



**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES**

Marché n°2026-0078-00-00-MPF

**Acheteur**

**Numih France**

12 rue Michel Labrousse

CS 93668

31036 Toulouse Cedex 1

Siret n° 18310021300028

**Mise à disposition et maintenance d'une solution de gestion et de diffusion de SMS**

Accepté sans réserve à ....., le .....

Cachet de l'entreprise, Nom - Prénom et qualité du signataire

**NB** : Tout comme l'ensemble des documents de la consultation, le présent document ne peut être modifié à l'initiative du Titulaire.

## SOMMAIRE

<b>Article 1. Objet du marché .....</b>	<b>4</b>
1.1 Présentation de Numih France .....	4
1.2 Réglementations applicables au marché .....	4
1.2.1 Réglementations complémentaires applicables au contexte du marché. 4	
1.2.1.1 Réglementation sur la protection des données personnelles (annexe ST/STU) .....	5
1.2.1.2 Réglementation sur les communications électroniques (Code des postes et communications électroniques/Arcep) .....	5
1.2.1.3 Réglementation sur l'hébergement de données de santé (HDS).....	5
<b>Article 2. Description du besoin .....</b>	<b>5</b>
2.1 Vue globale .....	5
2.1.1 <b>Maintien de la double compatibilité technique – Recours à la sous-traitance</b> .....	6
2.2 Fonctionnalités obligatoires demandées : .....	6
2.3 Fonctionnalité qui serait appréciée : .....	7
2.3.1 Fonctionnalité RCS .....	7
2.4 Plateforme SaaS pour les établissements de santé .....	8
2.5 Fonctionnalités de la plateforme SaaS pour Numih France .....	10
2.6 Description des APIs attendues .....	11
2.7 Description et paramètres de la première API (Usage général) .....	12
2.8 Description et paramètres de la deuxième API (Usage DPI) .....	15
2.9 Description et paramètres de l'API pour les mini-sites .....	17
2.10 Principe général de routage .....	18
2.10.1 Option de routage local.....	18
2.10.2 Modalités d'activation .....	18
2.10.3 Tarification .....	18
2.10.4 Évolutivité .....	19
2.11 Conformité des routes .....	19
2.11.1 Obligation de transparence sur le routage.....	19
2.11.2 Cohérence tarifaire (anti-prix anormalement bas) .....	19
<b>Article 3. Analyse de risque simplifiée.....</b>	<b>19</b>
3.1 Fonctionnalités du service .....	19
3.2 Gestion des interfaces.....	20
3.3 Gestion des comptes et des habilitations .....	20
<b>Article 4. Environnement d'exécution du marché .....</b>	<b>21</b>
4.1 Environnement technique .....	21
4.2 Environnement applicatif .....	21
4.3 Interopérabilité et interfaces externes.....	21
4.4 Livrables de la prestation.....	22

4.5	Volumétrie, dimensionnement et performance .....	22
<b>Article 5.</b>	<b>Conditions d'exécution des prestations .....</b>	<b>22</b>
5.1	Intervention à distance .....	23
5.2	Supervision du service .....	23
5.3	Organisation et méthodologie.....	23
5.4	Organisation du support et modalités de gestion des incidents.....	23
5.4.1	Modalités générales du support .....	23
5.4.2	Outils de ticketing.....	24
5.4.3	Processus de support et d'escalade .....	24
5.4.4	Suivi et reporting du support .....	24
5.5	Réversibilité .....	24
5.5.1	Absence de restitution des données .....	24
5.5.2	Prestations attendues pendant la réversibilité.....	25
5.5.3	Durée et calendrier de réversibilité .....	25
5.5.4	Traçabilité et conformité.....	25
<b>Article 6.</b>	<b>Suivi et engagements du Titulaire.....</b>	<b>25</b>
6.1	Niveau d'engagement en cas d'incident .....	25
6.2	Niveaux de service (SLA) du titulaire.....	25
6.3	Maintenance .....	26
6.3.1	Évolutives.....	26
6.3.2	Correctives.....	27
<b>Article 7.</b>	<b>Comitologie et pilotage du marché .....</b>	<b>28</b>
7.1	Calendrier et Comitologie .....	28
7.1.1	Calendrier .....	28
7.1.2	Réunions.....	28
7.1.2.1	Réunion de lancement.....	29
7.1.2.2	Réunion de fin de transition.....	29
7.1.2.3	Réunion de pilotage.....	29
7.2	Phase de transition.....	30
7.3	Phase de production.....	30
7.4	Phase de réversibilité .....	30
<b>Article 8.</b>	<b>Clauses de sécurité .....</b>	<b>31</b>
8.1	Sécurité du Titulaire.....	31
8.2	Audits de sécurité techniques.....	31
8.3	Incident de sécurité .....	32
<b>Article 9.</b>	<b>Classification des vulnérabilités et délais de correction</b>	<b>32</b>

## Article 1. Objet du marché

Numih France souhaite renouveler sa solution de gestion et de diffusion de SMS à partir des Systèmes d'Information de Centres Hospitaliers.

Le champ d'application de la solution est à très large spectre. L'ensemble du Système d'Information, producteur d'informations de différents types, peut être concerné par l'émission de SMS, aussi bien pour le personnel hospitalier, les personnels d'établissements privés, que pour la patientèle ou l'institution.

Le principe de base est d'offrir une solution aux adhérents et clients de Numih France, simple, d'usage intuitif, simple à intégrer et permettant des envois de masse ou unitaires à des tarifs très compétitifs et leur laissant l'autonomie nécessaire pour imaginer de nouveaux flux à partir de la solution retenue.

La solution préconisée est de disposer, en aval du Système d'Information, d'une solution universelle permettant à chaque application et à chaque utilisateur référencé d'émettre des SMS.

La solution de diffusion de SMS de Numih France est déployée dans deux cent établissements. Le renouvellement de la solution doit être transparent pour les établissements. Les services et les données mis en place avec le fournisseur actuel doivent être repris.

Numih France, issu de la fusion entre le Mipih et le SIB, possède à ce jour plusieurs APIs utilisées en production venant de 2 fournisseurs différents.

Les options utilisées aujourd'hui sont détaillées dans ce document. Afin de fournir un service équivalent, des options équivalentes doivent être proposé par le titulaire.

Le service étant en production, il est impératif de garantir une continuité de service pour les établissements de santé.

Une période de transition ou l'ancienne offre fonctionnera en parallèle de la nouvelle offre est prévue.

### 1.1 Présentation de Numih France

Numih France est une structure publique de coopération inter-hospitalière spécialisée dans l'informatique, travaillant avec des établissements de santé répartis sur l'ensemble du territoire (Centres Hospitaliers Universitaire, Centres Hospitaliers, Établissements de Santé Privés d'Intérêt Collectif, Hôpitaux locaux, Maison de retraite, Établissement d'hébergement pour personnes âgées dépendantes, Établissements de santé privés d'intérêt collectif...).

Éditeur de progiciels hospitaliers et de santé sur des domaines complémentaires s'appuyant sur des dizaines d'années d'expérience, et hébergeur de données de santé certifié depuis 2018, Numih France accompagne les établissements de santé dans la construction et le développement de leur système d'information.

### 1.2 Réglementations applicables au marché

#### 1.2.1 Réglementations complémentaires applicables au contexte du marché

Le Titulaire est tenu de respecter les exigences réglementaires présentes et à venir qui couvrent le champ fonctionnel du présent marché.

### 1.2.1.1 Réglementation sur la protection des données personnelles (annexe ST/STU)

Dans le cadre de ce présent marché, le Titulaire du marché est considéré comme un sous-traitant ultérieur au sens du règlement (UE) 2016/679 relatif à la protection des données à caractère personnel (RGPD).

A ce titre, le Titulaire devra compléter l'annexe RGPD jointe au présent marché.

### 1.2.1.2 Réglementation sur les communications électroniques (Code des postes et communications électroniques/Arcep)

Le Titulaire s'engage à respecter l'ensemble des dispositions applicables aux opérateurs de communications électroniques telles que prévues par le Code des postes et des communications électroniques (CPCE), ainsi que les décisions adoptées par l'Arcep.

A ce titre, le Titulaire garantit notamment :

- Le respect des obligations d'identification des expéditeurs (ex : SMS avec nom de l'établissement).
- La mise en œuvre de mesures de prévention et de lutte contre les SMS frauduleux (smishing), via le filtrage anti-spam de l'Arcep.
- L'utilisation de numéros émetteurs autorisés (Sender ID, short code, etc.).

### 1.2.1.3 Règlementation sur l'hébergement de données de santé (HDS)

Dans le cas où le Titulaire est amené à héberger des données de santé au sens du Code de la santé publique, il s'engage à être pleinement conforme aux exigences de la certification HDS pour les activités d'hébergement concernées. Le Titulaire s'engage à maintenir cette conformité pendant toute la durée du marché et à fournir les justificatifs attestant de cette certification.

Dans le cas où le Titulaire recourt à un sous-traitant pour l'hébergement de données de santé, il s'engage à en informer préalablement Numih France. Conformément à l'article R.1111-11 du Code de la santé publique, le Titulaire s'engage également à transmettre à Numih France l'ensemble des informations et mentions obligatoires requises en matière de sous-traitance.

## Article 2. Description du besoin

### 2.1 Vue globale

Le titulaire devra fournir un service d'envoi de messages courts (SMS) à destination de terminaux mobiles, conforme aux standards en vigueur, garantissant une haute délivrabilité, une traçabilité des envois, et une compatibilité avec l'ensemble des opérateurs mobiles nationaux.

Ce service doit être accessible et appelable de plusieurs manières pour répondre à l'ensemble des usages historiques existants et pouvoir répondre à de nouveaux usages.

Les différents usages majeurs :

- Le premier usage majeur concerne l'envoi de rappel de rendez-vous, l'envoi de codes à usage unique, l'envoi de notifications depuis la France, incluant les DOM-TOM.
- La mise à disposition d'une plateforme SaaS et de mini-sites pour les établissements de santé.
- Le second usage permet depuis le DPI de Numih France d'envoyer des notifications et rappels de rdv.

### 2.1.1 Maintien de la double compatibilité technique – Recours à la sous-traitance

Afin d'assurer la continuité du service et d'éviter une rupture d'exploitation, il est précisé que le pouvoir adjudicateur dispose actuellement de deux interfaces techniques distinctes (API) d'envoi de SMS, associées à deux prestataires différents.

Dans la mesure où la convergence vers une API unique impliquerait des coûts de portage significatifs et disproportionnés, tant pour l'acheteur que pour les bénéficiaires du service, le présent marché autorise expressément le titulaire à recourir à la sous-traitance pour assurer la compatibilité et la continuité du service sur les deux interfaces existantes.

Ce recours à la sous-traitance devra respecter les dispositions du Code de la commande publique, notamment en matière de déclaration, d'acceptation et d'agrément des sous-traitants par le pouvoir adjudicateur (article 6.3 CCAP). Le titulaire demeure en tout état de cause pleinement responsable de la bonne exécution des prestations, y compris celles réalisées par ses sous-traitants.

## 2.2 Fonctionnalités obligatoires demandées :

- Fournir un service d'envoi de SMS
  - Il doit être possible d'envoyer des SMS à des destinataires à minima pour les pays suivants : France Métropolitaine, Martinique, Guadeloupe, La Réunion, Mayotte, Guyane Française, Madagascar, Principauté de Monaco, Principauté d'Andorre, Norvège, Etats Unis d'Amérique, Canada, Australie, Maroc, Tunisie, Algérie, Espagne, Royaume Uni, Italie, Belgique, Luxembourg, Allemagne, Suisse, Pays-Bas, République Tchèque, Croatie, Hongrie, Roumanie, Grèce, Pologne, Suède, Danemark, Finlande, Turquie, Portugal, Irlande. Les pays disponibles non listés ci-dessus sont à ajouter avec le tarif associé dans le BPU. Les pays nécessitant une procédure d'ouverture et/ou demandant des frais de mise en service et/ou des frais d'abonnement devront être obligatoirement accompagnée de la procédure détaillée pour l'activation vers cette destination et le cas échéant des coûts associés,
  - Il doit être possible de programmer les envois ou de les envoyer instantanément,
  - Il doit être possible d'envoyer des sms en masse ou à l'unité.
  - La solution doit proposer des options de publipostage,
  - La solution doit proposer une possibilité de dédoublonner les numéros en doublons au sein des listes de diffusion,
  - Il doit être possible de gérer les réponses aux SMS envoyés,
  - Il doit être possible d'envoyer des SMS avec un émetteur personnalisé ou via un numéro court pour les SMS permettant aux destinataires de répondre (selon disponibilité dans le pays de destination),
  - Les destinataires doivent pouvoir utiliser le STOP SMS (gestion d'une liste noire),
  - Plusieurs moyens d'intégration (APIs) doivent être proposés. A minima, une API webservice (REST), une API type servlet (appel d'URL sécurisée en POST) et une API mail2sms,
  - La solution doit proposer une possibilité de créer et héberger des mini-sites qui sera accessible par les destinataires via un lien court dans le SMS. Les mini-sites doivent être hébergés par le titulaire. Les mini-sites doivent être sécurisés et personnalisables par établissement. Un modèle de page sera établi pour chaque établissement souhaitant utiliser la fonctionnalité. Ce mini site affichera un logo, un titre, un texte et un QR Code. Le titre, le texte et le contenu du QR Code devront être envoyés en paramètres via l'API pour chaque SMS.
  - Le suivi des remises des SMS devra être possible via des codes retours (erreurs, accusé de réceptions). Les messages devront être référencés pour tous les opérateurs ou mieux encore génériques, y compris les opérateurs MVNO [Mobile Virtual Network Operator].



- Mettre à disposition une plateforme en SaaS
  - La plateforme SaaS doit permettre à Numih France de créer les comptes des établissements de santé et piloter l'activité et l'utilisation du service.
  - La plateforme logicielle doit pouvoir gérer plusieurs environnements, un par établissement de santé.
  - Numih France sera l'administrateur de cette plateforme et gèrera les environnements des Centres Hospitaliers en matière de création de l'environnement et des utilisateurs de cet environnement. La solution devra être personnalisable par Numih France (A minima permettre l'ajout de son logo, ...).
  - La solution devrait être personnalisable pour les établissements (A minima, permettre l'ajout du logo de l'établissement, ...).
  - La plateforme SaaS doit permettre aux établissements de santé d'envoyer des SMS, de gérer et piloter l'usage du service dans l'établissement, de préparer des modèles de SMS, de gérer des listes de contacts, d'envoyer des messages pré-enregistrés à une liste de contacts pré-enregistrée,
  - Des documentations détaillées en Français, doivent être fournies. Une pour la partie administration par Numih France (manuel administrateur) et une seconde à destination des établissements (manuel utilisateur de la plateforme SaaS).
- Mettre à disposition des APIs
  - Les différentes API seront utilisées pour réaliser des intégrations avec le SI des établissements de santé.
  - A minima doivent être proposées : une api type servlet (appel d'URL en POST), une api de type webservice (REST) et une api type mail2sms.
  - Le titulaire pourra fournir plusieurs API pour répondre aux différentes API en production. Il a la possibilité de fournir des API venant de sous-traitants.
  - Le titulaire décrira les moyens de communication et d'interopérabilité intégrés à sa solution en termes d'interfaces, d'API, de Webservices, de requêtes https, tout autre moyen de communication non listé.
  - Une documentation détaillée, exhaustive et en Français doit être fournie pour chaque API.

## 2.3 Fonctionnalité qui serait appréciée :

### 2.3.1 Fonctionnalité RCS

Bien qu'aucune expression de besoin explicite n'ait été formulée à ce jour par les utilisateurs, l'évolution des pratiques et des technologies justifie l'introduction de cette fonctionnalité à titre anticipatif dans le présent marché, afin de garantir une capacité d'adaptation aux futures demandes.

En complément, le service devra permettre, de manière native et par interfaçage, la prise en charge du protocole RCS (Rich Communication Services), afin de permettre l'envoi de messages enrichis (texte long, images, boutons interactifs, accusés de réception, etc.), dans les conditions suivantes :

- Fonctionnalité RCS
  - Le titulaire devra assurer la détection automatique de la compatibilité RCS côté terminal et opérateur, avec bascule automatique vers le canal SMS si le RCS n'est pas supporté.
  - Le prestataire s'engage à ne pas altérer la confidentialité ou l'intégrité des données transmises via RCS et à utiliser des flux sécurisés (ex. : TLS).
  - Le titulaire devra fournir un espace de gestion de contenus RCS ou une API permettant la création, l'édition et la gestion de campagnes RCS.

- Le prestataire devra respecter les prérequis imposés par les opérateurs mobiles et les éventuelles certifications requises (ex. : Google Verified Sender).
- Il devra également garantir que l'usage du RCS respecte l'ensemble des dispositions légales et réglementaires applicables, notamment en matière de protection des données personnelles, de consentement explicite des destinataires et de lutte contre le spam.
- Le titulaire précisera dans sa réponse les modalités techniques d'intégration du RCS, les limitations connues (par opérateur ou terminal), ainsi que les niveaux de service (taux de délivrabilité, latence, disponibilité, etc.) spécifiques au canal RCS.

## 2.4 Plateforme SaaS pour les établissements de santé

Une plateforme SaaS doit permettre aux utilisateurs des établissements de santé d'accéder à un environnement propre à chaque établissement. Cette plateforme doit être accessible depuis internet via une authentification. Une authentification à double facteur est souhaitée. Un filtrage par IP doit être proposé.

Cette plateforme SaaS doit être sécurisée et doit avoir été auditée récemment d'un point de vue sécurité. Le rapport d'audit sera exigé par Numih France.

La plateforme doit permettre :

- De paramétrer les comptes utilisateurs
  - Les informations suivantes sont à renseigner lors de la création d'un compte : Identifiant, mot de passe, civilité, nom, prénom, type de compte, adresse, code postal, ville, pays, mail, téléphone, paramétrage d'un solde en crédit ou illimité.
  - L'outil doit permettre d'ajouter du crédit à un utilisateur, de modifier un utilisateur ou de le supprimer.
- De paramétrer les émetteurs
  - Le libellé de l'émetteur (11 caractères minimum), la description de l'émetteur et le compte ou le sous compte auquel il est rattaché
  - La possibilité de supprimer un émetteur
  - La personnalisation de l'émetteur n'est pas disponible pour les SMS avec réponse. Dans ce cas les SMS sont envoyés avec un numéro court.
- De paramétrer le compte et les sous-comptes
  - Langue par défaut, Préfixe international, Fuseau horaire, Emetteur par défaut, mode d'envoi par défaut, Stratégie d'envoi par défaut, les URLs de Callback pour les accusés de réception et pour le STOP sms. La possibilité de choisir le mode de routage des réponses (URL de Callback ou boîte de réception du compte).
- De consulter une boîte de réception
  - Cette boîte de réception doit permettre de consulter les réponses envoyées par les destinataires des SMS. L'outil doit permettre de filtrer sur une période les réponses reçues ou de rechercher un numéro de destinataire. Il doit être possible d'exporter le résultat en tenant compte des filtres appliqués.
- De gérer la liste noire
  - Il doit être possible de consulter la liste des destinataires ayant répondu STOP à un SMS. Il doit être possible d'ajouter par compte ou sous-compte des numéros à la liste noire, et doit être possible de supprimer un numéro de cette liste noire.
  - Il doit être possible de rechercher sur une plage de dates ou par numéro si un expéditeur est enregistré dans la liste noire. Il doit être possible d'exporter la liste en tenant compte des filtres appliqués.



- Un numéro enregistré dans la liste noire ne doit pas être destinataire de SMS, il ne doit pas y avoir de facturation de sms dans ce cas.
- De générer ses propres messages paramétrables (publipostage) ;
  - Les messages doivent pouvoir contenir des balises qui seront remplacées par des valeurs d'un fichier csv multicolonnes.
  - Voir le paragraphe publipostage du chapitre « Options et paramètres des APIs »
- D'enregistrer des messages préparés à l'avance
  - Un message prédéfini doit être composé d'un titre et du contenu du message. Un indicateur affiche automatiquement le nombre de caractères utilisés le contenu et le nombre de SMS qui seront utilisés pour envoyer ce message.
- De disposer d'une gestion d'annuaires
  - Il doit être possible de créer des listes de contacts. Une liste de contacts est définie par un nom et la liste des numéros de destinataires. Les numéros en doublons doivent être supprimés automatiquement des listes.
  - Il doit être possible de modifier une liste de contacts en changeant le nom, en ajoutant ou supprimant des destinataires.
  - Il doit être possible de supprimer une liste de contacts
  - Il doit être possible d'exporter une liste de contact vers un fichier (csv).
  - Il doit être possible d'importer une liste de contact à partir d'un fichier (csv).
- D'effectuer un envoi simple :
  - A un destinataire en saisissant le numéro, plusieurs destinataires en saisissant les numéros ou sélectionner une liste de contacts existante.
  - En saisissant le message à envoyer ou en sélectionnant un message préparé à l'avance.
  - D'envoyer le message immédiatement ou de différer l'envoi en saisissant la date et heure souhaités.
  - De sélectionner ou non un émetteur préenregistré (sinon le message sera envoyé via un numéro court).
- D'effectuer un envoi enrichi :
  - A un destinataire, plusieurs destinataires ou sélectionner une liste de contact existante.
  - En saisissant le message envoyé ou en sélectionnant un message préparé à l'avance.
  - D'envoyer le message immédiatement ou de différer l'envoi (date et heure).
  - De sélectionner un émetteur (Numéro court ou émetteur préenregistré).
  - En saisissant un message et en ajoutant un contenu de type média (MMS), un lien court (URL raccourci), un QR Code ou un code barre, un contenu de type HTML.
- De consulter les envois programmés
  - L'outil doit permettre de consulter les envois programmés qui ne sont pas encore envoyés en indiquant la date et heure d'envoi, le mode d'envoi, l'émetteur, les destinataires, le type et le message.
  - Il doit être possible de supprimer un envoi programmé non envoyé.
- De consulter les statistiques
  - L'outil doit permettre de filtrer sur le compte principal, un sous compte particulier ou sur l'ensemble des comptes d'un établissement.
  - L'outil doit disposer de filtres sur une période, par type de message, nombre de messages aboutis
  - Il doit être possible d'exporter les données en fonction des filtres appliqués.
- De consulter la traçabilité

- L'outil doit permettre de consulter l'historique des messages envoyés pour le compte principal, pour un sous-compte ou pour l'ensemble des comptes d'un établissement.
- Il doit être possible de filtrer sur une période (dates et heures), de rechercher un numéro de destinataire, de filtrer par mode d'envoi ou par statuts (code retour d'expédition).
- La liste des résultats doit présenter la date et heure d'envoi, le mode d'envoi, l'émetteur, le destinataire, le type et le statut d'envoi. Il doit être possible de consulter le message envoyé.
- Il doit être possible d'exporter les données en tenant compte des filtres appliqués.
- De gérer la liste des IP autorisées
  - Pour chaque compte ou sous-compte il doit être possible de définir la liste des adresses IP (v4) autorisées à appeler l'API.
  - Si aucune adresse IP n'est définie pour un compte ou un sous compte, n'importe quelle adresse IP pourra utiliser l'API.
  - Il doit être possible de consulter la liste des IP autorisées pour chaque compte ou sous-compte.
  - Il doit être possible de supprimer une IP de la liste des IP autorisées
- De gérer les clés d'API
  - Il doit être possible d'afficher la liste des clés API existantes pour chaque compte ou sous-compte.
  - Il doit être possible de créer une ou plusieurs clés d'API pour un compte ou un sous-compte ? Une description doit être saisie lors de la création.
  - Les clés d'API sont visibles uniquement au moment de leur création. Par la suite, par sécurité, elles ne sont visibles que partiellement.
  - Il doit être possible de désactiver, activer ou supprimer une clé d'API.
  - La liste des clés API doit afficher la clé partiellement, la date et heure de dernière édition de chaque clé et sa description.

## 2.5 Fonctionnalités de la plateforme SaaS pour Numih France

La plateforme SaaS doit permettre à Numih France de :

- Visualiser les comptes des établissements :
  - L'outil doit permettre de visualiser la liste des comptes établissements existants (Identifiant, Dénomination, Solde, Libellé, date et heure de création du compte). Des filtres et un champ doivent permettre de rechercher des établissements.
- Créer et gérer les comptes des établissements de santé :
  - Lors de la création ou modification d'un compte il doit être possible d'indiquer : l'identifiants, le mot de passe principal, la civilité, le nom et le prénom du représentant légal, l'adresse, le code postal, la ville, le pays, le téléphone, le mail de contact, le mail de facturation, le taux de tva.
  - La solution proposée doit permettre pour chaque compte établissement de de personnaliser le logo pour mettre le logo de l'établissement de santé.
  - L'outil doit permettre de paramétrer un seuil de crédit à partir duquel une alerte est envoyée à une adresse mail paramétrable de Numih France.
  - Il ne doit pas y avoir de blocage ou de limitation d'envoi de SMS pour un établissement de santé. Dans le cas où il y a un système de plafond, le système doit être débrayable par paramétrage.
  - Il doit être possible de réinitialiser le mot de passe du compte principal.
  - L'outil doit donner une vision d'ensemble sur chaque compte établissement et permettre de :

- Visualiser les préférences du compte,
  - Visualiser la liste des restrictions d'accès aux API (liste des IP autorisées),
  - Visualiser la liste noire,
  - Visualiser les carnets d'adresses,
  - Visualiser la tarification,
  - Visualiser l'activité (traces et logs),
  - Visualiser le détail de la consommation,
  - Exporter l'historiques avec des filtres par :
    - Période (Dates et heures),
    - SMS vers un pays particulier,
    - SMS longs,
    - La consommation journalière,
    - Les statistiques par pays,
    - Les statistiques par statuts,
    - Par délai d'écoulement
    - Un compte, un sous-compte ou l'ensemble des comptes/sous-comptes d'un établissement),
  - Visualiser la liste des clé API (affichées partiellement),
  - Visualiser la liste des sous-comptes
  - Visualiser les relevés de facturation de l'établissement.
- Consulter les messages envoyés par les établissements de santé
    - L'outil doit permettre de consulter les messages envoyés par l'établissement (par le compte principal, par un des sous-comptes ou par l'ensemble des comptes). Des filtres doivent être disponibles pour recherche par rapport à une période de dates et heures. Il doit être possible d'exporter en tenant compte des filtres appliqués.
  - Disposer d'un outil statistique paramétrable
    - Il doit être possible de filtrer sur une période donnée, par type de message, nombre de messages aboutis, ...) et possédant des outils d'export de données pour l'ensemble des environnements des Centres Hospitaliers ;
  - Disposer d'un outil de facturation du nombre de SMS envoyé par établissement ;
    - Chaque mois, le titulaire doit envoyer à Numih France la facturation des SMS consommés avec le détail du nombre de sms consommés par pays destinataire et par établissement.
    - Le montant facturé à Numih France ne doit pas être visible par les établissements dans la plateforme SaaS. Les établissements ne doivent avoir accès qu'à la quantité de SMS consommés.

## 2.6 Description des APIs attendues

Numih France utilise aujourd'hui en production 3 APIs différentes (issues de 2 fournisseurs différents).

1. La première API pour un usage général, majoritairement du rappel de rendez-vous venant de logiciels multiples et du MFA.
2. La deuxième API, pour un usage interfacé directement dans Dossier Patient Informatisé (DPI) de Numih France, utilisé dans une quarantaine d'établissements de santé.
3. La troisième API, pour usage des mini-sites permet d'envoyer un message qui se traduit par l'affichage du mini-site pour le destinataire, affichant un message et un QrCode.

Les différents types d'API attendu sont :

- Une API par appel d'URL (API 1 Usage général)
  - Mise à disposition d'une servlet appellable par URL POST.
  - Cette API doit prendre en compte les options et paramètres ci-dessous.
  - Le résultat peut être renvoyé directement via la requête au format XML.
- Une API via webservices (API 1 Usage Général & API 2 DPI)
  - Mise à disposition de webservices (Très forte préférence pour le type REST).
  - Cette API doit prendre en compte les options et paramètres ci-dessous.
  - Le résultat peut être transmis directement via la réponse du webservice.
- Une API mail2sms
  - Le mode mail2sms doit permettre via l'envoi d'un mail (adresse à préciser) d'envoyer un ou plusieurs SMS.
  - Les options et paramètres décrits ci-dessous sont à indiquer dans l'objet du mail.
  - Le corps du mail correspond au message envoyé.
  - Le publipostage doit être disponible, les variables sont indiquées dans le corps du mail.
  - En pièce jointe un fichier csv contient la liste des destinataires et des variables à remplacer dans le corps du mail (cf publipostage).
  - Pouvoir mettre à disposition de l'outil des fichiers en mode texte (fichier CSV) pour des envois massifs de SMS ;

## 2.7 Description et paramètres de la première API (Usage général)

Afin de garantir le même niveau de service aux établissements de santé, les APIs doivent proposer options et paramètres ci-dessous :

- La clé d'API,
  - Paramètre obligatoire à chaque appel
  - La clé API créé dans la plateforme SaaS qui est rattachée au compte ou sous-compte qui sera utilisé pour l'envoi
  - Ce paramètre peut être remplacé par un couple « login » et « mot de passe » (sensible à la casse). Dans ce cas-là, le mot de passe peut être substitué par un hash SHA256 (avec des lettres minuscules uniquement). Dans le cas où le hash n'est pas SHA256, une évolution sera à prévoir.
- Le destinataire,
  - Paramètre obligatoire à chaque appel
  - Le numéro de destinataire au format international. Il n'est pas nécessaire de préfixer le numéro avec « + » ou encore « 00 ». Si le numéro est fourni au format national, il doit être tenté d'appliquer le préfixe international par défaut associé au compte.
  - Pour un envoi groupé, il doit être possible d'indiquer les numéros séparés par des points virgules. La limite doit être de 5000 numéros pour une seule requête.
- Le message,
  - Paramètre obligatoire à chaque appel
  - Le message envoyé au destinataire avec un encodage conforme à la valeur du paramètre charset.
  - Il doit être possible d'envoyer des messages segmentés qui seront envoyés en plusieurs SMS. Un maximum de 8 segments (parties) doit être permis.
- Le coding,
  - Paramètre optionnel

- Par défaut Alphanet GSM 7bits. Messages de 160 caractères par SMS, 153 caractères lors d'une concaténation en UDH 6 octets (ou 152 caractères si UDH 7 octets).
- Un tableau des caractères spéciaux et/ou comptants double devra être communiqué.
- Le charset,
  - Paramètre optionnel
  - Par défaut doit être iso88591
  - Préciser s'il y a d'autres charsets autorisés.
- L'UDH,
  - Paramètre optionnel
  - Par défaut doit être un entête de 6 (255 références possibles)
  - Possibilité de passer avec un entête de 7 (255<sup>2</sup> références possibles).
  - Possibilité de désactiver la concaténation
- Le mode,
  - Paramètre optionnel
  - Expert (par défaut)
  - Mode réponse
- L'origine,
  - Paramètre optionnel
  - Par défaut c'est la valeur configurée pour le compte qui est utilisée
  - Indiquer l'émetteur qui sera utilisé pour l'envoi
  - L'émetteur doit avoir été déclaré dans la plateforme SaaS au préalable.
  - Non pris en compte dans le cas du mode réponse (numéro court)
- Le type,
  - Paramètre optionnel
  - Par défaut : Le SMS est enregistré dans la mémoire (Carte SIM ou mobile) du téléphone.
  - « Flash » ou équivalent : Le SMS est directement affiché à l'écran du mobile et n'est pas enregistré dans la mémoire (Carte SIM ou mobile) du téléphone
- La stratégie d'envoi,
  - Paramètre optionnel
  - Par défaut c'est la valeur configurée pour le compte qui est utilisée
  - Communication interpersonnelle privée (entre personnes physiques).
    - Cette stratégie intègre les communications privées entre personnes physiques. L'envoi de messages à caractère commercial par le biais de cette stratégie n'est pas autorisé. La présence d'un numéro en liste noire globale ou privative n'est pas vérifiée.
  - Message d'alerte / Notification proactive / Livraison de service ou de contenu.
    - Cette stratégie intègre les alertes, notifications proactives, ainsi que la livraison de services ou de contenus. L'envoi de messages à caractère commercial par le biais de cette stratégie n'est pas autorisé. La présence d'un numéro en liste noire globale ou privative n'est pas vérifiée.
  - Communication de groupe sans caractère commercial
    - Cette stratégie intègre les communications sans caractère commercial vers un groupe fermé d'utilisateurs. L'envoi de messages à caractère commercial par le biais de cette stratégie n'est pas autorisé. La présence d'un numéro en liste noire globale n'est pas vérifiée. Cependant, la présence d'un numéro en liste noire privative est vérifiée.
  - Communication à caractère commercial
    - Cette stratégie intègre les communications à caractère commercial/marketing. Pour rappel, les messages marketing regroupent toute offre ou promotion d'un



service, même gratuit. La présence d'un numéro en liste noire globale ou privative est vérifiée. Vous devez fournir une solution de désinscription aux destinataires à l'intérieur de votre message. L'envoi de messages marketing est interdit le soir après 20h00, le matin avant 8h00 ainsi que le dimanche et les jours fériés.

- La date d'envoi,
  - Ce paramètre est facultatif
  - Permet d'envoyer le message à une date ultérieure (date=JJ/MM/AAAA).
  - Ce paramètre doit être utilisé conjointement au paramètre « heure ».
  - Par défaut, ou si la date/heure est passée, l'envoi doit être immédiat.
- L'heure d'envoi,
  - Ce paramètre est facultatif.
  - Permet d'envoyer le message à une heure ultérieure (heure=HH:MM)
  - L'heure est au format 24H heure de Paris (UTC+1). Ce paramètre doit être utilisé conjointement au paramètre « date ».
  - Par défaut, ou si les date et heure sont passées, l'envoi doit être immédiat.
- L'identifiant,
  - Ce paramètre est facultatif (format id=xx avec xx de 0 à 9999999999)
  - Si un identifiant est passé, l'API doit retourner OK suivi du numéro d'identifiant passé.
- Le callback,
  - Ce paramètre est facultatif.
  - Si le paramètre callback=1 est ajouté à la requête, les accusés de réception doivent être envoyés sur l'URL de Callback définir dans le compte ou le sous-compte.
- Le complément de Callback,
  - Ce paramètre est facultatif.
  - En complément de l'utilisation de « callback », ce paramètre permet de définir des données additionnelles de votre composition qui seront retournées à la fin de l'URL (en GET) lors de l'appel de votre script.
  - Exemple : mon\_client=123&ma\_campagne=456
  - Ainsi notre exemple devient : cvar=mon\_client%3D123%26ma\_campagne%3D456
- La vocalisation,
  - Ce paramètre est facultatif, par défaut non activé.
  - Ce paramètre doit permettre d'activer la vocalisation pour les numéros fixes de France Métropolitaine (+33) présents dans la liste des destinataires. Si non décroché il doit y avoir un rappel automatique 10 fois maximum. Chaque nouveau rappel doit être espacé de 10 minutes supplémentaires et cumulables par rapport au précédent.
- Le publipostage,
  - Ce paramètre est facultatif, par défaut non activé
  - Cette option doit permettre de personnaliser le message pour chaque destinataire via l'intermédiaire de variables ou balises. L'activation de l'envoi personnalité doit être activable par un paramètre d'activation (personnalise=1).
  - Les variables de remplacement sont à coupler au numéro du destinataire dans un paramètre dédié « dest » formaté de la manière suivante :
    - « numéro;variable1;variable2,numéro;variable1;variable2,numéro;variable1;variable2 »
  - Dans le message le remplacement s'effectuera de la manière suivante :
    - « %0% » est remplacé par le « numéro » du destinataire (format international)
    - « %1% » est remplacé par la valeur « variable1 »



- « %2% » est remplacé par la valeur « variable2 »
- Il doit être possible d'utiliser au moins 10 variables (numéro de destinataire compris, donc de 0 à 9).
- Indiquer les séquences d'échappement ou variables permettant d'intégrer les caractères « , » (virgule) ou « ; » (Point-virgule) dans le contenu des variables.
- Le publipostage doit permettre d'atteindre 5000 destinataires par requête.
- Envoi d'URL raccourcies
  - Activation d'envoi de lien raccourci
    - Ce paramètre est facultatif, par défaut non activé.
    - Paramètre d'activation de la fonctionnalité de raccourcissement de lien
  - Durée de validité d'un lien raccourci
    - Ce paramètre est facultatif,
    - Ce paramètre doit permettre à minima de définir la durée de vue du lien raccourci en 1 et 30 jours. 30 est la valeur par défaut.
  - Suppression du préfixe https
    - Ce paramètre est facultatif, par défaut activé
    - Permet de retirer le préfixe https sur le lien raccourci généré (ce qui permet de gagner quelques caractères).
  - Forçage de redirection https
    - Ce paramètre est facultatif, par défaut activé
    - Ce paramètre permet de forcer le https au lieu du http en activant ce paramètre.

**Note importante:**

**Toutes les fonctionnalités sont obligatoires dans l'API et la réponse du titulaire.**

La mention « Ce paramètre est facultatif » indique que ce paramètre doit être disponible, son utilisation sera un choix de Numih France.

## 2.8 Description et paramètres de la deuxième API (Usage DPI)

L'API d'envoi de SMS au sein du DPI SILLAGE est principalement utilisée pour de la confirmation de rendez-vous et les rappels de ceux-ci aux patients. Le DPI utilise également cette fonctionnalité au travers du module eDen pour notifier les patients et/ou praticien lors du dépôt d'un nouveau document dans l'espace personnel par exemple.

Cette api au format servlet HTTP est mise à disposition sous la forme d'une URL en méthode POST comportant les paramètres body (application/x-www-form-urlencoded) suivant :

- Le nom d'utilisateur (username),
  - Le nom d'utilisateur du compte utilisé pour l'envoi du SMS.
  - Ce champ est obligatoire.
- Le mot de passe (password),
  - Le mot de passe de l'utilisateur du compte utilisé pour l'envoi du SMS.
  - Ce champ est obligatoire.
- L'identifiant de routage (serviceid),
  - L'identifiant de routage (optionnel) celui-ci permet de gérer plusieurs offres différentes sur un compte unique
  - (Par exemple : une offre pour des messages Alerting et une offre pour des messages Marketing en France).
- L'émetteur personnalisé (sender),
  - Le champ de personnalisation de l'émetteur sur 11 caractères alphanumériques.
- Le numéro de téléphone (msisdn),
  - Le numéro de téléphone pour la réception du SMS.

- Ce champ est obligatoire.
- Note : Ce champs peut contenir jusqu'à 500 numéros de téléphone séparé par une virgule au format international.
- L'encodage du message (encoding),
  - Le paramètre d'encodage utilisé pour l'encodage du message.
  - Par défaut ISO-8859-1
- Le message (msg),
  - Le contenu du message à envoyer.
  - Ce champ est obligatoire.
- L'identifiant métier (remoteid),
  - Champ libre limité à 250 caractères alphanumériques,
  - Permet de fournir un identifiant métier renvoyer dans les accusés de réception et réponses.
  - Pour les envois multiples, il est possible d'utiliser un seul remoteid pour tout le push, ou un remoteid par msisdn.
- L'activation de l'unicode (allowunicode)
  - Permet l'utilisation de l'Unicode.
  - Sans ce paramètre, le message sera converti pour être envoyé en utilisant l'alphabet GSM
- Date et heure d'émission du message (timetosend),
  - Au format yyyy-MM-dd HH:mm:ss ex : 2038-01-19 04:14:08
- Création d'un couple unique (uniqueid)
  - Avec le msisdn, crée un couple unique qui permettra de garantir que le même message n'est pas envoyé plusieurs fois, même en cas de réitération d'un envoi.

De plus les entêtes http suivante sont utilisé lors de l'appel à l'API :

- Charset : l'encodage de la requête http différent de l'encodage du SMS.

En réponse de cette appel une réponse au format JSON contenant par message le résultat de l'envoi (ce résultat est nommée ticket dans ce format). Le ticket d'un envoi doit contenir à minima les informations suivantes :

- Numéro de téléphone du destinataire
  - Le numéro de téléphone auquel le SMS est envoyé
- Nombre de SMS utilisé
  - Le nombre de SMS utilisé pour acheminer le message au destinataire
- Code de retour de l'envoi
  - Entier valant 0 si aucune erreur indiquant la raison de l'échec de l'envoi
  - Les différentes valeurs possibles sont :
    - -1 : Authentication failed
    - -2 : Invalid destination address. Champ msisdn mal formaté.
    - -3 : Invalid operator
    - -4 : No route defined. Tentative d'envoi dans un pays dont l'offre n'est pas câblée.
    - -5 : No transaction found
    - -6 : Parameter "method" not found. Check parameters
    - -7 : Time to send not allowed
    - -8 : Datacoding scheme invalid
    - -9 : Serviceid not found
    - -10 : Message too long
    - -11 : Not enough credit
    - -12 : Invalid parameter
    - -13 : PushAction not found
    - -14 : Maximum message limit

- -15 : PID invalid
- Raison de ce code de retour
  - En plus du code de retour le ticket comporte le message explicite de ce code de retour dans ce champ.
- Numéro de ticket (numéro de l'envoi pour la traçabilité)
  - Il s'agit d'un uuid permettant de retrouver dans l'historique l'envoi du message

## 2.9 Description et paramètres de l'API pour les mini-sites

Le service doit permettre au destinataire de recevoir un SMS contenant une URL raccourcie menant vers un mini-site (ex ci-dessous) contextualisé à un établissement de santé (Un mini-site par établissement de santé).

Le mini site doit afficher le logo de l'établissement de santé, un titre, un texte, un QR Code et un pied de page.

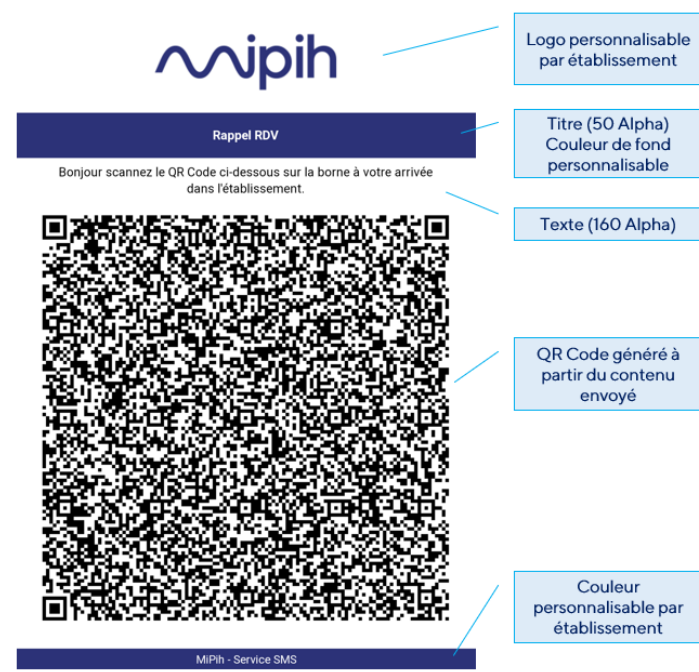
Le titre, le texte et le contenu du QR Code doivent pouvoir être transmis via la même API que l'envoi du SMS et via des paramètres dédiés.

Il doit être possible de passer en paramètre la durée de vie de l'URL raccourcie.

Chaque établissement de santé aura un « modèle » de mini-site ou il devra être possible de personnaliser :

- Le logo de l'établissement
- La couleur de fond du bandeau contenant le titre
- La couleur de fond du bandeau du bas de page.

Sur la page modèle d'un établissement, à la demande du Numih France et par établissement, il doit être possible de modifier l'ordre du texte et du QR Code dans le mini-site.



- Contenu (Contenu du QR Code),
  - Le contenu qui sera utilisé pour générer le QR Code sur la page du mini site vers laquelle pointer le mini lien contenu dans le SMS.
  - QR Code (ISO 18004). Limite de caractères numériques : maximum 7 089, caractères alphanumériques : maximum 4 296

- Niveau de redondance par défaut : H (soit environ 30%).
- Titre ,
  - Un texte de XX caractères qui sera affiché sur le bandeau du haut (sous le logo de l'établissement).
- Texte,
  - Un texte de 160 caractères qui sera affiché sous le titre mini site.
- DureeDeVie,
  - Champ numérique permettant de définir la durée de vie du lien généré, entre 1 et 730 jours (soit deux ans) à compter de la date de génération.
  - En cas d'envoi différé, vous devez tenir compte du décalage dans le temps.

## 2.10 Principe général de routage

Par défaut, pour les pays autres que la France, l'acheminement des SMS s'effectuera via des routes internationales standard.

Le pouvoir adjudicateur précise que la grande majorité des clients finaux est située en France métropolitaine et en outre-mer.

### 2.10.1 Option de routage local

Le titulaire devra proposer, en complément, une option de routage via des routes locales pour certains pays (Maroc, Belgique, ...).

Cette option ne sera pas activée par défaut et devra pouvoir être mise en œuvre à la demande, au cas par cas, pour certains clients ou établissements se trouvant dans le pays concerné.

### 2.10.2 Modalités d'activation

Le titulaire devra décrire précisément la procédure d'activation des routes locales pour un établissement dans un pays avec les étapes nécessaires, les délais de mise en œuvre et les prérequis éventuels (techniques, réglementaires, contractuels) ;

Il devra aussi indiquer les éventuelles contraintes spécifiques par pays :

- Enregistrement d'expéditeur (Sender ID),
- Obligations réglementaires locales,
- Restrictions de contenu ou d'usage,
- Les modalités de support et d'accompagnement lors de l'activation.

Le titulaire devra garantir que l'activation puisse être réalisée sans interruption de service et sans impact sur les autres clients.

### 2.10.3 Tarification

Le titulaire devra distinguer clairement :

- Les tarifs applicables aux routes internationales standard
- Pour les pays demandés, les tarifs applicables aux routes locales

À ce titre, il devra fournir une grille tarifaire détaillée par pays demandé et par type de route en précisant les éventuels :

- Coûts d'activation
- Frais de mise en conformité (ex : enregistrement d'expéditeur)
- Coûts récurrents associés
- Indiquer les différences de tarification entre routes locales et internationales, en les justifiant (qualité, conformité, performance)

Toute évolution tarifaire devra être encadrée conformément aux dispositions du marché.

#### 2.10.4 Évolutivité

Le pouvoir adjudicateur pourra :

- Par avenant, ajouter ou retirer des pays concernés par l'option de routage local
- Demander l'activation de cette option pour de nouveaux clients ou établissements en cours d'exécution du marché

Le titulaire devra être en capacité de répondre à ces demandes dans des délais raisonnables, qu'il précisera dans son offre.

### 2.11 Conformité des routes

Devront être justifiés tout recours, même partiellement, à des mécanismes d'acheminement reposant sur :

- des contournements des voies officielles opérateurs,
- des pratiques de transformation de trafic (notamment A2P vers P2P),
- des infrastructures de type SIM farm ou équivalent,
- ou tout autre procédé non conforme aux réglementations locales et aux conditions des opérateurs.

Le titulaire devra indiquer explicitement si les routes proposées sont de type "direct to operator (DTO)", "SS7", ou "grey/alternative".

#### 2.11.1 Obligation de transparence sur le routage

Sur demande, le titulaire devra être en mesure de :

- Décrire précisément :
  - La nature de ses interconnexions (directes opérateurs ou via agrégateurs),
  - Le nombre d'intermédiaires impliqués dans l'acheminement,
  - Les pays dans lesquels il dispose d'accords directs.
- Démontrer l'existence d'accords directs avec les opérateurs et devra garantir que l'ensemble des routes utilisées respecte :
  - Les réglementations locales des pays de destination,
  - Les exigences des opérateurs (notamment en matière de trafic A2P),
  - Les obligations d'enregistrement d'émetteur le cas échéant.

#### 2.11.2 Cohérence tarifaire (anti-prix anormalement bas)

Une attention particulière sera portée aux offres présentant des tarifs significativement inférieurs aux prix de marché.

Le pouvoir adjudicateur se réserve le droit de demander toute justification nécessaire.

À défaut d'explication satisfaisante, l'offre pourra être rejetée comme reposant sur des pratiques de routage non conformes.

## Article 3. Analyse de risque simplifiée

### 3.1 Fonctionnalités du service

Ce paragraphe liste les risques pouvant impacter les principales fonctionnalités du service d'envoi de SMS.

Le titulaire devra mettre en œuvre les mesures nécessaires pour prévenir, détecter et corriger les incidents associés à ces risques, notamment :

- Risque de détournement de la fonction d'annulation ou de programmation de l'envoi de SMS par malveillance interne ou compromission.
- Risque d'usurpation d'identité lors de l'accès à l'interface d'administration ou aux API, permettant un usage frauduleux du service ou une compromission de l'infrastructure.
- Risque de non-délivrabilité ou de retards dans les envois. Délai ou échec d'acheminement des SMS, impactant le bon fonctionnement des services clients ou d'alerte (ex : messages critiques non reçus).
- Risque de saturation du service ou indisponibilité. Interruption ou ralentissement du service, causé par une attaque DDoS, une surcharge ou une défaillance technique.
- Risque de compromission de données personnelles. Interception, fuite ou altération des données à caractère personnel (ex. numéros de téléphone, contenus de messages), entraînant un risque RGPD.
- Risque d'accès non autorisé à l'interface d'administration ou à l'API. Utilisation frauduleuse du compte prestataire pour envoyer des SMS en masse ou accéder aux données.
- Risque de détournement de l'API (ex : rebond pour du spam ou du phishing). Utilisation abusive de l'infrastructure pour envoyer des messages frauduleux sous l'identité du client.
- Risque de non-conformité réglementaire (ex : opt-in / opt-out, mentions légales). Envoi de SMS non conformes à la réglementation (notamment en matière de consentement ou d'horaires d'envoi), exposant le client à des sanctions.
- Risque de dépendance à un seul fournisseur technique en cas d'incident. Si la solution repose sur un unique fournisseur SMS, une indisponibilité pourrait avoir un impact critique (d'où l'intérêt de prévoir la multi-connectivité dans le marché).
- Risque de modification malveillante ou non autorisée des paramètres tarifaires ou d'usage. Modifications qui pourraient entraîner une surfacturation ou un contournement des plafonds contractuels.

## 3.2 Gestion des interfaces

- Risque de compromission des systèmes d'information interconnectés, en cas d'attaque informatique ciblant le service d'envoi de SMS, pouvant entraîner la diffusion de code malveillant, l'injection de données corrompues ou l'ouverture de vecteurs d'attaque vers d'autres briques du système d'information de l'acheteur.
- Risque d'interruption ou de dégradation des systèmes interconnectés, en cas de transmission de messages contenant un contenu ou une syntaxe non conforme (mauvais encodage, champs obligatoires manquants, données erronées), pouvant provoquer des erreurs d'interprétation ou une corruption de traitement côté client.

## 3.3 Gestion des comptes et des habilitations

- Risque d'attribution d'habilitations non conformes au principe du besoin d'en connaître, pouvant permettre à un utilisateur non autorisé d'accéder à des informations confidentielles ou à des



fonctionnalités sensibles du service (modification de paramètres d'envoi, accès aux historiques, export de données, etc.).

- Risque d'usurpation de comptes inactifs ou non désactivés, notamment suite à un départ, un changement de fonction ou une absence de nettoyage régulier des habilitations, exposant le système à des usages non autorisés du service.

## **Article 4. Environnement d'exécution du marché**

### **4.1 Environnement technique**

Le titulaire doit fournir une infrastructure technique sécurisée, disponible et performante pour permettre l'envoi de SMS via des interfaces accessibles par l'établissement.

- Les serveurs utilisés pour le traitement et la transmission des SMS devront être situés dans l'Union européenne.
- Le titulaire doit disposer de mécanismes de haute disponibilité et de reprise d'activité (PRA/PCA).
- Le Titulaire devra prendre en compte les différents environnements mis à disposition ou attendus :
  - o Environnement de développement/test pour la validation initiale des interfaces et l'intégration technique.
  - o Environnement de préproduction pour les tests utilisateurs et la validation d'homologation.
  - o Environnement de production, stable, sécurisé et conforme aux exigences de disponibilité du marché.
- L'architecture du système repose sur un modèle n-tiers, cloisonnant les couches présentation, logique métier, accès aux données et services externes.

### **4.2 Environnement applicatif**

Une interface d'administration accessible en ligne (SaaS), sécurisée, permettant la supervision des envois, la gestion des comptes, la consultation des historiques et des statistiques.

Une API sécurisée REST/JSON permettant l'envoi automatisé de messages, leur suivi (accusés de réception, statuts, etc.) et la gestion des campagnes (https/TLS 1.2 ou supérieur).

Un module de gestion des journaux d'envoi et des logs de traçabilité, interrogeable ou exportable à des fins d'audit.

### **4.3 Interopérabilité et interfaces externes**

Le titulaire doit garantir la compatibilité avec les systèmes applicatifs de l'établissement via :

- Une API documentée (OpenAPI/Swagger ou documentation équivalente à fournir),
- Des formats standards de données (JSON obligatoirement et XML en option),
- Une capacité de journalisation pour le suivi des événements et une infrastructure de supervision ou de collecte de logs.
- L'API doit pouvoir être appelée depuis des applications tierces (ex. : logiciels de gestion de rendez-vous ou de soins).
- Le titulaire devra assurer un support technique pour les intégrations.

## 4.4 Livrables de la prestation

Les livrables suivants sont attendus au titre du marché :

- Dossier d'architecture technique et applicative de la solution.
- Plan d'intégration et de test des interfaces.
- Documentation technique de l'API (swagger, schéma de flux, authentification, quotas, erreurs, etc.).
- Fiche de volumétrie prévisionnelle.
- Procédures d'exploitation, de supervision, de maintenance et d'escalade.
- Rapport de recette technique et de validation fonctionnelle.
- Journal de suivi des envois (statut des messages, taux de succès, échecs, logs anonymisés),
- Statistiques de volumétrie mensuelles sur les envois (nombre de messages envoyés, taux de succès, messages non remis),
- Certificats ou attestations de conformité (hébergement UE, sécurité, RGPD).
- Rapport d'audit de sécurité le plus récent (moins d'un an).

## 4.5 Volumétrie, dimensionnement et performance

Le service SMS de Numih France est utilisé par deux cents établissements de santé. Le volume global de SMS envoyé pour l'ensemble des établissements est de **14 millions de SMS par an environ**.

- Chaque établissement utilisant la plateforme SaaS possède à minima un compte principal.
  - En général, les établissements utilisent peu de sous-comptes.
  - Un établissement possède plus de 40 sous-comptes.
- Environ 80 établissements utilisent l'API pour envoyer unitairement des SMS
  - SMS MFA ou SMS métier comme du rappel de Rendez-vous
  - La majorité des établissements utilisent l'envoi de SMS immédiat avec personnalisation de l'émetteur et la vocalisation via l'API servlet.
  - Quelques établissements utilisent le service via les APIs webservice ou mail2SMS.
- Environ 40 établissements utilisent l'API DPI pour effectuer du rappel de rendez-vous

Le service devra être scalable, le titulaire devra indiquer ses capacités d'absorption en termes de nombre de SMS simultanés par minutes/par heure.

Le Titulaire doit proposer un service avec un niveau de performance compatible avec l'usage du service par les personnels des établissements : le temps de réponse perçu par l'utilisateur doit être raisonnable en fonctionnement nominal.

Le Titulaire produit, à la demande de Numih France, les indicateurs de performance qui seront définis dans le cadre de l'exécution du marché.

Le Titulaire doit fournir un paramétrage permettant pour un compte de limiter le volume de sms envoyés mensuellement, ou de débrayer tout contrôle pour permettre une consommation sans limite.

## Article 5. Conditions d'exécution des prestations

Le présent article définit les modalités d'exécution des prestations attendues dans le cadre du marché, notamment les conditions d'intervention, les exigences de maintenance et supervision, ainsi que l'organisation des parties prenantes.

## 5.1 Intervention à distance

Le Titulaire interviendra principalement à distance, que ce soit pour les phases de cadrage, d'intégration, de supervision ou de maintenance.

Les échanges se feront par visioconférence, outils collaboratifs, courriel ou téléphone.

## 5.2 Supervision du service

Le Titulaire devra mettre en œuvre une supervision technique proactive du service incluant :

- Le suivi des métriques clés (taux de délivrabilité, latence d'envoi, erreurs API, consommation de quotas)
- Des alertes en cas de dysfonctionnement ou d'indisponibilité (mail, webhook ou portail)
- La fourniture d'un rapport de supervision mensuel incluant les incidents, les performances et les actions correctives engagées.
- Des interfaces de monitoring accessibles par le pouvoir adjudicateur ou ses représentants sont recommandées.

## 5.3 Organisation et méthodologie

Le Titulaire devra proposer dans son offre :

- Une organisation adaptée à la nature du marché moyens humains & techniques)
- Une méthodologie claire d'exécution des prestations (planification, suivi des tâches, points de contrôle, communication) ;
- Les outils utilisés pour la gestion des incidents, des livrables et de la communication (ex : outil de ticketing, plateforme de versioning, planning partagé).

Le pouvoir adjudicateur se réserve le droit de valider ou d'exiger des ajustements dans l'organisation du Titulaire si celle-ci n'apparaît pas compatible avec les exigences du marché.

## 5.4 Organisation du support et modalités de gestion des incidents

Le titulaire s'engage à assurer un support technique couvrant :

- Les modalités du support (jours/heures, niveaux d'incident, langue),
- L'outil de ticketing,
- Le processus de support détaillé (escalade, délais de réponse, rôles).

### 5.4.1 Modalités générales du support

Le Titulaire s'engage à assurer un service de support technique couvrant l'ensemble des fonctionnalités du service fourni.

Les modalités sont les suivantes :

- Support en français obligatoire, au minimum par courriel et plateforme de ticketing.
- Disponibilité du support : jours ouvrés (du lundi au vendredi) de 8h00 à 18h00 (CET/CEST).
- Possibilité de prise en charge étendue (soirs, week-ends) en cas d'incident critique, selon SLA ou conditions spécifiques.
- Accès garanti aux mises à jour de sécurité, aux correctifs, et à l'historique des interventions.

### 5.4.2 Outils de ticketing

Le Titulaire devra mettre à disposition une plateforme de ticketing en ligne dédiée au marché, répondant aux exigences suivantes :

- Création, suivi et mise à jour des tickets par le pouvoir adjudicateur.
- Identification par numéro de ticket, statut, priorité, demandeur, date de création/modification.
- Possibilité de joindre des pièces (logs, captures, extraits de messages).
- Journalisation de l'ensemble des échanges.
- Accès à un tableau de bord récapitulatif des demandes ouvertes, en cours ou résolues.

Le pouvoir adjudicateur pourra exiger l'intégration ou la compatibilité avec ses propres outils (via API ou interface manuelle).

### 5.4.3 Processus de support et d'escalade

Le processus de traitement des incidents devra inclure les étapes suivantes :

1. Création du ticket par le pouvoir adjudicateur ou via détection automatique.
2. Accusé de réception automatique et affectation d'un référent technique chez le Titulaire.
3. Analyse préliminaire et qualification du ticket (niveau 1, 2, 3).
4. Traitement de l'incident dans les délais contractualisés.
5. Communication régulière avec le responsable de projet ou référent du pouvoir adjudicateur.
6. Clôture du ticket avec validation du demandeur.
7. Archivage et documentation pour audit ou traçabilité future.

En cas de non-respect des délais ou d'incident récurrent, un processus d'escalade hiérarchique devra être prévu, avec la possibilité de faire intervenir un chef de projet senior ou une direction technique chez le Titulaire.

### 5.4.4 Suivi et reporting du support

Le Titulaire devra fournir un rapport mensuel ou trimestriel de support comprenant :

- Nombre de tickets ouverts / clos / en cours par niveau.
- Délai moyen de prise en charge et de résolution.
- Analyse des récurrences éventuelles.
- Taux de satisfaction ou d'acceptation des solutions proposées.

Ces rapports seront examinés lors des comités de pilotage de marché, organisés selon la fréquence dans le CCTP ou en accord avec Numih France.

## 5.5 Réversibilité

À l'issue du marché, ou en cas de résiliation anticipée, le Titulaire devra garantir une réversibilité complète, ordonnée et sécurisée du service technique d'envoi de SMS, permettant au pouvoir adjudicateur de migrer vers une solution alternative sans rupture de service ni perte d'informations essentielles.

### 5.5.1 Absence de restitution des données

Aucune donnée nominative ou métier n'étant stockée ou transférée vers l'acheteur dans le cadre du service, aucune restitution de données n'est attendue.

Toutefois, le Titulaire demeure responsable de la conservation légale des journaux et des logs de traçabilité (statuts d'envoi, horodatages, numéros de téléphone, messages transmis) pour la durée légale applicable, y compris après la fin du contrat.

### 5.5.2 Prestations attendues pendant la réversibilité

Le Titulaire devra notamment :

- Fournir la documentation technique complète permettant de reprendre les intégrations (API, webhook, interfaces).
- Transmettre un état de configuration des environnements et des éventuels flux interfacés.
- Assurer un accompagnement technique (ateliers, échanges techniques, hotline réversibilité) pour la mise en œuvre du nouveau prestataire.
- Fournir des extractions exhaustives des comptes, sous-comptes et toutes informations qui seraient nécessaires pour la reprise de l'existant pour permettre au nouveau titulaire de reprendre l'activité et assurer une continuité de service.
- Procéder à la clôture sécurisée des comptes d'accès du pouvoir adjudicateur et à la désactivation définitive des interfaces.

### 5.5.3 Durée et calendrier de réversibilité

La réversibilité s'exécutera sur une période maximale de [1 à 2 mois], à compter de la notification de fin de contrat ou selon les modalités prévues dans le CCAP.

Le Titulaire s'engage à collaborer activement pendant cette période, sans interruption de service, et sans facturation supplémentaire au titre de cette assistance, sauf disposition contraire précisée au BPU ou à l'acte d'engagement.

### 5.5.4 Traçabilité et conformité

Le Titulaire reste responsable, pendant et après la réversibilité, de la conservation et de l'accessibilité des données de traçabilité à des fins de contrôle ou d'audit administratif ou judiciaire.

Toute conservation ou suppression anticipée non autorisée pourra faire l'objet de sanctions contractuelles.

## Article 6. Suivi et engagements du Titulaire

### 6.1 Niveau d'engagement en cas d'incident

Les actions correctives sont engagées selon les délais d'intervention suivants, en fonction de la sévérité de l'incident ou de la demande.

Classification		Délai de prise en compte	Garantie de Temps de Rétablissement (GTR)
Sévérité de l'incident ou de la demande	Critique (Sévérité 1)	15 minutes	04h00 - 7j/7 24H24
	Haute / urgente (Sévérité 2)	30 minutes	08h00 ouvrées
	Normal (Sévérité 3)	01h00	24h00 (J+1)
Demande de service		04h00	48h00 (J+2)

- Durée maximale d'arrêt acceptable (DMIA) : 24 heures

### 6.2 Niveaux de service (SLA) du titulaire

Tableau des exigences minimales à respecter dans le cadre de la fourniture d'un service d'envoi de SMS.

Rubrique	Exigence minimale	Commentaires / Détails
<b>Disponibilité du service</b>	≥ 99,9 % mensuelle	Hors maintenance planifiée ; mesure sur 24h/24, 7j/7
<b>Maintenance planifiée</b>	≤ 4 h / mois	Notifiée 72h à l'avance
<b>Délai d'envoi SMS - Transactionnels</b>	≤ 5 secondes dans 95 % des cas	Exemple : OTP, alertes
<b>Délai d'envoi SMS - Informatifs</b>	≤ 60 secondes dans 95 % des cas	Exemple : campagnes, rappels
<b>Taux de réussite d'envoi</b>	≥ 98 % pour les numéros valides	Hors erreurs utilisateur (ex. numéro erroné)
<b>Réessaie en cas d'échec</b>	3 tentatives dans un délai de 15 minutes	Pour les échecs non imputables à l'acheteur
<b>Traçabilité &amp; logs</b>	Accès aux logs via interface ou API sécurisée	Inclut les raisons d'échec
<b>Support technique</b>	Jours ouvrés (L-V), 9h à 18h	Contact par ticket et e-mail
<b>Réactivité - incident critique (P1)</b>	Prise en charge < 1h / Rétablissement < 4h	Incident de type arrêt complet du service
<b>Rapport mensuel de performance</b>	Obligatoire	Doit inclure : disponibilité, taux de réussite, délais, incidents, MTTR
<b>Pénalités - Disponibilité &lt; 99,9 %</b>	5 % du montant mensuel (entre 99,5 % et 99,9 %)	
<b>Pénalités - Délai non respecté</b>	2 % par tranche de 5 % de dépassement	Concernant les délais transactionnels

## 6.3 Maintenance

Numih France assure la maintenance de niveau 1 et 2 et transmet au Titulaire la maintenance de niveau 3 :

- Niveau 1 : assistance aux utilisateurs
- Niveau 2 : traitement des problématiques liées à des incidents connues et répertoriées, liées à de l'interopérabilité
- Niveau 3 : traitement des problématiques nécessitant une intervention au sein du code source ou de la responsabilité du Titulaire

Le périmètre des niveaux de support sera précisé au sein d'un RACI support partie intégrante du Plan Assurance Qualité.

Le Titulaire informe Numih France de toute opération de maintenance dans un délai minimum de 10 jours avant l'opération de maintenance.

Le Titulaire s'engage à programmer ses interventions de maintenance ayant un impact sur la disponibilité du service en dehors de la plage horaire de 8h à 18 h jours ouvrés. Dans la mesure du possible et selon les circonstances, les interventions ne sont pas recommandées à partir du jeudi après-midi et les veilles de jours fériés.

Le Titulaire devra fournir un service de maintenance corrective, évolutive et préventive, comprenant :

- La prise en charge des anomalies détectées ou signalées, selon un plan de niveau de service (SLA) défini contractuellement ;
- La mise à jour de la documentation technique après chaque évolution ;
- La gestion des mises à jour de sécurité ou des patches critiques ;
- Un canal de support technique accessible pendant les jours ouvrés, avec la possibilité d'escalade pour les incidents majeurs.

### 6.3.1 Évolutives

La maintenance évolutive inclut :

- La mise à disposition des versions comprenant les évolutions réglementaires, légales, fonctionnelles hormis des évolutions majeures qui pourraient exiger des moyens exceptionnels,
- La mise à disposition des versions prenant en compte les évolutions fonctionnelles pour les modules existants et acquis,



- La révision de la solution suite à un changement ou une évolution des environnements de base supportant la solution, validés par Numih France.

#### Livrables attendus et délais d'exécution

Livrables	Délais	Vérification
<b>Spécifications fonctionnelles des évolutions prévues <i>si applicable</i></b>	Lors des comités amont à la livraison de la version	10 jours
<b>Dossier de conception et d'architecture <i>si impact sur le DAT</i></b>		
<b>Rapports de test</b>	5 jours après la livraison de la version	10 jours
<b>Manuel d'installation mis à jour <i>si applicable</i></b>	Lors du comité suivant	10 jours
<b>DAT mis à jour <i>si applicable</i></b>		
<b>Manuel d'exploitation mis à jour <i>si applicable</i></b>		
<b>Manuel utilisateur mis à jour <i>si applicable</i></b>		
<b>Manuel administrateur mis à jour <i>si applicable</i></b>		
<b>Documentation du catalogue de données mi à jour <i>si applicable</i></b>		

### 6.3.2 Correctives

La maintenance corrective a pour but de corriger les anomalies de fonctionnement entraînant un défaut ou une indisponibilité. Total ou partiel de la solution.

Cette maintenance est également assurée par la mise à disposition de versions intermédiaires de la solution intégrant les corrections.

Le Titulaire met à disposition les versions correctives de ses solutions, même si aucun incident n'a été détecté et ouvert auprès de sa Hotline.

Le Titulaire est responsable de la maintenance de son service. A ce titre il assure ou met à disposition les éléments permettant à Numih France d'assurer :

- Le bon fonctionnement des infrastructures mises en place
- Le suivi de l'évolution des capacités
- La gestion de l'obsolescence
- L'application des patches (y compris Sécurité) et montée de version
- La gestion des incidents
- La gestion des autorisations spécifiques liées aux ouvertures de pare-feu, etc.

#### Livrables attendus et délais d'exécution

Livrables	Délais	Vérification
<b>Rapports de test</b>	2 jours après la livraison du correctif	5 jours
<b>Manuel d'installation mis à jour <i>si applicable</i></b>	Lors du comité suivant	2 jours
<b>DAT mis à jour <i>si applicable</i></b>		
<b>Manuel d'exploitation mis à jour <i>si applicable</i></b>		
<b>Manuel utilisateur mis à jour <i>si applicable</i></b>		
<b>Manuel administrateur mis à jour <i>si applicable</i></b>		
<b>Documentation du catalogue de données mis à jour <i>si applicable</i></b>		
<b>Fiche d'incident renseignée</b>	A la clôture du ticket	5 jours

## **Article 7. Comitologie et pilotage du marché**

Le service est jugé critique pour Numih France.

À ce titre il est nécessaire de prévoir des modalités de suivi des différentes phases du service.

Les actions à réaliser par le titulaire dans le cadre du suivi du marché sont sous la responsabilité de l'interlocuteur en charge du pilotage du marché :

- Planifier toutes les réunions
- Animer toutes les réunions
- Préparer le support de réunion
- Fournir le compte-rendu pour chaque réunion

Les critères de fin de transition doivent être définies par les parties et faire l'objet d'une validation formelle en comité de pilotage.

Toute décision prise lors des réunions de lancement, de pilotage ou lors de réunion exceptionnelle devront être validées par Numih France et tracées.

### **7.1 Calendrier et Comitologie**

#### **7.1.1 Calendrier**

Le calendrier attendu pour la mise à disposition du service par le Titulaire sera le suivant :

- Réunion de lancement
  - Sous 15 jours suite à la notification du marché
  - Cette réunion a pour objectif de démarrer le projet.
- Réunion de fin de transition
  - Au plus tard 2 mois suite à la notification du marché
- Cette réunion a pour objectif de valider la solution
- Mise en œuvre de la solution
  - Au plus tard 3 mois suite à la notification du marché
- Réunion de passage en production
  - Dès que la solution est mise en œuvre
  - Validation de la conformité de la solution
  - Cette réunion a pour objectif de définir la date de bascule vers le service du nouveau titulaire

La phase de mise en œuvre intégrera :

- la gestion de projet nécessitant la mise en place de comités,
- la formation au logiciel pour les différents types d'utilisateurs (administrateur, gestionnaire, ...),
- de l'accompagnement pour le paramétrage du logiciel,
- de l'accompagnement à la reprise de l'existant et migration vers le service du nouveau titulaire
- et de l'assistance pour la mise en œuvre des interfaces.

#### **7.1.2 Réunions**

Les réunions entre les parties auront lieu dans les locaux de Numih France ou en audio ou en visioconférence, au choix de Numih France.

Le titulaire aura la charge de préparer le support correspondant à l'ordre du jour de chaque réunion planifiée et le transmettre au plus tard 2 jours ouvrés précédant la réunion.

Chaque réunion fera l'objet d'un compte-rendu qui sera rédigé par le titulaire et qui sera envoyé au plus tard 5 jours après chaque réunion. Le compte-rendu reprendra les points à l'ordre du jour ainsi que les points abordés en réunion.

A chaque réunion de pilotage (suivi et bilan final), le titulaire fournira un reporting régulier de son activité. Le reporting doit notamment permettre à Numih France de suivre l'utilisation, les engagements et la sécurité des activités.

#### 7.1.2.1 Réunion de lancement

Une réunion de lancement sera organisée par le titulaire quinze jours au plus tard après la notification du marché.

Cette réunion a pour objectif de démarrer le projet.

Elle a pour ordre du jour :

- Présentation de l'équipe Numih France et des différentes responsabilités des intervenants
- Présentation de l'équipe du titulaire et des différentes responsabilités des intervenants
- Présentation de la solution de fourniture de SMS
- Présentation des fonctionnalités obligatoires
- Présentation des exigences de sécurité
- Présentation du planning de la période de transition
- Présentation des critères de fin de transition
- Présentation du Pilotage, suivi et reporting mis en place intégrant la présentation du tableau de bord des indicateurs
- Présentation des premiers éléments de pilotage, suivi et reporting
- Présentation de tout élément permettant de cadrer et maîtriser la qualité du service rendu
- Ambiguïtés éventuelles à lever

#### 7.1.2.2 Réunion de fin de transition

Une réunion de fin de transition sera organisée par le titulaire à la fin de la transition et au plus tard 2 mois après le début du marché.

Cette réunion a pour objectif de valider la solution.

Les éléments abordés traiteront de la bonne intégration de la nouvelle solution et prendront en compte a minima les éléments suivants :

- Rappel du périmètre
- Synthèse des actions réalisées lors de la transition
- Validation technique : intégration API
- Validation des engagements
- Conformité sécurité
- Impact sur les utilisateurs
- Plan de Post-bascule : proposition d'un monitoring et d'une réactivité renforcés
- Validation de la phase de transition par Numih France

#### 7.1.2.3 Réunion de passage en production

Une réunion de passage en production sera organisée par le titulaire à la suite de la mise en œuvre de la solution.

Cette réunion a pour objectif d'acter le passage en production et définir la date de bascule vers le service du nouveau titulaire.

#### 7.1.2.4 Réunion de pilotage

Une réunion de suivi se tiendra trimestriellement la première année. Le rythme pourra être ajusté en accord avec Numih France.

Ces réunions de pilotage permettront de suivre les engagements réciproques du titulaire et de Numih France, les objectifs communs et les plans d'action associés.

Le titulaire présentera notamment les éléments suivants :

- Tableau de bord des Indicateurs : indicateurs SLA, indicateurs incidents, Tickets
- Suivi des indicateurs SLA

- Suivi des indicateurs en cas d'incidents
- Suivi des tickets
- Zoom sur les 10 établissements les plus consommateurs de SMS et nombre de SMS consommés associés
- Suivi contractuel et financier
- Présentation de la feuille de route, présentation des nouvelles fonctionnalités à venir

Le titulaire peut proposer de nouveaux indicateurs afin d'améliorer la qualité du service rendu.

## 7.2 Phase de transition

Les objectifs de la phase de transition sont :

- Assurer la continuité de service
- Valider les intégrations techniques
- Valider les performances du nouveau fournisseur
- Sécuriser la bascule finale

Afin de garantir la continuité de service et la qualité du service, une période de transition structurée doit être mise en place.

Une approche progressive est attendue afin de sécuriser chaque étape et garantir le succès de la bascule finale. Le titulaire détaillera la phase de transition qu'il propose de mettre en œuvre pour reprendre les comptes, sous-comptes, et toutes informations nécessaires pour la reprise de l'existant et assurer la continuité de service.

## 7.3 Phase de production

Cette phase concerne le passage en fonctionnement nominal du service intégrant le support de la solution.

Pendant cette phase nominale, des comités de pilotage seront mis en place sur toute la durée du marché pour assurer le suivi du service (suivi de la qualité, des incidents et des engagements), comme indiqué dans le chapitre précédent.

En complément des comités réguliers, des réunions ponctuelles pourront être organisées à l'initiative du titulaire ou de Numih France, en fonction des besoins identifiés au cours de l'exécution du marché. Ces réunions auront pour objet de traiter des sujets spécifiques nécessitant un échange approfondi ou une prise de décision rapide. A l'issue de ces réunions, un compte rendu sera rédigé par le titulaire et transmis à Numih France dans un délai raisonnable.

## 7.4 Phase de réversibilité

Lors de la phase de réversibilité, Numih France souhaite mettre en place une période de suivi rapproché. Pendant cette période, le Titulaire s'engage à collaborer activement.

## Article 8. Clauses de sécurité

Pour Rappel : la charte sécurité du système d'information de Numih France, énonce les exigences relatives à la sécurité de ses systèmes d'information. Elle est applicable et à signer dans les contextes ci-dessous :

- Pour les prestataires externes, ayant accès dans le cadre de leur mission à tout ou partie des Systèmes d'Information de Numih France.
- Pour les Titulaires de marché associés aux technologies de l'information et de la communication (ordinateurs, logiciels, développements ou hébergement d'application via le web) ainsi qu'aux fournitures et services annexes

Lorsque le candidat a obtenu une certification de sécurité (HDS, 27001, RGS, ...) sur le périmètre de la prestation visée par le présent marché, un certificat en cours de validité est à fournir.

Dans le cadre de la réalisation de la prestation, le Titulaire s'engage à mettre en application les règles ci-dessous. Les tableaux doivent être complétés par la description de la mise en œuvre et des éventuels écarts. Il revient à Numih France d'apprécier ces réponses, d'exiger si nécessaires des compléments et in fine d'accepter les risques résiduels liés aux éventuels écarts. Certaines exigences peuvent être sous responsabilité partagée.

### 8.1 Sécurité du Titulaire

Le terme Plateforme (d'intervention) désigne le Système d'Information propriétaire et sous responsabilité du Titulaire utilisé pour rendre le service (plateforme d'hébergement, de connexion aux infrastructures de Numih France ou de ses adhérents, etc.).

Les exigences de sécurités sont contenues dans l'annexe « *Exigences sécurité Marché SMS.xlsx* »

Pour chaque exigence, le titulaire doit indiquer s'il est :

- Conforme
- Partiellement conforme
- Non conforme

Et présenter les mesures correspondantes mises en œuvre.

### 8.2 Audits de sécurité techniques

Les services ou produits fournis par le Titulaire devront être accompagnés de rapports d'audit de sécurité.

Numih France pourra réaliser, à ses frais, des audits de sécurité complémentaire des services. Ces audits seront réalisés dans le cadre d'un protocole défini entre les parties et avec un délai de prévenance minimal d'un mois.

Toute vulnérabilité doit être corrigée selon les conditions définies à l'article 9

### 8.3 Incident de sécurité

Toute partie qui a connaissance d'un incident de sécurité impactant ou pouvant impacter le Services et ses données doit en informer l'ensemble des parties prenantes.

Pour tout incident impact les Données à Caractère Personnel, les Délégués à la Protection des Données (DPD) des parties doivent en être informés.

Les contacts Numih France sont [rssi@numihfrance.fr](mailto:rssi@numihfrance.fr) et [dpo@numihfrance.fr](mailto:dpo@numihfrance.fr).

## Article 9. Classification des vulnérabilités et délais de correction

L'échelle ci-après suit le Common Vulnerability Scoring System ([CVSS](#)).  
Les délais de correction sont adaptés pour un service en production.

Criticité	Définition	Délai de correction
Négligeable	<b>Non considéré comme une vulnérabilité ou dont le score est inférieur à 1,9</b> Point que l'auditeur a souhaité relever, ou risque négligeable	À intégrer dans la prochaine évolution du périmètre concerné (soumis à validation de l'éditeur)
Faible	<b>Concerne tous les scores compris entre 2 et 3.9</b> Tous les risques de sécurité représentant une menace faible pour le système audité	À intégrer dans la prochaine évolution du périmètre concerné
Moyen	<b>Concerne tous les scores compris entre 4 et 6.9</b> Tous les risques de sécurité représentant une menace pouvant conduire à la récolte d'informations sensibles.	Selon analyse effectuée, dans les 3 mois en moyenne
Élevée	<b>Concerne tous les scores compris entre 7 et 8.9</b> Tous les risques de sécurité représentant une menace significative pour la sécurité. L'attaquant ne possède pas les accès complets sur le système audité. Des informations très sensibles sont compromises.	10 à 30 jours
Critique	<b>Concerne tous les scores supérieurs à 9</b> Risque critique pour le système d'information et nécessitant une correction immédiate ou imposant en arrêt immédiat du service.	5 à 10 jours