENS. |

### Exigences de Disponibilité

#### Définitions applicables

| Exigences | Description générale |
| --- | --- |
|  | La disponibilité est la capacité des services à remplir leurs fonctions sur une plage déterminée. Cet indicateur met en évidence les nombres d’heures d’interruption mensuelle hors créneau de maintenance planifiée.  Une fonction est considérée comme indisponible lorsque l'usage du service est impossible du fait du défaut de fonctionnement d'une fourniture ou d'un service sous la responsabilité du Titulaire ou lorsque les temps de réponse dépassent les temps de réponse acceptables (cf. §6.2.5 Exigences de Performance).  Sont inclus dans les indisponibilités constatées sur la période considérée :   * Les indisponibilités des fonctions critiques d’un système, qui sont comptabilisées avec un coefficient de 100 % ; * Les fonctions critiques pour le SI MESDMP sont notamment :   + Connexion à l’ENS,   + Accès à la page d’accueil,   + Accès au profil médical,   + Accès aux documents et les API liées,   + Accès à la messagerie,   + Agenda,   + L’outil de support,   + L’outil de supervision,   + Mobile,   + Store et API liées,   + Enrôlement,   + Portail éditeur (comprend le PACS). * Les indisponibilités liées a des changements en production qui n’ont pas fait l’objet de dérogation auprès de la Cnam   La liste des fonctions critiques est consignée dans le Plan d’Assurance Qualité (PAQ) établi entre la Cnam et le Titulaire. Elle est tenue à jour dans le PAQ et revue semestriellement en Comité de suivi contractuel et financier  Le taux de disponibilité se définit comme le pourcentage de temps où le service est opérationnel. Il est calculé chaque mois de la manière suivante : (Temps total de la période - Temps d’indisponibilité) / Temps total de la période  Le début de l’indisponibilité est le début effectif de l’arrêt, remonté via une alerte des sondes à la console de supervision, ou à défaut selon le relevé dans les fichiers des traces techniques du service. La fin de l’indisponibilité est la fin effective de l’incident, et donc le retour à une situation nominale pour les utilisateurs, constatée par les sondes applicatives (ou mécanisme équivalent) et communiquée par le Titulaire à la Cnam. |
|  | Les services du Titulaire doivent donc être en mesure de supporter toutes les pointes de charge dues à des événements particuliers (Campagne de communication, Opération spéciales, etc.) sans aucune dégradation des temps d’accès. La technologie employée par le Titulaire doit permettre une scalabilité et faciliter l’augmentation des capacités et des performances. |
|  | Les paragraphes sur la disponibilité s’appliquent sur le territoire métropolitain et sur les DROM. |

#### DIS1 - Commun à tous les Environnements

| Exigences | Description générale |
| --- | --- |
|  | Le Titulaire s’engage à mettre en place la mesure de la disponibilité de l’ensemble des environnements (incluant les aspects réseaux) au travers de mécanismes spécifiques prévus à cet effet (sondes applicatives ou tout autre dispositif équivalent), qui simulent des utilisateurs fictifs et mesurent périodiquement l’accès aux différents services, selon la période définie dans le Plan d’Assurance Qualité. |
|  | Les sondes ou autres mécanismes de mesure de disponibilité proposé(e)s par le Titulaire doivent respecter les exigences fonctionnelles de sécurité pour les systèmes en production, et ne doivent pas générer des traces fonctionnelles ni être comptabilisées dans la volumétrie d’activité. |
|  | Les sondes de disponibilité ou mécanismes équivalents doivent être implémentés pour tous les environnements accessibles par la Cnam, et la population auxquels ils sont destinés (Professionnels de Santé, Organismes, assurés adhérents, etc.).  La Cnam doit acceder en temps réél aux mesures issues de ces sondes. |
|  | Les indicateurs de disponibilité sont calculés et publiés tout au long de la journée pour une vérification régulière, en complément des dispositifs de supervision déjà établis. Ces indicateurs doivent être consolidés par le Titulaire et mis à disposition de la Cnam de façon hebdomadaire et mensuelle, afin de vérifier le respect des objectifs de disponibilité.  En cas de non-respect des exigences calculées mensuellement, la Cnam peut appliquer les pénalités définies au CCAP. |
|  | Une alerte vers le service de supervision du Titulaire doit être générée quand les sondes ou autres mécanismes de mesure équivalents détectent une indisponibilité de tout ou partie des services. |
|  | La Cnam doit reçevoir une communication immédiate pour toute indisponibilité totale ou partielle constatée du ou des services au début et à la fin de l’incident (Mail, SMS, Bandeau déroulant sur outils, et ouverture d’un ticket dans l’outil de ticketing Cnam pour suivi, etc.).  Dans ce cas, le Titulaire doit entrer dans le processus de gestion d’incident tel que défini dans le PAQ. |
|  | Les utilisateurs du système doivent être informés des indisponibilités programmées et constatées par un message approprié, dont le contenu doit être validé par la Cnam avant envoi :   * Pour une indisponibilité programmée, le délai minimal de prévenance exigé est de 15 jours calendaires avant l’interruption programmée ; * Pour une indisponibilité de tout ou partie des services, la Cnam doit être prévenue dans un délai de 15min suivant le début d’interruption.   Conformément aux exigences de Maintenabilité exprimées au *§6.3.3 Exigences de Maintenabilité Opérationnelle*, toute indisponibilité, programmée ou non, est décomptée, dès lors qu’elle survient durant une plage de service.  Si ces niveaux d’exigence ne sont pas atteints, la Cnam peut appliquer les pénalités définies au CCAP. |
|  | Le Titulaire met à disposition de la Cnam les indicateurs reflétant l’état de disponibilité des services, des performances et le volume d’activité en temps réel. Ces indicateurs doivent permettre d’apprécier l’état des services du point de vue utilisateur final à tout moment.  Si ces niveaux d’exigence ne sont pas atteints ou si ces indicateurs ne sont pas mis à disposition, la Cnam peut appliquer les pénalités définies au CCAP. |
|  | Tous dysfonctionnements détectés par les mécanismes de suivi de la disponibilité déclenchent automatiquement le processus de gestion des incidents (détaillé dans le Plan d’Assurance Qualité). |
|  | Le Titulaire doit se munir à ses frais des outils adéquats et nécessaires pour mener à bien ses missions. La Cnam visant à consommer l’offre d’hébergement (si la PSE visée au §7.4 La durée et le point de départ des prestations seront précisés dans le CCTP final.  P2 - PSE – Hébergement est retenue) et d’Exploitation sous forme de services, celle-ci ne peut pas se voir facturer l’acquisition de quelconques licences produits ou logiciels autour des activités de suivi de la disponibilité. |
|  | Afin de faciliter toute action de Réversibilité auprès de la Cnam ou de tout autre repreneur, le Titulaire s’engage à s’appuyer tout au long de la prestation sur des outils et matériels standard, à jour, et maintenus, dans le cadre des activités citées ci-dessus et relatives aux environnements et services hébergés. |

#### DIS2 - Environnement Production

| Exigences | Description générale |
| --- | --- |
|  | |  |  | | --- | --- | | Disponibilité | A titre indicatif la durée maximale cumulée d'indisponibilité par mois correspond à : | | 99,9%, 24h sur 7j/7 | 43 minutes 12 secondes |   En cas d’indisponibilité/d’échec de la solution, la solution doit disposer d’un mécanisme de reprise permettant à l’utilisateur de reprendre son activité de la manière la plus transparente et automatisée possible lors du redémarrage des services :   * Sans perte de travail ; * Avec une protection des données ; * Avec une notification de l’échec / de l’indisponibilité. |
|  | Une cellule de crise opérationnelle doit être mise en place pour toute indisponibilité de la production dont la résolution est estimée supérieure à 1 heure. |
|  | Les changements applicatifs doivent être effectués sans interruption de service (redondance), ou dans l’impossibilité, font l’objet d’une dérogation pour une plage définie auprès de la Cnam. |
|  | Afin d'assurer la haute disponibilité exigée de la production, le Titulaire s'engage à mettre en oeuvre un dispositif applicatif actif/actif sur les deux datacenters distants. |

#### DIS3 - Environnements Certification éditeur

| Exigences | Description générale |
| --- | --- |
|  | |  |  | | --- | --- | | Disponibilité | A titre indicatif la durée maximale cumulée d'indisponibilité par mois correspond à : | | 99,8%, 4h-22h sur 7j/7 | 1 heure |   En cas d’indisponibilité/d’échec de la solution, la solution doit disposer d’un mécanisme de reprise permettant à l’utilisateur de reprendre son activité de la manière la plus transparente et automatisée possible lors du redémarrage des services :   * Sans perte de travail ; * Avec une protection des données ; * Avec une notification de l’échec / de l’indisponibilité. |

#### DIS4 - Environnements Pré-Production

| Exigences | Description générale |
| --- | --- |
|  | |  |  | | --- | --- | | Disponibilité | A titre indicatif la durée maximale cumulée d'indisponibilité par mois correspond à : | | 99.5% 8h-20h sur 5j/7 Jours ouvrés | 1 heures 12 minutes |   En cas d’indisponibilité/d’échec de la solution, la solution doit disposer d’un mécanisme de reprise permettant à l’utilisateur de reprendre son activité de la manière la plus transparente et automatisée possible lors du redémarrage des services :   * Sans perte de travail ; * Avec une protection des données ; * Avec une notification de l’échec / de l’indisponibilité. |
|  | Sur Demande de la Cnam, le Titulaire s’engage à rafraichir l’environnement à une date et pour un jeu de données identifié, dans un délai de 2 jours ouvrés. |
|  | Les environnements de pré-production doivent couvrir l'ensemble du périmètre de la production et séparés de la production. |

#### DIS5 - Autres Environnements

| Exigences | Description générale |
| --- | --- |
|  | |  |  | | --- | --- | | Disponibilité | A titre indicatif la durée maximale cumulée d'indisponibilité par mois correspond à : | | 99.5% 8h-20h sur 5j/7 Jours ouvrés | 1 heures 12 minutes | |
|  | Sur Demande de la Cnam, le Titulaire s’engage à rafraichir l’environnement à une date et pour un jeu de données identifié, dans un délai de 2 jours ouvrés. |

#### DIS6 – FO MESDMP

| Exigences | Description générale |
| --- | --- |
|  | L’infrastructure DevSecOps proposée doit disposer d’un mécanisme de reprise permettant à l’utilisateur de reprendre son activité de la manière la plus transparente et automatisée possible lors du redémarrage des services :   * Sans perte de travail ; * Avec une protection des données ; * Avec une notification de l’échec / de l’indisponibilité.   En cas d’indisponibilité du réseau, le FO MESDMP embarque des mécanismes permettant à l’usager de poursuivre a minima les principales actions.   |  |  |  |  | | --- | --- | --- | --- | | Environnements | Disponibilité | Durée max d’indisponibilité par interruption | Durée maximale cumulée d’indisponibilité par mois | | Production | 99,8 %, 24x7 | 43 minutes | 1 heure 30 | | Environnements hors prod : développement, recette, bench, etc. | 97,7 %, 8h-20h, jours ouvrés | 2 heures | 6 heures |   La définition de ces cibles de disponibilité constitue un des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations. afin de mettre en place les métriques en regard des exigences pour les utilisateurs et de l’analyse de risque d’une perte de disponibilité. |
|  | Une cellule de crise opérationnelle doit être mise en place pour toute indisponibilité de la production dont la résolution est estimée supérieure à 1 heure. |

### Exigences de Volumétrie

Les volumétries des flux sont décrites dans le paragraphe 3.5.5 Métriques de MESDMP.

| Exigences | Description générale |
| --- | --- |
|  | La solution doit être capable de porter les flux synchrones et asynchrones existants et futurs |
|  | Le Titulaire doit être capable de gérer et de prendre en charge les accès en provenance de tous les utilisateurs dotés des moyens nécessaires. |
|  | Quel que soit le niveau d’activité réelle constatée, le Titulaire s’engage à maintenir une capacité d’hébergement suffisante pour le bon fonctionnement de la solution (cf paragraphe 0 La durée et le point de départ des prestations seront précisés dans le CCTP final.  P2 - PSE – Hébergement. |
|  | Sur la base des métriques fournies au paragraphe 3.5.5 Métriques de MESDMP, le Titulaire propose une projection technique sur le dimensionnement de l’infrastructure, par composant, selon la montée en charge par année. |
|  | L’architecture proposée et les dispositifs la constituant doivent être suffisamment scalables et réactifs pour soutenir d’éventuels pics d’activité (à hauteur de 10 fois l’activité moyenne), quelles qu’en soient les origines : Augmentation de fréquentation, augmentation d’usage, traitements de masse, extension de fonctionnalités, etc. |
|  | L’architecture proposée doit permettre un passage à l’échelle de la population nationale de la France soit plus de 60 millions d’utilisateurs sur l’ensemble des éléments qui constituent le MSEDMP et ses ressources. La Cnam souhaite attirer particulièrement l’attention du Titulaire sur la ressource Espace d’échange de messagerie au regard de cette exigence de scalabilité. |

### Exigences de Performance

| Exigences | Description générale |
| --- | --- |
|  | La solution doit être scalable, c'est-à-dire avoir la capacité à s’adapter à un changement d’ordre de grandeur de la demande (cf. volumétrie ou nombre d’utilisateurs) et en particulier avoir la capacité à maintenir ses fonctionnalités et ses performances (dont contrat de services en lien avec l’exploitation globale de la solution) en cas de forte demande et sans qu’il soit nécessaire de revoir l’architecture applicative de la solution. |
|  | Le Titulaire doit respecter les temps de réponse suivants :   |  |  | | --- | --- | | Environnement | Temps de réponse pour tous appels à MESDMP | | Production  Certification des éditeurs | Inférieur à 1 seconde dans 95% des cas  3 secondes dans les 5% des autres | | Autres environnements | Inférieur à 3 secondes dans 95% des cas  5 secondes dans les 5% des autres |  |  |  | | --- | --- | | Environnement | Temps de réponse pour tous appels au SI externes au travers du MESDMP | | Production  Certification des éditeurs | Inférieur à 0.25 seconde dans 95% des cas  0.5 seconde dans les 5% des autres | | Autres environnements | Inférieur à 0.5 seconde dans 95% des cas  1 seconde dans les 5% des autres |  |  |  | | --- | --- | | Environnement | Temps de réponse pour tous appels d’API exposées par le MESDMP | | Production  Certification des éditeurs | Inférieur à 0.25 seconde dans 95% des cas  0.5 seconde dans les 5% des autres | | Autres environnements | Inférieur à 0.5 seconde dans 95% des cas  1 seconde dans les 5% des autres.  Dans le cas où cette exigence ne peut être tenue à cause d’une dépendance vers des composants ne faisant pas partie du périmètre de l’accord-cadre et ne sont donc pas de la responsabilité du Titulaire, le temps imputable au Titulaire ne doit pas excéder les temps de réponse mentionnés dans ce tableau |   La mesure des performances doit se faire en continu. La durée de référence pour le calcul de la performance est 15 minutes.  L’ensemble des appels à MESDMP sont pris en compte unitairement pour le calcul des temps de réponse (il ne s’agit pas d’une moyenne).  Dans le cadre d’un scénario fonctionnel où MESDMP fait appel à un SI tiers, une répartition du temps de réponse entre MESDMP et les différents SI appelés doit être définie par la Cnam. |
|  | La solution doit être en mesure de traiter 100% de l’activité flux d’une journée sur une durée de 4h pour prendre en compte les pics de charge.  Le non-respect du traitement de l’activité de la journée dans les délais peut faire l’objet de pénalités. |
|  | Les traitements synchrone ou asynchrone ne doivent pas être concurrent des services appelés par les utilisateurs. |
|  | Les temps de réponse sont calculés au niveau de l’IHM et comprennent l’ensemble des temps de réponse (réseau, machine, interface) tel que la Cnam le perçoit. |
|  | Les indicateurs de temps de réponse sont calculés quotidiennement avec une granularité du quart d’heure pour une vérification régulière et consultable en temps réél. Ces indicateurs doivent être consolidés par le Titulaire et mis à disposition de la Cnam de façon quotidienne, hebdomadaire et mensuelle, afin de vérifier le respect des objectifs de performance.  En cas de non-respect des exigences calculées mensuellement, la Cnam peut appliquer les pénalités définies au CCAP. |
|  | Le Titulaire a la responsabilité de mener des tests de performances pour s’assurer qu’une nouvelle version répond aux exigences demandées. |
|  | Les tests de performance sont réalisés afin d’extrapoler une volumétrie estimée égale a minima à 30% de la volumétrie de la production cible. |
| Surveillance temps de réponse du SI-ENS | Seuls les environnements Production et Editeurs sont pénalisables au titre de la présente exigence.  La Cnam reçoit une « alerte/communication » en cas de dépassement du temps de réponse de MESDMP pendant une période supérieure à 15 minutes (ce qui correspond à deux mesures consécutives ne respectant pas le temps de réponse demandé) :   * Si le temps de réponse est supérieur ou égal à 10 secondes, ce dépassement implique l’ouverture d’un incident bloquant (côté Titulaire mais également à destination de la Cnam pour information) et déclenche le début d’une plage d’indisponibilité du service, en considérant chaque heure où il y a le dépassement du temps de réponse (cf. CCAP). * Si le temps de réponse dépasse les limites définies en EXG\_PERF\_2 (notamment « Temps de réponse pour tous appels à MESDMP ») et est inférieur à 10 secondes, ce dépassement implique l’ouverture d’un incident grave (côté Titulaire mais également à destination de la Cnam pour information) et déclenche le début d’une plage d’indisponibilité du service, en considérant chaque journée où il y a le dépassement du temps de réponse (cf. CCAP). |
| Surveillance des temps de réponse des SI en aval du SI-ENS | La Cnam reçoit une « alerte/communication » en cas de dépassement du temps de réponse sur l’un des appels de MESDMP pendant une période supérieure à 15 minutes d’un système informatique appelé par MESDMP.  Le Titulaire se fonde sur les temps de réponse des SI appelés communiqués par la Cnam. |
| Mécanisme de Sonde | Un mécanisme de sondes applicatives ou tout autre mécanisme équivalent, mis en œuvre par le Titulaire, doit permettre d’avoir des temps de réponse des services indicatifs afin d’avoir une perception du service avec les mesures en temps réel.  Les temps de réponse se mesurent indépendamment sur chaque fonctionnalité suivant des scénarios fonctionnels définis lors de la conception.  Les mesures opérées doivent garantir un suivi « bout-en-bout » de toutes les fonctionnalités de MESDMP à travers tous les composants, services et équipements situés entre le poste utilisateurs et les serveurs BO du Titulaire (même si certaines briques ne sont pas de sa responsabilité).  Le Titulaire doit mettre en place des métriques de performances se décomposant ainsi :   * Le temps de réponse depuis un poste hors du réseau du Titulaire pour chaque fonctionnalité de MESDMP * Le temps de réponse au sein du SI MESDMP (l’intervalle de temps entre l’entrée du SI MESDMP et la sortie du SI MESDMP moins le temps passé dans un SI appelés par MESDMP) * Le temps de réponse des SI appelés par MESDMP (ex. : SI-Cnam ou partenaires) |
| Mécanisme de Sonde | Pour la prise de mesure des temps de réponse par les sondes ou tout autre mécanisme équivalent, le Titulaire :   * Ne doit pas générer des données pérennes au sein de MESDMP * Ne doit pas impacter l’ensemble des métriques de MESDMP * Ne doit pas impacter les données d’un SI appelé par MESDMP |
| Mécanisme de Sonde | Lors de la phase de construction de chaque évolution de la solution, le Titulaire en lien avec la Cnam doit définir le(s) nouveau(x) scénario(s) fonctionnel(s) ou modifier le(s) scénario(s) fonctionnel(s) existant(s) de prise de temps de réponse. |
| Mécanisme de Sonde | Les sondes de mesure de performances proposées par le Titulaire doivent respecter les exigences fonctionnelles de sécurité pour les systèmes en production, cependant elles ne doivent pas générer des traces fonctionnelles ni être comptabilisées dans la volumétrie d’activité. Les sondes de performance sont destinées à tous les environnements. |

### Exigences de Continuité

#### PCA – Continuité & Redondance

| Exigences | Description générale |
| --- | --- |
|  | Un plan de continuité des services est établi et maintenu par le Titulaire tout au long de l’accord-cadre, pour assurer les disponibilités exigées des différents environnements du service et des interfaces externes associées.  Ce plan répond aux objectifs de disponibilité et d’intégrité demandés par la Cnam en termes de Durée d'Indisponibilité Maximale Admissible (DIMA) et de Perte de Données Maximale Admissible (PDMA). |
|  | En cas de sinistre, et en complément des engagements de Disponibilité de services exprimé, le Titulaire s’engage à assurer une PDMA égale à 0, et une Durée d'Indisponibilité Maximale Admissible DIMA inférieure ou égale à 43 minutes et 12 secondes. |
|  | Le Titulaire assure la mise à disposition des moyens nécessaires en termes de locaux, fourniture et gestion des fluides (climatique, électrique, réseaux, etc.), sécurité (gestion des accès aux sites, aux salles, aux systèmes d’information, etc.) permettant de couvrir les niveaux d’exigences imposés par les Normes, Agréments et Réglementations en vigueur (cf. EXG\_PAQ\_8) (cf. §7.4P2 - PSE – Hébergement) |
|  | Le Titulaire garantit un hébergement a minima certifié Tiers III + ou supérieur, pour tous les éléments de configuration, les solutions et services fournis à la Cnam (cf. §7.4P2 - PSE – Hébergement). |
|  | Le Titulaire assure la mise en œuvre de tous les moyens matériels, logiciels et réseaux nécessaires pour assurer l’atteinte des engagements de services au travers d’une Architecture Adaptée.  Les mécanismes et processus associés sont détaillés dans le Plan d’Assurance Qualité. |
|  | Le Titulaire garantit les mécanismes et Processus assurant la continuité des services nécessaires à son fonctionnement interne (Informatique, Télécom et Humain) en cas de sinistre (supervision, support, administration, etc.) afin de respecter les engagements de services.  Les mécanismes et processus associés sont détaillés dans le Plan d’Assurance Qualité. |
|  | Le Titulaire s’engage à réaliser, a minima 1 fois par an, un test de continuité de service partiel et global de toutes les solutions et services assurés pour le compte de la Cnam.  Ce test fait l’objet d’une planification partagée avec la Cnam afin d’en déterminer la date.  Lors de chaque test, le Titulaire doit démontrer le bon fonctionnement de son plan de continuité par :   * Les résultats des tests et vérifications réalisées * Les traces et logs de bascules * Un compte rendu et un REX associé   À l’occasion du test, la Cnam peut demander à opérer des vérifications de bon fonctionnement à son niveau.  Chaque test doit être matérialisé par la production d’un PV de Validation à la charge du Titulaire. |
|  | Le Titulaire doit garantir la localisation géographique des données appartenant à la Cnam et que l’hébergement de ces données (cf. §7.4P2 - PSE – Hébergement) pour le compte de la Cnam soit conforme à la réglementation en vigueur en fonction de la nature des données stockées (cf. HDS, RGPD, CNIL, etc.). |
|  | La solution du Titulaire doit pouvoir continuer à fonctionner en mode dégradé sur l’ensemble des fonctionnalités intégrées à MESDMP en cas de coupure des interfaces avec le SI Cnam et/ou partenaires, cue ce soit suite à des coupures involontaires ou dans le cas maitrisé d’isolation temporaire des S.I. Le Titulaire doit donc prévoir des interfaces bouchonnées et proposer une gestion de reprise maitrisée des flux après chaque coupure d’interface. |

#### PRA – Sauvegarde et Restauration

| Exigences | Description générale |
| --- | --- |
|  | Le Titulaire doit proposer une solution de PRA avec a minima deux sites géographiques distincts pour l’hébergement de ses infrastructures applicatives, de préférence avec des contraintes physiques et environnementales différentes (cf. §7.4P2 - PSE – Hébergement). En cas de co-localisation dans la même région des datacenters hébergeurs proposés par le Titulaire, une externalisation des sauvegardes couvrant le défaut régional doit être mise en place. Enfin, en cas d’externalisation des sauvegardes sur un 3ème site, sa participation à l’activité 6 « Sauvegardes externalisées des données de santé » de la certification HDS doit être confirmée. Cette solution de PRA doit être validée par la Cnam afin de confirmer son adéquation à couvrir les risques attendus. |
|  | Indépendamment des mécanismes mis en œuvre pour la Continuité des services, le Titulaire doit garantir une sauvegarde périodique des systèmes (cf. §7.4P2 - PSE – Hébergement), des configurations et des données ; et que ces dernières soient stockées Hors Ligne et hors site afin de garantir l’intégrité des données et de prévenir toute altération des données (corruption, effacement, attaque virale, etc.).  Les sauvegardes ainsi produites doivent être stockées de manière sécurisée, leur nombre et leur durée de rétention communiqués à la Cnam.  En cas d’audit, le Titulaire doit être en mesure de fournir les traces et comptes rendus de bonne exécution des Sauvegardes périodiques.  Ces éléments doivent être détaillés dans le Plan d’Assurance Qualité. |
|  | Le Titulaire s’engage à réaliser régulièrement des Tests de restaurations aléatoires visant à confirmer le bon fonctionnement des sauvegardes réalisées. En cas d’audit, le Titulaire doit être en mesure de fournir les traces et PV des tests de Restauration réalisés.  Ces éléments doivent être détaillés dans le Plan d’Assurance Qualité. |
|  | Le Titulaire s’engage à réaliser, a minima 1 fois par an, un Test PRA partiel et Global de toutes les solutions assurées pour le compte de la Cnam.  Ce test fait,l’objet d’une planification partagée avec la Cnam afin d’en déterminer la date.  Lors de chaque test, le Titulaire doit démontrer le bon fonctionnement de son PRA, par :   * Les résultats des tests et vérifications réalisées * Les traces et logs de reprise * Un compte rendu et un REX associé   À l’occasion du test, la Cnam peut demander à opérer des vérifications de bon fonctionnement à son niveau.  Chaque Test doit être matérialisé par la production d’un PV de Validation à la charge du Titulaire. |

### Exigences de Supervision et métrologie

|  |  |
| --- | --- |
| Exigences | Description générale |
|  | Le Titulaire met en place les moyens nécessaires pour surveiller dans sa globalité l’ensemble des services hébergés (flux compris). Il met en œuvre les mécanismes  :   * De remontée d’information auprès de la Cnam sous forme de communication (Mail et SMS, ticketing, etc.) pour tous les évènements mettant en cause le fonctionnement nominal des différents environnements et des solutions que le Titulaire exploite (recette fonctionnelle, formation, pré-production, production, etc.). La cinématique de communication doit être mise en relation avec le Processus de Gestion des Incidents et détaillé dans le Plan d’Assurance Qualité. * D’accès de la Cnam à l’état et l’avancement des traitements et de leurs volumes traités OK ou en échec (portail, CR, etc.). |
|  | Le Titulaire doit présenter l’outil de supervision qu’il utilise et les éléments supervisés dans l’architecture. Une supervision réseaux, process, composants, ressources, services, tests de vie et scenarii fonctionnels (« expérience utilisateur ») doit être implémentée et exécutée pour garantir la qualité de service de l'application.  En particulier, la liste des éléments de configuration, processus ou services à surveiller doit être fournie et documentée (méthode d'accès), ainsi que la fréquence des Tests et de rejeux (permettant d’assurer un délai de Détection optimal, et un Délai de Prise en Compte conforme aux niveaux de services). |
|  | Le Titulaire assure une continuité sur les 3 niveaux de supervision (Métier, Applicatif et Technique). |
|  | Le Titulaire présente et met en place des mécanismes de détection et de remontées des Non-Evénements, permettant d’alerter sur une absence de Flux ou une absence d’activité prolongée.  Ces mécanismes de Non-Evénements font l’object de remontée d’information auprès de la Cnam au même titre que les évènements mettant en cause le fonctionnement nominal des différents environnements et des solutions que le Titulaire héberge.  Les critères et seuils appliqués sont, au préalable, soumis et validés avec la Cnam. |
|  | Le Titulaire doit fournir des rapports périodiques sur les exigences de performance et de disponibilité :   * Temps de réponse (réseau et services applicatifs) * Traitements d’interfaces (chargement, échanges, volumes) * Traitements internes (états, durées, volumes) * Supervision de l’état de l’infrastructure, des composants socle technique, des composants applicatifs.   La périodicité de ces rapports, pouvant aller jusqu’à du temps réel, est définie avec la Cnam durant la phase d’initialisation.  Entre les périodes, le pilotage Cnam doit avoir accès à ces informations en temps réel pour s’assurer du bon fonctionnement des services. |
|  | Le Titulaire met en œuvre un Planning capacitaire des infrastructures et environnements mis à la disposition de la Cnam.  Ce planning capacitaire est publié et présenté périodiquement à la Cnam. |
|  | Le Titulaire met à disposition de la Cnam les indicateurs reflétant l’état de disponibilité des services, des performances et le volume d’activité en temps réel et sous Forme de Tableaux de Bord. Ces indicateurs doivent permettre d’apprécier l’état des services du point de vue utilisateur final, et ce, au travers de toutes les briques traversées (qu’elles soient sous la responsabilité du Titulaire ou non). |
|  | Le Titulaire met à disposition de la Cnam les moyens nécessairespour communiquer avec les robots de supervision côté Cnam (Compte d’exploitation, url, simulation d’actions, description du scénario, etc.). Ces robots doivent pouvoir déclencher automatiquement le processus de gestion des incidents du Titulaire.  Les interfaces mises à disposition des robots pour cette automatisation sont décrites dans l’offre du Titulaire. |
|  | Tous dysfonctionnements détectés par l’outil de supervision déclenchent automatiquement le processus de gestion des incidents. Le process de Gestion des Incidents doit être détaillé dans le Plan d’Assurance Qualité. |
|  | Le Titulaire doit se munir, à ses frais, des outils adéquats et nécessaires pour mener à bien ses missions. La Cnam visant à consommer l’offre d’hébergement (si la PSE visée au §7.4 est retenue) et d’Exploitation sous forme de services, celle-ci ne peut se voir facturer l’acquisition de quelconques licences produits ou logiciels autour des activités de supervision et de métrologie. |
|  | Afin de faciliter toute action de Réversibilité auprès de la Cnam ou de tout autre repreneur, le Titulaire s’engage à s’appuyer tout au long de la prestation sur des outils standard, à jour, et maintenus, dans le cadre des activités citées ci-dessus et relatives aux environnements et services hébergés. |

### Exigences Environnement logiciel

|  |  |
| --- | --- |
| Exigences | Description générale |
|  | Un environnement logiciel : Il s’agit de la mise à disposition de tout le périmètre applicatif de l’accord-cadre MESDMP. |

Durant la durée d’exécution de l’accord-cadre, le Titulaire doit fournir les environnements dans trois situations :

* + Cas 1 : Dans le cadre de maintenabilité des services hébergés de l’accord-cadre par le Titulaire
  + Cas 2 : Dans le cadre des prestations d’évolution des services hébergés par le Titulaire
  + Cas 3 :Dans le cadre de l’évolution du parc applicatif du SI-Cnam par la Cnam. C'est-à-dire lorsque la Cnam fait évoluer son parc applicatif et a besoin d’environnements pour les différentes phases d’un projet Cnam.

En fonction du lotissement des évolutions, une version peut comporter des évolutions faites par le Titulaire (Cas 2) et des évolutions faites par la Cnam (Cas 3).

|  |  |
| --- | --- |
| Exigences | Description générale |
| Cas 1 | Le Titulaire est chargé de fournir tous les environnements décrits ci-dessous nécessaires au bon déroulement du maintien en condition opérationnelle et de sécurité des services hébergés par le Titulaire, accessibles par les utilisateurs et la Cnam (Cas 1) :   * Environnements de démonstration et formation :   + Accès : Réseau Cnam et Hors réseau Cnam   + Interconnexion : 2 options sont à prévoir :     - Utilisation de bouchons simulant les accès aux SI-Cnam     - Interconnexion : SI-Cnam   + Type : Hors production   Ils sont utilisés pour des démonstrations ou de la formation. Ils contiennent des données fictives.  Sur chaque environnement applicatif, la version installée peut être celle de la version en production ou une autre version suivant la demande de la Cnam.  Le Titulaire doit fournir et maintenir les jeux de données de cet environnement.   * Environnements de pré-production (N et N+1):   + Accès : Réseau Cnam et Hors réseau Cnam   + Interconnexion : SI-Cnam   + Type : Hors production   L’environnement de pré-production doit permettre de reproduire un incident dans les conditions identiques à l’environnement de production, de même que réaliser les benchmarks, audits de sécurité, des tests en conditions réelles avant la mise en production ; par exemple, pour valider une modification de paramétrage par un administrateur fonctionnel.  Pour offrir un maintien en condition opérationnel et de sécurité optimal sans incidence sur le Planning des évolutions en cours, le Titulaire doit mettre à disposition 2 environnements accessibles en parallèle à la Cnam. Un dans la version actuelle de la production (N) et un dans le cas d’une livraison d’évolutions en cours (N+1) et destinées à être testées.   * Environnements de certification des éditeurs :   + Accès : Réseau Cnam et Hors réseau Cnam   + Interconnexion : SI-Cnam   + Type : Hors production   Ils sont utilisés par les éditeurs dans le processus de l’ENS-compatibilité. Ils sont accessibles à travers les interfaces publiées nécessaires aux bons fonctionnements des logiciels éditeurs en production.  Cet environnement servit de version de référence (version en production ou une autre version) nécessaire dans le cadre du plan d’évolution de l’application.   * Environnement de production :   + Accès : Réseau Cnam et Hors réseau Cnam   + Interconnexion : SI-Cnam   + Type : Production   L’environnement de production est accessible aux utilisateurs agréés. Il est le seul environnement à contenir des données réelles. |
| Cas 2 | Le Titulaire est chargé de fournir tous les environnements décrits ci-dessous nécessaires pour le bon déroulement des phases du cycle de vie projet des services hébergés par le Titulaire, accessibles par la Cnam (Cas 2) :   * Environnements de recette fonctionnelle :   + Accès : Réseau Cnam et réseau du titulaire du DMP   + Interconnexion : SI-Cnam   + Type : Hors production   Avant passage en recette fonctionnelle, le Titulaire doit s’assurer de la conformité de sa solution avec les exigences de performance et sécurité.  L’environnement de recette fonctionnelle est utilisé par la Cnam pendant la phase d’intégration et recette pour valider les différents services ou évolutions majeures considérés comme critiques. Le Titulaire doit mettre à disposition de la Cnam, pendant toute la durée d’exécution de l’accord-cadre, un environnement de recette sanctuarisé pour permettre les tests fonctionnels incluant les jeux de données. Dans le cadre de la recette fonctionnelle :   * + - Un environnement sert de version de référence (version en production ou une autre version) nécessaire dans le cadre du plan d’évolution de l’application.     - Un environnement sert de version à tester portant les évolutions nécessaires dans le cadre du plan d’évolution de l’application.   Ces environnements doivent permettre la recette de la solution de bout en bout (incluant le flux voix et les autres canaux) depuis des PMFs de la Cnam.   * Environnements de pré-production :   + Accès : Réseau Cnam et Hors réseau Cnam   + Interconnexion : SI-Cnam   + Type : Hors production   L’environnement de pré-production doit permettre de répéter la mise en production et faire une recette de pré-production avant la mise en production définitive de la version. |
| Cas 3 | Le Titulaire est chargé de fournir tous les environnements décrits ci-dessous nécessaires pour le bon déroulement des phases du cycle de vie de l’évolution du parc applicatif du SI-Cnam par la Cnam, accessibles par la Cnam (Cas 3) :   * Environnements fabricant (ou développement) :   + Accès : Réseau Cnam   + Interconnexion : Aucune   + Type : Hors production   Il est utilisé pendant la phase de développement par le Titulaire pour réaliser les services initiaux, les évolutions et les maintenances correctives ainsi que les tests unitaires.   * Environnements d’intégration :   + Accès : Réseau Cnam   + Interconnexion : SI-Cnam   + Type : Hors production   Dans le cadre de la réalisation d’une évolution d’un module applicatif de la Cnam au sein du SI-Cnam, la Cnam (ou ses prestataires) doit réaliser les tests d’intégration sur un environnement sans bouchon applicatif.  Le Titulaire doit mettre à disposition un environnement de ses services hébergés pour permettre aux environnements d’intégration de la Cnam de s’interfacer.  Il est utilisé par le Titulaire pendant la phase d’intégration et recette interne du Titulaire pour valider les différents services.   * Environnements de recette fonctionnelle :   + Accès : Réseau Cnam   + Interconnexion : SI-Cnam   + Type : Hors production   Dans le cadre de la réalisation d’une évolution d’un module applicatif de la Cnam au sein du SI-Cnam, la Cnam (ou ses prestataires) doit réaliser les tests de recette fonctionnelle sur un environnement sans bouchon applicatif.  Le Titulaire doit mettre à disposition des environnements de ses services hébergés pour permettre aux environnements de recette fonctionnelle de la Cnam de s’interfacer.  Il est utilisé par la Cnam pendant la phase de recette fonctionnelle pour valider les différents services.   * Environnements de performances (Bench) :   + Accès : Réseau Cnam   + Interconnexion : SI-Cnam   + Type : Hors production   Dans le cadre de la réalisation d’une évolution d’un module applicatif de la Cnam au sein du SI-Cnam, la Cnam (ou ses prestataires) doivent réaliser les tests de performances sur un environnement sans bouchon applicatif.  Le Titulaire doit mettre à disposition des environnements de ses services hébergés pour permettre aux environnements de recette de performances de la Cnam de s’interfacer.  Ils sont utilisés par le Titulaire pour garantir la conformité aux exigences.   * Environnements de pré-production :   + Accès : Réseau Cnam et Hors réseau Cnam   + Interconnexion : SI-Cnam   + Type : Hors production   Dans le cadre de la réalisation d’une évolution d’un module applicatif de la Cnam au sein du SI-Cnam, la Cnam (ou ses prestataires) doit réaliser les tests de recette fonctionnelle sur un environnement sans bouchon applicatif.  Le Titulaire doit mettre à disposition des environnements de ses services hébergés pour permettre aux environnements de pré-production de la Cnam de s’interfacer.  Il est utilisé par la Cnam pendant la phase de recette pré-production pour valider le passage en production |
|  | Le Titulaire doit utiliser un outillage pour la gestion des tests ainsi que l’automatisation de l’ensemble des tests de non régression, et fournit les rapports de tests associés. |
|  | Le Titulaire met en place un processus automatisé de dépersonnalisation des données de production pour le passage aux environnements hors production |
|  | Le Titulaire met en place un processus industrialisé et automatisé pour la mise à jour des différents environnements (Retour arrière, déploiement évolution, correctif) afin de limiter au maximum leur indisponibilité ainsi que fiabiliser et automatiser les tâches répétitives. |
|  | Afin de faciliter toute action de Réversibilité auprès de la Cnam ou de tout autre repreneur, le Titulaire s’engage à s’appuyer tout au long de la prestation sur des outils standard et à jour, dans le cadre des activités citées ci-dessus relatives aux environnements logiciels préalablement définis. |
| Environnement Formation | Le Titulaire se met en capacité de réinitialiser régulièrement les jeux de données de formation, soit à la demande de la Cnam soit selon un calendrier défini. |
| Environnement de certification éditeurs | Le Titulaire met en place un service permettant de gérer simultanément 30 éditeurs pour satisfaire à l’agrément de leur(s) logiciel(s), qui reproduisent à périmètre fonctionnel a minima à l’identique du système MESDMP en production. |
| Environnements de certification éditeurs | Le Titulaire réinitialise régulièrement les jeux de données de certification éditeurs, soit à la demande de la Cnam soit selon un calendrier défini, selon la fréquence de réinitialisation par environnement applicatif de certification éditeurs. |
| Environnements de certification éditeurs | Des ressources du Titulaire peuvent être mobilisées en tant que de besoin pour apporter une assistance technique sur le service de certification des éditeurs :   * Lors de la mise à disposition d’un environnement applicatif de certification éditeurs ; * En cas de difficultés techniques rencontrées par l’entité, définie par la Cnam, en charge de la certification au moment de la préparation ou du déroulement d’une session de formation, ou à l’issue de celle-ci (réinitialisation des données pour la session suivante, etc.). * En cas de difficultés techniques rencontrées par un éditeur pour se connecter à l’environnement applicatif. |
|  | Le Titulaire gère différents environnements de tests, étanches entre eux, afin de permettre la tenue de plusieurs campagnes de tests de manière concomitante. |
| Jeux de données | Le Titulaire doit contribuer à la constitution d’un jeu de données de test transverse avec la Cnam et les acteurs des SI-ENS et SI-Cnam. Le Titulaire intervient pour constituer, maintenir et mettre à disposition les jeux de données afin d’assurer une cohérence de entre SI-ENS et SI-Cnam pour tous les environnements hors production |

### Exigences spécifique liée au cluster de composants WAF

|  |  |
| --- | --- |
| Exigences | Description générale |
|  | Le cluster de WAF qui protège MES est constitué de matériels physiques dédiés de marque Ubika : deux WAF par site, donc quatre WAF, le tout en cluster actif/actif. Ces WAF terminent les session SSL/TLS qui entrent dans le SI et aboutent les connexions web vers les équilibreurs de charge. Ils réalisent un certain nombre de traitements à ce niveau (validation du respect des contrats de service des accès aux API REST, enrichissement des requêtes avec des entêtes particuliers, filtrage des attaques, réalisation de « virtual patching » en cas de découverte d’une vulnérabilité qui ne peut pas être corrigée dans l’immédiat, etc.) et alimentent le SIEM du SOC. Ces équipements qui opèrent un traitement spécifique à MES sont sous responsabilité de mise en place, exploitation, MCO et MCS du Titulaire, quel que soit le lieu de leur hébergement. |

## Exigences générales

Le Titulaire doit utiliser des outils et des méthodes en se référant à l’état de l’art et aux standards du marché.

Les différentes exigences sont regroupées par famille ci-après.

### Exigences de réversibilité

| Exigences | Description générale |
| --- | --- |
|  | En cas d’affermissement de la tranche optionnelle considérée, le Titulaire s'engage à assurer la réversibilité du service, afin de permettre à la Cnam de reprendre, ou de faire reprendre par un / des tiers désigné(s) par elle, la fourniture du service et ce, dans les meilleures conditions et sans discontinuité du service.  La Cnam, ou le tiers désigné par elle, est dénommé dans le présent chapitre le « Repreneur ».  Les livrables attendus au titre de cette prestation sont listés au §7.12 Liste des livrables principaux. |
|  | Dans le cadre du processus de réversibilité, le Titulaire fournit au Repreneur toute l'assistance et les informations nécessaires et utiles à la restitution de la connaissance et de la responsabilité opérationnelle.  Au cours de la période de réversibilité, le Titulaire assure les activités qui lui sont attribuées dans le cadre de la transition avec les équipes du Repreneur. |
|  | S’agissant des droits de propriété intellectuelle, le Titulaire applique les stipulations de l’article du CCAP relatif à la cession des droits de propriété intellectuelle (cf. CCAP ). |
|  | Un responsable unique du projet de réversibilité est désigné au sein des équipes du Titulaire comme interlocuteur privilégié du Repreneur |
|  | Le Titulaire s’engage à inclure une clause de réversibilité dans les dispositifs contractuels le liant aux sous-traitants à qui il délègue une partie des éléments inclus aux périmètres de réversibilité susvisés.  Le Titulaire communique à la Cnam les preuves afférentes |
|  | Le Titulaire s’engage à collaborer loyalement avec les équipes du Repreneur. |
|  | Le Titulaire s’engage à fournir un plan de destruction de l’entièreté des composants relatifs à la prestation (données applicatives, données techniques, données de gestion, codes, documentations, etc.) présents sur les différents supports (magnétiques ou autres) qu’il possède et à le mettre en œuvre après accord de la Cnam. Les preuves de destructions sont communiquer par le Tituaire à la Cnam sans délai. Les frais de cette destruction sont à la charge du Titulaire. |
|  | Lors de la prestation Prise de connaissance et Initialisation de l’accord-cadre, le Titulaire s’engage à fournir un plan de réversibilité global. |
|  | Lors de la phase de préparation de la réversibilité, le Titulaire doit effectuer des tirs à blanc et fournir à la Cnam les rapports et preuves de bonne excécution. |
| Préparation de la réversibilité | Tout au long de l’accord-cadre, le Titulaire met à jour les plans de réversibilité des services et construit un plan de réversibilité global précisant :   * Les outils, les normes et standards définis par le Titulaire, et contrôlés par la Cnam, pour l’exécution de la réversibilité ; * L’inventaire précis : * De la documentation produite dans le cadre de l’accord-cadre, des versions afférentes à chaque documentation et du statut de ces versions ; * Des développements réalisés pour la fourniture des services ; * Les règles de maintien à jour des applications et de leur documentation ; * Les procédures d’exploitation et les dossiers de mise en œuvre des outils logiciels et matériels ; * Les conditions de transfert de droit de propriété des applications développées aux fins de l’accord-cadre ainsi que, le cas échéant, le droit d’utilisation des logiciels utilisés par le Titulaire; * Les conditions de transfert de compétences du Titulaire vers le Repreneur ; * Le plan de bascule des services sans interruption de service du SI MESDMP (applications, données, documentations, outils, logiciels, matériels) ; * Le plan de décomissionnement ; * Les macros plannings des opérations pour la réversibilité, qu’elles soient à engager par le Titulaire ou le Repreneur. |
| Préparation de la réversibilité | Le Titulaire prévoit d’effectuer une fois par an une revue des plans de réversibilité, dont une bascule à blanc, pour évaluer leur faisabilité et leur conformité par rapport aux normes et standards définis, et identifie les points à améliorer dans un délai de 3 mois. Un bilan est remis à la Cnam, sans délai, à l’issue de la revue et du plan d’amélioration. |
| Préparation de la réversibilité | La Cnam se réserve le droit d’évaluer ou faire évaluer ces plans de réversibilité et exige, le cas échéant, les mesures d’amélioration nécessaires. |
| Exécution de la réversibilité | La réversibilité est organisée en 3 phases :   * La première phase d’initialisation et de préparation de la réversibilité vise à mettre à jour le plan de réversibilité et à planifier l’exécution de la réversibilité, en lien avec le Repreneur ;   Cette phase est à réaliser dans une période de 3 mois maximum à partir du démarrage de la prestation de réversibilité.   * La deuxième phase vise à exécuter la réversibilité. A l’issue de cette phase, le Repreneur reprend de manière opérationnelle les services et est responsable de la qualité de service ;   Cette phase est à réaliser dans une période de 7 mois maximum après la phase d’initialisation et de préparation.   * La troisième phase porte sur le soutien ponctuel au Repreneur pendant une période de 3 mois après la reprise opérationnelle du service par celui-ci (Vérification de Service Régulier chez le Repreneur).   Pendant les deux premières phases de la réversibilité, le service est assuré par le Titulaire selon les conditions, modalités et niveaux de services définis. Durant cette période, le Titulaire ne peut en aucune façon modifier ou réduire ses prestations et ses obligations. |
| Exécution de la réversibilité | Les travaux à la charge du Titulaire dans le cadre de l’exécution de la réversibilité recouvrent :   * La conduite, l’organisation et la planification du projet de réversibilité, sur son périmètre de responsabilité, * La fourniture de toute la documentation nécessaire pour la reprise de l’exploitation et de la maintenance des différents composants concernés par la réversibilité : * Toute la documentation produite, ainsi que tous les objets techniques (code sources, scripts, modèles de données, etc.) nécessaires à la compréhension, à la réalisation, à l’hébergement, le cas échéant, à l’exploitation et à la maintenance du système, * Les plans de tests et les jeux de données associés le plan de qualité d’exploitation, comprenant notamment : * Les procédures et modes opératoires conformes ITIL précisés dans les exigences du maintien en conditions opérationnelles des services ; * Les dossiers d’exploitation (contenant la description succincte de l’application, les contraintes de service, le schéma d’architecture technique et les alertes et procédures associées) ; * La liste et configuration des matériels et logiciels systèmes nécessaires ; * Le paramétrage nécessaire et les procédures pour le réaliser ; * Les échanges inter-applicatifs (internes et externes) et leurs modalités ; * Le plan de sauvegarde et de restauration (liste des objets sauvegardés, durée de rétentions, etc.) ; * Les tests de transfert vers le Repreneur, * Le transfert vers le Repreneur des éléments logiciels et données, * Le transfert vers le Repreneur des données de production de MESDMP en respectant les exigences de sécurité ainsi que la documentation nécessaire à la reprise des données, * L’assistance technique au Repreneur lors de la construction de l’infrastructure matérielle et applicative et de la recette des composants construits (nota : la recette sur le site du Repreneur est assurée par ce dernier), * La formation du personnel du Repreneur à l’ensemble des connaissances, modes opératoires et spécificités des services MESDMP à reprendre, * La planification d’engagement et de désengagement des équipes afin de permettre au Repreneur de préparer la reprise de chantier avec ses propres moyens. |
| Exécution de la réversibilité | Durant la phase de réversibilité, le Titulaire reste en responsabilité de MESDMP jusqu’au démarrage des services chez le Repreneur, marquant pour ce dernier le début de la vérification du service régulier. A ce titre il doit effectuer un suivi régulier et fournir un bilan mensuel du déroulement des opérations. |
| Soutien ponctuel au Repreneur | Pendant la phase de soutien ponctuel au Repreneur, le Titulaire s’engage sur une période de 3 mois à compter de la reprise du service par le Repreneur à cet effet à répondre à toute demande d’assistance, même ponctuelle, formulée par le Repreneur. |
| Soutien ponctuel au Repreneur | Pendant la phase de soutien ponctuel au Repreneur, le niveau de service attendu du Titulaire pendant cette phase est celui attendu au titre du support de niveau 3 sur le périmètre Hébergement (si PSE Hébergement est retenue) et Exploitation et sur le périmètre applicatif. |
|  | Selon le jalon défini conjointement entre le Titulaire et le Repreneur en phase d’initialisation/préparation (jalon validé par la Cnam), le Titulaire assure le décomissionnement complet sur son site et en fournit les preuves à la Cnam.  Le décommissionnement se fait au maximum dans un délai de deux mois.  Cette action de décommissionnement clôture la prestation de Réversibilité par le Titulaire |

### Exigences de sécurité

#### Obligation du Titulaire

Les exigences de sécurité définies dans le présent CCTP et le Plan d’Assurance Sécurité sont des exigences à destination du Titulaire ayant pour objectif de pallier ou réduire les principaux risques liés à l’exécution de l’accord-cadre.

Le Titulaire respecte les exigences de sécurité et exécute l’ensemble de ses obligations de résultats et de moyens tout au long de l’accord-cadre.

Conformément au RGPD, le Titulaire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l’état de l’art en vue d'optimiser la protection des données et éviter les risques ci-dessus.

En particulier, il informe la Cnam des risques d’une opération envisagée, des incidents éventuels ou potentiels et de la mise en œuvre éventuelle d’actions correctives ou de prévention.

Le Titulaire informe préalablement la Cnam de toute opération susceptible de provoquer l’indisponibilité (ou une dégradation des performances) du service, la dégradation d'intégrité et/ou de confidentialité des données.

Le Titulaire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations. Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l’état de l’art : la découverte de failles dans son système d'information, l'évolution des technologies et des capacités d'attaques doivent être prises comptes.

#### Démarche du Plan d’Assurance Sécurité

Le PAS en annexe comprend l’ensemble des exigences de sécurité liées à l’environnement du Titulaire utilisé dans le cadre de la prestation.

Lors de la prestation Prise de connaissnce et initialisation, le Titulaire doit rédiger la version finale du PAS et élaborer les dispositifs de sécurité afférents pour démontrer le respect des exigences de sécurité.

Pendant toute la durée d’exécution de l’accord-cadre :

* + Les dispositifs de sécurité mis en œuvre doivent évoluer conformément à l’état de l’art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l’évolution des techniques doivent être pris en compte.
  + Le Titulaire doit réaliser l’auto-évaluation de conformité aux exigences de sécurité stipulées par la Cnam et suivre les indicateurs de sécurité. Il informe la Cnam des risques, des incidents et de proposition de mise en conformité ayant trait à la sécurité.
  + Le PAS peut faire l’objet d’évolution dont les modalités sont précisées dans le document lui-même, le Titulaire s’engage à mettre à jour le PAS conformément aux directives de la Cnam.

Il est rappelé que le PAS ne peut avoir pour objet ni pour effet de modifier les engagements et obligations souscrits au titre de l’accord-cadre.

En plus des exigences de sécurité du PAS, le Titulaire respecte les exigences spécifiques suivantes :

| Exigences | Description générale |
| --- | --- |
| Application périmètre SSI | Le Titulaire s’engage à mettre en place l’ensemble des éléments cités dans le CCTP et le PAS afin de maintenir les conditions de sécurité dès le début de l’accord cadre. Une analyse d’écart doit être réalisée deux semaines avant le début de la bascule des services pour permettre d’identifier les risques résiduels par rapport au niveau de sécurité exigé (périmètre SSI).  A l’ouverture du service en production, le Titulaire reconduit toutes les mesures de sécurité décrites dans l’existant (annexes : « MESDMP\_Annexe 11\_Description générale des mécanismes de chiffrement »  » et « MESDMP\_Annexe 12\_Description détaillée de la protection des données  »), ou à défaut met en place de mesures permettant de traiter les risques de manière similaire. |

#### SEC1 – Conformité réglementaire HDS

| Exigences | Description générale |
| --- | --- |
| Conformité réglementaire | Dans la mesure où les données à caractère personnel traitées sont des données de santé, des obligations spécifiques quant à leur hébergement sont introduites par l’article  L.1111-8 du Code de la santé publique.  Le Titulaire doit-être certifié HDS sur l’ensemble des activités couvertes par les deux périmètres de la certification HDS :   * Prestation d’hébergeurs d’infrastructure physique * Prestation d’hébergeurs info géreurs.   Le Titulaire s’il ne propose pas lui-même l’hébergement de la solution s’engage à ce que l’hébergement proposé soit certifié HDS afin que l’ensemble des activités réalisées par le tiers hébergeur soit certifié HDS.  Le Titulaire doit être certifié HDS sur l’ensemble des activités applicables au référentiel, et ce pendant toute sa durée, sans discontinuité temporelle. Le Titulaire communique annuellement la preuve à la Cnam. |

#### SEC2 – Disponibilité

| Exigences | Description générale |
| --- | --- |
| Protection anti-DDOS | Les mesures de protection de l’infrastructure hébergeant la plateforme MES contre les attaques de type déni de service distribué doivent faire l’objet d’une étude spécifique visant à déterminer le niveau de protection adéquat devant être mis en œuvre.  L'ensemble des processus, mécanismes et outils attendus sont décrits dans le PAS au §5.6 GESTION DE L'EXPLOITATION ET DES COMMUNICATIONS (GEC). |

#### SEC3 - Contrôle d’accès

| Exigences | Description générale |
| --- | --- |
| Référentiel des identités | Le Titulaire de l’accord-cadre est responsable de l’intégrité, de la confidentialité, de la qualité, et de la véracité des identités stockées au sein du référentiel.  Il s’agit des exploitants et administrateurs de l’application.  L’ensemble des utilisateurs de l’application sont gérés par l’application.  L'ensemble des processus, mécanismes et outils attendus sont décrits dans le PAS au §5.7 CONTROLE DE L'ACCES ET DES HABILITATIONS (CAH). |
| Enrôlement, Identification et Authentification des Titulaires | Les processus d’enrôlement, identification et authentification des titulaires d’un compte MES doivent être conformes au niveau requis par le cadre règlementaire applicable et positionné à ce jour au niveau substantiel.  L'ensemble des processus, mécanismes et outils attendus sont décrits dans le PAS aux §5.4 SECURITE LIEE AUX RESSOURCES HUMAINES (SRH), 5.5 SECURITE PHYSIQUE (SPH), 5.7 CONTROLE DE L'ACCES ET DES HABILITATIONS (CAH) |
| Protocole support à l’authentification et à la gestion des identités | Les protocoles d’authentification doivent être repris par le Titulaire (Open ID Connect (OIDC), OAUTH2, etc.).  La compatibilité avec le service FranceConnect est à respecter.  Une compatibilité ascendante aux recommandations de sécurité de l’ANSSI relatives à l’ensemble de ces protocoles doit être assurée par le Titulaire tout au long de la durée de l’accord-cadre**.** |
| Authentification des tiers Professionnels de santé, issus de la Sphère sociale et des usagers | Les modalités d’authentification des Professionnels de Santé et acteurs de la sphère sociale doivent répondre aux exigences formulées par la PGSSI-S et de la PSSI-MCAS. Ces modalités doivent rester conformes à toute évolution des référentiels de sécurité des professionnels de Santé, acteurs de la sphère sociale et l’ensemble des usagers. |
| Protections des APIs | Le Titulaire doit garantir :   * Un processus de contrôle d'accès des API rigoureux associé à un suivi précis (applicable également pour l’ensemble sous-traitants éventuels); * Une sécurisation des API utilisant les dernières normes de cryptage et de protocoles de sécurité décris par l’ANSSI et dans ce PAS ; * Un contrôle de conformité des appels API ; * Une cartographie des API régulière pour que les mises à jour et les correctifs soient appliqués à temps.   L’ensemble de ces éléments de politique de sécurité sont formalisés dans un document mis à disposition de la Cnam par le Titulaire avant l’ouverture de service pour validation.  L'ensemble des processus, mécanismes et outils attendus sont décrits dans le PAS au §5.8 SECURITE DU DEVELOPPEMENT (DEM) |

#### SEC4 – Protection des données

| Exigences | Description générale |
| --- | --- |
| Pseudonymisation de la donnée | Le Titulaire doit reprendre les processus et les outils mis en place pour la pseudonymisation des données, le contrôle d’intégrité et le chiffrement des données. |
| Protection des données | Les périmètres applicables au chiffrement de la donnée sont :   * Le support de stockage de longue durée chiffré avec AES-256 * Les volumes Linux sensibles chiffrés via des mécanismes ajoutés au noyau linux * Les données applicatives dans les bases de données chiffrées avec des clés créées à l'aide d'un cluster de HSM qualifiés par l'ANSSI * Le transport des données chiffré avec SSL/TLS et des certificats X.509 délivrés par une Autorité de Certification qualifiée RGS par l’ANSSI.   Le chiffrement est basé sur un cluster de HSM qualifié au niveau renforcé par l’ANSSI embarquant un KMS.  L’objectif de ces systèmes de protection des données est d’empêcher la réidentification, par un tiers non dûment identifié et habilité à cette action, des données de santé pouvant transiter ou étant hébergées sur la plateforme, aux données administratives ou au profil du titulaire d’un compte MES.  L’ensemble des périmètres et des mécanismes sont décrits dans le PAS. Les pratiques associées doivent suivre les recommandations de l'ANSSI. |

#### SEC5 – Sécurité réseau

| Exigences | Description générale |
| --- | --- |
| Sécurité des flux entrant et sortant | Tout flux entrant ou sortant de la plateforme MES doit être chiffré à l’aide du protocole TLS 1.2 minimum non renégociable à niveau inférieur.  Une compatibilité ascendante aux recommandations de sécurité relatives à TLS de l’ANSSI doit être assurée par le Titulaire tout au long de la durée de l’accord-cadre. |
| Authentification des composants | Des mécanismes d’authentification des composants internes visant à protéger les échanges doivent être mis en œuvre par le Titulaire.  Les mécanismes d'authentification sont décrits dans l’offre du Titulaire.  L'ensemble des processus, mécanismes et outils attendus sont décrits dans le PAS aux §5.6 GESTION DE L'EXPLOITATION ET DES COMMUNICATIONS (GEC) et 5.7 CONTROLE DE L'ACCES ET DES HABILITATIONS (CAH) |
| Protection contre les attaques applicatives et réseau (SOC) | Le Titulaire doit, par le biais d’une équipe de sécurité organisée autour d’un SOC, réaliser une surveillance active, préventive et en temps réel de l'état de la sécurité de la plateforme MES. Ceci en vue de détecter toutes vulnérabilités ou tentatives d’intrusion et ainsi être en capacité soit de corriger ou de juguler une intrusion.  L'ensemble des processus, mécanismes et outils attendus sont décrits dans le PAS aux §5.3 GESTION DE CRISE SSI – CONTINUITE D’ACTIVITE (CRI), 5.8 SECURITE DU DEVELOPPEMENT (DEM), 5.10 GESTION DES INCIDENTS (GDI).  A titre d’information, en 2022, le nombre de requêtes depuis Internet bloquées par le WAF et signalées dans le SIEM du SOC en tant qu’évènements de sécurité est de l’ordre d’environ 500.000 par semaine, avec une forte variance selon les semaines.  Seules les attaques qui proviennent de sources particulièrement virulentes ou les attaques particulièrement élaborées conduisent à créer un incident pour avoir un traitement spécifique (le plus souvent, blocage de l’IP source de l’attaque). Cela correspond à environ une vingtaine d’incidents de ce type par semaine.  Les autres types d’évènements de sécurité (mésusage détecté, tentative d’authentification incorrecte, etc.) conduisent, pour ceux dont la Cnam juge qu’ils méritent un traitement, à des incidents se répartissant comme ceci :   * Environ 50 incidents sécurité par an de niveau de priorité P2 et P3, ne nécessitant pas la création d’une cellule de crise, de tous types, * Environ 12 incidents sécurité par an de niveau de priorité P1, nécessitant la création d’une cellule de crise.   L’ouverture de nouveaux services, dont le Store d’échange avec des services tiers, devrait conduire à une augmentation du nombre d’incidents, puisque la surface d’attaque s’accroit. Le Titulaire utilise son expérience et son expertise sécurité de ce domaine pour évaluer l’augmentation prévisible du nombre d’incidents liés à cette ouverture. |
| Protection contre les attaques applicatives et réseau | Le Titulaire présente l’ensemble des mesures de sécurité technique mises en œuvre afin d’assurer la défense en profondeur et ce pour chaque environnement composant le SI-MES.  L'ensemble des processus, mécanismes et outils attendus sont décrits dans le PAS au §5.6 GESTION DE L'EXPLOITATION ET DES COMMUNICATIONS (GEC) |

#### SEC6 – Traçabilité

| Exigences | Description générale |
| --- | --- |
|  | Le premier composant en capacité de créer un identifiant de corrélation en entrée du SI doit définir un identifiant de corrélation valide pour une transaction ou une session donnée.  Les composants en situation de recevoir le flux portant cet identifiant doivent le véhiculer et le tracer.  L’identifiant de corrélation vise à faciliter la protection contre les attaques applicatives et réseau, tant sur le SI MES que sur le SI de la Cnam.  L'ensemble des processus, mécanismes et outils attendus sont décrits dans le PAS aux §5.6 GESTION DE L'EXPLOITATION ET DES COMMUNICATIONS (GEC) et 5.7 CONTROLE DE L'ACCES ET DES HABILITATIONS (CAH) |

#### SEC7 – Homologation RGS

| Exigences | Description générale |
| --- | --- |
|  | Cet environnement possède un jeu de données propre à son contexte (anonymisation des données, comptes dédiés, etc.)  Lors de chaque évolution de la plateforme de services et avant toute ouverture de service, même lors d’une phase d’expérimentation, le service MES doit faire l’objet d’une homologation au Référentiel Général de Sécurité sur l’ensemble du périmètre de la prestation. Le Titulaire de l’accord-cadre met en œuvre l’ensemble des ressources nécessaires à la réalisation des audits visant à :   * Valider la bonne mise en œuvre des mesures de sécurisation identifiée par l’analyse de risque du Titulaire, * Valider le niveau de sécurité de la version homologuée et identifier les risques résiduels ; * Accompagner le responsable de traitement dans le cadre de cette procédure ; * Garantir une transparence totale sur les preuves de conformité du référentiel RGS, en fournissant les justificatifs associés sur l’ensemble du périmètre applicable ; * Garantir que les processus de patchs de sécurité sont adaptés et associés aux exigences RGS.   Une matrice de responsabilité pour le processus d'homologation doit être définie par le Titulaire. Elle doit permettre de clarifier les rôles et les responsabilités de chaque partie impliquée dans le processus. Cette matrice doit être approuvée conjointement avec la Cnam lors de la prestation P1.1 - Pdc\_Init : Prise de connaissance et Initialisation. |
|  | Le Titulaire doit mettre à disposition un environnement de tests d’intrusion accessible depuis le Web étant une copie de l’environnement de production (en termes de fonctionnalités, points d’accès, etc.). |
| NIS | Le Titulaire doit mettre en œuvre l'ensemble des outils, processus afin de faire l'objet d'une homologation NIS. Cette homologation est amenée à évoluer avec les dernières directives nationales et applicables au contexte du projet (NIS 2).  Le Titulaire doit présenter sa démarche dès le début de l’accord-cadre.  Les choix proposés doivent être compatibles avec NIS et être réfléchis en conséquence. La conformité au référentiel NIS doit être intégrée dès le départ ("NIS by design"), son coût est inclus dans le coût forfaitaire de la prestation de référence. |
| Certifications | Le Titulaire doit mettre en œuvre l'ensemble des outils, mécanismes et processus afin de valider l’ensemble des conformités et homologations suivantes :   * HDS (décrit dans EXG\_SEC\_1.1) * ISO 27001 * ISO 27701 * ISO 27018 (uniquement si hébergement Cloud) * PRIS pour le scope de réponse à incidents (CISRT) * PDIS pour le scope de détection d’incidents (SOC) * PASSI pour les audits de sécurité   L’ensemble de ces certifications sont applicables pendant toute la durée de l’accord-cadre, sans discontinuité temporelle. Le Titulaire communique à la Cnam, annuellement, la ou les preuve(s). |
| Conformité aux référentiels | Le Titulaire doit mettre en œuvre l'ensemble des outils, mécanismes et processus afin de valider l’ensemble des conformités et homologations suivantes :   * ISO 27701 * ISO 27018 (uniquement si hébergement Cloud) * PRIS pour le scope de réponse à incidents (CISRT) * PDIS pour le scope de détection d’incidents (SOC) * PASSI pour les audits de sécurité   L’ensemble de ces certifications sont applicables pendant toute la durée de l’accord-cadre, sans discontinuité temporelle. Le Titulaire communique à la Cnam, annuellement, la ou les preuve(s). |

### Exigences de Maintenabilité Opérationnelle

#### MNT - Maintenance préventive, corrective, évolutive, standard et réglementaire

|  |  |
| --- | --- |
| Exigences | Description générale |
|  | Le Titulaire est responsable de tous les logiciels et interfaces développés ou mis en œuvre. Il prend à sa charge leur maintenance corrective dans le cadre des prestations de maintien en condition opérationnelle et de sécurité des services. |
|  | Le Titulaire s’engage, pour tout nouveau développement, sur la qualité du code des logiciels développés, sur le respect des normes fixées pour la réversibilité de fin d’accord-cadre, ainsi que les exigences fonctionnelles de sécurité. |
|  | Le Titulaire planifie et réalise les opérations de maintenance (par exemple pour des réorganisations, modifications de paramètres des bases de données, modifications de la répartition du stockage physique, ec.) en respectant un délai de prévenance établi avec la Cnam de 15 jours calendaires (détaillé dans le Plan d’Assurance Qualité). Ce délai peut être adapté en fonction du niveau d’urgence de la maintenance à opérer, mais toujours avec communication et validation préalable par la Cnam du créneau envisagé. |
|  | Le Titulaire planifie et réalise :   * Les opérations de maintenance en Production sans interruption du service * Les opérations de maintenance en Hors-Production sans interruption du service, ou à défaut en dehors des plages de disponibilité prévues au présent CCTP.   En cas de non-respect, toute indisponibilité est répercutée sur les indicateurs de disponibilité prévus au présent CCTP. En cas de non respects des seuils, la Cnam peut appliquer les pénalités définies au CCAP. |
|  | Le Titulaire assure les actions proactives et réactives d'amélioration des systèmes (optimisation des serveurs, mise à jour de sécurité, augmentation des ressources systèmes, etc.) |
|  | Le Titulaire est tenu de réaliser les actions nécessaires en vue de rendre conforme la solution à la réglementation en vigueur, y compris des évolutions concernant les exigences de la CNIL ou en lien avec les référentiels d’interopérabilités nationaux : Cnam et ANS. |
|  | Le Titulaire assure la maintenance évolutive standard de la solution prévue dans le cadre de sa roadmap éditeur. A ce titre, il fournit à la Cnam l’ensemble des mises à jour et nouvelles versions y compris majeures de la solution. |
|  | Afin de faciliter toute action de Réversibilité auprès du Repreneur, le Titulaire s’engage à s’appuyer tout au long de la prestation sur des produits, outils et langages standard et à jour, dans le cadre des activités citées ci-dessus et relatives aux environnements, services et solutions hébergés. |
|  | Le Titulaire s’engage à souscrire tous les contrats de maintenance logiciel et matériel jugés nécessaires pour garantir les niveaux de service demandés.  Ces contrats doivent être souscrits auprès des constructeurs et/ou éditeurs et renouvelés chaque année. |
|  | De manière préventive, le Titulaire de l’accord-cadre identifie et propose les évolutions nécessaires concernant l’architecture fonctionnelle, applicative et technique. Cette démarche vise à réduire les risques de dégradation des performances du système en regard d’une montée significative des volumétries (données, nombre d’utilisateurs, etc.). La maintenance préventive doit également permettre de maintenir et d’améliorer le niveau de qualité de l’application et de réduire les coûts de la maintenance corrective et d’éviter toute obsolescence technique du produit. |
|  | Au titre de la maintenance préventive, le Titulaire est en charge de :   * L’identification des risques et de l’étude des améliorations à apporter à l’application (application, base de données, architecture, retour des analyses des tickets utilisateurs, etc.) afin de maintenir le niveau de service conforme aux exigences ou de prévenir des risques de dégradation des performances ; * L’identification et l’analyse des impacts sur l’application de la réalisation ou non des opérations de maintenance préventive (impact de l’absence de travaux de maintenance préventive, composants impactés par les opérations de maintenance, etc.) ; * La définition de plans d’actions nécessaires au maintien de la qualité de service. |
|  | A minima tous les trimestres, le Titulaire fournit le compte-rendu d’activité de la prestation de maintien en conditions opérationnelles, les risques opérationnels identifiés sur le fonctionnement de l’application en production et les actions de maintenance préventive associées. |

#### GDC – Gestion des Changements et Mises en Production

|  |  |
| --- | --- |
| Exigences | Description générale |
|  | Le Titulaire assure la déclaration et la traçabilité de toute opération réalisée de manière directe ou indirecte sur l’un des éléments de configuration de son SI, délivrant ou contribuant à un service pour lequel la Cnam est client. La traçabilité et la déclaration de ces opérations sont réalisées conformément aux processus de Gestion de la Configuration et de Gestion des Changements détaillés dans le Plan d’Assurance Qualité. |
|  | Avant toute installation en production, le Titulaire s’engage à respecter un déploiement sur les environnements Hors-Prod et à accomplir les opérations suivantes : Tests de Non-Régression, Tests de Robustesse, Tests aux Limites, Tests de sécurité, Tests de la procédure de retour arrière, etc. |
|  | En cas d’évolution Fonctionnelle, le Titulaire s’engage à solliciter la Cnam pour planification et réalisation d’une Recette Fonctionnelle adaptée.  La bonne Fin desdits Tests doit être systématiquement matérialisée par la production d’un PV produit par le responsable de la prestation afin d’accompagner la demande de Changement en Production. |
|  | Pour tout passage en Comité d’Approbation des Changements d’une Demande (à l’initiative du Titulaire ou de la Cnam) concernant tout ou partie des solutions hébergées par le Titulaire pour le compte de la Cnam, celle-ci doit être systématiquement notifiée de sa planification (dans le respect des délais de prévenance établis) et de la Décision finale du Comité.  Cette redescente d’information doit être opérée au travers de la comitologie établie entre le Titulaire et la Cnam (et détaillée dans le Plan d’Assurance Qualité). |
|  | Le Titulaire planifie et réalise :   * Les opérations de Mise en Production sans interruption du service. * Les opérations de Mise en Hors-Production sans interruption du service, ou à défaut en dehors des plages de disponibilité prévues dans le présent CCTP   En cas de non-respect, toute indisponibilité est répercutée sur les indicateurs de disponibilité prévus au présent CCTP. En cas de non respects des seuils, la Cnam peut appliquer les pénalités définies au CCAP. |
|  | Les opérations de mises en production doivent être effectuées en accord avec la Cnam et dans les respects des planifications établies.  Le non-respect du planning peut entrainer l’application des pénalités définies au CCAP. |

### Exigences de Recette

|  |  |
| --- | --- |
| Exigences | Description générale |
|  | Les produits (MESDMP et produits connexes) sont testés en sortie de fabrication par le Titulaire, en sortie de recette fonctionnelle et en préproduction dans des environnements fiables et adaptés, incluant les temps. |
|  | Les plans de test et des cas du test du Titulaire doivent être compatibles avec l’outil de la Cnam : HP/ALM.  La livraison par le Titulaire des plans de test, des cas de test et des campagnes de recette doit être faite dans un format qui puisse être intégré automatiquement dans l’outil HP/ALM de la Cnam. |
|  | Les données de tests relatifs à la recette fonctionnelle doivent être pseudonymisées. |
| Katalon | Le Titulaire doit récupérer les scripts Katalon et les mettre à niveau pour accompagner les évolutions réalisées. |
| Tests API | Les API sont testées via Postman. Le catalogue des jeux de données des API doit vivre pour permettre la bonne réalisation des tests. |
| Tests sur médias réels | Concernant la partie mobile, les tests doivent pouvoir être réalisés sur des médias diversifiés (*devices)* réels, en batterie, afin de disposer de résultats plus réalistes. |
|  | Pour pouvoir prononcer l'acceptation, la Cnam vérifie la recevabilité de la livraison au regard des livrables attendus.  Pour être déclarée recevable, la livraison doit remplir a minima les conditions suivantes :   * Exhaustivité des composants livrés, * Les résultats de qualimétrie sont conformes aux attendus de la barrière qualité de la Cnam, * Les développements respectent les normes, exigences et bonnes pratiques indiquées par la Cnam, * La documentation est à jour des dernières modifications, * Les composants sont installables.   Ces conditions sont, le cas échéant, affinées dans le PAQ. |
|  | Pour le cycle en V : Vérification de service régulier (VSR)  La phase de Vérification en Service Régulier (VSR) démarre le lendemain du jour de mise en production, la durée est fixée dans le bon de commande.  La fin de VSR ne peut être prononcée que si l’ensemble des anomalies graves et bloquantes détectées pendant la VSR ont été corrigées, livrées et testées en production. |

### Exigences de Support

#### SUP - Support technique et applicatif

| Exigences | Description générale |
| --- | --- |
|  | Le Titulaire prend en charge le support du MESDMP sur l’ensemble des briques le composant.  Sur le périmètre Hébergement (cf. §7.4 « P2 - PSE – Hébergement ») et Exploitation, le Titulaire assure les niveaux 1, 2, et 3.  Sur le périmètre applicatif et métier, le Titulaire assure les niveaux 2 et 3 (MOE/TMA/HDS). |
|  | Le Titulaire met en œuvre les processus et outil de support en respectant les bonnes pratiques du référentiel ITIL.  Les agents Cnam assurant le N1 et et le Pilotage doivent avoir les accès nécessaires à la gestion des tickets ainsi qu’aux requêtes de suivi. |
|  | Les moyens de communication et les outils entre les utilisateurs, la Cnam et le Titulaire sont finalisés lors de la prestation de prise de connaissance et initialisation de l’accord-cadre.  Néanmoins, le Titulaire doit offrir plusieurs moyens de contact du support pour les agents de l’Assurance Maladie pour ouvrir un ticket d’incident, d’anomalie ou une demande :   * Outil de gestion des tickets (ex. : ClearQuest côté Cnam voir annexes 5 à 8) * Mails * Téléphone   Quelle que soit l’interface, le Titulaire doit émettre en retour un accusé de réception électronique indiquant la bonne prise en compte de l’incident ou de la demande. |
|  | Dans le cas d’un outillage différent autour de la « Gestion des Anomalies / Incidents / Demandes », entre le Titulaire et la Cnam, le Titulaire doit inclure, dans son offre, les moyens d’Inter-connectivités bidirectionnelles avec les outils de la Cnam :   * Outil du Titulaire -> Outil Cnam (ICD) * Outil Cnam (ClearQuest) -> Outil du Titulaire   Les passerelles et « ponts » inter-outils au sein de la Cnam restent du ressort de la Cnam (ICD <-> CleaQuest). |
|  | Jusqu’à mise en œuvre d’un outillage interconnecté pour la gestion des tickets, le Titulaire s’engage à les suivre, les renseigner et faire évoluer leur statut tout au long du traitement de ces dernières, et ce, directement dans l’outil Cnam (ex. : ClearQuest). |
|  | Le Titulaire garantit le maintien de l’inter-connectivité des outils de ticketing en cas de montée de version des produits, d’évolution des besoins ou de changement d’outil (côté Cnam comme côté Titulaire). |
|  | Les moyens du Titulaire doivent s’adapter au niveau d’activité et à la montée en charge du système. |
| Réversibilité | Fournir les éléments permettant de mettre en œuvre une réversibilité au moindre coût en cas de changement de Titulaire de l’accord-cadre de support. |
| Interconnexion avec interrégime | Le Titulaire maintient et garantit l’interconnexion avec l’inter-régime. |
| Gestion du consentement | Gérer le consentement des usagers qui solliciteraient le support par le biais du téléphone et non pas du MESDMP (et qui ne disposeraient pas de courriel). |
| Accès agents | L’accès à l’outil support métier ou à ses interfaces doit être sécurisé par l’identification de l’agent support autorisé. |
| Vérification de l’identité du demandeur | L’outil support doit être capable d’identifier un titulaire/futur titulaire d’un compte MESDMP par son INS mais également sur ses Traits d’identité.  Cette exigence s’applique aussi au demandeur.  Si le demandeur est différent du titulaire ou si le titulaire est mineur, une vérification du consentement ou du lien OD principal / AD doit être effectuée. |
| Création de l’ENS | L’outil doit permettre la création du MESDMP pour certains cas en se basant sur des services de la sécurité sociale et en émettant l’évènement attendu par le service de pilotage MESDMP. |
| Actions sur l’ENS | Pour un titulaire d’un MESDMP sans compte, l’outil support doit permettre de :   * Transmettre la demande de fermeture du MESDMP * Transmettre la demande de réouverture du MESDMP   D’autres actions peuvent être amenées à intégrer cette exigence. |
| Actions sur les données du titulaire | L’outil support doit pouvoir accéder aux données indispensables au titulaire pour l’accès à son compte :   * Modification des coordonnées de contact * D’autres données pourront être intégrées dans cette exigence. |
| Traçabilité des actions | Toutes les actions du support doivent être tracées (qui, quoi, comment et quand). Ces traces doivent être consultables par l’usager. |
| Consultation des traces | L’outil doit être en capacité (via l’api Profil) de consulter les traces concernant les actions effectuées sur le MESDMP d’un titulaire (ceci dès la création), mais également la trace de la notification individuelle et de son éventuelle opposition. |
| Escalade au niveau supérieur | L’outil doit permettre d’informer le niveau de support supérieur en précisant le niveau de criticité de la situation. |
| Indicateurs d’exploitation | Un système de remontée d’indicateurs d’exploitation doit informer le support métier des incidents en cours. |
| Visibilité sur outil | Mettre en œuvre une solution permettant d’avoir une visibilité sur l’outil de ticketing (volume et détail des tickets / qualité) |
| Outil partagé | Mettre en œuvre un outil du marché ou une évolution de PSN1 pour permettre un partage entre tous les acteurs de l’ensemble du périmètre MESDMP . |

#### GDD - Gestion des Demandes

| Exigences | Description générale |
| --- | --- |
|  | Le Titulaire doit utiliser un outillage pour la gestion des demandes.  Dans le cas d’un outil propre au Titulaire, celui-ci doit pouvoir être accessible aux utilisateurs Cnam désignés (création, gestion et suivi des demandes).  Cet outil doit avoir les fonctionnalités suivantes :   * Identification du demandeur * Coordonnées du demandeur * Priorité * Les références du ticket si suite à un incident * L’entité à l’origine de la création du ticket (Titulaire/Cnam et organismes) * La nature du dysfonctionnement * La description * Le dépôt d’une pièce jointe si nécessaire.   Dans le cas d’une création dans un outil propre au Titulaire, un mail est envoyé à l’initiateur Cnam de la demande avec un lien permettant d’accéder à la demande directement dans l’outil du Titulaire.  L’information de la nature de la demande doit apparaitre dans ce mail.  La prise en charge des demandes est couverte dans le cadre des prestations de maintien en conditions opérationnelles des différents systèmes. |
|  | Le Titulaire constitue et met à jour, tout au long de l’accord-cadre, le catalogue des demandes incluant les délais de prévenance et de réalisation.  Les demandes peuvent être formulées par la Cnam pour l’ensemble des environnements techniques mis à disposition par le Titulaire. |
|  | Les demandes réalisées doivent être associées à des procédures de retour arrière potentiel (sauf exception, qui doit être indiquée dans le catalogue des services) et éventuellement leur prise en compte doit pouvoir être différée. |
|  | En cas de demande du Titulaire vers la Cnam, cette demande doit être exprimée dans les outils de la Cnam (Clearquest ou ICD) et adressée avec les informations nécessaires à ces outils pour être conforme aux processus de la Cnam. |
|  | Le processus de Gestion des Demandes doit être détaillé dans le Plan d’Assurance Qualité. |

#### GDI - Gestion des Incidents (ou anomalies)

| Exigences | Description générale |
| --- | --- |
|  | En tant que centre de support, le Titulaire veille au bon renseignement des tickets d’incident (ou anomalie) :   * L’identification du ou des sites concernés, l’identification de l’utilisateur ou de la ligne concernée ; * Une capture d’écran pour une IHM ; * Les références du ticket d’incident ; * L’entité à l’origine de la création du ticket (Titulaire/Cnam et organismes) ; * La cause du dysfonctionnement ; * La date et heure du début du dysfonctionnement ; * La date et heure de la fin du dysfonctionnement ; * La durée totale de dysfonctionnement ; * La sévérité de l’incident (cf. définition dans l’exigence EXG\_GDI\_9); * La description à l’ouverture du ticket ; * La responsabilité de l’incident ; * L’historique des interventions relatives à l’incident ; * Nouvel Incident (ou Anomalie) : Pour tous les incidents (ou anomalies), lors de leur analyse il faut déterminer s’il s’agit d’une régression. * Si des incidents sont liés entres eux (plusieurs signalements pour un même incident), la liste des tickets liés * Si le correctif nécessite la création d’un ticket dans un outil différent, l’identifiant du ticket dans cet outil doit aussi être indiqué afin d’assurer un tracabilité. |
|  | Le Titulaire doit utiliser un outillage pour la gestion des anomalies et des incidents.  Cet outil doit pouvoir s’interfacer avec les outils de gestion de la Cnam (ICD).  Cet outil doit être accessible par les utilisateurs désignés par la Cnam (création, gestion et pilotage des tickets).  L’outil de ticketing doit permettre de :   * Créer, de suivre et de tracer les contacts clients et des incidents, conformément aux engagements de qualité * Gérer la prise en charge et la mise en œuvre des procédures d’escalade tickets vers les niveaux 1, 2, 3 * Gérer plusieurs états du ticket jusqu’à sa clôture * Permettre plusieurs vues des échanges d’un ticket afin que l’utilisateur ne puisse voir que la réponse finale à son ticket |
|  | Si l’anomalie/l’incident est détecté(e) par la supervision :   * La procédure d’ouverture de ticket doit être automatisée pour optimiser les délais de Prise en Compte. * Le Titulaire a également un engagement de proactivité dans l’ouverture des tickets d’incidents et doit en notifier l’ouverture aux équipes Cnam concernées par mail et/ou téléphone / outil de gestion des tickets. |
|  | Le Titulaire a la responsabilité de réaliser le diagnostic initial et le pilotage de la gestion de l’incident jusqu’à sa résolution ; |
|  | En cas d’indisponibilité avérée, le Titulaire produit systématiquement un Rapport d’Incident. Celui-ci doit être rattaché à l’incident dans l’outil de gestion des tickets (visible du pilotage Cnam).  il doit comporter :   * Numéro d’incident/d’anomalie * Date et heure de début / détection / Résolution * Cause / Origine * Impact * Actions de résolution / correction * Plan d’actions ou axe d’amélioration |
|  | Le Titulaire a la charge :   * D’organiser, d’animer et de rédiger les Ordres du jour et les Compte-rendus des différents comités tels que convenus avec la Cnam et détaillés au sein du Plan d’Assurance Qualité. * La périodicité des comités est à adapter en fonction de la situation et de leur nature. * De réaliser des Tableaux de bord de suivi des anomalies et incidents en cours et/ou clôturées, sur des indicateurs de résolutions d’anomalies et d’incidents par typologie, par priorité/sévérité/gravité, temps de résolutions des anomalies et Incidents par Niveaux d’Engagements (SLA), etc.   Ces points sont précisés lors de la prestation P1.1 - Pdc\_Init : Prise de connaissance et Initialisation. |
|  | Le Titulaire a l’obligation de donner l’accès à l’outil de ticketing à des utilisateurs désignés par la Cnam. Ces derniers doivent a minima avoir des habilitations permettant :   * Le suivi opérationnel des tickets (création de tickets, intervention sur leur cycle de vie) * Le pilotage et la génération du reporting nécessaire. |
|  | Le Titulaire a l’obligation de mettre à disposition des agents AM une FAQ, de l’actualiser au fil de l’eau et de mettre à jour une base de connaissance de manière systématique. |
|  | La définition de la sévérité des Anomalies/Incidents de production est la suivante:   * Anomalie/Incident bloquant(e) : * Il s’agit de tout incident ou anomalie de fonctionnement rendant impossible l’utilisation en production des services dans leur ensemble du MESDMP. * Il peut aussi s’agir d’une attaque sécurité avérée. * Il peut également s’agir d’un incident ou d’une anomalie affectant l’intégrité ou la confidentialité ou l’auditabilité du système (c’est-à-dire une anomalie conduisant à fermer l’une des applications du MESDMP). * Il peut également s’agir de la détection d’une vulnérabilité jugée critique par la Cnam (c’est-à-dire une vulnérabilité conduisant à fermer l’une des applications du MESDMP). * Anomalie/Incident grave :   + Il s’agit de tout incident ou anomalie de fonctionnement restreignant l’utilisation en production des services pour tout ou partie de leurs fonctionnalités (hors cas bloquant mentionné ci-avant);   + Il peut également s’agir de la détection d’une vulnérabilité jugée élevée par la Cnam ;   + Il peut s’agir d’une anomalie/incident gênant dont l’occurrence est importante (au-delà de 50 tickets) * Anomalie/Incident gênante :   + Il s’agit de tout incident ou anomalie mineur(e) de fonctionnement permettant toutefois l’utilisation complète en production des services dans l’ensemble de leurs fonctionnalités, même si celle-ci se fait au moyen d’une procédure de contournement.   Pour toute demande de support, d’analyse, de contournement ou de correction formulée par la Cnam au Titulaire, ce dernier est tenu de traiter ces demandes en respectant les délais de réactivité définis ci-après :   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Sévérité | Analyse et correction | | | | | |  | Prise en compte de la demande | Diagnostic | Contournement | Résolution | Rattrapage/ correction données | | | Bloquante | 15mn | 1h | 2h | 4h | 24h | | | Grave | 30mn | 6h | 16h | 24h | 48h | | | Gênante | 4h | 5j | 10j | 48j | 5j | | |
|  | Les différents délais exprimés à EXG\_GDI\_9 se réfèrent tous à l’heure de l’évènement initial :   * Apparition de l’alerte, * Réception du mail de déclaration, * Réception de l’appel de déclaration, * Ouverture du ticket par le déclarant,   À titre indicatif, la prise en compte est considérée opérée dès lors où le ticket a été affecté nominativement à un intervenant dans les équipes du Titulaire.  Les délais sont calculés relativement aux horaires d’ouverture et de disponibilité mentionnés dans le chapitre 6.2.3 Exigences de Disponibilité.  Le processus et les modalités d’échanges relatifs aux demandes de support sont définis dans le Plan d’Assurance Qualité, lors de la prestation P1.1 - Pdc\_Init : Prise de connaissance et Initialisation.  Des calculs d’indicateurs de résolutions (GTR) sont réalisés entre la date et heure de début d’un incident (cf. Heure de l’évènement initial définie ci-dessus) et la date et heure de fin qui correspond à la date et heure de résolution du ticket. |
|  | Dans le cas « d’une anomalie / d’un incident » bloquant(e) où la correction dépend de correctifs non encore disponibles chez l’éditeur ou son mainteneur, le Titulaire doit fournir un plan d’action détaillé dans un délai de 24 heures.  En cas de résolution impossible dans les délais établis ci-dessus, les délais applicables pour les phases ou les opérations de contournement restent en vigueur. |
|  | Le process de Gestion des Incidents (ou Anomalies) doit être détaillé dans le Plan d’Assurance Qualité. |
|  | En cas de non-respect des exigences précisées, la Cnam peut appliquer les pénalités définies au CCAP. |
|  | Dans tous les cas « d’anomalie / d’incident », lors de leur analyse, le Titulaire doit déterminer :   * S‘il s’agit d’une régression; * S’il/elle entre dans le cadre d’une VSR ou non. |

#### GDP - Gestion des problèmes

| Exigences | Description générale |
| --- | --- |
|  | En parallèle de la gestion des incidents, le Titulaire doit mettre en place une gestion des problèmes (au sens ITIL du terme).  Ce service vise à minimiser la récurrence des incidents et leur impact via une gestion et une étude post-mortem des incidents et évènements constatés sur le service fournis.  À ce titre, le Titulaire est responsable de :   * L’identification, l’enregistrement et la classification des problèmes ; * L’investigation et le diagnostic des problèmes ; * La mise à disposition sans surcoût de ressources expert pour effectuer cette dernière tâche ; * La prévention dynamique et proactive des problèmes (analyse des tendances, ciblage des actions de support, etc.) ; * La rédaction de procédures standard de résolution, à destination des centres de services, lorsque la cause d’un problème a été identifiée ; * La correction à la source de l’origine des dysfonctionnements constatés.   La façon dont le Titulaire envisage d’implémenter cette gestion des problèmes ainsi que la comitologie associée est précisée dans l’offre du Titulaire.  De même, le process de Gestion des Problèmes lui-même doit être détaillé dans le Plan d’Assurance Qualité. |

#### CRI - Gestion de Crise

|  |  |
| --- | --- |
| Exigences | Description générale |
|  | Le Titulaire a la responsabilité de mettre en place une cellule de crise pour la gestion des incidents ou des problèmes liés à l’exploitation de la solution ou pour tout autre problème d’exploitation qui sont à définir lors de la P1.1 - Pdc\_Init : Prise de connaissance et Initialisation.  Sur demande argumentée de la Cnam, le Titulaire met en place une organisation de crise dans le but de parvenir à une résolution le plus rapidement possible, en mobilisant rapidement les compétences adéquates.  Une cellule de crise opérationnelle doit être mise en place pour toute indisponibilité de la production dont la résolution est estimée supérieure à 1 heure.  En cas de demande émanant de la Cnam, le Titulaire doit mettre en place la cellule de gestion de crise sous 4 heures après formulation de la demande.  Le Titulaire fournit également les moyens de communication utiles à la circulation de l’information et, en cas de crise, notifie les usagers de l’évolution de l’incident au moins toutes les heures.  Le dispositif de gestion de crise ainsi que les moyens de communication mis en place sont décrits dans l’offre du Titulaire. |
|  | Le process de Gestion de Crise doit être détaillé par le Titulaire dans le Plan d’Assurance Qualité. |

#### IRR - Gestion des irritants

| Exigences | Description générale |
| --- | --- |
| Gestion des irritants | Le Titulaire doit mettre en place un processus de gestion des irritants pour traiter les dysfonctionnements perçus par l’utilisateur (lenteurs, coupures aléatoires, etc.) mais non constatés par les outils de supervision ou non-reproductibles par le Titulaire. Dans ce cas particulier, le Titulaire doit mettre en œuvre les moyens nécessaires permettant de rendre factuel le ressenti utilisateur.  Le processus et les outils de mesure sont détaillés dans l’offre du Titulaire.  Le process de Gestion des irritants doit être détaillé dans le Plan d’Assurance Qualité. |

### Exigences de Gestion des Risques

| Exigences | Description générale |
| --- | --- |
|  | Le Titulaire met en œuvre une Gestion des Risques, dans le respect des standards et bonnes pratiques.  À ce titre, une étude doit être menée lors de la prestation P1.1 - Pdc\_Init : Prise de connaissance et Initialisation afin d’initier une première évaluation des risques pouvant impacter le Projet de mise en œuvre initiale, et le maintien en condition opérationnelle et de sécurité après passage en service continu. Une analyse de ces mêmes risques doit être alors réalisée afin de déterminer les objectifs permettant de rendre les risques acceptables et ainsi tenir les engagements en termes de Planning et de niveaux de services. |
|  | Un tableau de bord est établi par le Titulaire et actualisé régulièrement afin de garantir que les plans d’actions identifiés soient menés à bien, et que tout nouveau risque relevé soit qualifié et adressé.  En annexe un modèle de tableau de bord est fourni pour exemple : « MESDMP\_Annexe 25\_Matrice de Gestion des risques »  Le niveau de risque est préconisé par le Titulaire et doit être validé par la Cnam.  Un point sur la gestion des risques est à réaliser mensuellement en s’appuyant sur le Tableau de bord précédemment cité.  Le process de Gestion des risques doit être détaillé dans le Plan d’Assurance Qualité |
|  | Le Titulaire assure cette gestion des risques avec la norme Ebios (norme utilisée à ce jour).  La Cnam se réserve le droit de changer de méthode. Le Titulaire en est averti sous deux mois pour mise en œuvre de ce changement. |

# Prestations adressées par l’accord-cadre

## Planning indicatif des prestations

Une simulation des prestations à réaliser est présentée ci-après. Elle permet d’illustrer la mécanique des prestations à compter du T0, correspondant à la date de prise d’effet de l’accord-cadre.

Les candidats retenus pour déposer une offre sont invités à proposer une planning qui sera discuté lors des négociations.



Dès la prise d’effet de l’accord-cadre:

* + Démarrage de la prestation P1.1 - Pdc\_Init : Prise de connaissance et Initialisation afin de permettre au Titulaire de prendre connaissance du SI et d’initialiser l’accord-cadre,
  + Démarrage de la pestation P1.2 - Rep : Reprise de l’existant.

Après validation de la reprise de l’existant et de la bascule des services  :

* + Démarrage de la prestation P4 - Trans : Transverse,
  + Démarrage de la prestation P5 - Run\_MCO-S : Run, MCO et MCS afin de permettre au Titulaire d’assurer le Run sur l’ensemble du MESDMP (FO +BO)
  + Démarrage de la prestation P7 - SMS\_Mail : Run SMS et Mail afin de permettre au Titulaire de couvrir l’envoi de SMS et Mail.

Le démarrage des prestations P3 - Conv : Convergence des systèmes MES et DMP et P6 – Homologation NIS/NIS-2 constitue un des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

En parallèle et au cours de l’accord-cadre :

* + Commandes d’unités d’oeuvre à l’initiative de la Cnam au regard des besoins complémentaires à adresser par le Titulaire.

## P1.1 - Pdc\_Init : Prise de connaissance et Initialisation

### Objet

La prestation démarre à la date d’effet de l’accord-cadre et a pour objectif de mettre en place le fonctionnement du Programme MESDMP. Cette prestation consiste notamment, pour le Titulaire :

* + A mettre en place l'organisation et les moyens nécessaires pour assurer les services attendus dans le cadre de l’accord-cadre,
  + A mettre en place la gouvernance et les différents comités/rituels communs avec les équipes de la Cnam,
  + A réaliser la réunion de lancement avec les équipes de la Cnam (kick off), dans le premier mois suivant la date d’effet de l’accord-cadre,
  + A finaliser une première version du PAQ,
  + A finaliser une première version du PAS,
  + A mettre en place les méthodes de travail et outils associés relatifs à l'Agilité, le DevSecOps et le CI/CD,
  + Le cas échéant, si la Cnam décide de ne pas retenir la PSE relative à l’hébergement, à mettre en place les modalités de fonctionnement avec le Centre de Service Hébergement (CSH) de la Cnam dans le cadre de la tranche optionnelle To2,
  + A préparer la phase de convergence des systèmes MES et DMP.

Cette prestation se termine au terme de la bascule des services sous responsabilité du Titulaire, et est remplacée par la prestation P4 - Trans : Transverse.

### Exigences spécifiques

Les exigences sont les mêmes que celle de la prestation P4 - Trans : Transverse (cf §7.6.2).

### Livrables

Les livrables sont listés §7.12 « Liste des livrables principaux » et seront précisés dans le CCTP final.

### Durée et point de départ des prestations

Les prestations démarrent à la date d’effet de l’accord-cadre.

La durée des prestations est estimée à un an.

## P1.2 - Rep : Reprise de l’existant

Les prestations P1.2 - Rep : Reprise de l’existant et P3 - Conv : Convergence des systèmes MES et DMP sont, par nature, intimement liées. La réponse technique à l’une est donc fortement adhérente avec la réponse technique de l’autre.

La stratégie d’enchainement, voire de « recouvrement », entre ces deux prestations fait partie des sujets sur lesquels la Cnam attend particulièrement des propositions de la part des candidats retenus pour déposer une offre, y compris dans sa dimension financière, et qui seront discutées lors des négociations.

### Objet

Cette prestation porte sur la reprise des périmètres MES et DMP existants.

L’offre du Titulaire contient un ou plusieurs scénarios de reprise, ainsi que la mise en œuvre du scénario choisi avec la Cnam pour basculer les services des deux dispositifs (DMP et MES) vers le même datacenter avec des exigences fortes de durée de reprise (**maximum 12 mois à partir de la date de prise d’effet de l’accord-cadre**) et de continuité de service lors de la bascule des services, pour l’ensemble des environnements (Production et hors production).

Le ou les scenarios de reprise proposés font partie des sujets sur lesquels la Cnam attend particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

Le Titulaire doit également traiter la reprise des données de ces deux dispositifs, adapter les outils de supervision, de log, des sauvegardes, des outils d’administration et d’exploitation, des process et outillage de la Gestion des Incidents et Gestion des Changements, et mettre en place les dispositifs de sécurité.

Le Titulaire doit tenir compte de la décision de la Cnam de retenir ou non la PSE relative à l’hébergement.

Le Titulaire conserve le stack technique de MES dans la reprise (et la convergence).

En cas d’hébergement en interne (Tranche optionnelle To2), le Titulaire doit :

1. Identifier très rapidement le pré-requis éxigés à la Cnam afin de tenir les délais de cette reprise et la continuité lors de la bascule des services;
2. Collaborer avec les équipes Cnam pour opérer la reprise de l’hébergement dans les datacenters de la Cnam.

La stratégie de reprise et de bascule des services des deux dispositifs MES et DMP vers l’environement cible (du Titulaire) sont des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

Cette prestation de reprise couvre *a minima* les travaux suivants :

* + La conduite, l’organisation et la planification des prestations de reprise ;
  + Les modalités et le plan de bascule des services ;
  + La reprise et l’adaptation de toute la documentation pour reprise de l’exploitation et de la maintenance des différents composants repris, dont a minima les dossiers d’architecture (HLD, LLD, DAT), les dossiers d’exploitation ;
  + Le transfert de connaissances nécessaire à la réalisation des prestations ;
  + La mise en place des environnements (y compris les environnements de formation, éditeurs LPS, éditeurs pour Store, etc.) et leur homologation nécessaire ;
  + La récupération des éléments logiciels et l’initialisation de la gestion de configuration (développements) dans les nouveaux environnements ;
  + La mise en place de l’automatisation des recettes ;
  + Le CI/CD sécurisé ;
  + Le dispositif sécurité et le SOC ;
  + La supervision (technique et applicative) partagée et accessible par la Cnam ;
  + La mise en place les interconnexions nécessaires ;
  + La mise à disposition du personnel adéquat pour permettre la reprise de connaissances, qualifier les modes opératoires de reprise ;
  + L’apprentissage du pilotage de l’exploitation ;
  + La planification de l’engagement et du désengagement des équipes afin de permettre la transition.
  + Le pilotage global de la prestation de reprise de l’existant (avancement, planning, risques, etc.).

La reprise doit être sans impact sur les critères de disponibilité, d'intégrité, de confidentialité et d'auditabilité (DICA) pour les utilisateurs des services.

Toutes les étapes relatives aux transferts et aux manipulations des données doivent se dérouler en gardant un niveau de sécurité au moins équivalent à celui mis en place dans le cadre de l’hébergement de données de santé.

Ceci implique notamment :

* + L’utilisation de canaux de transfert dédiés et sécurisés par l’usage de certificats serveurs de part et d’autre des plateformes sources et cibles ;
  + Le chiffrage des données qui vont transiter par ces canaux ;
  + De s’assurer de la conservation de l’intégrité des données transférées entre la plateforme source et la plateforme cible.

Il est précisés que le dispositif contractuel propre à chacun des cédants est fondé sur une réversibilité comportant trois phases :

* + La première phase d’initialisation adresse la préparation de la Réversibilité vers le Repreneur (i.e le Titulaire).
  + La deuxième phase vise à exécuter la réversibilité selon les termes de la reprise. A l’issue de cette phase, le Repreneur reprend de manière opérationnelle les services et est responsable de la qualité de service avec l’accompagnement des cédants.
  + La troisième phase porte sur un désengagement des cédants avec un soutien ponctuel pendant une période de 3 mois, après la bascule des services.

Il est précisé que la durée cumulée des phases 1 et 2 ne peut pas excéder 12 mois.

Les détails de l’existant MES infrastructure et sécurité sont présentés dans l’annexe « MESDMP\_Annexe 09\_Documents-Réversibilité sortante MES ».

### Le cadre organisationnel

Le Titulaire nomme un responsable opérationnel de la reprise qui travaille en étroite collaboration avec les directeurs de projet de la Cnam et les responsables opérationnels des cédants.

Un groupe de travail est mis en place dès le début de la prestation. Celui-ci rassemble les équipes du Titulaire, des cédants et de la Cnam. Le Titulaire met en place un avancement hebdomadaire (risques, livrables, suivi des activités, tableaux de bord, etc.) et un comité de pilotage mensuel dédié à la reprise de l’existant (arbitrages, suivi global, consolidation planning, présentation des éventuels difficultés, etc.).

Le Titulaire met en place une organisation miroir, y compris s’agissant du profil des intervenants, à celle des cédants pour faciliter le transfert de connaissances sur l’ensemble du perimètre.

### Appropriation des connaissances

Le transfert des connaissances concerne plusieurs axes :

* + L’appropriation du code source ;
  + L’exploitation courante de l’application ;
  + La connaissance métier / fonctionnelle du service ;
  + La connaissance de l’architecture technique ;
  + L’appropriation des moyens de tests, de la matrice de test ;
  + La gestion des phases de validation et la relation avec les Éditeurs.

Le plan de transfert est proposé par le Titulaire et validé par la Cnam.

### Récupération des tickets d’incidents

Le Titulaire met en place les moyens nécessaires pour reprendre l’historique de l’ensemble des incidents, anomalies, problèmes ayant eu lieu sur la plateforme concernant le SI.

Le Titulaire est seul responsable de l’intégration des données fournies dans ses systèmes de gestion.

Ces données reprises sont exploitables (recherche, filtres, édition, changement de status, etc.) et constituent la base historique des tickets d’incidents.

### Récupération des tests automatisés

La Cnam est attentive à la mise en place de tests automatisés pour fiabiliser la qualité des réalisations et permettre un déploiement continu du projet. Le rapport positif des tests automatisés est une condition nécessaire à toutes mises en production.

Une attention particulière est apportée à la reprise intégrale du patrimoine de test (scénarii fonctionnels et techniques, données de test, etc.) mis en place sur les SI, afin de mettre en œuvre opérationnellement les tests fonctionnels, de performance et de sécurité dès la phase de reprise.

### Récupération des données

Une migration des données existantes et des traces actuellement en production doit être réalisée vers le dispositif du Titulaire.

Cette migration doit se faire :

* + Sous réserve du respect des droits des patients (transfert des dossiers) et des conditions de sécurité ;
  + Sans interruption ou interruption minimale des services MES et DMP (service 24/7) aux Professionnels de santé ;
  + Avec le positionnement d'une information d'indisponibilité de service à destination des Usagers, s'il y a interruption.

### Reprise des outils de monitoring des systèmes

La reprise doit inclure la mise en place des outils de monitoring de l’ensemble du système pour reprendre a minima, et à l’identique, les éléments monitorés et supervisés dans les systèmes existants.

La supervision doit permettre d’alerter en cas de variation importante ou d’absence de volume sur l’ensemble des traitements afin de detecter un comportement inhabituel, même en cas de bon fonctionnement.

Le pilotage Cnam doit avoir accès à ces informations en temps réel pour s’assurer du bon fonctionnement des services et accéder aux volumétries/avancements des traitements.

L’ensemble des éléments doivent être monitorés y compris la couche d’hébergement, le cas échéant, si la Cnam décide de retenir la PSE relative à l’hébergement.

Les éléments a monitorer sont notamment :

* + L'infra réseau, serveur et de stockage,
  + Les bases de données, les VM, les POD,
  + Les topics kafka,
  + Les sauvegardes,
  + Les événements usagers / PS,
  + Les flux applicatifs entrants / sortants
  + etc.

### Mise en oeuvre d’une plateforme d’intégration continue et de déploiement continu afin de reprendre le patrimoine MES et DMP

La livraison des développements validés doit être faite en flux continu.

La reprise doit inclure la mise en place d’une plateforme d’intégration continue et de déploiement continu permettant d’avoir l’intégralité des développements validés continuellement accessible par la Cnam.

#### Description générale de la forge d’intégration et de déploiement continus

La forge CI/CD constitue l’outillage technique nécessaire à la mise en œuvre opérationnelle du processus DevSecOps. Elle est constituée d’un pipeline CI/CD (intégration continue, déploiement continu) complètement automatisé. Chacun de ses composants est dédié au projet et n’offre des services qu’aux systèmes d’information adressés par le présent CCTP. Son accès est protégé par les mêmes moyens de protection que le reste des composants du projet : pour y accéder, il faut disposer d’un poste géré par un SIA (système d’information d’administration) et traverser les bastions. Les composants de la forge sont tous regroupés dans une zone sécurisée nommée « zone outils », cette zone étant uniquement interconnectée avec les différents environnements avec lesquels elle a besoin de communiquer pour intégrer les composant du SI et les déployer dans les différents environnements d’exécution de production et hors production cibles.

Les communications entre cette « zone outils » et ses adhérences avec le monde extérieur constitué des environnements de production, des environnements hors production, des bastions et des réseaux d’administration, sont protégées par des pare-feux ne laissant transiter que les flux nécessaires et suffisants à son bon fonctionnement.

#### Processus

Le processus DevSecOps, décrit par ailleurs dans le présent CCTP, s’appuie sur la forge CI/CD. Les modalités d’imbrication des outils de la forge CI/CD avec le processus DevSecOps sont décrites dans l’offre du Titulaire.

#### Exigences fonctionnelles

La forge CI/CD est un outillage complètement automatisé, qui inclut des validations à chaque étape du processus d’intégration et de déploiement.

Cette forge bloque tout déploiement incorrect par l’intermédiaire d’une phase d’exécution de tests de non régression, de tests unitaires et de tests fonctionnels automatisés. Elle bloque, en outre, tout déploiement en cas d’erreur rapportée par un des outils qui la composent (erreur de compilation, d’édition de liens, d’intégration, absence d’une dépendance, etc.).

Elle permet à l’inverse une intégration et un déploiement sans aucune intervention humaine, quand tous les tests se sont déroulés avec succès et que tous les outils qui la composent indiquent avoir réalisé correctement leurs tâches respectives.

Tous les accès de la forge à des dépôts de binaires externes sont réalisés via l’intermédiaire d’un outil de gestion de dépôts de binaires et par l’intermédiaire d’un relai (proxy applicatif) dédié à la forge, afin de contrôler l’accès aux ressources externes sollicitées et de disposer de traces des activités CI/CD.

La forge met en œuvre des mécanismes de garantie d’intégrité des codes source produits par les développeurs et des binaires produits par les outils d’intégration (ex. : les images Docker). L’offre du Titulaire détaille les mécanismes qu’il met en œuvre pour atteindre cet objectif, en mettant en avant sa capacité à s’aligner avec les moyens et méthodes à l’état de l’art.

La forge met en œuvre des mécanismes automatisés pour identifier les vulnérabilités présentes dans les sources, dans les dépendances rapatriées ainsi que dans les binaires produits (images Docker par exemple). L’offre du Titulaire détaille les mécanismes qu’il met en œuvre pour atteindre cet objectif, en mettant en avant sa capacité à s’aligner avec les moyens et méthodes à l’état de l’art.

#### Exigences techniques

La forge respecte le même schéma de haute disponibilité que le reste du système d’information. Elle est donc en haute disponibilité multi-sites. Elle peut néanmoins être résiliente en mode actif / passif plutôt qu’en mode actif / actif. En cas de perte d’un site, elle doit pouvoir fonctionner sur l’autre site de manière autonome.

Les outils de cette forge doivent à tout moment être déployés dans une version maintenue par la communauté sous-jacente quand il s’agit d’un logiciel libre ou par un éditeur dans les autres cas. Ainsi, le Titulaire met à jour ces outils pour assurer cette exigence. En outre, la stratégie de mise à jour vers une version récente, quand plusieurs versions d’un même outil sont maintenues, est précisée dans l’offre du Titulaire. Les arguments permettant de comprendre la pertinence de la stratégie mise en œuvre par le Titulaire, au regard des exigences de maintien à l’état de l’art et d’innovation affichées par la Cnam, sont précisées dans son offre. Si un outil n’est plus maintenu, le Titulaire doit proposer à la Cnam plusieurs alternatives, éclairer la Cnam sur l’alternative la plus à même de reprendre la fonction réalisée par l’outil qui disparaît, et faire évoluer la forge en y substituant l’outil dont le support disparaît par le nouvel outil choisi par la Cnam, en prenant soin d’éviter toute interruption du service CI/CD.

#### Outillage

Pour chaque outil, l’acquisition des licences et autres éventuels abonnements et actifs nécessaires à son fonctionnement est réalisée par le Titulaire et reste à sa charge, sauf quand le contraire est expressément précisé.

La forge est construite autour d’un pipeline intégrant les outils suivants :

* + L’outil SCA nommé « OWASP Dependency Check », ou un outil similaire, permettant de détecter les vulnérabilités publiques connues et présentes dans les dépendances externes intégrées au code développé spécifiquement dans le projet. La base des vulnérabilités publiques utilisée par l’outil doit être mise à jour quotidiennement. Dans le cas du choix d’un outil similaire, les avantages apportés par ce choix, tant en terme de disponibilité, de performances, de niveau de qualité du service rendu et d’innovation sont précisés dans l’offre du Titulaire.
  + L’outil SonarQube d’analyse de la qualité du code et de la sécurité, ou un outil similaire. Dans le cas du choix d’un outil similaire, les avantages apportés par ce choix, tant en terme de disponibilité, de performances, de niveau de qualité du service rendu et d’innovation sont précisés dans l’offre du Titulaire.
  + L’outil de parcours statique de code source (« static scan ») en vue de détection de vulnérabilités, édité par la société Fortify. Les licences sont fournies par la Cnam.
  + L’outil d’analyse orientée sécurité d’images Docker nommé Trivy, ou un outil similaire. Dans le cas du choix d’un outil similaire, les avantages apportés par ce choix, tant en terme de disponibilité, de performances, de niveau de qualité du service rendu et d’innovation sont précisés dans l’offre du Titulaire.
  + L’outil de gestion de code source GitLab. La version, version CE (édition communautaire) ou de la version EE (entreprise), est précisée dans l’offre du Titulaire accompagnée de l’argumentaire sur le choix de la version.
  + L’outil d’orchestration de pipelines CI/CD nommé Jenkins.
  + Le coffre-fort de gestions des secrets de Hashicorp.
  + L’outil Helm de déploiement de « charts » en environnement OpenShift.
  + L’outil Maven pour compiler et créer des archives à partir de sources Java.
  + L’outil Ansible pour enchaîner des « playbooks » de déploiement ou de mise à niveau de systèmes distants. Dans son offre, le Titulaire précise, dans son offre, s’il adjoint la console Tower associée à l’outil Ansible, et argumente son choix.
  + Le dépôt de binaires Nexus de Sonatype, ou un outil similaire. Dans le cas du choix d’un outil similaire, les avantages apportés par ce choix, tant en terme de disponibilité, de performances, de niveau de qualité du service rendu et d’innovation sont précisés dans l’offre du Titulaire.
  + L’outil Katalon d’automatisation de tests, ou un outil similaire. Dans le cas du choix d’un outil similaire, les avantages apportés par ce choix, tant en terme de disponibilité, de performances, de niveau de qualité du service rendu et d’innovation sont précisés dans l’offre du Titulaire.

Pour chacun des outils libres de la liste d’outils précédente dont il existe une version communautaire et une version soumise à licences, la version choisie par le Titulaire est précisée dans son offre accompagnée de l’argumentaire sur le choix de la version.

Les outils proposés par le Titulaire pour atteindre au mieux les exigences fonctionnelles et techniques indiquées précédemment sont définis dans son offre. Le Titulaire explicite clairement les fonctions apportées et le mode d’intégration des outils complémentaires dont il enrichit le pipeline CI/CD.

#### Cycle de vie des environnements

Le Titulaire précise comment la forge CI/CD est mise à profit pour créer ou supprimer automatiquement et rapidement un nouvel environnement (environnement à prendre au sens production, pré-production, développement, tests, etc.), en cas de besoin. La création et la préparation (i.e. le « provisionning ») de machines virtuelles, ou de nœuds OpenShift, ou encore de « namespace » au sein d’un cluster OpenShift existant, font partie intégrante du périmètre des tâches à réaliser lors de la création d’un nouvel environnement. Si des limitations existent dans l’automatisation de la création ou de la suppression automatique d’un environnement, le Titulaire justifie en détail les étapes qu’il réalise alors de manière manuelle au cours du processus de création/suppression d’un environnement.

#### Indicateurs

Le Titulaire collecte et consolide des indicateurs issus de l’outillage de la forge, il les rassemble au sein de tableaux de bords réalisés pour et présentés à chaque comité DevSecOps. Des exemples de tableaux de bord de ce type sont fournis dans son offre accompagnés d’un argumentaire sur leur pertinence vis-à-vis des objectifs de sécurité et d’agilité.

Ces indicateurs doivent notamment permettre de suivre l’évolution de l’état des développements logiciels et des bibliothèques adhérentes intégrées au sein du SI, en montrant par exemple l’évolution des quantités de bugs, de suspicions de code incorrect (« code smells »), de taux de code dupliqué, de bibliothèques tierces vulnérables, et tout autre indicateur quantitatif que le soumissionnaire peut juger adéquat de produire, selon différentes dimensions :

* + Dimension temporelle, par ex. au fil des déploiements ou selon l’évolution des numéros de version du code,
  + Dimension technique, par ex. par branche de code (développement, alpha-release, pre-release, release, etc.),
  + Dimension fonctionnelle, par ex. par dépôt de sources, ou par groupe de dépôts participant à la réalisation d’une fonction spécifique.

Les indicateurs peuvent être déclinés par niveau de criticité, quand cela a un sens : la remontée des vulnérabilités peut par exemple prendre la forme d’un indicateur pour les vulnérabilités critiques, un autre pour les vulnérabilités majeures, puis mineures, etc.

### Livrables

Les livrables attendus au titre de cette prestation et mis à jour en fin de prestation de reprise sont :

* + Le PV de la bascule des services des dispositifs DMP et MES sans ou avec interruption minimale du service
  + L’ensemble de la documentation existante mise à jour tenant compte des adaptations et optimisations effectuées dans le cadre de la prestation
  + Le dossier d’architecture décrivant la solution MESDMP
  + Les documents afférents à l’environnement de production et hors production tels que le Dossier architecture technique, la matrice des flux, la matrice d’habilitation, le Dossier d’exploitation, le Dossier de Tests et de Validation (DTV) et tout autre document pour le respect des exigences
  + Une plateforme d’intégration continue
  + L’environnement de production opérationnel avec le parc applicatif fonctionnel
  + Les environnements hors production opérationnels avec le parc applicatif fonctionnel
  + La prise en responsabilité sur le code MES et DMP par le titulaire.

Les livrables sont listés §7.12 « Liste des livrables principaux » et seront précisés dans le CCTP final.

### Exigences spécifiques

| Exigences | Description générale |
| --- | --- |
| Durée de la reprise | Le Titulaire met en œuvre le scénario choisi avec la Cnam pour basculer les deux dispositifs (DMP et MES) vers le même datacenter avec des exigences fortes de durée de reprise (**maximum 12 mois** à partir de la prise d’effet de l’accord-cadre) pour l’ensemble des environnements (Production et hors production). |
| Continuité des services durant la bascule en production | Le Titulaire met en œuvre le plan de bascule de la production MES et DMP garantissant la continuité des services MES et DMP, c'est à dire sans interruption ou avec une durée minimale d'interruption des services. |
| 1ère Phase : Préparation de la reprise | Lors de la 1ère Phase de la reprise : Préparation de la reprise  Le Titulaire construit un plan de reprise global en collaboration avec la Cnam et les cédants, en précisant :   * Les outils, les normes et standards définis par le Titulaire, et validés par la Cnam, pour l’exécution de la reprise ; * Les plannings des opérations de reprise ; * L’inventaire précis des fournitures à reprendre ; * Les modalités de continuité des services et d’exploitation ; * Les modalités de la prise en main de la MCO et de la MCS ; * Les conditions de transfert de droit de propriété des applications développées aux fins de l’accord-cadre, de licences, etc. ; * Les modalités de transfert des clés de chiffrement. |
| 2ème Phase : Exécution de la reprise | Lors de la 2ème Phase de la reprise : Exécution de la reprise  Le Titulaire exécute le plan de reprise construit et validé à l’issue de la phase 1 :   * Réception et appropriation des compétences métier et fonctionnelle ; * Réception et appropriation des compétences technique, sécurité, etc. ; * Réception et appropriation des compétences méthodologiques ; * Réception et appropriation de toutes les fournitures identifiées en phase 1 ; * Mise en œuvre de tous les contextes (développement, intégration, tests, production, etc.). |
| 3ème Phase : Prise de responsabilité par le Titulaire | Lors de la 3ème Phase de la reprise : Prise de responsabilité par le Titulaire  Le Titulaire prend l’entière responsabilité du périmètre au terme de la reprise. Il dispose d’un support des cédants sur une période de trois (3) mois à compter de la reprise du service pour répondre à toute demande d’assistance, même ponctuelle.  Le Titulaire doit se rendre disponible pour participer aux formations et instances de transfert de compétences mis en place par les cédants. |

### Durée et point de départ des prestations

La durée et le point de départ des prestations seront précisés dans le CCTP final.

## P2 - PSE – Hébergement

Les paragraphes suivants décrivent les prestations attendues par le Titulaire, le cas échéant, si la Cnam décide de retenir la PSE relative à l’hébergement.

### Objet

La prestation adresse la mise en œuvre, l’administration et le maintien en condition opérationnelle de l’infrastucture destinée à l’exploitation, au développement et à la maintenance des services MESDMP, comprenant matériels et logiciels pour le Réseau, les serveurs, les sauvegardes/restauration et la sécurité.

En début de prestation P1.1 - Pdc\_Init : Prise de connaissance et Initialisation (cf. §7.2), le Titulaire présente le plan de mise en œuvre de la partie hébergement destinée à la reprise des périmètres existants MES et DMP.

Le candidat s’appuie sur la description de l’intrastructure technique existante (cf §3.2.3 Architecture Technique de MES et §3.4.3 Architecture Technique du DMP) et sur les dossiers d’architecture technique pour présenter une offre dans le cadre de la procédure avec négociation.

L’hébergement fait partie des sujets sur lesquels la Cnam attend particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

Le candidat présente sa solution d’hébergement du MES et du DMP au sein de l’infrastructure de ses Datacenters, et doit tenir compte notamment des impératifs de délai de reprise (i.e voir les exigences de la prestation de reprise de l’existant présentée au §7.3 du CCTP) et de continutité des services. Le plan d’hébergement du candidat doit respecter a minima les exigences spécifiques liées à l’hébergement visées ci-après.

Au cours de la prestation P1.2 - Rep : Reprise de l’existant (cf. §7.3), le Titulaire met en œuvre tous les éléments de l’infrastructure réseau, serveurs et sécurité tels que prévus dans le plan de reprise présenté à la Cnam.

La mise en œuvre des différents services d’hébergement est faite dans le respect des exigences sécurité (cf. PAS).

### Exigences spécifiques

Les exigences d’hébergement définies dans le présent CCTP en lien avec des services particuliers (ex. : Sécurité §6.3.2.3) ainsi que les exigences spécifiques ci-après sont à prendre en compte :

| Exigences | Description générale |
| --- | --- |
| Bâtiments et matériels | Noté Tier 3 ou +, le dispositif du Titulaire se présente en deux Datacenters en actif/actif pour garantir la Haute Disponibilité.  Le dispositif présenté doit disposer d’un site de sauvegardes situé au minimum à 150 km des datacenters principaux permettant la reprise d’activité des services en cas de sinistre majeur.  Les sites hébergeant l’infrastructure doivent être localisés, idéalement, en France métropolitaine, en compatibilité avec les exigences du RGDP et avec les clauses d’audit fixées au CCAP, ainsi que les équipes qui administrent l’infrastructure (communication en langue française avec les équipes de la Cnam). |
| Modèle hébergement | L’hébergement doit être de type « Cloud privé » ou « infrastructure dédiée ». En cas de « Cloud privé », l’hébergement doit être qualifié « SecNumCloud ».  L’engagement du Titulaire pour être à terme qualifié « SecNumCloud » sera apprécié.  En revanche, toute mutualisation de l’infrastructure avec d’autre(s) client(s) est exclue. |
| Réseau – Accès Internet | L’accès Internet doit être redondé et sécurisé (multiples FAI, disponibilité via BGP, anti-DDOS) et garantir une bande passante minimale de 1Gbps. |
| Urbanisation de l’architecture technique | La solution d’hébergement du Titulaire doit être architecturée en respectant les exigences visées au §6.2 « Exigences d’Architecture et d’Exploitation ».  En outre, elle doit garantir une ségrégation parfaite entre les environnements de production et hors production. |
| Protection périmétrique de l'hébergement | Le Titulaire veille à isoler la chaîne de collecte des flux de production (i.e : équipements pare-feu/IPS/WAF/bastion dédiés) des autres contextes de hors production et Editeurs. |
| Dimensionnement | La solution d’hébergement du Titulaire doit être dimensionnée pour assurer la reprise de tous les environnements existants de Production et hors production du MES et du DMP.  Le tableau ci-dessous donne des éléments de dimensionnement en terme de stockage et de nombres de VM des environnements à héberger par rapport la production :   |  |  | | --- | --- | | Contextes à héberger | Ratio Production | | Production | 100% | | Instances Pré-production | 50% | | Instance Editeurs | 20% | | Instance Tests de performance | 30% | | Instances Intégration/Recette | 20% | | Instance Dev | 5% | |
| Valorisation du « Run hébergement » | Le périmètre du Run hébergement concerne l’administration des comptes, l’administration et la supervision des équipements serveurs, réseau et sécurité, des machines virtuelles et la maintenance en conditions opérationnelles du dispositif d’hébergement.  Pour ce « Run hébergement », le Titulaire s’engage à maintenir une capacité d’hébergement selon les métriques suivantes :   * 600 To utiles mensuels **pour la production** dont 400 To en stockage objet et le reste en stockage BDD et fichiers pour moitié. * 300 machines virtuelles exploitées mensuellement **pour la production** * 18 serveurs physiques VMware (ESXI) **pour la production**   Les candidats se basent sur les exigences de dimensionnement pour leur évaluation du coût de l’hébergement (cf. EXG\_PSE\_6 supra).  Les modalités de facturation, fondées sur une montée en charge progressive, et les inducteurs de coûts font partie des sujets sur lesquels la Cnam attend particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.  Le stockage indiqué est utile (hors besoin RAID, hors stockage libre, hors sauvegarde, hors PRA).  Le nombre de machines virtuelles s’entend pour les besoins de l’ensemble de la production, hors PRA. |
| Droit d’accès et CMDB | Le Titulaire communique à la Cnam chaque mois la liste des droits d’accès aux équipements hébergés ainsi que la CMDB. |
| Catalogue de services | Le Titulaire communique à la Cnam, en début de prestation, le catalogue de services d’hébergement et SLA associé.  Ce catalogue couvre a minima le périmètre suivant :   * Les ressources Réseau (raccordement intersites, répartiteur de charge, segmentation, DNS, synchronisation NTP, VPN, MPLS, etc.) * Les ressources techniques (pare-feu réseau, pare-feu applicatif, serveur physique, VM, Conteneurs, stockage fichier, stockage bloc, stockage objet, boîtiers HSM, etc.) * SOC/SIEM * La sécurité (administration des comptes, bastion, gestion des habilitations, SOC/SIEM) * Les services d’administration et de supervision. |
| Outil de gestion des incidents | Le Titulaire s’assure que l’outil de gestion des incidents utilisé dans le cadre de la prestation d’hébergement s’interface avec l’outil de gestion des incidents du périmètre Run applicatif afin de disposer d’une vue globale sur les incidents.  En outre, le Titulaire donne accès à son outil aux équipes de la Cnam. |
| Conformité réglementaire (Cf PAS) | Dans la mesure où les données à caractère personnel traitées sont des données de santé, des obligations spécifiques quant à leur hébergement sont introduites par l’article L. 1111-8 du Code de la santé publique.  Le Titulaire doit-être certifié HDS sur l’ensemble des activités couvertes par la certification HDS, et ce pendant toute sa durée, sans discontinuité temporelle. |

### Livrables

Les livrables sont listés §7.12 « Liste des livrables principaux » et seront précisés dans le CCTP final.

### Durée et point de départ des prestations

La durée et le point de départ des prestations seront précisés dans le CCTP final.

## P3 - Conv : Convergence des systèmes MES et DMP

Les prestations P1.2 - Rep : Reprise de l’existant et P3 - Conv : Convergence des systèmes MES et DMP sont, par nature, intimement liées. La réponse technique à l’une est donc fortement adhérente avec la réponse technique de l’autre.

La stratégie d’enchainement, voire de « recouvrement », entre ces deux prestations fait partie des sujets sur lesquels la Cnam attend particulièrement des propositions de la part des candidats retenus pour déposer une offre, y compris dans sa dimension financière, et qui seront discutées lors des négociations.

### Objet

Les prestations adressées sont notamment les suivantes. Leur contenu est décrit dans le §3.6 « Architecture envisagée à 3 ans (MES + DMP = MESDMP) ».

* + IHMs BSP
  + API Santé PS
  + Ressources Partagées
  + MES – API et Ressources Usagers
  + Socle des fonctions Transverses
  + Convergence des systèmes de diffusion des SMS et mails
  + Convergence, rationalisation des solutions technologiques, et consolidation de leurs instances, mises en œuvre notamment dans le domaine des middleware (Kafka/ActiveMQ. PostgreSQL/Oracle, CI-CD, etc.)
  + Le cas échéant, si la Cnam décide de retenir la PSE : Convergence et rationalisation des infrastructures (Pare-feu réseau, pare-feu applicatif, répartiteurs de charge, segmentation VLAN et plans IP, Serveurs physiques, solutions de stockage, de sauvegarde, Systèmes de virtualisation, gabarits d’instances de VM, Autres thèmes à identifier).

Les prestations relatives à la convergence des systèmes MES et DMP font des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations. Les candidats précisent notamment le périmètre, le calendrier et le coût associé à chacune des prestations. Les prestations doivent intégrer la convergence technologique des deux systèmes actuels DMP et MES.

### Exigences spécifiques

Les exigences seront précisées dans le CCTP final.

### Livrables

Les livrables sont listés §7.12 « Liste des livrables principaux » et seront précisés dans le CCTP final.

### Durée et point de départ des prestations

La durée et le point de départ des prestations seront précisés dans le CCTP final.

## P4 - Trans : Transverse

### Objet

Cette prestation consiste notamment à :

* + Assurer l’organisation globale des prestations conformément aux principes, responsabilités et méthodes décrites dans le présent CCTP et précisés dans le PAQ et l’offre du Titulaire.
  + Ajuster la gouvernance et le suivi de l’accord-cadre à travers les instances de pilotage définies dans le cadre du §5 Cadre organisationnel du CCTP, du PAQ et du PAS.
  + Remonter mensuellement toute non-conformité à la Cnam.
  + Assurer que tous les livrables contractuels, les PAQ, PAS et autres documents (dossiers d’architecture fonctionnelle applicative et technique, matrice des flux, dossier de mise en œuvre et d’exploitation, RGPD, cartographie des données, CMDB, droits d’accès et matrice d’habilitation, analyse de risques) sont mis à jour régulièrement, et communiqués à la Cnam dès mise à jour, et appliqués par l’ensemble des équipes.
  + Effectuer et mettre à jour la Gestion des risques conformément aux stipulations du présent CCTP.
  + Produire les documents de référence et reportings réguliers, intégrant les indicateurs et preuves associés, notamment les inducteurs et les métriques d’usages des services.
  + Assurer le pilotage et le suivi global de l’activité (Produit, Delivery, Releases, Mises en production, MCO et MCS). Il est précisé que dans le cadre d’une commande d’UO le pilotage et le suivi des chantiers et des releases est intégré aux UO.
  + Assurer le fonctionnement de la cellule technique (direction services) pour le maintien en conditions opérationnelles du dispositif. Il est précisé que les ressources de la cellule technique peuvent évoluer dans le cadre d’une commande d’UO, les ressources de la cellule techniques évoluent dans les (nota : les ressources – ex. : les architectes de la Design Authority nécessaires à l’évolution du dispositif - sont intégrées aux UO.
  + Assurer l’automatisation, la sécurisation et le bon fonctionnement de la chaîne de CI/CD.
  + Assurer le bon fonctionnement DevSecOps au sein du programme.

### Exigences spécifiques

| Exigences | Description générale |
| --- | --- |
| Comitologie | Préparer en amont des instances visées au §5 Cadre organisationnel avec support transmis 24 heures à l’avance et fourniture du CR et RIDA de ces instances sous 72 heures. |
| Documentations | Assurer la mise à jour de la base documentaire (PAQ, documents visés dans le PAS, Dossiers d’architecture fonctionnelle applicative et technique, Matrice des flux, Dossier de mise en œuvre et d’exploitation, RGPD, Cartographie des données, CMDB, droits d’accès et matrice d’habilitation, analyse de risques, documents de réversibilité). |
| Indicateurs et inducteurs | La fourniture des indicateurs et inducteurs contractuels doit être accompagnée des preuves nécessaires à la vérification par la Cnam. |
| Gestion des risques | Le Titulaire respecte les exigences en matière de risques conformément au §6.3.6 Exigences de Gestion des Risques. |
| Cellule technique - Design Authority | Le Titulaire doit assurer le fonctionnement de la cellule technique (direction services) pour le maintien en conditions opérationnelles du dispositif. |
| CI/CD | Le Titulaire doit assurer l’automatisation, la sécurisation et le bon fonctionnement de la chaîne de CI/CD |
| DevSecOps | Le Titulaire doit assurer le bon fonctionnement DevSecOps au sein du programme. |

### Livrables

Les livrables sont listés §7.12 « Liste des livrables principaux » et seront précisés dans le CCTP final.

### Durée et point de départ des prestations

La durée et le point de départ des prestations seront précisés dans le CCTP final.

## P5 - Run\_MCO-S : Run, MCO et MCS

### Objet

Le Titulaire met en œuvre les prestations d’exploitation, administration du dispositif, de support, de maintien en conditions opérationnelles (MCO) et de maintien en conditions de sécurité (MCS).

Cette prestation couvre le MCO/MCS des applications reprises (MES, DMP).

Le Maitien en Condition Opérationnelle (MCO) regroupe l’ensemble des opérations nécessaires pour garantir le bon fonctionnement du dispositif MESDMP.

Le MCS (Maintien en Conditions Sécurité) inclut notamment les activité suivantes :

* + Produire la documentation d’une politique de MCS, maintenue à jour tout au long de l’accord-cadre. Cette documentation inclut les procédures de veille de sécurité, de vérification des mises à jour et d’analyse de leurs impacts, les délais d’application des mises à jour et la gestion des exceptions ;
  + Mettre en place une veille sécurité, pour détecter les vulnérabilités affectant les composants du périmètre de l’accord-cadre dès qu’elles sont annoncées publiquement ou de manière plus confidentielle par les constructeurs/éditeurs directement auprès de leurs clients, ou encore quand elles sont signalées par la Cnam au Titulaire ; piloter la mise en œuvre de cette veille ;
  + Appliquer les patch de sécurité et corriger les vulnérabilités dans les délais prévus au présent CCTP ;
  + Appliquer en production et hors production les correctifs de sécurité jugés critiques par la Cnam sous 5 jours calendaires, appliquer les autres correctifs de sécurité sous 30 jours. Ceci ne se substitue pas aux délais exigés pour traiter les incidents et vulnérabilités, puisque le traitement des incidents et vulnérabilités peut être résolu par d’autres moyens que l’application de correctifs, par exemple, par la mise en place de mécanismes permettant d’empêcher que la vulnérabilité soit exploitable ;
  + Faire en sorte que tous les logiciels et matériels utilisés soient maintenus par l’éditeur, le constructeur ou la communauté libre s’il s’agit d’un logiciel libre ;
  + Maintenir et créer de règles de détection d’incidents de sécurité dans le SOC ;
  + Réaliser des Tableaux de Bord des activités MCS ;
  + Mettre à jour la gestion de risques en fonction des activités du MCS.

La prestation couvre, à la date de rédacction du CCTP :

* + 15 millions de comptes MES actifs
  + 3 millions de comptes accédés par mois
  + 20 millions de transactions PS/ES par mois (alimentation MESDMP)
  + 3,5 millions de messages PS envoyés par mois

Les modalités de facturation, fondées sur une montée en charge progressive, et les inducteurs de coûts font partie des sujets sur lesquels la Cnam attend particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

A titre indicatif, le dispositif de gestion du MCO applicatif gère environ 400 tickets par mois répartis comme suit :

* + 75% de tickets traités par le N2
  + 25% de tickets traités par le N3

### Exigences spécifiques

| Exigences | Description générale |
| --- | --- |
| **EXG\_RUN\_1** | Pour la prestation Run, hors services d’hébergement (cf. §7.4 P2 - PSE – Hébergement), le Titulaire s’engage à couvrir l’exploitation et le maintien en conditions opérationnelles des services de MESDMP quel que soit le niveau d’activité sur MESDMP. |
| **EXG\_RUN\_2** | Pour la prestation MCO applicative, le Titulaire s’engage à mettre en place un dispositif organisationnel permettant le traitement des anomalies dans le respect des délais de prise en compte définis au §6.3.5.36.3.5.3 « GDI - Gestion des Incidents (ou anomalies) ». |

### Livrables

Les livrables sont listés §7.12 « Liste des livrables principaux » et seront précisés dans le CCTP final.

### Durée et point de départ des prestations

Les prestations démarrent après bascule des services.

La durée des prestations sera précisé dans le CCTP final.

## P6 – Homologation NIS/NIS-2

### Objet

Le Titulaire doit mettre en œuvre l'ensemble des outils et processus permettant à MESDMP d’obtenir l’homologation NIS. Cette homologation est amenée à évoluer afin de respecter les dernières directives nationales et applicables au contexte du projet (NIS-2).

La démarche proposée par le Titulaire est décrite dans son offre.

Les dispositifs proposés doivent être compatibles avec NIS, puis NIS-2, et être réfléchis en conséquence. La conformité au référentiel NIS, puis NIS-2, doit être intégrée dès le départ (« NIS by design ») et n’est pas soumise à une commande supplémentaire ni incluse dans un autre forfait du présent CCTP.

### Exigences spécifiques

Les exigences seront précisées dans le CCTP final.

### Livrables

Les livrables sont listés §7.12 « Liste des livrables principaux » et seront précisés dans le CCTP final.

### Durée et point de départ des prestations

La durée et le point de départ des prestations seront précisés dans le CCTP final.

En terme de délai, les directives NIS, puis NIS-2, contiennent notamment des exigences pour les Systèmes d'Informations concernés ainsi que les processus et moyens d'exploitation (ex.: le SIA est un moyen d'exploitation), ainsi que les interfaces externes de ces Systèmes d'Informations (ex. : SI CNAM, MSSANTE, les services tiers, etc.).

* + Périmètre de la reprise des systèmes DMP et MES : Lors de la phase de reprise des systèmes d’information DMP et MES, le Titulaire doit proposer des évolutions vers la conformité NIS, puis NIS-2, si cela n'affecte pas la qualité et les délais de la reprise. Une fois la phase de reprise terminée, le Titulaire s'engage à faire évoluer les systèmes repris pour qu'ils soient conformes à NIS, puis NIS-2, tout au long de l’accord-cadre, en respectant les délais prévus par ces directives.
  + Périmètre des processus, moyens d’exploitation et adhérences entre ces SI et d’autres SI : en ce qui concerne les processus et moyens d'exploitation, ainsi que les interfaces externes de ces systèmes d'information, la conformité à NIS, puis NIS-2, est exigée pendant toute la durée d’exécution de l’accord-cadre.

## P7 - SMS\_Mail : Run SMS et Mail

### Objet

La prestation adresse l’émission de notifications auprès des professionnels de santé (PS) existants dans le DMP (SMS et mails). Le Titulaire a la charge de :

* + Génèrer les notifications,
  + Les diffuser auprès des PS.

### Exigences spécifiques

| Exigences | Description générale |
| --- | --- |
|  | Le Titulaire s’engage à générer les notifications au fil de l’eau. |
|  | Le Titulaire s’engage à diffuser les SMS/Mail à partir de la prestation P1.1 - Pdc\_Init : Prise de connaissance et Initialisation jusqu’à la convergence des systèmes de notifications (cf. §7.5 P3 - Conv : Convergence des systèmes MES et DMP). |
|  | Le Titulaire s’engage à produire des indicateurs sur les SMS et mails générés et envoyés (ou transmis à l’opérateur). La liste précise des indicateurs attendus est définie dans le PAQ. |

En cas de non-respect des exigences calculées mensuellement, la Cnam peut les pénalités définies au CCAP.

### Livrables

Les livrables attendus sont notamment :

* + LVR : Indicateurs mensuels de volumétrie et de qualité de la génération et de l’acheminement des SMS et mails précisant :
* Nombre de SMS envoyés par typologie métier;
* Nombre de Mails envoyés par typologie métier.

Les livrables sont listés §7.12 « Liste des livrables principaux » et seront précisés dans le CCTP final.

### Durée et point de départ des prestations

Cette prestation est réalisée dans le cadre de la fabrication et la mise en place des cas d’utilisations métier nécéssitant l’envoi de SMS/Mail.

Le point de départ des prestations seront précisés dans le CCTP final.

La durée de la prestation est de 6 mois renouvelable, sur décision de la Cnam, avec un préavis d’un mois, pendant toute la durée d’exécution de l’accord-cadre.

Les modalités de facturation, fondées sur une montée en charge progressive, et les inducteurs de coûts font partie des sujets sur lesquels la Cnam attend particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

## To1 – Réversibilité (tranche optionnelle)

### Objet

Le Titulaire s'engage à assurer la réversibilité du service (voir 1ère exigence en « 6.3.1 Exigences de réversibilité »).

### Exigences spécifiques

Les exigences sont décrites au sein du présent CCTP, au §6.3.1 Exigences de réversibilité.

### Livrables

Les livrables sont listés §7.12 « Liste des livrables principaux » et seront précisés dans le CCTP final.

### Durée et point de départ des prestations

En cas d’affermissement de la tranche, la date de démarrage est définie dans la décision d’affermissement communiquée par la Cnam.

Le cas échéant, la Cnam complète la prestation par la commande d’UO de Réversibilité (voir §7.11.1 « Catalogue d’UO).

## Prestations à bons de commandes

Le Titulaire s’engage à répondre aux commandes éventuelles des unités d’œuvre (UO) détaillées dans le CCTP.

### Catalogue d’Unités d’œuvre (UO)

Le catalogue d'unités d’œuvre (UO) décrit les prestations pouvant être commandées, par la Cnam, à la survenance du besoin, pendant toute la durée d'exécution de l'accord-cadre.

L’ensemble des frais du Titulaire est inclus dans le prix des unités d'œuvre indiqués en annexe de l’acte d’engagement. Les prix comprennent les coûts de pilotage et de suivi des prestations à bons de commande et les dépenses de toute nature inhérentes à l’exécution des prestations, dont notamment les frais d'hébergement, de déplacement, de logistique. Le Titulaire n’est fondé à réclamer aucun supplément de prix du fait d'une erreur d'évaluation de sa part sur la charge de travail ou les moyens de nature nécessaires à l'exécution des prestations.

Les conditions d’établissement des bons de commande sont décrites dans le CCAP.

Les unités d’œuvre seront détaillées dans l’annexe « MESDMP\_Annexe 03\_Catalogue Unités D’œuvre » du CCTP final.

### Liste des unités d’œuvre (UO)

Le tableau d’UO ci-dessous correspond à une 1ère version des UO prévues.

Il est demandé que les candidats fassent des propositions pour les UO avec l’indication « UO à définir ».

Les UO de cette liste sont des sujets sur lesquels la Cnam attend plus particulièrement des propositions de la part des candidats retenus pour déposer une offre, et qui seront discutées lors des négociations.

| **Phase** | **N° U.O** | **Code U.O** | **Libellé de l'U.O** |
| --- | --- | --- | --- |
| 1 - Cadrage | 1\_1 | CADR\_CAD | Cadrage d'un chantier cycle en V |
| 1\_2 | CADR\_AGILE | Cadrage d'un chantier AGILE |
| 1\_3 | CADR\_EXI | Etude de l'existant |
| 1\_4 | CADR\_PRO | Etude d'Impact liée à une montée de version d'un Progiciel |
| 1\_5 | CADR\_IMPACT | Etude d'Impact liée au changement d'un composant sur lequel s'appuie la solution |
| 1\_6 | CADR\_EXPERTISE | Etude d'expertise technique et fonctionnelle |
| 1\_7 | AN\_USAG | Analyse d’usage |
| 2 - Conception | 2\_1\_S | **(UO A DEFINIR)** | Etude de faisabilité technique - Simple |
| 2\_1\_M | **(UO A DEFINIR)** | Etude de faisabilité technique - moyenne |
| 2\_1\_C | **(UO A DEFINIR)** | Etude de faisabilité technique - complexe |
| 2\_2\_1 | MER\_AGILE\_INIT\_1 | Phase de mise en route - Réalisation Agile |
| 2\_2\_2 | MER\_AGILE\_INIT\_2 | Phase de mise en route - Réalisation Agile et assistance au pilotage Agile |
| 2\_2\_3 | MER\_AGILE\_INIT\_3 | Phase de mise en route - Réalisation Agile et assistance au pilotage en Agilité à l'échelle |
| 2\_3 | CONC\_SFGCEX | Création SFG à partir d'un cas d'utilisation |
| 2\_4 | CONC\_SFGMEX | Modification SFG à partir d'un cas d'utilisation |
| 2\_5 | DEV\_CMREQ | Assistance à la réalisation des SFG |
| 2\_6 | CONC\_CTG | Conception technique générale |
| 2\_7 | CONC\_MAQCRE | Création d'une maquette dynamique |
| 2\_8 | CONC\_MAQMOD | Modifier une maquette dynamique |
| 2\_9 | CONC\_SFDCU | SFD à partir d'un cas d'utilisation |
| 2\_10 | CONC\_SFDEC | SFD sur écran |
| 2\_11 | CONC\_PARAPRO | Spécifications du paramétrage Progiciel |
| 2\_12 | CONC\_CONTINTERF | Spécifications détaillées d'un service. |
| 2\_13 | CONC\_BENCHREAL | Réalisation du Cahier des charges de Bench |
| 2\_14 | CONC\_BENCHMODIF | Mise à jour du Cahier des charges de Bench |
| 2\_15 | CONC\_MIGTECH | Analyse, choix et rédaction de la conception technique de la migration technique d'une application |
| 3 - Développement | 3\_1 | DEV\_RG\_DATA | Implémentation de règle de gestion |
| 3\_2 | DEV\_PARAPRO | Implémentation du paramétrage dans le Progiciel |
| 3\_3 | DEV\_CIHM | Création d'un écran |
| 3\_4 | DEV\_MIHM | Modification d'un écran |
| 3\_5 | DEV\_CSM | Création d'un service métier |
| 3\_6 | DEV\_MSM | Modification d'un service métier |
| 3\_7 | DEV\_CBATCH | Création d'un batch |
| 3\_8 | DEV\_MBATCH | Modification d'un batch |
| 3\_9\_1 | DEV\_EDITION1 | Création ou Modification d'une extraction de données simples |
| 3\_9\_2 | DEV\_EDITION2 | Création ou Modification de documents dématérialisés |
| 3\_10 | DEV\_CMREQ | Création ou Modification de scripts |
| 3\_11 | DEV\_CONSO\_INTERFACE | Consommation d'une interface mise à disposition par une autre application |
| 3\_12 | DEV\_MT | Migration Technique |
| 3\_14\_S | DEV\_AGILE\_SMALL | Développement Agile Small |
| 3\_14\_M | DEV\_AGILE\_MEDIUM | Développement Agile Medium |
| 3\_14\_L | DEV\_AGILE\_LARGE | Développement Agile Large |
| 3\_15\_S | DEV\_AGILE\_MOB\_SMALL | Développement Agile Mobile -Small |
| 3\_15\_M | DEV\_AGILE\_MOB\_MEDIUM | Développement Agile Mobile - Medium |
| 3\_15\_L | DEV\_AGILE\_MOB\_LARGE | Développement Agile Mobile -Large |
| 3\_16\_1 | DEV\_AGILE\_Tuning\_1  **(UO A DEFINIR)** | *[UO / profils niveau 1]* |
| 3\_16\_2 | DEV\_AGILE\_Tuning\_2  **(UO A DEFINIR)** | *[UO / profils niveau 2]* |
| 3\_16\_3 | DEV\_AGILE\_Tuning\_3  **(UO A DEFINIR)** | *[UO / profils niveau 3]* |
| 4 - Recette | 4\_1 | REC\_RFAB | Assistance à la réalisation de la recette Fabricant-Tests Système |
| 4\_2 | REC\_ASSREC | Assistance au support à la recette d'intégration |
| 4\_3 | REC\_ASSRFONC | Assistance au support à la recette fonctionnelle |
| 4\_4 | REC\_ASSBENCH | Assistance au Bench |
| 4\_5 | REC\_ASSRPP | Support à la recette de pré-production |
| 4\_6 | REC\_ALIGREC | Alignement de composants suite changement de socle et/ou d'environnement de recette |
| 4\_7 | REC\_ASSINSTALPRO | Assistance à distance à l'installation de la solution Progicielle sur des environnements (hors production) de la Cnam |
| 4\_9 | E\_REC-RF | Réalisation de la recette fonctionnelle (sur un composant MESDMP |
| 4\_10 | E\_REC-LIV | Recette des prestations par la Cnam et livraison d'une version |
| 5 - Mise en production | 5\_1 | MEP\_ASSINSTALLPRO | Assistance sur site à l'installation de la solution Progicielle dans l'environnement de production |
| 6 MCO | 6\_1 | MCO\_MCMTP | Montée en compétence métier et technique d'une solution externe type Progiciel |
| 6\_2 | MCO\_ELE | Etat des lieux de l'existant |
| 6\_3 | MCO\_ETF | Expertise technique ou fonctionnelle |
| 6\_4 | MCO\_AHO | Astreinte hors plages horaires |
| 6\_5 | MCO\_APPH | Astreinte Prolongation Plage Horaire |
| 6\_6 | MCO\_ISHHO | Intervention hors plage horaires (nuit, weekend ou jour férié) |
| 6\_7 | MCO\_INITPRO | Initialisation Progiciel |
| 6\_8 | MCO\_CTLSPRO | Corrections, tests des anomalies, livraison et support aux utilisateurs d'une solution externe type Progiciel |
| 6\_9 | MCO\_CTLS | Corrections, tests des anomalies, livraison et support aux utilisateurs hors solution externe type Progiciel |
| 6\_10 | MCO\_RESP | Réversibilité Progiciel |
| 6\_11 | MCO\_RES | Réversibilité hors Progiciel |
| 7 - Accompagnement Projets | 7\_1 | PIL\_ASS | Assistance pilotage projet |
| 8 - Services | 8\_1 | E\_SERV\_EDIT | Accompagnement des éditeurs de service numérique en santé dans le référencement de sa solution au Store de l’ENS |
| 9 - Support utilisateurs | 9\_1 | S\_N1\_FORM | Formation d'un agent au support utilisateurs niveau 1 (renfort) |
| 9\_2 | S\_N1\_ASSIST | Support utilisateurs niveau 1 (renfort) |
| 10 - Projets techniques | 10\_1 | T\_ARC | Conception d'architecture technique |
| 10\_2 | T\_ING\_STD | Ingénierie d'infrastructure, ingénierie technique d'applications, ingénierie de base de données standard |
| 10\_3 | T\_ING\_CPX | Ingénierie d'infrastructure, ingénierie technique d'applications, ingénierie de base de données complexes |
| 10\_4\_S | T\_ING\_SEC\_S | Etude des solutions de sécurité - Simple |
| 10\_4\_M | T\_ING\_SEC\_M | Etude des solutions de sécurité - Moyen |
| 10\_4\_C | T\_ING\_SEC\_C | Etude des solutions de sécurité - Complexe |
| 10\_5\_S | T\_CO\_REAL\_SEC\_S | Conception et Réalisation des solutions de sécurité - Simple |
| 10\_5\_M | T\_CO\_REAL\_SEC\_M | Conception et Réalisation des solutions de sécurité - Moyen |
| 10\_5\_C | T\_CO\_REAL\_SEC\_C | Conception et Réalisation des solutions de sécurité - Complexe |
| 10\_6\_S | T\_PIL\_SEC\_TECH\_S | Pilotage de la sécurité et technique - Simple |
| 10\_6\_M | T\_PIL\_SEC\_TECH\_M | Pilotage de la sécurité et technique - Moyen |
| 10\_6\_C | T\_PIL\_SEC\_TECH\_C | Pilotage de la sécurité et technique - Complexe |
| 10\_7 | T\_DC | Intervention technique en Data Center |
| 11 - Innovation | 11\_1 | INNOV\_PANEL | Panelistes |
| 11\_2 | INNOV\_Persona | Définition de persona |
| 11\_3 | INNOV\_Formation\_panel | Formation panel test Utilisateurs |
| 11\_4 | INNOV\_ClubU | Appui au Club Utilisateurs |
| 11\_5 | **(UO A DEFINIR)** | Lead UX [pilotage des UX, recherche UX/benchmarck, veille, etc.] |
| 11\_6 | INNOV\_CommunityMng | Community Manager |
| 11\_7 | INNOV\_DataSc | Data Scientist |
| 12 - Produit | 12\_1 | PRODUIT\_LeadPM  **(UO A DEFINIR)** | Lead PM [équivalent Avengers : UO appui au Product Management et Project Management ; porteur de la transversalité et des adhérences ; soft skills : acteur souple pour trouver solution sans tenir compte de contexte d'organisation] |
| 12\_2 | PRODUIT\_PO-PPO  **(UO A DEFINIR)** | PO et PPO [décharger / accompagner les PO] |
| 12\_3 | PRODUIT\_UX  **(UO A DEFINIR)** | UX transverse |
| 12\_4 | PRODUIT-Rec  **(UO A DEFINIR)** | Prestation recette |
| 13 - Run | 13\_1 | **(UO A DEFINIR)** | UO de valorisation du Run |
| 14 - Réversibilité | 14\_1 | R\_1\_MOIS | 1 mois supplémentaire de réversibilité au-delà de la To1 |

### Grille de lecture du catalogue d'unités d’œuvre

Les unités d’œuvre sont classées par phases sans que cela ne produise d’effet sur les modalités de commande des UO.

La Cnam utilise plusieurs méthodes de pilotage / réalisation des projets notamment «Cycle en V» et «Agile». Certaines phases regroupent des unités d’œuvre de ces deux méthodes, d’autres ne concernent qu’une méthode particulière.

Les différentes phases sont :

1. Cadrage
2. Conception
3. Développement
4. Recette
5. Mise en production
6. MCO/MCS
7. Accompagnement projets
8. Services
9. Support utilisateurs
10. Projets techniques
11. Innovation
12. Produit
13. Run
14. Réversibilité

Chaque unité d’œuvre est décrite par :

* + Sa phase.
  + Son type (regroupements en termes de méthode ou type de prestations attendues).
  + Son code.
  + Son libellé.
  + La charge estimée par la Cnam : cette charge est l’estimation par la Cnam de la quantité de travail à fournir pour la réalisation des prestations objet de l'unité d'œuvre par une équipe interne Cnam.
  + Les entrants : liste d’éléments fournis par la Cnam afin de permettre au Titulaire de réaliser les prestations.
  + Les livrables : liste des éléments à fournir par le Titulaire dans le cadre des prestations. La validation de ces livrables par la Cnam constitue une condition à l’admission des prestations.
  + La métrique définit l'unité de mesure de l'unité d’œuvre (UO). Au sein d'un projet, le Titulaire s'engage à optimiser avec la Cnam, le décompte des unités d'œuvre afin d'obtenir une évaluation juste et sincère des tâches à réaliser couvertes par cette UO. Le Titulaire s'engage à capitaliser sur les livrables déjà produits afin optimiser l'utilisation des unités d'œuvre. Pour le respect de cet engagement, le Titulaire produit systématiquement un état des optimisations avérées, il est adossé à l'État Préparatoire à la Commande.
  + Son(es) profil(s) : type(s) d’intervenant attendu(s) pour la réalisation des prestations objet de l’unité d’œuvre.
  + Sa description (prestations attendues).

### Etat préparatoire à la Commande (EPC)

Le Titulaire fournit un État Préparatoire à la Commande (EPC) qui comprend deux parties :

* + La compréhension des travaux à réaliser intégrant a minima les hypothèses de réalisation (impacts, risques, planning, liste des composants techniques à modifier, liste des documents à modifier, etc.)
  + Le descriptif du type d'UO et de leur nombre correspondant à la valorisation des travaux à réaliser.

|  |  |  |  |
| --- | --- | --- | --- |
| Porteur | Contributeurs | Support | Obligatoire / Facultatif |
| Le Titulaire | L’équipe de réalisation | Modèle d’Etat Préparatoire à la Commande (EPC) | Obligatoire et généralement rédigée en fin de cadrage ou de Sprint 0 |
| Objectif | Fournir à la Cnam des éléments chiffrés lui permettant, après validation, d'émettre un bon de commande.  L’Etat Préparatoire à la Commande (EPC) issu du cadrage donne lieu à une commande de prestations qui vaut engagement. Le Titulaire s’engage à livrer le logiciel convenu, dans les délais convenus, au coût convenu, tels que fixés dans la commande.  En l’absence de communication d’un EPC dans le délai énoncé par la Cnam, cette dernière établit un bon de commande sur le fondement de ses propres estimations. Le Titulaire dispose du délai définit dans le CCAP, à compter de la date de réception du bon de commande, pour faire part de ses observations. Le Titulaire se conforme aux bons de commande qui lui sont notifiés, que ceux-ci aient ou non fait l'objet d'observations de sa part. | | |

NB : En l’absence de communication d’un EPC dans le délai énoncé par la Cnam, cette dernière établit un bon de commande sur le fondement de ses propres estimations. Le Titulaire dispose du délai défini dans le CCAP, à compter de la date de réception du bon de commande, pour faire part de ses observations. Le Titulaire se conforme aux bons de commande qui lui sont notifiés, que ceux-ci aient ou non fait l'objet d'observations de sa part.

### Conditions particulières

#### MCO/MCS

A titre liminaire, il est rappelé que les développements Agile ne génèrent pas de MCO/MCS (cf. §5.3.1.1 « Grands principes agiles »).

Le cas échéant, lorsque le développement, cycle en V, d’un nouveau composant a pour effet d’augmenter le périmètre du MCO et/ou MCS, la Cnam commande des UO de MCO/MCS. Le développement d’un composant qui remplace un composant existant déjà inclus dans le périmètre du MCO/MCS ne fait pas l’objet d’une commande de MCO/MCS.

#### Développements Agile

Le Titulaire assure des affectations de ressources et une organisation permettant de garantir la force de production prévue, en tenant compte des congés et des sollicitations hors développements (Correctifs, etc.). Le Titulaire communique, a minima mensuellement, à la Cnam le détail des ressources affectées et son organisation. La Cnam considère que le Titulaire doit prévoir pour les équipes assurant les développements, et en permanence, les ressources pour tenir compte d’absences de tout ordre et les sollicitations hors développements. Ainsi, la capacité effective de ces ressources doit être constante et linaire pendant toute la durée d’exécution de l’accord-cadre.

## Liste des livrables principaux

Le tableau ci-dessous liste des exemples de livrables attendus dans le cadre des prestations.

Ce tableau sera précisé dans une prochaine du CCTP.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Livrables principaux | Prise de connaissance, Initialisation et Reprise | Transverse | RUN, MCO, MCS | Evolution, expertise | Réversibilité |
| Pilotage |  |  |  |  |  |
| Ordre du jour, Support et Compte rendu et RIDA des toutes les instances de pilotage | X | X |  |  | X |
| Planning Accord-cadre | X | X |  |  |  |
| Tableaux de bords de pilotage (reporting, volumétrie, capacity planning, suivi financier, etc.) |  | X |  |  |  |
| Plan de gestion des risques et plan d'actions associés |  | X |  |  |  |
| Autres livrables de pilotages identifiés dans le cadre de réalisation du PAQ lors de la prestation P1-1 |  | X |  |  |  |
| Dossier Sécurité |  |  |  |  |  |
| Politique de sécurité SI (PSSI) | X | X | X | X | X |
| Analyse de risque de l’accord-cadre | X | X | X | X | X |
| Plan de management de la sécurité SI : Plan assurance Sécurité (PAS) | X | X | X | X | X |
| Audit de conformité avec le référentiel NIS | X | X | X | X | X |
| Audit de conformité avec le référentiel NIS-2 | X | X | X | X | X |
| Plan Assurance Qualité |  |  |  |  |  |
| Plan Assurance Marché | X | X | X | X | X |
| Plan Qualité de Gestion des Evolutions (PQGE) | X | X | X | X | X |
| Plan Qualité de Gestion des Services (PQGS) | X | X | X | X | X |
| Plan de réversibilité en fin de d’accord-cadre (PR) | X | X | X | X | X |
| Convention de service (CS) | X | X | X | X | X |
| Plan de gestion de crise (PGC) | X | X | X |  | X |
| Plan de la qualité de réalisation, intégrant les normes et méthodes fixées, pour assurer la réversibilité en fin d’accord-cadre | X | X | X | X | X |
| En lien avec la production, l'hébergement (le cas échéant) et l'exploitation |  |  |  |  |  |
| Environnement de production | X |  | X | X | X |
| L'ensemble des environnements de MESDMP hors production | X |  | X | X | X |
| Processus de gestion du catalogue de services | X |  | X | X | X |
| Processus de gestion de l'amélioration continue des services | X |  | X | X | X |
| Processus de gestion des configurations | X |  | X | X | X |
| Processus de gestion de la disponibilité | X |  | X | X | X |
| Processus de gestion des évènements | X |  | X | X | X |
| Processus de gestion des incidents | X |  | X | X | X |
| Processus de gestion des problèmes | X |  | X | X | X |
| Processus de gestion des demandes de service | X |  | X | X | X |
| Processus de gestion des irritants | X |  | X | X | X |
| Processus de gestion des risques | X |  | X | X | X |
| Processus de gestion de la supervision | X |  | X | X | X |
| Processus de gestion du niveau de service | X |  | X | X | X |
| Processus de gestion de suivi de la capacité | X |  | X | X | X |
| Processus de gestion de mise en production | X |  | X | X | X |
| Plan de gestion de continuité des activités | X |  | X | X | X |
| Manuel d’installation du système et des interfaces | X |  | X | X | X |
| Plan de conduite du changement | X |  | X | X | X |
| Dossier des normes et règles de développement | X |  | X | X | X |
| Manuel d’installation du système et des interfaces | X |  | X | X | X |
| Mise à jour des incidents et anomalies sous l'outil de ticketing de la Cnam |  |  | X | X | X |
| Procédures automatiques fournies par le N3 pour permettre au N1 de répondre aux demandes de support |  |  | X |  | X |
| Fiche « reflexes » fournies par N2 ou N3 pour permettre au N1 de répondre aux demandes de support |  |  | X |  | X |
| Enrichissement de la base de connaissance et des FAQ |  |  | X |  | X |
| Rapport mensuel des indicateurs de l’accord-cadre |  |  | X |  | X |
| Rapports mensuels et annuel d’activité du N3 médical |  |  | X |  | X |
| Rapports mensuels et annuel d’activité du N3 |  |  | X |  | X |
| Rapports mensuels et annuel d’activité des demandes de services |  |  | X |  | X |
| Dossier D'architecture : Fonctionnelle, Applicative et Technique |  |  |  |  |  |
| Cartographie et Urbanisation de MESDMP | X |  | X | X | X |
| Dossier d'architecture fonctionnelle intégrant les évolutions fonctionnelles référencées par version | X |  |  | X | X |
| Dossier d'architecture applicative et technique (DAAT) intégrant les évolutions référencées par version. | X |  | X | X | X |
| Dossier des interfaces propre à une version avec les impacts sur architectures et les interfaces du SI-ENS | X |  |  | X | X |
| En lien avec l'évolution de la solution |  |  |  |  |  |
| Document d’étude du besoin (DE) comprenant la faisabilité technique |  |  |  | X | X |
| Document d’étude du besoin (DE) comprenant l'impact technique |  |  |  | X | X |
| Backlog |  |  |  | X |  |
| Note de cadrage |  |  |  | X | X |
| Matrice des exigences |  |  |  | X | X |
| Note de calibrage (DE) |  |  |  | X | X |
| Etats préparatoires à la commande (EPC) |  |  |  | X | X |
| Dossier de spécifications fonctionnelles générales | X |  |  | X | X |
| Dossier de spécifications fonctionnelles détaillées | X |  |  | X | X |
| Dossier de spécifications techniques générales | X |  |  | X | X |
| Dossier de spécifications techniques détaillées | X |  |  | X | X |
| En lien avec les tests |  |  |  |  |  |
| Contribution du Dossier recette (LDR) y compris les Plan de test organisationnel Recette fonctionnelle et Pré-production | X |  |  | X | X |
| Matrice de test, Plan de test et cas de test pour chaque phase de test | X |  |  | X | X |
| Jeux de données des différents plans de tests | X |  | X | X | X |
| Campagne de test, bilan et Compte rendu de test pour chaque phase de tests | X |  |  | X | X |
| Matrice de test, plan de test et cas de test pour les tests de performance | X |  | X | X | X |
| Compte rendu des tests de performances | X |  | X | X | X |
| Matrice de test et Plan de tests automatisés de non régression | X |  |  | X | X |
| Matrice de test et Plan de tests automatisés pour le suivi de la performance et de la disponibilité des services | X |  |  | X | X |
| En lien avec la réversibilité |  |  |  |  |  |
| Plans de réversibilité, comprenant les macros plannings et plans d’engagement et désengagement des équipes |  |  |  |  | X |
| Inventaire précis des éléments cédés par le Titulaire y compris les données et les traces |  |  |  |  | X |
| Plannings détaillés de la réversibilité ainsi que les différents bilans sur le déroulement des opérations |  |  |  |  | X |
| Plan de destruction des données post-réversibilité |  |  |  |  | X |
| Composants techniques et fonctionnels liés à la reprise des données |  |  |  |  | X |
| Données de production de MESDMP |  |  |  |  |  |
| Documents fonctionnels, techniques, organisationnels, comptes rendus, historique des évolutions, référentiels constitués, cartographie à jour du périmètre de données |  |  |  |  | X |
| Liaisons intersites avec le dimensionnement suffisant au transfert des données pour toute la durée de la réversibilité |  |  |  |  | X |
| Supports et logistique de formation du personnel du Repreneur |  |  |  |  | X |

# Liste des annexes

xxx : consultable à la Cnam par les candidats retenus pour présenter une offre dans le cadre de la Procedure avec négociation

xxx : remise aux candidats retenus pour présenter une offre dans le cadre de la Procedure avec négociation

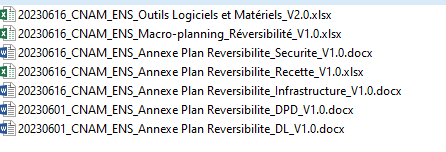
xxx : remise avec une version ultérieure du CCTP

* 1. MESDMP\_Annexe 01 – Personas
  2. MESDMP\_Annexe 02\_PAS
  3. MESDMP\_Annexe 03\_Catalogue Unités D’œuvre
  4. MESDMP\_Annexe\_04\_Documentation technique pour les Opérateurs MSSanté :

<https://mssante.fr/is/doc-technique>

* 1. MESDMP\_Annexe 05 – Manuel Utilisation Clear Quest – FS-FT
  2. MESDMP\_Annexe 06 – Workflow Clear Quest Fiche de Signalement
  3. MESDMP\_Annexe 07 – Workflow Clear Quest Fiche Tiers
  4. MESDMP\_Annexe 08 – Workflow Clear Quest Demande de service
  5. MESDMP\_Annexe 09\_Documents-Réversibilité sortante MES

(Plan de réversibilité de la prestation MES actuelle et ses annexes)



* 1. MESDMP\_Annexe 10\_Inventaire DMP
  2. MESDMP\_Annexe 11\_Description générale des mécanismes de chiffrement
  3. MESDMP\_Annexe 12\_Description détaillée de la protection des données
  4. MESDMP\_Annexe 13\_DMP-Dossier Architecture Applicative et Technique
  5. MESDMP\_Annexe 14\_DMP-Description Technique
  6. MESDMP\_Annexe 15\_MES-Outils Logiciels
  7. MESDMP\_Annexe 16\_MES-Dossier Architecture Logicielle Back-End
  8. MESDMP\_Annexe 17\_MES-Dossier Architecture Logicielle Front-End
  9. MESDMP\_Annexe 18\_MES-VMs Inventaire
  10. MESDMP\_Annexe 19\_MES-Référentiel des composants
  11. MESDMP\_Annexe 20\_MES\_FR-CNAM-ENS-HLD
  12. MESDMP\_Annexe 21\_DMP-AV-HSM
  13. MESDMP\_Annexe 22\_MES-Matrice des flux
  14. MESDMP\_Annexe 23\_PAQ\_Indicateurs\_Exemple de sommaire
  15. MESDMP\_Annexe 24\_Plan d’Assurance Qualité – Exemple de sommaire
  16. MESDMP\_Annexe 25\_Matrice de Gestion des risques
  17. MESDMP\_Annexe 26\_Scénario\_d’audit\_accessibilité
  18. MESDMP\_Annexe 27\_Scénario écoscore
  19. MESDMP\_Annexe 28\_Clients\_rapports\_SI\_PIL-DMP
  20. MESDMP\_Annexe 29\_Codes sources

1. CTI : Centre de traitement informatique

   CEIR : Centre éditique informatique régional [↑](#footnote-ref-2)