 <b>MINISTÈRES SOCIAUX</b> <i>Liberté Égalité Fraternité</i>		<b>Secrétariat général</b> <b>Direction du numérique</b>
	CCTP	

# CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

## Objet du marché

**Fourniture de prestations, de licences associées, d'assistance, de réalisation, de maintenance, de formation, et de support, à la mise en place de systèmes de bulles sécuritaires pour les projets actuels et à venir de la direction du numérique des ministères sociaux « DNUM »**

**(Bulles sécuritaires DNUM)  
PRA007011**

## SOMMAIRE

<b>1</b>	<b>PREAMBULE</b>	<b>1</b>
<b>2</b>	<b>CONTEXTE</b>	<b>2</b>
2.1	PRESENTATION DE LA DIRECTION DU NUMERIQUE DES MINISTÈRES SOCIAUX	2
2.1.1	Missions et activités de la dnum	2
2.1.2	Chiffres clés du système d'information des ministères	3
2.1.3	les enjeux du numérique et des SI en 2020	3
2.2	DES DONNÉES À PROTÉGER	4
2.3	LA VOLONTÉ DE CONSTRUIRE DES OUTILS MUTUALISÉS ENTRE ARS ET /OU POUR LES MINISTÈRES SOCIAUX	4
2.4	DES OUTILS DÉCISIONNELS PARTAGÉS	5
2.5	ARCHITECTURE APPLICATIVE	7
<b>3</b>	<b>OBJET DU MARCHÉ</b>	<b>8</b>
3.1	SCÉNARIOS ET ATTENTES	8
3.2	NATURE ET ENTENDUE DES PRESTATIONS	11
3.3	ACTIVITÉ 1 - INITIALISATION DES PRESTATIONS	12
3.3.1	Objet	12
3.3.2	Description	12
3.3.3	unités d'œuvre de cette activité	13
3.3.4	Modalités de validation	13
3.4	ACTIVITÉ 2 - REPRISE DE L'EXISTANT	13
3.4.1	Objet	13
3.4.2	Description	14
3.4.3	Unités d'œuvre de cette activité	14
3.4.4	Modalité de validation	16
3.5	ACTIVITÉ 3 - MISE EN PLACE DES SCÉNARIOS ET MIGRATION D'UN SCÉNARIO À L'AUTRE	16
3.5.1	Objet	16
3.5.2	Description	16
3.5.3	Unités d'œuvre de cette activité	16
3.5.4	Modalités de validation	20
3.6	ACTIVITÉ 4 - LIVRAISON DES TOKEN UTILISATEURS PAR TRANCHE	20
3.6.1	Objet	20
3.6.2	Description token physique	20
3.6.3	Unités d'œuvre de cette activité – token physique	20
3.6.4	Description token logiciel	20
3.6.5	Unités d'œuvre de cette activité – token logiciel	21
3.6.6	Modalités de validation	21
3.7	ACTIVITÉ 5 - FORMATION	21
3.7.1	Objet	21
3.7.2	Description	21
3.7.3	Unités d'œuvre de cette activité	22
3.7.4	Modalités de validation	22
3.8	ACTIVITÉ 6 – MAINTENANCE CORRECTIVE AU-DELÀ DE LA PÉRIODE DE GARANTIE	22
3.8.1	Objet	22
3.8.2	Description	22

	<b>Bulles sécuritaires DNUM</b>	

3.8.3	l'unité d'œuvre de cette activité .....	23
3.8.4	Modalités de validation .....	23
3.9	ACTIVITE 7 - EXPLOITATION DES BRIQUES DE SECURITE.....	23
3.9.1	Objet .....	23
3.9.2	Description.....	23
3.9.3	Unités d'œuvre de cette activité .....	24
3.9.4	Modalités de validation .....	24
3.10	ACTIVITE 8 – FOURNITURE DE LICENCES .....	24
3.10.1	Objet .....	24
3.10.2	Modalités d'exécution .....	26
3.10.3	Modalités de validation .....	26
3.11	ACTIVITE 9 - ASSISTANCE AU PROJET.....	26
3.11.1	Objet .....	26
3.11.2	Description et unités d'oeuvre de cette activité.....	26
3.11.3	Modalités de validation .....	27
3.12	ACTIVITE 10 - TRANSFERT DE COMPETENCES - REVERSIBILITE.....	27
3.12.1	Objet .....	27
3.12.2	Description.....	28
3.12.3	Unités d'œuvre de cette activité .....	29
3.12.4	Modalités de validation .....	29
<b>4</b>	<b>PILOTAGE ET SUIVI DE PROJET-----</b>	<b>30</b>
<b>5</b>	<b>EXIGENCES EN MATIERE DE SECURITE-----</b>	<b>31</b>
5.1	REGLES GLOBALES .....	31
5.2	ARCHITECTURE .....	32
5.3	IDENTITY ACCESS MANAGEMENT .....	32
5.4	TRACES .....	32
5.5	PROTECTION DES DONNEES (LOGS , TRACES ET DOCUMENTS ECHANGES (DAT, ...)).....	33
5.6	PROTECTION DES COMMUNICATIONS .....	33
5.7	SURVEILLANCE .....	33
<b>6</b>	<b>RACI-----</b>	<b>34</b>
	<b>ANNEXES ET LIENS UTILES-----</b>	<b>35</b>
6.1	GLOSSAIRE.....	35

	<b>Bulles sécuritaires DNUM</b>	

## 1 PREAMBULE

Les Agences régionales de Santé sont désignées dans le présent CCTP sous l'appellation «ARS». Le projet est sous la responsabilité de la direction du numérique du ministère en charge de la santé.

La société retenue pour l'exécution du présent marché est désignée dans le présent CCTP sous l'appellation « TITULAIRE ».

	<b>Bulles sécuritaires DNUM</b>	

## 2 CONTEXTE

### 2.1 PRESENTATION DE LA DIRECTION DU NUMERIQUE DES MINISTÈRES SOCIAUX

#### 2.1.1 MISSIONS ET ACTIVITES DE LA DNUM

Sous l'égide du secrétariat général, la direction du numérique des ministères sociaux (DNUM) porte la transformation numérique pour offrir aux agents comme aux métiers des services fluides et performants et apporter ainsi sa contribution à l'efficacité des politiques publiques.

La DNUM (ex-DSI) des ministères sociaux a été créée par le décret n° 2019-1412 du 20 décembre 2019 portant diverses dispositions relatives à l'administration centrale des ministères chargés des affaires sociales et l'arrêté du 27 décembre 2019 portant organisation de la direction du numérique.

Elle intègre en outre le service à compétence nationale des systèmes d'informations mutualisés des agences régionales de santé (SCN SIM ARS) créé par l'arrêté du 2 janvier 2020.

La DNUM a pour missions :

- De conseiller et d'appuyer la transformation numérique des ministères afin de développer la simplification, la performance et l'offre de nouveaux services au public ;
- De développer, de déployer et de maintenir les produits numériques et projets de systèmes d'information relatifs aux politiques publiques conduites par les ministères et de valoriser le patrimoine de leurs données ;
- De garantir la cohérence stratégique, applicative et technique des systèmes d'information des ministères et de rechercher toutes les mutualisations et optimisations pertinentes en leur sein ainsi qu'au niveau interministériel ;
- De concevoir, de déployer et de mettre en œuvre l'environnement de travail numérique des agents, afin de contribuer à leur efficacité et à leur mobilité, d'assurer le service de support-utilisateur pour l'administration centrale et de le coordonner pour les services territoriaux ;
- De concevoir et de piloter les services d'infrastructures des systèmes d'information, et de veiller à la confiance numérique et à la sécurité des systèmes et des données, en lien avec le haut fonctionnaire de défense et de sécurité ;
- D'assurer, en lien avec les agences régionales de santé, la conception et le pilotage de leurs systèmes d'information mutualisés.

	<b>Bulles sécuritaires DNUM</b>	

Appelée à jouer un rôle déterminant dans la transformation numérique des ministères sociaux, la DNUM a été une des toutes premières directions dans l'ensemble des ministères, à ouvrir un incubateur de services numériques à l'automne 2017. Ce mode de construction des services numériques a montré son efficacité, en permettant d'associer directement les agents porteurs et d'obtenir très vite des résultats ciblés.

La DNUM s'est toujours positionnée dans une perspective interministérielle, elle propose et met en œuvre l'ensemble des mutualisations et optimisations utiles entre les différents périmètres ministériels.

En s'inscrivant dans ce cadre interministériel, la DNUM consacre ainsi des ressources plus importantes aux besoins métiers des ministères sociaux, domaine où la proximité et la connaissance de ces métiers, sont essentielles aux développements de services de qualité et à valeur ajoutée.

### 2.1.2 CHIFFRES CLES DU SYSTEME D'INFORMATION DES MINISTERES

- Une direction du numérique au service d'une vingtaine de délégations ou directions réparties dans quatre secteurs ministériels, mais aussi d'opérateurs tels que l'ASC, le CNG etc.
- Une direction en appui des services territoriaux des ministères sociaux ;
- Une direction de 200 professionnels aux métiers multiples et évolutifs : développement, pilotage des évolutions des SI, management de projets, cycle de vie des applications, appui méthode, qualité, sécurité, assistance aux utilisateurs, etc. ;
- 124 marchés publics actifs ;
- 50 prestataires en appui sur site ;
- 4 700 postes de travail gérés directement en administration centrale ;
- La responsabilité de la cohérence des 30 000 postes de travail que comptent l'ensemble des services coordonnés par la DNUM raccordés au réseau des ministères sociaux ;
- 40 000 boîtes aux lettres de messagerie ;
- Plus de 350 applications ;
- 380 sites raccordés au réseau interministériel de l'Etat (RIE).

### 2.1.3 LES ENJEUX DU NUMERIQUE ET DES SI EN 2020

Le système d'information des ministères sociaux porte aujourd'hui un double enjeu : d'une part impulser la stratégie numérique, tournée vers les agents, les citoyens, les entreprises, les professionnels de santé et les associations, au cœur des métiers de nos ministères, et d'autre part moderniser et fiabiliser son fonctionnement dans un contexte de cyber-menace croissant.

Ces enjeux se déclinent en 2020 sur 4 axes, structurant le plan de travail de la DNUM :

	<b>Bulles sécuritaires DNUM</b>	

- **Conseiller et appuyer la transformation numérique des politiques publiques**
- **Concevoir et développer les produits, applications et services numériques en appui des politiques publiques**
- **Développer l'environnement de travail numérique des agents et fournir les outils quotidiens permettant de gagner en efficacité et en mobilité**
- **Poursuivre le plan de transformation et de sécurisation du système d'information des ministères sociaux**

## 2.2 DES DONNEES A PROTEGER

---

Les projets de la DNUM peuvent héberger des données sensibles qui nécessitent la mise en place de bulles sécuritaires. On trouvera particulièrement (cette liste n'est pas exhaustive) :

- ▶ Les données du PMSI présentes notamment dans les projets Diamant portant sur un recueil pseudonymisé de l'activité hospitalière ;
- ▶ Le résumé de passage des urgences « données sans identifiant » ;
- ▶ Les répertoires nominatifs des professionnels de santé RPPS hébergés dans Diamant ;
- ▶ Les données de santé nominatives recueillies dans le cadre de la crise sanitaire liée au COVID et hébergées dans l'entrepôt national COVID ;
- ▶ Les données anonymes et agrégées issues des bordereaux de cotisations sociales gérées dans le cadre de projets décisionnels ;
- ▶ Les données financières des établissements sanitaires et médico-sociaux ;
- ▶ Les données capacitaires des établissements sanitaires et médico-sociaux ;
- ▶ Etc.

## 2.3 LA VOLONTE DE CONSTRUIRE DES OUTILS MUTUALISES ENTRE ARS ET /OU POUR LES MINISTÈRES SOCIAUX

---

Dans le cadre du schéma directeur du SI des ARS validé en CNP, il a été décidé :

- ▶ De construire un socle fonctionnel et technique commun assurant l'homogénéité, la fiabilité la cohérence des données, et la sécurisation des données ;

	<b>Bulles sécuritaires DNUM</b>	

- ▶ De mettre en œuvre ce socle commun en se basant sur des outils concrets, solides et partagés ;
- ▶ D'inscrire les projets dans une logique de mutualisation permettant le rapprochement des logiques locales, régionales et nationales.

Au moment de la publication du présent appel d'offre, trois systèmes d'information bénéficient d'une bulle sécuritaire :

- DIAMANT ;
- Entrepôt national Covid ;
- Atlasanté.

## 2.4 DES OUTILS DECISIONNELS PARTAGES

---

DIAMANT est un outil :

- ▶ Décisionnel : Les systèmes d'information décisionnel s'articulent autour de quatre grandes fonctions que sont la collecte, le stockage, la distribution et l'exploitation de données disponibles dans des sources distinctes :
- ▶ Collecte, nettoyage et consolidation des données : cette fonction permet d'extraire les données des systèmes de production et de les adapter à un usage décisionnel.
- ▶ Stockage : cette fonction permet de centraliser les données structurées et traitées afin qu'elles soient disponibles pour un usage décisionnel.
- ▶ Distribution : cette fonction permet de faciliter l'accessibilité des informations selon les fonctions et les types d'utilisation.

DIAMANT offre aux décideurs des ARS des données fiables, actualisées, en infra annuel leur permettant de suivre les établissements de santé, publics comme privés, sous leur responsabilité :

- ▶ Sur le Portail DIAMANT, l'utilisateur accède aux tableaux de bord et aux fonctions d'analyse ;
- ▶ En sus du Portail, les « Cubes » DIAMANT offrent à l'utilisateur expert la possibilité d'approfondir les analyses via des requêtes ad hoc ;
- ▶ Inter-ArS : il est fondé sur un principe de mutualisation des meilleurs pratiques, des moyens et des ressources pour définir, développer, héberger et exploiter l'outil décisionnel pour les adhérentes. Initiative de 4 ARH à l'origine, le projet fédère à ce jour l'ensemble des ARS ;
- ▶ Maîtrisé : Il fournit aux directeurs et à leurs équipes, via une série de tableaux de bord et d'indicateurs sélectionnés et organisés ;
- ▶ des données et informations significatives (taux de référence, tendances, évolution, comparaison...) relatives à l'activité, au domaine financier, à la qualité ;
- ▶ des alertes leur permettant d'objectiver et d'orienter le processus de décision ;



	<b>Bulles sécuritaires DNUM</b>	

- ▶ Il constitue un support au dialogue au sein même des agences et avec les établissements de santé publics et privés dans le cadre des négociations et des suivis (CPOM, CREF, Autorisations...). La mise en visibilité et le partage de l'information favorise en effet les échanges entre les acteurs ;
- ▶ Il met à disposition des indicateurs annuels (tableaux de bord dits stratégique), et infra annuels ;
- ▶ **ANTicipation** : les décideurs sont en capacité de mesurer les écarts, et d'anticiper la non-réalisation des objectifs fixés (EPRD, CPOM). La mise à disposition en infra annuel de données transverses et l'anticipation des dérives éventuelles permet d'engager/promouvoir les actions nécessaires au redressement des situations jugées critiques et de les suivre.

### **Entrepôt national Covid et AtlaSanté**

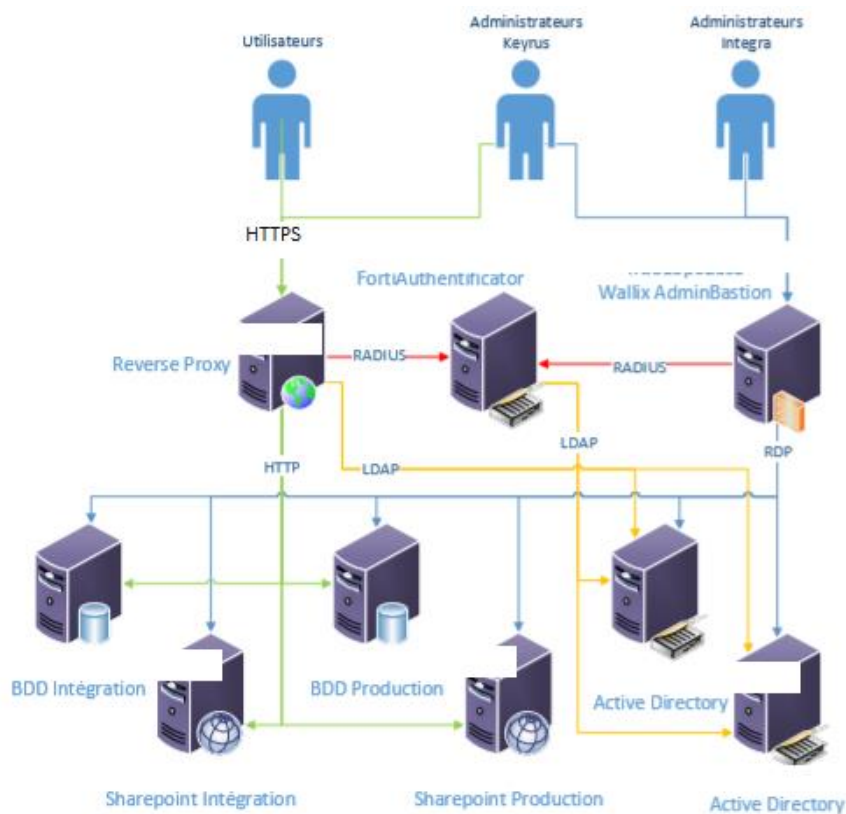
Ce système reçoit des sources assurance maladie et laboratoires (SI-DEP) en lien avec le SARS-COV-2, virus COVID19, il est en cours de transformation vers de nouveaux objectifs.

## Bulles sécuritaires DNUM

### 2.5 ARCHITECTURE APPLICATIVE

L'architecture bulle sécuritaire actuelle de DIAMANT est la suivante :

**Le schéma ci-après décrit l'architecture Diamant. L'architecture d'Entrepôt covid est sensiblement similaire.**



Il faudra retenir à la lecture du chapitre 3 du présent document que :

- Diamant se situe en scénario 2, scénario intermédiaire ;
- Vaccins et Entrepôt Covid en scénario 3, scénario élevé ;
- AtlaSanté qui est sous la même bulle sécuritaire qu'entrepôt est en scénario 1.

	<b>Bulles sécuritaires DNUM</b>	

### 3 OBJET DU MARCHÉ

Le présent marché a pour objet de sécuriser les infrastructures et les applications gérant des données sensibles par une bulle sécuritaire.

Pour ce faire, plusieurs scénarios sont envisagés pour définir les conditions dans lesquelles le TITULAIRE assure les prestations demandées conformément aux documents contractuels. Le principe de l'accord cadre à bons de commandes est donc retenu au travers d'unités d'œuvre qui seront commandées au fur et à mesure des besoins.

Le présent marché repose sur architecture fonctionnelle dite des 3 tiers :

- Un tiers qui développe et exploite
- Un tiers qui héberge
- Un tiers qui pose un bastion sur les serveurs à protéger « l'objet du présent marché »

Ainsi les projets qui seront mis sous bulle sécuritaire disposent en dehors de ce marché d'un hébergeant HDS, et d'une maîtrise d'œuvre. La maîtrise d'œuvre et l'hébergeant accèdent aux données. L'objet du marché est de mettre en place des bulles sécuritaires permettant de superviser les actions réalisées sur les données mais sans y accéder. **Le titulaire ne peut être juge et partie.**

**L'hébergement et la maîtrise d'œuvre des projets à protéger sont hors périmètre du présent marché.**

En conséquence, l'hébergeant et la maîtrise d'œuvre ne peuvent répondre à la présente sollicitation.

#### 3.1 SCENARIOS ET ATTENTES

L'objectif de la mise en place d'une bulle sécuritaire est de se conformer aux exigences du référentiel de sécurité du SNDS pour les projets liés ou non aux données SNDS.

Le concept de bulle sécuritaire envisagé consiste à mettre en place un système de traçage vidéo-logiciel des opérateurs manipulant les données des systèmes ciblés. Ce système est selon les scénarios adossé à un accès avec authentification forte. Dans tous les cas de figure, un bastion sécurise l'accès des maîtrises d'œuvre aux données.

L'accord cadre à bons de commandes pour la mise en place de bulles sécuritaires prévoira trois scénarios : un scénario a minima, un scénario intermédiaire et un scénario élevé.

Dans la suite de ce document :

- On entendra par maîtrise d'œuvre, les équipes d'administrateurs des systèmes, de développeurs et d'administration de l'hébergement.
- Le périmètre à tracer « video logiciel » pour la maîtrise d'œuvre portera sur toute manipulation de données arrivant par FTP sécurisé puis déversées dans la base de données serveur (serveur de développement, serveur de test et de production) jusqu'à leur chargement dans les cubes décisionnels ou dans les systèmes tiers

	<b>Bulles sécuritaires DNUM</b>	

«autre technologie» ainsi que tout traitement réalisé par la suite par la maîtrise d'œuvre sur le périmètre des projets ciblés.

- Le Titulaire devra reprendre l'existant des trois projets couverts par trois bulles sécuritaires et réaliser à la demande du pouvoir adjudicateur, pour chaque nouveau projet nécessitant une bulle sécuritaire, les prestations commandées pour mettre en œuvre le scénario correspondant.
- La base installée de bulles sécuritaires de la DNUM repose sur Wallix et Fortinet.

	<b>Bulles sécuritaires DNUM</b>	

**Le scénario a minima (1) prévoit :**

Pour la Maitrise d'Oeuvre (5 utilisateurs, potentiellement 5 simultanés) :

- ▶ une surveillance vidéo-logiciel de type wallix / traçabilité de type wallix à construire par le titulaire pour les accès aux données sur le SFTP et aux données hébergés en base SQL serveur, postgres,...
- ▶ Une authentification forte de type Token / sur Radius ou équivalent à construire par le titulaire.

Pour les utilisateurs des systèmes ciblés :

- ▶ hors périmètre du présent appel d'offres

**Le scénario intermédiaire(2) prévoit :**

Pour la Maitrise d'Oeuvre (5 utilisateurs, potentiellement 5 simultanés) :

- ▶ Une surveillance vidéo-logiciel de type wallix / traçabilité de type wallix à construire par le titulaire pour les accès à l'ensemble des serveurs de la plateforme, ...
- ▶ Une authentification forte de type Token / sur Radius ou équivalent à construire par le titulaire

Pour les utilisateurs des systèmes ciblés, pour 10 utilisateurs

- ▶ **Une authentification forte de type Token / sur Radius ou équivalent à construire par le titulaire**

**Le scénario élevé (3) prévoit :**

Pour la Maitrise d'œuvre (5 utilisateurs, potentiellement 5 simultanés) :

- ▶ une surveillance vidéo-logiciel de type wallix / traçabilité de type wallix à construire par le titulaire pour les accès aux données sur le FTP et aux données hébergés en base SQL serveur, postgres,...
- ▶ Une authentification forte de type Token / sur Radius ou équivalent à construire par le titulaire

Pour tous les utilisateurs, pour 5 utilisateurs,

- ▶ **Une surveillance vidéo-logiciel de type wallix / traçabilité de type wallix à construire par le titulaire**
- ▶ Une authentification forte de type Token / sur Radius ou équivalent à construire par le titulaire

NB les token seront des dispositifs physiques token ou token sur mobile ou PC. L'utilisation des token sur PC est à utiliser en dernier recours (lorsque les deux autres modalités sont impossibles) car son niveau de sécurité est inférieur aux précédentes.

Pour chacun des scénarios le titulaire est responsable de la fourniture d'une prestation sur le champ qui lui est dévolu par le scénario. Cette prestation complète inclut installation, licences, paramétrage, formation, garantie d'un an. Les briques correspondants à l'outil de traçabilité vidéo-logiciel ainsi que l'outil de gestion de l'authentification forte seront hébergés sur un espace virtualisé dédié distinct de l'environnement de production, de développement et de recette, ou sur l'environnement de développement et de recette.

	<b>Bulles sécuritaires DNUM</b>	

Les outils installés ne devront pas perturber tant la maîtrise d'œuvre que la qualité de service offerte aux utilisateurs des projets en production.

**Au-delà des paramétrages nécessaires pour les produits wallix et Fortinet, des développements sur mesure sont à effectuer pour l'authentification forte.**

**L'authentification est à double facteur : login password et OTP Fortinet.**

**En effet les utilisateurs qui devront utiliser l'authentification forte Fortinet accèdent à des systèmes qui ne connaissent pas le mode cession. Il peut s'agir de TCD Excel accédant en HTTPS à des cubes SSAS sous MS-BI, ou à des projets WEB ne connaissant pas le mode cession, ou autres solutions ne connaissant pas le mode cession.**

***Le titulaire devra pour chaque bulle réaliser les développements permettant à fortinet de maintenir une cession ouverte pendant classiquement 4 heures ou pendant une durée qui sera spécifiée par le pouvoir adjudicateur. Ces développements à la charge du titulaire font partie intégrante des UO SCN1, SCN2 et SCN3. Ces développements seront réalisés en logiciel libre sur des serveurs en OS libres que le titulaire aura spécifié. Pour ces développements le titulaire devra avant réalisation proposer plusieurs scénarii au pouvoir adjudicateur. La durée estimée de ces développements, indépendamment des processus d'installation et de paramétrage varie de 25 à 35 jours ouvrés***

## 3.2 NATURE ET ENTENDUE DES PRESTATIONS

Le projet concerné par cet appel d'offres, est donc exclusivement réservé au domaine sécuritaire.

Les durées sont définies en jours ouvrés.

Les activités sont réalisées dans les locaux du TITULAIRE avec des réunions à la DNUM des ministères sociaux.

Tous les livrables documentaires sont à transmettre à la DNUM au format électronique sur la suite Microsoft 2016, ou ultérieur.

Les charges de pilotage doivent être incluses dans chacune des prestations décrites ci-dessous.

Il convient de préciser que :

Chaque bulle est autonome. Le wallix, le Fortitoken et le reverse proxy de chaque bulle ne sont pas mutualisés avec une autre bulle. Les projets de bulles sont clairement séparés.

Les différents firewalls, anti-DOS, WAF, antivirus, EDR, et SIEM et autres protections internet sont du ressort de l'hébergeant c'est-à-dire hors procédure.

	<b>Bulles sécuritaires DNUM</b>	

Chaque projet dispose de son organisation pour distribuer des token aux utilisateurs finaux. Le titulaire met à disposition les tokens et forme le distributeur de token à la gestion des tokens.

Les composants Wallix/Fortitoken/reverse proxy sont hébergés sur des Machines virtuelles fournies par l'hébergeur HDS. Le titulaire devra gérer l'exploitation et la sécurité de ces équipements (MCO/MCS). L'accès VPN à ces équipements est obligatoire.

La DNUM devient propriétaire des licences que le titulaire fournit.

### 3.3 ACTIVITE 1 - INITIALISATION DES PRESTATIONS

#### 3.3.1 OBJET

Cette activité a pour objet de permettre au TITULAIRE de fixer l'organisation et les moyens à mettre en œuvre pour exécuter les différentes prestations, de s'approprier la connaissance et de prendre en compte les caractéristiques techniques et fonctionnelles de l'environnement des projets de la DNUM.

Les activités des UO INIT 1 et 2 sont parallélisées (CF UO).

#### 3.3.2 DESCRIPTION

Le TITULAIRE s'engage, conformément à son offre, à réaliser les prestations suivantes :

- ▶ Organisation de la réunion de lancement et présentation des intervenants désignés pour l'exécution du marché ;
- ▶ Confirmation de l'équipe définitive chargée de réaliser le présent marché, correspondant aux profils proposés dans l'offre du TITULAIRE ;
- ▶ Prise de connaissance de l'environnement technique :
  - Architecture technique,
  - Organisation de la documentation des livrables,
  - Etat des lieux,
  - Composants techniques qu'il va livrer.

Pendant la phase d'initialisation des prestations, la DNUM s'engage à mettre à disposition du TITULAIRE la documentation existante à savoir les DAT (Documentation d'architecture technique.)

A l'issue des activités INIT 1 et 2 (CF Unités d'Œuvre), le TITULAIRE remet à la DNUM le Plan Assurance Qualité en mettant à jour le PAQ contenant à minima :

- ▶ La formalisation des relations entre la DNUM et le TITULAIRE ;
- ▶ Les normes de qualité de production des livrables ;
- ▶ Les processus de validation des livrables ;
- ▶ Les indicateurs de suivi et de pilotage des prestations du marché ;

	<b>Bulles sécuritaires DNUM</b>	

- ▶ La définition des modalités de coordination entre le TITULAIRE lui-même et les TITULAIRES externes et/ou internes en charge des différents domaines d'activité ;
- ▶ Les méthodes d'analyse des risques détaillées en précisant le rythme d'analyse ;
- ▶ Les méthodes pour les tests unitaires et la recette des livrables.

### 3.3.3 UNITES D'ŒUVRE DE CETTE ACTIVITE

Code de l'unité d'œuvre	Prestation	Livrables	Délai maximum de production des livrables à compter de la notification du bon de commande (jours ouvrés)
INIT1	Lancement	-Support de la réunion de lancement -compte-rendu de la réunion de lancement ; - liste nominative des intervenants du TITULAIRE pour la durée du projet et leurs C.V. correspondant aux profils prévus dans son offre.	5
INIT2	Prise de connaissance environnement	- liste des questions posées au client et des réponses fournies par celui-ci ; - bilan de la prise de connaissance comprenant : l'évaluation des compétences acquises relatives à l'application, l'estimation du degré d'autonomie, la liste des tâches effectuées en collaboration avec les ARS, les remarques ou les réserves du TITULAIRE sur les éléments manquants ou insuffisants ; - méthodologie retenue pour préparer et réaliser les prestations objet du marché ; - PAQ finalisé à partir du PAQ fournit dans la réponse du candidat - Planning mis à jour - Connaissance des composants disponible acquise	7

### 3.3.4 MODALITES DE VALIDATION

La validation de la prestation donne lieu à l'établissement d'un procès-verbal de service fait. En cas de dépassement des délais fixés, le Ministère applique les pénalités prévues à cet effet dans le CCAP.

## 3.4 ACTIVITE 2 - REPRISE DE L'EXISTANT

### 3.4.1 OBJET

Cette activité, a pour objet de permettre à un nouveau TITULAIRE de reprendre les trois bulles sécuritaires Diamant, Vaccins, Entrepôt Covid et AtlaSanté et d'assurer la continuité du service fournie par ces bulles.



	<b>Bulles sécuritaires DNUM</b>	

### 3.4.2 DESCRIPTION

Le titulaire dispose à compter de l'émission du bon de commande d'au plus 45 jours calendaires pour s'approprier les plateformes actuelles sans altérer les services de production. Le pouvoir adjudicateur remet au titulaire les DAT des deux bulles à l'initialisation des prestations.

A l'issue des 45 jours, le titulaire produit un document explicatif pour chaque bulle décrivant les opérations nécessaires pour apporter une modification sur la bulle. A l'appui du document, le pouvoir adjudicateur est en mesure d'évaluer l'appropriation.

### 3.4.3 UNITES D'ŒUVRE DE CETTE ACTIVITE

Code de l'unité d'œuvre	Prestation	Livrables	Délai maximum de production des livrables à compter de la notification du bon de commande (jours ouvrés)
REX-A	Prise de connaissance et appropriation de l'ensemble de l'architecture	Le titulaire décrit l'architecture existante et propose un schéma général d'exploitation des trois bulles sécuritaires	7

Code de l'unité d'œuvre	Prestation	Livrables	Délai maximum de D'appropriation
REX-D	Reprise de la bulle DIAMANT	Le titulaire est opérationnel sur la compréhension du fonctionnement de la bulle DIAMANT et son exploitation. Il est à même de prendre en compte des demandes d'évolution. Le titulaire produit un document explicatif pour chaque bulle décrivant les opérations nécessaires pour apporter une modification sur la bulle.	15

Code de l'unité d'œuvre	Prestation	Livrables	Délai maximum de D'appropriation
REX-S	Reprise de la bulle Vaccin	Le titulaire est opérationnel sur la compréhension du fonctionnement de la bulle Vaccin, et son exploitation. Il est à même de prendre en compte des demandes d'évolution Le titulaire produit un document explicatif pour chaque bulle décrivant les opérations nécessaires pour apporter une modification sur la bulle	15

Code de l'unité d'œuvre	Prestation	Livrables	Délai maximum de D'appropriation
REX-E	Reprise de la bulle entrepôt Covid	Le titulaire est opérationnel sur la compréhension du fonctionnement de la bulle entrepôt Covid et son exploitation. Il est à même de prendre en compte des demandes d'évolution Le titulaire produit un document explicatif pour chaque bulle décrivant les opérations nécessaires pour apporter une modification sur la bulle	15

	<b>Bulles sécuritaires DNUM</b>	

	<b>Bulles sécuritaires DNUM</b>	

#### 3.4.4 MODALITE DE VALIDATION

La validation de la prestation donne lieu à l'établissement d'un procès-verbal de service fait. En cas de dépassement des délais fixés, le Ministère applique les pénalités prévues à cet effet dans le CCAP.

### 3.5 ACTIVITE 3 - MISE EN PLACE DES SCENARIOS ET MIGRATION D'UN SCENARIO A L'AUTRE

#### 3.5.1 OBJET

Mise en place du scénario retenu. Le choix de chaque scénario est réalisé par l'administration au travers de bon de commande de l'UO correspondante au scénario

#### 3.5.2 DESCRIPTION

Le TITULAIRE rédige le dossier de mise en place du scénario commandé, ou de la migration de scénario commandé, en conformité avec l'existant et s'assure de la couverture des exigences exprimées par la DNUM.

Les éléments à décrire dans ce dossier, sont les suivants (à adapter selon le périmètre du bon de commande traité) :

- ▶ L'intégration des nouvelles briques logiciel du titulaire sur l'ensemble des espaces de stockage du système ;
- ▶ Les évolutions sur la partie autorisations et habilitations ;
- ▶ L'évolution de l'architecture ;
- ▶ Les impacts sur l'historisation et l'archivage ;
- ▶ Les impacts des nouvelles fonctionnalités sur les aspects reprises sur incident ;
- ▶ ...

#### 3.5.3 UNITES D'ŒUVRE DE CETTE ACTIVITE

##### Mise en place des scénarios

**Pour chacun des scénarios ou passage d'un scénario à l'autre, le titulaire est responsable de la fourniture d'une prestation sur le périmètre qui lui est dévolu par le scénario. Cette prestation complète inclut installation, licences, paramétrage, formation, garantie d'un an. Pour chaque livraison le titulaire fournit un dossier d'architecture et un dossier de recette. La DNUM se réserve le droit de compléter le dossier de recette.**

Les UO SCN 1, 2 et 3 sont des UO de construction (build) de bulles et de formation à leur usage. Ces UO ne comprennent pas la maintenance et l'exploitation des bulles (principes du build et du run). En conclusion, ces UO sont des UO de build.

Si une nouvelle bulle est commandée, le pouvoir adjudicateur commandera une UO SCNX et les UO Maint et Expl. sauf abandon du projet suite à la construction (build).

	<b>Bulles sécuritaires DNUM</b>	

Code de l'unité d'œuvre	Niveau de complexité	Composition	Livrables	Délai maximum de production des livrables à compter de la notification du bon de commande (jours ouvrés)
Unité d'œuvre des scénarios				
SCN1	Faible	Mise en place du scénario 1 L'UO SCN1 inclut les licences qui lui sont associées et nécessaires à son exécution	Fourniture des prestations d'assistance, de réalisation et installation, de maintenance, de formation, à la mise en place d'un système de Bulle sécuritaire sur le système décisionnel pour <b>le scénario 1</b> . La cotation de cette UO inclut la fourniture de 5 token physiques ou logiciels sur mobile, pour la maîtrise d'œuvre.	30
SCN2	moyen	Mise en place du scénario 2 L'UO SCN2 inclut les licences qui lui sont associées et nécessaires à son exécution	Fourniture des prestations d'assistance, de réalisation et installation, de maintenance, de formation, à la mise en place d'un système de Bulle sécuritaire sur le système décisionnel pour <b>le scénario 2</b> . La cotation de cette UO inclut la fourniture de 5 token physiques ou logiciels sur mobile pour la maîtrise d'œuvre. (La cotation des token utilisateurs apparait dans des UO spécifiques)	30
SCN3	Moyen	Mise en place du scénario 3 L'UO SCN3 inclut les licences qui lui sont associées et nécessaires à son exécution	Fourniture des prestations d'assistance, de réalisation et installation, de maintenance, de formation, à la mise en place d'un système de Bulle sécuritaire sur le système décisionnel pour <b>le scénario 3</b> . La cotation de cette UO inclut la fourniture de 5 token physiques ou logiciels sur mobile pour la maîtrise d'œuvre et 5 pour les	30

	<b>Bulles sécuritaires DNUM</b>	

Code de l'unité d'œuvre	Niveau de complexité	Composition	Livrables	Délai maximum de production des livrables à compter de la notification du bon de commande (jours ouvrés)
			utilisateurs. (La cotation des token utilisateurs apparait dans des UO spécifiques)	
Unités d'œuvre de migration d'un scénario à l'autre				
SCN1V2	moyen	Passage du scénario 1 vers le scénario 2	Dès lors qu'un scénario a été livré, il se peut que des dispositions réglementaires ou des décisions de l'administration centrale, nous amènent à migrer d'un scénario à l'autre dans le cadre de ce marché. <b>Enfin il est fort probable que le déroulé des scénarios soit lié à une montée en charge progressive de la sécurisation d'une nouvelle bulle lors des processus d'homologation.</b> Aussi le candidat cotera dans le cadre de ces 3 UO le cout respectif de chacune de ces migrations. Lors de ces opérations de migration, Le titulaire intervient en binôme avec la maitrise d'œuvre afin de garantir la qualité des paramétrages de cette migration. (La cotation des token utilisateurs apparait dans des UO spécifiques)	25
SCN1V3	moyen	Passage du scénario 1 vers le scénario 3		25
SCN2V3	faible	Passage du scénario 2 vers le scénario 3		15
			Pour ces trois UO, le titulaire fournit un dossier de migration ainsi qu'un plan de recette de migration, la DNUM se réserve le droit de	

	<b>Bulles sécuritaires DNUM</b>	

Code de l'unité d'œuvre	Niveau de complexité	Composition	Livrables	Délai maximum de production des livrables à compter de la notification du bon de commande (jours ouvrés)
			compléter le dossier de recette.	

	<b>Bulles sécuritaires DNUM</b>	

### 3.5.4 MODALITES DE VALIDATION

La validation de la prestation donne lieu à l'établissement d'un procès-verbal de service fait. En cas de dépassement des délais fixés, le Ministère applique les pénalités prévues à cet effet dans le CCAP.

## 3.6 ACTIVITE 4 - LIVRAISON DES TOKEN UTILISATEURS PAR TRANCHE

### 3.6.1 OBJET

Le candidat devra fournir les coûts des token par tranche. Chaque coût s'établit dès lors que la tranche inférieure sera consommée.

### 3.6.2 DESCRIPTION TOKEN PHYSIQUE

Fourniture de token physiques par paquets de 20 pour chaque tranche

Pour cette unité d'œuvre le titulaire appliquera les délais de livraison. Ces derniers peuvent être inférieurs au maximum exigé, s'il l'a prévu dans son offre. Dans le BPU, le titulaire le prix correspond à 20 token physiques dans chaque tranche.

### 3.6.3 UNITES D'ŒUVRE DE CETTE ACTIVITE – TOKEN PHYSIQUE

Code de l'unité d'œuvre	Niveau de complexité	Description	Livrables	Délai maximum de livraison à compter de la notification du BC (jours ouvrés).
Cout par tranche				
TOK1P20	NA	Livraison de token pour 40 à 100 token	Livraison de token(s) Physiques par paquets de 20, <b>le prix indiqué dans le BPU portera sur le cout de fourniture de 20 token</b> , prix incluant le cout de livraison à la DNUM ou à son représentant par pli recommandé.	7
TOK2P20	NA	Livraison de token pour 101 à 500 token		7
TOK3P20	NA	Livraison de token pour 501 à 1000 token		7
TOK4P20	NA	Au-delà de 1001 token		7

### 3.6.4 DESCRIPTION TOKEN LOGICIEL

Fourniture de token logiciels sur mobile ou sur PC par lot de 20 pour chaque tranche

	<b>Bulles sécuritaires DNUM</b>	

Pour cette unité d'œuvre le titulaire appliquera les délais de livraison prévus au marché. Ces derniers peuvent être inférieurs au maximum exigé, s'il l'a prévu dans son offre. Dans le BPU, le prix correspond à 20 token logiciel dans chaque tranche.

### 3.6.5 UNITES D'ŒUVRE DE CETTE ACTIVITE – TOKEN LOGICIEL

Code de l'unité d'œuvre	Niveau de complexité	Description	Livrables	Délai maximum de livraison à compter de la notification du BC (jours ouvrés).
Cout par tranche				
LTOK1P20	NA	Livraison de token pour 20 à 500 token	Livraison de token(s) sur téléphone mobile ou PC par paquets de 20, <b>le prix indiqué dans le BPU portera sur le cout de fourniture de 20 token</b> , prix incluant le cout de livraison	7
LTOK2P20	NA	Livraison de token pour 501 à 1000 token		7
LTOK3P20	NA	Livraison de token pour 1001 à 1500 token		7
LTOK4P20	NA	Livraison de token pour 1501 à 2000 token		7
LTOK5P20	NA	Livraison de token pour plus de 2000 token		7

### 3.6.6 MODALITES DE VALIDATION

La validation de la prestation donne lieu à l'établissement d'un procès-verbal de service fait. En cas de dépassement des délais fixés, le Ministère applique les pénalités prévues à cet effet dans le CCAP.

## 3.7 ACTIVITE 5 - FORMATION

### 3.7.1 OBJET

Le TITULAIRE forme de nouvelles personnes de la maitrise d'œuvre au-delà de la formation incluse dans les scénarios SCNXX. Les formations auront lieu dans les locaux de la maitrise d'œuvre ou en distanciel.

### 3.7.2 DESCRIPTION

Les prestations attendues sont les suivantes : Réalisation des formations techniques à l'usage des briques installées.



	<b>Bulles sécuritaires DNUM</b>	

### 3.7.3 UNITES D'ŒUVRE DE CETTE ACTIVITE

Code de l'unité d'œuvre	Niveau de complexité	Description	Livrables	Délai maximum de mise à disposition d'un formateur
Formation Utilisateur				
FORM1	Moyen	Formation de la maîtrise d'œuvre sur le site de la maîtrise d'œuvre à l'usage des briques que le titulaire a installés	Formation	15
FORM2	Moyen	Formation avancée de la maîtrise d'œuvre sur le site de la maîtrise d'œuvre à l'usage des briques que le titulaire a installés	Formation avancée proposant des pistes d'améliorations dans le cadre de l'usage des briques installées	15
REDACE	Moyen	Mise à jour de la documentation en cas de changement de version des briques installées	Document de formation	15

### 3.7.4 MODALITES DE VALIDATION

La validation de la prestation donne lieu à l'établissement d'un procès-verbal de service fait. En cas de dépassement des délais fixés, le Ministère applique les pénalités prévues à cet effet dans le CCAP.

## 3.8 ACTIVITE 6 – MAINTENANCE CORRECTIVE AU-DELA DE LA PERIODE DE GARANTIE

### 3.8.1 OBJET

Cette activité a pour objet de définir les conditions dans lesquelles le TITULAIRE assure les évolutions et les corrections pendant et au-delà de la période de garantie. Une UO spécifique « UO Maint » est déclenchée dès lors que la période de garantie expire.

### 3.8.2 DESCRIPTION

La prestation de maintenance évolutive comporte :

- ▶ l'étude et le diagnostic des anomalies ;
- ▶ les propositions de solutions de contournement ;
- ▶ la correction ;
- ▶ les tests de non-régression et la livraison ;
- ▶ la mise à jour de la documentation ;
- ▶ la gestion de la configuration des composants du système maintenu.
- ▶ Durée de l'UO Maint 1 an.

Le service est ouvert aux heures de travail, les jours ouvrés 8H-18H.

	<b>Bulles sécuritaires DNUM</b>	

Les délais de correction des anomalies sont les suivants :

Type d'anomalie	Définition des niveaux de priorité	Délai maximum de prise en compte	Délai de fourniture d'une correction ou solution de contournement
Anomalie bloquante	anomalie rendant impossible l'utilisation d'une ou plusieurs fonctionnalités de DIAMANT	1 jour	1 journée
Anomalie majeure	anomalie autre que bloquante impliquant un fonctionnement en mode dégradé d'une ou plusieurs fonctionnalités du système	1 Jour	5 jours ouvrés
Anomalie mineure	Désigne toute demande de modification du système par rapport à sa spécification	1 jour	10 jours ouvrés

### 3.8.3 L'UNITÉ D'ŒUVRE DE CETTE ACTIVITÉ

L'UO **Maint** permet de disposer d'un support et d'intervention en cas d'anomalie pendant un an au-delà de la période de garantie. En termes d'évaluation de charge, le titulaire devra intervenir jusqu'à 5 jours dans l'année, au-delà une unité d'œuvre d'assistance sera déclenchée.

NB : l'UO Maint ne couvre pas les coûts de maintenance logicielle des bulles sécuritaires.

### 3.8.4 MODALITÉS DE VALIDATION

La validation de la prestation donne lieu à l'établissement d'un procès-verbal de service fait. En cas de dépassement des délais fixés, le Ministère applique les pénalités prévues à cet effet dans le CCAP.

## 3.9 ACTIVITÉ 7 - EXPLOITATION DES BRIQUES DE SÉCURITÉ

### 3.9.1 OBJET

Cette activité a pour objet de définir les conditions dans lesquelles le TITULAIRE assure l'exploitation des briques de sécurité installées sur une durée d'un an et en assure la supervision.

### 3.9.2 DESCRIPTION

La prestation d'exploitation comporte :

- ▶ Le maintien en conditions opérationnelles des briques de sécurité ;
- ▶ La supervision à distance des briques de sécurité ;
- ▶ La gestion de la configuration et la mise à niveau des composants du système de sécurité ;
- ▶ La mise en place d'évolutions rendues nécessaires par l'évolution de la réglementation, RGPD, ...

	<b>Bulles sécuritaires DNUM</b>	

### 3.9.3 UNITES D'ŒUVRE DE CETTE ACTIVITE

L'UO EXPL\_D couvre ce périmètre pour le projet Diamant.

L'UO EXPL\_S couvre ce périmètre pour le projet Vaccins.

L'UO EXPL\_C couvre ce périmètre pour le projet entrepôt Covid.

L'UO EXPL\_01 sera déclenchée pour un nouveau projet de scénario intermédiaire.

### 3.9.4 MODALITES DE VALIDATION

La validation de la prestation donne lieu à l'établissement d'un procès-verbal de service fait. En cas de dépassement des délais fixés, le Ministère applique les pénalités prévues à cet effet dans le CCAP.

## 3.10 ACTIVITE 8 – FOURNITURE DE LICENCES

---

### 3.10.1 OBJET

Cette activité a pour objet de définir les conditions dans lesquelles le TITULAIRE assure la fourniture des licences logicielles.

	<b>Bulles sécuritaires DNUM</b>	

	Référence (ou équivalent)	désignation
wallix	BEL-SM1	Bastion core, Bastion Session Manager. Licensing: - EITHER 50 Resources max, 25 Users max, 25 Concurrent Sessions max, - OR 5 Users max, 250 Resources max, 25 Concurrent Sessions max, - OR 5 Concurrent Sessions max, 250 Resources max, 25 Users max.
wallix	BEL-SM2	Bastion core, Bastion Session Manager. Licensing: - EITHER 100 Resources max, 25 Users max, 25 Concurrent Sessions max, - OR 10 Users max, 250 Resources max, 25 Concurrent Sessions max, - OR 10 Concurrent Sessions, 250 Resources, 25 Users max.
wallix	BEL-SM3	Bastion core, Bastion Session Manager. Licensing: - EITHER 250 Resources max, 35 Users max, 35 Concurrent Sessions max, - OR 25 Users max, 350 Resources max, 35 Concurrent Sessions max, - OR 25 Concurrent Sessions max, 350 Resources max, 35 Users max.
	<b>BASTION ENTRY LEVEL: WALLIX BASTION USERS</b>	
wallix	BEL-USER1	Extra Bastion User for Bastion Entry Level
	<b>BASTION ENTRY LEVEL: WALLIX BASTION RESOURCES</b>	
wallix	BEL-SM-TGT1	Extra Bastion SM resource for Bastion Entry Level BEL-SMX
wallix	BEL-CUS-TGT1	Extra Bastion SM concurrent session for Bastion Entry Level BEL-SMX
	<b>Maintenance pour les contrats existants.</b>	
wallix	WSM-BR1-R	BRONZE Contract renewal: 8am-7pm (CET) territory business days for 1 year
wallix	WSM-BR3-R	BRONZE Contract renewal: 8am-7pm (CET) territory business days for 3 years
	<b>Contrat de support pour les nouvelles licences</b>	
wallix	WSM-BR1	BRONZE Contract: 8am-7pm (CET) territory business days for 1 year - 5 days a week
wallix	WSM-BR3	BRONZE Contract: 8am-7pm (CET) territory business days for 3 years - 5 days a week
fortinet	FAC-VM-BASE	Base FortiAuthenticator-VM with 100 user license. Unlimited vCPU. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0, and Xen Virtual Machine platforms
fortinet	FAC-VM-100-UG	Adds 100 users to FortiAuthenticator-VM
fortinet	FAC-VM-1000-UG	Adds 1,000 users to FortiAuthenticator-VM
fortinet	FAC-VM-10000-UG	Adds 10,000 users to FortiAuthenticator-VM
fortinet	FC1-10-0ACVM-248-02-DD	24x7 FortiCare Contract (1 - 500 USERS)
fortinet	FC2-10-0ACVM-248-02-DD	24x7 FortiCare Contract (1 - 1100 USERS)
fortinet	FC3-10-0ACVM-248-02-DD	24x7 FortiCare Contract (1 - 5100 USERS)
fortinet	FC4-10-0ACVM-248-02-DD	24x7 FortiCare Contract (1 - 10100 USERS)
Symantec	RSSL-WC-2A	Symantec RapidSSL WildCard Certificat, 2 ans

	<b>Bulles sécuritaires DNUM</b>	

NB : pour les licences fortinet DD=12

### 3.10.2 MODALITES D'EXECUTION

Le titulaire doit planifier et organiser la livraison des licences sur le site du ministère avec l'équipe projet et fournir systématiquement un bon de livraison ou équivalent définissant le contenu de cette livraison.

Le titulaire se connecte sur les plates-formes Wallix et fortinet et installe les licences et leurs mises à jour.

Le délai de livraison fourni par le titulaire dans sa réponse devient contractuel et sera reporté dans le bon de commande.

### 3.10.3 MODALITES DE VALIDATION

Le ministère vérifie la conformité de la livraison par rapport au bon de commande et au bon de livraison ou équivalent. La validation d'une livraison donne lieu à l'établissement d'un procès-verbal de réception.

En cas de retard de livraison des licences, le Ministère applique les pénalités prévues à cet effet dans le CCAP.

## 3.11 ACTIVITE 9 - ASSISTANCE AU PROJET

### 3.11.1 OBJET

Cette activité a pour objet de définir les conditions dans lesquelles le TITULAIRE apporte son assistance pour la production de statistiques et pour des commandes ponctuelles d'assistance.

### 3.11.2 DESCRIPTION ET UNITES D'OEUVRE DE CETTE ACTIVITE

Code de l'unité d'œuvre	Prestation	Description	Livrables
STATAN	Production de statistiques des traces du système de type Wallix à intervalles de une fois par mois  Durée : 1 an	Le titulaire relève les traces produites par l'outil vidéologique et produit à intervalle de 2 fois par ans en ses locaux des tableaux explicites concernant les traces.	Tableaux statistiques
STATAC	Production de statistiques des traces du système de type Wallix à la commande	Le titulaire devra coter le cout de la relève d'une trace spécifique et de son interprétation demandée de façon ponctuelle.	Analyse et interprétation d'une trace d'une trace

	<b>Bulles sécuritaires DNUM</b>	

Code de l'unité d'œuvre	Prestation	Description	Livrables
AST1	Le titulaire sera amené tout au long du marché à apporter une expertise simple, à la demande sous la forme d'une prestation d'assistance sur site ou à distance d'une durée de 5 jours	Le titulaire intervient à la demande de la DNUM sur site pour apporter son expertise Il s'agira d'une assistance simple d'une durée de 3 à 5 jours pour laquelle il documentera son intervention	-assistance technique, intervention sur les briques, paramétrage  Durée de 3 à 5 jours
AST2	Le titulaire sera amené tout au long du marché à apporter une expertise simple, à la demande sous la forme d'une prestation d'assistance sur site ou à distance d'une durée de 10 jours	Le titulaire intervient à la demande de la DNUM sur site pour apporter son expertise Il s'agira d'une assistance simple d'une durée de 3 à 5 jours pour laquelle il documentera son intervention.  Il pourra dans le cadre de cette Unité d'œuvre apporter une expertise à la DSI du ministère en charge de la santé.	Assistance technique, intervention sur les briques, paramétrage  durée de 7 à 10 jours
AST3	Le pouvoir adjudicateur commande une quotité de 25 heures d'intervention consommables heure par heure	Le titulaire intervient à la demande de la DNUM sur site ou à distance pour apporter son expertise. Le titulaire cotera dans le BPU le prix de 25 heures d'intervention	Durée 1H

### 3.11.3 MODALITES DE VALIDATION

La validation de la prestation donne lieu à l'établissement d'un procès-verbal de service fait. En cas de dépassement des délais fixés, le Ministère applique les pénalités prévues à cet effet dans le CCAP.

## 3.12 ACTIVITE 10 - TRANSFERT DE COMPETENCES - REVERSIBILITE

### 3.12.1 OBJET

	<b>Bulles sécuritaires DNUM</b>	

Cette activité, a pour objet de décrire les conditions dans lesquelles le TITULAIRE assure le transfert de la documentation et de toutes les compétences nécessaires au personnel de la DNUM ou à celui-ci d'un autre TITULAIRE désigné par la DNUM afin d'assurer la continuité du service et la poursuite des prestations du présent marché.

### 3.12.2 DESCRIPTION

Le TITULAIRE réalise le transfert de connaissances et de compétences sur l'ensemble des activités du marché vis-à-vis de la nouvelle équipe, qu'elles soient internes à la DNUM ou externes.

Le TITULAIRE garantit qu'il continuera durant la phase de réversibilité à fournir les prestations contractuelles, dans des conditions identiques. Le TITULAIRE garantit qu'il assistera la DNUM ou tout tiers désigné par elle avec toute la diligence nécessaire pour ce type d'obligation afin de mener à bien la réversibilité.

Le transfert de compétence et l'assistance à la réversibilité comprennent au minimum les phases détaillées suivantes :

Le support et l'accompagnement pour la prise de connaissance de l'application objet du transfert de compétence :

- ▶ Au titre de cette phase, le nouveau TITULAIRE ou l'équipe de la DNUM prend connaissance du contexte fonctionnel et technique de l'application. Dès l'activation du bon de commande de cette prestation, une réunion de lancement est planifiée ayant pour objet la présentation par l'ancien TITULAIRE au nouveau TITULAIRE ou à l'équipe de la DNUM de l'application objet du transfert de compétences.
- ▶ Pour cette prise de connaissance, le nouveau TITULAIRE ou l'équipe de la DNUM qui prend en charge ensuite le « maintien en état de fonctionnement » de l'application est assuré de bénéficier des fournitures de l'ancien TITULAIRE (matériels, logiciels, documentation). Au cours de cette phase de prise de connaissance, l'ancien TITULAIRE mettra à disposition du nouveau TITULAIRE ou de l'équipe de la DNUM les matériels, logiciels, documentation et locaux nécessaires à cette prestation. Le nouveau TITULAIRE ou l'équipe de la DNUM pourra également compter sur la disponibilité des personnels de l'ancien TITULAIRE.

L'inventaire des applications et documentations :

- ▶ Le TITULAIRE en fin de marché réalise un inventaire exhaustif des applications, des briques logicielles et documentations qui seront mises à la disposition de la DNUM
- ▶ Cet inventaire est soumis à l'approbation de la DNUM et fera foi pour juger des cas de perte, destruction ou vol d'applications ou documentations afférentes.
- ▶ Les prestations ont lieu dans les locaux du l'ancien et du nouveau TITULAIRE selon les phases.

	<b>Bulles sécuritaires DNUM</b>	

Les livrables de cette prestation sont :

- ▶ Le plan de réversibilité ;
- ▶ Un support pour une présentation orale qui contiendra :
  - Une documentation fonctionnelle des briques fournies ;
  - Une documentation technique de des briques fournies ;
  - Une documentation d'exploitation des briques fournies.
- ▶ Les comptes rendus des sessions et des ateliers de réversibilité faisant apparaître le contenu, la méthode et les résultats d'évaluation, les intervenants et les participants, le suivi de l'activité d'assistance technique et la documentation support ;
- ▶ La liste de l'ensemble des livrables du marché (documentation technique, supports de formation ...).

### 3.12.3 UNITES D'ŒUVRE DE CETTE ACTIVITE

Code de l'unité d'œuvre	Prestation	Livrable	Délai maximum de production des livrables à compter de la notification du bon de commande (jours ouvrés)
TRANSF1	Transfert de compétence classique	Le plan de réversibilité ; Un support pour une présentation orale : documentations fonctionnelle, technique et d'exploitation de l'application ; Les comptes rendus des sessions et des ateliers de réversibilité ; La liste de l'ensemble des livrables du marché.	20
TRANSF2	Transfert de compétence avec assistance à l'exploitation sur site chez le nouvel exploitant (assistance de 2 jours par semaine pendant 2 mois)	Le plan de réversibilité ; Un support pour une présentation orale : documentations fonctionnelle, technique et d'exploitation de l'application ; Les comptes rendus des sessions et des ateliers de réversibilité ; La liste de l'ensemble des livrables du marché.	20

La prestation de transfert de compétences intervient si nécessaire en fin de marché. Le délai de production des livrables et de démarrage de l'activité est dans chaque cas de 20 jours ouvrés à compter de la réception de la commande émise par la DNUM.

### 3.12.4 MODALITES DE VALIDATION

La validation de la prestation donne lieu à l'établissement d'un procès-verbal de service fait. En cas de dépassement des délais fixés, le Ministère applique les pénalités prévues à cet effet dans le CCAP.



	<b>Bulles sécuritaires DNUM</b>	

## 4 PILOTAGE ET SUIVI DE PROJET

Un comité de pilotage se réunit une fois par an, sauf lors de problème exceptionnel. Il est mis en place avec le TITULAIRE. Il a pour fonction d'assurer le pilotage et revoit en synthèse l'avancement du planning et des livrables, les risques, la qualité, les actions et décisions.

Le comité de pilotage se réunit sous la responsabilité de la DNUM. Le TITULAIRE a la charge de préparer l'ordre du jour, le support de présentation et d'assurer la rédaction du compte-rendu sous un délai d'un mois avant la tenue du comité de pilotage

	<b>Bulles sécuritaires DNUM</b>	

## 5 EXIGENCES EN MATIERE DE SECURITE

Le TITULAIRE faisant partie de la chaîne de traitement du SNDS (en tant que système fils) doit apporter la preuve du respect des règles du Référentiel de sécurité du SNDS, du Règlement européen sur la Protection des Données à caractère Personnel, de la Politique Générale de Sécurité des Systèmes d'Information en santé (PGSSI-S), de la Politique de Sécurité des Systèmes d'Information pour les Ministères Chargés des Affaires Sociales (PSSI MCAS), des règles applicables dans le cadre du Référentiel Général de Sécurité (RGS) et de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [...].

Il devra être conforme au guide de l'ANSSI sur les passerelles internet sécurisées<sup>1</sup>.

Il devra disposer d'une certification iso27001 qui devra être applicable dans le cadre du présent marché.

Il apportera tous les éléments nécessaires à la bonne conformité de ses prestations en regard des exigences présentées.

### 5.1 REGLES GLOBALES

Tout hébergement d'application par un tiers doit être encadré par un contrat dans lequel les éléments suivants sont pris en compte :

- ▶ **Disponibilité** des services proposés, incluant les pénalités en cas de défaillance. Pour lever toute ambiguïté, les indicateurs de service et de performance doivent être clairement définis.
- ▶ **Intégrité** des éléments techniques qu'il a installés
- ▶ **Confidentialité** de l'ensemble des éléments transmis, tous les éléments transmis par le ministère sont confidentiels sauf avis contraire et autorisation formelle.
- ▶ **Protection des éléments échangés** : des mécanismes de chiffrement des données utilisant des clefs de chiffrement maîtrisées par son client doivent être mis en œuvre.
- ▶ **Réversibilité** des sources, des applications à la fin du contrat.
- ▶ **Destruction** irréversible des documents et des sources au décommissionnement de tout ou partie d'application et nécessairement à la fin de contrat. La fourniture d'un certificat formel de destruction est obligatoire.
- ▶ **Garantie de maintien en conditions opérationnelles de sécurité** en cas de découverte de vulnérabilités sur les briques du système d'information sous la responsabilité du TITULAIRE.
- ▶ Un **Plan d'Assurance Sécurité** sera rédigé par le candidat s'engageant contractuellement à mettre en œuvre et à maintenir le niveau d'exigences sécurité (référentiels nommés ci-dessus) dans le temps.
- ▶ Chaque Administrateur doit signer une Charte Administrateur décrivant notamment ses devoirs et responsabilités.

<sup>1</sup> [https://www.ssi.gouv.fr/uploads/2019/06/anssi-guide-passerelle\\_internet\\_securisee-v3.pdf](https://www.ssi.gouv.fr/uploads/2019/06/anssi-guide-passerelle_internet_securisee-v3.pdf)

	<b>Bulles sécuritaires DNUM</b>	

En outre :

- ▶ Tout service porté par un tiers doit pouvoir être audité. Ainsi, des audits de vulnérabilités et des tests d'intrusions doivent pouvoir être réalisés. Le contrat doit inclure le processus d'organisation de ce type d'audit en accord avec le Responsable de la Sécurité Numérique (RSN).
- ▶ Les contrats doivent être définis en accord avec la Direction Juridique de l'entité (DAJ).

## 5.2 ARCHITECTURE

Le tiers hébergeur est responsable des infrastructures qu'il met à disposition de l'entité, il doit néanmoins se conformer aux éléments suivants :

- ▶ L'accès aux interfaces d'administration des systèmes d'exploitation, des middlewares, des bases de données ou de tout autre élément technique ne doit être réalisé qu'au travers d'un proxy d'administration (Bastion).
- ▶ Le bastion devra être paramétré afin de :
  - Ne pas être accessible directement depuis la zone internet ;
  - Gérer les profils couplant utilisateurs, environnement, usage ;
  - Enregistrement des traces de connexion, et les traces des actions réalisées par tous les utilisateurs comme les administrateurs fonctionnels et techniques et par les développeurs ;
- ▶ L'accès direct à Internet des composants est interdit. Tous les accès doivent être filtrés sur le principe d'une liste blanche validée par le RSN autorisant les connexions vers les seuls domaines identifiés (mise en place d'un proxy).
- ▶ Les traces informatiques générées doivent être exportées en temps réel vers le système d'information du représentant du pouvoir adjudicateur.

## 5.3 IDENTITY ACCESS MANAGEMENT

- ▶ Un contrôle d'accès basé sur les rôles (RBAC) doit garantir le cloisonnement logique des accès aux systèmes et doit être revu périodiquement ;
- ▶ L'usage de compte non nominatif est à proscrire ;
- ▶ Les accès à la plateforme ne sont réalisés qu'en authentification forte via Token ;
- ▶ Exceptions : aucun compte ne doit déroger à ces règles, si toutefois une exception devait être nécessaire, une validation du RSN est nécessaire.

## 5.4 TRACES

- ▶ Enregistrement des traces de connexion, les traces des actions réalisées par tous les utilisateurs comme les administrateurs fonctionnels et techniques ;
- ▶ Les logs seront sous la forme vidéo et timeline des actions ;

	<b>Bulles sécuritaires DNUM</b>	

- ▶ La gestion des traces doit être clairement décrite ; des événements collectés, au stockage, aux accès...<sup>2</sup> ;
- ▶ Les logs seront à valeur probante, doivent être protégés selon les règles de l'art ;
- ▶ Les logs pourront être collectés par le Ministère ;
- ▶ L'accès aux logs & enregistrements doivent être strictement filtrés et tracés.

## 5.5 PROTECTION DES DONNEES (LOGS , TRACES ET DOCUMENTS ECHANGES (DAT, ...))

- ▶ La nature et la sensibilité des données collectées et traitées doivent être définies en coopération avec le RSN,
- ▶ Les systèmes de fichiers (stockage, sauvegarde...), qu'ils soient physiques ou virtuels, doivent être chiffrés conformément à l'état de l'art (aujourd'hui en utilisant l'algorithme AES 256 minimum),
- ▶ La gestion des clés de chiffrement (création, révocation...) doit pouvoir être contrôlée par le représentant du pouvoir adjudicateur

## 5.6 PROTECTION DES COMMUNICATIONS

- ▶ Les réseaux Internet et locaux permettant l'accès ou l'administration des briques hébergées (plateforme, middleware, application...) dans le « cloud » sont des réseaux « public » ne permettant pas de garantir la confidentialité des communications. Il est donc obligatoire de mettre en place un chiffrement des communications (quel que soit le protocole utilisé). Toute dérogation doit être validée par le RSN.
- ▶ La communication avec ou entre les tiers applicatifs ne doit pouvoir se faire qu'au travers de protocoles intégrant les mécanismes de sécurité d'authentification et de chiffrement : utilisation des standards WS-Security pour la protection des Web Services (notamment par une authentification mutuelle à base de certificats). Toutes les communications doivent être explicitement autorisées : par défaut, toute communication est interdite.
- ▶ Les flux nécessaires aux opérations ponctuelles doivent être fermés en dehors de plages de maintenance (sauvegarde).

## 5.7 SURVEILLANCE

- ▶ Des solutions de détection et/ou prévention d'intrusions doivent être mises en œuvre. Chaque composant mis en œuvre doit être surveillé (monitoring technique réseau serveurs et applicatif). Le ministère doit pouvoir accéder à la console de supervision en lecture. Les traces informatiques générées doivent être envoyées en temps réel sur le système d'information du ministère.
- ▶ Tout incident de sécurité détecté par les équipes du prestataire doit être immédiatement porté à la connaissance des équipes sécurité du ministère.

<sup>2</sup> [https://www.ssi.gouv.fr/uploads/IMG/pdf/NP\\_Journalisation\\_NoteTech.pdf](https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Journalisation_NoteTech.pdf)

	<b>Bulles sécuritaires DNUM</b>	

## 6 RACI

Rôle de services	DNUM	Maitrise d'œuvre	Titulaire du présent marché	Hébergeur HDS
<b>Infrastructure cloud</b>				
Administration des ressources (hosts / Stockage / réseau)	(I)			x
Evolution des ressources	(A)			x
Contrôle et suivi des ressources (Filer, VMs)	(I)			x
<b>Environnement système bulle</b>				
Exploitation des équipements composant la "bulle sécurisée", MCO/MCS	(I)		x	
Supervision du RP	(I)		x	
Support des solutions (bastion, FAC, RP)	(I)		x	
Gestion des accès utilisateurs (bastion, FAC)	(A)		x	
Exploitation des logs stockés	(A)		x	
Gestion de la sauvegarde	(A)			x
Demandes d'évolution	(A)		x	
Gestion du certificat (si-diamant.fr)	(A)		x	
<b>Environnement applicatif</b>				
Gestion des Logiciels socles du serveur applicatif	(I)	x		
Scripts pour l'import-export de fichiers	(I)	x		
Gestion des Logiciels applicatifs		x		
Scripts de déchiffrement des fichiers xml ATIH / SESAN / DARES et d'import en base des données		x		
Administration de la base de données	(I)	x		
Scripts d'extraction de données et de rapports		x		
Renouvellement des certificats DNUM et ATIH	(I)	x		
<b>Environnement système</b>				
Exploitation de l'OS du serveur applicatif, MCO/MCS	(I)			x
Chiffrement / déchiffrement des disques				x
Supervision des services et hôtes	(I)			x
Gestion des secrets liés aux systèmes	(I)			x
Gestion des accès utilisateurs (VPN, bastion, FTP, renouvellement des identifiants)	(A)			x
Exploitation des logs stockés	(A)			x
Gestion de la sauvegarde	(A)			x

x : responsable

(I) : informé

(A) : autorité

	<b>Bulles sécuritaires DNUM</b>	

## ANNEXES ET LIENS UTILES

### 6.1 GLOSSAIRE

Terminologie	Description
ARH	Agences Régionales de l'Hospitalisation qui ont été remplacées par les ARS (loi du 21 Juillet 2009)
ARS	Agence Régionale de Santé : Organisme issu de la fusion totale ou partielle des ARH, des DRASS-DDASS, des GRSP (groupement régional de santé), URCAM union régionale des caisses d'assurance maladie), MRS (mission régionale de la santé) et CRAM (caisse régionale d'assurance maladie)
CCAM	Classification commune des actes médicaux
CCAM	Catalogue de classification des Actes Médicaux (ex NGAP-nomenclature générale des actes professionnels)
CCAS	Centre Communaux d'Action Sociale
CDARR	Catalogue des activités de rééducation-réadaptation
CH, CHU, CHRU	Centre Hospitalier, Centre Hospitalier Universitaire, Centre Hospitalier Régional et Universitaire
CIM10	Classification internationale des maladies
CLIC	Centre Local d'Information et de Coordination (gérontologique)
CMC	Catégorie Majeure Clinique
CMD	Catégorie Majeure de Diagnostic
CME	Commission Médicale d'Etablissement : regroupe les praticiens médicaux d'un même établissement élus par leurs confrères pour représenter la communauté médicale d'un même établissement
CRAM	Caisse Régionale d'Assurance Maladie
DA	Domaine d'Activité (regroupement de GHM)
DE, DES, DESC, DU	Diplôme d'Etat, Diplôme d'Etudes Spécialisées, Diplôme d'Etudes Spécialisées Complémentaires, Diplôme Universitaire
DGS	DGS Direction Générale de la Santé : Service du secrétariat d'Etat à la Santé chargé de l'étude et de la préparation de la politique de santé. Elle appuie son travail sur des enquêtes ponctuelles, annuelles ou pluriannuelles. Pour la santé mentale, par exemple, la DGS a mis sur pied la "fiche patient".
DGOS	Direction générale de l'offre de Soins : rattachée au Ministère de la Santé
DNUM	Direction du numérique du ministère en charge de la santé
EHPAD	Etablissement d'hébergement pour personnes âgées dépendantes
EPS	Etablissement public de santé
Etablissement Ex DG	Etablissements anciennement sous dotation globale (ex DG)
Etablissement Ex OQN	Etablissements anciennement sous objectifs quantifiés (Ex OQN)

	<b>Bulles sécuritaires DNUM</b>	

<b>GHM</b>	Groupe homogène de malade. La classification en GHM utilisée en MCO et SSR repose sur le classement des séjours en un nombre limité de groupes de séjours présentant une similitude médicale et un coût voisin. Elle permet un classement exhaustif et unique : tout séjour aboutit dans l'un des 512 groupes de la classification selon un algorithme de décision qui se fonde sur les informations médico-administratives contenues dans le RSS
<b>GHPC</b>	Groupes Homogènes prise en charge (HAD)
<b>GHS</b>	le Groupe homogène de séjour est le tarif applicable à un GHM. Un tableau de correspondance GHM / GHS est publié sur le site ATIH
<b>GHT</b>	Groupe homogène de tarifs. L'échelle des GHT est la même pour les deux secteurs d'hospitalisation, public et privé.
<b>GMD</b>	Groupe Morbidité Dominante
<b>GP</b>	Groupe de Planification (regroupement de GHM)
<b>Grille AGIRR</b>	Outil utilisé pour évaluer l'Autonomie Gérontologique des Groupes Iso Ressources (utilisé par les services du Conseil Général pour l'évaluation de l'APA-allocation Personnalisée d'Autonomie-mais aussi par nombre d'institutions : CRAM, MSA,...)
<b>HAD</b>	Hospitalisation à domicile
<b>HDJ</b>	Hôpital de jour
<b>ICR</b>	Indice de Coût Relatif : Unité d'œuvre des actes produits par les services médico-techniques, indiquant le degré de mobilisation de ressources humaines et matérielles nécessaires directement nécessaires à leur production.
<b>INSERM</b>	Institut National de la Santé et de la Recherche Médical
<b>IVA</b>	IVA SSR indice de valorisation de l'activité. Choix d'un modèle multivarié (définition de variables expliquant la consommation de ressource comme les soins médicaux, de RR, de nursing, la dépendance, l'âge...) additif (somme des valeurs (en point) des différentes variables En gardant la journée pondérée des RHS) de points
<b>MCO</b>	Médecine- Chirurgie – Obstétrique
<b>MCO</b>	Appellation commune des services de court séjour. Par définition : Médecine, Chirurgie Obstétrique
<b>MPR</b>	Médecine Physique et de Réadaptation
<b>MPU</b>	Service de Médecine Post Urgence
<b>MSA</b>	Mutualité Sociale Agricole
<b>PMSI</b>	Programme de Médicalisation du Système d'Information : description des soins en fonction de la pathologie (relevé hebdomadaire- Justification des soins)
<b>PSPH</b>	Participant au Secteur Public Hospitalier
<b>PSY</b>	Psychiatrie
<b>RAPSS</b>	Résumé Anonymisé Par Sous-Séquence (domaine HAD)
<b>RHA</b>	Résumé Hebdomadaire Anonymisé (domaine SSR)
<b>RSA</b>	Résumé de Sortie Anonymisé (domaine MCO)

	<b>Bulles sécuritaires DNUM</b>	

<b>SAE</b>	Statistique d'Activité des Etablissements : Demandée à tous les établissements de santé en France depuis 1994, elle a suivi la H80, et prend en compte, non seulement l'hospitalisation, mais également l'activité ambulatoire.
<b>SAU</b>	Service d'accueil des urgences
<b>SCN</b>	Service à compétence nationale rattaché à la DNUM
<b>SLD</b>	Soins de longue durée
<b>SROS:</b>	Schéma Régional d'Organisation Sanitaire dispose du CROS (Comité régional d'Organisation Sanitaire) et de la COMEX (Commission exécutive du CROS)
<b>SRPR</b>	Service de Réadaptation Post Réanimation
<b>SSIAD</b>	Service de Soins Infirmiers A Domicile
<b>SSMED 1</b>	Service de soins de suite médicalisés de haut niveau (ou très spécialisé) impliquant un plateau technique minimum, un personnel paramédical formé et une permanence médicale spécialisée (pneumo, cardio,...)
<b>SSMED 2</b>	Service de soins de suite médicalisés généralistes ou polyvalents : la permanence médicale doit être assurée. L'intervention de spécialiste peut être ponctuelle. Pas de techniques de soins particulières
<b>SSR</b>	Soins de Suite et de Réadaptation
<b>TAA(ou T2A)</b>	Tarification A l'Activité
<b>Unité EVC/EPR</b>	Unités accueillant des patients en états végétatifs chroniques